www.mruni.eu

Sigutė STANKEVIČIŪTĖ

DAKTARO DISERTACIJA

ASMENS DUOMENŲ RINKIMO ELEKTRONINĖJE ERDVĖJE TEISĖSAUGOS IR ŽVALGYBOS TIKSLAIS REGLAMENTAVIMAS

SOCIALINIAI MOKSLAI,
TEISĖ (S 001)
VILNIUS, 2020

MYKOLO ROMERIO UNIVERSITETAS

MYKOLO ROMERIO UNIVERSITETAS

Sigutė Stankevičiūtė

ASMENS DUOMENŲ RINKIMO ELEKTRONINĖJE ERDVĖJE TEISĖSAUGOS IR ŽVALGYBOS TIKSLAIS REGLAMENTAVIMAS

Daktaro disertacija
Socialiniai mokslai, teisė (S 001)

Vilnius, 2020

Daktaro disertacija rengta 2013–2019 metais, ginama Mykolo Romerio universitete pagal Mykolo Romerio universitetui su Vytauto Didžiojo universitetu Lietuvos Respublikos švietimo, mokslo ir sporto ministro 2019 m. vasario 22 d. įsakymu Nr. V-160 „Dėl doktorantūros teisės suteikimo“ suteiktą doktorantūros teisę.

Mokslinis vadovas:
prof. dr. Vidmantas Egidijus Kurapka (Mykolo Romerio universitetas, socialiniai mokslai, teisė, S 001).

PAGRINDINIAI SUTRUMPINIMAI

108 Konvencija	1981 m. yra Europos Tarybos 1981 m. Konvencija dėl asmenų apsaugos ryšium su asmens duomenų automatizuotu tvarkymu
Angl.	Anglų kalba
AOTD	Antrasis operatyvinių tarnybų departamentas prie Krašto apsaugos ministerijos
Asmens duomenų apsaugos pamatinis sprendimas	Europos Tarybos Pamatinis Sprendimas Nr. 2008/977/TVR „Dėl asmens duomenų, tvarkomų vykdant policijos ir teisminį bendradarbiavimą baudžiamosiose bylose, apsaugos“
BDAR arba Bendrasis asmens duomenų apsaugos reglamentas	2016 m. balandžio 27 d. Europos Parlamento ir Tarybos reglamentas (ES) 2016/679 dėl fizinių asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo ir kuriuo panaikinama Direktyva 95/46/EB
BK	Lietuvos Respublikos baudžiamasis kodeksas
BPK	Lietuvos Respublikos baudžiamojo proceso kodeksas
Direktyva dėl privatumo ir elektroninių ryšių	Europos Parlamento ir Tarybos 2002 m. liepos 12 d. 2002/58/EB Direktyva dėl asmens duomenų tvarkymo ir privatumo apsaugos elektroninių ryšių sektoriuje
Direktyva Nr. 95/46 arba 1995 m. asmens duomenų apsaugos direktyva	1995 m. spalio 24 d. Europos Parlamento ir Tarybos direktyva 95/46/EB dėl asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo
Duomenų saugojimo direktyva	2006 m. kovo 15 d. Europos Parlamento ir Tarybos direktyvoje 2006/24/EB dėl duomenų, generuojamų arba tvarkomų teikiant viešai prieinamas elektroninių ryšių paslaugas arba viešuosius ryšių tinklus, saugojimo
ECPA	Komunikacijos elektroninėje erdvėje privatumo aktas (angl. *Electronic Communication Privacy Act*)
EĮPO	Europos įrodymų pateikimo orderis
EĮSO	Europos įrodymų saugojimo orderis
EK	Europos Komisija
El. erdvė	Elektroninė erdvė
EO 12333	Vykdomasis nurodymas 12333 (angl. *Executive Order 12333*)
ES	Europos Sąjunga
ESTT	Europos Sąjungos Teisingumo Teismas
ET	Europos Taryba

ET Rekomendacijos arba Rekomendacijos	Tarybos dokumentu yra Europos Tarybos Ministrų Komiteto 1987 m. rugsėjo 17 d. Rekomendacijos Nr. R(87)15 valstybėms narėms dėl asmens duomenų naudojimo policijos sektoriuje
EŽTK	Europos žmogaus teisių ir pagrindinių laisvių apsaugos konvencija
EŽTT	Europos žmogaus teisių teismas
FISA	Užsienio žvalgybos elektroninėje erdvėje aktas (angl. *Foreign Intelligence Surveillance Act*)
FISA apeliacinis teismas	Užsienio žvalgybos el. erdvėje apeliacinis teismas (angl. *Foreign intelligence surveillance court of review (FISA court of review*)
FISA teismas	Užsienio žvalgybos el. erdvėje teismas (angl. *Foreign intelligence surveillance court (FISA court)*)
JAV	Jungtinės Amerikos Valstijos
Konstitucija	Lietuvos Respublikos Konstitucija
Kt.	Kita
LAT	Lietuvos Aukščiausiasis Teismas
MTEP	Moksliniai tyrimai ir eksperimentinė plėtra
NSA	Jungtinių Amerikos Valstijų Nacionalinio saugumo agentūra (angl. *National Security Agency*)
PNR direktyva	2016 m. balandžio 27 d. Europos Parlamento ir Tarybos direktyva (ES) 2016/681 dėl keleivio duomenų įrašo (PNR) duomenų naudojimo teroristinių nusikaltimų ir sunkių nusikaltimų prevencijos, nustatymo, tyrimo ir patraukimo už juos baudžiamojon atsakomybėn tikslais
SCA	Saugomos komunikacijos aktas (angl. *Stored Communications Act)*
t. t.	taip toliau
Teisėsaugos tikslais tvarkomų asmens duomenų apsaugos direktyva	Europos Parlamento ir Tarybos direktyva dėl fizinių asmenų apsaugos kompetentingoms institucijoms tvarkant asmens duomenis nusikalstamų veikų prevencijos, tyrimo, nustatymo ar traukimo baudžiamojon atsakomybėn už jas arba baudžiamųjų sankcijų vykdymo tikslais ir dėl laisvo tokių duomenų judėjimo
VSD	Valstybės saugumo departamentas
Žr.	Žiūrėti

TURINYS

ĮVADAS

Temos aktualumas. Elektroninė erdvė buvo sukurta siekiant dalintis duomenimis[1], ne juos saugoti[2]. Kas tada turėtų asmens duomenis saugoti? Asmens duomenų šaltinis – žmogus – neturi galimybių apsaugoti savo duomenų, kadangi jų valdytojais yra paslaugas el. erdvėje teikiantys juridiniai asmenys, o naudotojais – ne tik pats paslaugų teikėjas, bet ir kiti juridiniai asmenys, teisėsaugos ir žvalgybos institucijos. Teiginys, kad asmens duomenys yra XXI a. nafta[3] yra vartojamas dažnai. Tačiau, jeigu paklaustumėme visuomenės kaip mūsų asmens duomenys generuoja paslaugas elektroninėje erdvėje teikiančioms įmonėms pelną, didesnį už valstybių nacionalinius biudžetus[4], paaiškinimo iš statistinio, išsilavinimo šioje srityje neturinčio ir joje nedirbančio, asmens negautumėme. Nors dėka Europos Sąjungos (toliau – ES) asmens duomenų apsaugos reformos dalis asmenų žino, kad jie turi teisę į asmens duomenų apsaugą. Tačiau priešprieša šiam žinojimui yra teiginys „aš neturiu ko slėpti“. Todėl visuomenei susidaro įspūdis, kad iš el. erdvės tapimo kiekvieno iš mūsų gyvenimo neatsiejama dalimi, nauda ir tenka tik mums patiems, nes gauname paslaugas, o įsigaliojus Bendrajam asmens duomenų reglamentui dar ir galime kontroliuoti savo asmens duomenų judėjimą[5]. Iš tikrųjų dėl mūsų naudojimosi el. erdve nauda tenka tiek mums paslaugas teikiančioms įvairių sričių įmonėms (elektroninių ryšių tiekėjai, socialinių tinklų teikėjai, mobiliųjų įrenginių kūrėjai, reklamos paslaugų teikėjai ir kt.) ir valstybinėms institucijoms. JAV kurdama internetą neplanavo, jog civilis jo panaudojimas sugražins prie jo kūrimo ištakų – el. erdvės naudojimo nacionalinio saugumo užtikrinimo tikslais. Pastarųjų metų asmens duomenų nutekinimo skandalai JAV[6], noras vykdyti masinį asmenų stebėjimą kovos su COVID-19 tikslais[7] rodo, kad nauda valstybėms iš masinio asmenų naudojimosi el. erdve pasireiškia per masinį asmens duomenų naudojimą ne tik verslo, bet ir valstybės poreikių tenkinimui, dažniausiai teisėsaugos ir žvalgybos tikslais. Taigi, kas turėtų saugoti mūsų

---

1 Elektroninė erdvė yra JAV užsakymu vykdytų mokslinių tyrimų kariniais tikslais rezultatas šiandien visuomenės plačiai naudojamas dėl to, kad JAV mokslinių tyrimų rezultatus išslaptino, o verslo subjektai rado būdą kaip iš el. erdvės gauti pelną ją pritaikant visuomenės poreikiams. Plačiau apie tai žr. https://www.history.com/news/who-invented-the-internet.

2 John R. Vacca, *Computer and Information Security Handbook* (Morgan Kaufmann, 2009), 4.

3 „The World's Most Valuable Resource Is No Longer Oil, but Data“, *The Economist*, žiūrėta 2020 m. rugpjūčio 30 d., https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data.

4 Milan Babic, Jan Fichtner ir Eelke M. Heemskerk, „States versus Corporations: Rethinking the Power of Business in International Politics“, *The International Spectator* 52, no. 4 (2017): 20–43, doi:10.1080/03932729.2017.1389151. Darius Mikutavičius, „„Microsoft“ vertė pirmą kartą pasiekė trilijono dolerių ribą“, *lrt.lt*, žiūrėta 2020 m. rugpjūčio 30 d., https://www.lrt.lt/naujienos/mokslas-ir-it/11/1052527/microsoft-verte-pirma-karta-pasieke-trilijono-doleriu-riba.

5 „What Are the Advantages of the Internet?“, *Computer Hope*, žiūrėta 2020 m. rugpjūčio 30 d., https://www.computerhope.com/issues/ch001808.htm.

6 „NSA Collecting Phone Records of Millions of Verizon Customers Daily“, *The Guardian*, žiūrėta 2020 m. rugpjūčio 30 d., https://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order.

7 „9/11 Saw Much of Our Privacy Swept aside. Coronavirus Could End It Altogether“, *CNN*, žiūrėta 2020 m. rugpjūčio 30 d., https://edition.cnn.com/2020/05/16/tech/surveillance-privacy-coronavirus-npw-intl/index.html.
„The Price Of Covid-19 Freedom May Be Eternal Spying“, Bloomberg, žiūrėta 2020 m. rugpjūčio 30 d., https://www.bloombergquint.com/view/coronavirus-contact-tracing-apps-mean-spying-end-to-data-privacy.

asmens duomenis, jei pati el. erdvė to nedaro? Vienas iš apsaugos mechanizmų turėtų būti teisinis reglamentavimas.

Teisės į asmens duomenų apsaugą galiojimu teisėsaugos ir žvalgybos institucijoms asmens duomenis renkant elektroninėje erdvėje klausimu pradėjau domėtis daugiau nei metams likus E. Snowden informacijos apie masinį asmens duomenų rinkimą nutekinimo. Praėjo septyni metai, tačiau ši tema iki šiol išliko aktuali, kadangi ji liečia du lygiaverčius visuomenės interesus – žmogaus teisės į asmens duomenų apsaugą užtikrinimą elektroninėje erdvėje ir tos teisės atsisakymo, iš pirmo žvilgsnio, vardan apsaugos nuo dar didesnės grėsmės – terorizmo, nusikalstamumo ir pavojaus nacionaliniam saugumui. Tačiau riba tarp teisių suvaržymo vardan didesnių vertybių apsaugos nepažeidžiant pačios didžiausios vertybės – demokratijos – yra labai trapi. Tokius mokslininkų nuogąstavimus galime pamatyti pvz. profesorės, JAV elektroninės žvalgybos teismo patariamojo organo Amici Curia narės L. K. Donohue knygoje, kurioje autorė iškelia hipotezę, kad JAV vykdomas masinis asmens duomenų rinkimas elektroninėje erdvėje yra analogiškas XIII a. galiojusiai antikonstitucine pripažintai teisei Karūnos įgaliotiems asmenims bent kada įsibrauti į bent kurio iš Didžiosios Britanijos valdose esančio asmens namus[8]. Nepaisant mokslininkų ir visuomeninių judėjimų nuo 2013 m. akcentuojamos grėsmės teisės asmens duomenų apsaugą užtikrinime šiuos duomenis teisėsaugos ir žvalgybos institucijoms renkant el. erdvėje, esminių pokyčių teisės aktuose kol kas neįvyko.

Šiuo metu egzistuoja du demokratijos užtikrinimo teisėsaugos ir žvalgybos institucijoms renkant asmens duomenis el. erdvėje užtikrinimo mechanizmai, pasireiškiantys teisės į asmens duomenų apsaugą suteikimu arba išsamiu asmens duomenų rinkimo elektroninėje erdvėje teisėsaugos ir žvalgybos tikslais reglamentavimu. Pirmasis modelis yra taikomas Europoje, antrasis – JAV. Pirmasis – Europos modelis – pasižymi tuo, kad asmeniui įtvirtinama teisė į asmens duomenų apsaugą, tačiau asmens duomenų rinkimas teisėsaugos ir žvalgybos tikslais teisės aktuose yra reglamentuojamas padrikai. Antrasis – JAV modelis – pasižymi tuo, kad teisė į asmens duomenų apsaugą, kaip tokia, nėra tiesiogiai suteikiama, tačiau asmens duomenų rinkimas elektroninėje erdvėje teisėsaugos ir žvalgybos tikslais yra detaliai reglamentuojamas specialiais įstatymais, bei yra įsteigti specialūs teismai teisėsaugos ir žvalgybos asmens duomenų rinkimo elektroninėje erdvėje prašymų sankcionavimui ir su tuo susijusių bylų nagrinėjimui. Kadangi JAV ir Europos supranacionalinis asmens duomenų rinkimo el. erdvėje teisėsaugos ir žvalgybos tikslais reglamentavimas įtakoja viso likusio pasaulio valstybių teisinius reglamentavimus, įskaitant Lietuvą, todėl JAV ir Europos supranacionalinės teisės teisinio reglamentavimo analizė yra disertacijos uždaviniais.

Ištirtumas. Asmens duomenų rinkimas el. erdvėje teisėsaugos ir žvalgybos tikslais mokslinių tyrimų objektu tapo dėl teisės į privatumą, vėliau peraugusios į teisę į asmens duomenų apsaugą, apimties išplėtimo iš fizinės aplinkos į el. erdvę. Klausimas kaip užtikrinti pusiausvyrą tarp teisėsaugos ir žvalgybos institucijų poreikio rinkti

[8] Laura K. Donohue, *The Future of Foreign Intelligence: Privacy and Surveillance in a Digital Age*, 1 edition (New York: Oxford University Press, 2016), 76.

asmens duomenis el. erdvėje ir asmens teisės į asmens duomenų apsaugą įgyvendinimo yra dažnai keliamas[9], bet iki šiol neatsakytas. Kadangi informacija apie asmens duomenų rinkimą el. erdvėje teisėsaugos ir žvalgybos tikslais nėra viešai prieinama, todėl šios srities mokslinius tyrimus įtakoja keli faktoriai: mokslininko geografinė lokacija ir su asmens duomenų apsauga susiję viešai žinomi reikšmingi įvykiai. Europos mokslininkų susidomėjimui asmens duomenų apsauga žvalgybos ir teisėsaugos srityje įtaką darė į viešumą nutekinama informacija apie asmens duomenų rinkimo mastus ir vykdomas programas. Tai skatino ir įstatymų leidybos procesus. Pirmoji didesnio susidomėjimo banga buvo 2013 m. po buvusio JAV Nacionalinės žvalgybos agentūros (NSA) kontraktoriaus E. Snowden paviešintos informacijos apie PRISM programą[10]. Siekiant surasti asmens duomenų apsaugos būdus ir nustatyti *privacy by design* principo panaudojimo galimybes teisėsaugos veikloje buvo pradėti vykdyti keli EK finansuojami tarptautiniai Septintosios bendrosios programos mokslinių tyrimų projektai[11], atsirado mokslinių publikacijų, visų pirma Oksfordo ir Harvardo universitetų profesorių[12], apie teisinės asmens duomenų apsaugos reikšmę ir ypatybes, EK užsakymu jungtinė ES mokslininkų grupė parengė apžvalginę studiją apie privatumo apsaugą JAV[13]. Antroji didesnio susidomėjimo banga buvo Europos Sąjungos Teisingumo Teismui (toliau – ESTT) „Saugaus uosto“ principą pripažinus neužtikrinančiu teisinės asmens duomenų apsaugos dėl JAV žvalgybos institucijų galimybės naudoti šiuos asmens duomenis[14]. Tuo metu dauguma mokslininkų analizavo teismo sprendimą ir tolimesnius ES veiksmus. Nors, kaip matysime toliau disertacijoje, JAV žvalgybos institucijos teisiškai gali rinkti asmens duomenis net nesančius JAV, todėl „Saugaus uosto“ principo panaikinimas neišsprendžia tikrosios problemos. Tai rodo mokslinių tyrimų siaurumą ir platesnio pobūdžio tyrimų reikalingumą. Na ir trečioji mokslininkų domėjimosi asmens duomenų apsauga banga yra susijusi su 2018 m. ES

---

[9] Jing Ran, „Striking the Balance between Privacy and Governance in the Age of Technology“, 11 (2016): 20.

[10] „NSA Collecting Phone Records of Millions of Verizon Customers Daily“, *The Guardian*, žiūrėta 2020 m. rugpjūčio 30 d., https://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order.

[11] „Supporting fundamental rights, PrIvacy and Ethics in surveillaNce Technologies“, *Cordis*, žiūrėta 2020 m. rugpjūčio 30 d., https://cordis.europa.eu/project/id/261698.

[12] Pvz., H Akın Ünver, „Politics of Digital Surveillance, National Security and Privacy“, 23, žiūrėta 2020 m. rugpjūčio 30 d., https://edam.org.tr/wp-content/uploads/2018/04/Chrest_Surveillance2.pdf. Clive Norris ir kt., *The Unaccountable State of Surveillance: Exercising Access Rights in Europe*, Issues in Privacy and Data Protection (Springer International Publishing, 2017), doi:10.1007/978-3-319-47573-8. Aaron Nance, „Taking the Fear Out of Electronic Surveillance in the New Age of Terror Note“, *UMKC Law Review* 70, Nr. 3 (2002 2001): 751–80. „Electronic Surveillance Recent Legislation“, *Harvard Law Review* 122, no. 4 (2009 2008): 1271–78. David S. Kris, „The Rise and Fall of the FISA Wall Symposium – Spies, Secrets, and Security: The New Law of Intelligence: The Foreign Intelligence Surveillance Act“, *Stanford Law & Policy Review* 17, no. 2 (2006): 487–530. Laura K. Donohue, „FISA Reform“, *I/S: A Journal of Law and Policy for the Information Society* 10, no. 2 (2015 2014): 599–640. Stephen I. Vladeck, „The FISA Court and Article III Cybersurveillance in the Post-Snowden Age“, *Washington and Lee Law Review* 72, no. 3 (2015): 1161–80. William C. Banks, „The Death of FISA Symposium – 9/11 Five Years On: A Look at the Global Response to Terrorism“, *Minnesota Law Review* 91, no. 5 (2007 2006): 1209–1301.

[13] Francesca Bignami, „The US legal system on data protection in the field of law enforcement. Safeguards, rights and remedies for EU citizens“, *European Parlament*, žiūrėta 2020 m. rugsėjo 10 d., https://www.europarl.europa.eu/thinktank/en/document.html?reference=IPOL_STU(2015)519215.

[14] Pvz. Dan Jerker B. Svantesson, „Cross-Border Data Transfers after the CJEU's Safe Harbour Decision: A Tale of Gordian Knots“, *Alternative Law Journal* 41, no. 1 (2016): 39–42.

asmens duomenų apsaugos reforma[15]. Tačiau dauguma trečiosios bangos mokslinių tyrimų yra susiję su komercine teisės į asmens duomenų apsauga puse, kurios įgyvendinimo nuostatos yra įtvirtintos Bendrajame asmens duomenų apsaugos reglamente[16]. Nepriklausomai nuo to, kuriai mokslinių tyrimų bangai priklauso, mokslininkai savo publikacijose analizuoja tik pavienius asmens teisės į asmens duomenų apsaugą žvalgybos ir teisėsaugos veikloje aspektus. Tačiau ši teisė ir jos apribojimo bei galiojimo mechanizmai yra kompleksiniai, todėl ir kompleksiniai tyrimai yra reikalingi.

Didžiausią dalį mokslinių publikacijų apie asmens duomenų rinkimą el. erdvėje teisėsaugos ir žvalgybos tikslais sudaro JAV teisės normų ir teismų precedentų analizė. Mokslinių publikacijų apie reglamentavimą JAV gausa gali būti paaiškinama tuo, kad JAV yra pirmoji pasaulio valstybė asmens duomenų rinkimą el. erdvėje pradėjusi reglamentuoti dar 1968 m., kuomet el. erdvė apėmė tik telefoninius pokalbius ir IV JAV Konstitucijos pataisa įtvirtintą teisę į privatumą iš fizinės aplinkos išplėtusi į el. erdvę. Tuo tarpu Europoje tai buvo padaryta tik 1981 m. ET priėmus Konvenciją dėl asmenų apsaugos ryšium su asmens duomenų automatizuotu tvarkymu, o ET Rekomendacijos dėl asmens duomenų tvarkymo policijos tikslais buvo paskelbtos 1987 m, t. y. 19 metų vėliau nei pirmasis tai reglamentuojantis teisės aktas JAV[17]. JAV tuo metu jau buvo sukurta visa asmens duomenų rinkimo el. erdvėje teisėsaugos ir žvalgybos tikslais teisinė bazė ir ji nuolat tobulinama iki šiol. Nuo pat atsiradimo 1968 m. JAV asmens duomenų rinkimą teisėsaugos ir žvalgybos tikslais reglamentuojantys teisės aktai dažnai buvo teisminių ginčų ir mokslinių diskusijų objektu. Todėl ir mokslinių tyrimų dėl JAV asmens duomenų rinkimo el. erdvėje teisėsaugos ir žvalgybos tikslais, paprastai, susijusiais su teismų sprendimais bylose, yra pakankamai daug. Tačiau JAV mokslininkų tyrimo objektu yra tai, kas svarbu JAV ir liečia JAV asmenų privatumo, ne Europos gyventojų apsaugą, todėl mokslininkai daugiausiai analizuoja Elektroninės komunikacijos privatumo akto (angl. *The Electronic Communications Privacy Act (ECPA)*) nuostatų taikymą[18]. Užsienio žvalgybos elektroninėje erdvėje akto (angl.

---

[15] Pvz. Yi-Hsuan Chen, „EU Data Protection Law Reform: Challenges for Service Trade Liberalization and Possible Approaches for Harmonizing Privacy Standards into the Context of GATS, The", *Spanish Yearbook of International Law* 19 (2015): 211–20. Marija Boban, „Digital Single Market and EU Data Protection Reform with Regard to the Processing of Personal Data as the Challenge of the Modern World The Legal Challenges of Modern World", *Economic and Social Development, 16th International Scientific Conference on Economic and Social Development: The Legal Challenges of Modern World* 16 (2016): 191–201. Marina Skrinjar Vidovic, „EU Data Protection Reform: Challenges for Cloud Computing Notes", *Croatian Yearbook of European Law and Policy* 12 (2016): 171–206.

[16] Julius Zaleskis, *Europos Sąjungos bendrasis duomenų apsaugos reglamentas ir asmens duomenų apsaugos teisė: monografija*, Teisinė literatūra (Vilnius: Registrų centras, 2019).

[17] „Council of Europe Committee of Ministers Recommendation No. R(87) 15 to the Member States on regulating the use of personal data in the police sector", *Osce Polis*, žiūrėta 2020 m. rugsėjo 1 d., https://polis.osce.org/council-europe-committee-ministers-recommendation-no-r87-15-member-states-regulating-use-personal.

[18] Deirdre K. Mulligan, „Reasonable Expectations in Electronic Communications: A Critical Perspective on the Electronic Communications Privacy Act The Future of Internet Surveillance Law: A Symposium to Discuss Internet Surveillance, Privacy & (and) the USA Patriot Act: Surveillance, Records & (and) Computers", *George Washington Law Review* 72, no. 6 (2004 2003): 1557–98. Laura L. Clukey, „The Electronic Communications Privacy Act of 1986: The Impact on Software Communication Technologies Comment", *Software Law Journal* 2, no. 2 (1988 1987): 243–64. Ariana R. Levinson, „Toward a Cohesive Interpretation of the Electronic Communications Privacy Act for the Electronic Monitoring of Employees", *West Virginia Law Review* 114, no. 2 (2012 2011): 461–530. Robert A. Fiatal, „The Electronic Communications Privacy Act: Addressing Today's Technology (Part 1) Legal Digest", *FBI Law Enforcement Bulletin* 57,

Foreign Intelligence Surveillance Act (FISA)) nuostatos yra analizuojamos, tačiau paprastai tik tiek, kiek tai liečia netiesioginį JAV asmenų asmens duomenų rinkimą el. erdvėje, renkant duomenis apie ne JAV asmenis[19]. Informacijos apie Vykdomosios valdžios nurodymą 12 333 (angl. *Executive Order 12 333*) yra itin mažai, mokslinių tyrimų šia tema – taip pat, nors, manoma, kad dabar Vykdomosios valdžios nurodymas (angl. *Executive Order 12 333*) gali būti pagrindinė teisinė masinio asmens duomenų rinkimo el. erdvėje priemonė[20]. Stanfordo universitetas 2013–2014 m. organizavo nuotolinius mokymus apie asmens duomenų rinkimą el. erdvėje teisėsaugos ir žvalgybos tikslais teisinį reglamentavimą JAV, kuriuose dalyvavo ir disertacijos autorė. 2015 m. Thomson Reuters leidykla išleido 2 dalių 2000 puslapių apimties knygą „*The Law of Electronic Surveillance*“[21]. Tai yra pirmoji JAV ir apskritai pasaulyje tokio pobūdžio knyga, kurioje unifikuotai apžvelgiamas teisinis JAV federalinio lygio asmens duomenų rinkimo el. erdvėje reglamentavimas. Tačiau kadangi šios knygos yra skirtos JAV rinkai, todėl ir mokslinis tyrimas yra atliekamas per JAV asmenų teisių apsaugos prizmę. Užsienio žvalgybos elektroninėje erdvėje teisės akto (angl. *Foreign Intelligence Surveillance Act*) nuostatos taikomos ne JAV asmenų atžvilgiu, knygoje apžvelgiamos labai siaurai, Vykdomosios valdžios nurodymas (angl. *Executive Order 12 333*) bei jo taikymo praktika arba asmens duomenų rinkimas vadovaujantis Baudžiamojo proceso kodekso 41 straipsniu, suteikiančiu teisę įsilaužti į bent kurioje pasaulio vietoje esančio bent kokios pilietybės asmens kompiuterį ar kitą įrenginį, iš viso nėra įtraukti į šios knygos turinį ir joje neminimi.

Asmens duomenų rinkimas el. erdvėje vyksta kitaip nei įprastinėje fizinėje aplinkoje. Renkant duomenis el. erdvėje yra neišvengiamas teisėsaugos ir žvalgybos institucijų bendradarbiavimas su verslo ir mokslo subjektais, nes duomenys, dažniausiai, yra renkami ne pačių teisėsaugos ir žvalgybos institucijų, o, jų nurodymu, el. ryšių paslaugų, paslaugų el. erdvėje teikėjų, duomenų brokerių (angl. *data broker*) ar el. žvalgybos paslaugų teikėjų. Duomenų ir literatūros apie teisėsaugos ir žvalgybos institucijų bendradarbiavimą su privačiomis įmonėmis (verslo subjektais), jo formas ir pobūdį yra labai mažai. 2018 m. išleistoje knygoje „Habeas Data: Privacy vs. the Rise of Surveillance Tech“ C. Farivar rašo apie tai, kaip įmonių kuriamos technologijos įtakoja žvalgybos

---

no. 2 (1988): 25–30. Ariana R. Levinson, „Toward a Cohesive Interpretation of the Electronic Communications Privacy Act for the Electronic Monitoring of Employees“, *West Virginia Law Review* 114, no. 2 (2012 2011): 461–530.

[19] William C. Banks, „The Death of FISA Symposium – 9/11 Five Years On: A Look at the Global Response to Terrorism“, *Minnesota Law Review* 91, no. 5 (2007 2006): 1209–1301. David S. Kris, „The Rise and Fall of the FISA Wall Symposium – Spies, Secrets, and Security: The New Law of Intelligence: The Foreign Intelligence Surveillance Act“, *Stanford Law & Policy Review* 17, no. 2 (2006): 487–530.

[20] Mark Jaycox, „A Primer on Executive Order 12333: The Mass Surveillance Starlet“, *Electronic Frontier Foundation*, June 2, 2014, žiūrėta 2020 m. rugsėjo 1 d., https://www.eff.org/deeplinks/2014/06/primer-executive-order-12333-mass-surveillance-starlet. „Reagan-Era Order on Surveillance Violates Rights, Says Departing Aide“, *The New York Times*, žiūrėta 2020 m. rugsėjo 1 d., https://www.nytimes.com/2014/08/14/us/politics/reagan-era-order-on-surveillance-violates-rights-says-departing-aide.html. Barton Gellman ir Ashkan Soltani, „NSA Surveillance Program Reaches 'into the Past' to Retrieve, Replay Phone Calls“, *Washington Post*, March 18, 2014, sec. National Security, https://www.washingtonpost.com/world/national-security/nsa-surveillance-program-reaches-into-the-past-to-retrieve-replay-phone-calls/2014/03/18/226d2646-ade9-11e3-a49e-76adc9210f19_story.html.

[21] James Carr ir Patricia Bellia, *The Law of Electronic Surveillance, 2017-2 Ed.*, 1 dalis, (Clark Boardman Callaghan, 2017).

pajėgumus[22]. Privacy international yra parengusi studiją apie augančią elektroninės žvalgybos paslaugų rinką[23]. Tačiau nė viename darbe nėra vertinamos teisėsaugos, žvalgybos ir verslo subjektų bendradarbiavimo formos ir asmens duomenų apsaugos galimybės bei teisinio reglamentavimo spragos. Atsakymui į šiuos klausimus nusprendžiau skirti paskutinį disertacijos skyrių, kadangi tokio bendradarbiavimo apimtys, pasak ENISA[24], didėja, o reglamentavimo ar bent koordinavimo šioje srityje kol kas nėra.

Lietuvoje mokslinės diskusijos apie asmens duomenų rinkimą el. erdvėje teisėsaugos ir žvalgybos tikslais taip pat yra keliamos. Paminėtini šie Lietuvos mokslininkai analizuojantys susijusias Lietuvos Respublikos kriminalinės žvalgybos įstatymo ir Baudžiamojo proceso kodekso (toliau – BPK) nuostatas: D. Štitilis[25], M. Laurinaitis[26], R. A. Petrauskas[27], R. Ažubalytė[28], G. Goda[29], A. Gutauskas[30], R. Jurka[31], L. Belevičiaus[32], P. Pakutinskas[33], A. Panomariovas ir R. Ramanauskas[34], P. Tarasevičius[35],

---

22 Cyrus Farivar, *Habeas Data: Privacy vs. the Rise of Surveillance Tech* (Brooklyn: Melville House, 2018).2018

23 „The Global Surveillance Industry", Privacy International, žiūrėta 2020 m. rugpjūčio 30 d., https://www.privacyinternational.org/sites/default/files/2017-12/global_surveillance_0.pdf.

24 Catherine Stupp, „EU agency asks Commission to 'avoid fragmentation' in new cyber security plans", *Euractive*, žiūrėta 2020 m. rugsėjo 1 d., http://www.euractiv.com/section/cybersecurity/news/eu-agency-asks-commission-to-avoid-fragmentation-in-new-cybersecurity-plans/

25 Darius Štitilis, „Elektroninių ryšių kontrolės nusikaltimų tyrimo tikslias teisiniai aspektai", *Informacijos mokslai : mokslo darbai* 34 (2005): 103–110. Rimantas Alfonsas Petrauskas ir Darius Štitilis, „Monitoring Electronic Communications: Privacy Issues", *Monitoring, Supervision and Information Technology : Proceedings of the First International Seminar of the Legal Framework for the Information Society (LEFIS) on Monitoring, Supervision and Information Technology, 15 June 2006, Rotterdam*, 2006, 5–20. Darius Štitilis ir Marius Laurinaitis, „IP telefonija – iššūkis elektroninių ryšių kontrolės, siekiant ištirti nusikaltimus, teisiniam reguliavimui", *Socialinių mokslų studijos*, no. 1 (2009): 205–221.

26 Darius Štitilis ir Marius Laurinaitis, „IP telefonija – iššūkis elektroninių ryšių kontrolės, siekiant ištirti nusikaltimus, teisiniam reguliavimui", *Socialinių mokslų studijos*, no. 1 (2009): 205–221.

27 Rimantas Alfonsas Petrauskas ir Darius Štitilis, „Monitoring Electronic Communications: Privacy Issues", *Monitoring, Supervision and Information Technology : Proceedings of the First International Seminar of the Legal Framework for the Information Society (LEFIS) on Monitoring, Supervision and Information Technology, 15 June 2006, Rotterdam*, 2006, 5–20.

28 Rima Ažubalytė, „Privataus asmens gyvenimo ribojimas slaptomis priemonėmis: (ne)kokybiško įstatymo problema", *Jurisprudencija* 26, no. 2 (2019): 260–291, doi:10.13165/JUR-19-26-2-02. Rima Ažubalytė, „Baudžiamojo proceso principai: teisės spragų šalinimas", *Lietuvos Respublikos baudžiamojo proceso kodeksui – 10 metų: recenzuotų mokslinių straipsnių, skirtų Lietuvos ir užsienio šalių baudžiamojo proceso, baudžiamosios teisės ir kriminalistikos aktualijoms ir problematikai, rinkinys*, 2012, 13–34

29 Gintaras Goda, „Procesinių prievartos priemonių Lietuvos Respublikos baudžiamojo proceso kodekso projekte samprata, klasifikacija ir turinys", *Teisė*, (2000): 17–27. Gintaras Goda, *Vertybiniai prioritetai baudžiamajame procese: monografija*, (Vilnius: Registrų centras, 2014).

30 Aurelijus Gutauskas, „Kriminalinė žvalgyba ir privatus žmogaus gyvenimas", *Teisė* 113 (2019): 8–26, doi:10.15388/Teise. 2019.113.1.

31 Raimondas Jurka, „Įrodymų perdavimo Europos Sąjungos valstybių narių baudžiamojoje justicijoje iššūkiai ir atradimai", *Jurisprudencija,* (2019, 26(2)), 322.

32 Linas Belevičius, „Techninių priemonių panaudojimo tiriant nusikaltimus teisinis reglamentavimas", *Jurisprudencija : mokslo darbai* 29 (2002): 72–85.

33 Paulius Pakutinskas, „Elektroninių komunikacijų teisinio reguliavimo modeliai", (daktaro disertacija, Mykolo Romerio universitetas, 2009).

34 Artūras Panomariovas ir Ramūnas Ramanauskas, „Slaptumas – tiesos baudžiamajame procese nustatymo priemonė", *Jurisprudencija : mokslo darbai*, no. 75 (2005): 50–57.

35 Petras Tarasevičius, „Techninių priemonių naudojimo kriminalinėje žvalgyboje teisėtumo problemos", *Teisė*, 2017, 84–99, doi:10.15388/Teise.2017.105.11114.

R. Marcinauskaitė[36], M. Civilka ir L. Šlapimaitė[37], J. Dešriūtė[38]. Lietuvos mokslininkai moksliniuose straipsniuose analizuoja privataus gyvenimo ribojimo elektroniniuose ryšiuose ir IP telefonijose siekiant ištirti nusikaltimus teisinio reglamentavimo ypatumus Lietuvoje. Autorės disertacijoje asmens duomenų rinkimo el. erdvėje teisėsaugos ir žvalgybos tikslais reglamentavimo Lietuvoje analizė yra paremta palyginimu su JAV teisiniu reglamentavimu ir teismų praktika. Disertacijoje taip pat yra apžvelgiamos teisinės prisijungimų prie elektroninės erdvės prielaidos (angl. *Government Hacking*) Lietuvos Respublikos kriminalinės žvalgybos įstatyme ir BPK. R. Ažubalytė moksliniame straipsnyje analizuoja kaip Lietuvos teismai privalo spręsti BPK ir Kriminalinės žvalgybos įstatymo spragas dėl asmens duomenų rinkimo el. erdvėje. Disertacijoje atlikta JAV teisės aktų ir teismų precedentų istorinė analizė parodė, kad analogiška situacija buvo ir yra JAV (2.2. disertacijos poskyris). Pirmasis pasaulyje asmens duomenų rinkimą el. erdvėje reglamentuojantis teisės aktas 1968 m. atsirado kaip 1967 m. JAV Aukščiausiojo Teismo sprendimo byloje *Berger v. New York* rezultatas. Disertacijoje atlikta istorinė JAV teismų sprendimų ir teisės aktų genezės analizė gali būti reikšminga Lietuvos Respublikos teismams, kadangi jiems šiuo metu tenka spręsti labai panašias problemas, kurias sprendė ir JAV teismai. A. Gutauskas moksliniame straipsnyje analizuoja kiek kriminalinės žvalgybos naudojamos priemonės gali teisėtai skverbtis į privatų žmogaus gyvenimą[39]. P. Pakutinsko daktaro disertacija „Elektroninių komunikacijų teisinio reguliavimo modeliai“[40] yra artimiausia autorės disertacijai. P. Pakutinskas disertacijoje analizavo elektroninių komunikacijų teisinio reguliavimo modelius, tačiau jo disertacija neapima asmens duomenų teisinės apsaugos klausimų[41], kurie yra šios disertacijos objektu.

Mokslinis naujumas ir reikšmė. Disertacijoje yra pirmasis mokslinis darbas, kuriame istoriniu ir lyginamuoju metodu yra analizuojamos bendrosios (JAV) ir kontinentinės teisės (Lietuvos) tradicijų šalių bei supranacionalinio lygmens (ET ir ES) asmens duomenų rinkimo el. erdvėje teisėsaugos ir žvalgybos tikslais teisinio reglamentavimo ypatumai dėl teisės į asmens duomenų apsaugą užtikrinimo. Nors JAV reglamentavimas taip turi trūkumų (pvz. vienas iš jų – JAV teisės aktais siekiama užtikrinti tik JAV piliečių ar nuolatinių gyventojų teisę į asmens duomenų apsaugą, kiti asmenys ar jų asmens duomenys teisės į asmens duomenų apsaugą JAV jurisdikcijoje neturi, todėl JAV vykdomos ne JAV asmenų masinio asmens duomenų rinkimo programos yra teisėtos JAV teisės aktų atžvilgiu), tačiau dar 1968 m. buvo priimtas pirmasis teisės aktas, skirtas šios srities reglamentavimui, ir nuo to laikotarpio vis priimami nauji arba pataisomi galiojantys teisės aktai, o teismų vaidmuo teisėkūroje yra aktyvus.

---

[36] Renata Marcinauskaitė, „Nusikalstamos veikos elektroninėje erdvėje“, (daktaro disertacija, Mykolo Romerio universitetas).

[37] Mindaugas Civilka ir Lina Šlapimaitė, „Asmens duomenų samprata elektroninėje erdvėje“, *Teisė*, 96 (2015): 126–148.

[38] Justina Dešriūtė, „Esminiai asmens duomenų apsaugos baudžiamajame procese reformos Europos Sąjungoje aspektai ir jų įtaka nacionaliniam teisiniam reguliavimui“, *Teisės problemos*, 1 (91), (2016): 25–51.

[39] Aurelijus Gutauskas, „Kriminalinė žvalgyba ir privatus žmogaus gyvenimas“, *Teisė* 113 (2019): 8–26, doi:10.15388/Teise.2019.113.1.

[40] Petras Tarasevičius, „Techninių priemonių naudojimo kriminalinėje žvalgyboje teisėtumo problemos“, *Teisė*, 2017, 84–99, doi:10.15388/Teise.2017.105.11114.

[41] Paulius Pakutinskas, „Elektroninių komunikacijų teisinio reguliavimo modeliai“, (daktaro disertacija, Mykolo Romerio universitetas, 2009), 7.

Tyrimo rezultatai rodo, kad ES ir ET teisės įtaka asmens duomenų apsaugai kuomet jie yra renkami el. erdvėje teisėsaugos ir žvalgybos tikslais yra minimali ir daugiausiai pasireiškia tik per šios teisės suteikimą asmenims ir teismų interpretavimą dėl apribojimų teisėtumo ir pagrįstumo, todėl seniausias teisinio reglamentavimo ištakas turinčių JAV teisės normų ir teismų praktikos istorinė analizė bei palyginimas su teisiniu reglamentavimu Lietuvoje ir gerosios teisinio reglamentavimo patirties perėmimas butų naudingas Lietuvos teisės aktų tobulinimui.

Tyrimo objektas. Asmens duomenų rinkimo elektroninėje erdvėje teisėsaugos ir žvalgybos tikslais teisinis reglamentavimas.

Disertacijos **mokslinė problema** formuluojama keliant tokius klausimus:

1. Kaip reglamentuoti asmens duomenų rinkimą elektroninėje erdvėje teisėsaugos ir žvalgybos tikslais Lietuvos teisės aktuose, kad būtų užtikrinama teisė į asmens duomenų apsaugą?
2. Kokie asmens duomenų rinkimo elektroninėje erdvėje teisėsaugos ir žvalgybos tikslais reglamentavimo JAV ir kitų šalių gerosios praktikos elementai galėtų būti adaptuoti Lietuvos teisės aktuose?
3. Kaip ES ir ET asmens duomenų rinkimo elektroninėje erdvėje teisėsaugos ir žvalgybos tikslais teisinis reglamentavimas įtakoja teisinę praktiką Lietuvoje?
4. Kodėl ir kaip asmens duomenų rinkimo elektroninėje erdvėje teisėsaugos ir žvalgybos tikslais reglamentavimas JAV apriboja Lietuvos gyventojų teisės į asmens duomenų apsaugą ir privatumą įgyvendinimą?
5. Kaip teisėsaugos ir žvalgybos institucijų bendradarbiavimas su privačiais juridiniais asmenimis dėl asmens duomenų rinkimo elektroninėje erdvėje įtakoja teisės į asmens duomenų apsaugą įgyvendinimą?

Tikslas. Ištirti teisinio asmens duomenų rinkimo elektroninėje erdvėje teisėsaugos ir žvalgybos tikslais teisinio reglamentavimo ypatumus bei išskirti gerosios praktikos pavyzdžius pagal kuriuos būtų galima tobulinti Lietuvos teisės aktus.

Uždaviniai:

1. Įvertinti asmens duomenų rinkimo elektroninėje erdvėje teisėsaugos ir žvalgybos tikslais reglamentavimą bendrosios teisės tradicijos valstybėje (JAV atvejis) ir išskirti gerąją praktiką, naudotiną teisiniame reglamentavime Lietuvoje;
2. Įvertinti asmens duomenų rinkimo elektroninėje erdvėje teisėsaugos ir žvalgybos tikslais reglamentavimą supranacionaliniu lygmeniu (Europos atvejis);
3. Nustatyti ir įvertinti asmens duomenų rinkimo el. erdvėje teisėsaugos ir žvalgybos tikslais teisinio reglamentavimo santykį su teise į asmens duomenų apsaugą kontinentinės teisės tradicijos valstybėje (Lietuvos atvejis);
4. Identifikuoti dispozityvaus teisėsaugos, žvalgybos institucijų ir privačių juridinių asmenų bendradarbiavimo formas ir įvertinti probleminius teisės į asmens duomenų apsaugą aspektus;
5. Atsižvelgiant į nustatytus gerosios praktikos pavyzdžius parengti asmens duomenų rinkimo elektroninėje erdvėje teisėsaugos ir žvalgybos tikslais reglamentavimo Lietuvoje tobulinimo pasiūlymus.

Ginamieji teiginiai:

1. Asmens duomenų rinkimo el. erdvėje teisėsaugos ir žvalgybos tikslais reglamentavimas Lietuvos Respublikos teisės aktuose įtvirtinant specialiąsias normas tik dėl komunikacijos turinio rinkimo realiuoju laiku, istorinio pobūdžio asmens duomenų rinkimą ir teisėtą prisijungimą prie elektroninių ryšių įrenginių reglamentuojant kitų procesinių veiksmų atlikimui skirtomis normomis, neužtikrina teisės į asmens duomenų apsaugą teisėtam apribojimui keliamų reikalavimų.
2. Lietuvos teisės aktuose adaptavus JAV praktiką dėl istorinio pobūdžio asmens duomenų rinkimo el. erdvėje teisėsaugos ir žvalgybos tikslais bei JAV, Vokietijos, Didžiosios Britanijos, Lenkijos, Italijos, Nyderlandų ir Prancūzijos gerąją praktiką dėl teisėto prisijungimo prie elektroninės erdvės įrenginių reglamentavimo BPK ir Kriminalinės žvalgybos įstatymo nuostatos taptų aiškios ir tiksliau apibrėžtos, atitiktų EŽTK, Europos Sąjungos pagrindinių teisių chartijoje ir Lietuvos Respublikos Konstitucijoje įtvirtintiems teisėtiems teisės į asmens duomenų apsaugą apribojimų pagrindams.
3. ES ir ET lygiu asmens duomenų rinkimo teisėsaugos ir žvalgybos tikslais reglamentavimas šiuo metu pasireiškia tik bendrojo pobūdžio teisės į asmens duomenų apsaugą suteikimu, kuri EŽTT ir ESTT praktika yra išplečiama į el. erdvę. EŽTT ir ESTT praktika Lietuvos teismai vadovaujasi vertindami teisės į asmens duomenų apsaugos suvaržymo būtinumą, tačiau Lietuvos teisės aktai tik dalinai atitinka EŽTT praktiką dėl teisės į asmens duomenų apsaugą apribojančio įstatymo aiškumo, apribojimo proporcingumo ir sankcionavimo būtinumo.
4. JAV teisės aktuose įtvirtintas asmens duomenų rinkimo teisėsaugos ir žvalgybos tikslais reglamentavimas asmens duomenų apsaugą garantuoja tik JAV asmenims, todėl JAV žvalgybos tikslais Lietuvos gyventojų asmens duomenys gali būti teisėtai renkami vadovaujantis FISA ir EO 12 333 teisės aktų nuostatomis nepriklausomai nuo pačio asmens fizinės buvimo vietos Lietuvos Respublikoje.
5. Teisėsaugos ir žvalgybos institucijoms asmens duomenis elektroninėje erdvėje renkant dispozityvios, viešai neskelbiamos bendradarbiavimo su privačiais juridiniais asmenimis sutarties pagrindu, teisės į asmens duomenų apsaugą įgyvendinimas priklauso nuo šalių pasirenkamos sutarčiai taikytinos teisės ir asmens duomenų apsaugos nuostatų buvimo ar nebuvimo. Toks asmens duomenų rinkimo pagrindas sudaro sąlygas piktnaudžiauti teisės į asmens duomenų apsaugą suvaržymu.

Metodologija. Disertacijos tikslui pasiekti ir uždaviniams įgyvendinti naudojami skirtingi mokslinių tyrimų metodai. Duomenys disertacijai renkami vadovaujantis *teisinių dokumentų analizės, mokslinės literatūros analizės, nestruktūruoto ir struktūruoto ekspertų interviu, stebėjimo metodais.* Surinkti duomenys apdorojami taikant šiuos teorinius metodus: *sisteminės analizės, istorinį ir lyginamąjį*.

Teisinių dokumentų analizės metodu tiriama JAV, ES, ET, Lietuvos teisės aktai. Šio metodo taikymo tikslas – ištirti buvusį ir esamą asmens duomenų rinkimo teisėsaugos ir žvalgybos tikslais teisinį reglamentavimą JAV, ES, ET ir Lietuvoje. Bendrosios

teisės tradicijų šalyse teismo precedentai yra labai svarbūs, todėl kokybinis JAV teismų precedentų tyrimas svarbus vertinant ir aiškinant teisės normas, jų pakeitimus, praktinį taikymą užtikrinant IV JAV Konstitucijos pataisa įtvirtintą teisę į privatumą bei kartu asmens duomenų apsaugą. JAV teismų sprendimai disertacijos tyrimui yra svarbūs ir lyginamuoju požiūriu, kadangi kai kurios dabar galiojančios Lietuvos teisės aktų nuostatos yra panašios į seniau galiojusias JAV, bet pakeistas teismų sprendimų pagrindu. EŽTT ir ESTT sprendimai dėl teisės į asmens duomenų apsaugą disertacijos tyrimui buvo reikšmingi dėl EŽTK ir Europos žmogaus teisių chartijoje įtvirtintos teisės į asmens duomenų apsaugą galiojimo ir apribojimų apimties aiškinimo. Lietuvos teismų sprendimai – dėl Kriminalinės žvalgybos įstatymo ir BPK nuostatų praktinio taikymo klausimų išaiškinimo.

Mokslinės literatūros analizės metodas naudojamas siekiant atskleisti JAV ir Europos mokslininkų požiūrį ir jų atliktų mokslinių tyrimų rezultatus dėl teisės į asmens duomenų apsaugą įgyvendinimo asmens duomenis el. erdvėje renkant teisėsaugos ir žvalgybos tikslais, šią sritį reglamentuojančių teisės aktų pakeitimus ir bei jų poveikį. Mokslinės literatūros analizė taip pat padėjo surasti paaiškinimą, kodėl žvalgybos institucijos teisiškai gali rinkti duomenis apie užsieniečius, įskaitant duomenų rinkimą el. erdvėje. Pastebėta tendencija, kad nors teisės į asmens duomenų apsaugą užtikrinimas šiuos duomenis renkant teisėsaugos ir žvalgybos tikslais yra globali problema, dauguma mokslinės literatūros yra nukreipti į šios teisės užtikrinimą nacionaliniu lygiu.

Kadangi elektroninė erdvė pasižymi greita technologine raida, atitinkamai todėl ir teisinis reglamentavimas šioje srityje yra dinamiškas ir įtakojamas politinių bei didelę galią turinčių technologinių įmonių (Facebook, Google, Apple ir kt.) sprendimų. Disertacijoje analizuojamos pasaulinės tendencijos, todėl *stebėsenos metodas* taikomas siekiant disertacijos tematikoje turėti aktualią informaciją ir gebėti prognozuoti būsimus pokyčius arba tų pokyčių poreikį. Stebėsenos objektas – pasauliniai dienraščiai *„Financial Times“, „The Economist“, „The Guardian“, „Reuters“, „politico.eu“, Massachussets Technology Review (MIT)* žurnalas.

Nestruktūrizuoto interviu metodas taikomas probleminių reglamentavimo Lietuvoje aspektus nustatymui. Nestruktūrizuotas interviu vykdomas su šešiais ekspertais, turinčiais skirtingos patirties tyrimo objekto atžvilgiu. Dėl disertacijos temos jautrumo ekspertams sudaryta galimybė išlikti anoniminiais, interviu turinio neviešinti. Todėl keturių ekspertų tapatybė negali būti atskleista, likę du yra Vytauto Didžiojo universiteto profesorius, Lietuvos atstovas NATO STO darbo grupėje dr. Tomas Krilavičius ir Alius Navickas (Finansinių nusikaltimų tyrimo tarnyba). Interviu metu visiems ekspertams buvo pateikiami nevienodi klausimai, jie buvo formuojami atsižvelgiant į kiekvieno eksperto pateiktą informaciją ir veiklos sritį. Autorė disertacijos tema taip pat diskutavo su užsienio mokslininkais: ESSCA School of Management prof. dr. Ana Dimitrova, kurios viena iš mokslinių tyrimų sričių yra asmens duomenų rinkimo el. erdvėje reglamentavimas JAV, Europolo asmens duomenų apsaugos ekspertu dr. Jan Ellermann, IBM Q ambasadoriumi dr. Piotr Biskupski, Mysterium Network įkūrėju Robertu Višinskiu. Disertacijoje remiamasi tik nekonfidencialia informacija.

Struktūruoto interviu metodo tikslas įvertinti BPK 154 str. taikymo praktikos tendencijas ir probleminius aspektus. Struktūruoto interviu metu būdu buvo apklausti 22 pačių ikiteisminio tyrimo institucijų deleguoti tyrėjai. Prašymai atlikti tyrimą buvo išsiųsti visoms ikiteisminio tyrimo institucijoms oficialiai nurodytais el. paštais, tačiau tyrime dalyvauti sutiko tik septynios ikiteisminio tyrimo institucijos. Tyrime dalyvavusios institucijos: Specialiųjų tyrimų tarnyba, Finansinių nusikaltimų tyrimų tarnyba, Muitinės kriminalinė tarnyba, Vilniaus apskrities vyriausiasis policijos komisariatas, Vilniaus apskrities vyriausiojo policijos komisariato Kriminalinės policijos organizuoto nusikalstamumo tyrimo valdyba, Kauno apskrities vyriausiasis policijos komisariatas ir Utenos apskrities vyriausiasis policijos komisariatas. Visiems respondentams buvo pateikti vienodi klausimai. Tyrimo rezultatai naudojami disertacijos 4.1.1. poskyryje.

Tyrimo objekto pobūdis, teisinį reglamentavimą elektroninių asmens duomenų rinkime teisėsaugos ir žvalgybos tikslais įtakojantys skirtingi veiksniai (skirtingas nacionalinis teisinis reglamentavimas, teismų sprendimai, politiniai veiksniai, technologinių įmonių vaidmuo ir kt.) reiškia, kad yra reikalingas sisteminis požiūris į tyrimo objekto problematiką, todėl tyrimo rezultatų analizei buvo tikslinga naudoti *sisteminės analizės metodą*. *Istorinio tyrimo* metodas padėjo nustatyti asmens duomenų rinkimo el. erdvėje reglamentavimo doktrininį pagrindą, teisinio reglamentavimo evoliuciją bei ją įtakojančius veiksnius. Disertacijos skyriai taip pat yra išdėstyti istoriniu chronologiniu požiūriu nuo seniausiai sukurto teisinio reglamentavimo iki naujausio (JAV, ET, ES ir Lietuva). *Lyginamasis* metodas naudojamas viso tyrimo metu. Juo taip pat remtasi rengiant pasiūlymu jis buvo naudojamas kaip tobulinti asmens duomenų rinkimo el. erdvėje teisėsaugos ir žvalgybos tikslais reglamentavimą Lietuvoje. Kadangi teisinis elektroninių asmens duomenų rinkimo teisėsaugos ir žvalgybos tikslais reglamentavimas atsirado JAV ir yra labiausiai išplėtotas ir kadangi didžioji dauguma ES gyventojų asmens duomenų keliauja atviru internetu per JAV arba yra saugomi JAV esančiuose ar JAV įmonėms priklausančiuose ne JAV teritorijoje esančiuose serveriuose, o reglamentavimą Lietuvoje įtakoja ET ir ES teisinis reglamentavimas, todėl lyginamojo metodo pagalba buvo lyginama JAV, ET, ES ir Lietuvos teisės aktų nuostatos ir teismų praktika.

1. ASMENS DUOMENŲ ELEKTRONINĖJE ERDVĖJE KONCEPTAS

Teisės į privatumą ir asmens duomenų apsaugą „gimtine“ yra laikoma Europa, pagrindiniu teisiniu šaltiniu – Europos žmogaus teisių konvencija[42]. Tačiau tokios teisės atsiradimo idėja pirmą kartą kilo ne Europoje, o JAV. Čia 1890 m. Harward Law Review[43] pasirodė pirmasis mokslinis straipsnis apie asmens privatumo apsaugą. Teisės į asmens duomenų apsaugą istorijai S. Warren ir L. D. Brandeis straipsnis „The Right to Privacy“ svarbus to dėl, kad jame pirmą kartą:

1) iškelta asmens privatumo (ir netiesiogiai asmens duomenų) kaip teisinio apsaugos objekto lygiagretaus turtui idėja ir kad asmuo turi turėti teisę būti vienas (angl. *the Right to be Alone*);
2) asmens privatumo ir duomenų apsaugos poreikis siejamas ne su žmogaus prigimtimi ir šimtmečius besivyščiusia jo buitimi, o su inovacijomis, mokslo ir technologijų pažanga[44].

Šie du lozungai iki šiol yra kartojami tiek teisės aktuose, tiek moksliniuose straipsniuose, tiek politiniuose debatuose plačiau nekomentuojant tų teiginių prasmės ir reikšmės.

Šiandien teisiniai asmens duomenų apsaugos neapibrėžtumai ir technologijų pažanga dažniausiai atsiranda dėl interneto ir elektroninės erdvės keliamų iššūkių. Netolimoje ateityje ši tendencija gali pasikeisti ir pagrindiniu mokslinių tyrimų objektu gali tapti neuro duomenys[45] ar mūsų DNR, o ne serveriuose ar debesų kompiuterijoje saugomi ir dabar „elektroniniais“ laikomi, asmens duomenys[46]. Bet, kad suprastumėme ateities asmens duomenų apsaugos iššūkius, visų pirma reikia išspręsti tuos, kurie kyla šiandien. Šio įvadinio disertacijos skyriaus tikslas yra apibrėžti kas yra privatumas, asmens duomenys, koks yra santykis tarp teisės į asmens duomenų apsaugą ir teisės į privatumą, kas yra elektroninė erdvė ir kokius asmens duomenis mes generuojame elektroninėje erdvėje tam, kad tolimesniuose disertacijos skyriuose būtų aiški minėtų sąvokų apimtis, reikšmė ir sąsajos tarp jų.

Privatumas. Dažnai naujos technologijos, įskaitant žvalgybos, yra kvestionuojamos kaip pažeidžiančios privatumą[47]. Teisę į privatumą asmenims suteikia Visuotinės žmogaus teisių deklaracijos 12 str., Europos

---

[42] „European Privacy Framework“, *Privacy Europe*, žiūrėta 2020 m. rugsėjo 1 d., https://www.privacy-europe.com/european-privacy-framework.html.

[43] Samuel D. Warren ir Louis D. Brandeis, „The Right to Privacy“, *Harvard Law Review* 4, no. 5 (1890): 193–220, doi:10.2307/1321160.

[44] Rachel L. Finn, David Wright ir Michael Friedewald, „Seven Types of Privacy“, in *European Data Protection: Coming of Age*, ed. Serge Gutwirth et al. (Dordrecht: Springer Netherlands, 2013), 3–32, doi:10.1007/978-94-007-5170-5_1.

[45] Dara Hallinan ir kt., „Neurodata and Neuroprivacy: Data Protection Outdated?“, *Surveillance & Society* 12, no. 1 (November 20, 2013): 55–72, doi:10.24908/ss.v12i1.4500.

[46] Yanan Wang ir kt., „Probe Computing Model Based on Small Molecular Switch“, *BMC Bioinformatics* 20, no. 8 (June 10, 2019): 285, doi:10.1186/s12859-019-2767-8.

[47] David Lyon, „Surveillance after September 11“, *Sociological Research Online*, November 7, 2017, doi:10.5153/sro.643.

Sąjungos pagrindinių teisių chartijos 7 str., nacionalinės valstybių Konstitucijos, įstatymai. Teisės aktai paties privatumo apibrėžimo nepateikia, o siekiant pateikti universalų apibrėžimą vis dar yra atliekami moksliniai tyrimai ir rengiamos mokslinės publikacijos[48]. Universalaus apibrėžimo kol kas nėra pateikto, bet mokslininkai sutinka, kad privatumo sąvoka yra socialinė, todėl jos, kaip ir visų socialinių sąvokų, apibrėžimas priklauso nuo ją apibrėžiančio asmens[49]. R. Clarke buvo pirmasis mokslininkas, kuris 1995 m. privatumą suskirstė į keturias kategorijas, o 2013 m. šį savo skirstymą papildė penkta kategorija taip išryškindamas jo daugialypumą:

1) asmens fizinio kūno privatumas (angl. *privacy of the person* arba kitaip „*bodily privacy*“) – apima asmens fizinį kūną ir jo vientisumą;
2) asmens elgesio privatumas (angl. *privacy of personal behaviour*) – apima visus asmens elgesio aspektus, įskaitant socialiai jautrius, pvz. asmens seksualinį, politinį ir religinį elgesį;
3) asmeninės komunikacijos privatumas (angl. *privacy of personal communications*) – apima bent kokias komunikacijas ir jų formas;
4) asmens duomenų privatumas (angl. *privacy of personal data*) – apima visus duomenis apie asmenį;
5) asmeninės patirties privatumas (angl. *privacy of personal experience*) – apima visus mūsų veiksmus, kuriais mes įgyjame vienokios ar kitokios patirties. R. Clarke teigia, kad kiekvieną dieną mūsų atliekami veiksmai (pvz., knygų skaitymas, pokalbiai telefonu, susitikimai su kitais asmeninis, ėjimas į kiną ir t. t.) formuoja mūsų unikalią patirtį. Iki XXI a. įrašai apie tokių veiksmų atlikimą nebuvo renkami. Dabar tai yra neišvengiama dėl pačių technologijų veiklos pobūdžio, todėl tapo asmens privatumo dalimi[50].

R. Clarke privatumo kategorijos nors ir logiškos, bet turi vieną ydą: yra technologiškai pasenusios. Jos, kaip ir dauguma teisės aktų, eina ne kartu su technologijos arba prieš jas, o paskui. Tą pripažįsta ir pats R. Clarke 2013 m. papildydamas iki tol buvusias keturias privatumo kategorijas penktąja.

Technologinės pažangos ypatumus labiau atitinka R. Clarke tyrimo pagrindu kitos mokslininkų grupės struktūrizuotas privatumo skirstymas į septynias rūšis[51]:

1) asmens fizinio kūno privatumas (angl. *privacy of the person)* reiškia asmens teisę informacijos apie savo kūną, jo funkcionavimą ir charakteristikas (pvz., geneti-

---

48 „Opinion 4/2007 on the concept of personal data“, *Article 29 Working Party,* žiūrėta 2020 m. rugsėjo 1 d., https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_en.pdf.Paul M. Schwartz, „Property, Privacy, and Personal Data“, *Harvard Law Review* 117, no. 7 (2004 2003): 2056–2128. Gloria Gonzalez Fuster, „Un-Mapping Personal Data Transfers“, *European Data Protection Law Review (EDPL)* 2, no. 2 (2016): 160–68.

49 Colin J Bennett, *Regulating Privacy: Data Protection and Public Policy in Europe and the United States*, (Cornell University Press, 1992). Debbie V. S. Kasper, „The Evolution (or Devolution) of Privacy“, *Sociological Forum* 20, no. 1 (March 1, 2005): 72, doi:10.1007/s11206-005-1898-z.

50 „Roger Clarke's 'Privacy Introduction and Definitions'“, *Roger Clarke*, žiūrėta 2020 m. rugsėjo 1 d., http://www.rogerclarke.com/DV/Intro.html#Priv.

51 Serge Gutwirth, Ronald Leenes, Paul de Hert ir kt, eds., *European Data Protection: Coming of Age* (Dordrecht: Springer Netherlands, 2013), doi:10.1007/978-94-007-5170-5, Michael Friedewald, Rachel Finn, ir David Wright, *Seven Types of Privacy*, 2013, 3–32, doi:10.1007/978-94-.

nį kodą, biometrinius duomenis) neatskleidimą pačiam asmeniui to nežinant ir nepageidaujant;
2) elgesio ir veiksmų privatumas (angl. *privacy of behavior and action*) reiškia asmens teisę į politinių įsitikimų, religinio, seksualinio elgesio neatskleidimą tretiesiems asmenims tiek esant privačioje, tiek viešoje erdvėje pačiam asmeniui to nežinant ir nepageidaujant;
3) komunikacijos privatumas (angl. *privacy of communication*) reiškia asmens teisę į bent kokios formos komunikacijos neatskleidimą pačiam asmeniui to nežinant ir nepageidaujant;
4) duomenų ir vaizdų privatumas (angl. *privacy of data and image*) reiškia asmens teisę į bent kokios formos duomenų ir vaizdų neatskleidimą pačiam asmeniui to nežinant ir nepageidaujant;
5) minčių ir jausmų privatumas (angl. *privacy of thoughts and feelings*) reiškia asmens teisę mąstyti taip kaip ji(s) nori;
6) vietos ir erdvės privatumas (angl. *privacy of location and space*) reiškia asmens teisę judėti viešoje ir privačioje erdvėje pagal savo paties pasirinktą trajektoriją be galimybės būti identifikuotam, sekamam arba stebimam asmeniui to nežinant ir nepageidaujant;
7) asociacijų privatumas (įskaitant grupės privatumą) (angl. *privacy of association (including group privacy)*) – reiškia asmens teisę asocijuoti save su bent kuo, kuo ji(s) nori ir dalyvauti tos grupės veikloje to neatskleidžiant kitiems.

Gali susidaryti įspūdis, kad šios septynios privatumo kategorijos asmeniui suteikia daug laisvės. Tačiau kaip ir kiekvienos teisės, teisės į asmens duomenų apsaugą ribos yra ten, kur prasideda kito asmens teisės[52].

Nors disertacija yra apie asmens duomenų rinkimą elektroninėje erdvėje teisėsaugos ir žvalgybos tikslais, tačiau iliustruodama privatumo daugialypiškumą ir tai, kad viena technologija gali pažeisti kelias privatumo kategorijas, noriu pateikti kelis pavyzdžius iš disertacijos rašymo metu dar tik besivystančių technologijų.

- Viso kūno skeneriai (angl. *whole body imaging scanners*) dabar jau yra naudojami daugelyje oro uostų atliekant aviacijos saugumo patikrą. Jų veikimo principas yra toks – skeneris nuskenuoja visą asmens kūną skenerio nuotraukoje atspindėdamas ne standartinės formos žmogaus kontūrą, kurį keleiviai mato praėję pro jį, o nuogą to asmens kūną[53]. Nors mokslininkai[54] ir žmogaus teisių aktyvistai mano, kad tokios priemonės yra neproporcingos, ypač vaikų atžvilgiu[55], institucijos laikosi priešingos pozicijos teikdamos, kad oro uostuose naudojami skeneriai

[52] Alfonsas Vaišvila, *Teisės teorija: vadovėlis*, 4-asis leid ed. (Vilnius: Justitia, 2014).

[53] „The Impact of the Use of Body Scanners in the Field of Aviation Security on Human Rights, Privacy, Personal Dignity, Health and Data Protection", *European Commission*, 2016, žiūrėta 2020 m. rugsėjo 1 d., https://ec.europa.eu/transport/modes/air/consultations/2009_02_19_body_scanners_en.

[54] Demetrius Klitou, „Backscatter Body Scanners – A Strip Search by Other Means", *Computer Law & Security Review* 24, no. 4 (January 1, 2008): 317, doi:10.1016/j.clsr.2008.05.005.

[55] „Body Scanners", *American Civil Liberties Union*, žiūrėta 2020 m. rugsėjo 1 d., https://www.aclu.org/other/body-scanners.

nesaugo nuotraukų[56]. Tačiau nuotraukų saugojimo funkciją šie skeneriai turi[57]. Ir JAV jau buvo toks atvejis, kai aviacijos saugumo patikros skenerių nuotraukos iš vieno JAV oro uosto buvo nutekintos ir paviešintos internete[58]. Taigi aviacijos saugumo patikrai naudojami skeneriai gali pažeisti kūno privatumą (kadangi nuotraukose matosi nuogas kūnas), elgesio privatumą (kadangi matosi ne tik kūno formos, bet ir patalogijos, implantai ir kt.), asmens duomenų ir vaizdų privatumą (kadangi nuotrauka turi fizinę išraišką vaizdo forma) ir vietos ir erdvės privatumą (kadangi gali būti susiejama su asmens buvimu atitinkamame oro uoste atitinkamu laiku).

- Žmogaus tobulinimo technologijos (angl. *human enhancement technologies*) – tai tokios technologijos, kurios gali patobulinti asmenį farmakologiniu (pvz. vaistai, narkotinės medžiagos) arba technologiniu būdu (pvz. smegenų kompiuteris, genų inžinerija)[59]. Tiek nelegalios, tiek tam tikros legalios farmakologinės medžiagos (antidepresantai, methylphenidatas (Ritalinas), aspirinas) įtakoja asmens elgesį. Schutz ir Friedewal teigia, kad šių vaistų naudojimą galima laikyti galimybe kontroliuoti kito asmens elgesį tam asmeniui to nežinant ir nesutinkant[60]. Analogišką tik stipresnį ir platesnio pobūdžio poveikį galima pasiekti smegenų kompiuteriais. Dauguma kuriamų smegenų kompiuterių paremti principu, kad ne jie, o juos valdo žmogaus smegenys t. y. asmens smegenų impulsai įjungia, išjungia atitinkamą įrenginį[61]. Tačiau yra galimas ir atvirkštinis variantas kuomet kompiuteris turėtų galimybę veikti asmens smegenis ir tokiu būdu valdyti asmenį. 2019 m. vasarą Microsoft investavo 1 milijardą JAV dolerių į Elon Musk įmonę, kurios tikslas yra sukurti dirbtinio intelekto patobulinimą – žmogaus smegenų dirbtinį intelektą, dirbtinio intelekto ir smegenų sintezę – AGI (angl. *artificial general intelligence*)[62]. Kita Elon Musk įmonė „Neuralink", kuria ultraplonus siūlus, skirtus implantuoti į asmens smegenis tam, kad žmogaus smegenų ir kompiuterio arba dirbtinio intelekto sąsaja būtų stipresnė[63]. Taigi

---

[56] „Impact Assessment on the use of security scanners at UK airports", *Department for Transport*, žiūrėta 2020 m. rugsėjo 1 d., http://webarchive.nationalarchives.gov.uk/+/http://www.dft.gov.uk/consultations/open/2010-23/ .

[57] Serge Gutwirth, Ronald Leenes, Paul de Hert, ir kt, *European Data Protection: Coming of Age* (Springer Science & Business Media, 2012), 12.

[58] „Opinion of the European Economic and Social Committee on the Communication from the Commission to the European Parliament and the Council on the Use of Security Scanners at EU airports, COM(2010) 311 final", *European Economic and Social Committee,* 2011, 49–52, žiūrėta https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52011AE0361 .

[59] Andreas Wolkenstein, Ralf J. Jox ir Orsolya Friedrich, „Brain–Computer Interfaces: Lessons to Be Learned from the Ethics of Algorithms", *Cambridge Quarterly of Healthcare Ethics* 27, no. 4 (2018): 635–46, doi:10.1017/S0963180118000130.

[60] Philip Schütz ir Michael Friedewald, „Technologies for Human Enhancement and their impact on privacy", *Privacy, data protection and ethical issues in new and emerging technologies: Five case studies*, eds. Rachel Finn and David Wright.

[61] Dennis J. McFarland ir Jonathan R. Wolpaw, „Brain-Computer Interfaces for Communication and Control", *Communications of the ACM* 54, no. 5 (2011): 63, doi:10.1145/1941487.1941506.

[62] Cade Metz, „With $1 Billion From Microsoft, an A.I. Lab Wants to Mimic the Brain – The New York Times", žiūrėta 2020 m. rugsėjo 1 d., https://www.nytimes.com/2019/07/22/technology/open-ai-microsoft.html.

[63] Alex Knapp, „Elon Musk Sees His Neuralink Merging Your Brain With A.I.", žiūrėta 2020 m. rugsėjo 1 d., https://www.forbes.com/sites/alexknapp/2019/07/17/elon-musk-sees-his-neuralink-merging-your-brain-with-ai/#4dcca3b14b07.

šiuo metu kuriama ir, jos sėkmės atveju, svarbiausiu šimtmečio atradimu laikoma AGI technologija ne tik bus asmens smegenų pagrindu veikiantis kompiuteris, bet ir turės galimybę daryti įtaką žmogaus smegenims, kas reiškia galimybę veikti ir kontroliuoti žmogų. 2019 m. kinų mokslininkai paskelbė sėkmingai pakeitę dar negimusių kūdikių DNR[64]. Nors į klausimą kada žmogų galima laikyti žmogumi – nuo jo gimimo ar gyvybės užsimezgimo – dar nėra visuotinio susitarimo[65], sėkmingas Kinijos mokslininkų eksperimentas pakeičiant dar negimusių, tačiau užsimezgusių kūdikių DNR[66] gali būti dar vienu privatumo pažeidimo pavyzdžiu. DNR korekcijos buvo atliktos apvaisintiems, tačiau į motinos gimdą dar neinplantuotiems kiaušinėliams. Dalis gyvybės mokslų atstovų gyvybės pradžia laiko pastojimo momentą, kuomet apvaisinta kiaušialąstė įsitvirtina į moters gimdą. Kita dalis gyvybės pradžia laiko apvaisinimą[67]. Įvykus apvaisinimui nebelieka spermatozoido ir kiaušialąstės, susiformuoja zigota, kuri pakeliui iki gimdos sienelės tampa blastule. Disertacijos autorė palaiko pastarąją poziciją. Todėl bent kokie DNR pakeitimai įvykus apvaisinimui reiškia teisės į privatumą pažeidimą, kuriam restitucija yra neįmanoma. Šiuo atveju yra pažeidžiamos vėlgi kelios privatumo kategorijos: kūno privatumas (modifikuojamas dar negimusio asmens kūnas), duomenų ir vaizdų privatumas (visas DNR kodas yra nuskaitomas ir modifikuojamas), elgesio ir veiksmų bei minčių ir jausmų (DNR pakeitimais galima keisti tuos asmens polinkius, kuriuos jis turi genetiškai).

- Antros kartos biometrijos prietaisai (angl. *second generation biometrics*) apima kintančius (pvz. balsas, kalba) ir fiziologinius (pvz. širdies ritmas, feromonai) kūno parametrus nuotoliniu ir nenuotoliniu būdu matuojančius ir analizuojančius prietaisus[68]. Antrosios kartos biometrijos prietaisai gali pažeisti visas septynias privatumo kategorijas. S. Venier ir E. Mordini šią technologiją apibūdina kaip žmogaus orumą visišku kūno skaitmenizavimu ir profiliavimu pažeidžiančią technologiją[69]. Antros kartos biometrijos prietaisų paskirtis yra ne vien tik asmens identifikavimas, bet ir profiliavimas bei kategorizavimas. Pavyzdžiui, balso ir

---

64 Antonio Regalado,„EXCLUSIVE: Chinese Scientists Are Creating CRISPR Babies“, *MIT Technology Review*, žiūrėta 2020 m. rugsėjo 1 d., https://www.technologyreview.com/2018/11/25/138962/exclusive-chinese-scientists-are-creating-crispr-babies/.

65 „BBC – Ethics – Abortion: When Is the Foetus 'Alive'?“, žiūrėta 2020 m. rugsėjo 1 d., http://www.bbc.co.uk/ethics/abortion/child/alive_1.shtml.

66 Antonio Regalado, „China's CRISPR Babies: Read Exclusive Excerpts from the Unseen Original Research“, *MIT Technology Review*, accessed August 10, 2020, https://www.technologyreview.com/2019/12/03/131752/chinas-crispr-babies-read-exclusive-excerpts-he-jiankui-paper/. Preetika Rana, „How a Chinese Scientist Broke the Rules to Create the First Gene-Edited Babies“, *Wall Street Journal*, 2019, https://www.wsj.com/articles/how-a-chinese-scientist-broke-the-rules-to-create-the-first-gene-edited-babies-11557506697.

67 Donna Harrison, „Mokslo įrodymai neigia abortų šalininkų argumentus apie gyvybės pradžią“, *Laisvos Visuomenės Institutas*, žiūrėta 2020 m. rugsėjo 1 d., https://laisvavisuomene.lt/mokslo-irodymai-neigia-abortu-salininku-argumentus-apie-gyvybes-pradzia/.

68 Silvia Venier ir Emilio Mordini, „Second-generation biometrics“, in *Privacy, data protection and ethical issues in new and emerging technologies: Five case studies*, eds. Rachel Finn and David Wright, 25 November 2011. Projekto „Privacy and emerging fields of science and technology: Towards a common framework for privacy and ethical assessment“ rezultatas. Prieiga internete: https://www.prescient-project.eu/prescient/inhalte/download/PRESCIENT_D2.pdf .

69 Venier ir Mordini, *supra note*, 68.

kalbos atpažinimo technologijos gali būti naudojamos įrašyti, analizuoti ir atskleisti asmens komunikaciją, įskaitant jos turinį, kuriame gali atsispindėti asmens mintys ir įsitikinimai[70]. Nuotolinis matavimų pobūdis sudaro galimybę tuos pačius matavimus tuo pačiu metu atlikti asmenų grupei jiems to nežinant. Kadangi jų veikimo diametras apima tam tikrą aiškiai apibrėžtą teritoriją, todėl antros kartos biometrijos prietaisais galima rinkti visų toje teritorijoje esančių asmenų biometrinius duomenis. Biometriniai duomenys BDAR patenka į specialių asmens duomenų kategoriją, todėl tokių duomenų tvarkymas yra galimas tik BDAR 9 str. 2 d. įtvirtintomis aplinkybėmis, pvz. esant asmens sutikimui, kurio neįmanoma gauti biometrinius duomenis renkant nuotoliniu būdu viešose vietose.

1 lentelė. *„Naujos kartos technologijų poveikis asmens privatumui"*.

	Viso kūno skeneriai	Žmogaus tobulinimo technologijos	Antros kartos biometrijos prietaisai
Asmens fizinio kūno privatumas	x	x	x
Elgesio ir veiksmų privatumas	x	x	x
Komunikacijos privatumas		x	x
Duomenų ir vaizdų privatumas	x	x	x
Minčių ir jausmų privatumas		x	x
Vietos ir erdvės privatumas			x
Asociacijų privatumas	x		x

1 lentelėje yra pavaizduota, kaip viena technologija gali pažeisti kelias privatumo kategorijas. Pateisinant elektroninės erdvės, kaip technologijos, nesaugumą yra sakoma, kad ji buvo kuriama ne saugoti asmens duomenis, o jais dalintis[71]. Analogiškai naujosios technologijos taip yra kuriamos turint kažkokį tikslą, pvz. sukurti smegenų kompiuterį, sukurti antros kartos biometrinius duomenis matuojančius prietaisus. Naujų technologijų kūrėjų tikslu nėra tikslas apsaugoti asmens privatumą. Nors inovatyvių produktų kūrimas yra finansuojamas ne vien tik nacionalinių institucijų, bet ir investicinių fondų, verslo angelų, privačių investuotojų lėšomis, tačiau bent jau valstybinėms inovatyvių projektų kūrimą finansuojančioms institucijoms į finansavimo sąlygas

[70] Serge Gutwirth, Ronald Leenes, Paul de Hert, ir kt., eds., *European Data Protection: Coming of Age* (Springer Netherlands, 2013), 16, doi:10.1007/978-94-007-5170-5.

[71] John R. Vacca, *Computer and Information Security Handbook* (Morgan Kaufmann, 2009).

įtraukus reikalavimą pagrįsti, kad kuriama technologija nepažeis asmenų teisės į privatumą, būtų ugdomas kūrėjų sąmoningumas. Autorės duomenimis, toks reikalavimas nėra taikomas nei vienoje mokslinių tyrimų ir inovacijų projektus finansuojančioje institucijoje. Autorės nuomone, poveikio privatumui vertinimas (angl. *privacy impact assesment*) turėtų būti numatytas visuose naujų technologijų kūrimą finansuojančių institucijų projektų finansavimo sąlygų aprašuose. Nors teisė į privatumą nėra absoliuti[72], tačiau naujomis kuriamomis technologijomis neetiškai ir neteisėtai pažeidžiant asmens privatumą galima sukelti negrįžtamus fizinius ir emocinius padarinius asmeniui. Todėl teisė į privatumą nėra tik teisė būti vienam. Tai yra ir teisė gyventi oriai.

Ne visi mokslininkai privatumą apibrėžia per socialinę prizmę. Pavyzdžiui, Daniel L. Solove privatumą aiškina kaip „visiškai skirtingų, tačiau susijusių dalykų visumą“[73]. Jis, kaip ir D. Kaspar[74] privatumą apibrėžia per problemas, kurias kelia:

1) informacijos rinkimas – pvz., elektroninė žvalgyba, paslaugų teikėjų vykdomas informacijos rinkimas;
2) informacijos tvarkymas – pvz., apibendrinimas, duomenų nesaugumas, galimas identifikavimas, antrinis naudojimas ir pašalinimas;
3) informacijos sklaida – pvz., atskleidimas, konfidencialumo įsipareigojimų pažeidimas;
4) invazija – pvz., įsilaužimas, informacijos nutekinimas, tikslingas įsiterpimas į informacijos perdavimą[75].

Nors šis požiūris į privatumą yra visiškai priešingas prieš tai disertacijoje aprašytam, tačiau kartu ir susijęs. Aukščiau minėtos septynios privatumo kategorijos tik tada gali būti pažeistos, kai yra išreikštos kažkokios formos informacija – duomenimis arba vaizdais. Vadinasi ir teisinę apsaugą privatumas įgyja ir gali būti pažeidžiamas tik tada tai visos aukščiau minėtos privatumo formos įgyja informacijos išraišką. Pažvelgus į lentelę Nr.1 „Naujos kartos technologijų poveikis asmens privatumui“ pamatysite, kad visais atvejais naujos atsirandančios technologijos gali potencialiai pažeisti duomenų ir vaizdų privatumo kategorijas. Bet ne vien tik jas. Autorės nuomone, Daniel L. Solove apibrėžimas labiau atskleidžia teisės į asmens duomenų apsaugą turinį nei privatumą. Todėl disertacijoje privatumas bus suvokiamas per septynias jo kategorijas, kurių viena yra duomenų ir vaizdų privatumas. Analogiškai, EŽTK 8 str. įtvirtinta teisė į privatumą apima ir teisę į asmens duomenų apsaugą, nors ankstyvosiose bylose EŽTT asmens duomenų apsaugos nelaikė sudėtine EŽTK 8 straipsnio dalimi[76]. Tačiau

---

[72] „Guide on Article 8 of the Convention – Right to respect for private and family life“, *European Court of Human Rights*, 7, žiūrėta 2020 m. rugpjūčio 23 d., https://www.echr.coe.int/Documents/Guide_Art_8_ENG.pdf.

[73] Hamza S. Dawood, „Understanding Privacy, by Daniel J. Solove Book Note“, *Osgoode Hall Law Journal* 47, no. 4 (2009): 819–20.

[74] Debbie V. S. Kasper, „The Evolution (or Devolution) of Privacy“, *Sociological Forum* 20, no. 1 (2005): 76, doi:10.1007/s11206-005-1898-z.

[75] Daniel J. Solove, „I've Got Nothing to Hide and Other Misunderstandings of Privacy“, *San Diego Law Review* 44, no. 4 (2007): 745–72.

[76] Franziska Boehm, *Information Sharing and Data Protection in the Area of Freedom, Security and Justice: Towards Harmonised Data Protection Principles for Information Exchange at EU-Level* (Berlin Heidelberg: Springer-Verlag, 2012), 81, doi:10.1007/978-3-642-22392-1.

pripažindamas, kad EŽTK yra „gyvasis instrumentas“, kurio turinys ir interpretacija kinta atsižvelgiant į šiuolaikinio gyvenimo aktualijas[77] ir atsiradus nenuginčijam asmens duomenų apsaugos poreikiui, EŽTT savo poziciją pakeitė[78]. Taigi dabar tiek mokslininkai, tiek EŽTT laikosi tos pozicijos, kad nors EŽTK 8 straipsnio formuluotėje tiesiogiai nėra kalbama apie asmens teisę į duomenų apsaugą, tačiau teisė į asmens duomenų apsaugą yra sudėtinė asmens teisės į privatumą dalis[79, 80].

Asmens duomenys. Skirtingai nuo teisės į privatumą, teisė į asmens duomenų apsaugą atsirado Europoje dėl ekonominio poreikio užtikrinti laisvą informacijos judėjimą tuo pačiu metu saugant asmenį[81]. Nuo 2018 m. įsigaliojus BDAR visoje ES galioja vieningas asmens duomenų apibrėžimas – tai bet kokia informacija apie fizinį asmenį, kurio tapatybė nustatyta arba kurio tapatybę galima nustatyti. Analogiškas asmens duomenų apibrėžimas galiojo ir 1994 m. asmens duomenų apsaugos direktyvoje. Apibrėždama asmens duomenis EK pasirinko platų jų apibrėžimo variantą siekdama, kad jis apimtų bent kokią su asmeniu susijusią informaciją[82]. Nustatyti ar konkreti informacija gali būti laikoma asmens duomenimis, nėra paprasta. Todėl vadovaudamasis BDAR pateiktu apibrėžimu J. Zaleckis[83], kaip ir 29 WP, išskiria keturis asmens duomenų elementus:

1) informacija – bent kokios išraiškos formos (alfabetinės, numerologinės, fonetinės, grafinės, fotografinės, akustinės ir kt.) duomenys. Informacija gali būti tiek objektyvi (pvz. kraujo tyrimo rezultatai), tiek subjektyvi (pvz. nuomonė). Kad informacija taptų asmens duomenimis nėra reikalinga, kad ji būtų patvirtinta kaip teisinga. Net ir neteisinga, melaginga informacija gali būti laikoma asmens duomenimis[84], jei atitinka kitus žemiau įvardintus kriterijus. Informacijos turinys taip pat gali būti įvairus. Privati informacija apie asmenį visuomet bus laikoma asmens duomenimis, tačiau lygiai taip pačiai asmens duomenimis gali būti laiko-

---

[77] „Europos Žmogaus Teisių Teismo 1978 m. balandžio 28 d. sprendimas byloje Tyrer prieš Jungtinę Karalystę (Nr. 5856/75)“, *Hudoc*, žiūrėta 2020 m. rugsėjo 7 d., https://hudoc.echr.coe.int/fre#{%22itemid%22:[%22001-57587%22]}. „Europos Žmogaus Teisių Teismo 1995 m. kovo 23 d. sprendimas byloje Loizidou prieš Turkiją (Nr. 15318/89)“, *Hudoc*, žiūrėta 2020 m. rugsėjo 7 d., https://hudoc.echr.coe.int/fre#{%22itemid%22:[%22001-57920%22]}. „Europos Žmogaus Teisių Teismo 2005 m. vasario 4 d. sprendimas byloje Mamatkulov ir Askarov prieš Turkiją (Nr. 46827/99 ir 46951/99)“, *Hudoc,* žiūrėta 2020 m. rugsėjo 7 d., https://hudoc.echr.coe.int/fre#{%22itemid%22:[%22001-68183%22]}.

[78] „Europos Žmogaus Teisių Teismo 2006 m. birželio 29 d. sprendimas byloje Panteleyenko prieš Ukrainą (11901/02)“, *Hudoc*, žiūrėta 2020 m. rugsėjo 7 d., https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22002-3281%22]}. „Europos Žmogaus Teisių Teismo 2008 m. gruodžio 4 d. sprendimas byloje S. ir Marper prieš Jungtinę Karalystę (Nr. 30562/04 ir 30566/04)“, *Hudoc*, žiūrėta 2020 m. rugsėjo 7 d., https://hudoc.echr.coe.int/fre#{%22itemid%22:[%22001-90051%22]}. „Europos Žmogaus Teisių Teismo 1997 m. sprendimas byloje Z. prieš Suomiją (Nr. 22009/93)“, *Hudoc*, žiūrėta 2020 m. rugsėjo 7 d., https://hudoc.echr.coe.int/rus#{%22itemid%22:[%22001-58033%22]}.

[79] Boehm, *op. cit.,* 75, 81.

[80] Todėl nors tik Europos Sąjungos pagrindinių teisių chartijoje yra nurodyta, kad „Kiekvienas turi teisę į savo asmens duomenų apsaugą“, yra laikoma, kad teisė į asmens duomenų apsaugą Europoje visų pirma yra ET, o ne ES idėja ir jos apsauga visų pirma yra įtvirtinta ET ir tik paskui ES lygiu (pastarajai tapus ET nare) atsižvelgiant į EŽTT praktiką, kuri yra ypatingai svarbi teisės į asmens duomenų apsaugą plėtros ir tapimo sudėtine EŽTK 8 straipsnio dalimi kontekste.

[81] Serge Gutwirth, Ronald Leenes ir Paul de Hert, eds., *Reforming European Data Protection Law*, Issues in Privacy and Data Protection (Springer Netherlands, 2015), 16, doi:10.1007/978-94-017-9385-8.

[82] *Ibid.*

[83] Zaleskis, *supra note 16*, 92.

[84] „Opinion 4/2007 on the concept of personal data“, *Article 29 Working Party,* 6, žiūrėta 2020 m. rugsėjo 1 d., https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_en.pdf.

ma ir bent kokia kita informacija, įskaitant darbo santykiais susijusią informaciją, pavyzdžiui gydytojo išrašytas receptas vaistams, net jeigu pacientas yra anonimiškas, yra laikoma asmens duomenimis ne vien tik apie pacientą, bet ir apie receptą išrašiusį gydytoją[85]. El. laiško turinys, stebėjimo kameromis užfiksuotas asmens atvaizdas, netgi vaiko piešinys[86], gali būti laikoma asmens duomenimis. Kauno apylinkės teismo 2013 m. birželio 7 d. nuosprendyje baudžiamojoje byloje (bylos Nr. 1-680-530/2013) buvo neteisingai aiškinta, kas gali būti laikoma asmens duomenimis. Teismas nurodė, kad asmens susižinojimo neliečiamumo objektas yra pasikeitimas privataus pobūdžio informacija, bet tik tarp privačių asmenų. Teismas laikė, kad įmonių vadovų tarpusavio susirašinėjimas, tarnybinis bendravimas nėra teise į asmens duomenų apsauga saugoma socialinių santykių sritis[87]. Iš tikrųjų informacija apie asmenį yra laikoma asmens duomenimis nepriklausomai nuo to ar asmuo atlieka savo profesines funkcijas, ar ne[88].

2) informacijos sąsajumas – informacija yra susijusi su asmeniu, kai ji yra apie tą konkretų asmenį[89], kai duomenys yra naudojami arba gali būti naudojami įvertinti konkretų asmenį[90], įtakoti asmens teises, elgesį ar pomėgius[91]. Ta pati informacija tam tikrais atvejais gali būti laikoma asmens duomenimis, kitais – ne. Pavyzdžiui, konkretaus nekilnojamojo turto vertė naudojama siekiant iliustruoti nekilnojamojo turto kainas atitinkamame rajone nebus laikoma asmens duomenimis. Tačiau to paties nekilnojamojo turto vertė naudojama siekiant nustatyti mokesčius, kuriuos konkretus asmuo turės mokėti, jau yra laikoma asmens duomenimis[92].
3) galimybė nustatyti tapatybę (identifikuoti). Laikoma, kad jeigu iš atitinkamos grupės asmenų išskyrus vieną iš jų yra galima nustatyti išskirtojo asmenybę, tuomet renkami duomenys yra asmens duomenimis. Asmenį identifikuojančia informacija yra laikoma jo identifikacinis numeris, fiziologiniai ir genetiniai požymiai, asmens pareigos, vardas, pavardė, apranga ir kt. Asmens duomenimis informacija yra laikoma nepriklausomai nuo to ar konkretus asmuo gali būti identifikuojamas tiesiogiai, ar netiesiogiai. Tiesiogiai asmenį galima identifikuoti pagal jo vardą, pavardę, asmens identifikavimo numerį, buvimo vietos duomenis ir interneto identifikatorių, netiesiogiai – pagal fizinės, fiziologinės, genetinės,

---

85 *Ibid.*, 7.

86 Teismo ekspertizės metu atliekant neuroprichiatrinį testą dėl mažamečio globos, mažamečio asmens yra prašoma nupiešti savo šeimos piešinį. Piešinyje atsispindi mažamečio jausmai ir nuomonė apie kiekvieną šeimos narį. Taigi, piešinyje yra atskleidžiama vaiko psichiatrinė būklė (sveikatos būklė) bei tėvo ir motinos elgesys vaiko atžvilgiu. Todėl piešinys gali būti laikomas asmens duomenimis.

87 „Kauno apylinkės teismo 2013 m. birželio 7 d. nuosprendis baudžiamojoje byloje Nr. 1-680-530/2013“, eTeismai, žiūrėta 2020 m. rugsėjo 1 d., https://eteismai.lt/byla/128140400772250/1-680-530/2013.

88 „Opinion 4/2007 on the concept of personal data“, *Article 29 Working Party,* 6, žiūrėta 2020 m. rugsėjo 1 d., https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_en.pdf.

89 *Ibid.*, 9.

90 *Ibid.*

91 *Ibid.*, 11.

92 „Opinion 4/2007 on the concept of personal data“, *Article 29 Working Party,* 9, žiūrėta 2020 m. rugsėjo 1 d., https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_en.pdf.

psichinės, ekonominės, kultūrinės ar socialinės tapatybės požymius[93] (pvz. pagal telefono adresą, automobilio valstybinius numerius, paso numerį, IP adresą) arba kombinaciją įvairių požymių, kurie asmenį išskiria iš kitų asmenų grupės ir sudaro galimybes nustatyti jo asmenybę. Todėl pseudonimizuoti duomenys yra laikomi asmens duomenimis, o anonimizuoti duomenys – ne.

4) fizinis asmuo – asmens duomenimis laikomi duomenys susiję su fiziniu asmeniu. Juridinio asmens duomenys nėra laikomi asmens duomenimis. Kas yra laikoma fiziniu asmeniu apibrėžia valstybių civiliniai kodeksai. Paprastai, fiziniu asmeniu asmuo yra laikomas nuo gimimo iki mirties[94].

Aukščiau pristatytas Daniel L. Solove pasirinktas privatumo apibrėžimo būdo, privatumą atskleidžiant per galimus jo pažeidimo variantus, svarbiausia dalimi yra informacija, duomenys. Tuo tarpu R. Clarke privatumo apibrėžimo centrinė ašis yra žmogus: tiek jo fizinis kūnas, tiek emocinis-vidinis pasaulis. Šių dviejų mokslininkų pozicija iliustruoja ir du skirtingus požiūrius į privatumą ir asmens duomenis – JAV ir Europos – įtakotus skirtingos valstybės politikos, vizijos ir galimybių technologijas naudoti politinių, ekonominių ir kt. sprendimų priėmimui. Tai atsispindi ir asmens duomenų apsaugą reglamentuojančiuose teisės aktuose.

Elektroninių ryšių tinklas – perdavimo sistemos ir (arba) komutavimo bei maršruto parinkimo įranga, kitos priemonės, įskaitant pasyviuosius tinklo elementus, leidžiančios perduoti signalus laidinėmis, radijo, optinėmis ar kitomis elektromagnetinėmis priemonėmis, įskaitant palydovinius tinklus, fiksuotuosius (kanalų ir paketų komutavimo, įskaitant internetą) ir judriuosius antžeminius tinklus, elektros perdavimo kabelines sistemas (kiek jos naudojamos signalams perduoti), tinklus, naudojamus radijo ir (arba) televizijos programoms transliuoti (retransliuoti), ir kabelinės televizijos bei mikrobangų daugiakanalės televizijos tinklus neatsižvelgiant į perduodamos informacijos pobūdį[95].

Šiuo metu plačiausiai naudojamas elektroninių ryšių tinklas yra internetas[96].

Internetas[97]. 2020 m. internetas švenčia savo 60 m. jubiliejų[98]. Per tuos 60 metų internetas keitėsi, plėtėsi jo apimtys, vis dar tebesikeičia. Iš ikiprekybinių pirkimų būdu tik JAV kariniais tikslais kurtos[99], vėliau akademiniams ir komerciniams tikslams nau-

---

[93] „Bendrasis asmens duomenų apsaugos reglamentas“, EUR-Lex, 4 str. 1 p., žiūrėta 2020 m. rugsėjo 1 d., https://eur-lex.europa.eu/legal-content/LT/TXT/?uri=CELEX%3A32016R0679 .

[94] Lietuvos Respublikos civilinio kodekso 2.2.1. straipsnis: „Fizinio asmens civilinis teisnumas atsiranda asmens gimimo momentu ir išnyksta, jam mirus“.

[95] „Lietuvos Respublikos elektroninių ryšių įstatymas“, *eTar,* 3 str. 16 d., žiūrėta 2020 m. rugsėjo 1 d., https://www.e-tar.lt/portal/lt/legalAct/TAR.82D8168D3049/asr .

[96] „New Data Shows That Mobile Internet Is Used More but Phone Call Remains Most Popular Communication“, *European Commission*, (2016), žiūrėta 2020 m. rugsėjo 1 d., https://ec.europa.eu/digital-single-market/en/news/new-data-shows-mobile-internet-used-more-phone-call-remains-most-popular-communication.

[97] Pasaulinė susietų kompiuterinių tinklų, naudojančių standartinį interneto protokolą, sistema.

[98] Interneto prototipas – ARPAnet – buvo sukurtas 1960 m. Plačiau apie tai žr. http://info.isoc.org/internet/historylbrief‘html (Harvard Law School Library).

[99] Evan Andrews, „Who Invented the Internet?“, *HISTORY*, žiūrėta 2020 m. rugsėjo 1 d., https://www.history.com/news/who-invented-the-internet.

dotos technologijos, jis išsivystė iki pasaulinio tinklo – pagrindinės technologijos naudojamos (post)moderniojoje visuomenėje[100]. Todėl šiandieninis interneto apibrėžimas gali būti neaktualus po keleto metų, kaip ir prieš 60 m. naudotas apibrėžimas jau yra neaktualus šiandiena. Internetas (angl. *Internet*) – tai pasaulinis kompiuterių tinklas, jungiantis visuotinius ir vietinius kompiuterių tinklus[101], naudojantis standartinį interneto protokolą. Pats žodis „internetas" atsirado 1983 metais, kuomet buvo apjungtas karinis tinklas MILNET ir civilinis tinklas ARPNET, o jungtinis darinys pavadintas internetu. Pačioje pradžioje, 1969 metais, internetas jungė keturis kompiuterius. 1985 metais jį jau sudarė virš 2000 įrenginių. Po to pasaulinis tinklas pradėjo augti eksponentiškai ir pirmąjį milijoną pasiekė 1991 metais. Didelį postūmį tolimesniam jo paplitimui davė naujos internetinių puslapių kūrimo technologijos, kurių pagrindą sudarė hiperteksto koncepcija. Tokių svetainių tinklas buvo pavadintas „Pasauliniu voratinkliu" (angl. World Wide Web arba sutrumpintai WWW)[102].

Elektroninių ryšių paslauga – kaip apibrėžta Lietuvos Respublikos ryšių reguliavimo įstatyme paprastai už atlygį teikiama paslauga, kurią visiškai ar daugiausia sudaro signalų perdavimas elektroninių ryšių tinklais, įskaitant telekomunikacijų paslaugas ir perdavimo (siuntimo) paslaugas transliavimui (retransliavimui) naudojamais tinklais. Elektroninių ryšių paslaugos neapima elektroninių ryšių tinklais ar naudojant elektroninių ryšių paslaugas perduodamos informacijos turinio teikimo ar redakcinės turinio kontrolės paslaugų, tarp jų informacinės visuomenės paslaugų, kurių visiškai ar daugiausia nesudaro signalų perdavimas elektroninių ryšių tinklais[103]. Disertacijos rašymo metu Europoje vyko diskusijos, ką laikyti elektorninių ryšių paslaugų teikėjais: ar jie apima tik telekomunikacijų bendroves, ar visus juridinius asmenius, kurie teikia komunikacijos elektroninėje erdvėje paslaugas. Diskusijas dėl paslaugų elektroninėje erdvėje teikėjų priskyrimo arba nepriskyrimo elektroninių ryšių paslaugų teikėjams 2018 m. sprendė ESTT[104]. Teismas *SkypeOut byloje* (C-142/18) konstatavo, kad Skype paslauga kuomet yra skambinama ne kitam Skype vartotojui, bet į fiksuoto ar mobiliojo ryšio telefono numerį turėtų būti laikoma elektroninių ryšių paslauga nors Skype elektroninių signalų perdavimą SkypeOut paslaugos funkcionavimui teikia ne pats, o sutarties su elektroninių ryšių tinklų tiekėju pagrindu, bet nesant šios sutarties *SkypeOut* paslaugos teikimas būtų negalimas[105]. *Gmail byloje* (C-193/18) ESTT priėjo

---

[100] Christian Oggolder, „From Virtual to Social: Transforming Concepts and Images of the Internet", *Information & Culture: A Journal of History* 50, no. 2 (2015): 181, doi:10.1353/lac.2015.0008.

[101] Vilius Stakėnas. *Internetas*. Visuotinė lietuvių enciklopedija, T. VIII (Imhof-Junusas). – Vilnius: Mokslo ir enciklopedijų leidybos institutas, 2005. 177.

[102] „Developments in the Law: The Law of Cyberspace", *Harvard Law Review* 112, no. 7 (1999): 1579, doi:10.2307/1342414.

[103] „Lietuvos Respublikos elektroninių ryšių įstatymas", *eTar,* 3 str. 15 d., žiūrėta 2020 m. rugsėjo 1 d., https://www.e-tar.lt/portal/lt/legalAct/TAR.82D8168D3049/asr .

[104] Christoph Engelmann ir Josina Johannsen, „ECJ Clarifies Scope of Telecoms Regulation for OTT Services", *Technology's Legal Edge*, July 23, 2019, https://www.technologyslegaledge.com/2019/07/ecj-clarifies-scope-of-telecoms-regulation-for-ott-services/.

[105] „Skype Communications Sàrl v Institut belge des services postaux et des télécommunications (IBPT)", *Curia*, žiūrėta 2020 m. rugsėjo 1 d., http://curia.europa.eu/juris/document/document.jsf?text=&docid=214741&pageIndex=0&doclang=EN&mode=req&dir=&occ=first&part=1.

prie išvados, kad *Gmail* negali būti laikomas elektroninių ryšių paslaugų teikėju, kadangi teikdamas elektroninio pašto paslaugą pats *Gmail* nedalyvauja signalų perdavime, kuris yra vienas iš elektroninių ryšių paslaugos apibrėžimo elementų[106]. Paslaugos priskyrimo elektroninių ryšių paslaugai *SkypeOut* ir *Gmail* bylose ESTT sprendė pagal tai ar paslaugos teikimas visiškai arba daugiausiai apima elektroninių signalų perdavimą ar tik paslaugos teikimą ir šios paslaugos teikėjas tiesiogiai (pats) ar netiesiogiai (per trečiuosius asmenis) nedalyvauja elektroninių signalų perdavime. Tačiau 2018 m. gruodžio 11 d. Europos Parlamentas ir Taryba priėmė direktyvą (ES) 2018/1972, kuria nustatomas Europos elektroninių ryšių kodeksas[107]. Šiame kodekse yra pateikiamas naujas elektroninių ryšių paslaugų apibrėžimas, pagal kurį minėti du ESTT sprendimai tampa nebeaktualūs, kadangi kodekse pateikiamas naujas nei iki šiol galiojantis elektroninių ryšių paslaugų apibrėžimas. Pagal naują apibrėžimą ne tik telekomunikacijų bendrovės, bet ir OTT paslaugas (angl. *over the top services*) teikiančios įmonės, įskaitant Gmail, WhatsApp, Viber ir kt. turės būti laikomos teikiančiomis elektroninių ryšių paslaugas[108]. Įsigaliojus kodeksui ESTT anksčiau minėti ESTT sprendimai taps nebeaktualūs. Europos elektroninių ryšių kodekso nuostatos į ES valstybių narių nacionalinius teisės aktus turės būti perkeltos iki 2020 m. gruodžio 11 d. Iki šios datos turės būti pakeistos ir Elektroninių ryšių reguliavimo įstatymo nuostatos.

Elektroninė erdvė (angl. *cyber space* arba *electronic space*[109]). Elektroninės erdvės apibrėžimas priklauso nuo atitinkamo laikmečio technologijų ir nacionalinių teisės aktų. Tai yra kintančio pobūdžio sąvoka. Manytina, kad artimiausias įvykis įtakosiantis elektroninės erdvės sampratos pasikeitimus yra 5G ryšio paplitimas pasaulyje. F. D. Kramer teigimu egzistuoja 28 skirtingi elektroninės erdvės apibrėžimai[110]. Teisinėje literatūroje labai dažnai yra pateikiamas abstraktus elektroninės erdvė apibrėžimas. Tarkim, M. Kiškis, R. Petrauskas, I. Rotomskis ir D. Štitilis teigia, kad elektroninė erdvė – tai pasaulinė viešai ir visuotinai prieinama kompiuterių tinklų sistema, per kurią yra keičiamasi informacija [111]. Labai panašus abstraktus el. erdvės apibrėžimas yra naudojamas daugelyje mokslinių publikacijų. Bet tokio pobūdžio apibrėžimai neatsako į klausimą kokie elementai sudaro el. erdvę, todėl nėra aišku ką ji apima, o ko ne. Politiniai – kariniai dokumentai el. erdvės elementų atžvilgiu yra tikslesni. Pavyzdžiui, NATO Cooperative Cyber Defense Center of Excellence parengtame

---

[106] „Google LLC v Bundesrepublik Deutschland“, *Curia*, žiūrėta 2020 m. rugsėjo 1 d., http://curia.europa.eu/juris/document/document.jsf?text=&docid=214944&pageIndex=0&doclang=EN&mode=req&dir=&occ=first&part=1.

[107] „2018 m. gruodžio 11 d. Europos Parlamento ir Tarybos direktyva (ES) 2018/1972, kuria nustatomas Europos elektroninių ryšių kodeksas“, *EUR-Lex*, žiūrėta 2020 m. rugsėjo 1 d., https://eur-lex.europa.eu/legal-content/LT/TXT/?uri=CELEX:32018L1972.

[108] Elena Gil González, Paul De Hert ir Vagelis Papakonstantinou, „The Proposed ePrivacy Regulation: The Commission's and the Parliament's Drafts at a Crossroads?“, Brussels Privacy Hub, Working Paper, Vol 6, No. 20, 2020.

[109] Saskia Sassen, „Electronic Space and Power“, *Journal of Urban Technology* 4, no. 1 (April 1997): 1–17, doi:10.1080/10630739708724545.

[110] Franklink D. Kramer, „Cyberpower and National Security: Policy Recommendations for a Strategic Framework“, National defence University Press, žiūrėta 2020 m. rugsėjo 4 d., https://ndupress.ndu.edu/Portals/68/Documents/Books/CTBSP-Exports/Cyberpower/Cyberpower-I-Chap-01.pdf?ver=2017-06-16-115055-617 .

[111] Mindaugas Kiškis ir kt., *Teisės informatika ir informatikos teisė: vadovėlis*, (Vilnius: Mykolo Romerio universitetas, 2006), 11.

Talino vadove (angl. *Tallinn Manual*) teigiama, kad elektroninė erdvė – tai „aplinka, susidedanti iš fizinių ir nefizinių komponentų, kuriai būdingas kompiuterio įtaisų ir elektromagnetinio spektro panaudojimas duomenims saugoti, modifikuoti ir keistis per kompiuterių tinklą“[112]. Kompiuteris Talino vadove yra apibrėžiamas kaip neintegruotas (pvz. asmeninis kompiuteris, išmanus telefonas, tinklo serveris) ir integruotas (pvz. į radaro sistemą, orlaivį) duomenis tvarkantis įrenginys[113]. Pentagono Karinių ir susijusių terminų žodyne (angl. *Dictionary of Military and Assosiated Terms*) elektroninė erdvė apibrėžiama kaip globali informacinės aplinkos sritis, susidedanti iš nepriklausomų informacinių technologijų infrastruktūros tinklų, įskaitant internetą, telekomunikacijų tinklus, kompiuterių sistemas, valdytojus ir tvarkytojus[114]. Tačiau tiksliausias elektroninės erdvės apibrėžimas buvo pateiktas JAV kariuomenės užsakytame tyrime, kurį vykdė Harvardo ir Stanfordo universitetų mokslininkų grupė[115]. Mokslininkų grupės teigimu elektroninė erdvė yra globali ir dinamiška aplinka (nuolat besikeičianti) apibūdinama elektronų ir elektromagnetinio spektro naudojimu tam, kad būtų sukurta, saugoma, modifikuojama, besikeičiama, dalijamasi ir ištraukiama informacija. Elektroninė erdvė apima:

a) fizinę infrastruktūrą ir telekomunikacijų įrenginius plačiąja prasme, kurie dalyvauja kompiuterių tinklų ryšyje (SCADA[116] įrenginius, išmaniuosius telefonus, plančetes, kompiuterius, serverius ir t. t.);
b) kompiuterių sistemas ir susijusią programinę įrangą, kuri užtikrina aplinkos operacines funkcijas ir ryšius;
c) tinklus tarp kompiuterių sistemų;
d) tinklų tinklus, kurie jungia kompiuterių sistemas;
e) vartotojų prieigos ir tarpinių maršrutų taškus;
f) duomenis (angl. *constituent data or resident data*)[117].

Disertacijoje bus vadovaujamasi pastaraja el. erdvės samprata, nors Lietuvos Respublikos kibernetinio saugumo įstatyme yra pateikta siauresnė elektroninės erdvės samprata neapimanti aukščiau pateikto apibrėžimo c, d ir e punktų.

Elektroninės erdvės sąvoka teisinėje literatūroje yra vartojama apibrėžiant pvz. nusikaltimus (angl. *cyber crimes*, rečiau vartojamas *electronic crimes*), jurisdikciją (angl. *jurisdiction in cyber space*)[118], interneto[119], informacinių technologijų (informatikos)[120]

---

112 „Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations“, *Cambridge University Press*, 211.

113 *Ibid.*, 210.

114 Marco Mayer ir Luigi Martino, „International Politics in the Digital Age“, 8, žiūrėta 2020 m. rugsėjo 4 d., https://www.academia.edu/14336129/International_Politics_in_the_Digital_Age.

115 *Ibid.*, 5.

116 Supervizorinio valdymo ir duomenų atvaizdavimo sistema.

117 Mayer ir Martino, *supra note*,114.

118 Alan Davidson, „Jurisdiction in Cyberspace“, *The Law of Electronic Commerce* (Cambridge University Press, 2009), doi:10.1017/CBO9780511818400.011.

119 Darius Štitilis ir kt., *Interneto ir technologijų teisė: vadovėlis*, Teisinė literatūra (Vilnius: Registrų centras, 2016).

120 Mindaugas Kiškis ir kt.., *Teisės informatika ir informatikos teisė: vadovėlis*, (Vilnius: Mykolo Romerio universitetas, 2006).

ar elektroninių ryšių teisę[121]. Kibernetinės erdvės ir elektroninės erdvės sąvokos yra vartojamos kaip sinonimai. Tačiau elektroniniai ryšiai, internetas ir elektroninė erdvė nėra tapačios sąvokos, todėl nevartotinos kaip sinonimai[122]. Elektroninės ar kibernetinės erdvės sąvokos vartojimo pasirinkimas priklauso nuo konteksto. Pvz., literatūroje anglų kalba pačiai erdvei apibrėžti dažniau yra naudojama kibernetinės erdvės sąvoka[123], tačiau paslaugos vadinamos ne kibernetinėmis, o elektroninėmis[124]. Lietuvoje kibernetinės erdvės apibrėžimas yra įtvirtintas Kibernetinio saugumo įstatyme nurodant, kad tai yra aplinka, kurią sudaro kompiuteriai ir kita ryšių ir informacinių technologijų įranga ir juose sukuriama ir (arba) jais perduodama elektroninė informacija[125]. Tačiau, pvz. Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatyme, Lietuvos Respublikos saugios laivybos įstatyme, Lietuvos Respublikos asmens tapatybės kortelės ir paso įstatyme yra vartojama ir elektroninės erdvės sąvoka, nors jos apibrėžimo nei viename iš jų nėra pateikto. Pačiame Kibernetinio saugumo įstatyme įtvirtintame kibernetinės erdvės apibrėžime taip pat yra vartojamas ne kibernetinės, bet elektroninės informacijos terminas, kuris, vadovaujantis Kibernetinio saugumo įstatymo 2 str. 2 d., apima ir informaciją, ir duomenis. *Convention on Cybercrime*[126] lietuvių kalba yra vadinama Konvencija dėl elektroninių nusikaltimų[127]. Tokio pobūdžio nusikaltimai lietuvių kalba yra vadinami elektroniniais nusikaltimais arba nusikaltimais elektroninėje erdvėje[128], nors angliškai paprastai vartojama *cybercrime* sąvoka. Asmens duomenų rinkimas elektroninėje erdvėje teisėsaugos ir žvalgybos tikslais angliškai paprastai yra vadinamas „*electronic surveillance*“[129]. Asmens duomenų rinkimui elektroninėje erdvėje kariniais tikslais gali būti vartojama „*cyber collection*“[130] sąvoka. Sąvokos „*electronic surveillance*“ apimtis taip pat yra traktuojama skirtingai. Gali būti laikoma, kad ji apima tik el. ryšių tinklais perduodamų duomenų rinkimą ir stebėseną[131], bet gali būti suvokiama ir plačiau – kaip apimanti asmens duomenų rinkimą visoje el. erdvėje[132] tiek teisėsaugos, tiek žvalgybos tikslais. Pastaruoju požiūriu bus vadovaujamasi ir šioje disertacijoje.

---

121 Irmantas Jarukaitis, *Elektroninių ryšių teisė* (Vilnius: Eugrimas, 2005).

122 „Developments in the Law: The Law of Cyberspace“, *Harvard Law Review* 112, no. 7 (May 1999): 1574, doi:10.2307/1342414.

123 Nors yra vartojama ir elektroninės erdvės sąvoka. Žr. pvz. Saskia Sassen (1997) Electronic space and power, Journal of Urban Technology, 4:1, 1-17, DOI: 10.1080/10630739708724545.

124 Žr. pvz., Ida Lindren ir Gabriella Jansson, „Electronic services in the public sector: A conceptual framework“, *Government Information Quarterly*, 30(2) (2013):163–172.

125 „Lietuvos Respublikos kibernetinio saugumo įstatymas“, *eTar*, žiūrėta 2020 m. rugsėjo 10 d., https://www.e-tar.lt/portal/lt/legalAct/5468a25089ef11e4a98a9f2247652cf4/asr.

126 „Convention on Cybercrime“, *Council of Europe*, žiūrėta 2020 m. rugsėjo 10 d., https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185.

127 „Konvencija dėl elektroninių nusikaltimų“, *eSeimas*, žiūrėta 2020 m. rugsėjo 10 d., https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/TAIS.228195.

128 Marcinauskaitė, *supra note*, 36.

129 Carr ir Bellia, *supra note,* 21.

130 Jacob G. Oakley, „Cyber Collection“, in *Waging Cyber War: Technical Challenges and Operational Constraints*, ed. Jacob G. Oakley (Berkeley, CA: Apress, 2019), 57–70, doi:10.1007/978-1-4842-4950-5_5.

131 Carr ir Bellia, *supra note,* 21.

132 Jonathan Mayer, Patrick Mutchler ir John C. Mitchell, „Evaluating the Privacy Properties of Telephone Metadata“, *Proceedings of the National Academy of Sciences* 113, no. 20 (May 17, 2016): 5536–41, doi:10.1073/pnas.1508081113.

Asmens duomenys elektroninėje erdvėje. Nuo 2013 m. moksliniuose straipsniuose apie asmens duomenų stebėseną el. erdvėje teisėsaugos ir žvalgybos tikslais dažnai yra vartojamos dvi sąvokos: komunikacijos turinys (angl. *content of communcation*) ir metaduomenys (angl. *metadata*). Tokio asmens duomenų skirstymo ištakos yra siejamos su JAV teismo 1878 m. sprendimu byloje *Ex parte Jackson*[133]. Pastarojoje byloje teismas atskyrė popieriniame voke esančio laiško turinį nuo visos kitos informacijos, kurią galima sužinoti apie tą laišką, jo neatplėšus – siuntėją, gavėją, jų adresus, siuntimo laiką, datą, netgi laiško svorį. Panašiai ir dabar yra išskiriamas komunikacijos turinys ir metaduomenys[134].

Komunikacijos turinys yra pati žinutė[135]. Komunikacijos el. erdvėje turinio pavyzdžiu yra el. laiškas, sms žinutė, Viber, WhatsApp žinutė, pokalbis telefonu ir kt. Komunikacijos turinio išraiškos forma gali būti įvairi: tekstinė, grafinė, vaizdinė arba garsinė. Tačiau, yra manoma, kad komunikacijos turiniu gali būti laikoma tik privataus pobūdžio informacija. Todėl, pvz. žinutės ant socialinių tinklų sienos, viešos Twitter žinutės (postai) dalies mokslininkų yra nelaikomos komunikacijos turiniu[136]. Tačiau viešas prieinamumas nereiškia informacijos buvimo asmens duomenimis paneigimo[137]. Todėl dalis mokslininkų atviro kodo žvalgybos (angl. *open source intelligence)* naudojamus duomenis laiko asmens duomenimis. Kita dalis palaiko žvalgybos institucijas šių duomenų nelaikydami asmens duomenimis[138]. EŽTT 2004 m. byloje *Editions Plon v. France* konstatavo, kad kai asmeninė informacija paskelbiama internete, poreikis ją apsaugoti nebegali būti laikomas prioritetiniu, nes praktikoje pripažįstama, kad ji tapo paskelbta plačiu mastu ir nuo to laiko nebelaikoma konfidencialia[139]. Tačiau 2010 m. EŽTT pateikė paaiškinimą, kad net ir netekus konfidencialumo apsaugos, turi būti garantuojama privataus gyvenimo ir reputacijos apsauga[140]. Pasak M. Civilkos minimas EŽTT sprendimas atskleidžia reikšmingą takoskyrą tarp asmens duomenų viešumo ir jų apsaugos – pats duomenų paviešinimas nesuteikia teisės juos naudoti

---

133 Steven M. Bellovin ir kt., „It's Too Complicated: How the Internet Upends Katz, Smith, and Electronic Surveillance Law", *Harvard Journal of Law & Technology (Harvard JOLT)* 30, no. 1 (2017 2016): 1–102.

134 *Ibid.*

135 „Content Communication, Relational Communication", *Hanging the Mirror*, žiūrėta 2020 m. rugsėjo 1 d., https://hangingthemirror.com/2018/02/13/content-communication-relational-communication-1-of-2/.

136 Jemima Stratford ir Tim Johnston, „The Snowden 'Revelations': Is GCHQ Breaking the Law?", *European Human Rights Law Review* 2014, no. 2 (2014): 129–41.

137 Danah Boyd, „Privacy and Publicity in the Context of Big Data", žiūrėta 2020 m. rugsėjo 1 d., https://www.danah.org/papers/talks/2010/WWW2010.html.

138 Quirine Eijkman ir Daan Weggemans, „Open Source Intelligence and Privacy Dilemmas: Is It Time to Reassess State Accountability Special Section: Security versus Privacy: What Is Europe Heading For", *Security and Human Rights* 23, no. 4 (2012): 285–96.

139 „Éditions Plon v. France", *European Court of Human Rigghts*, žiūrėta 2020 m. rugsėjo 1 d., https://hudoc.echr.coe.int/eng#{%22fulltext%22:[%22%C3%89ditions%20Plon%20v.%20France%22],%22documentcollectionid2%22:[%22GRANDCHAMBER%22,%22CHAMBER%22],%22itemid%22:[%22001-61760%22]} .

140 „Europos žmogaus teisių teismo 2010 m. gruodžio 16 d. sprendimas byloje Aleksey Ovchinnikov v. Russia", *Hudoc*, žiūrėta 2020 m. rugsėjo 1 d., https://hudoc.echr.coe.int/eng#{%22fulltext%22:[%22Aleksey%20Ovchinnikov%20v.%20Russia%22],%22documentcollectionid2%22:[%22GRANDCHAMBER%22,%22CHAMBER%22],%22itemid%22:[%220-01-102322%22]}.

kitais tikslais nei tais, dėl kurių jie buvo paviešinti internete[141]. Analogiška ir JAV teisės mokslininkės H. Nissenbaum pozicija[142].

Komunikacijos turinys el. erdve yra perduodamas ne mums įprastai matoma forma (žodine, video ar paveikslėlio), bet užšifruotas (angl. *encrypted*). Apie tai, kad tuo metu buvusiomis moderniomis ryšių perdavimo priemonėmis perduodama komunikacija turi būti šifruojama 1976 m. moksliniame darbe rašė W. Diffie ir M. Hellman[143]. JAV stengėsi kontroliuoti komunikacijos turinio šifravimą. Iki 2000 m. JAV draudė savo įmonėms jų sukurtas šifravimo priemones parduoti į kitas šalis. Todėl likusiame pasaulyje buvo naudojama paprastesnė šifravimo sistema nei JAV[144]. Kita vertus, JAV iki 1997 m. galiojo „key escrow" sistema, įpareigojusi JAV el. erdvės paslaugas ir technologijas teikiančias įmones suteikti komunikacijos atšifravimo raktus JAV Vykdomajai valdžiai[145]. Tačiau tokia griežta JAV kontrolė dėl el. erdve perduodamo komunikacijos turinio šifravimo bei noras turėti atšifravimo kodus sąlygojo didelius JAV įmonių nuostolius ir buvo kritikuojama pasauliniu mastu. 2015 m. Jungtinių Tautų Specialusis pranešėjas Žmogaus teisių tarybai teigdamas, kad „valstybės turi vengti imtis priemonių, tokių kaip atgalinės durys, silpna šifravimo sistema bei „key escrow", kurios susilpnina žmonių saugumą el. erdvėje[146], sulaukė tarptautinio teisėsaugos institucijų palaikymo[147]. Tačiau nuo 2015 m. debatai dėl šifravimo nenurimo, o tik dar labiau aštrėjo[148], ypač plačiai pradėjus naudoti ištisinį šifravimą (angl. *end to end encryption*). Ištisinis šifravimas nuo kitų šifravimų būdų skiriasi tuo, kad tik informacijos siuntėjo ir informacijos gavėjo įrenginiai turi užšifravimo ir atšifravimo kodus. El. erdvėje perimto tokios komunikacijos turinio negali atšifruoti žvalgybos ir teisėsaugos institucijos, o paslaugas el. erdvėje teikiantys juridiniai asmenys nesutinka kurti ištisinio šifravimo atšifravimo kodų arba spragas (angl. *backdoor*), kad teisėsaugos ir žvalgybos institucijos galėtų perskaityti turinį[149]. Dauguma paslaugų el. erdvėje teikėjų (pvz.

---

141 Civilka ir Šlapimaitė, *supra note,* 37.

142 Helen Nissenbaum, „Privacy as Contextual Integrity Symposium – Technology, Values, and the Justice System", *Washington Law Review* 79, no. 1 (2004): 119–58.

143 Whitfield Diffie ir Martin E. Hellman, „New Directions in Cryptography", *IEEE Transactions on Information Theory* 22, no. 6 (1976): 644–54, žiūrėta 2020 m. rugsėjo 1 d., https://ee.stanford.edu/~hellman/publications/24.pdf.

144 „Doomed to Repeat History? Lessons from the Crypto Wars of the 1990s", *New America*, žiūrėta 2020 m. rugsėjo 1 d., http://newamerica.org/cybersecurity-initiative/policy-papers/doomed-to-repeat-history-lessons-from-the-crypto-wars-of-the-1990s/.

145 Mirja Gutheil ir Quentin Liger, „Legal Frameworks for Hacking by Law Enforcement: Identification, Evaluation and Comparison of Practices", *European Parlament,* 2017, 18, žiūrėta 2020 m. rugpjūčio 22 d., https://www.europarl.europa.eu/RegData/etudes/STUD/2017/583137/IPOL_STU(2017)583137_EN.pdf.

146 David Kaye, „Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, A/HRC/29/32", 2015, žiūrėta 2020 m. rugsėjo 1 d., https://ap.ohchr.org/documents/dpage_e.aspx?si=A/HRC/29/32.

147 „On Lawful Criminal Investigation That Respects 21st Century Data Protection – Europol and ENISA Joint Statement", *Europol*, žiūrėta 2020 m. rugpjūčio 22 d., https://www.europol.europa.eu/publications-documents/lawful-criminal-investigation-respects-21st-century-data-protection-europol-and-enisa-joint-statement-0.

148 Harold Abelson ir kt., „Keys Under Doormats: Mandating Insecurity by Requiring Government Access to All Data and Communications", 2015, žiūrėta 2020 m. rugsėjo 1 d., https://dspace.mit.edu/handle/1721.1/97690.

149 „The Government Wants Tech Companies to Give Them a Backdoor to Your Electronic Life", *The Guardian*, žiūrėta 2020 m. rugsėjo 1 d., https://www.theguardian.com/commentisfree/2014/oct/17/government-internet-backdoor-surveillance-fbi.

Viber, WhatsApp, Facebook, Gmail, TikTok ir kt.) turinio perdavimui el. erdve naudoja ištisinį šifravimą. Vadinasi, nors žvalgybos ir teisėsaugos institucijos ir surenka užšifruotą el. komunikacijos el. erdve turinį, tačiau perskaityti gali tik tą, kuris nėra užšifruotas ištisiniu šifravimu.

Metaduomenys. Iki E. Snowden informacijos apie NSA masinį asmens duomenų rinkimą nutekinimo, JAV teismai ir mokslininkai metaduomenų nelaikė asmens duomenimis, arba laikė juos mažesnį pavojingumą asmens privatumui keliančiais duomenimis nei komunikacijos turinys[150] JAV teisės aktuose taip pat paprastai yra numatytos paprastesnės procedūros tokių duomenų rinkimui[151], o ES ir ES valstybių narių nacionaliniuose teisės aktuose metaduomenų sąvoka iš viso nėra vartojama[152]. Dažniausiai metaduomenys yra apibrėžiami kaip duomenys apie duomenis. Bet ką tai reiškia ir kokie tai duomenys yra?

J. Pomerantz kiekvieną knygos „Metadata" skyrių pradeda teiginiu, kad metaduomenys visada supa mus[153]. Ir jeigu viskas vyksta technologiškai tvarkingai, mes to niekada nežinome ir nejaučiame. Dėl šios priežasties apie metaduomenų reikšmę ir panaudojimo galimybes diskusijos prasidėjo tik 2013 m. E. Snowden per dienraštį *The Guardian* paviešinus informaciją apie JAV Nacionalinės žvalgybos agentūros (NSA) vykdytas masines metaduomenų rinkimo programas[154]. Šiandien metaduomenys asocijuojasi su technologijomis. Tačiau pirmosios metaduomenų kūrėjos ir naudotojos yra bibliotekos. Pirmoji metaduomenų forma yra knygų bibliografiniai aprašai, pirmą kartą pradėti naudoti 235 m. prieš Kristų Aleksandrijos bibliotekoje ir sukurti ne informacinių technologijų specialisto, o rašytojo Challimachus[155]. Todėl įsivaizduoti kas yra metaduomenys yra paprasčiau naudojantis knygų bibliografijos aprašo nei el. laiško ar skambučio pavyzdžiu. Knygos bibliografinius duomenis paprastai sudaro knygos pavadinimas, autorius, išleidimo data, tematika, vieta bibliotekos lentynose ir puslapių skaičius. Tai yra išoriniai metaduomenys apie knygą. Tačiau kiekviena knyga savyje taip pat turi metaduomenis. Dalis jų sutampa su bibliografinio aprašo duomenis, tačiau šie duomenys yra daug platesni – tai ir knygos viršeliai ir paprastai pirmame vidiniame ir (arba) paskutiniame lape esanti bibliografinė informacija, netgi knygos turinys.

Dauguma mūsų, jau skaitydami knygą, sąmoningai neskaito jos bibliografinių metaduomenų. Todėl gali kilti klausimas, kam metaduomenys yra reikalingi. Atsakymą

---

150 Russell A. Miller, *Privacy and Power: A Transatlantic Dialogue in the Shadow of the NSA-Affair* (Cambridge University Press, 2017), 369.

151 Plačiau apie tai trečiame disertacijos skyriuje.

152 Sophie Stalla-Bourdillon, Evangelia Papadaki ir Tim Chown, „Metadata, Traffic Data, Communications Data, Service Use Information... What Is the Difference? Does the Difference Matter? An Interdisciplinary View from the UK", SSRN Scholarly Paper (Rochester, NY: Social Science Research Network, 2015), 1, https://papers.ssrn.com/abstract=2625181.

153 Jeffrey Pomerantz, *Metadata*, The MIT Press Essential Knowledge Series (Cambridge, Massachusetts ; London, England: The MIT Press, 2015).

154 Glenn Greenwald, Ewen MacAskill ir Laura Poitras, „Edward Snowden: The Whistleblower behind the NSA Surveillance Revelations", *The Guardian*, 2013, žiūrėta 2020 m. rugsėjo 1 d., https://www.theguardian.com/world/2013/jun/09/edward-snowden-nsa-whistleblower-surveillance.

155 Pomerantz, *supra note*, 153: 6.

galima iliustruotu A. Korzybski mintimi, kad ir „žemėlapis nėra teritorija“[156]. Kalbą, A. Korzybski prilygino žemėlapiui sakydamas, kad žodis apie daiktą nereiškia paties daikto, bet yra to daikto apibūdinimas. Analogiškai, metaduomenis mes galime prilyginti „žemėlapiui“. Metaduomenų dėka mes galime susidaryti įspūdį apie, šiuo atveju, knygą – profiliuoti – bei surasti jos vietą net ir didžiausioje bibliotekoje. Tikėtina dėl to, metaduomenys daugelio yra apibrėžiami kaip duomenys apie duomenis[157]. Tačiau IT prasme duomenys reiškia visiškai skirtingus dalykus. Duomenys (angl. *data*) IT prasme yra „žalia“ medžiaga, dažnai egzistuojanti 0 ir 1 pavidalu ir žmogui nesuteikianti jokios informacijos ir yra reikalinga informacijos judėjimui tarp įrenginių[158]. Teisine prasme žodis „duomenys“ paprastai prilyginamas informacijai, bet iš tikrųjų jie nėra lygu informacijai, o ja tampa tada, kai įrenginiai juos iššifruoja į žmogui suprantamos informacijos formą[159]. Todėl metaduomenų apibrėžimas kaip duomenų apie duomenis nėra tikslus. Jų esmę tiksliau perteikia J. Pomerantz pateiktas apibrėžimas – kad tai yra teiginiai apie potencialų informacijos objektą[160]. Todėl, autorės nuomone, ir JAV vartojama asmenį identifikuojančios informacijos terminas (angl. *personal identifical information*) vietoj Europoje vartojamo asmens duomenų sąvokos technologine prasme tikslesnis. Tačiau, siekiant išvengti dviprasmybių, disertacijoje tiek kalbat apie metaduomenis, tiek apie turinio duomenis bus naudojama asmens duomenų sąvoka.

Metaduomenys egzistuoja ne tik el. erdvėje ir į tipus gali būti skirstomi įvairiai. Pavyzdžiui, J. Pomerantz metaduomenis skirsto į:

1) aprašomuosius (angl. *descriptive*);
2) administracinius (angl. *administrative)*;
3) struktūrinius (angl. *structural*);
4) saugojimo (angl. *preservation*);
5) naudojimo (angl. *use*).

Tačiau ne visi metaduomenys yra asmens duomenys[161]. Todėl disertacijai aktualiausiais yra S. Stalla-Bourdillon, E. Papadaki ir T. Chown naudojamas asmens duomenis sudarančių komunikacijos el. erdvėje metaduomenų grupavimas. Autoriai mokslinėje publikacijoje iliustruoja, jog tie patys duomenys technologiniu požiūriu gali būti skirtingu pavidalu. Metaduomenys el. erdvėje gali būti informacija apie perduodamą komunikaciją (angl. *communication in transit*) arba informacija apie jau perduotą ir asmeniui matomą komunikaciją (angl. *storred communication*). Minėti autoriai metaduomenis skirsto į:

1) tinklo lygio metaduomenis (angl. *network level metadata*);

---

156 Alfred Korzybski, *A Non-Aristotelian System and Its Necessity for Rigour in Mathematics and Physics: Abstract*, 1931, 745.

157 Bryce Newell ir Joseph Tennis, „Me, My Metadata, and the NSA: Privacy and Government Metadata Surveillance Programs“, 2014, doi:10.9776/14109.

158 Pomerantz, *supra note*, 153: 20.

159 *Ibid*.

160 *Ibid*., 26.

161 „Not Everything Is About You – Including Your Metadata“, *Digby von Muenster*, 2017, žiūrėta 2020 m. rugpjūčio 23 d., https://www.dvmlaw.com/not-everything-including-metadata/.

2) programos lygio metaduomenis (angl. *application level metadata*);
3) paslaugos naudojimo metaduomenis (angl. *service use metadata*)[162].

Tinklo ir programos lygio metaduomenys yra duomenys apie el. erdvėje perduodamą informaciją, o paslaugos naudojimo metaduomenys yra duomenys apie jau perduotą komunikaciją ir yra renkami ir saugomi serveriuose[163].

Tinklo lygio metaduomenys yra reikalingi siunčiančio ir gaunančio įrenginio tarpusavio komunikacijai per IP adresą ir atrodo pvz. taip:
Siuntėjo IP: 152.78.64.100
Gavėjo IP: 212.58.224.83
Siuntėjo uostas (port): 53100
Gavėjo uostas (port): 80
Protokolas: TCP.

Vadinasi, tinklo lygio metaduomenys gali atskleisti nedidelę asmens duomenų dalį. Programos lygio metaduomenys apima visus komunikacijos el. erdvėje duomenis. El. erdvėje perduodamų duomenų (informacijos realiu laiku) paketą sudaro ne tik tai, kas paprastai teisės aktuose yra laikoma metaduomenimis (pvz. siuntėjo/gavėjo el. pašto adresai, el. laiško tema, specialūs URL), bet ir komunikacijos turinio duomenys, kurie gali būti užšifruoti (angl. *encrypted*) arba neužšifruoti (angl. *not encrypted*). Tai reiškia, kad komunikacijos perdavimo metu, technologiniu požiūriu, jos turinys taip pat yra metaduomenimis. Tinklo lygio duomenų rinkimo technologija nėra sudėtinga[164]. Perrimti programos lygio metaduomenis yra reikalinga sudėtingesnė technologija, tačiau tai padaryti įmanoma. Perėmus programos lygio metaduomenis, tuo atveju, jeigu turinys nėra užkoduotas, arba kitaip yra užkoduotas naudojant TL kodavimą (angl. *transport layer encryption*), jį galima perskaityti. Paprastai, tokiu atveju teisėsaugos ir žvalgybos institucijos turi kreiptis į elektroninių paslaugų teikėjus. Tačiau dauguma komunikacijos el. erdvėje priemonių (pvz. Messenger, Instagram, WhatsApp) naudoja ištisinio kodavimo sistemas (angl. *end to end encryption*). Tokiu atveju, tik gavėjas ir siuntėjas gali perskaityti komunikacijos el. erdvėje turinį, kadangi šifravimo ir iššifravimo kodus turi tik siuntėjo ir gavėjo įrenginiai, o ne paslaugų teikėjas ar el. ryšių tinklų operatorius. Debatai dėl privalomo įrankio teisėsaugai ir žvalgybai atšifruoti užšifruotą komunikacijos el. erdvėje turinį JAV yra vadinasi „amžinais"[165]. Kol kas JAV nėra priimtas teisės aktas įpareigojantis paslaugų el. erdvėje teikėjus sukurti spragas teisėsaugos ir žvalgybos institucijoms. Tačiau toks aktas buvo priimtas Australijoje[166].

---

[162] Stalla-Bourdillon, Papadaki ir Chown, *supra note*, 152:5.

[163] *Ibid.*

[164] Stalla-Bourdillon, Papadaki ir Chown, *supra note*, 152:6.

[165] „What Is End-to-End Encryption? Another Bull's-Eye on Big Tech", *The New York Times*, žiūrėta 2020 m. rugpjūčio 23 d., https://www.nytimes.com/2019/11/19/technology/end-to-end-encryption.html.

[166] Jonathan Mayer, „Content Moderation for End-to-End Encrypted Messaging", 9, žiūrėta 2020 m. rugsėjo 4 d., https://www.cs.princeton.edu/~jrmayer/papers/Content_Moderation_for_End-to-End_Encrypted_Messaging.pdf Jamie Tarabay, „Australian Government Passes Contentious Encryption Law", *The New York Times*, December 6, 2018, sec. World, žiūrėta 2020 m. rugsėjo 4 d., https://www.nytimes.com/2018/12/06/world/australia/encryption-bill-nauru.html.

Trečioji metaduomenų grupė – paslaugos naudojimo metaduomenys – apima tinklo lygio metaduomenis ir programos lygio metaduomenis. Pagrindinis skirtumas tarp jų yra tas, kad paslaugos naudojimo metaduomenys neapima komunikacijos turinio ir yra saugomi serveriuose. Tie patys metaduomenys tuo metu kol jie yra perduodami el. ryšio tinklu, yra tinklo lygio ir programos lygio metaduomenimis.

Komunikacijos elektroninėje erdvėje metaduomenų sąvoka yra vartojama JAV, o Europoje yra vartojamos srauto duomenų (angl. *traffic data*) ir vietos nustatymo duomenų (angl. *location data*) sąvokos. Ar galime šias tris sąvokas laikyti tapačiomis?

Lietuvos Respublikos elektroninių ryšių įstatyme srauto duomenys yra apibrėžiami kaip duomenys, tvarkomi siekiant perduoti informaciją elektroninių ryšių tinklu ir (arba) tokio perdavimo apskaitai (3 str. 57 p.). Vietos nustatymo duomenys – elektroninių ryšių tinkluose arba teikiant elektroninių ryšių paslaugas tvarkomi duomenys, nurodantys faktinio elektroninių ryšių paslaugų naudotojo galinių įrenginių geografinę buvimo vietą (3 str. 81 p.). 2006 m. kovo 15 d. Europos Parlamento ir Tarybos direktyvoje 2006/24/EB dėl duomenų, generuojamų arba tvarkomų teikiant viešai prieinamas elektroninių ryšių paslaugas arba viešuosius ryšių tinklus, saugojimo (toliau – Duomenų saugojimo direktyva)[167] buvo pateiktas srauto ir vietos nustatymo duomenų sąrašas. Srauto duomenys apima duomenis būtinus:

1) ryšio šaltiniui nustatyti ir išsiaiškinti[168];

2) ryšio paskirties taškui nustatyti[169];

3) ryšio datai, laikui ir trukmei nustatyti[170];

---

[167] 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

[168] 1) susiję su fiksuoto telefono ryšio tinklu ir judriuoju telefono ryšiu:
   i) telefono numeris, iš kurio skambinta;
   ii) abonento ar registruoto naudotojo vardas ir pavardė (pavadinimas) bei adresas;
2) susiję su interneto prieiga, interneto elektroniniu paštu ir interneto telefonija:
   i) suteikti naudotojų atpažinimo kodai;
   ii) naudotojo atpažinimo kodas ir telefono numeris, suteikti bet kokiam ryšiui, patenkančiam į viešąjį telefono tinklą;
   iii) abonento ar registruoto naudotojo, kuriam ryšio metu buvo suteiktas interneto protokolo (IP) adresas, naudotojo atpažinimo kodas ar telefono numeris, vardas ir pavardė (pavadinimas) ir adresas.

[169] 1) susiję su fiksuoto telefono ryšio tinklu ir judriuoju telefono ryšiu:
   i) rinktas telefono numeris ar numeriai (telefono numeris (-iai), į kurį (-iuos) skambinta), o papildomų paslaugų, pvz., skambučių peradresavimo ar skambučių persiuntimo atvejais – telefono numeris arba numeriai, į kuriuos nukreiptas skambutis;
   ii) abonento (-ų) ar registruoto (-ų) naudotojo (-ų) vardas (-ai) ir pavardė (-s) (pavadinimas (-ai)) bei adresas (-ai);
2) susiję su internetu perduodamu elektroniniu paštu ir internetine telefonija:
   i) telefono skambučių internetu numatomo (-ų) gavėjo (-ų) naudotojo atpažinimo kodas ar telefono numeris;
   ii) abonento (-ų) ar registruoto (-ų) naudotojo (-ų) vardas (-i) ir adresas (-i) ir telefono skambučių internetu numatomo (-ų) gavėjo (-ų) naudotojo atpažinimo kodas;

[170] 1) susiję su fiksuoto telefono ryšio tinklu ir judriuoju telefono ryšiu – ryšio pradžios ir pabaigos laikas bei data;
2) susiję su prieiga prie interneto, internetu perduodamu elektroniniu paštu ir internetine telefonija:
   i) prisijungimo prie interneto ir atsijungimo nuo interneto prieigos paslaugų data ir laikas tam tikroje laiko juostoje ir dinamiškas ar statiškas interneto protokolo (IP) adresas, kurį ryšiui suteikė prieigos prie interneto paslaugos teikėjas, ir abonento ar registruoto naudotojo atpažinimo kodas;
   ii) prisijungimo prie interneto ir atsijungimo nuo internetu perduodamo elektroninio pašto paslaugos ar internetinės telefonijos paslaugos data ir laikas tam tikroje laiko juostoje;

4) ryšio tipui nustatyti[171];

5) naudotojų ryšio įrangai ar tam, kas turėtų būti ryšio įranga, nustatyti [172].

Vietos nustatymo duomenys apima duomenis būtinus judriojo ryšio įrangos vietai nustatyti[173].

Taigi, srauto duomenys yra metaduomenimis, kuriuos tvarko el. ryšių tinklų paslaugų teikėjai. Tačiau el. erdvėje metaduomenis tvarkyti gali ne tik el. ryšių tinklų paslaugų teikėjai, bet ir visi paslaugų el. erdvėje teikėjai. Pastarųjų tvarkomi metaduomenys yra platesnės apimties nei el. ryšio tinklų paslaugų teikėjų. Pavyzdžiui, vietos nustatymo duomenis el. ryšių tinklų paslaugų teikėjai renka vadovaudamiesi įrenginio prisijungimo prie el. ryšio bokšto informacija. Tuo tarpu Google Maps vietos nustatymo duomenis renka pagal GPS signalo informaciją. GPS signalas nėra perduodamas el. ryšių tinklų teikėjų, todėl neapima vietos nustatymo duomenų pagal El. ryšių direktyvą arba Lietuvos Respublikos elektroninių ryšių įstatymą. Tačiau šie duomenys yra metaduomenimis. Metaduomenimis taip pat yra ir komunikacijos el. erdvėje turinys jo perdavimo el. erdve metu. Vadinasi, metaduomenų sąvoka yra platesnė už srauto ir vietos nustatymo duomenų sąvokas.

Nors metaduomenų sąvokos vartojimas atsirado dėl JAV įtakos ir nei ES, nei valstybių narių galiojančiuose teisės aktuose kol kas nėra naudojamas komunikacijos elektroninėje erdvėje kontekste[174], tačiau tai, kad ši sąvoka yra įtvirtinta Reglamento dėl teisės į privatų gyvenimą ir asmens duomenų apsaugos elektroninių ryšių projekte rodo, kad ji netrukus bus pradėta naudoti i ES teisės aktuose[175]. Reglamento dėl teisės į privatų gyvenimą ir asmens duomenų apsaugos elektroninių ryšių pasiūlymo projekte yra įtvirtinta, kad elektroninių ryšių duomenys yra elektroninių ryšių turinys ir elektroninių ryšių metaduomenys (Pasiūlymo 4 str. 3 d. a p). Elektroninių ryšių

---

171 1) susiję su fiksuoto telefono ryšio tinklu ir judriuoju telefono ryšiu – telefoninio ryšio paslauga, kuria pasinaudota;
2) susiję su interneto prieiga, internetu perduodamu elektroniniu paštu ir internetine telefonija — interneto paslauga, kuria pasinaudota;

172 1) susiję su fiksuoto telefono ryšio tinklu – telefono numeriai, į kuriuos ir iš kurių skambinta;
2) susiję su judriuoju telefono ryšiu:
i) telefono numeriai, į kuriuos ir iš kurių skambinta;
ii) kviečiančiosios šalies tarptautinis judriojo ryšio abonento identifikatorius (IMSI);
iii) kviečiančiosios šalies tarptautinis judriojo ryšio įrangos identifikatorius (IMEI);
iv) kviečiamosios šalies tarptautinis judriojo ryšio abonento identifikatorius (IMSI);
v) kviečiamosios šalies tarptautinis judriojo ryšio įrangos identifikatorius (IMEI);
vi) iš anksto apmokėtų anoniminių paslaugų atveju paslaugos pirminio aktyvavimo data ir laikas bei žyma vietovės (Cell ID), iš kurios paslauga buvo aktyvuota;
3) susiję su interneto prieiga, internetu perduodamu elektroniniu paštu ir internetine telefonija:
i)telefono, iš kurio skambinama, numeris naudojamas tiesioginio rinkimo interneto ryšiu;
ii) skaitmeninė abonento linija (DSL) ar kiti pranešimo siuntėjo galiniai tinklo taškai;

173 1) vietovės žyma (Cell ID) ryšio pradžioje;
2) duomenys, padedantys nustatyti geografinę įrangos buvimo vietą pagal vietovės žymas (Cell ID) tuo laikotarpiu, kai ryšio duomenys išsaugomi.

174 Metaduomenų sąvoka yra vartojama apibūdinant elektroniniu parašu pasirašyto dokumento metamuomenis, tačiau ne komunikacijos elektroninėje erdvėje metu generuojamus duomenis.

175 „Pasiūlymas dėl Europos Parlamento ir Tarybos reglamento dėl teisės į privatų gyvenimą ir asmens duomenų apsaugos elektroninių ryšių sektoriuje, kuriuo panaikinama Direktyva 2002/58/EB (Reglamentas dėl privatumo ir elektroninių ryšių), COM/2017/010 final – 2017/03 (COD)“, *EUR-Lex*, žiūrėta 2020 m. rugsėjo 4 d., https://eur-lex.europa.eu/legal-content/LT/TXT/?uri=CELEX%3A52017PC0010 .

turinys yra apibrėžiamas kaip turinys, kuriuo keičiamasi naudojantis elektroninių ryšių paslaugomis, pavyzdžiui, tekstas, balsas, vaizdo įrašai, vaizdai ir garsas (Pasiūlymo 4 str. 3 d. b p). Elektroninių ryšių metaduomenys apibrėžiami kaip elektroninių ryšių tinkle tvarkomi duomenys elektroninių ryšių turiniui perduoti, platinti ar juo keistis, taip pat duomenys, naudojami ryšių operacijos šaltiniui ir paskirties vietai atsekti ir atpažinti, duomenys apie įrenginio vietą, gauti teikiant elektroninių ryšių paslaugas, ryšio operacijos data, laikas, trukmė ir tipas (Pasiūlymo 4 str. 3 d. c punktas). Taigi Pasiūlymo rengėjai vadovaujasi JAV praktika ir siūlo pakeisti dabar ES teisės aktuose vartojamas srauto ir vietos nustatymo duomenų sąvokas. Disertacijos autorė taip pat pritaria tendencijai komunikaciją el. erdvėje skirstyti į turinio ir metaduomenis, todėl disertacijoje bus vartojamos pastarosios sąvokos.

JAV vaidmuo asmens duomenų rinkime el. erdvėje teisėsaugos ir žvalgybos tikslais. Asmens duomenų apsaugos reglamentavime šiuos duomenis renkant teisėsaugos ir žvalgybos tikslais JAV vaidmuo yra esminis. Kadangi:

1. Internetas, kuris sąlygojo masinį el. erdvės naudojimą, buvo sukurtas JAV kariniais tikslais vykdyto ikiprekybinio pirkimo metu[176];
2. Įmonės, kurios užima didžiausią paslaugų el. erdvėje teikimo rinkos dalį, yra JAV (Gmail, Amazon, Facebook, WhatsApp ir t. t.);
3. Dauguma Europos elektroninėje erdvėje generuojamų asmens duomenų yra saugoma JAV esančiuose serveriuose, arba keliaudami į kitų valstybių serverius kerta JAV teritoriją[177]. Tai reiškia, kad tiems duomenims galioja JAV elektroninės žvalgybos teisė (angl. *electronic surveillance law*);
4. Informacija apie tai, kad žvalgybos ir teisėsaugos institucijos vykdo masinį asmens duomenų rinkimą elektroninėje erdvėje, 2013 m. buvo paviešinta JAV NSA kontraktoriaus.
5. JAV yra pirmoji valstybėje, kurioje buvo priimti teisės aktai, reglamentuojantys asmens duomenų rinkimą el. erdvėje teisėsaugos ir žvalgybos tikslais, nors asmens duomenų apsauga daugelyje kitų sričių yra palikta savireguliacijai[178]. Kartu JAV yra pirmoji valstybė pasaulyje, kurioje elektroninės žvalgybos teisė yra išskiriama kaip atskira teisės šaka;
6. Reglamento dėl teisės į privatų gyvenimą ir asmens duomenų apsaugos elektroninių ryšių pasiūlymo projekte įtvirtinta elektroninės erdvės asmens duomenis skirstyti į turinio ir metaduomenis rodo, kad ES perima JAV praktiką.

Disertacija yra išdėstyta chronologiniu požiūriu nuo seniausių asmens duomenų rinkimą elektroninėje erdvėje reglamentuojančių teisės aktų atsiradimo iki naujausių. Atsižvelgiant į tai, kad pirmieji pasaulyje asmens duomenų rinkimą elektroninėje erdvėje teisėsaugos ir žvalgybos tikslais reglamentuojantys teisės aktai atsirado JAV teismų precedentų įtakos dėka, pradėsiu nuo JAV reglamentavimo apžvalgos.

---

176 Andrews, *supra note*, 99.

177 Stalla-Bourdillon, Papadaki ir Chown, *supra note*, 152.

178 Paul M. Schwartz and Daniel J. Solove, „Reconciling Personal Information in the United States and European Union Essay“, *California Law Review* 102, no. 4 (2014): 877–916.

2. ASMENS DUOMENŲ RINKIMO ELEKTRONINĖJE ERDVĖJE TEISĖSAUGOS IR ŽVALGYBOS TIKSLAIS REGLAMENTAVIMAS BENDROJOJE TEISĖJE (JUNGTINIŲ AMERIKOS VALSTIJŲ ATVEJO ANALIZĖ)

2.1. Asmens duomenų rinkimo elektroninėje erdvėje reglamentavimo ypatybės

JAV paprastai yra pristatomos kaip viena iš tų valstybių, kurios užima dominuojančią padėtį pasaulyje[179] ir tiesiogiai bei netiesiogiai įtakoja likusias pasaulio valstybes [180]. Todėl biržos makleriui, visų pirma rekomenduojama išmanyti JAV ekonomiką, bent kurios mokslo srities atstovui – JAV mokslininkų įdirbį toje srityje, gydytojui – naujausias gydymo technologijas, taikomas JAV, o kiekvienam asmeniui, bent minimaliai – apie JAV asmens duomenų apsaugos sistemą. Kodėl? – nes:

1. elektroninės erdvės ištakos yra JAV;
2. asmens duomenų rinkimo el. erdvėje teisėsaugos ir žvalgybos tikslais teisės šakos (angl. *Electronic Surveillance Law*) ištakos yra JAV;
3. kiekvieno iš mūsų didžioji dauguma elektroninių duomenų arba keliauja per JAV teritoriją, arba yra laikoma JAV teritorijoje esančiuose serveriuose[181], o likusieji elektroniniai duomenys taip pat teisiškai gali būti prieinami JAV žvalgybos institucijoms[182].

Po E. Snowden nutekinimo apie masinį asmens duomenų rinkimą asmenims gali kilti klausimai ar mūsų asmens duomenys yra apsaugoti; ar dėl JAV vykdomo masinio asmens duomenų rinkimo mes galime sakyti, kad turime realiai veikiančią teisę į asmens duomenų apsaugą? Ir net jeigu atsakymas būtų ne, tai savaime nereiškia, kad mūsų asmens duomenys šiuo metu turi didesnę apsaugą Europoje.

Kad suprastume kaip veikia mūsų teisės į asmens duomenų apsaugą sistema JAV, visų pirma turime žinoti, kad JAV teisės sistema yra kitokia, nei mums įprasta ES valstybių teisės sistema ne tik asmens duomenų apsaugos srityje. JAV teisės sistema yra sudaryta iš tripakopio federalinio ir 50 valstijų teisinio reglamentavimo. Federaliniu lygiu pagrindinis aukščiausią galią turintis teisės aktas yra JAV Konstitucija, žemesnę galią turintys teisės aktai yra įvairūs statutai ir galiausiai teisės aktų hierarchijoje žemiausią vietą užima institucijų priimami įsakymai. Ta pati sistema egzistuoja ir 50 JAV

---

[179] „Most Powerful Countries | US News Best Countries“, žiūrėta 2020 m. rugsėjo 4 d., https://www.usnews.com/news/best-countries/power-rankings .

[180] „The Global Influence of the United States“, *Study.Com*, žiūrėta 2020 m. rugsėjo 4 d., https://study.com/academy/lesson/the-global-influence-of-the-united-states.html

[181] „NSA Slides Explain the PRISM Data-Collection Program“, *The Washington Post*, žiūrėta 2020 m. rugsėjo 4 d., https://www.washingtonpost.com/wp-srv/special/politics/prism-collection-documents/ .

[182] Axel Arnbak ir Sharon Goldberg, „Loopholes for Circumventing the Constitution: Unrestricted Bulk Surveillance on Americans by Collecting Network Traffic Abroad“, *Michigan Telecommunications and Technology Law Review* 21, no. 2 (2015 2014): 317–62.

valstijų: kiekviena valstija turi savo konstituciją, statutus ir įsakymus. Valstijų teisės aktai galioja tik konkrečios valstijos teritorijoje ir nesaisto federalinės valdžios. Tuo tarpu federaliniai teisės aktai saisto federalinės valdžios institucijas ir visų 50 valstijų institucijas. Šis bendrasis teisės aktų hierarchijos modelis egzistuoja ir JAV teisiniame asmens duomenų apsaugos reglamentavime. Tai yra viena iš priežasčių, kodėl JAV ir Europos teisiniai asmens duomenų apsaugos modeliai yra visiškai skirtingi[183]. Yra teigiančių, jog tam tikrais atvejais JAV teisė į asmens duomenų apsaugą yra stipresnė nei ES[184]. Galima rasti teigiančių, kad JAV apskritai nėra teisės į asmens duomenų apsaugą. Tačiau toks teiginys yra paremtas ne visišku JAV teisinės sistemos išmanymu ir ES teisinės sistemos bruožų ieškojimu ten, kur jų nėra – valstybėje, nepriklausančioje ES ir ET.

Esminis JAV ir Europos asmens duomenų apsaugos modelių skiriamasis akcentas yra tas, kad JAV nėra vieno pamatinio teisės akto (tokio kaip sutartis, reglamentas ar direktyva, kas egzistuoja Europoje), kuris būtų viso reglamentavimo pamatiniu dokumentu, o nuo prezidento Klintono prezidentavimo laikotarpio asmens duomenų apsauga apskritai didžiąja dalimi JAV buvo palikta savireguliacijai[185]. JAV asmens duomenų apsaugos sistemos modelis – sektorinis[186], paremtas federalinio[187] ir valstijų reguliavimo[188] sąveika šalia kurios egzistuoja dar ir teisiškai neįpareigojantis atskirų viešojo ir privataus sektorių subjektų sukurtas reglamentavimas dažnai įvardijamas „gerąja praktika“[189]. Sektorinis JAV asmens duomenų apsaugos reglamentavimas pasireiškia tuo, kad federaliniai visose valstijose galiojantys asmens duomenų apsaugą reglamentuojantys teisės aktai yra priimami tik tam tikrų sektorinių klausimų reglamentavimui[190] ir dažniausiai yra sudedamoji tam tikrą sritį reglamentuojančio teisės akto dalimi, bet ne atskiru teisės aktu. Paprastai federaliniu lygiu reglamentuojamos tos sritys, kuriose asmenys patys nebūtų pajėgūs kontroliuoti savo asmens duomenų naudojimo ir jų apsaugoti[191]. Vienas iš tų sektorių – teisėsaugos ir žvalgybos institucijų veikla.

Antrasis JAV reglamentavimo ypatumas yra tas, kad teisė į asmens duomenų apsaugą tiesiogiai JAV teisės aktuose nėra įtvirtinta, kaip ji tiesiogiai nėra įtvirtinta ir EŽTK. IV JAV Konstitucijos pataisa yra saugomas asmens privatumas, kuris, analogiškai

---

183 Paul M. Schwartz ir Daniel J. Solove, „Reconciling Personal Information in the United States and European Union“, 102 California. Law. Review. 877 (2014), 1.

184 Peter Swire ir DeBrae Kennedy-Mayo, „How Both the EU and the U.S. Are 'Stricter' Than Each Other for the Privacy of Government Requests for Information“ *Emory University School of Law*, žiūrėta 2020 m. rugsėjo 4 d., http://law.emory.edu/elj/content/volume-66/issue-3/articles/both-eu-us-stricter-privacy-requests-information.html .

185 Francesca Bignami, „The US Legal System on Data Protection in the Field of Law Enforcement. Safeguards, Rights and Remedies for EU Citizens“, žiūrėta 2020 m. rugsėjo 4 d., https://www.europarl.europa.eu/thinktank/en/document.html?reference=IPOL_STU(2015)519215 .

186 Daniel J. Solove, „The Growing Problems with the Sectoral Approach to Privacy Law“, *TeachPrivacy*, 2015, žiūrėta 2020 m. rugsėjo 4 d., https://teachprivacy.com/problems-sectoral-approach-privacy-law/ .

187 Schwartz ir Solove, *op. cit*, 183.

188 „Data Protection Law – HG.Org“, žiūrėta 2020 m. rugpjūčio 12 d., 2020, https://www.hg.org/data-protection.html.

189 Stephen P Mulligan, Wilson C Freeman ir Chris D Linebaugh, „Data Protection Law: An Overview“, 79, žiūrėta 2020 m. rugsėjo 4 d., https://fas.org/sgp/crs/misc/R45631.pdf

190 Shawn Marie Boyne, „Data Protection in the United States: U.S. National Report“, SSRN Scholarly Paper (Rochester, NY: Social Science Research Network, 2017), doi:10.2139/ssrn.3089004.

191 *Ibid*.

EŽTK, tik teismų praktikos ir nukentėjusią šalį gynusių advokatų išmanumo dėka[192], nuo 1967 m. gali būti interpretuojamas kaip apimantis ir asmens duomenų apsaugą[193]. Asmens duomenų sąvoka JAV iki 2018 metų ES asmens duomenų reformos taip pat buvo retai vartojama. Paprastai vietoj jos buvo ir vis dar yra vartojama asmenį identifikuojančios informacijos sąvoka (angl. *Personally identifiable information (PII)*), kuri apibrėžiama kaip informacija, kuri viena arba kartu su kita turima informacija gali padėti identifikuoti asmenį apie kurį ji yra[194]. Nors apibrėžimas yra labai panašus į asmens duomenų apibrėžimą, skiriasi tik tai, kad asmenį identifikuojančios informacijos atveju yra akcentuojama informacija, duomenys, o asmens duomenų atveju – žmogus. Galbūt todėl ir JAV teisės sistema yra orientuojama į duomenų rinkimo el. erdvėje procedūrų reglamentavimą, o Europoje – į teisės asmeniui į asmens duomenų apsaugą suteikimą. Tačiau disertacijoje toliau bus naudojama tik viena – asmens duomenų sąvoka – tiek kalbant apie JAV, tiek apie Europos modelius.

Vienas iš įdomiausių ir kartu mums, europiečiams, svarbiausių JAV asmens duomenų apsaugos reglamentavimo ypatumų yra skirtingi apsaugos lygiai asmenims, priklausantiems JAV asmenų kategorijai (angl. *USA persons*) ir šiai kategorijai nepriklausantiems (angl. *non USA persons)*. Skirstymo į JAV ir ne JAV asmenis ištakos yra 1972 m. teismo praktika *Keith* byloje[195]. Byloje buvo analizuojamas be teismo leidimo vykdomas radikalios JAV teritorijoje veikiančios grupuotės telefoninių pokalbių pasiklausymo atitikimas IV JAV Konstitucijos pataisai. Teismas, motyvuodamas tuo, kad turi būti daromas skirtumas tarp paprastų nusikaltimų ir nusikaltimų, susijusių su nacionaliniu saugumu tyrimo, kadangi jie skiriasi savo grėsme visuomenei, konstatavo, kad kuomet tyrimo tikslas yra nacionalinio saugumo užtikrinimas, JAV asmenų atžvilgiu IV JAV Konstitucijos pataisa yra taikoma ir teismo leidimas duomenų rinkimui el. erdvėje yra reikalingas. Teismas *Keith* byloje išskyrė vidinės ir išorinės grėsmės nacionaliniam saugumui aspektus, pasisakydamas, kad vietinės vidinės saugumo grėsmės atveju IV JAV Konstitucijos pataisa privalo būti taikoma, o klausimą ar ji taikoma išorinių grėsmių atveju, kuomet veikia užsienio subjektai ar jų agentai (angl. *foreign powers or agents thereof*), t. y. ne JAV asmenys, nepriklausomai nuo to ar šalies viduje ar už jos ribų – paliko neatsakytu[196]. Po kelių metų teismo sprendimo *Keith* byloje pagrindu buvo priimtas įstatymas – Užsienio žvalgybos elektroninėje erdvėje aktas (angl. *Foreign Intelligence Surveillance Act*) (toliau – *FISA*) – kuriame jau buvo įtvirtintas skirtingas teisės į asmens duomenų apsaugą užtikrinimo lygis JAV ir ne JAV asmenims.

JAV asmenų (angl. *USA person*) sąvoka yra vartojama keliuose aktuose ir visuose juose ji suprantama skirtingai[197]. Vadovaujantis FISA JAV asmenimis yra laikomi,

---

[192] Farivar, *supra note*, 22.

[193] „Katz v. United States“, *FindLaw*, žiūrėta 2020 m. rugsėjo 4 d., https://caselaw.findlaw.com/us-supreme-court/389/347.html.

[194] Jake Frankenfield, „How Personally Identifiable Information (PII) Works“, *Investopedia*, žiūrėta 2020 m. rugsėjo 4 d., https://www.investopedia.com/terms/p/personally-identifiable-information-pii.asp .

[195] „United States v. United States District Court“, *FindLaw*, žiūrėta 2020 m. rugsėjo 4 d., https://caselaw.findlaw.com/us-supreme-court/407/297.html

[196] Bignami, *supra note*, 185:22.

[197] Žr. pvz., „50 U.S. Code § 1801 – Definitions“, *LII / Legal Information Institute*, žiūrėta 2020 m. rugsėjo 4 d., https://www.law.cornell.edu/uscode/text/50/1801 .

asmenys turintys ryšį su JAV: JAV piliečiai, nuolatiniai JAV gyventojai, asmenų susivienijimas, kurio didžioji dauguma narių yra JAV piliečiai arba nuolatiniai JAV gyventojai, jeigu nė vienas iš narių neatitinka „užsienio subjekto“ (angl. *foreign power*) sąvokos[198]. Atitinkamai ne JAV asmenimis (angl. *non USA persons)* yra laikomi visi kiti asmenys. Kadangi JAV asmenų atžvilgiu galioja IV JAV Konstitucijos pataisa, suteikianti teisę į privatumą, o ne JAV asmenų atžvilgiu ši Konstitucijos pataisa negalioja[199], tai reiškia, kad JAV teisės aktais yra saugomi tik JAV asmenų asmens duomenys, nors šių duomenų rinkimas yra reglamentuojamas ir ne JAV asmenų atžvilgiu. Todėl JAV yra dvilypė ir žvalgybos veiklą elektroninėje erdvėje reglamentuojanti sistema: vienos FISA nuostatos yra taikomos JAV asmenų atžvilgiu, kitos – ne JAV asmenų atžvilgiu. Tačiau pastaraisiais metais dėl elektroninės erdvės specifiškumo paaiškėjus, jog praktiškai neįmanoma renkant duomenis el. erdvėje nustatyti ar jų subjektas yra JAV ar ne JAV asmuo[200], pradėjo ryškėti dirbtinio skirstymo į JAV ir ne JAV asmenų susiliejimo tendencija. Nors kol kas dar tik civilinėje byloje, bet teismo jau buvo kartą pasisakyta, kad Komunikacijos elektroninėje erdvėje privatumo aktas (angl. *Electronic Communication Privacy Act*) (toliau – ECPA) tam tikrais atvejais gali būti taikomas ir apsaugą pagal IV JAV Konstitucijos pataisą suteikti ir ne JAV asmeniui[201]. Iš kitos pusės, teisėsaugos institucijos, kurios iš esmės turi jurisdikciją tik JAV teritorijos atžvilgiu[202], informaciją apie JAV asmenis pradėjo rinkti vadovaudamosi užsienio žvalgybą reglamentuojančiu teisės aktu ir jo procedūromis – FISA[203]. Tai reiškia, kad teismai pamažu ima kvestionuoti teisės į asmens duomenų apsaugą suteikimą tik JAV asmenims. Tai yra pasaulietiškas požiūris – juk tokias pačias teises iš tikrųjų turi visų likusių civilizuotų demokratinių valstybių gyventojai, tik jos yra suteikiamos skirtingais tų valstybių teisės aktais. Jeigu JAV teismų praktika ir toliau bus vystoma šia linkme, atsižvelgiant į tai, kad visi elektroninių asmens duomenų rinkimą reglamentuojantys teisės aktai buvo teismų praktikos rezultatai, tai, autorės nuomone, labai tikėtina, kad JAV panaikins teisės aktuose įtvirtintą diskriminaciją ryšių su JAV turėjimo pagrindu.

Dar vienas pažymėtinas JAV asmens duomenų rinkimo el. erdvėje reglamentavimo ypatumas irgi yra *Keith* bylos rezultatas: skirtingų nusikalstamų veikų tyrimas ir užkardymas reglamentuojamas skirtingais teisės aktais. Jeigu asmens duomenys elektroninėje erdvėje yra renkami siekiant ištirti įprastines nusikalstamas veikas, tuomet tokias nusikalstamas veikas tiria teisėsaugos institucijos, o jų veikla reglamentuojama ECPA. Tačiau jeigu tyrimo objektas yra nusikalstamos veikos, susijusios su nacionali-

198 Žr. pvz., „50 U.S. Code § 1801 – Definitions“, *LII / Legal Information Institute*, žiūrėta 2020 m. rugsėjo 4 d., https://www.law.cornell.edu/uscode/text/50/1801

199 Joanna Kulesza, „USA Cyber Surveillance and EU Personal Data Reform: PRISM's Silver Lining?“, SSRN Scholarly Paper (Rochester, NY: Social Science Research Network, 2014), 4, https://papers.ssrn.com/abstract=2599274. Alexander Trowbridge, „NSA Spying: Ally Anger Justified?“, žiūrėta 2020 m. rugsėjo 8 d., https://www.cbsnews.com/news/nsa-spying-ally-anger-justified/.

200 Donohue, *supra note*, 8.

201 „Teisėjo Andrew J. Guilford atskiroji nuomonė byloje Suzlon Energy Ltd. v. Microsoft Corp., No. 10-35793 (9th Cir. 2011)“, US courts, žiūrėta 2020 m. rugsėjo 8 d., http://cdn.ca9.uscourts.gov/datastore/opinions/2011/10/03/10-35793.pdf.

202 Ahmed Ghappour, „Searching Places Unknown: Law Enforcement Jurisdiction on the Dark Web“, *Stanford Law Review* 69, no. 4 (2017): 1075–1136.

203 Donohue, *supra note*, 8.

niu saugumu, tuomet jas tiria ir užkardo bei asmens duomenis el. erdvėje renka žvalgybos institucijos, vadovaudamosi vėlgi dvejais viešai skelbiamais teisės aktais:

1) FISA – kuris yra įstatymo lygmens;

3) EO 12 333 – prezidento (vykdomosios valdžios) dekreto lygmens.

Nepaisant visų šių ypatumų, palyginus su Europa, JAV asmens duomenų apsaugos elektroninių asmens duomenų rinkimo nusikalstamų veikų tyrimo tikslais atveju užuomazgos pradėjo atsirasti labai anksti – 1967 m. Nuo to laikotarpio vis atsirasdavo papildomos apsaugos sritys ar jų elementai. Tuo tarpu Europoje buvo daugiau plėtojama teisės į asmens duomenų apsaugą plačiąja prasme doktrina, o teisėsaugos ir žvalgybos veikla elektroninių asmens duomenų rinkimo atžvilgiu neturi atskiro teisinio reglamentavimo. Viršnacionaliniu lygiu Europos Taryba (toliau – ET) 1989 m. priėmė rekomendacinio pobūdžio Rekomendacijas apskritai dėl asmens duomenų tvarkymo teisėsaugos sektoriuje, o ES tik 2018 m. – Teisėsaugos tikslais tvarkomų asmens duomenų direktyvą. Tačiau žvalgybos institucijų veikla nereglamentuojama ES lygiu, asmens duomenų rinkimas el. erdvėje – taip pat. Taigi JAV reglamentavimas šioje srityje, priešingai nei apskritai asmens duomenų apsaugos srityje, palyginus su Europa, yra labai detalus. Bet ar kad tas reglamentavimas užtikrina teisę į asmens duomenų apsaugą?

2.2. Asmens duomenų rinkimas elektroninėje erdvėje teisėsaugos tikslais

2.2.1. Teismo precedentų vaidmuo teisės į privatumą apsaugoje

2016 m. minint JAV Konstitucijos dieną buvo akcentuojama jos preambulės žodžių „mes, Jungtinių Amerikos Valstijų gyventojai“, prasmė, kad valdžios institucijos privalo tarnauti šalies gyventojams[204]. Tų pačių JAV Konstitucijos žodžių ta pati prasmė buvo raktas, kuriuo JAV Aukščiausias teismas pasinaudojo aiškindamas IV JAV Konstitucijos pataisoje įtvirtintos teisės į privatumą galiojimą ne tik fizinėje aplinkoje, bet ir elektroninėje erdvėje. IV JAV Konstitucijos pataisa numato, kad asmuo yra saugomas nuo nepagrįstų jo paties, jo namų, dokumentų ir daiktų kratų[205]. Pirminis šios JAV Konstitucijos pataisos interpretavimas teigė, kad IV JAV Konstitucijos pataisa saugo asmenį nuo fizinio kišimosi į jo gyvenimą. Todėl ir krata JAV ilgai buvo suvokiama ir aiškinama tik kaip galinti būti susijusi tik su fiziškai apčiuopiamu objektu: žmogaus kūnu, jo namais, dokumentais ar daiktais. Teismai laikėsi pozicijos, kad jeigu nėra sąveikos su fizine aplinka, tuomet teisėsaugos institucijų veiksmai nėra krata, jiems nėra reikalingas teismo leidimas ir asmenų teisės tokiu atveju nėra saugomos vadovaujantis IV JAV Konstitucijos pataisa. Laikantis šios teismų praktikos teisėsaugos institucijos iki 1967 m. galėjo teisėtai nesankcionuotos klausytis telefoninių pokalbių, kadangi

[204] „U.S. Senate: Constitution Day“, *US Senate*, žiūrėta 2020 m. rugsėjo 4 d., https://www.senate.gov/artandhistory/history/common/generic/ConstitutionDay.htm.

[205] IV JAV Konstitucijos pataisoje yra įtvirtinta „The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized“.

telefoninių pokalbių vyksmo vieta ne fizinė aplinka, o kvazi aplinka – elektroninė erdvė, o teisėsaugos institucijoms juos perimant asmuo fiziškai nėra paveikiamas[206].

Teisinė asmens duomenų apsaugos elektroninėje erdvėje doktrina aiškinant IV JAV Konstitucijos pataisą buvo pradėta formuoti 1967 m. balandžio mėnesį. *Berger v. New York* byloje[207] teismas įtvirtinto teisėsaugos institucijų vykdomo telefoninių pokalbių turinio perėmimo sąlygas, nors dar nepasisakė dėl IV JAV Konstitucijos pataisos galiojimo elektroninei erdvei. Elektroninis asmens duomenų rinkimas tapo šios bylos objektu tik todėl, kad pasiklausymo įrenginys buvo neteisėtai infiltruotas fizinėje aplinkoje. Visgi *Berger v New York* byloje teismas suformulavo pirmąsias teisėto teisėsaugos institucijų veikimo sąlygas, kurios yra iki šiol, su tam tikromis išimtimis, taikomos ir elektroninei erdvei. Teisėsaugos institucijos, pasak teismo, teisėtai gali prieiti prie aktualiu laiku vykstančių telefoninių pokalbių turinio tik, jei yra visos šios sąlygos:

1) teismo orderis (angl. *court warrant*), kuriam taikomi įprastiniai tikėtinos priežasties (angl. *probable cause*) buvimo ir apibrėžtumo (angl. *particularity*) reikalavimai – teisėsaugos institucijos kreipdamosi į teismą privalo įrodyti, kad telefoninio pokalbio turinys gali atskleisti įrodymų apie nusikalstamą veiką ir konkrečiai apibrėžti kokiam telefono numeriui jis bus taikomas;
2) konkrečiai apibrėžtas laiko terminas;
3) asmeniui, kurio telefoninių pokalbių teisėsaugos institucijos klausėsi turi būti apie tai pranešta;
4) jeigu teisėsaugos institucijoms klausantis pokalbio paaiškėja, kad jis yra neaktualus tyrimui, šio pokalbio klausymasis turi būti nutrauktas, telefoninių pokalbių klausymasis turi būti sumažintas;
5) norint atnaujinti pasiklausymą yra reikalingas naujas teismo orderis, kuriam gauti reikia naujo teisėto pagrindo[208].

JAV asmens duomenų apsaugos el. erdvėje doktrinai svarbiausias įvykis yra 1967 m. pabaigoje teismo sprendimas byloje *Katz v. United States*[209]. Šioje byloje teismas konstatavo, kad IV JAV Konstitucijos pataisa „saugo asmenis, ne fizines vietas“, todėl telefoninių pokalbių turinio perėmimas yra krata, kuriai taikoma IV JAV Konstitucijos pataisa ir ji yra teisėta tik tuo atveju, jeigu vykdama pagal kratos orderį (angl. *search warrant*)[210]. Vadovaujantis moderniuoju IV JAV Konstitucijos pataisos aiškinimu, ji saugo ne tik fizinę asmens aplinką, kadangi moderniųjų technologijų amžiuje asmens privatumo poreikis apsiriboja ne tik ja, ji išsiplečia į nematerialią erdvę ir nematerialius objektus, todėl ir šia Konstitucijos pataisa yra saugoma viskas, kam asmuo tikisi privatumo ir ką visuomenė laiko, kad jo tikėjimasis privatumo yra pagrįstas[211]. *Katz v.*

---

[206] „Olmstead v United States“, *FindLaw*, žiūrėta 2020 m. rugsėjo 4 d., https://caselaw.findlaw.com/us-supreme-court/277/438.html Paul Jr. Larkin, „The Fourth Amendment and New Technologies“, *The Heritage Foundation*, žiūrėta 2020 m. rugsėjo 4 d., https://www.heritage.org/report/the-fourth-amendment-and-new-technologies.

[207] „Berger v. New York“, *FindLaw*, žiūrėta 2020 m. rugsėjo 4 d., https://caselaw.findlaw.com/us-supreme-court/388/41.html.

[208] *Ibid.*

[209] Katz v. United States. *supra note*, 193.

[210] *Ibid.*

[211] *Ibid.*

United States byla svarbi dar ir dėl to, kad atskirąją nuomonę pateikęs teisėjas Harlan sukūrė privatumo testo precedentą, vėliau įtvirtintą *Smith v. Maryland* byloje[212]. Atskirojoje nuomonėje buvo suformuluotos dvi taisykles kaip nustatyti ar asmens tikėjimasis privatumo yra pagrįstas. Visų pirma, reikia nustatyti ar konkretus asmuo konkrečiu atveju tikisi privatumo (subjektyvus privatumo tikėjimosi elementas) ir antra, ar privatumo tokiomis aplinkybėmis tikėtų vidutinis JAV pilietis (objektyvus privatumo tikėjimosi elementas)[213].

Tačiau *Katz* byloje suformuotas pagrįsto privatumo nustatymo testas yra kritikuojamas tiek mokslininkų[214], tiek paties teismo[215]. Yra teigiama, kad spręsdamas pagrįsto privatumo tikėjimosi klausimą teisėjas vadovaujasi ne „vidutinio asmens", o savo privatumo poreikio suvokimu[216], jei jau teisėsaugos institucijos atlieka tyrimą, tai, vadinasi, vidutinis statistinis asmuo mano, jog pagrįstai, todėl automatiškai privatumo tikėjimasis yra nepagrįstas[217], ekonominiai ir socialiniai veiksniai (tokie kaip socialiniai tinklai, debesų kompiuterija ir kt.) verčia asmenį atsisakyti savo privatumo[218], o galimybė, jog informaciją el. erdvėje gali bent kada neteisėtai perimti hakeriai reiškia, jog asmuo turėtų suvokti, kad el. erdvė nėra privati vieta[219].

Visgi, nepaisant pagrįsto privatumo doktrinos, suformuotos *Katz* byloje privalumų ir trūkumų, *Katz* byla JAV privatumo apsaugos kontekste yra svarbiausia dėl to, kad nustatė, jog tuo metu pagrindinė komunikacijos el. erdvėje priemonė – telefoniniai pokalbiai – patenka į IV JAV Konstitucijos apsaugos apimtį ir tam, kad teisėsaugos institucijos galėtų perimti šiuos asmens duomenis, yra reikalinga IV JAV Konstitucijos pataisoje numatytas teismo išduotas kratos orderis (angl. *search warrant*).

Teismo *Katz v. United States* ir *Burger v. New York* bylose suformuotą doktriną, kad realiu laiku vykstančių telefoninių pokalbių klausymuisi yra reikalingas specialus teismo leidimas – kratos orderis (angl. *search warrant*) – 1968 m. JAV Parlamentas įtvirtino Trečiojoje antraštėje – Kelis aspektus apimančios nusikaltimų kontrolės ir saugių gatvių akte (angl. *Title III Omnibus Crime Control and Safe Street Act)* (vėliau pakeistame į Telefoninių pokalbių klausymosi aktą (angl. *Wiretap act*)), numatančiame perteklinio esamuoju laiku vykstančių asmens telefoninių pokalbių ir kitos elektroninės komunikacijos rinkimo, naudojimo ir atskleidimo draudimą, išskyrus pačiame teisės akte numatytas išimtas. Viena iš tų išimčių – teisėsaugos institucijų vykdomas rinkimas telefoninių pokalbių klausymo orderio (angl. *wiretap order*) pagrindu. Šiame teisės akte yra įtvirtinti analogiški *Burger v. United States* byloje išdėstyti reikalavimai telefoninių pokalbių klausymo orderiui (angl. *wiretap order*) gauti

---

212 „Smith v. Maryland", *FindLaw*, žiūrėta 2020 m. rugsėjo 4 d., https://caselaw.findlaw.com/us-supreme-court/442/735.html.

213 Susan Freiwald, „A First Principles Approach to Communications' Privacy", SSRN Scholarly Paper (Rochester, NY: Social Science Research Network, 2008), https://papers.ssrn.com/abstract=1132421.

214 Farivar, *Habeas Data*, 2018.

215 „United States v. Jones", FindLaw, žiūrėta 2020 m. rugsėjo 4 d., https://caselaw.findlaw.com/us-5th-circuit/1364966.html

216 Farivar, *supra note*, 22.

217 *Ibid.*

218 *Ibid.*

219 Carr ir Bellia, *supra note,* 21.

ir įtvirtinti du papildomi: 1) išvardintos konkrečios nusikalstamos veikos, kurių užkardymui ir tyrimui teisėsaugos institucijos gali kreiptis, o teismas gali išduoti telefoninių pokalbių klausymo orderį (angl. *wiretap order*); 2) numatytas reikalavimas teisėsaugos institucijoms prašyme dėl telefoninių pokalbių klausymo orderio (angl. *wiretap order*) nurodyti, kodėl kitos nusikalstamų veikų tyrimo priemonės yra neefektyvios. Telefoninių pokalbių klausymosi akte (angl. *Wiretap act*) taip pat yra įtvirtinta asmens galimybės ginčyti telefoninių pokalbių klausymo orderio (angl. *wiretap order*) pagrįstumą ir kreiptis į teismą dėl ieškinio dėl žalos patirtos dėl neteisėtomis priemonėmis vykdyto pokalbių pasiklausymo[220].

Vėlesnė teisminė doktrina dėl IV JAV Konstitucijos pataisos aiškinimo nebuvo taip orientuota į asmens privatumo gynimą, kaip *Katz* byloje. Pavyzdžiui, *Katz v. United States* byloje 1968 m. teismas pasisakė, kad asmuo skambindamas iš telefono būdelės pagrįstai tikisi privatumo, tačiau 1971 m. byloje *United States v. White* buvo pasisakyta, kad jeigu asmuo kitam asmeniui leido įeiti į savo namus, vadinasi jis nebegali pagrįstai tikėtis privatumo ir privalo suvokti, jog jo pokalbiai gali būti įrašinėjami[221]. Reikšminga išimtis, kada asmuo negali tikėtis privatumo buvo suformuota 1976 m. ir 1979 m. bylose *United States v. Miller*[222] ir *Smith v. Maryland*[223] iki šiol vadinama „trečiosios šalies doktrina". *United States v. Miller*[224] ir *Smith v. Maryland*[225] teismas konstatavo, kad jei vieną kartą asmuo atsisakė savo privatumo, tai jo jau niekada nebegali pagrįstai tikėtis[226]. Trečiosios šalies doktrinos esmė – trečiajai šaliai (telekomunikacijų ir elektroninių paslaugų tiekėjui) suteikiama informacija nėra privati, kadangi asmuo žino, kad ją suteikia ir suteikia savo noru[227]. Telekomunikacinių paslaugų bendrovė teismų buvo lyginama su informantu. Aukščiausiasis teismas eilėje bylų yra pasisakęs, kad savanoriškai trečiajai šaliai – informantui – atskleista informacija nėra saugoma IV JAV Konstitucijos pataisos, nepriklausomai nuo to ar trečioji šalis yra policijos pareigūnas ar paprastas pilietis ir nepriklausomai nuo to ar informacija buvo įrašyta ar ne[228]. Tačiau tai nereiškia, kad tokio pobūdžio informacija gali būti teisėsaugos ir žvalgybos institucijų perimta nesankcionuotai. Sankcionavimas vis tiek yra reikalingas, tik paprastesnė jo gavimo procedūra. Trečiajai šaliai perduotų duomenų rinkimui yra

---

220 „18 U.S. Code Chapter 119 – Wire and Electronic Communications Interception and Interception of Oral Communications", *Legal Information Institute*, žiūrėta 2020 m. rugsėjo 4 d., https://www.law.cornell.edu/uscode/text/18/part-I/chapter-119

221 „United States v. White", *FindLaw*, žiūrėta 2020 m. rugsėjo 4 d., https://caselaw.findlaw.com/us-5th-circuit/1278977.html.

222 „United States v. Miller", *FindLAw*, žiūrėta 2020 m. rugsėjo 4 d., https://caselaw.findlaw.com/us-3rd-circuit/1177040.html.

223 Smith v. Maryland, *supra note*, 212.

224 United States v. Miller, *op. cit.*, 222.

225 Smith v. Maryland, *supra note*, 212.

226 „*Cf.* SEC v. Jerry T. O'Brien, Inc.", *FindLAw*, žiūrėta 2020 m. rugsėjo 4 d., https://caselaw.findlaw.com/us-supreme-court/467/735.html.

227 Orin Kerr, „The Case for the Third-Party Doctrine", *Michigan Law Review* 107, no. 4 (2009): 563.

228 Žr. pvz. United States v. White, *supra note*, 221. „Hoffa v. United States", *FindLaw*, žiūrėta 2020 m. rugsėjo 4 d., https://caselaw.findlaw.com/us-supreme-court/385/293.html. „Lewis v. United States", *FindLaw*, žiūrėta 2020 m. rugsėjo 4 d., https://caselaw.findlaw.com/dc-court-of-appeals/1048783.html. „Lopez v. United States", *FindLaw*, žiūrėta 2020 m. rugsėjo 4 d., https://caselaw.findlaw.com/dc-court-of-appeals/1123691.html. „On Lee v. United States", *FindLaw*, žiūrėta 2020 m. rugsėjo 4 d., https://caselaw.findlaw.com/us-supreme-court/343/747.html.

reikalingas ne telefoninių pokalbių klausymo orderis (angl. *wiretap order*), o teismo šaukimas (angl. *subpoena*)[229]. Pagal JAV teisę teismo šaukimas (angl. *subpoena*) yra administracinis procesinis dokumentas, kuriuo nurodoma asmeniui pateikti tam tikrą informaciją valstybinei ar vietos administracinei institucijai. Nors kaip ir pagrįsto privatumo nustatymo testo taip ir trečiosios šalies doktrinos pagrįstumu abejoja tiek mokslininkai[230], tiek teismai[231], iki šiol ji yra nors ir ginčijama, bet vis dar galiojančia ir JAV teisinėje sistemoje įtvirtinta praktika. Taigi kokių JAV piliečių asmens duomenų rinkimui yra taikomi paprastesni reikalavimai?

Telefoninių pokalbių atveju trečiosios šalies doktrina apima: paskyros informaciją (angl. *account information*), komunikacijos meta duomenis (informacija apie komunikaciją, nesudarančią komunikacijos turinio) bei komunikacijos turinį, kurį asmuo savanoriškai atskleidė paslaugų teikėjui ir sutiko su tuo, kad jis būtų įrašomas (pavyzdžiui, įrašomas skambutis paslaugų teikėjui dėl nusiskundimo jo teikiamomis paslaugomis). Tačiau trečiosios šalies doktrina neapima viso kito komunikacijos turinio, t. y. paties telefoninio pokalbio, kuomet telekomunikacinių paslaugų teikėjas veikia tik kaip tarpininkas, bet ne kaip gavėjas[232]. O pastaraisiais metais teismų praktika pamažu krypsta ta linkme, kad bent koks komunikacijos turinys, nepriklausomai nuo to ar telekomunikacinių paslaugų teikėjas veikia kaip tarpininkas ar kaip gavėjas yra saugomas IV JAV Konstitucijos pataisos[233].

Dar vienas atvejis, kuomet teismų praktika laikosi pozicijos, jog į IV JAV Konstitucijos pataisą reikėtų žiūrėti lanksčiau teisėsaugos ir žvalgybos institucijų naudai buvo įtvirtinta *Olivier v. United States*[234] bei *United States v. Dunn*[235] bylose. *Katz v. United States* byloje teismas akcentavo, kad asmens privatumo apsauga negali apsiriboti konkrečiai apibrėžta fizine erdve, nes saugomas asmuo, ne teritorija, tuo suponuojant absoliučią asmens apsaugą bent kurioje teritorijoje, jei jis pagrįstai tikisi privatumo, tačiau 1984 m. *Olivier v. United States*[236] bei 1987 m. *United States v. Dunn*[237] bylose buvo konstatuota, kad asmuo negali tikėti privatumo atvirose vietose, kadangi tokiose

---

229 Smith v. Maryland, *supra note*, 212., United States v. Miller, *supra note*, 222.

230 Kerr, *supra note*, 227:563. Wayne R. LaFave, *Search and Seizure, A Treatise on the Fourth Amendment, Fourth Edition, 6 Volume Set*, 5th edition (Thomson West, 2004), 747. Richard M Thompson Ii, „The Fourth Amendment Third-Party Doctrine", (Congressional Research Service, 2014), 17. Michael W. Price, „Rethinking Privacy: Fourth Amendment Papers and the Third-Party Doctrine", *Journal of National Security Law and Policy* 8, no. 2 (2016 2015): 247–300.

231 Stephen E. Henderson, „Learning from All Fifty States: How to Apply the Fourth Amendment and Its State Analogs to Protect Third Party Information from Unreasonable Search", *Catholic University Law Review* 55, no. 2 (2006 2005): 373–438.

232 Katz v. United States. *supra note*, 193.

233 „The Third-Party Doctrine in the Wake of a „Seismic Shift"", *American Bar*, žiūrėta 2020 m. rugsėjo 10 d., https://www.americanbar.org/groups/litigation/committees/privacy-data-security/practice/2019/third-party-doctrine-wake-of-seismic-shift/.

234 „*Oliver v. United States*", *FindLaw, žiūrėta 2020 m. rugsėjo 4 d.,* https://caselaw.findlaw.com/dc-court-of-appeals/1318002.html.

235 *Ibid.,* „United States v. Dunn", *FindLaw, žiūrėta 2020 m. rugsėjo 4 d.,* https://caselaw.findlaw.com/us-9th-circuit/1266164.html.

236 *Oliver v. United States, op. cit., 234.*

237 *Ibid.*, United States v. Dunn, *op. cit.*, 235.

vietoje „Karūna“ visada gali lankytis pagal bendrąją teisę (angl. *common law*)[238]. Taigi, *Katz b*yloje už modernųjį Konstitucijos aiškinimą pasisakęs teismas vėlesnėse savo bylose tarsi bandė sušvelninti savo poziciją teisėsaugos ir žvalgybos institucijų naudai. Bet dabar vėl yra grįžtama prie IV JAV Konstitucijos pataisos, kaip visų pirma saugančios asmens privatumą, aiškinimo ir piliečių apsaugos nuo antikonstitucinio moderniųjų žvalgybos įrenginių panaudojimo. 2001 m. teismas nurodė, kad nesankcionuotas nuotolinis temperatūros stebėjimo prietaiso naudojimas siekiant nustatyti, kas yra namuose, pažeidžia asmens teisę į privatumą[239]. 2012 m. *United States v. Jones* byloje teismas nurodė, kad teismo nesankcionuotas GPS sekimo prietaiso pritvirtinimas prie automobilio ir nuolatinis asmens stebėjimas šio prietaiso pagalba pažeidžia asmens teisę į privatumą ir IV JAV Konstitucijos pataisos nuostatas[240]. Panašiai teismas pasisakė ir kitose bylose[241]. Tačiau didžiausia intriga buvo 2018 m. *Apple v United States* byla, kurioje buvo laukiama teismo sprendimo, kaip manoma, turėjusio turėti lemiamą įtaką sprendžiant kas yra aukščiau: teisė į asmens duomenų apsaugą, JAV technologijų gigante laikomos Apple prestižas ar žvalgybos institucijų interesai nacionalinio saugumo užtikinimo kontekste.

Nors žemesnės instancijos teismai ir tenkino FTB prašymą įpareigoti Apple sukurti programinę įrangą, kuri sudarytų jiems iki tol technologiškai neįmanomą galimybę – nesėkmingai bandyti atrakinti teroro akto vykdymu įtariamo mirusio asmens telefoną – koks būtų buvęs Aukščiausiojo teismo sprendimas nėra aišku. FTB atsiėmė prašymą prieš pat teismo posėdį ir rado kitą būdą kaip apeiti Apple telefono apsaugą – paslaugų teikimo sutartį su hakeriu, kuris sukūrė programinę įrangą telefono atrakinimui. Spėjama, kad FTB hakerio paslauga kainavo 4 mln. dolerių. Manoma, kad Apple buvo paruošusi tokius argumentus, kurie visiškai nepaliko vilties FTB šią bylą laimėti[242].

Rašyti apie asmens duomenų apsaugą JAV ne veltui pradėjau nuo teismų praktikos analizės. Ji tiesiogiai įtakojo JAV įstatymų leidybą ir jos nuostatomis remiantis buvo kuriami teisę į asmens duomenų apsaugą elektroninių duomenų atžvilgiu reglamentuojantys teisės aktai. Todėl jos doktrinos pagrindinius bruožus būtina žinoti prieš pradedant teisės aktų – ECPA, FISA ir EO 12,333 – analizę.

2.2.2. Ikiteisminis tyrimas

Katz v. United States bylos pasekoje, elektroninė erdvė, kaip nusikalstamų veikų tyrimo vieta, JAV teisės aktuose buvo įtvirtinta 1968 m. Trečiojoje antraštėje – Kelis aspektus apimančios nusikaltimų kontrolės ir saugių gatvių akte (angl. *Title III Omnibus*

---

[238] „Hester v. United States“, *Legal Information Institute*, žiūrėta 2020 m. rugsėjo 4 d., https://www.law.cornell.edu/supremecourt/text/265/57 .

[239] „Kyllo v. United States“, *FindLaw, žiūrėta 2020 m. rugsėjo 4 d.,* https://caselaw.findlaw.com/us-supreme-court/533/27.html.

[240] *United States v. Jones*, *supra note*, 215.

[241] *Kyllo v. United States, op. cit., 239.* „Florida v. Jardines“, *FindLaw, žiūrėta 2020 m. rugsėjo 4 d.,* https://caselaw.findlaw.com/us-supreme-court/11-564.html. *„Maryland v. King“, FindLaw, žiūrėta 2020 m. rugsėjo 4 d.,* https://caselaw.findlaw.com/us-supreme-court/12-207.html.

[242] Farivar, *supra note,* 22: 55.

Crime Control and Safe Street Act). Šis teisės aktas reglamentavo realiuoju laiku vykstančios komunikacijos elektroninėje erdvėje perėmimo tvarką ir taisykles. Nors nuo 1968 m. iki dabar komunikacijos rūšys ir pobūdis bei teisėsaugos institucijų poreikiai ir galimybės[243] labai pasikeitė, tačiau Telefoninių pokalbių klausymosi akte įtvirtinta sekimo elektroninėje erdvėje sąvoka iš esmės išliko nepakitusi[244]. 1968 m. Kelis aspektus apimančios nusikaltimų kontrolės ir saugių gatvių aktas įtvirtino dvi duomenų rinkimo elektroninėje erdvėje rūšis: telefoninių pokalbių klausymąsi (angl. *wiretapping*), klausymąsi per pasiklausymo įrangą (angl. *bugging*) ir elektroninį klausymąsi (angl. *electronic eavesdropping*). Telefoninių pokalbių klausymasis buvo apibrėžiamas kaip laidinės komunikacijos perėmimas (pvz. komunikacijos laidiniais telefonais), o klausymąsi per pasiklausymo įrangą (angl. *bugging*) ir elektroninis klausymasis (angl. *electronic eavesdropping*) – kaip miniatiūrinių elektroninių įrenginių naudojimas komunikacijos klausymui, transliavimui ar įrašymui[245]. 1986 m. buvo priimtos Kelis aspektus apimančios nusikaltimų kontrolės ir saugių gatvių akto pataisos – Elektroninės komunikacijos privatumo aktas (angl. *Electronic Communications Privacy Act*) (toliau – ECPA). ECPA yra iki šiol galiojantis teisės aktas, kuris reglamentuoja elektroninių ryšių paslaugų teikėjų saugomų duomenų rinkimą. Pasak Teisingumo departamento (angl. *Departament of Justice (DoJ)*) ECPA skirta apsaugoti elektroninę komunikaciją jos vykimo realiuoju laiku, keliavimo elektroninėje erdvėje bei istorinės komunikacijos saugojimo metu[246]. Asmens duomenų rinkimas elektroninėje erdvėje visų pirma asocijuojasi tiesiogiai su pačių teisėsaugos ir žvalgybos institucijų vykdomu rinkimu, tačiau ECPA reglamentuoja per tarpininkus – elektroninių paslaugų teikėjus – vykdomą asmens duomenų rinkimą elektroninėje erdvėje. Tiesioginis asmens duomenų rinkimas elektroninėje erdvėje yra reglamentuojamas kitais teisės aktais: EO 12333, FISA, Baudžiamojo proceso 41 straispniu. Pažymėtina ir tai, kad ECPA yra taikoma tik teisėsaugos institucijoms, žvalgybos institucijų veiklos šis teisės aktas nereglamentuoja.

ECPA sudaro 3 skirsniai, kurie patys yra laikomi atskirais teisės aktais:

1. Telefoninių pokalbių klausymosi aktas (angl. *Wiretap act*);
2. Saugomos komunikacijos aktas (angl. *Stored Communications Act (SCA)*);
3. Įeinančios ir išeinančios komunikacijos registravimo aktas (angl. *Pen/Trap register act*).

1994 m. ECPA buvo papildyta Pagalbos teisėsaugos institucijoms aktu (angl. *Assitance for Law enforcement act*), 2001 m. Amerikos susivienijimo ir stiprinimo teikiant tinkamas priemones, reikalingas perimti ir trukdyti terorizmui aktu (angl. *Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and*

---

243 Simon Kuper, „Edward Snowden and the Millennial Conscience“, 2019, žiūrėta 2020 m. rugsėjo 4 d., https://www.ft.com/content/0d0114fe-1ea3-11e9-b126-46fc3ad87c65.

244 Carr ir Bellia, *supra note,* 21: 2.

245 *Ibid.,* 3.

246 „The Electronic Communications Privacy Act ECPA Regulates How Information Stored“, *American Military University*, žiūrėta 2020 m. rugsėjo 4 d., https://www.coursehero.com/file/p24shsm4/The-Electronic-Communications-Privacy-Act-ECPA-regulates-how-information-stored/.

Obstruct Terrorism Act (USA PATRIOT act)), 2006 m. JAV PATRIOT pakartotinio pripažinimo aktais, 2015 m. ECPA pataisomis (angl. *ECPA Amendments Act of 2015*) ir Elektroninių laiškų privatumo aktu (angl. *the Email Privacy Act*)[247].

Atitinkamai ECPA asmenų komunikaciją skirsto į 3 grupes, kuri visa yra laikoma komunikacija el. erdvėje:

1) laidinė komunikacija – tai bent koks žodinės komunikacijos perdavimas laidais, kabeliais arba kitomis panašomis komunikacijos perdavimo priemonėmis;
2) žodinė komunikacija – tai žodžiais ar kitokio pobūdžio garsais išreikšta komunikacija, kuomet asmuo tikisi privatumo, neapimanti elektroninės komunikacijos;
3) elektroninė komunikacija – tai bent koks ženklų, signalų, raštų, paveiksliukų, garsų, duomenų ir kt. informacijos perdavimas laidinėmis, radijo, elektromagnetinėmis, fotoelektroninėmis arba fotooptinėmis priemonėmis šalies viduje ir išorėje, išskyrus laidinę ir žodinę komunikaciją bei kitas numatytas išimtis.

Teismų praktikoje yra pripažinta, kad vadovaujantis ECPA teisėsaugos institucijos gali rinkti tiek įvykusios, tiek realiuoju laiku vykstančios elektroninės komunikacijos metaduomenis ir jos turinį esantį: el. laiškuose[248], SMS žinutėse[249], viešos ir privačios komunikacijos socialiniuose tinkluose[250], privačius Youtube video[251], istorinę mobiliojo ryšio nustatymo vietos informaciją (angl. *historical cell site location information*)[252]. Tačiau to pagrindas skiriasi priklausomai nuo objekto ir rinkimą reglamentuojančio akto.

Pirmoji ECPA dalis – Telefoninių pokalbių klausymosi aktas (angl. *Wiretap act*) – reglamentuoja realiu laiku vykstančios laidinės ir elektroninės komunikacijos turinio perėmimą[253]. Vadovaujantis Telefoninių pokalbių klausymosi aktu, realiuoju laiku vykstančios laidinės ir elektroninės komunikacijos turinio rinkimas, naudojimas ir atskleidimas yra draudžiamas, išskyrus tame akte įtvirtintas išimtis[254]. Viena iš tų išimčių yra teisėsaugos vykdomas realiuoju laiku vykstančios laidinės ir elektroninės komunikacijos rinkimas pagal telefoninių pokalbių klausymosi orderį (angl. *wiretap order*), kuriam yra taikomi visi *Berger v. New York* byloje suformuoti principai[255]. Taigi,

---

[247] Richard M. Thompson II ir Jared P. Cole, „Stored Communications Act: Reform of the Electronic Communications Privacy Act (ECPA)“, (Congressional Research Service, 2015), 12.

[248] „Theofel v. Farey-Jones“, *FindLaw*, žiūrėta 2020 m. rugsėjo 4 d., https://caselaw.findlaw.com/us-9th-circuit/1419886.html.

[249] „Quon v. Arch Wireless Operating Co., Inc.“, *FindLaw*, žiūrėta 2020 m. rugsėjo 4 d., https://caselaw.findlaw.com/us-9th-circuit/1144813.html.

[250] „Crispin v. Christian Audigier“, *CaseTex*, žiūrėta 2020 m. rugsėjo 4 d., https://casetext.com/case/crispin-v-christian-audigier.

[251] „Viacom Intern. Inc. v. YouTube Inc.“, *FindLaw*, žiūrėta 2020 m. rugsėjo 4 d., https://caselaw.findlaw.com/us-2nd-circuit/1597925.html.

[252] „In Re of the United States for Historical Cell Site Data, 747 F. Supp. 2d 827“, *CaseText*, žiūrėta 2020 m. rugsėjo 4 d., https://casetext.com/case/in-re-us-for-historical-cell-site-data.

[253] „Electronic Communications Privacy Act of 1986“, žiūrėta 2020 m. rugsėjo 4 d., https://it.ojp.gov/PrivacyLiberty/authorities/statutes/1285.

[254] „18 U.S. Code § 2511 – Interception and Disclosure of Wire, Oral, or Electronic Communications Prohibited“, *Legal Information Institute*, žiūrėta 2020 m. rugsėjo 4 d., https://www.law.cornell.edu/uscode/text/18/2511.

[255] Telefoninių pokalbių klausymosi orderis yra teisėtas tik tada kai yra: 1) teismo orderis (angl. *warrant*), kuriam taikomi įprastiniai tikėtinos priežasties (angl *probable cause*) buvimo ir apibrėžtumo (angl. *particularity*) reikalavimai – teisėsaugos institucijos kreipdamosi į teismą privalo įrodyti, kad telefoninio pokalbio turinys gali atskleisti įrodymų apie nusikalstamą veiką ir konkrečiai apibrėžti kokiam telefono numeriui jis bus taikomas;

norėdamos rinkti realiuoju laiku vykstančią laidinę ir elektroninę komunikaciją teisėsaugos institucijos turi kreiptis į teismą su prašymu dėl siūlomo orderio ir pagrįsti jo reikalingumą. Telefoninių pokalbių klausymosi orderio (angl. *wiretap order*) reikalingumui pagrįsti teisėsaugos institucijos privalo įrodyti tikėtiną priežastingumą (angl. *probable cause*) ir apibrėžtumą (angl. *particularity*), nurodyti laiko trukmę. Gavęs tokį prašymą, teismas patikrina jo pagrįstumą pagal Telefoninių pokalbių klausymosi aktą (angl. *Wiretap act*) ir išduoda arba neišduoda specialų teismo telefoninių pokalbių klausymosi orderį (angl. *wiretap warrant*). Turėdamos teismo orderį teisėsaugos institucijos kreipiasi į telefoninių ar kitų elektroninės komunikacijos paslaugų teikėjus, kurie teismo orderio pagrindu suteikia teisėsaugos institucijoms techninę pagalbą dėl prisijungimo prie realiu laiku vykstančios asmens komunikacijos elektroninėje erdvėje[256]. Tačiau telefoninių pokalbių klausymosi orderis (angl. *wiretap warrant*) gali būti taikomas ne visų nusikalstamų veikų tyrimui, o tik Telefoninių pokalbių klausymosi akte (angl. *Wiretap act*) įvardintų nusikalstamų veikų atžvilgiu[257] bei tik tuo atveju, jeigu teisėsaugos institucijos sugeba pagrįsti teismui, kad kitais nusikalstamų veikų tyrimo metodais negali surinkti reikiamų duomenų arba jie yra per daug pavojingi[258]. Jeigu teisėsaugos institucijų veiksmai pagal telefoninių pokalbių klausymosi orderį (angl. *wiretap warrant*) sukelia asmenims žalą, tuomet jie turi teisę pareikšti civilinį ieškinį[259]. Tuo atveju, jeigu duomenys yra renkami nesilaikant Telefoninių pokalbių klausymosi akto (angl. *Wiretap act*) nuostatų, jie pripažįstami niekiniais teisme. Nors „Užnuodyto medžio ir jo vaisių“ doktrina paprastai yra taikoma JAV, tačiau asmens duomenų rinkimo elektroninėje erdvėje atveju ji taikoma ne visuomet.

Dar vienas Telefoninių pokalbių klausymosi akto (angl. *Wiretap act*) ypatumas yra tas, kad teismai privalo skelbti statistinę informaciją apie išduotus telefoninių pokalbių klausymosi orderius (angl. *wiretap warrant*). Žemiau esančiame paveiksle pateikti JAV teismų administracijos duomenys apima laikotarpį nuo 2005 m. iki 2015[260].

---

2) konkrečiai apibrėžtas laiko terminas;

3) asmeniui, kurio telefoninių pokalbių įrašai buvo teisėsaugos peržiūrėti, turi būti apie tai pranešta;

4) jeigu teisėsaugos institucijoms klausantis pokalbio paaiškėja, kad jis yra neaktualus tyrimui, šio pokalbio klausymasis turi būti nutrauktas, telefoninių pokalbių klausymasis turi būti sumažintas;

5) norint atnaujinti įvykusių telefoninių pokalbių turinio peržiūrėjimą yra reikalingas naujas teismo orderis, kuriam gauti reikia naujo teisėto pagrindo.

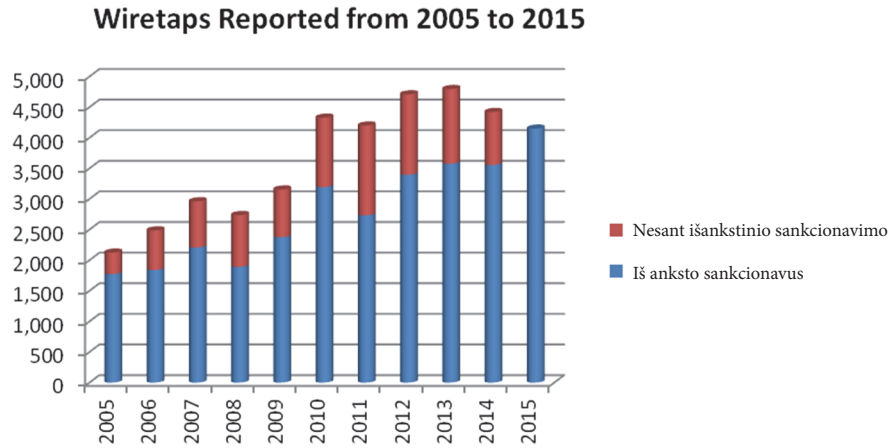
256 „18 U.S. Code § 2518 – Procedure for Interception of Wire, Oral, or Electronic Communications“, *Legal Information Institute*, žiūrėta 2020 m. rugsėjo 4 d., https://www.law.cornell.edu/uscode/text/18/2518.

257 18 U.S.C. § 2518(5), *Legal Information Institute*, žiūrėta 2020 m. rugsėjo 4 d., https://www.law.cornell.edu/uscode/text/18/2518.

258 *Ibid.*

259 18 U.S.C. § 2818(8)(d), *Legal Information Institute*, žiūrėta 2020 m. rugsėjo 4 d., https://www.law.cornell.edu/uscode/text/18/1028.

260 „Wiretap Report 2015“, *United States Courts*, žiūrėta 2020 m. rugsėjo 4 d., http://www.uscourts.gov/statistics-reports/wiretap-report-2015.



1 pav. *Telefoninių pokalbių klausymosi orderių skaičius 2005–2015 m.*

Telefoninių pokalbių klausymosi orderiai (angl. *wiretap warrant*) dažniausiai yra vartojami dėl telefoninių pokalbių (95%), tik 5 % yra vartojami kitoms telekomunikacinėms priemonėms[261]. 85% atvejų telefoninių pokalbių klausymosi orderiai (angl. *wiretap warrant*) yra naudojami nusikalstamų veikų, susijusių su narkotinėmis priemonėmis, užkardymui ir tyrimui[262]. Kiekvieno telefoninių pokalbių klausymosi orderio (angl. *wiretap warrant*) pagrindu perimtos telekomunikacijos metu yra sužinoma informacija vidutiniškai apie 100 kitų asmenų ir išklausoma vidutiniškai apie 3000 pokalbių[263]. Visais atvejais telefoninių pokalbių klausymosi orderių (angl. *wiretap warrant*) naudojimo atvejais įtariamasis asmuo yra sulaikomas, tačiau kaltinamai pareiškiami retai (pvz. 2015 m. tik 13,5%)[264]. Nuo 2015 m. pastebima įdomi tendencija, jog teisėsaugos institucijos nesinaudojo teise apie veiksmus, kuriems reikalingas telefoninių pokalbių klausymosi orderis (angl. *wiretap warrant*) atlikti iš anksto ir informuoti teismą per Telefoninių pokalbių klausymosi akto (angl. *Wiretap act*) numatytą terminą[265]. Nors ir atrodytų, jog to priežastimi galėtų būti teisėsaugos institucijų disciplinuotumas, tačiau Laura K. Donohue tai sieja su 2001 m. atsivėrusia galimybe teisėsaugos institucijoms rinkti duomenis elektroninėje erdvėje vadovaujantis ne tik

---

261 „Types of Surveillance Used, Arrests, and Convictions for Intercepts Installed January 1 Through December 31, 2015“, *United States Courts,* žiūrėta 2020 m. rugsėjo 4 d., https://www.uscourts.gov/sites/default/files/data_tables/wiretap_6_1231.2015.pdf.

262 „Major Offenses for Which Court-Authorized Intercepts Were Granted Pursuant to 18 U.S.C. § 2519 January 1 Through December 31, 2015“, *United States Courts,* žiūrėta 2020 m. rugsėjo 4 d., http://www.uscourts.gov/sites/default/files/data_tables/wiretap_3_1231.2015.pdf.

263 *Ibid.*

264 „Wiretap Report 2015“, *supra note*, 260.

265 „Wiretap Report 2017“, *United States Courts*, žiūrėta 2020 m. rugsėjo 4 d., http://www.uscourts.gov/statistics-reports/wiretap-report-2017.

Telefoninių pokalbių klausymosi akto (angl. *Wiretap act*), bet ir FISA[266]. Nuo 2017 m. prasidėjęs šimtaprocentinis telefoninių pokalbių klausymosi orderių (angl. *wiretap warrant*) nenaudojimas tai patvirtina[267].

Antroji ECPA dalis – Saugomos komunikacijos aktas (angl. *Stored Communications Act)* (toliau – SCA aktas). Šio teisės akto tikslas buvo teisiškai reglamentuoti įvykusių elektroninių komunikacijų duomenų, nesančių pačiu komunikacijų turiniu, naudojimą[268]. Duomenis, nesančius komunikacijos turiniu, SCA akto priėmimo laikotarpiu sudarė, pvz.: telefoninių skambučių istorija: informacija apie asmenį (vardas, pavardė, gyvenamosios vietos adresas, el. pašto adresas, telefono numeris) ir informacija apie skambutį (kokiam numeriui, iš kokio numerio skambinta, skambučio pobūdis (įeinantis, išeinantis), skambučio trukmė ir skambučio data[269]. Rengiant teisės aktą buvo vadovautasi logika, kad minėta informacija nėra tokia jautri kaip telefoninių pokalbių turinys, paprastai ją gali gauti pats duomenų subjektas, todėl jos apsauga gali būti mažesnė nei realiu laiku vykstančių pokalbių telefonu turinio perėmimui pagal Telefoninių pokalbių klausymosi aktą (angl. *Wiretap act*). Atsižvelgiant į tai SCA akte buvo įtvirtinta trečiosios šalies doktrina, pagal kurią teisėsaugos prieiga prie telefoninių pokalbių išklotinių nėra nei poėmiu, nei krata (angl. *neither search nor seizure*), ir atitinkamai todėl IV JAV Konstitucijos apsauga nebuvo taikoma ir todėl teismo orderis (angl. *court warrant*) nebuvo reikalingas, pakako teismo šaukimo (angl. *subpoena*)[270].

Tačiau laikotarpiu iki 2010 m. buvo susiklosčiusi labai įdomi praktika – nebuvo teisės akto, kuris reglamentuotų jau įvykusios (istorinės), tačiau vis dar saugomos komunikacijos el. erdvėje (pvz. el. laiškų, žinučių) turinio rinkimo. Todėl iki 2010 m. laikotarpio teisėsaugos institucijos šią informaciją galėjo rinkti visiškai be jokio teismo sankcionavimo, analogiškai kaip tel. pokalbių galėjo klausytis iki 1967 m. *Katz* bylos sprendimo įtakoto Telefoninių pokalbių klausymosi akto (angl. *Wiretap act*) priėmimo. 2010 m. byloje *United States v. Warshak* JAV Aukščiausiajam teismui konstatavus, kad teisėsaugos institucijoms norint perimti debesyje esančią informaciją IV JAV Konstitucija galioja ir teisėtas tokių duomenų rinkimas yra tik esant teismo sankcionuotam orderiui[271], nesankcionuotas asmens duomenų rinkimas buvo pripažintas neteisėtu. Tačiau tik nuo 2015 m. m. priėmus SCA akto pataisą – Elektroninių laiškų privatumo aktą (angl. *Email Privacy Act*) istorinės saugomos komunikacijos el. erdvėje turinys pateko į SCA akto apimtį. Nepaisant to, kad dabar šis teisės aktas apima ir

---

266 Donohue, *supra note*, 8: 26.

267 „Wiretap Report 2017“, *supra note*, 265.

268 18 U.S.C. Chapter 121 §§ 2701–2712, *Legal Information Institute*, žiūrėta 2020 m. rugsėjo 4 d., https://www.law.cornell.edu/uscode/text/18/part-I/chapter-121.

269 18 U.S. C. 2703 (c) (2), *Legal Information Institute*, žiūrėta 2020 m. rugsėjo 4 d., https://www.law.cornell.edu/uscode/text/18/2703.

270 Kerr, *supra note*, 227.

271 Sophia Cope, „House Advances Email Privacy Act, Setting the Stage for Vital Privacy Reform“, *Electronic Frontier Foundation*, 2016, žiūrėta 2020 m. rugsėjo 4 d., https://www.eff.org/deeplinks/2016/04/house-advances-email-privacy-act-setting-stage-vital-privacy-reform. „Coalition Letter in Support of Email Privacy Act (April 26)“, *Center for Democracy and Technology*, žiūrėta 2020 m. rugsėjo 4 d., https://cdt.org/insights/coalition-letter-in-support-of-email-privacy-act-april-26/.

komunikacijos turinio rinkimą, SCA išliko mažiausiai apsaugos privatumui suteikiantis ECPOJE[272] ir kartu labai daug dviprasmiškų nuostatų turintis teisės aktas, kurias teisėsaugos institucijos ir teismai aiškina skirtingai[273]. Kurias ir kaip taikyti SCA akto nuostatas priklauso ne tik nuo duomenų, kuriuos norima rinkti, bet ir nuo įmonės, į kurią norima kreiptis, veiklos pobūdžio, ir tų duomenų saugojimo būdo.

Duomenis, kurias teisėsaugos institucijos renka vadovaudamosi SCA aktu, yra 3 grupių:

1) pagrindinė abonento informacija (angl. *basic subscriber information*)[274] – vardas, pavardė, adresas;
2) kiti ne turininio pobūdžio įrašai ir informacija (angl. *other non content records and information*)[275] – duomenis apie vietinius ir nevietinius telefoninius pokalbius, jų dažnumą ir trukmę, paslaugų teikimo trukmę (įskaitant paslaugų teikimo pradžią) ir suteikiamų paslaugų tipus, telefono, kito įrenginio numerį ar kitokį abonemento numerį, identifikuojančią informaciją, įskaitant bent kurį laikinąjį interneto ryšio adresą ir informaciją apie apmokėjimus už suteiktas paslaugas (įskaitant kredito kortelės ar banko sąskaitos numerį);
3) turinys (angl. *content*)[276], kurio apsauga priklauso nuo to ar jis yra laikomas esančiu elektroninėje saugykloje (angl. *ellectronic storage*) ar ne[277]. Turiniu pagal SCA aktą yra laikoma pvz. SMS ir kitos tekstinės žinutės[278], el. laiškai[279], siuntų sekimo ir skrydžių numeriai, esantys el. laiškuose[280].

Yra penkios teismo leidimo rinkti asmens duomenis rūšys, kurias teisėsaugos institucijos gali prašyti išduoti:

1. Neperskaityto komunikacijos turinio (el. laiškų, balso pašto ir kt.), saugomam trumpiau nei 180 d. rinkimui pagrindas yra kratos orderis (angl. *search warrant*);
2. Neperskaityto komunikacijos turinio (el. laiškų, balso pašto ir kt.), saugomam ilgiau nei 180 d. rinkimui teismo šaukimas (angl. *subpoena*) arba D orderis (angl. *D order*), kratos orderis (angl. *search warrant*);

---

272 „United States v. Councilman“, *CaseLaw*, žiūrėta 2020 m. rugsėjo 4 d., https://caselaw.findlaw.com/us-1st-circuit/1290871.html.

273 Carr ir Bellia, *supra note,* 21: 535.

274 18 U.S. Code §2703(c)(2), *Legal Information Institute*, žiūrėta 2020 m. rugsėjo 4 d., https://www.law.cornell.edu/uscode/text/18/2703.

275 18 U.S. Code §2703(c)(1), *Legal Information Institute*, žiūrėta 2020 m. rugsėjo 4 d., https://www.law.cornell.edu/uscode/text/18/2703.

276 18 U.S. Code §2510(8), *Legal Information Institute*, žiūrėta 2020 m. rugsėjo 4 d., https://www.law.cornell.edu/uscode/text/18/2510.

277 Carr ir Bellia, *supra note,* 21: 539.

278 „Loop AI Labs Inc v. Gatti“, *CaseText*, žiūrėta 2020 m. rugsėjo 4 d., https://casetext.com/case/loop-ai-labs-inc-v-gatti-13. „Mintz v Mark Bartelstein & Associates, Inc.“, *CaseText*, žiūrėta 2020 m. rugsėjo 4 d., https://casetext.com/case/mintz-v-mark-bartelstein-assocs-1?q=Mintz%20v%20Mark%20Bartelstein%20%26%20Associates,%20Inc.%20&PHONE_NUMBER_GROUP=C&sort=relevance&p=1&type=case.

279 „Optiver Australia Pty. Ltd. & Anor v. Tilbra Trading Pty. Ltd. & Ors.“, *CaseText*, žiūrėta 2020 m. rugsėjo 4 d., https://casetext.com/case/optiver-australia-pty-ltd-v-tibra-trading-pty-ltd.

280 „In Re Yahoo Mail Litig., Case No. 13-CV-04980-LHK“, žiūrėta 2020 m. rugsėjo 4 d., https://casetext.com/case/in-re-yahoo-mail-litig-1.

3. Atidaryto el. laiško, klausomo balso pranešimo ir kt. – nėra aišku, manoma, kad SCA aktas netaikomas ir renkama turėtų būti pagal teismo šaukimą (angl. *subpoena*)[281];
4. Neturininio pobūdžio informacijos rinkimui – D orderis (angl. *D order*), kratos orderis (angl. *search warrant*);
5. Pagrindinei abonento informacijai (angl. *basic subscriber information*) – teismo šaukimas (angl. *subpoena*) arba kratos orderis (angl. *search warrant*)[282].

Įdomu yra tai, kad, išskyrus pirmu atveju, teisėsaugos institucijos gali rinktis, kurio teismo leidimo pagrindu duomenis rinks ir jeigu turi išduotą kratos orderį (angl. *search warrant*), tai gali rinkti visą kitą informaciją dėl kurios kratos orderis (angl. *search warrant*) nėra išduotas ne tik kad pakartotinai nesankcionavus, bet ir net neinformavus teismo[283].

Visus šiuos duomenis teisėsaugos institucijos, vadovaujantis SCA aktu ir turėdamos atitinkamą teismo sankcionavimą, gali rinkti tik iš elektroninių paslaugų teikėjų (angl. *electronic communication service*)[284], pvz. telefoninio ryšio operatorių ir el. pašto paslaugų teikėjų[285] bei nuotolinių kompiuterių paslaugų teikėjų (angl. *remote computer services providers*)[286], pavyzdžiui, debesų kompiuterijos paslaugų teikėjų (pvz. Google, Amazon) nepriklausomai nuo to ar tai yra pagrindinė verslo subjekto veikla ar ne. Bet tai dar ne viskas: rinkti gali tik tuo atveju, jei jie savo paslaugas siūlo viešai visuomenei[287], o turinio rinkimo atveju – tik tuos asmens duomenis, kurie yra paslaugų teikėjo elektroninėje saugykloje (angl. *electronic storage*)[288] arba kompiuterių saugykloje (angl. *computer storage*)[289]. Kur vėlgi apsauga priklauso priklausomai nuo to, kurioje saugykloje asmens duomenys yra. Jeigu informacija nepatenka į šias dvi duomenų saugojimo kategorijas ir vietas, SCA aktas yra netaikomas.

Praktikoje taikyti minėtas SCA akto nuostatas yra labai sudėtinga. Teisingumo departamentas (angl. *Department of Justice*) yra parengęs Naudojimosi vadovą[290], kurio rekomendacijos ne visada sutampa su teismų pozicija[291]. Sudėtingiausias klausimas

---

281 Carr ir Bellia, *supra note,* 21: 553.

282 *Ibid.*

283 *Ibid.*

284 Carr ir Bellia, *supra note,* 21: 537.

285 „Quon v. Arch Wireless Operating Cp., Inc.“, *CaseLaw*, žiūrėta 2020 m. rugsėjo 4 d., https://caselaw.findlaw.com/us-9th-circuit/1144813.html. „In Re applications of U. S. for orders Pursuant to title 18, U. S. Code Section 2703(d)“, *CaseLaw*, žiūrėta 2020 m. rugsėjo 4 d., https://casetext.com/case/in-re-application-of-us-2. Kaufman v Nest Seekers“, *CaseLaw*, žiūrėta 2020 m. rugsėjo 4 d., https://casetext.com/case/kaufman-v-nest-seekers.

286 18 U. S. Code §2711(2), *Legal Information Institute*, žiūrėta 2020 m. rugsėjo 4 d., https://www.law.cornell.edu/uscode/text/18/2711.

287 Pascal Pour Elle, Ltd. v. Jin, *CaseLaw*, žiūrėta 2020 m. rugsėjo 4 d., https://casetext.com/case/pascal-pour-elle-ltd-v-jin.

288 Carr ir Bellia, *supra note,* 21: 541.

289 *Ibid.*, 542-543.

290 „U.S. DOJ Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations“, *Public Intelligence*, žiūrėta 2020 m. rugsėjo 4 d., https://publicintelligence.net/u-s-doj-searching-and-seizing-computers-and-obtaining-electronic-evidence-in-criminal-investigations/.

291 Carr ir Bellia, *supra note,* 21: 546.

teisėsaugos institucijoms yra nustatyti, kada asmens duomenys yra laikomi esančiais elektroninėje saugykloje (angl. *electronic storage*). Teisingumo departamento (angl. *Department of Justice*) pozicija yra, kad elektroninėje saugykloje (angl. *electronic storage*) duomenys yra tik iki to momento, kol jie dar gavėjo nėra atidaryti. Pasak Teisingumo departamento (angl. *Department of Justice*) tai yra skiriamasis bruožas tarp el. paslaugų teikėjų ir nuotolinių kompiuterių paslaugų teikėjų (angl. *remote computer services providers*), kadangi adresato neatidaryti duomenys yra el. paslaugų teikėjų sistemoje, o perskaityti – jau nuotolinių kompiuterių paslaugų teikėjų (angl. *remote computer services providers*)[292], kurie gali sutapti su el. paslaugų teikėjais, bet gali ir nesutapti. Kodėl tai yra svarbu nustatyti? Nes skiriasi jų apsauga ir teismo leidimų sankcionavimo procedūros[293]. Kas, mano manymu, dabartinėmis technologinėmis galimybėmis, yra visiškai nelogiška žiūrint iš asmens teisų apsaugos pozicijų ir tik sukelia painiavos pačioms teisėsaugos institucijoms.

Kaip pavyzdį išanalizuokime asmens el. laiškų turinio rinkimo atvejį. El. laiškas, tol kol jis yra kelyje iš siuntėjo B pas gavėją A, nepatenka į SCA akto apimtį ir tokio laiško apsaugai galioja patys griežčiausi reikalavimai, numatyti Telefoninių pokalbių klausymosi akte (angl. *Wiretap act*), kadangi yra laikoma jog iš siuntėjo B pas gavėją A keliaujantis el. laiškas yra realiuoju laiku vykstanti komunikacija[294]. El. laiško siuntimo procesas iš viso užtrunka tik sekundės dalį. Taigi tą sekundės dalį el. laiško turiniui galioja pati griežčiausia apsauga. Gavėjo A gautas, bet dar neatidarytas el. laiškas yra laikomas laikinai saugomu el. paslaugų teikėjo elektroninėje saugykloje (angl. *in temporary electronic storage*)[295]. Tokių laiškų turinio rinkimui nebe Telefoninių pokalbių klausymosi akto (angl. *Wiretap act*), o SCA akto nuostatos jau yra taikomos ir teisėsaugos institucijos tokius el. laiškus gali rinkti turėdamos teismo kratos orderį (angl. *search warrant*). Atidarytas ir perskaitytas el. laiškas yra laikomas jau esančiu nuotolinėje kompiuterių saugykloje (angl. *remote computer storage*)[296]. Tokio laiško bei ilgiau nei 180 d. neperskaityto laiško turinio rinkimui teisėsaugos institucijoms teismo šaukimo (angl. *subpoena*)[297]. Atsakymo, kaip traktuoti skaitomą, bet dar neperskaitytą el. laišką, kol kas nėra. Autorės manymu, skirtingi apsaugos lygiai to paties el. laiško turinio rinkimui yra nelogiški, kadangi pvz. asmuo gali savo mobiliojo telefono darbalaukyje matyti dalį arba visą gauto, tačiau dar neatidaryto, el. laiško turinį. Toks el. laiškas, vadovaujantis SCA aktu, turi didesnę apsaugą, nei perskaitytas. Todėl asmuo, neatidaręs laiško, tačiau žinantis jo turinį, turi didesnę teisių apsaugą, nei tas,

---

[292] „Steve Jackson Games, Inc. v. United States Secret Service", *US Supreme Court*, žiūrėta 2020 m. rugsėjo 4 d., https://law.justia.com/cases/federal/district-courts/FSupp/816/432/1976489/. „U.S. DOJ Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations", *op. cit.*, 290: 123.

[293] Tim Cushing Fri, „Appeals Court: Stored Communications Act Privacy Protections Cover Opened And Read Emails", *Techdirt.*, žiūrėta 2020 m. rugsėjo 4 d., https://www.techdirt.com/articles/20190311/20480141775/appeals-court-stored-communications-act-privacy-protections-cover-opened-read-emails.shtml.

[294] „U.S. DOJ Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations", *op. cit.*, 290.

[295] „U.S. DOJ Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations", *supra note*, 290:124. Carr ir Bellia, *supra note,* 21: 542.

[296] *Ibid.*

[297] „U.S. DOJ Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations", op. cit., 290.

kuris atidarė. Pastarojo, asmens teisių apsauga dar labiau sumažėja po 180 d. Tuo tarpu taip niekada ir neatidariusio asmens, bet turinį žinančio, ir po 180 d. teisės saugomos griežčiausiu SCA akte įtvirtintu teismo sankcionavimo būdu – kratos orderiu (angl. *search warrant*). Taip pat nėra aišku, kaip yra traktuojamas ištrintas el. laiškas – esančiu nuotolinėje kompiuterių saugykloje (angl. *remote computer storage*), o galbūt nuotolinė kompiuterių saugykla (angl. *remote computer storage*) nebeapima šios sąvokos, kadangi asmuo A ištrinto el. laiško atžvilgiu nebesinaudoja nuotolinės kompiuterių saugyklos (angl. *remote computer storage*) paslaugomis. Taip pat iki 2018 m. buvo neaišku ar SCA aktas yra taikomas tik JAV, ar ir už JAV teritorijos ribų tuo apeinant teisėsaugos institucijų tarpusavio pagalbos sutartis. Technologiškai debesyje (angl. *cloud*) saugoma informacija gali nebūtinai būti JAV, nors paslaugų teikėjas paslaugas teikia JAV, ji gali būti kitoje valstybėje arba išskaidyta – dalis vienoje valstybėje, dalis kitoje. Iki 2015 m. teisėsaugos institucijos el. komunikacijos turinį galėjo rinkti iš nuotolinės debesų kompiuterijos (angl. *remote cloud computing*) paslaugų teikėjų nepriklausomai nuo to ar tas turinys buvo saugomas JAV ar bent kurioje kitoje valstybėje esančiuose serveriuose. Tačiau 2013 m. Microsoft inicijuota byla[298], šį suvokimą pakeitė. Nors pirmos instancijos teismas Microsoft skundą atmetė pasisakydamas, kad SCA akto veikimas nėra apribotas teritorija[299], Microsoft nesutikdama su tuo kreipėsi į apeliacinį teismą, kurio sprendimas buvo Microsoft naudai. Tačiau šis apeliacinio teismo sprendimas buvo apskųstas Aukščiausiajam teismui. Galutinį sprendimą Aukščiausias teismas turėjo priimti 2018 m. pabaigoje, tačiau kaip ir *Apple* byloje[300], nenorėdama rizikuoti sprendimu, kuris gali būti jo nenaudai, Teisingumo departamentas (angl. *Departmatent of Justice*) rado kitą būdą kaip išspręsti šį ginčą[301]. Sprendimą, šiuo atveju priėmė JAV Senatas, Microsoft, Apple ir kitų debesų kompiuterijos paslaugas teikiančių teikėjų pritarimu[302] priimdamas naują teisės aktą – Užsienyje esančių duomenų naudojimo teisėtumą apibrėžiantį aktą arba CLOUD aktą (angl. *Clarifying Lawful Overseas Use of Data Act arba the Cloud act (the CLOUD act)*). CLOUD akto esmė: teisėsaugos institucijos, turėdamas teismo išduotą kratos orderį (angl. *search warrant*) gali kreiptis į kompiuterių paslaugų teikėjus (angl. *computer service providers*), kad šie pateiktų JAV asmenų komunikacijos turinį, saugomą užsienyje esančiuose serveriuose. Kompiuterių paslaugų teikėjai (angl. *computer service providers*) gali atsisakyti suteikti prašomus duomenis tuo atveju, jeigu to negali padaryti pagal valstybės, kurioje yra saugomi duomenys, asmens duomenų apsaugą reglamentuojančius teisės aktus

---

298 „Microsoft Corp. v. United States“, *Harvard Law Review*, žiūrėta 2020 m. rugsėjo 4 d., https://harvardlawreview.org/2016/12/microsoft-corp-v-united-states/.

299 Zack Whittaker, „How One Judge Single-Handedly Killed Trust in the US Technology Industry“, *ZDNet*, žiūrėta 2020 m. rugsėjo 4 d., https://www.zdnet.com/article/how-one-judge-single-handedly-killed-trust-in-the-us-technology-industry/.

300 „United States v. Apple Inc.“, *CaseLaw*, žiūrėta 2020 m. rugsėjo 4 d., https://caselaw.findlaw.com/us-2nd-circuit/1702133.html.

301 Greg Stohr, „Justice Department Asks Court to Drop Microsoft Email Case“, *Bloomberg.Com*, 2018, žiūrėta 2020 m. rugsėjo 4 d., https://www.bloomberg.com/news/articles/2018-03-31/justice-department-asks-high-court-to-drop-microsoft-email-case.

302 Mary Jo Foley, „Microsoft Bullish on Congress' Inclusion of CLOUD Act in Funding Bill“, *ZDNet*, žiūrėta 2020 m. rugsėjo 4 d., https://www.zdnet.com/article/microsoft-bullish-on-congress-inclusion-of-cloud-act-in-funding-bill/.

tai yra draudžiama arba toks išdavimas pažeistų JAV asmens teises pagal tos valstybės įstatymus. Iki *Microsoft* bylos SCA aktas buvo labai patogus teisėsaugos institucijoms, kadangi leido apeiti įprastines abipusės pagalbos baudžiamosiose bylose sutartis ir norimą informaciją gauti greičiau ir paprasčiau tiesiogiai iš įmonių. CLOUD aktas, priklausomai nuo serverio buvimo vietos, JAV asmenims gali suteikti netgi aukštesnę teisių apsaugą nei jie turi JAV. Bet tai irgi sudaro dviprasmišką situaciją, kadangi asmens el. laiškai gali būti saugomi skirtingose valstybėse, nors jis naudojasi to paties paslaugų teikėjo paslaugomis. CLOUD aktas laikomas gera iniciatyva, tačiau ta iniciatyva tapo neišbaigtu ir spragų turinčiu teisės aktu.

Trečioji ECPA dalis – Įeinančios ir išeinančios komunikacijos registravimo aktas (angl. *Pen Registers and Trap and Trace Devices Act*[303]) – reglamentuoja informacijos apie išeinančius ir įeinančius būsimus telefoninius skambučius, internetinę komunikaciją (įeinančią, išeinančią) ir lankytinus el. tinklapius (IP adresai) rinkimą[304]. Vadovaujantis Įeinančios ir išeinančios komunikacijos registravimo aktu (angl. *Pen Registers and Trap and Trace Devices Act*) teisėsaugos institucijos turi teisę rinti informaciją apie vien tik išeinančią arba vien tik įeinančią elektroninę komunikaciją, tačiau gali būti renkama informacija ir apie abi elektronines komunikacijos grupes. Iki *Katz v. United States* bylos teisėsaugos institucijos šią informaciją galėjo rinkti savarankiškai be teismo leidimo[305], vėliau praktika pasisuko ta linkme, kad tapo reikalingas teismo leidimas, nes buvo pripažinta, kad informacijos apie būsimus telefoninius pokalbius rinkimas patenka į IV JAV Konstitucijos pataisos taikymo apimtį[306]. JAV Senatas 1986 m. priėmęs Įeinančios ir išeinančios komunikacijos registravimo aktą (angl. *Pen Registers and Trap and Trace Devices Act*) uždraudė perimti informaciją apie įeinančius ir išeinančius telefoninius pokalbius[307], išskyrus teisės akte numatytas išimtis[308]. Viena iš tų išimčių – teisėsaugos institucijų veikla pagal specialų teismo orderį (angl. *pen trap order*) vadovaujantis Įeinančios ir išeinančios komunikacijos registravimo aktu[309]. Kaip veikia Įeinančios ir išeinančios komunikacijos registravimo aktas?

Teisėsaugos institucijos, turėdamos teismo išduotą orderį (angl. *pen trap order*) kreipiasi į paslaugų teikėjus, kad jie, teismo orderio pagrindu, suteiktų techninę pagalbą renkant informaciją apie jų abonento būsimą elektroninę komunikaciją. Informacija, kurią teisėsaugos institucijos teismo orderio pagrindu gali perimti, apima tik metaduomenis, sudarančius informaciją apie rinktus numerius, numerių maršrutus, skambinusius numerius, ir signalo informaciją, IP adresatą (angl. *dialing, routing,*

---

303 18 U. S. Code §3121-3127, *Legal Information Institute*, žiūrėta 2020 m. rugsėjo 4 d., https://www.law.cornell.edu/uscode/text/18/3121.

304 18 U. S. Code §3127(3), *Legal Information Institute*, žiūrėta 2020 m. rugsėjo 4 d., https://www.law.cornell.edu/uscode/text/18/3127.

305 Smith v. Maryland, *supra note*, 212.

306 Katz v. United States. *supra note*, 193.

307 18 U.S. Code §3121, *Legal Information Institute*, žiūrėta 2020 m. rugsėjo 4 d., https://www.law.cornell.edu/uscode/text/18/3121.

308 *Ibid.*

309 18 U. S. Code §3122, *Legal Information Institute*, žiūrėta 2020 m. rugsėjo 4 d., https://www.law.cornell.edu/uscode/text/18/3122.

addressing and signaling information)[310]. Komunikacijos turinys ir informacija apie atsiskaitymą nepatenka į Įeinančios ir išeinančios komunikacijos registravimo pagrindu gauto teismo orderio taikymo apimtį.

Teisėsaugos institucijų prašymo teismui turinys taip pat yra labai paprastas. Teismas turi įsitikinti tik tokio pobūdžio informacijos būtinumu[311] ir patikrinti ar teisėsaugos prašyme yra įvardinta konkreti tokią informaciją rinksianti teisėsaugos institucija[312]. Spręsdamas orderio (angl. *pen trap order)* išdavimo klausimą jis neanalizuoja byloje esančių įrodymų kaip telefoninių pokalbių klausymo orderio (angl. *wiretap order*) atveju, kuomet yra renkamas realiuoju laiku vykstančios komunikacijos turinys. Taigi teismo vaidmuo asmens teisių apsaugoje dėl asmens duomenų rinkimo Įeinančios ir išeinančios komunikacijos registravimo akto pagrindu yra simbolinis. Situaciją dėl asmens teisių apsaugos sušvelnina tik tai, kad yra numatytas maksimalus teismo orderio (angl. *pen/trap order*) galiojimo terminas – 60 dienų[313]. Teisės aktas neįpareigoja apie tai, kad teisėsaugos institucijos rinks ar rinko asmens duomenis pranešti pačiam asmeniui. Tačiau mes turime dar vieną pavyzdį kaip pačios paslaugas asmeniui teikiančios įmonės imasi veiksmų tam, kad būtų užtikrintos jų klientų teisės. Kai kurios iš paslaugas teikiančių įmonių[314] savo vidaus politiką reglamentuojančiuose teisės aktuose yra numačiusios pareigą pranešti savo klientams apie tai, jeigu teismo įsakymo pagrindu buvo vykdomas informacijos apie jų skambučius rinkimas, todėl tokiu atveju šių komunikacines paslaugas teikiančių įmonių klientai sužino apie teisėsaugos institucijų veiksmus. Taigi „gerosios įmonių praktikos" pagrindu šiuo atveju teisė į asmens duomenų apsaugą yra užtikrinama labiau nei teisės aktais.

Akcentuotina tai, kad ECPA nuostatos, saugančius asmenis nuo neteisėto telekomunikacijos ir elektroninių paslaugų teikėjų veikimo, vadovaujantis naujausia JAV teismų praktika, yra taikomos tiek JAV asmenų, tiek ne JAV asmenų atžvilgiu[315]. *Suzlon Energy Ltd v. Microsoft Corp*[316] byloje teismas konstatavo, kad „ECPA nuostatos galioja „asmenų", kurie nėra skirstomi į JAV ir ne JAV, atžvilgiu". Tokį savo sprendimą teismas argumentavo teisine logika, kad norint visiškai apsaugoti asmenis yra privaloma ECPA taikymą privaloma išlėsti, nepriklausomai nuo to, kad ta komunikacija buvo adresuota (JAV ar ne JAV asmeniui) ir iš kur ta komunikacija buvo gauta (JAV

---

310 18 U. S. Code §3127(4), *Legal Information Institute*, žiūrėta 2020 m. rugsėjo 4 d., https://www.law.cornell.edu/uscode/text/18/3127.

311 18 U. S. Code §3121, *Legal Information Institute*, žiūrėta 2020 m. rugsėjo 4 d., https://www.law.cornell.edu/uscode/text/18/3121.

312 18 U. S. Code §3121, *Legal Information Institute*, žiūrėta 2020 m. rugsėjo 4 d., https://www.law.cornell.edu/uscode/text/18/3121.

313 „Barnett v State", *CaseLaw*, žiūrėta 2020 m. rugsėjo 4 d., https://caselaw.findlaw.com/al-court-of-criminal-appeals/1096220.html.

314 „Privacy: An Overview of Federal Statutes Governing Wiretapping and Electronic Eavesdropping", žiūrėta 2020 m. rugsėjo 4 d., https://www.everycrsreport.com/reports/98-326.html.

315 Bignami, *supra note*, 185:21.

316 „Suzlon Energy Ltd v. Microsoft Corp.", *US Supreme Court*, žiūrėta 2020 m. rugsėjo 4 d., https://law.justia.com/cases/federal/appellate-courts/ca9/10-35793/10-35793-2011-10-03.html.

ar ne JAV asmens)[317]. Apsiribojimas vien tik JAV asmenimis elektroninių paslaugų teikėjams sukeltų daug sunkumų, kuriuos būtų labai sudėtinga išspręsti. Elektroninių paslaugų teikėjas, tokiu atveju, kažkaip turėtų nustatyti ar konkrečios paskyros turėtojas yra JAV pilietis ar nuolatinis JAV gyventojas, kuriems yra taikoma IV JAV Konstitucijos apsauga. Jeigu taip, ar JAV asmeniu buvo visą laiką, ar ne, nuo kada iki kada juo buvo ar yra ir t. t. Tą padaryti yra neįmanoma[318]. Nepaisant didelio žingsnio teismų praktikoje į priekį, visgi civilinėje *Suzlon Energy Ltd v. Microsoft Corp* byloje teismas pasisakė tik dėl JAV teritorijoje esančiuose serveriuose esančios ne JAV asmens informacijos naudojimo pažeidimo, kurį įvykdė elektroninių paslaugų teikėjas. Todėl lieka neaišku ar ECPA taikoma informacijai, esančiai ne JAV teritorijoje veikiančiuose serveriuose ir ar tai yra taikoma ir teismuose. Oficialių atsakymų į šiuos klausimus kol kas nėra pateikta, todėl traktuoti, kad civilinės bylos analogija bus perkelta į baudžiamąjį persekiojimą, kol kas nėra pagrindo.

2.2.3. Teisėsaugos institucijų prisijungimai prie elektroninės erdvės įrenginių

Vykdomosios valdžios vykdomi prisijungimai prie elektroninės erdvės (angl. *government hacking*) taip pat yra laikoma kontraversiška valstybės institucijų vykdoma asmenų sekimo priemone[319]. Vykdomosios valdžios prisijungimai prie elektroninės erdvės (angl. *government hacking*) yra vykdoma pagal Baudžiamojo proceso kodekso 41 straipsnį (angl. Rule 41). Šių prisijungimų prie elektroninės erdvės esmę sudaro vykdomosios valdžios institucijų pareigūnų galimybė įsilaužti į asmens kompiuterį[320], patekti per anonimę programinę įrangą (angl. *anonymized software*) be įsilaužimo[321], naudoti kompiuterio mikrofoną[322] ar vaizdo kamerą[323] atlikti kitus veiksmus. Šių vykdomosios valdžios institucijų veiksmų priežastys ir tikslai gali būti įvairūs, o skaidru-

---

317 Mu-Chia Kao, „9th Circuit: ECPA Protects Domestic Communications of Non-US Citizens“, ILI Student Blog, žiūrėta 2020 m. rugsėjo 4 d., https://blogs.law.nyu.edu/privacyresearchgroup/2012/03/9th-circuit-ecpa-protects-domestic-communications-of-non-us-citizens/.

318 *Ibid.*

319 Jonathan Mayer, „Government Hacking“, *Yale Law Journal* 127, no. 3 (2018 2017): 570–663.

320 „Going Dark: Encryption, Technology, and the Balances Between Public Safety and Privacy“, *Federal Bureau of Investigation*, žiūrėta 2020 m. rugsėjo 4 d., https://www.fbi.gov/news/testimony/going-dark-encryption-technology-and-the-balances-between-public-safety-and-privacy. Sabrina I. Pacifici, „House Homeland Security Report – Going Dark, Going Forward: A Primer on the Encryption Debate“, BeSpacific, žiūrėta 2020 m. rugsėjo 4 d., https://www.bespacific.com/house-homeland-security-report-going-dark-going-forward-a-primer-on-the-encryption-debate/.

321 Roger Dingledine, Nick Mathewson ir Paul Syverson, „Tor: The Second-Generation Onion Router“, žiūrėta 2020 m. rugsėjo 4 d., https://www.researchgate.net/publication/2910678_Tor_The_Second-Generation_Onion_Router.

322 Mayer, *op cit,* 319.

323 „United States v. Torres“, *CaseLaw*, žiūrėta 2020 m. rugsėjo 5 d., https://caselaw.findlaw.com/us-8th-circuit/1214998.html. „United States v. Biasucci“, *CaseText*, žiūrėta 2020 m. rugsėjo 5 d., https://casetext.com/case/united-states-v-biasucci. „United States v. Cuevas-Sanchez“, *CaseText*, žiūrėta 2020 m. rugsėjo 5 d., https://casetext.com/case/us-v-cuevas-sanchez. „United States v. Mesa-Rincon“, *CaseText*, žiūrėta 2020 m. rugsėjo 5 d., https://casetext.com/case/us-v-mesa-rincon. „United States v. Koyomejian“, *CaseText*, žiūrėta 2020 m. rugsėjo 5 d., https://casetext.com/case/us-v-koyomejian. „United States v. Falls“, *CaseLaw*, žiūrėta 2020 m. rugsėjo 5 d., https://caselaw.findlaw.com/us-2nd-circuit/1207287.html. „United States v. Williams“, *CaseLaw*, žiūrėta 2020 m. rugsėjo 5 d., https://caselaw.findlaw.com/dc-court-of-appeals/1191178.html.

mas – minimalus[324]. Manoma, kad kai kurios Teisingumo Departamento agentūros ir FTB turi vidines hakerių-darbuotojų komandas, tačiau gali samdyti ir išorinius sekimo paslaugas teikiančius asmenis (ekspertus) ar įmones[325].

Equation Group – tai Kaspersky laboratorijos 2015 m. atrasta hakerių grupuotė[326]. Kaspersky laboratorijos atstovai *Equation Group* laiko stipriausių hakerių grupuote, naudojančia sudėtingiausias technikas ir turinčią stipriausius kibernetinio karo ginklus[327]. Manoma, kad ji gali būti NSA dalimi arba yra galimai susijusi su NSA ir JAV vykdomu asmens duomenų rinkimu[328] ir kibernetinėmis atakomis[329]. 2016 m. rugpjūčio 16 d. buvo įsilaužta į pačią *Equation group*[330]. Teigiama, kad po įsilaužimo juodojoje rinkoje[331] pasirodžiusi informacija patvirtina Kaspersky Lab prielaidas apie *Equation group* sąsajas su NSA[332]. Už 1 milijoną bitkoinų (578 mln. JAV dolerių)[333] parduodamos informacijos bei slaptų įsilaužimo ir sekimo įrankių tikrumo patvirtinimui juos nulaužę hakeriai viešai atskleidė dalį *Equation group* turėtos informacijos bei dalį slaptų įsilaužimo ir sekimo įrankių[334]. Tarp tos informacijos – ir E. Snowden 2013 m. atskleista informacija apie JAV vykdomą masinį asmens duomenų rinkimą[335]. Tai yra laikoma ekspertų nuomonės apie *Equation group* buvimą slaptu NSA padaliniu, pagrindimu, tačiau galutinai ši prielaida iki šiol liko nei įrodyta, nei patvirtinta[336]. Pats E. Snowden paskelbė neabejojantis, jog *Equation group* buvo nulaužta *Shadow brokers* slapyvardžiu pasivadinusių Rusijos saugumo tarnybos padalinių ir yra kaip atsakas

---

324 „Government Hacking“, *Privacy International*, žiūrėta 2020 m. rugsėjo 4 d., https://privacyinternational.org/learn/government-hacking.

325 Rhys Dipshan, „A Federal Policy Loophole Is Supporting the Hacking-for-Hire Market. Can It Be Closed?“, *Slate Magazine*, 2018, žiūrėta 2020 m. rugsėjo 5 d., https://slate.com/technology/2018/06/the-federal-policy-loophole-supporting-the-hacking-for-hire-market.html.

326 Dan Goodin, „How ‘Omnipotent’ Hackers Tied to NSA Hid for 14 Years—and Were Found at Last“, *Ars Technica*, 2015, žiūrėta 2020 m. rugsėjo 5 d., https://arstechnica.com/information-technology/2015/02/how-omnipotent-hackers-tied-to-the-nsa-hid-for-14-years-and-were-found-at-last/.

327 GReAT, „Equation: The Death Star of Malware Galaxy“, žiūrėta 2020 m. rugsėjo 5 d., https://securelist.com/equation-the-death-star-of-malware-galaxy/68750/.

328 Ellen Nakashima, „Powerful NSA Hacking Tools Have Been Revealed Online“, *Washington Post*, 2016, žiūrėta 2020 m. rugsėjo 5 d., https://www.washingtonpost.com/world/national-security/powerful-nsa-hacking-tools-have-been-revealed-online/2016/08/16/bce4f974-63c7-11e6-96c0-37533479f3f5_story.html.

329 Thomas Brewster, „Equation = NSA? Researchers Uncloak Huge ‘American Cyber Arsenal’“, žiūrėta 2020 m. rugsėjo 5 d., https://www.forbes.com/sites/thomasbrewster/2015/02/16/nsa-equation-cyber-tool-treasure-chest/#5b3df5c9417f. Goodin, *op. cit.,* 326.

330 Pierluigi Paganini, „The Alleged NSA’s Unit The Equation Group Has Been Hacked. Exploits and Tools Leaked Online“, *Security Affairs*, 2016, žiūrėta 2020 m. rugsėjo 5 d., https://securityaffairs.co/wordpress/50334/cyber-warfare-2/equation-group-hacked.html.

331 *Ibid.*

332 *Ibid.*

333 *Ibid.*

334 Swati Khandelwal, „The NSA Hack — What, When, Where, How, Who & Why?“, *The Hacker News*, žiūrėta 2020 m. rugsėjo 5 d., https://thehackernews.com/2016/08/nsa-hack-russia-leak.html.

335 Pierluigi Paganini, „The Alleged NSA’s Unit The Equation Group Has Been Hacked!“, *Security Affairs*, žiūrėta 2020 m. rugsėjo 5 d., http://securityaffairs.co/wordpress/50334/cyber-warfare-2/equation-group-hacked.html.

336 Khandelwal, *op. cit.,* 334.

į NSA atskleistą informaciją apie Rusiją[337]. Tačiau yra manančių, jog tai gali būti ir informacijos nutekinimas iš NSA vidaus[338]. O Šilko kelio operacijos metu pareigūnų kontroliuojamų ir JAV vyriausybei priklausančių bitkoinų judėjimas į *Shadow brokers* sąskaitą kibernetinio saugumo ekspertui netgi leido iškelti prielaidą apie pačios *Shadow brokers* sąsajas su JAV vyriausybe[339]. Nepriklausomai nuo to, kas įsilaužė ir (ar) atskleidė informaciją apie *Equation group*, tai rodo du dalykus: 1) kokiu neįsivaizduoju mastu ir priemonėmis JAV saugumo tarnybos gali veikti ir rinkti ir renka asmens duomenis el. erdvėje: pasitelkia pačius profesionaliausius elitiniais vadinamus hakerius, veikiančius ne tik paprastame internete, bet ir tamsiajame internete (angl. *dark web*) bei giliajame tamsiajame internete (angl. *deep dark web*) ir galinčius nulaužti praktiškai bent kokią sistemą, kurti kompiuterinius virusus bei programas ir jų pagalba rinkti asmens duomenis[340]; 2) bei tai, kad JAV ir viso pasaulio saugumo tarnybų surinkti asmens duomenys nėra saugūs ir būtent asmens duomenys gali tapti kibernetinio karo priemone ir įrankiu. Tačiau ar visa ši JAV vykdomosios valdžios institucijų veikla yra teisėta, ar gali vykdomosios valdžios institucijos įsilaužti į asmenų kompiuterius? JAV teisinėje sistemoje atsakymas yra „taip".

Nėra nei vieno JAV teismo sprendimo ar JAV mokslininkų pozicijos, kad kompetentingos JAV institucijos negali prisijungti prie asmens kompiuterio[341]. Tačiau mokslininkai kritikuoja šią kompetentingų JAV institucijų teisę paprastai motyvuodami, kad niekur nėra įtvirtintų ir tokių įgaliojimų[342]. Toks argumentas, pasak J. Mayer JAV teisinės sistemos požiūriu yra visiškai niekinis, kadangi JAV teisėsaugos institucijos turi plačius įgaliojimus tam, kad ištirtų nusikalstamas veikas ir pagautų įtariamuosius, įskaitant naujų ir tiesiogiai teisės aktuose neįtvirtintų technologijų naudojimą (angl. *novel techniques*)[343]. Pavyzdžiui 1977 m. byloje *United States v. New York Telephone Company* Aukščiausias teismas konstatavo, kad teisėsaugos institucijos gali naudoti įeinančios ir išeinančios komunikacijos registratorius[344], nors tuo metu ir 9 ateinančius metus dar nebuvo parengtas net Įeinančios ir išeinančios komunikacijos registravimo akto (angl. *Pen Registers and Trap and Trace Devices Act*) projektas. Aukščiausias teismas motyvavo, kad Baudžiamojo proceso kodekso 41 straipsnis yra labai lankstus ir apima visas kratas ir poėmius, nepriklausomai nuo to, kokia technologija jos atlieka-

---

337 Rob Price, „Edward Snowden: Russia Might Have Leaked Alleged NSA Cyberweapons as a 'Warning'", *Business Insider*, žiūrėta 2020 m. rugsėjo 5 d., https://www.businessinsider.com/edward-snowden-shadow-brokers-russia-leaked-nsa-equation-group-files-warning-dnc-hacking-2016-8.

338 Matt Suiche, „Shadow Brokers: The Insider Theory", *Medium*, 2017, žiūrėta 2020 m. rugsėjo 5 d., https://blog.comae.io/shadowbrokers-the-insider-theory-ded733b39a55.

339 „Who Are The Shadow Brokers?", *Cyber Security Intelligence*, žiūrėta 2020 m. rugsėjo 5 d., https://www.cybersecurityintelligence.com/blog/who-are-the-shadow-brokers-2684.html.

340 Cheryl Niemeier, „Rolling in the Deep Not Dark Web", *AALL Spectrum* 20, no. 6 (2016 2015): 23–25.

341 Ahmed Ghappour, „Searching Places Unknown: Law Enforcement Jurisdiction on the Dark Web", *Stanford Law Review* 69, no. 4 (2017): 1075–1136.

342 *Ibid.*

343 Mayer, *supra note*, 319.

344 „United States v. New York Telephone Company", *US Supreme Court*, žiūrėta 2020 m. rugsėjo 5 d., https://supreme.justia.com/cases/federal/us/434/159/.

mos[345]. Taigi 41 straipsnis apima kratas ir poėmius, atliekamas ir elektroninėje erdvėje. Vadinasi, Vykdomosios valdžios vykdomi prisijungimai prie elektroninės erdvės (angl. *governmental hacking*) yra teisėta, todėl pagrindinis klausimas turėtų būti ar yra numatytų apribojimų ir ar jie yra užtektini asmens teisių apsaugos požiūriu.

IV JAV Konstitucijos pataisos atžvilgiu prisijungimas prie asmens kompiuterio kompiuterį yra laikomas krata ir mokslininkų dažnai lyginamas su uždarytos talpos atidarymu (angl. *opening the closed container*)[346]. Vadovaujantis *Katz* byloje suformuotu testu yra sutinkama, kad asmuo turi pagrįstą pagrindą tikėtis privatumo (angl. *reasonable expectation of privacy*) tam, kas yra arba ką galima pamatyti per jo asmeninį kompiuterį, todėl nepažeisdamos IV JAV Konstitucijos pataisos ir asmens teisių JAV teisėsaugos institucijos gali prisijungti prie asmens kompiuterio kratos orderio (angl. *search warrant)* pagrindu arba, jeigu į kompiuterį įsilaužiama siekiant perimti informaciją esamuoju laiku – telefoninių pokalbių klausymo orderio (angl. *wiretap order*) pagrindu[347]. Išduodant bent kurį orderį probleminiu yra apibrėžtumo (angl. *particularlity*) klausimas, t. y. ką gali daryti į kompiuterį prie elektroninės erdvės įrenginio prisijungę pareigūnai. Ar kratos orderis (angl. *search warrant)* ir telefoninių pokalbių klausymo orderis (angl. *wiretap order*) bus apibrėžtas tik tada, jei teismui teisėsaugos institucijos pateiks konkrečių failų, kuriuos planuoja tirti sąrašą, ar jie gali naršyti ir analizuoti visą kompiuteryje esančią ar būsimą informaciją. Teismų praktika kaip vertinti apibrėžtumą (angl. *particularlity*) elektroninės informacijos atveju nėra vieninga[348]. Teisėsaugos institucijos gali įsilaužti ne tik į kompiuterį, bet ir į viešą kompiuterinę sistemą (pvz. tinklapį) nesant teismo orderio (angl. *warrant*), nes įsilaužimas į viešą kompiuterinę sistemą nėra laikomas patenkančiu į IV JAV Konstitucijos pataisą, kadangi yra laikoma, kad vieša kompiuterinė sistema yra vieša vieta, todėl joje negalima pagrįstai tikėtis privatumo[349].

Šilko kelio byla (angl. *silk road case*) yra iki šiol žinomiausias 41 straipsnio naudojimo pavyzdys. Šilko keliu buvo vadinama negali juodajame internete veikusi narkotikų, užsakomųjų žmogžudysčių ir kompiuterinių įsilaužimų pardavimo vieta[350]. Kadangi nelegali prekyba vyko tamsiajame internete (angl. *dark web*) prisijungiant per TOR anoniminį tinklą, todėl pirkėjai ir pardavėjai tikėjosi visiško anonimiškumo ne vien tik vieni prieš kitus, bet ir dėl teisėsaugos vykdomo interneto srautų stebėjimo. Vis dėlto, FTB pavyko ne tik prisijungti prie anoniminio tinklo, bet ir identifikuoti jo įkūrėją,

---

345 „United States v. New York Telephone Company“, *supra note*, 344.

346 Michael Paul Falzone, „Search and Seizure-Limitations on Closed Container Searches in Open Fields-United States v. Ramapuram Notes“, *Wake Forest Law Review* 17, no. 3 (1981): 478–96.

347 „In Re Warrant to Search Target Computer at Premises Unknown“, *CaseText*, žiūrėta 2020 m. rugsėjo 5 d., https://casetext.com/case/in-re-search.

348 Andrew Crocker, „With Remote Hacking, the Government's Particularity Problem Isn't Going Away“, *Just Security*, 2016, žiūrėta 2020 m. rugsėjo 5 d., https://www.justsecurity.org/31365/remote-hacking-governments-particularity-problem-isnt/.

349 Mayer, *supra note*, 319.

350 „Case 76: Silk Road (Part 1)“, *Casefile: True Crime Podcast*, 2018, žiūrėta 2020 m. rugsėjo 5 d., https://casefilepodcast.com/case-76-silk-road-part-1/. Joshuah Bearman, „The Untold Story of Silk Road, Part 2: The Fall“, *Wired*, 2015, žiūrėta 2020 m. rugsėjo 5 d., https://www.wired.com/2015/05/silk-road-2/.

jam padėjusius asmenis ir juos patraukti baudžiamojon atsakomybėn. Tai rodo, kad net ir anoniminiu laikytam tinkle, anonimiškumas yra tik sąlyginis[351]. Tačiau 2013 m. 41 straipsnio galiojimas buvo apribotas JAV jurisdikcija, todėl FTB tyrimo metu privalėjo bendradarbiauti su Prancūzijos teisėsaugos institucijomis[352]. Teritorijos ribotumą esant globaliai el. erdvei FTB laikė tyrimo kliūtimi[353], todėl Šilko kelio bylos pagrindu buvo pasiūlyta esminė 41 straipsnio pataisa. 2016 m. įsigaliojusi 41 straipsnio pataisa suteikia teisę JAV teismams išduoti JAV teisėsaugos ir vykdomosios valdžios institucijoms kratos orderį (angl. *search warrant*) prisijungti prie asmenų kompiuterių ir atlikti informacijos apie asmenis elektroninėje erdvėje paiešką, neapribota teismo veiklos teritorija[354]. Tai reiškia, kad nuo 2016 m. gruodžio 1 d. teisėsaugos ir žvalgybos institucijos gavę teismo kratos orderį (angl. *search warrant*) galės prisijungti prie asmens kompiuterio bent kurioje pasaulio valstybėje[355] arba anoniminėje elektroninėje erdvėje (pvz. TOR)[356].

Mokslininkų ir žmogaus teisių aktyvistų itin kritikuojama 41 straipsnio pataisa buvo iš dalies reabilituota 2017 m. balandžio 24 d. praėjus vos keliems mėnesiams nuo jos įsigaliojimo. Aliaskos apygardos teismas vadovaudamasis 41 straipsniu sankcionavo 30 dienų leidimą FTB prisijungti prie visų, nepriklausomai nuo jų buvimo teritorijos, globalaus blotnet[357] tinklo Kelihos aukų kompiuterius tam, kad neutralizuoti šio tinklo veikimą[358]. Tai buvo pirmas kartas istorijoje kuomet JAV apygardos teismas leido FTB prisijungti prie bent kurioje pasaulio vietoje esančio kompiuterio tam, kad jį išvalytų nuo C&C programinės įrangos (angl. *command and control (C&C) software*)[359]. FTB teismo kratos orderio (angl. *search warrant*) pagrindu galėjo „užkrėsti" blotnet tinklo Kelihos aukų kompiuterius, paversdama juos į supernodus (angl. *supernodes)*. Supernodai (angl. *supernodes)* paskirsto prisijungimo sąrašus (angl. *connection lists*) į kitų aukų kompiuterius tokiu būdu „užnuodijant" visą tinklą ir neleidžiant užkrėstiems kompiuteriams komunikuoti su Kelihos hakerių kontroliuojamais įrenginiais. Teisingumo departamentas informavo, kad FTB šio teismo leidimo pagrindu nerinko kompiuteriuose esančio turinio, tačiau siekiant informuoti asmenis apie FTB veiksmus, FTB rinko Kelihos aukų IP adresus.

---

351 Nicole Lee, „Anonymity Is Dead and Other Lessons from the Silk Road Trial | Engadget", žiūrėta 2020 m. rugsėjo 5 d., https://www.engadget.com/2015-02-08-silk-road-trial-lessons.html.

352 Jerzy Kosiński, „Deepweb And Darknet – Police View, 2015, žiūrėta 2020 m. rugsėjo 5 d., https://www.researchgate.net/publication/282333966

353 Orin S. Kerr ir Sean D. Murphy, „Government Hacking to Light the Dark Web", *Stanford Law Review*, 2017, žiūrėta 2020 m. rugsėjo 5 d., https://www.stanfordlawreview.org/online/government-hacking-to-light-the-dark-web/.

354 „Hacking the World, a Discussion of Changes to Rule 41", *Fourth Amendment Advisory Committee*, žiūrėta 2020 m. rugsėjo 5 d., https://www.fourthadvisory.org/news/2016/9/29/rule41-briefing.

355 Pierluigi Paganini, „US Supreme Court Allows FBI Hacking Computers Located Worldwide", *Security Affairs*, 2016, žiūrėta 2020 m. rugsėjo 5 d., https://securityaffairs.co/wordpress/46808/laws-and-regulations/46808.html.

356 Swati Khandelwal, „U.S. Supreme Court Allows the FBI to Hack Any Computer in the World", *The Hacker News*, žiūrėta 2020 m. rugsėjo 5 d., https://thehackernews.com/2016/04/fbi-hacking-power.html.

357 „What Is A Botnet?", žiūrėta 2020 m. rugsėjo 5 d., https://us.norton.com/internetsecurity-malware-what-is-a-botnet.html.

358 Dan Goodin, „Feds Deliver Fatal Blow to Botnet That Menaced World for 7 Years", *Ars Technica*, žiūrėta 2020 m. rugsėjo 5 d., https://arstechnica.com/tech-policy/2017/04/feds-deliver-fatal-blow-to-botnet-that-menaced-world-for-7-years/.

359 Aliya Sternstein, „FBI Allays Some Critics with First Use of New Mass-Hacking Warrant", *Ars Technica*, 2020 m. rugsėjo 5 d., https://arstechnica.com/tech-policy/2017/04/fbi-allays-some-critics-with-first-use-of-new-mass-hacking-warrant/.

2.3. Asmens duomenų rinkimas elektroninėje erdvėje žvalgybos tikslais

2.3.1. Bendrieji žvalgybos elektroninėje erdvėje principai

Visuomenės saugumo užtikrinimas JAV yra laikomas prezidento arba vykdomosios valdžios prerogatyva. 1968 m. priimtas Trečiosios antraštės Kelis aspektus apimančios nusikaltimų kontrolės ir saugių gatvių aktas (angl. *Title III Omnibus Crime Control and Safe Street Act)* draudė nesankcionuotą telefoninių pokalbių pasiklausimą (elektroninį sekimą), tačiau šis teisės aktas neribojo prezidento ir vykdomosios valdžios veiksmų nacionalinio saugumo sumetimais[360]. Trečiosios antraštės Kelis aspektus apimančios nusikaltimų kontrolės ir saugių gatvių akte (angl. *Title III Omnibus Crime Control and Safe Street Act)* buvo netgi įtvirtinta nuostata leidžianti žvalgybos institucijų nacionalinio saugumo sumetimais surinktą informaciją naudoti baudžiamojo proceso tikslais tuo išplečiant vykdomosios valdžios galias[361]. Būtent ši Trečiosios antraštės Kelis aspektus apimančios nusikaltimų kontrolės ir saugių gatvių akto (angl. *Title III Omnibus Crime Control and Safe Street Act)* nuostata 1972 m. tapo teisminio ginčo objektu. 1972 m. byloje *U. S. v. U. S. District Court* (dar vadinamojoje *Keith* byloje), teismas konstatavo, kad nesankcionuotas įrodymų el. erdvėje rinkimas apie JAV piliečius, nesusijusius su užsienio subjektais (angl. *foreign power*), prieštarauja IV Konstitucijos pataisai ir valdžių pasidalijimo doktrinai[362].

1972 m. *Keith* byloje teismas iškėlė du probleminius klausimus. Pirmasis klausimas susijęs su valdžių padalijimo doktrina: ar prezidentas turi teisę vykdyti elektroninį sekimą užsienio žvalgybos tikslais be parlamento ir teisminio sankcionavimo. Antrasis – susijęs su IV JAV Konstitucijos pataisa: ar užsienio žvalgybos elektroninėje erdvėje tikslais IV JAV Konstitucijos pataisa turėtų būti taikoma kitaip nei įprastinių nusikalstamų veikų tyrimo atveju. Šie klausimai iš dalies jau buvo tapę teisminio nagrinėjimo objektu ir iki *Keith* bylos, tačiau nors teismų pozicija nebuvo vieninga, didžioji dauguma teismų pasisakė prieš užsienio žvalgybos išimtį iš IV JAV Konstitucijos pataisos reglamentavimo apimties ir tradicinės valdžių padalijimo doktrinos[363]. *Keith* byloje teismas išskyrė išorines ir vidines grėsmes nacionaliniam saugumui. Vidinių grėsmių, t. y. kontržvalgybos atveju, pasak teismo, nesankcionuotas elektroninis sekimas nukreiptas prieš JAV asmenis buvo negalimas. Ar jis negalimas ir išorinių grėsmių atveju, kuomet elektroninio sekimo objektas ne JAV asmuo, teismas nepasisakė. Debatai dėl Prezidento galių nacionalinio saugumo užtikrinimo

---

360 William C. Banks ir M. E. Bowman, „Executive Authority for National Security Surveillance“, *American University Law Review* 50, no. 1 (2001 2001): 1–130. Lois A. Chiarella ir Michael A. Newton, „So Judge, How Do I Get That FISA Warrant: The Policy and Procedure for Conducting Electronic Surveillance“, *Army Lawyer* 1997, no. 10 (1997): 25–73.

361 James Carr ir Patricia Bellia, *The Law of Electronic Surveillance, 2017-2 Ed.*, 2 dalis, (Clark Boardman Callaghan, 2017), 443.

362 „U. S. v U. S. District Court for Eastern District of Michigan, Southern Division“, *US Supreme Court*, žiūrėta 2020 m. rugsėjo 5 d., https://supreme.justia.com/cases/federal/us/407/297/.

363 „U. S. v Buck“, CaseLaw, žiūrėta 2020 m. rugsėjo 5 d., https://caselaw.findlaw.com/us-5th-circuit/1054668.html. „Zweibon v. Mitchell“, *US Supreme Court*, žiūrėta 2020 m. rugsėjo 5 d., https://law.justia.com/cases/federal/district-courts/FSupp/444/1296/2149063/.

klausimais JAV tęsėsi jau daugiau nei 50 metų[364] iki priimant sprendimą *Keith* byloje. *Keith* bylos pasekoje 1976 m. buvo priimtas FISA – teisės aktas, kuris turėjo išspręsti diskusinius valdžios padalijimo ir prezidento įgaliojimų nacionalinio saugumo srityje bei IV JAV Konstitucijos pataisos taikymo klausimus. Tačiau vėlesni jo pakeitimai 2006 m.[365], 2007 m.[366], 2008 m.[367], 2015 m.[368], 2017 m.[369] rodo, kad tikslingai ar netikslingai pirminis FISA variantas neapėmė visų prezidento įgaliojimų nacionalinio saugumo klausimais dėl žvalgybos institucijų vykdomo elektroninio sekimo. Taip pat FISA nevisiškai užtikrino ir valdžių padalijimo principo laikymąsi, kadangi teisminis žvalgybos institucijų vykdomo elektroninio sekimo sankcionavimas pagal FISA yra reikalingas ne visais atvejais, o net ir tais atvejais, kai jis reikalingas, teismo vaidmuo yra formalus[370].

1978 m. priimtos FISA nuostatos reglamentavo elektroninį sekimą JAV viduje kai 1) elektroninė ar laidinė komunikacija vyksta JAV, arba, kai 2) bent viena iš elektroninės ar laidinės komunikacijos pusių (gavėjas ar siuntėjas) yra JAV asmuo, esantis JAV. 2005 m. į viešumą iškilus tik Prezidento sankcionuotai masinei „teroristų sekimo programai"[371], paaiškėjo dar viena FISA spraga, kuria pasinaudojo vykdomoji valdžia. Šis teisės nereglamentavo duomenų elektroninėje erdvėje rinkimo, kuomet yra pakankamas pagrindas manyti, kad asmuo yra už JAV ribų (angl. *person is reasonably believed to be outside USA*). Reaguodamas į tai Kongresas 2008 m. priėmė FISA pataisą įtraukusią JAV esančių duomenų kuomet yra pakankamas pagrindas manyti, kad asmuo yra už JAV ribų, rinkimą į FISA reglamentavimo apimtį[372]. Taigi, FISA nuostatos galioja duomenų, esančių JAV rinkimui, arba kai tai susiję su JAV asmeniu, esančiu JAV (galimas duomenų rinkimas JAV teritorijoje ir už JAV teritorijos ribų) arba kai asmens duomenys yra JAV, bet pats asmuo yra pagrįstai manoma esančiu ne JAV teritorijoje.

---

364 Carr ir Bellia, *supra note,* 361: 442.

365 „Terrorist Surveillance Act of 2006", *U. S. Congress*, žiūrėta 2020 m. rugsėjo 5 d., https://www.congress.gov/bill/109th-congress/senate-bill/3931?s=1&r=9.

366 „Protect America Act of 2007", *U. S. Congress*, žiūrėta 2020 m. rugsėjo 5 d., https://www.congress.gov/110/plaws/publ55/PLAW-110publ55.pdf.

367 „Foreign Intelligence Surveillance Act of 1978 Amendments Act of 2008", *U. S. Congress*, žiūrėta 2020 m. rugsėjo 5 d., https://www.congress.gov/bill/110th-congress/house-bill/6304 .

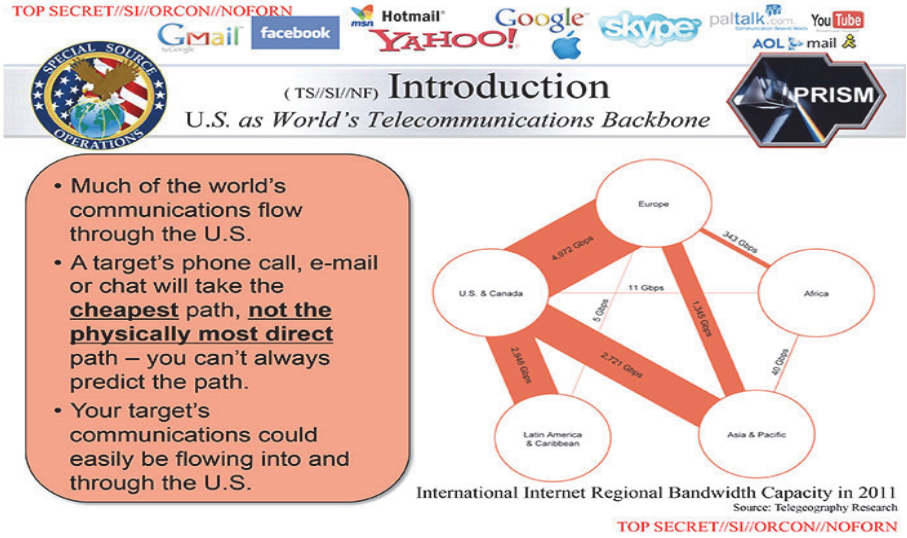
368 „2015 USA Freedom Act", *U. S. Congress*, žiūrėta 2020 m. rugsėjo 5 d., https://www.congress.gov/bill/114th-congress/house-bill/2048 .

369 „FISA Amendments Reauthorization Act of 2017", *U. S. Congress*, žiūrėta 2020 m. rugsėjo 5 d., https://www.congress.gov/bill/115th-congress/house-bill/4478.

370 Apie tai plačiau sekančiame disertacijos skyriuje.

371 Carr ir Bellia, *supra note,* 361: 447.

372 Carr ir Bellia, *supra note,* 361: 448.



2 pav. *2013 m. E. Snowden nutekinta duomenų judėjimo tarp Europos ir JAV schema, originalaus dokumento kopija*[373.]

2 paveiksle pavaizduota E. Snowden atskleista NSA vykdytos žvalgybos programos PRISM pristatymo schema rodo, kad didžioji dauguma Europos gyventojų asmens duomenų keliauja per JAV arba yra saugomi JAV esančiuose serveriuose. Tai reiškia, kad ne tik JAV, bet labai daug Europos ir viso likusio pasaulio gyventojų asmenų duomenų yra laikomi esančiais JAV, o asmenys yra už JAV ribų. Tai yra viena iš sąlygų JAV žvalgybos institucijoms rinkti duomenis vadovaujantis FISA. Tačiau ar tai, kad mūsų asmenų duomenys yra JAV, jau yra pakankamas pagrindas rinkimui ir ar tai automatiškai reiškia, kad jie yra renkami JAV žvalgybos institucijų?

Duomenų buvimo vieta yra ne vienintelis kriterijus FISA reglamentavimo apimčiai nustatyti. Vadovaujantis FISA gali būti renkami tik užsienio žvalgybos duomenys. Duomenis, kurie pagal FISA yra laikomi užsienio žvalgybos, apibrėžia duomenų subjektas ir duomenų rinkimo tikslas.

Duomenų subjektai gali būti:

1) JAV asmenys (angl. *USA person*). Bendra taisyklė yra ta, kad apie JAV asmenis paprastai negali būti renkama ir laikoma užsienio žvalgybos informacija (angl. *foreign intelligence information*) pagal FISA nebent ji tiesiogiai yra susijusi su to asmens veikla užsienio subjektui (angl. *foreign power*) arba užsienio subjekto agentui (angl. *agent of foreign power*)[374]. Tačiau, kaip pabrėžia FISA teismo ekspertė Laura K. Danohue, FISA yra tiesioginė grėsmė JAV asmenų teisių

[373] „NSA Slides Explain the PRISM Data-Collection Program", *The Washington Post*, žiūrėta 2020 m. rugsėjo 5 d., http://www.washingtonpost.com/wp-srv/special/politics/prism-collection-documents/.

[374] Carr ir Bellia, *supra note,* 361: 452.

užtikrinimui, kadangi FISA pagrindu yra surenkama labai daug informacijos apie JAV asmenis, tiesiogiai nesusijusius su užsienio subjektu (angl. *foreign power*) arba užsienio subjekto agentu (angl. *agent of foreign power*)[375]. Tai rodo, kad užtikrinti FISA nuostatų laikymąsi yra sudėtinga.

2) Ne JAV asmenys:
   a. Užsienio subjektai (angl. *foreign powers*):
      i. Oficialiai veikiantys užsienio subjektai (angl. *official foreign powers*)[376]. Apima JAV įsikūrusias tarptautiniu mastu pripažintas ir nepripažintas užsienio valdžias ar bent kokios formos jų komponentus[377]. Ši sąvoka apima, pavyzdžiui, užsienio ambasadas ir konsulatus bei bent kokią kitą užsienio atstovybės formą[378]. Po šia sąvoka patenka ir užsienio tautų grupuotės, jeigu esminė jos dalis yra sudaryta iš ne JAV asmenų. Tokios grupuotės turi būti įsisteigusios užsienyje ir kontroliuojamos iš užsienio[379]. Prie oficialios užsienio subjektų yra priskiriamos ir užsienyje įsteigtos užsienio valdžios kontroliuojamos įmonės[380] . Tokios įmonės nors ir yra privatūs subjektai į oficialios užsienio jėgos sąvokos buvo įtrauktos siekiant pabrėžti, kad ir privačios įmonės bus traktuojamos taip pat, kaip ir užsienio valdžios, kurioms jos tarnauja[381].
      ii. Neoficialiai veikiantys užsienio subjektai (angl. *unofficial foreign powers*)[382]. Ši sąvoka visų pirma apima užsienio teroristines grupes[383]. Manytina, kad nacionalinės JAV teroristinės grupės nepatenka į šią sąvoka ir duomenys apie jas turėtų būti renkami vadovaujantis ECPA[384]. Neoficialios užsienio subjektai (angl. *unofficial foreign powers*) apima ir užsienio politines organizacijas, jeigu didžioji dauguma jų narių yra ne JAV asmenys[385], taip pat politines partijas, turinčias tik sąlyginę autonomiją[386]. Prie šios sąvokos yra priskiriamos JAV įsteigtos, bet užsienio valdžios valdomos ar kontroliuojamos įmonės[387] bei įmonės, kurių didžiąją daugumą sudaro ne JAV asmenys, susijusios su masinio naikinimo ginklų proliferacija[388].

---

375 Donohue, *The Future of Foreign Intelligence*, 22.

376 50 U.S. Code § 1801(a)(1), (2) ir (3), *Legal Information Institute*, žiūrėta 2020 m. rugsėjo 5 d., https://www.law.cornell.edu/uscode/text/50/1801.

377 50 U.S. Code §1801(a)(1), *Legal Information Institute*, žiūrėta 2020 m. rugsėjo 5 d., https://www.law.cornell.edu/uscode/text/50/1801.

378 Carr ir Bellia, *supra note,* 361: 452.

379 *Ibid.*

380 *Ibid.,* 453.

381 *Ibid.*

382 50 U.S. Code §1801(a)(4), (5), (6) ir (7), *Legal Information Institute*, žiūrėta 2020 m. rugsėjo 5 d., https://www.law.cornell.edu/uscode/text/50/1801.

383 Carr ir Bellia, *supra note,* 361: 453.

384 *Ibid.*

385 *Ibid.*

386 *Ibid.*

387 *Ibid.*

388 *Ibid.*

b. Užsienio subjektų agentai (angl. *agents of foreign powers*). FISA yra įtvirtinti 10 atvejų, kuomet asmuo yra laikomas užsienio subjekto agentu, kuriuos galima sugrupuoti į dvi kategorijas priklausomai nuo to, ar jis yra JAV ar ne JAV asmuo. Ne JAV asmuo yra laikomas užsienio subjektų agentu:
   i. kai ne JAV asmuo JAV veikia kaip užsienio subjektų pareigūnas ar darbuotojas ar teroristinės organizacijos narys, nepriklausomai nuo to ar jis fiziškai yra JAV[389];
   ii. kai ne JAV asmuo veikia užsienio subjektui, vykdančiai slaptas veiklas JAV, ar yra jos įgaliotas, jei visos aplinkybės rodo, kad agentas pats yra įsitraukęs ar įtrauktas į tų slaptų veiklų vykdymą taip pat kaip ir bent kas kitas, kas veikia kartu su asmeniu, kuris yra įsitraukęs į tokias veiklas[390]. Šis apibrėžimas yra taikomas nepriklausomai nuo to ar slaptos veiklos yra laikomos nusikalstamomis pagal federalinius baudžiamosios teisės aktus[391];
   iii. kai ne JAV asmuo dalyvauja tarptautiniame terorizme ar pasirengime jį vykdyti[392]. Šis atvejis nuo pirmojo skiriasi tuo, kad asmuo neprivalo būti susijęs su teroristine grupe ir terorą aktą gali planuoti vykdyti ar vykdyti vienas. Šia nuostata FISA buvo papildyta 2008 m. siekiant kriminalizuoti ir teroristo vienišiaus (angl. *lonely wolf terrorist*) veiklą[393], tačiau, kaip teigia James G. Carr, gali būti naudojama ir tuo atveju, kai pritrūksta duomenų apie asmens ryšius su žinomomis teroristinėmis organizacijomis[394];
   iv. kai ne JAV asmenys yra įsitraukę į veiklas, susijusias su masinio naikinimo ginklais. Asmuo laikomas užsienio subjekto agentu nepriklausomai nuo to ar jis veikia kaip užsienio subjekto atstovas[395], ar vienas[396].

Antroji kategorija asmenų, kurie laikomi užsienio subjektų agentais, gali būti taikoma tiek JAV, tiek ne JAV asmenims:

   i. kai yra žinoma, kad asmenys yra įsitraukę į slaptas žvalgybos informacijos rinkimo operacijas užsienio subjekto naudai, jeigu tokios veikos turi ar gali turėti nusikalstamų veikų sudėtį pagal federalinę baudžiamąją teisę[397];

---

389 50 U.S. Code §1801(b)(1)(A), *Legal Information Institute*, žiūrėta 2020 m. rugsėjo 5 d., https://www.law.cornell.edu/uscode/text/50/1801.

390 50 U.S. Code §1801(b)(1)(B), *Legal Information Institute*, žiūrėta 2020 m. rugsėjo 5 d., https://www.law.cornell.edu/uscode/text/50/1801.

391 Carr ir Bellia, *supra note,* 361.

392 50 U.S. Code §1801(b)(1)(C), *Legal Information Institute*, žiūrėta 2020 m. rugsėjo 5 d., https://www.law.cornell.edu/uscode/text/50/1801.

393 Carr ir Bellia, *supra note,* 361: 454.

394 *Ibid.*

395 50 U.S. Code §1801(b)(1)(D), *Legal Information Institute*, žiūrėta 2020 m. rugsėjo 5 d., https://www.law.cornell.edu/uscode/text/50/1801.

396 50 U.S. Code §1801(b)(1)(E), *Legal Information Institute*, žiūrėta 2020 m. rugsėjo 5 d., https://www.law.cornell.edu/uscode/text/50/1801.

397 50 U.S. Code §1801(b)(2)(A), *Legal Information Institute*, žiūrėta 2020 m. rugsėjo 5 d., https://www.law.cornell.edu/uscode/text/50/1801.

ii. kai asmuo yra įtraukęs į bent kurią kitą slaptos žvalgybos veiklą pagal žvalgybos institucijos ar užsienio subjekto poreikį, jeigu tokios veikos turi ar gali turėti nusikalstamų veikų sudėtį pagal federalinę baudžiamąją teisę[398];
iii. kai yra žinoma, kad asmuo užsienio subjekto naudai dalyvauja ar gali dalyvauti sabotaže ar tarptautiniame terorizme ar pasirengime vykdyti sabotažą ar tarptautinį terorizmą[399];
iv. kai asmuo prisidengdamas netikra tapatybe apsigyvena JAV ir veikia užsienio subjekto naudai[400]. Ši nuostata į FISA buvo įtraukta 1999 m. siekiant apsaugoti JAV nuo neteisėto šnipinėjimo, vykdomo kito asmens tapatybe prisidengusio asmens, kuris prieš pradėdamas savo neteisėtą veiklą gali daug metų gyventi JAV[401];
v. kai asmuo bent kokiu būdu padeda aukščiau išvardintiems asmenims, laikomiems užsienio subjektų agentais[402].

Tačiau vėlgi JAV žvalgybos institucijos duomenis elektroninėje erdvėje gali rinkti apie užsienio subjektus ar užsienio subjektų agentus tik FISA įtvirtintiems tikslams pasiekti. FISA yra įtvirtinti nacionalinio saugumo tikslai dėl kurių gali būti renkami asmens duomenys gali būti grupuojami į tikslus, skirtus:

1) apginti JAV:
   a) nuo realios ar potencialios atakos;
   b) nuo sabotažo, tarptautinio terorizmo ar tarptautinio masinės destrukcijos ginklo naudojimo;
   c) slaptos žvalgybos veiklos. Žvalgybos informacijos turinys sudaro klasikinę kontržvalgybos informaciją, tačiau negali apimti informacijos apie politinę veiklą JAV[403].
2) rinkti bent kokią informaciją apie užsienio subjektą (angl. *foreign power*) arba užsienio subjekto agentą (angl. *agent of foreign power*), reikalingą JAV:
   a) saugumo ar nacionalinės gynybos užtikrinimui;
   b) vykdyti JAV užsienio politiką[404].

Taigi, JAV žvalgybos institucijos duomenis elektroninėje erdvėje turi teisę rinkti tik apie asmenis, patenkančius į užsienio subjekto arba užsienio subjekto agento apibrėžimą ir tik FISA konkrečiai apibrėžtiems nacionalinio saugumo tikslams. Tiesioginės FISA akto formuluotės, yra labai archajiškos ir sudaro įspūdį, kad liečia labai siaurą

---

398 50 U.S. Code §1801(b)(2)(B), *Legal Information Institute*, žiūrėta 2020 m. rugsėjo 5 d., https://www.law.cornell.edu/uscode/text/50/1801.

399 50 U.S. Code §1801(b)(2)(C), *Legal Information Institute*, žiūrėta 2020 m. rugsėjo 5 d., https://www.law.cornell.edu/uscode/text/50/1801.

400 50 U.S. Code §1801(b)(2)(D), *Legal Information Institute*, žiūrėta 2020 m. rugsėjo 5 d., https://www.law.cornell.edu/uscode/text/50/1801.

401 Carr ir Bellia, *supra note,* 361: 454.

402 50 U.S. Code §1801(b)(2)(E), *Legal Information Institute*, žiūrėta 2020 m. rugsėjo 5 d., https://www.law.cornell.edu/uscode/text/50/1801.

403 Carr ir Bellia, *supra note,* 361: 451-452.

404 *Ibid.*

duomenų subjektų ratą. Tačiau praktinė JAV žvalgybos institucijų veikla, remiantis viešai skelbiamais duomenimis, rodo, kad FISA apima platų asmenų ratą. Pavyzdžiui, Microsoft korporacija paskelbė, kad per pirmąjį 2016 m. pusmetį gavo daugiau nei 1000 žvalgybos paklausimų pagal FISA, palietusių apie 17 999 Microsoft klientų paskyras, kas yra net dvigubai daugiau nei 2015 m.[405]. 2017 m. Shadow Brokers nutekinta informacija rodo, jog CŽV duomenis vadovaujantis FISA el. erdvėje rinko apie užsienio civilinę infrastruktūrą, nepatenkančią nei į užsienio subjekto, nei į užsienio subjekto agento sąvoką: bankus, universitetus ir kt.[406]. Kaip tai galėjo nutikti ir ar niekas nekontroliuoja žvalgybos institucijų veiklos pagal FISA?

FISA bylas iki 1978 m. nagrinėjo bendrosios kompetencijos teismai[407]. 1978 m. FISA akto priėmimu bendrosios kompetencijos teismų jurisdikcija tokių bylų nagrinėjimui buvo panaikinta. Bendrosios kompetencijos teismų kompetencijos panaikinimas buvo argumentuojamas tuo, kad bendrosios kompetencijos teismų ėmimasis vertinti žvalgybos institucijų veiklos teisėtumą trukdė šių institucijų veiklai, kadangi jų veiklos principai ir veiklos reglamentavimas iš esmės skyrėsi nuo teisėsaugos institucijų, o teismai žvalgybos institucijų veiklą vertino panašiai kaip teisėsaugos institucijų. Siekiant užtikrinti valdžių pasidalijimo principą, FISA aktu taip pat buvo įkurti du specialūs teismai: Užsienio žvalgybos el. erdvėje teismas (angl. *Foreign intelligence surveillance court (FISA court)*) (toliau – FISA teismas)[408] bei apeliacinės instancijos teismas – Užsienio žvalgybos el. erdvėje apeliacinis teismas (angl. *Foreign intelligence surveillance court of review (FISA court of review)*) (toliau – FISA apeliacinis teismas), turėję užtikrinti JAV žvalgybos institucijų veiklos teisėtumą. FISA apeliacinis teismas yra vienas iš mažiausiai bylų pasaulyje turintis teismas. Nors jis ir yra įtvirtintas, tačiau apeliacijos yra teikiamos ypatingai retai – pirmoji apeliacija FISA apeliaciniame teisme buvo pateikta 2002 m., t. y. po 24 metų nuo teismo įsteigimo[409]. Viena iš priežasčių kodėl taip yra – nes asmenys nežino, kad jų elektroniniai asmenys duomenys yra renkami žvalgybos tikslais. FISA apeliacinis teismas nėra galutinės instancijos teismas. Apeliacijos dėl FISA peržiūros teismo sprendimų yra teikiamos JAV Aukščiausiajam teismui[410]. Tokiu būdu FISA akte buvo įtvirtintas kompromisas: žvalgybos institucijos gali vykdyti savo veiklą ir rinkti asmens duomenimis, tačiau jų veiklos teisėtumą turi prižiūrėti ir užtikrinti specialus teismas.

FISA oficialiai pakeitė ir iki 1978 m. žvalgybos institucijų veiklą įtvirtindama privalomą asmens duomenų rinkimo sankcionavimą, vykdomą FISA teismo užsienio

---

405 Dustin Volz, „Microsoft Says No Increase in U.S. Foreign Intelligence Surveillance Requests“, *Reuters*, 2017, žiūrėta 2020 m. rugsėjo 5 d., https://www.reuters.com/article/us-microsoft-surveillance-idUSKBN17F2G7.

406 „Share CSV Files Online – ShareCSV“, žiūrėta 2020 m. rugsėjo 5 d., http://www.sharecsv.com/s/9bc26c690cafb8774138caf8f0d8ea33/sanitized_ips.csv%20https://twitter.com/Snowden/status/851121195147767808.

407 Kris., *supra note,* 12.

408 „Report to Accompany S. 1566, the Foreign Intelligence Surveillance Act of 1978 (March 14, 1978)“, *US Senate*, žiūrėta 2020 m. rugsėjo 5 d., https://www.intelligence.senate.gov/sites/default/files/publications/95701.pdf.

409 „Justice Dept Appeal to the U.S. Foreign Intelligence Surveillance Court of Review“, accessed August 13, 2020, https://fas.org/irp/agency/doj/fisa/082102appeal.html.

410 Carr ir Bellia, *supra note,* 361.

žvalgybos telefoninių pokalbių klausymosi orderio (angl. *Foreign Intelligence wiretap order*) pagrindu. Reikalavimai užsienio žvalgybos telefoninių pokalbių klausymosi orderio (angl. *Foreign Intelligence wiretap order*) išdavimui yra panašūs į telefoninių pokalbių klausymo orderio (angl. *wiretap order*). Esminis skirtumas yra tas, kad tikėtino priežastingumo (angl. *probable cause*) reikalavimas yra suvokiamas kitaip nei Telefoninių pokalbių klausymosi akte (angl. *Wiretap act*). Vadovaujantis FISA yra laikoma, kad tikėtinas priežastingumas (angl. *probable cause*) egzistuoja, jeigu slapto sekimo elektroninėje erdvėje subjektas yra „užsienio subjektas" (angl. *foreign power*)[411] arba „užsienio subjekto agentas" (angl. *agent of foreign power*)"[412], kai tuo tarpu tradiciniu atveju tikėtinu priežastingumu (angl. *probable cause)* yra laikoma pakankamas pagrindas manyti, kad yra vykdoma ar gali būti vykdoma konkreti nusikalstama veika[413]. Tokia FISA nuostata atveria kelią asmens duomenų rinkimui el. erdvėje jo nesiejant su baudžiamajai teisei priešinga nusikalstama veika[414]. Nors vadovaujantis FISA užsienio-subjektas (angl. *foreign power*) gali būti tiek viešas, tiek privatus, tiek viešas-privatus sektorius, tačiau iš šių subjektų tik teroristinė organizacija pati iš savęs visais atvejais reiškia nusikalstamą veiką. Pažymėtina ir tai, kad FISA leidžia rinkti informaciją ne tik tiesiogiai apie užsienio subjektus ir užsienio subjektų agentus, bet su jais susijusius asmenis[415]. Ką tai reiškia?

Pavyzdžiui, teroristinės grupės narys A, kurio sekimui el. erdvėje FISA teismas išdavė orderį, gavo el. laišką iš savo kaimyno B, nesančio teroristinės organizacijos nariu ir nieko nežinančio apie kaimyno veiklą teroristinėje grupėje. Nepaisant to, kaimynas B tampa JAV žvalgybos objektu ir nuo to momento duomenys el. erdvėje yra renkami ne tik apie teroristinės grupės narį A, bet ir apie kaimyną B bei apie visus kitus jam rašančius asmenis ir t. t. Jeigu kaimynui B parašo dar du asmenys C ir D tai ir asmenys C ir D bei visi kam C ir D rašo arba kas parašo C ir D, tampa JAV žvalgybos objektu pagal FISA. Todėl Microsoft Corporation pateiktoje ataskaitoje yra nurodoma, kad pagal 1000 FISA orderių buvo renkama informacija apytiksliai apie 18 000 asmenų[416]. Iki kurios susijusių asmenų eilės JAV žvalgyba pagal FISA yra teisėta, oficialiai atsakymo nėra pateikto[417]. Vadinasi FISA sudaro galimybes praktiškai bent kurio asmens elektroniniams duomenims tapti žvalgybos institucijų objektu. Žmogaus teisių gynimo aktyvistai ir mokslininkai šį tiesiogiai nacionaliniam saugumui pavojaus nekeliančių asmenų elektroninį sekimą laiko žmogaus teisių ir demokratinės visuomenės principų pažeidimu[418].

---

411 50 U.S.C. § 1804(a)(3), 50 U.S.C. § 1823(a)(3), United States v. Bin Laden.

412 Carr ir Bellia, *supra note,* 361: 464.

413 Carr ir Bellia, *supra note,* 21.

414 Tik keli FISA atvejai sieja su nusikalstama veika – terorizmu.

415 Carr ir Bellia, *supra note,* 361: 483.

416 Volz., *supra note*, 405.

417 Donohue, *supra note*, 8: 74.

418 Elizabeth Goitein, „The NSA's Backdoor Search Loophole", *Boston Review*, 2013, žiūrėta 2020 m. rugsėjo 5 d., https://bostonreview.net/blog/elizabeth-goitein-nsa-backdoor-search-loophole-freedom-act. Donohue, *supra note*, 12: 631.

Asmens teisių užtikrinimo saugikliu turėtų būti specialūs FISA teismai, tačiau iki 2001 m. USA PATRIOT akto priėmimo šie teismai net neturėjo įgaliojimų interpretuoti ir aiškinti FISA nuostatų bei kvestionuoti žvalgybos institucijų veiklos teisėtumo[419]. Jie tiesiog tik veikė. Vienintelis jų įgaliojimas išduodant orderius buvo nustatyti, kad jis išduodamas prieš „užsienio subjektą" (angl. *foreign power*) arba „užsienio subjekto agentą" (angl. *agent of foreign power*)", o išdavus – patikrinti faktų, pateiktų dėl individualių orderių išdavimo, pagrįstumą[420]. Ir nors 2001 m. USA PATRIOT aktas suteikė specialiesiems teismams kompetenciją vertinti ir interpretuoti ir teisinį orderių išdavimo ir duomenų rinkimo el. erdvėje pagrindą, visgi šios bylos yra uždaros ir svarstomos duomenų subjektui nedalyvaujant[421] bei dažniausiai net nepaskelbiant viešosios nuomonės[422]. Todėl šie teismai yra vadinami „slaptaisiais teismais"[423]. Taip pat FISA teismai nevertina ar elektronine žvalgyba nėra pažeidžiamos asmens teisės, ypač ne JAV asmenų teisės. Iš tikrųjų FISA teismai net neturi nei jurisdikcijos, nei teisinio pagrindo vertinti kitų valstybių jų piliečių atžvilgiu galiojančių nacionalinių ir supranacionalinių teisės aktų, kurie jiems suteikia teisę į asmens duomenų apsaugą. Todėl manyti, kad FISA teismų atsiradimo tikslas buvo visų asmenų teisių apsauga, yra klaidinga. FISA teismai – tai būdas įrodyti, jog formaliai laikomasi valdžių padalijimo doktrinos. Kadangi šie teismai veikia tik formaliai, todėl iki šiol yra abejojama specialiųjų FISA teismų nešališkumu[424]. 2 lentelėje pateikti oficialiai skelbiami duomenys apie JAV žvalgybos institucijų prašymų sankcionavimą rodo, kad arba FISA teismai paklūsta žvalgybos institucijoms, nes jie neturi teisinių galių ir faktinės kompetencijos atmesti žvalgybos institucijų prašymų.

Kaip matome 2 lentelėje, tik 5 iš 1010 žvalgybos institucijų prašymų buvo atmesti 2015 m. Tai įrodo, kad FISA teismo vaidmuo yra tik simbolinis. Praktiškai jis neužtikrina žvalgybos institucijų veiklos teisėtumo, nes net neturi teisinių galių tą padaryti. Tačiau net ir tuo atveju, kai asmens duomenys el. erdvėje renkami vadovaujantis FISA, kad ir simbolinis, bet teismo leidimas ne visuomet yra reikalingas. Todėl iš pirmo žvilgsnio atrodantis toks mažas teismo leidimų išdavimų skaičius nereiškia, kad tik tais keliais atvejais asmens duomenys ir buvo renkami. FISA yra įtvirtinti keli atvejai, kai teismo sankcionavimas duomenų rinkimui el. erdvėje yra nereikalingas.

---

419 Viet D. Dinh ir Wendy J. Keefer, „FISA and the Patriot Act: A Look Back and a Look Forward Note", *Annual Review of Criminal Procedure* 35 (2006): iii–xxxiv.

420 Dinh ir Keefer, *supra note,* 419:8.

421 50 U.S.C. §1861(c), 1861(d), *Legal Information Institute*, žiūrėta 2020 m. rugsėjo 6 d., https://www.law.cornell.edu/uscode/text/50/1861.

422 Jameel Jaffer, „Secret Evidence in the Investigative State: FISA, Administrative Subpoenas, and Privacy Symposium: Secret Evidence and the Courts in the Age of National Security: Panel Report", *Cardozo Public Law, Policy, and Ethics Journal* 5, no. 1 (2007 2006): 7–26.

423 Lietuvoje asmenys taip pat negali susipažinti su žvalgybos institucijų teismui pateikta medžiaga apie juos. Todėl taip pat gali būti keliamas klausimas dėl atitikimo demokratinės valstybės principams.

424 Jaffer, *op. cit.,* 422: 8. Gerald H. Robinson, „We're Listening – Electronic Eavesdropping, Fisa, and the Secret Court", *Willamette Law Review* 36, no. 1 (2000): 51–82.

2 lentelė. *„Žvalgybos institucijų prašymai FISA teismui dėl sankcionavimo iki 2015* [425]*“.*

Straipsnis	Prašymų skaičius	Išduoti orderiai skaičius	Patikslinti orderiai	Atmesti prašymai
1805	80	57	23	0
1824	23	17	6	0
1805	754	623	126	5
1842	40	33	7	0
1861	68	61	7	0
1881a		0		0
1881b	0	0	0	0
1881c	45	45	0	0

Pirmas atvejis, kuomet teismo sankcionavimas nereikalingas esant Prezidento nurodymui. Tokiu atveju Generalinio prokuroro patvirtinimu, žvalgybos institucijos gali rinkti asmens duomenimis iki vienerių metų:

1) apie išimtinai tik užsienio subjektų komunikaciją bent kokiu pavidalu;
2) techninę informaciją, išskyrus žodinę komunikaciją, iš užsienio subjektų teritorijos[426].

Abejais atvejais duomenų rinkimas el. erdvėje yra galimas tik apie užsienio subjektą. Tačiau užsienio subjektas gali būti tiek oficialiai veikiantis, tiek neoficialiai, tiek privatus, tiek viešas asmuo, ir net formalaus teisminio sankcionavimo nebuvimas bei neseniai atskleista WikiLeaks informacija apie žvalgybos el. erdvėje objektus[427], rodo, kad šios dvi FISA išimtys yra labiau galimybė žvalgybos institucijoms laisvai veikti elektroninėje erdvėje ir stebėti kitas valstybes nei JAV nacionalinio saugumo apsaugos priemonė. Demokratija irgi yra nacionalinio saugumo dalis, o nedemokratiškų bruožų turinti žvalgybos institucijų veikla net ir siekiant nacionalinio saugumo užtikrinimo pati savaime gali tapti jam grėsme. Teismo nesankcionuotas NSA vykdomas masinis asmens duomenų rinkimas el. erdvėje pirmą kartą buvo iškilęs į viešumą 2005 m. dienraščiui *New York Times* išspausdinus straipsnį apie prezidento Bušo iniciatyva vykdomą slaptą asmenų sekimą. JAV telekomunikacijų bendrovės pateikė 40 skundų dėl masinio asmens duomenų rinkimo, tačiau jie visi buvo atmesti, o masinis duomenų rinkimas buvo nurodytas atitinkantis FISA nuostatas[428]. Atmetimo priežastimis galėjo būti tai, kad FISA teismai neturi kompetencijos vertinti žvalgybos institucijų prašymo sankcionuoti jų veiksmus el. erdvėje atitikimo teisei į asmens duomenų apsaugą, juolab ne JAV

[425] „Report of the Director of the Administrative Office of the U.S. Courts on activities of the Foreign Intelligence Surveillance Courts for 2015“, žiūrėta 2020 m. rugsėjo 6 d., http://www.uscourts.gov/sites/default/files/fisc_annual_report_2015.pdf.

[426] 50 U.S.C. § 1802(a)(1)(A), *Legal Information Institute*, žiūrėta 2020 m. rugsėjo 6 d., https://www.law.cornell.edu/uscode/text/50/1802

[427] „WikiLeaks – Intelligence“, žiūrėta 2020 m. rugsėjo 6 d., https://wikileaks.org/+-Intelligence-+.html.

[428] Eric Lichtblau, „Deal Reached in Congress to Rewrite Rules on Wiretapping – The New York Times“, žiūrėta 2020 m. rugsėjo 6 d., https://www.nytimes.com/2008/06/20/washington/20fisacnd.html.

asmenų atžvilgiu. Todėl kad iš tikrųjų asmens teisės būtų užtikrintos ne vien tik paslaugų teikėjai turi turėti pareigą ginti savo klientų teisę į asmens duomenų apsaugą, bet ir teisminės institucijos turi turėti kompetenciją vertinti ar ši teisė nėra pažeidžiama.

FISA 1805(e) yra įtvirtintas antras atvejis, kuomet duomenų rinkimui el. erdvėje teismo sankcionavimas nėra reikalingas – tai skubusis duomenų rinkimas el. erdvėje (angl. *emergency surveillance)*[429]. Esant skubiojo duomenų rinkimo el. erdvėje atvejui Generalinis prokuroras gali pats jį sankcionuoti, jeigu: 1) duomenis el. erdvėje reikia surinkti skubiau nei įmanoma gauti teismo sankcionavimą ir 2) jeigu egzistuoja visos aplinkybės teismo sankcionavimui gauti[430]. Tačiau šiuo atveju Generalinis prokuroras privalo informuoti FISA teismą apie tai, kad duomenis rinko FISA1805 (e) pagrindu ir per 7 dienas nuo tokio duomenų rinkimo pateikti teismui prašymą jį sankcionuoti[431].

Trečias atvejis, kuomet teismo sankcionavimas yra nereikalingas, kai yra tęsiamas duomenų el. erdvėje rinkimas apie ne JAV asmenį, kuris prieš tai, pagrįstai tikėtina, buvo ne JAV teritorijoje. Vadovaujantis FISA1805(f) žvalgybos institucijos vadovo sprendimu apie tai pranešus generaliniam prokurorui, 72 valandas yra leidžiama rinkti duomenis apie ne JAV asmenį, jeigu yra manoma, yra už JAV teritorijos ribų, jeigu yra tikėtina, kad egzistuoja grėsmė bent kurio žmogaus gyvybei ar yra sunkaus kūno sužalojimo tikimybė[432]. Per 72 valandų laikotarpį žvalgybos pareigūnai privalo kreiptis į teismą dėl tokios žvalgybos sankcionavimo arba perkvalifikuoti savo veiksmus į skubųjį duomenų rinkimo el. erdvėje atvejį pagal FISA 4805(e)[433].

Ketvirtas FISA įtvirtintas atvejis, kuomet teismo sankcionavimas yra nereikalingas – tai atsitiktinis duomenų rinkimas el. erdvėje[434]. FISA leidžia nesankcionuotai 90 dienų rinkti duomenis el. erdvėje kuomet žvalgybos institucijos išbando naują duomenų rinkimo el. erdvėje prietaisą, įrenginį ar mechanizmą[435]. Ilgesniam nei 90 dienų išbandymo periodui yra reikalingas Generalinio prokuroro leidimas[436]. Išbandymo metu surinkti asmens duomenys negali būti naudojami ir privalo būti sunaikinti po testavimo. Taip pat nesankcionuotai yra leidžiama duomenis rinkti, kuomet žvalgybos institucijų personalas yra apmokomas naudotis nauju duomenų rinkimo el. erdvėje įrankiu[437] arba yra testuojami jau naudojami duomenų rinkimo įrankiai[438]. Tačiau

---

429 Carr ir Bellia, *supra note,* 361: 459.

430 50 U.S.C. § 1805(g)(3), *Legal Information Institute*, žiūrėta 2020 m. rugsėjo 6 d., https://www.law.cornell.edu/uscode/text/50/1805.

431 50 U.S.C. § 1805(e)(1)(C), *Legal Information Institute*, žiūrėta 2020 m. rugsėjo 6 d., https://www.law.cornell.edu/uscode/text/50/1805.

432 50 U.S.C. § 1805 (f), *Legal Information Institute*, žiūrėta 2020 m. rugsėjo 6 d., https://www.law.cornell.edu/uscode/text/50/1805.

433 Carr ir Bellia, *supra note,* 361: 460.

434 *Ibid.*

435 50 U.S.C. § 1805(g), *Legal Information Institute*, žiūrėta 2020 m. rugsėjo 6 d., https://www.law.cornell.edu/uscode/text/50/1805.

436 Carr ir Bellia, *supra note,* 361: 460.

437 50 U.S.C. § 1805 (g)(3), *Legal Information Institute*, žiūrėta 2020 m. rugsėjo 6 d., https://www.law.cornell.edu/uscode/text/50/1805.

438 50 U.S.C. § 1805 (g)(2), *Legal Information Institute*, žiūrėta 2020 m. rugsėjo 6 d., https://www.law.cornell.edu/uscode/text/50/1805.

teisės akte nėra numatyta, kad kas nors tikrintų ar tikrai tie duomenys buvo sunaikinti ar, kad nebuvo naudojami.

Pažymėtina ir tai, kad FISA nereglamentuoja visos žvalgybos institucijų veiklos elektroninėje erdvėje[439]. Tam tikri žvalgybos institucijų metodai nepatenka į FISA įtvirtintą „elektroninės žvalgybos" sąvoką. Pavyzdžiui, FISA orderis yra nereikalingas renkant duomenis el. erdvėje, kai asmens tikėjimasis privatumo yra nepagrįstas vadovaujantis Trečiojo asmens doktrina[440] – tai reiškia, kai meta duomenys yra renkami tiesiogiai iš elektroninių paslaugų teikėjų FISA teismo sankcionavimas kratos orderio (angl. *search warrant*) pagrindu yra nereikalingas, tačiau yra reikalingas sankcionavimas teismo šaukimo (angl. *subpoena*) pagrindu. FISA nereglamentuoja ir duomenų, esančių ne JAV teritorijoje, rinkimo elektroninėje erdvėje[441]. Tik simbolinis FISA teismų vaidmuo bei FISA išimtys, kuomet net ir simbolinio teismo sankcionavimo žvalgybos institucijoms nereikia, duomenų rinkimas prezidento įgaliojimu, liudija FISA esant tik sąlygine ir labiau teorine asmens duomenų apsaugos priemone. Kadangi FISA numato tik vienintelį atvejį, kada asmeniui yra pranešama, kad jo duomenys buvo rinkti ar yra renkami – pareiškus įtarimą apie nusikalstamą veiką[442], o nusikalstamų veikų tyrimas nėra asmens duomenų rinkimo pagal FISA tikslas – reiškia, kad visais kitais atvejais asmenys niekada nesužino, jog jų duomenis el. erdvėje rinko JAV žvalgybos institucijos, todėl netenka teisės kvestionuoti JAV žvalgybos veiksmų teisėtumo, kuri yra sudėtinė teisės į asmens duomenų apsaugą dalimi.

2.3.2. Teismo sankcionuoto asmens duomenų rinkimo elektroninėje erdvėje metodai ir apimtys

FISA yra skirstoma į tradicinę ir modernią. Tradicinę FISA galima laikyti Telefoninių pokalbių klausymosi akto (angl. *Wiretap act*) analogu, skirtu užtikrinti balansą tarp piliečių teisių ir valstybės duomenų rinkimo el. erdvėje poreikių[443]. Visgi skirtingas šio teisės akto tikslas lėmė ir tam tikrus ypatumus lyginant su Telefoninių pokalbių klausymosi aktu (angl. *Wiretap act*) užtikrinant balansą tarp asmens teisių apsaugos ir valstybės interesų nacionalinio saugumo srityje. Tradicinė FISA buvo skirta būsimos komunikacijos el. erdvėje turinio rinkimo reglamentavimui FISA telefoninių pokalbių klausymo orderio (angl. *FISA wiretap order*) pagrindu. Modernioji FISA reglamentuoja ne tik būsimos komunikacijos turinio rinkimą, bet ir kitas, iš dalies ECPA analogiškas asmens duomenų rinkimo el. erdvėje slapto sekimo ir asmens duomenų rinkimo el. erdvėje rūšis:

---

439 Carr ir Bellia, *supra note,* 361: 456.

440 *Ibid*., 457.

441 *Ibid.*

442 50 U.S.C. § 1806(b), (c) ir (d), *Legal Information Institute*, žiūrėta 2020 m. rugsėjo 6 d., https://www.law.cornell.edu/uscode/text/50/1806.

443 Carr ir Bellia, *supra note,* 385: 461.

1) telefoninių pokalbių klausymasis (angl. *wiretap*)[444];
2) fizinės kratos[445];
3) įeinančios ir išeinančios komunikacijos stebėjimas [446];
4) veiklos įrašų rinkimas (angl. *business records*)[447];
5) mišri elektroninė žvalgyba (angl. *combined electronic surveillance*), apimanti tiek istorinių, tiek būsimų asmens duomenų rinkimą elektroninėje erdvėje. Mišri elektroninė žvalgyba atliekama JAV arba užsienyje, tačiau tik fiziškai užsienyje esančių ne JAV asmenų atžvilgiu, t. y. tuo atveju, kai užsienyje esančio asmens duomenys yra siunčiami į JAV esantį serverį arba į bent kurioje kitoje valstybėje esantį serverį, bet per JAV teritoriją. Ji nėra sankcionuojama teismo arba FISA teismo išduoto bendrojo orderio (angl. *combined order*) pagrindu, jeigu užsienyje esančio JAV piliečio asmens duomenys renkami JAV arba užsienyje[448].

Antroji, trečioji, ketvirtoji ir penktoji asmens duomenų rinkimo el. erdvėje rūšis sudaro moderniąją FISA, atveriančią kelią masiniam nediferencijuotam asmens duomenų rinkimui el. erdvėje (angl. *mass surveillance*). Nors ir pirminė FISA reglamentavimo apimtis yra JAV teritorijoje esančių asmens duomenų rinkimas, paskutinė FISA pataisa žvalgybos institucijoms suteikia teisę duomenis rinkti ir už JAV teritorijos ribų, jeigu renkami duomenys ne apie JAV asmenį, kai tie asmens duomenys ir ne JAV asmuo yra užsienio valstybėje.

FISA įeinančios ir išeinančios komunikacijos registravimo orderiai (angl. *FISA pen trap orders*).1998 m. FISA buvo papildyta įeinančios ir išeinančios komunikacijos registravimo orderiai (angl. *FISA pen trap orders*)[449], kurių pagrindu žvalgybos institucijos įgijo teisę rinkti būsimos komunikacijos el. erdvėje metaduomenis[450]. FISA įeinančios ir išeinančios komunikacijos registravimo orderiai (angl. *FISA pen trap orders*) veikimo principas yra labai panašus į įprastų įeinančios ir išeinančios komunikacijos registravimo orderių (angl. *pen trap orders*), išduodamų pagal Įeinančios ir išeinančios komunikacijos registravimo aktą (angl. *Pen Registers and Trap and Trace Devices Act*): žvalgybos institucijos pareigūnai pateikia FISA teismui sertifikavimą ir siūlomą orderį (angl. *certification and proposed order*), FISA teismas įvertina pateiktos informacijos atitikimą FISA įeinančios ir išeinančios komunikacijos

---

444 47 U.S.C. § 1801-12, *Legal Information Institute*, žiūrėta 2020 m. rugsėjo 6 d., https://www.law.cornell.edu/uscode/text/50/1801.

445 47 U.S.C. § 1821-29, *Legal Information Institute*, žiūrėta 2020 m. rugsėjo 6 d., https://www.law.cornell.edu/uscode/text/12/1821

446 47 U.S.C. § 1841-46, *Legal Information Institute*, žiūrėta 2020 m. rugsėjo 6 d., https://www.law.cornell.edu/uscode/text/47/227.

447 47 U.S.C. § 1861-62, *Legal Information Institute*, žiūrėta 2020 m. rugsėjo 6 d., https://www.law.cornell.edu/uscode/text/28/1861.

448 47 U.S.C. § 1881-81(g), *Legal Information Institute*, žiūrėta 2020 m. rugsėjo 6 d., https://www.law.cornell.edu/uscode/text/50/1881.

449 „Section 214 of USA PATRIOT ACT“, *US Congress*, žiūrėta 2020 m. rugsėjo 6 d., https://www.congress.gov/109/plaws/publ177/PLAW-109publ177.htm.

450 *Ibid.*

registravimo orderio (angl. *FISA pen trap order*) reikalavimams[451]. Nustatęs, kad pateikta informacija yra pakankama FISA įeinančios ir išeinančios komunikacijos registravimo orderio (angl. *FISA pen trap order*) išdavimui, FISA teismas jį išduoda[452]. Gavęs FISA įeinančios ir išeinančios komunikacijos registravimo orderį (angl. *FISA pen trap order*) žvalgybos institucijos pareigūnas jį pateikia el. ryšių tinklų arba el. paslaugų teikėjui, kad šis suteiktų FISA įeinančios ir išeinančios komunikacijos registravimo orderyje (angl. *FISA pen trap order*) nurodytus metaduomenis, sudarančius numerio rinkimo, maršruto el. erdvėje, adresato ir signalo informaciją (angl. *dialing, routing, addressing and signaling*) apie būsimą komunikaciją el. erdvėje[453]. Tačiau tarp FISA ir ECPA įeinančios ir išeinančios komunikacijos registravimo orderių (angl. *pen trap order*) yra ir esminių skirtumų. ECPA įeinančios ir išeinančios komunikacijos registravimo orderio (angl. *pen trap order*) pagrindu yra renkama informacija, aktuali teisėsaugai tiriant ir užkardant įprastas nusikalstamas veikas[454]. FISA įeinančios ir išeinančios komunikacijos registravimo orderio (angl. *FISA pen trap order*) pagrindu gali būti renkama informacija, reikalinga nacionalinio saugumo tikslais, kovai su terorizmu arba kontržvalgybos tikslais[455]. Pagal ECPA el. erdvėje surinktų įrodymų užginčijimas (angl. *suppression*) yra negalimas. FISA el. erdvėje surinktų įrodymų užginčijimo galimybė yra įtvirtinta. Asmuo gali prašyti pripažinti įrodymus nepagrįstais, jeigu asmens duomenys vadovaujantis FISA buvo surinkti nesilaikant FISA nustatytų reikalavimų[456].

3 paveiksle pavaizduoti statistiniai duomenys apie įeinančios ir išeinančios komunikacijos registravimo orderių (angl. *FISA pen trap order*) išdavimą rodo šio teismo orderio sankcionavimo mažėjimo tendenciją[457]. Nors duomenys yra ribotos apimties ir tik dalinai atspindi tikrąją situaciją apie įeinančios ir išeinančios komunikacijos registravimo orderių (angl. *FISA pen trap order*) išdavimą, tačiau jais vadovaujantis galima padaryti tam tikrų įžvalgų, kurios yra panašios situaciją su ECPA įeinančios ir išeinančios komunikacijos registravimo orderiais (angl. *pen trap order*).

FISA įeinančios ir išeinančios komunikacijos registravimo orderio (angl. *FISA pen trap order*) išdavimas ženkliai padidėjo po rugsėjo 11 d. teroro aktų JAV, o sumažėjo 2007 m. įsigaliojus Amerikos apsaugos aktui (angl. *Protect America Act*) ir 2008 įsigaliojus FISA pataisų aktui (angl. *FISA Amendment Act*), kuriuose įtvirtinti naujo tipo asmens duomenų rinkimo el. erdvėje mechanizmai – veiklos įrašų rinkimo orderiai (angl. *business records order*) ir 702 straipsnio orderiai (angl. *702 order*) – numatantys

---

451 Carr ir Bellia, *supra note,* 361: 461.

452 *Ibid.*

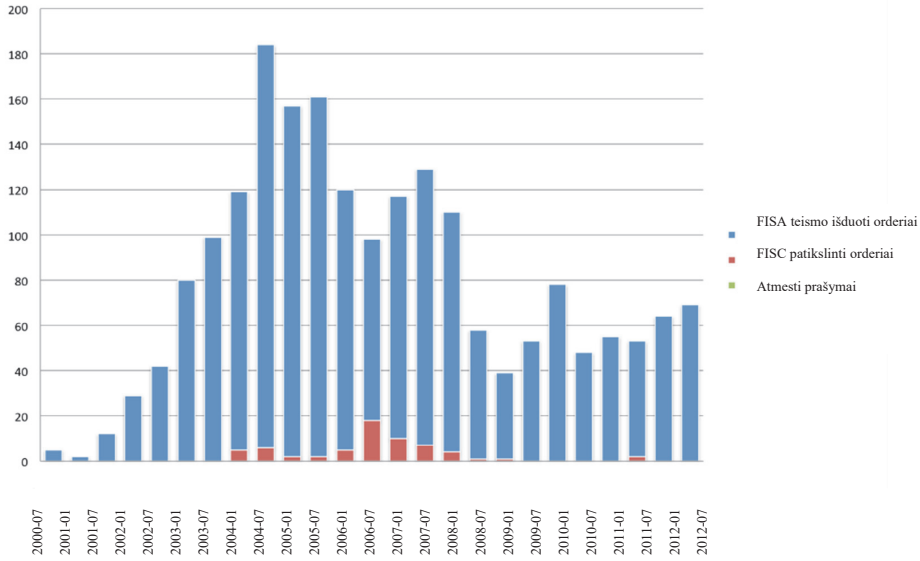
453 Carr ir Bellia, *supra note,* 361: 497.

454 *Ibid.*

455 *Ibid.*

456 Nick Harper, „FISA's Fuzzy Line between Domestic and International Terrorism Comment", *University of Chicago Law Review* 81, no. 3 (2014): 1123–64.

457 Office of the Inspector General, „A Review of the FBI's Use of Pen Register and Trap and Trace Devices Under the Foreign Intelligence Surveillance Act in 2007 through 2009 – Executive Summary", 7, žiūrėta 2020 m. rugsėjo 6 d., https://oig.justice.gov/reports/2015/o1506.pdf.



3 pav. *Įeinančios ir išeinančios komunikacijos registravimo orderių skaičius 2000–2012m.* [458].

ypatingai minimalų teismo vaidmenį sankcionavime. Taigi, FISA įeinančios ir išeinančios komunikacijos registravimo orderis (angl. *FISA pen trap order*) tam tikrą laikotarpį buvęs masinio asmens duomenų rinkimo el. erdvėje įrankiu šiuo metu yra praradęs savo populiarumą dėl vėliau įtvirtintų patogesnių ir dar labiau žvalgybos poreikiams pritaikytų FISA įrankių: veiklos įrašų rinkimo orderio (angl. *business records order*) ir 702 straipsnio orderio (angl. *702 order*).

FISA veiklos įrašų rinkimo orderis (angl. FISA business records order). FISA veiklos įrašų rinkimo orderis (angl. *FISA business records order*) – tai 2005 m. įtvirtinta FISA teismo sankcionavimo rūšis, kurios pagrindu žvalgybos institucijos renka asmenų istorinės komunikacijos metaduomenis. Labai abstrakčiai žiūrint FISA veiklos įrašų rinkimo orderį (angl. *FISA business records order*) galima laikyti ECPA teismo šaukimo (angl. *subpoena*) ir D orderio (angl. *D order*) hibridu[459]. Šio orderio pagrindu gali būti renkami visi neturininio pobūdžio veiklos metaduomenys, kas ECPA atveju gali būti renkami tik D orderio (angl. *D order*) pagrindu, kurio išdavimui yra reikalingas pakankamas pagrindas įtarimui (angl. *reasonable articlable suspition*). Taigi FISA veiklos įrašų rinkimo orderis (angl. *FISA business records order*) yra lengvesnis būdas gauti tokią pačią informaciją kokia gali būti renkama vadovaujantis ECPA, todėl, manoma, juo naudojasi ir teisėsaugos institucijos[460], atliekančios ir žvalgybos funkcijas.

[458] „EPIC – EPIC v. DOJ – Pen Register Reports“, *Electronic Privacy Information Center*, žiūrėta 2020 m. rugsėjo 6 d., https://epic.org/foia/doj/pen-reg-trap-trace/.

[459] Kadangi prieš sankcionuodamas šio tipo asmens duomenų rinkimą el. erdvėje teismas iš esmės įvertina ar yra sankcionavimo pagrindas, tačiau sankcionavimo pagrindas yra toks kaip teismo šaukimo (angl. *subpoena*) atveju.

[460] Jacob Sommer, „FISA Authority and Blanket Surveillance; A Gatekeeper without Opposition“, *Litigation* 40, no. 4 (2014 2013): 40–46.

FISA veiklos įrašų rinkimo orderio (angl. *FISA business records order*) pagrindu gali būti vykdomos masinio asmens duomenų rinkimo programos. 2006 m. FISA teismas sankcionavo D orderius (angl. *D order*) vietinių telefoninių ryšių metaduomenų rinkimui[461], tačiau iki 2013 m. kuomet E. Snowden viešai atskleidė informaciją apie NSA masinį asmens duomenų rinkimą, FISA teismas nebuvo pasisakęs apie masinio asmens duomenų rinkimo sankcionavimą FISA veiklos įrašų rinkimo orderio (angl. *FISA business records order*) pagrindu[462]. Telefoninio ryšio metaduomenų masinio rinkimo programa nėra vienintelė sankcionuota FISA teismo. 2010-2011 m. buvo vykdyta masinė mobiliojo ryšio telefonų buvimo vietos nustatymo duomenų programa. Tikėtina, kad iki šiol Centrinė žvalgybos agentūra (CŽV) FISA veiklos įrašų rinkimo orderio (angl. *FISA business records order*) pagrindu vykdo masinį finansinių asmens duomenų rinkimą[463]. Apie šią programą yra labai mažai žinoma. Manoma, jog yra ir daugiau masinio asmens duomenų rinkimo FISA veiklos įrašų rinkimo orderio (angl. *FISA business records order*) pagrindu programų apie kurias viešai nėra žinoma.

Kaip matome, dalį masinio asmens duomenų rinkimo (masinio sekimo) programų JAV vykdė ir galbūt vykdo FISA veiklos įrašų rinkimo orderio (angl. *FISA business records order*) pagrindu, o dalį FISA įeinančios ir išeinančios komunikacijos orderio (angl. FISA *pen trap order*) pagrindu. Kodėl žvalgybos institucijoms nepakanka FISA įeinančios ir išeinančios komunikacijos orderio (angl. FISA *pen trap order*) masiniam asmens duomenų rinkimui el. erdvėje vykdyti? Viena iš priežasčių yra ta, kad ne visi veiklos įrašai (angl. *business records*) yra susiję su komunikacija. Pavyzdžiui, CŽV Finansinių įrašų programos pagrindu renka finansinius duomenis, kurie nėra komunikacijos duomenimis[464]. Kita priežastis – ne visi duomenys, reikalingi žvalgybos institucijoms, yra tik atsirasiantys ateityje (angl. *prospective*). Pavyzdžiui, interneto metaduomenys, komunikacinių paslaugų teikėjų kaupiami telefoninių pokalbių metaduomenys yra duomenys jau apie buvusią, o ne apie būsimą komunikaciją, tad jų rinkti FISA įeinančios ir išeinančios komunikacijos orderio (angl. FISA *pen trap order*) pagrindu nėra galimybės. Ir galiausiai renkant asmens duomenis el. erdvėje FISA veiklos įrašų rinkimo orderio (angl. *FISA business records order*) pagrindu nėra įtvirtinto reikalavimo apie tai pranešti duomenų subjektui, o šis reikalavimas yra tokius duomenis renkant FISA įeinančios ir išeinančios komunikacijos orderio (angl. FISA *pen trap order*) order pagrindu, jeigu vėliau juos ketinama naudoti kaip įrodymus[465]. Taip pat įtariamasis neturi teisės prašyti teismo panaikinti dėl FISA įeinančios ir išeinančios komunikaci-

---

[461] Christopher Cooke, „Note: Securing Liberty: A Response to Debates on Section 215 of the Patriot Act Symposium Comments and Notes: Phone Records and the NSA: Protecting America vs. Protecting Americans' Privacy", *Georgetown Journal of Law & Public Policy* 12, no. 2 (2014): 889–96.

[462] „Transparency Report: THE USA FREEDOM Act Business Records FISA Implementation", žiūrėta 2020 m. rugsėjo 6 d., https://fas.org/irp/nsa/ufa-2016.pdf. Administration White Paper, „Bulk Collection of Telephony Metadata Under Section 215 of the USA PATRIOT Act", žiūrėta 2020 m. rugsėjo 6 d., https://fas.org/irp/nsa/bulk-215.pdf.

[463] Jonathan Mayer, „In NSA Appeals, DOJ Misleads About Medical and Financial Records", *Web Policy*, žiūrėta 2020 m. rugsėjo 6 d., http://webpolicy.org/2014/12/11/nsa-appeals-medical-financial-records/.

[464] Margaret Hartmann, „The CIA Collects Data in Bulk, Just Like the NSA", *Intelligencer*, žiūrėta 2020 m. rugsėjo 6 d., https://nymag.com/intelligencer/2013/11/cia-collects-data-in-bulk-just-like-the-nsa.html.

[465] Carr ir Bellia, *supra note,* 361.

jos orderio (angl. FISA *pen trap order*) pagrindu surinktų asmens duomenų, jie buvo surinkti nesant teisėto pagrindo (suppression), o jeigu jie būtų surinti FISA įeinančios ir išeinančios komunikacijos orderio (angl. FISA *pen trap order*) pagrindu tuomet įtariamasis turėtų teisę į įrodymo užginčijimą (angl. *suppression*), jei jis yra pirminis duomenų šaltinis[466]. Taigi FISA įeinančios ir išeinančios komunikacijos orderis (angl. FISA *pen trap order*) yra palankesnė priemonė masinio sekimo programoms, nes šio teismo sankcionavimo priemonės skaidrumas, naudojimo viešumas yra žymiai mažesnis nei FISA įeinančios ir išeinančios komunikacijos orderių (angl. FISA *pen trap order*).

FISA 702 straipsnio pagrindu priimami orderiai (angl. section 702 orders of FISA).702 straipsnio pagrindu priimami orderiai (angl. *section 702 orders of FISA*) į FISA buvo įtraukti 2007 m. Amerikos apsaugos aktu (angl. *Protect America Act*). Jų taikymo apimties specifika pasireiškia tuo, kad jie yra taikomi tik tuo atveju, kai renkami asmens duomenys yra JAV, tačiau asmuo yra už JAV valstybės ribų ir yra nelaikomas JAV asmeniu[467]. Kadangi didžioji dauguma asmens duomenų, laikomų debesų kompiuterijoje fiziškai yra JAV, nes debesų kompiuterijos paslaugų tiekėjų serveriai yra šioje šalyje[468] bei didžioji dauguma telekomunikacijos srautų susijusių su failų dalijimuisi elektroninėje erdvėje naudotojų būtent ir yra užsieniečiai, o šie failai fiziškai lieka JAV[469], vadinasi 702 straipsnio pagrindu priimami orderiai (angl. *section 702 orders of FISA*) gali būti taikomi didžiajai daugumai pasaulio debesų kompiuterijos ir telekomunikacinių paslaugų vartotojų, todėl yra nepaprastai plačios apimties asmens duomenų rinkimo ir sekimo elektroninėje erdvėje priemone.

Kuo FISA 702 straipsnio pagrindu priimami orderiai (angl. *section 702 orders of FISA*) yra ypatingi? Jie suteikia teisę žvalgybos institucijoms rinkti tiek turininio, tiek neturininio pobūdžio duomenis, esančius JAV serveriuose. O FISA 702 straipsnio pagrindu priimamų orderių (angl. *section 702 orders of FISA*) išdavimo procedūra yra ypatingai primityvi, nors teoriškai ir yra sankcionuojama teismo. Vienintelis dalykas, ką turi padaryti žvalgybos pareigūnas, norėdamas rinkti duomenis el. erdvėje, tai pateikti prašymą, kuriame turi būti nurodoma, kad užsienio žvalgyba yra esminis slapto duomenų rinkimo tikslas[470]. Užsienio žvalgybos tikslai ir apimtis nėra ribojama, todėl FISA 702 straipsnio pagrindu priimamais orderiais (angl. *section 702 orders of FISA*) pareigūnai gali teisėtai naudoti labai plačia apimtimi. Teikiant prašymą teismui sankcionuoti FISA 702 straipsnio pagrindu priimamą orderį (angl. *section 702 orders of FISA*) žvalgybos institucijoms nereikia pagrįsti nei tikėtinos priežasties (angl. *probable cause*), nei protingo sąmoningo įtarimo (angl. *reasonable articulable suspition*), netgi nereikia nurodyti ir pagrįsti ir aktualumo (angl. *relevance*). Tereikia, kad duomenų

---

466 Carr ir Bellia, *supra note,* 361.

467 William C. Banks, „Next Generation Foreign Intelligence Surveillance Law: Renewing 702 National Security in the Information Age: Are We Heading toward Big Brother: Symposium Issue 2017: Data Collection and Advancements in Surveillance Techniques“, *University of Richmond Law Review* 51, no. 3 (2017–2016): 675.

468 Alex Kimata, „Section 702 Malfisance“, *Colorado Technology Law Journal* 16, no. 2 (2018 2017): 455–80.

469 Kimata, *supra note*, 468.

470 Patrick Walsh, „Stepping on (or over) the Constitution's Line: Evaluating FISA Section 702 in a World of Changing Resonableness under the Fourth Amendment“, *New York University Journal of Legislation and Public Policy* 18, no. 4 (2015): 741–94.

rinkimas būtų nukreiptas į užsienio subjektą arba užsienio subjekto agentą. Viskas ko reikia – tai nurodyti, kad tikslas yra užsienio žvalgyba[471]. Kadangi FISA 702 straipsnio pagrindu priimti orderiai (angl. *section 702 ordersof FISA*) gali būti naudojami tik tuo atveju, kai asmuo išimtinai yra už JAV ribų ir nėra laikomas JAV asmeniu, todėl teikdamas prašymą teismui sankcionuoti FISA 702 straipsnio pagrindu priimtus orderius (angl. *section 702 orders*), žvalgybos pareigūnas privalo pagrįsti kaip žvalgybos institucija įsitikins, kad asmuo, kurio duomenys bus renkami, tikrai yra ne JAV, o bent kurioje kitoje pasaulio vietoje[472] bei kokiomis konkrečiai priemonėmis jie išvengs atsitiktinio JAV asmenų, duomenų rinkimo[473]. Ir nors teoriškai FISA 702 straipsnio pagrindu priimtų orderių (angl. *section 702 orders of FISA*) pagrindu yra draudžiama rinkti JAV asmenų duomenis, o vykdomoji valdžia ir FISA teismas tai neigia nurodydami, kad JAV asmenų asmens duomenų rinkimas yra vykdomas tik išimtinais atvejais, visgi yra manoma, kad tokių duomenų yra surenkama labai daug tuo pažeidžiant JAV Konstitucijos IV pataisa garantuojamas JAV asmenų teises[474]. Ir nors yra įtvirtintas masinio asmens duomenų rinkimo apsaugos svertas – reikalavimas prašyme FISA teismui nurodyti duomenų rinkimo minimalizavimo priemones, tačiau tai neapima surinktų duomenų naudojimo ir atskleidimo minimalizavimo[475] ir tuo šis reikalavimas skiriasi nuo Telefoninių pokalbių klausymosi akte (angl. *Wiretap act*) numatytų minimalizacijos procedūrų. Gavęs žvalgybos institucijos prašymą sankcionuoti FISA 702 straipsnio pagrindu priimamus orderius (angl. *section 702 orders of FISA*) teismas vertina ar jis atitinka reikalavimus keliamus pagal FISA 702 straipsnį ir gali prašyti žvalgybos instituciją pataisyti savo prašymą pagal teismo pateiktas pastabas[476]. Prašymams, atitinkantiems FISA 702 straipsnio reikalavimus, teismas vienerių metų laikotarpiui išduoda FISA 702 straipsnio pagrindu priimamą orderį (angl. *section 702 order of FISA*). Šio orderio ypatybė yra tai, kad tai yra vienas teismo leidimas visoms institucijos žvalgybos veikloms vienerių metų laikotarpiui, t. y. žvalgybos institucijos neturi atskirai dėl kiekvieno atvejo kreiptis į teismą[477]. Pasibaigus vienerių metų laikotarpiui žvalgybos institucijos vėl kreipiasi į teismą dėl to paties FISA 702 straipsnio pagrindu priimamo orderio (angl. *section 702 orders of FISA*) sankcionavimo[478]. Tokia praktika kartojasi iš metų į metus ir FISA teismas nėra nei vieno žvalgybos institucijos prašymo dėl FISA 702 straipsnio pagrindu priimamo orderio (angl. *section 702 orders of FISA*) sankcionavimo atmetęs. Taigi, teismo vaidmenį užtikrinant asmenų teises

---

471 Privacy and Civil Liberties Oversight Board, *Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act* (CreateSpace Independent Publishing Platform, 2015).

472 Kimata, *supra note*, 468.

473 Laura K. Donohue, „Section 702 and the Collection of International Telephone and Internet Content", *Harvard Journal of Law & Public Policy* 38, no. 1 (2015): 117–266.

474 Arnbak ir Goldberg, *supra note,* 182: 47.

475 Donohue, *supra note*, 473.

476 „50 U.S.C. § 1805(c)", *Legal Information Institute*, žiūrėta 2020 m. rugsėjo 6 d., https://www.law.cornell.edu/uscode/text/50/1805.

477 „50 U.S.C. § 1805(c)", *Legal Information Institute*, žiūrėta 2020 m. rugsėjo 6 d., https://www.law.cornell.edu/uscode/text/50/1805.

478 Donohue, *supra note*, 473.

pagal FISA 702 straipsnį procese dar labiau sumenkina tai, kad asmens duomenys yra renkami ne tiesiogiai FISA 702 straipsnio pagrindu priimto orderio (angl. *section 702 orders of FISA*) pagrindu.

Teismui sankcionavus FISA 702 straipsnio pagrindu priimtą orderį (angl. *section 702 orders of FISA*), žvalgybos institucijos pačios priima dviejų rūšių FISA 702 straipsnio direktyvas (angl. *section 702 directives of FISA*):

1) konkrečiai apibrėžtas direktyvas (angl. *targeted directives*), kurios yra adresuojamos konkrečioms paslaugas elektroninėje erdvėje teikiančioms įmonėms dėl konkrečių saugomų paskyrų ir būsimų duomenų (angl. *accounts stored and prospective data*), ir
2) masinio duomenų rinkimo el. erdvėje direktyvas (angl. *bulk surveillance directive*)[479]. Informacijos apie šias direktyvas nėra daug ir jos laikomos ypatingai slaptomis.

Ir nors pačios direktyvos ir FISA 702 straipsnio pagrindu priimami orderiai (angl. *section 702 order of FISA*) yra laikomi ypač kontraversiškomis asmens duomenų rinkimo el. erdvėje priemonėmis, tačiau iki šios būtent šios pačių žvalgybos institucijų priimtos FISA 702 straipsnio direktyvos (angl. *section 702 directives of FISA*) yra privalomos paslaugų elektroninėje erdvėje tiekėjams. FISA 702 straipsnio direktyvos (angl. *section 702 directives of FISA*) savo apimtimi yra labai panašios į telefoninių pokalbių klausymo orderį (angl. *wiretap order*) ir kratos orderį (angl. *search warrant*), nes įpareigoja paslaugų teikėją pateikti žvalgybos institucijoms tiek būsimos, tiek buvusios elektroninės komunikacijos turinį ir suteikti bent kokią kitą pagalbą[480], tačiau be FISA teismo, kaip asmens teisių apsaugos garanto, tiesioginio įtraukimo į šį procesą. Paslaugų elektroninėje erdvėje tiekėjai, kurie yra FISA 702 straipsnio direktyvų (angl. *section 702 directives of FISA*) adresatai gali būti el. ryšių bendrovės, el. pašto paslaugų teikėjai, interneto paslaugų teikėjai, socialinių tinklų paslaugų tiekėjai ir bent kurias kitas paslaugas el. erdvėje teikiantys subjektai[481]. FISA 702 straipsnio pagrindu priimamų orderių (angl. *section 702 order of FISA*) taikymo apimtis yra labai plati. Jis apima visą elektroninę komunikaciją ir debesų kompiuteriją ir tiek jau esamus duomenis, tiek atsirasiančius ateityje. Vienas iš reikalavimų FISA 702 straipsnio pagrindu priimamų orderių (angl. *section 702 order of FISA*) sankcionavimui yra asmens duomenų rinkimo minimalizavimas, tačiau tai, kad šio orderio pagrindu buvo vykdoma masinio asmens duomenų rinkimo programa PRISM[482] rodo, kad tai tėra tik formalumas, o pats orderis yra sukurtas arba tapęs masinio asmens duomenų rinkimo įrankiu, kuris praktiškai neužtikrina jokios ne JAV asmenų teisių apsaugos[483].

---

[479] Donohue, *supra note*, 473.

[480] Ashley Gorski, „This Secret Court Opinion Reveals Mystery Tech Firm Challenged NSA Surveillance Order", *American Civil Liberties Union*, žiūrėta 2020 m. rugsėjo 6 d., https://www.aclu.org/blog/national-security/privacy-and-surveillance/secret-court-opinion-reveals-mystery-tech-firm.

[481] „Standing, Surveillance, and Technology Companies", žiūrėta 2020 m. rugsėjo 6 d., https://harvardlawreview.org/2018/04/standing-surveillance-and-technology-companies/.

[482] Peter Margulies, „The NSA in Global Perspective: Surveillance, Human Rights, and International Counterterrorism Symposium: Citizenship, Immigration, and National Security after 9/11", *Fordham Law Review* 82, no. 5 (2014 2013): 2137–68.

[483] Liane Colonna, „Prism and the European Union's Data Protection Directive", *John Marshall Journal of Information Technology and Privacy Law* 30, no. 2 (2014 2013): 227–52.

Amerikos civilinių laisvių unija (angl. *American Civil Liberties Union*) (toliau – ACLU), bendradarbiaudama su žmogaus teisių apsaugos specialistas ir kitais teisininkais, bei el. paslaugų teikėjais, iškart po FISA 702 straipsnio įsigaliojimo pateikė skundą JAV Apygardos teismui dėl neribotos masinės asmens duomenų rinkimo el. erdvėje priemonės neteisėto įteisinimo[484]. ACLU savo skundą grindė tuo, kad FISA 702 straipsnis pažeidžia asmens teises bei I ir IV JAV Konstitucijos pataisas užtikrinančią kalbos laisvę ir draudžiančias teismo nesankcionuotą asmens duomenų rinkimą[485]. JAV Apygardos teismas atmetė ACLU skundą kaip nepagrįstą įrodymais, tačiau ACLU nesutikdama su teismo sprendimu 2011 m. pateikė apeliaciją JAV Apeliaciniam teismui, kuri 2013 taip pat buvo atmesta[486]. Šįkart apeliacinio skundo atmetimo priežastis buvo netinkamas pareiškėjas[487]. Tokiu būdu JAV teismai išvengė sprendimo, galėjusio pakeisti JAV žvalgybos institucijų veiklos principus. Todėl FISA 702 straipsnis ir toliau lieka galioti, o mokslininkai FISA laiko grėsme JAV piliečių teisėms ir lygina netgi su Demokratinėje Vokietijoje veikusia Stasi[488, 489].

PRISM – tai pagrindinės žinomos masinio asmens duomenų rinkimo sankcionuotos vadovaujantis FISA 702 straipsniu programos kodas[490]. PRISM programos pagrindu JAV ir Didžiosios Britanijos žvalgybos institucijos rinko duomenis iš mažiausiai 9 stambiausių JAV el. paslaugų teikėjų: Microsoft, Yahoo, Google, Facebook, Youtube, Skype, PalTak, Aol ir Apple[491]. 4 paveiksle pavaizduota E. Snowden dienraščiuose *Guardian* ir *Woshington Post* 2013 m. birželio 6 d. paviešinta slapta informacija rodo, kad NSA ir Didžioji Britanija vykdydama PRISM programą nuo 2007 m. iki 2013 m. tarpininkaujant didžiausiems el. paslaugų teikėjams, rinko jų klientų JAV serveriuose esančius duomenis, kurie apima tiek turininio pobūdžio informaciją, tiek ir metaduomenis.

Pasaulio lyderiai viešai pasmerkė PRISM programą, laikydami ją asmens teisių pažeidimu[492]. Tuo tarpu JAV nurodė, jog PRISM programa buvo vykdoma nepažeidžiant FISA 702 straipsnio nuostatų, telekomunikacijos bendrovės turėjo teisę nesutikti teikti

---

484 „ACLU Sues Over Unconstitutional Dragnet Wiretapping Law“, *American Civil Liberties Union*, žiūrėta 2020 m. rugsėjo 6 d., https://www.aclu.org/press-releases/aclu-sues-over-unconstitutional-dragnet-wiretapping-law.

485 „Amnesty International and etc. Complaint for Declaratory and Injunctive Relief“, žiūrėta 2020 m. rugsėjo 6 d., https://www.aclu.org/sites/default/files/pdfs/safefree/faa_complaint_20080710.pdf.

486 „Amnesty v. Clapper – Challenge to FISA Amendments Act“, *American Civil Liberties Union*, žiūrėta 2020 m. rugsėjo 6 d., https://www.aclu.org/cases/amnesty-v-clapper-challenge-fisa-amendments-act.

487 Tim Phillips, „Supreme Court Dismisses Lawsuit Challenging Warrantless Eavesdropping Law“, *Activist Defense*, 2013, žiūrėta 2020 m. rugsėjo 6 d., https://activistdefense.wordpress.com/2013/02/27/supreme-court-dismisses-lawsuit-challenging-warrantless-eavesdropping-law/.

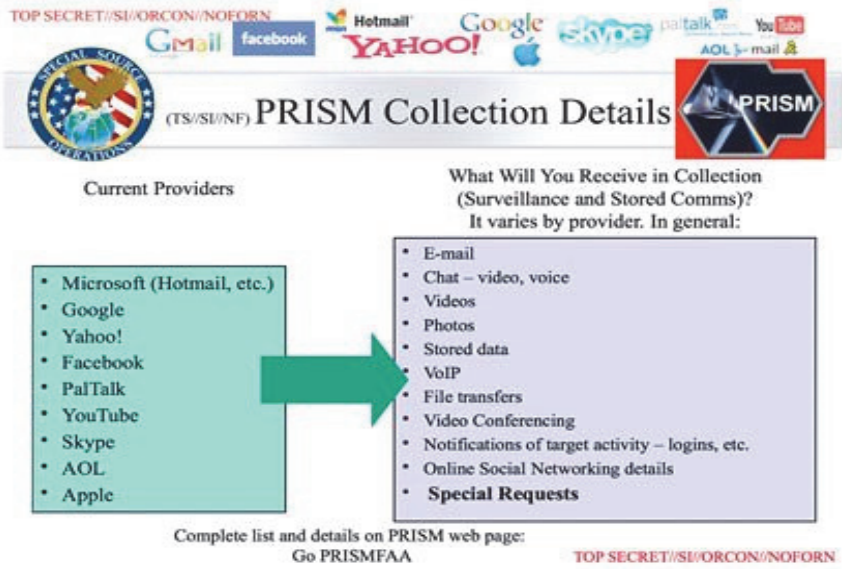
488 Tim Ferriss, „What Every American Needs to Know (and Do) About FISA Today“, *YouTube*, žiūrėta 2020 m. rugsėjo 6 d., https://www.youtube.com/watch?v=hIaWdH6XaBM.

489 Rytų Vokietijos valstybės institucija, atlikusi slaptosios policijos, vidaus ir užsienio žvalgybos bei kontražvalgybos funkcijas. Stasi buvo įkurta 1950 m. vasario 8 d. Socialistų vienybės partija, TSKP atitikmuo Vokietijoje, vadino Stasi Schild und Schwert der Partei (‚Partijos skydas ir kardas‘). Likviduota 1989 m., pradėjus griūti Berlyno sienai.

490 „NSA Prism Program Taps in to User Data of Apple, Google and Others“, *The Guardian*, 2013, žiūrėta 2020 m. rugsėjo 6 d., http://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data.

491 *Ibid.*

492 Laura Smith-Spark, „Merkel: Relations with U.S. 'severely Shaken' over Spying Claims“, *CNN*, žiūrėta 2020 m. rugsėjo 6 d., https://www.cnn.com/2013/10/24/world/europe/europe-summit-nsa-surveillance/index.html.



4 pav. *Asmens duomenų rinkimas pagal PRISM programą 2013 m., originalus dokumentas.*

duomenų žvalgybos institucijoms, tačiau čia teise nepasinaudojo, todėl PRISM programa buvo teisėta[493].

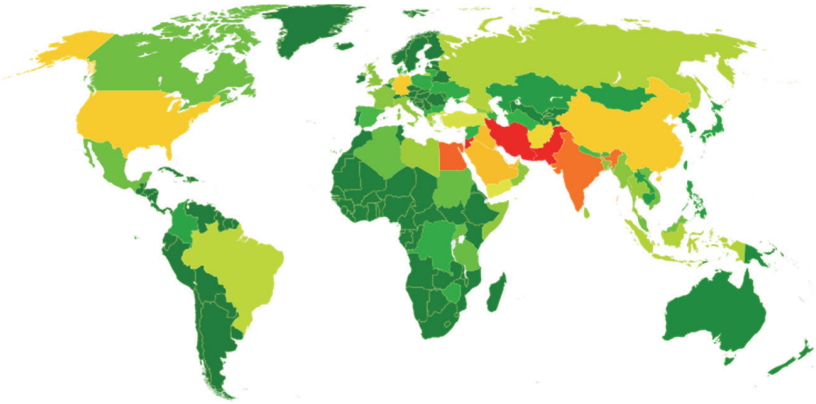
Nors masinio asmens duomenų rinkimo pagal PRISM programą tikslas yra kova su terorizmu[494], tačiau NSA paskelbtas masinio duomenų rinkimo subjektų žemėlapis (žiūrėti ž. 5 pav.) rodo, jog JAV žvalgybos institucijų taikiniu yra ne tik JAV oficialiai laikomos teroristinės valstybės[495], bet ir visas pasaulis, įskaitant pačią JAV. Žemėlapyje nuo tamsiai žalios (mažiausiai surinkta asmens duomenų) iki raudonos spalvų (daugiau surinkta asmens duomenų) spektrais yra pažymėta dažniausi ir rečiausi NSA taikiniai.

Kaip matome, Europoje, išskyrus Vokietiją, vyrauja tamsiai žalia ir šviesesnio atspalvio žalios spalvos. Tačiau prie šviesesnės žalios atspalvio spalvos, rodančios tos

493 „NSA Slides Explain the PRISM Data-Collection Program", *The Washington Post*, žiūrėta 2020 m. rugsėjo 4 d., https://www.washingtonpost.com/wp-srv/special/politics/prism-collection-documents/ .

494 „Facts on the Collection of Intelligence Pursuant to Section 702 of the Foreign Intelligence Surveillance Act", žiūrėta 2020 m. rugsėjo 6 d., https://web.archive.org/web/20130611065954/http://www.dni.gov/index.php/newsroom/press-releases/191-press-releases-2013/871-facts-on-the-collection-of-intelligence-pursuant-to-section-702-of-the-foreign-intelligence-surveillance-act.

495 22 U.S.C. § 2656(f), *Legal Information Institute*, žiūrėta 2020 m. rugsėjo 6 d., https://www.law.cornell.edu/uscode/text/22/2656f.



5 pav. *NSA masinio duomenų rinkimo subjektų žemėlapis.*[496]

valstybės piliečių didesnį nei minimalų asmens duomenų rinkimą, yra priskiriama ir Lietuva. Nors Europolo ataskaitose[497] Lietuva niekada nebuvo priskirta prie terorisčių agresorių, Lietuvoje nebuvo identifikuota nei viena veikianti teroristinė organizacija, o išskyrus 2016 m. terorizmo grėsmė buvo laikoma minimalia, Lietuvoje nebuvo įvykdytas nei vienas teroro aktas, viešai skelbiamų duomenų, kad Lietuva atitiktų užsienio subjekto ar užsienio subjekto sąvokas, nėra. Tuo tarpu Airijoje veikia net kelios teroristinės grupės[498], teroro aktų grėsmė yra didelė, tačiau ši valstybė yra priskiriama tamsiausios žalios spalvos kategorijai, reiškiančiai, kad asmens duomenų rinkimas apie šios valstybės piliečius yra minimalus. Daugiausiai asmens duomenų el. erdvėje NSA surinko apie Vokietiją. Vokietija yra išskiriama ir 2017 m. *Shadow Brokers* nutekintoje informacijoje apie CŽV vykdomą asmenų, nekeliančių grėsmės JAV nacionaliniam saugumui, asmens duomenų rinkimą[499]. Prie geltonos spalvos 2013 m. buvo priskiriama ir Kinija, nors terorizmas Kinijoje yra vidinis, nukreiptas prieš pačios valstybės vykdomą politiką ir nekelia išorinių grėsmių[500]. Tačiau Kinija grėsme JAV tapo dėl labai spartaus ekonominio augimo, kurį buvo galima prognozuoti jau 2013 m. 2018 m. prasidėjęs JAV-Kinijos prekybos karas[501] bei JAV jau nebesuvaldomas Kinijos tapimas

---

496 Šaltinis: „NSA Prism Program Taps in to User Data of Apple, Google and Others“, *The Guardian*, 2013, žiūrėta 2020 m. rugsėjo 6 d., http://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data.

497 „Europol in Brief 2018“, *Europol*, žiūrėta 2020 m. rugsėjo 6 d., https://www.europol.europa.eu/activities-services/main-reports/europol-in-brief-2018.

498 Michael P. O'Connor ir Celia M. Rumann, „Into the Fire: How to Avoid Getting Burned by the Same Mistakes Made Fighting Terrorism in Northern Ireland“, *Cardozo Law Review* 24, no. 4 (2003 2002): 1657–1752.

499 Scott Shane, Matthew Rosenberg ir Andrew W. Lehren, „WikiLeaks Releases Trove of Alleged C.I.A. Hacking Documents“, *The New York Times*, 2017, žiūrėta 2020 m. rugsėjo 6 d., https://www.nytimes.com/2017/03/07/world/europe/wikileaks-cia-hacking.html.

500 Phillip B. K. Potter, „Terrorism in China: Growing Threats with Global Implications“, *Strategic Studies Quarterly* 7, no. 4 (2013): 70–92.

501 „Trump's Trade War With China Is Officially Underway“, *The New York Times*, žiūrėta 2020 m. rugsėjo 6 d., https://www.nytimes.com/2018/07/05/business/china-us-trade-war-trump-tariffs.html.

konkurentė ekonomikoje, inovacijose ir moksle[502] – būtent tai, tikėtina, yra priežastis, kodėl jau 2013 m. ši šalis buvo žvalgybos programos, kurios tikslas nacionalinio saugumo užtikrinimas, taikiniu. Kita valstybė kelianti klausimų dėl terorizmo grėsmių JAV kėlimo yra Indija. Indija yra pažymėta oranžine spalva, rodančia, kad NSA perėmė daug šios šalies komunikacijos el. erdvėje duomenų, nors pati Indija nėra siejama su terorizmu ar grėsme būtent JAV nacionaliniam saugumui. Kaip ir Kinijoje, taip ir Indijoje, terorizmas yra vidinis, nukreiptas prieš pačią Indiją[503]. Tačiau Indija gali tapti JAV konkurente pasaulinėje rinkoje. E. Snowden paviešinti failai liudija, kad JAV žvalgybos objektu buvo Indijos vidinės politikos aktualijos, šalies strateginiai (branduolinė, kosmoso ir kita politika) bei prekybos interesai[504]. Plačiąja prasme žiūrint, ekonominės galios ir vaidmens pasaulyje silpimą, galima laikyti grėsme nacionaliniam saugumui, o ekonominis saugumas yra nacionalinio saugumo dalis. Tačiau programos vykdymo tikslas buvo kova su terorizmu. Terorizmas yra pateisinamas žvalgybos tikslas. Tačiau nepateisinama nekontroliuojama elektroninė žvalgyba kitos valstybės vidinės politikos aktualijų, strateginių (branduolinė, kosmoso ir kita politika) bei prekybos interesų nuspėjimo tikslais, kai visos valstybės elektroninės erdvės atžvilgiu turi ypač skirtingus pajėgumus, nes el. erdvė yra sukurta, todėl ir didžiąja dalimi kontroliuojama JAV.

Kontraversiškasis FISA 702 straipsnis galioti turėjo iki 2017 m. gruodžio 31 d. Tačiau JAV Baltųjų rūmų atstovas spaudai informavo Reuters, kad tokia, kokia yra dabar, FISA yra reikalinga nacionaliniam saugumui užtikrinti ir prezidentas D. Trump neketina jos keisti[505], todėl jos galiojimo laikas buvo pratęstas[506]. Kadangi tiesiogiai spaudimą dėl JAV teisės aktų teisėtumo ir atitikimo JAV Konstitucijos IV pataisą gali daryti tik JAV asmenys, todėl prezidentas D. Trump juos pasirinko sprendimo nekeisti FISA 702 straipsnio pateisinimo priemone ir akcentavo, kad FISA tikslas nėra rinkti JAV asmenų duomenis. FISA tikslas yra užsienio žvalgyba. Žmogaus teisių stebėjimo aktyvistai neigiamai vertina prezidento D. Trump sprendimą[507], visgi JAV piliečiai ir nuolatiniai gyventojai nesijaučia ypatingai sukrėsti ar nesaugūs. Po E. Snowden atskleistų faktų apie JAV ir Didžiosios Britanijos vykdytą masinę asmens duomenų rinkimo el. erdvėje programą, buvo atliktas tyrimas, kurio metu paaiškėjo, kad tik 52% amerikiečių yra susirūpinę asmens duomenų saugumu, bet tik savo pačių atžvilgiu, 44% sakė nesantys susirūpinę dėl valstybės vykdomos asmens duomenų rinkimo el. erdvėje politikos[508].

---

[502] „Red moon rising“, *The Economist*, žiūrėta 2020 m. rugsėjo 6 d., https://www.economist.com/leaders/2019/01/12/how-china-could-dominate-science. „The China Issue“, *Massachusetts Institite of Technology (MIT) Technology Review,* žiūrėta 2020 m. rugsėjo 6 d., https://www.technologyreview.com/magazines/the-china-issue/.

[503] C. Raj Kumar, „Human Rights Implications of National Security Laws in India: Combating Terrorism While Perserving Civil Liberties“, *Denver Journal of International Law and Policy* 33, no. 2 (2005 2004): 195–222.

[504] „NSA Spied on Indian Embassy and UN Mission, Edward Snowden Files Reveal“, *The Guardian*, 2013, žiūrėta 2020 m. rugsėjo 6 d., http://www.theguardian.com/world/2013/sep/25/nsa-surveillance-indian-embassy-un-mission.

[505] Dustin Volz ir Steve Holland, „White House Supports Renewal of Spy Law without Reforms: Official“, *Reuters*, 2017, žiūrėta 2020 m. rugsėjo 6 d., https://www.reuters.com/article/us-usa-trump-fisa-idUSKBN16855P.

[506] *Ibid.*

[507] „House Extends Surveillance Law, Rejecting New Privacy Safeguards“, *The New York Times*, žiūrėta 2020 m. rugsėjo 6 d., https://www.nytimes.com/2018/01/11/us/politics/fisa-surveillance-congress-trump.html.

[508] „The State of Privacy in America“, *Pew Research Center*, žiūrėta 2020 m. rugsėjo 6 d., https://www.pewresearch.org/fact-tank/2016/09/21/the-state-of-privacy-in-america/.

Tokie rezultatai, tikėtina, yra sąlygoti baimės tapti terorizmo aukomis. Paprastai tarp privatumo apsaugos ir apsaugos nuo terorizmo grėsmių, visuomet natūralus savisaugos instinktas lemia pasirinkimą aukoti privatumą vardan savo gyvybės. Juk privatumo praradimas nesukelia fizinio skausmo, kurio žmogus natūraliai bijo. Tačiau ar tikrai terorizmas kelia tokią didžiulę grėsmę JAV, kad būtų reikalingas masinis viso pasaulio gyventojų duomenų rinkimas el. erdvėje? Iš tikrųjų per pastarąjį dešimtmetį nuo teroro aktų JAV, tame tarpe vykdytų ir vidinių JAV ekstremistų, nepriklausančių džihadistams, žuvo mažiau nei 100 žmonių[509]. PRISM programos kaina per metus siekia apie 20 milijonų JAV dolerių[510]. Aišku, galima teigti, kad tai yra asmens duomenų rinkimo JAV programų efektyvumo įrodymas. Tačiau nėra tai patvirtinančių duomenų. Mokslininkų manymu, surenkami asmens duomenų kiekiai yra per dideli, kad juose būtų galima įžvelgti terorizmo apraiškas. Oficialiai skelbiamos informacijos, kad teroristinius aktus pavyko užkardyti dėl masinio asmens duomenų rinkimo, nėra. Pavyzdžiui, Reinhard Kreissl terorizmo apraiškų ieškojimą per masinį asmens duomenų rinkimą prilygina adatos ieškojimui šieno kupetoje[511]. Knygoje „Power Wars: The Relentless Rise of Presidential Authority and Secrecy" teigiama, kad JAV prezidento Bušo prezidentavimo laikotarpiu vykdytos (šiuo metu išviešintos) programos „Stellarwinds" metu iš visų el. erdvėje surinktų duomenų laikotariu 2002–2004 m. tik 1,2% buvo galima panaudoti kovoje su terorizmu. Asmens duomenų kiekiams padidėjus 2004–2006 m. 0% informacijos buvo galima panaudoti kovoje su terorizmu[512]. JAV politikos institutas „New Amerika Foundation" 2013 m. paskelbė tyrimo rezultatus apie NSA 2001–2013 m. vykdyto masinio asmens duomenų rinkimo vaidmenį užkardant terorizmą. Tyrimo rezultatai parodė, kad „masinis asmens duomenų rinkimas neturėjo reikšmės teroristinių aktų prevencijai"[513]. Viena iš problemų, kodėl masinis asmens duomenų rinkimas neprisideda arba tik neženkliai prisideda prie žvalgybos operacijų sėkmės yra ir reikšmingos informacijos atpažinimo ir dalijimosi tarp nacionalinių žvalgybos institucijų koordinacijos nebuvimas. Šią problemą Lietuvoje bus bandoma spręsti Generolo Jono Žemaičio Lietuvos karo akademijai kartu su MRU vykdant ikiprekybinį pirkimą (mokslinių tyrimų ir eksperimentinės plėtros paslaugų pirkimo projektas), kurio metu bus siekiama sukurti nacionalinę informacinio poveikio atpažinimo ir analizės ekosistemą (NAAS). O tai, kad JAV vykdė masinio asmens

[509] Jennifer Stisa Granick, *American Spies: Modern Surveillance, Why You Should Care, and What to Do About It* (Cambridge UK New York: Cambridge University Press, 2017), 5.

[510] „NSA Prism Program Taps in to User Data of Apple, Google and Others", *The Guardian*, 2013, žiūrėta 2020 m. rugsėjo 6 d., http://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data.

[511] Reinhard Kreissl, *Terrorism, mass surveillance and civil rights*, *CEPOL*, žiūrėta 2020 m. rugpjūčio 14 d., https://www.cepol.europa.eu/sites/default/files/26-reinhard-kreissl.pdf.

[512] Charlie Savage, *Power Wars: The Relentless Rise of Presidential Authority and Secrecy*, Revised edition (New York: Back Bay Books, 2017).

[513] Ellen Nakashima, „NSA Phone Record Collection Does Little to Prevent Terrorist Attacks, Group Says", *Washington Post*, 2014, žiūrėta 2020 m. rugsėjo 6 d., https://www.washingtonpost.com/world/national-security/nsa-phone-record-collection-does-little-to-prevent-terrorist-attacks-group-says/2014/01/12/8aa860aa-77dd-11e3-8963-b4b654bcc9b2_story.html. Peter Bergen ir kt., „Do NSA's Bulk Surveillance Programs Stop Terrorists", žiūrėta 2020 m. rugpjūčio 14 d. https://d1y8sb8igg2f8e.cloudfront.net/documents/Do-NSAs-Bulk-Surveillance-Programs-Stop-Terrorists.pdf.

duomenų sekimo el. erdvėje programas ir iki 2001 m. rugsėjo 11-osios teroro aktų[514], tačiau tai nepadėjo išvengti tragedijos, labiau liudija tai, kad masinis asmens duomenų rinkimas el. erdvėje nėra efektyvi kovos su terorizmu priemonė. Todėl retoriniu gali būti klausimas ar tikrai viso pasaulio gyventojų teisė į asmens duomenų apsaugą ir privatumą turi būti aukojamos vardan tariamai labai didelės terorizmo grėsmės JAV, po kuria, greičiausiai slepiasi JAV nenoras prarasti pasaulio ekonominės lyderės pozicijų?

2.3.3. Teismo nesankcionuotas asmens duomenų rinkimas Prezidento pavedimu

JAV prezidentas yra ypatingus įgaliojimus nacionalinio saugumo ir užsienio žvalgybos klausimais turinti figūra. Yra teigiama, kad prezidento įgaliojimai nacionalinio saugumo ir žvalgybos srityje yra jo fundamentinė galia, kurios išraiška yra Vykdomasis nurodymas 12333 (angl. *Executive Order 12333*) (toliau – EO 12333). EO 12333 buvo priimtas 1981 m. prezidento Reigano ir iš dalies pakeistas tris kartus[515] 2003 m.[516], 2004 m.[517] ir 2008 m.[518]. Kaip pažymi prof. Franceska Bignami priimdamas EO 12333 prezidentas Reiganas išplėtė ir taip plačius bei konkrečiai neapibrėžtus NSA įgaliojimus[519]. Nors 2013 m. pasaulis buvo sunerimęs dėl masinių asmens duomenų el. erdvėje rinkimo pagal FISA 702 straipsnį, tačiau ekspertai mano, kad ne FISA 702 straipsnis, o EO 12333 yra dažniausiai naudojama ir kartu mažiausiai skaidri asmens duomenų rinkimo el. erdvėje priemonė[520]. Tik, kadangi kol kas praktiškai nėra nutekinta informacijos apie asmens duomenų rinkimo programas pagal EO 12333, šis teisės aktas nėra sulaukęs tokio susidomėjimo, kaip FISA.

EO 12333 sudaro trys dalys. Pirmojoje dalyje yra įtvirtinti JAV žvalgybos institucijų tikslai, teisės ir pareigos. Antroji dalis reglamentuoja žvalgybos veiklų atlikimą ir draudžia žvalgybos operacijų metu vykdyti žmogžudystę. Trečiąją dalį sudaro bendrosios nuostatos, įsigaliojimas ir tvirtinimo Kongrese mechanizmas[521]. Vadovaujantis EO 12333 JAV žvalgybos institucijos turi teisę nesankcionuotos teismo rinkti tiek metaduomenis, tiek turininio pobūdžio asmens duomenis apie ne JAV asmenis elektroninėje erdvėje už JAV teritorijos ribų žvalgybos tikslais[522] . JAV asmenų duomenis

---

514 Granick, *supra note*, 509.

515 „EPIC – Executive Order 12333“, *Electronic Privacy Information Center*, žiūrėta 2020 m. rugsėjo 6 d., https://epic.org/privacy/surveillance/12333/.

516 „Presidential Documents“, žiūrėta 2020 m. rugpjūčio 14 d., https://www.govinfo.gov/content/pkg/FR-2003-01-28/pdf/03-2069.pdf.

517 „Executive Order: Strengthened Management of the Intelligence Community“, žiūrėta 2020 m. rugsėjo 6 d., https://georgewbush-whitehouse.archives.gov/news/releases/2004/08/20040827-6.html.

518 „Executive Order 13470“, žiūrėta 2020 m. rugsėjo 6 d., https://fas.org/irp/offdocs/eo/eo-13470.htm.

519 Francesca Bignami, „European Versus American Liberty: A Comparative Privacy Analysis of Anti-Terrorism Data-Mining“, 48 (GW Law Faculty Publications & Other Works, 2007): 91.

520 Arnbak ir Goldberg, *supra note,* 182.

521 „Executive Order 12333“, žiūrėta 2020 m. rugsėjo 7 d., https://www.dni.gov/index.php/ic-legal-reference-book/executive-order-12333.

522 Sherri J. Conrad, „Executive Order 12,333: Unleashing the CIA Violates the Leash Law Notes“, *Cornell Law Review* 70, no. 5 (1985 1984): 968–90.

leidžiama rinkti tik atsitiktinai. Surinkti duomenys gali būti saugomi iki 5 metų[523]. Nuo 1981 m. iki šiol EO 12333 nėra buvęs diskurso objektu nei Kongrese, nei teismuose[524].

EO 12333 ištakos yra siejamos su 1952 m. konkuruojančia teisėjo Jackson nuomone byloje Youngstown Sheet&Tube Co. v. Sawyer (arba „The Steel Seizure Case")[525]. Korėjos karo metu plieno gamyklų darbuotojai paskelbė streiką tokiu būdu iškeldami grėsmę karo pramonei ir kartu JAV pergalei kare. Prezidentas Trumanas teisėsaugos institucijoms nurodė atlikti kratą plieno gamyklų patalpose[526]. Iškilus tokio prezidento įsakymo teisėtumo klausimui didžioji dauguma JAV Aukščiausiojo teismo teisėjų pasisakė, kad toks prezidento veikimas buvo jo įgaliojimų viršijimas, todėl – neteisėtas. Teisėjai savo sprendimą grindė tuo, kad JAV prezidentas neturi teisės sankcionuoti kratos, tokią teisę turi tik teismas[527]. Teisėjas Jakson savo konkuruojančiame sprendime pateikė išsamią analizę, įrodančią, kad JAV prezidentas visgi turėjo teisę sankcionuoti kratą. Pirma, pasak teisėjo Jackson, prezidentas turi „aukščiausią vykdomąją galią (angl. *authority is at its maximum*)"[528]. Tai reiškia, kad prezidento sprendimas gali būti laikomas neteisėtu atitinkamoje srityje tik tuo atveju, jeigu vykdomoji valdžia iš viso neturėtų įgaliojimų toje srityje[529]. Vadovaujantis šia teisėjo įžvalga yra laikoma, kad tai yra pagrindas prezidento veiksmas vykdant vidinę nacionalinę – žvalgybą el. erdvėje pagal FISA[530]. Antra, teisėjas Jackson taip pat pasisakė, kad Prezidentas turi teisę veikti ne tik Kongreso aiškiai įvardintais būdais, bet ir tais, kurie tiesiogiai aiškiai nėra įvardijami arba kitaip – veikti ir tuomet, kai tokių įgaliojimų tiesiogiai neturi (angl. *„in a zone of Twilight"*)[531]. Būtent prezidento įgaliojimų veikti ir tuomet, kai tokių įgaliojimų tiesiogiai neturi (angl. *„in a zone of Twilight"*) ir yra laikoma prezidento nurodymu vykdoma užsienio žvalgyba EO 12333 pagrindu[532]. Nors teoriškai EO 12333 patenka į Kongreso prezidentui suteiktų galių apimtį, tačiau statutuose numatyti įgaliojai yra labai dviprasmiški, todėl labiau yra linkstama prie to, kad EO 12333 pagrindu priimami orderiai yra prezidento veikimo Kongreso aiškiai teisės aktuose neįvardintose srityse rezultatas[533]. Taigi asmens duomenų rinkimas el. erdvėje

---

[523] „United States Signals Intelligence Directive", žiūrėta 2020 m. rugpjūčio 14 d. https://www.dni.gov/files/documents/1118/CLEANEDFinal%20USSID%20SP0018.pdf.

[524] John Napier Tye, „Meet Executive Order 12333: The Reagan Rule That Lets the NSA Spy on Americans", *Washington Post*, 2014, žiūrėta 2020 m. rugsėjo 7 d., https://www.washingtonpost.com/opinions/meet-executive-order-12333-the-reagan-rule-that-lets-the-nsa-spy-on-americans/2014/07/18/93d2ac22-0b93-11e4-b8e5-d0de80767fc2_story.html.

[525] „Youngstown Sheet & Tube Co. v. Sawyer, (Jackson., J. concurring)", žiūrėta 2020 m. rugsėjo 7 d., https://www.law.cornell.edu/supremecourt/text/343/579.

[526] Deborah Pearlstein, „Before Privacy, Power: The Structural Constitution", *Journal of National Security Law and Policy* 9, no. 2 (2018 2017): 159–210.

[527] *Ibid.*

[528] „Youngstown Sheet & Tube Co. v. Sawyer, (Jackson., J. concurring)", žiūrėta 2020 m. rugsėjo 7 d., https://www.law.cornell.edu/supremecourt/text/343/579.

[529] *Ibid.*

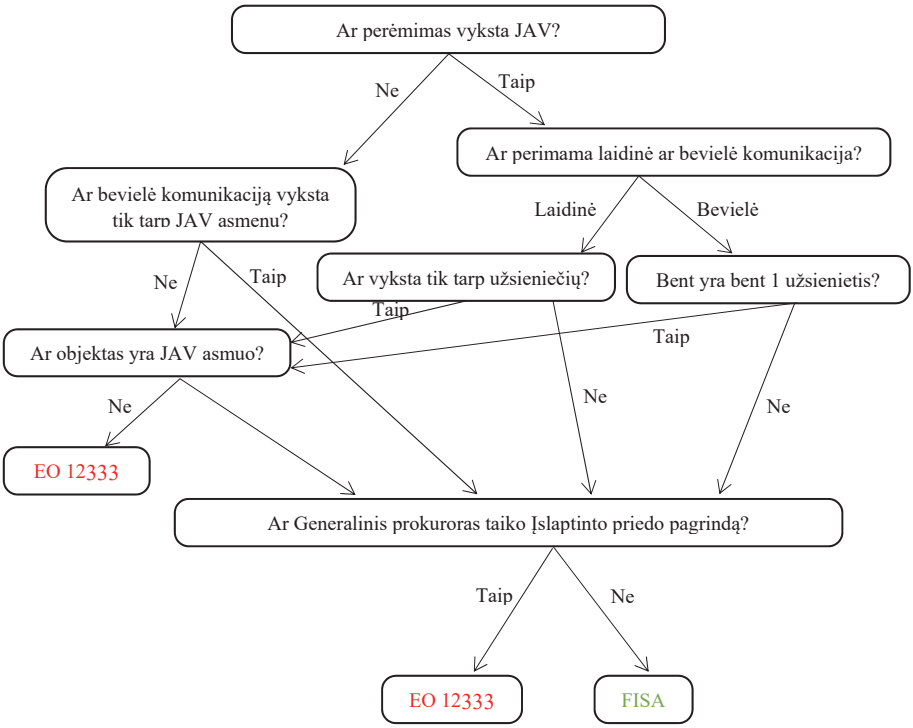
[530] *Ibid.*

[531] *Ibid.*

[532] „Justice Jackson's Test for the Exercise of Presidential Power (*Youngstown* 1952)", žiūrėta 2020 m. rugpjūčio 14 d., http://law2.umkc.edu/faculty/projects/ftrials/conlaw/jacksontest.html.

[533] Pearlstein, *supra note*, 526.

EO 12333 pagrindu reiškia, kad jie yra renkami nacionalinio saugumo užtikrinimui užsienio žvalgybos tikslais, tose srityse ir ta apimtimi, kuri nepatenka nei į ECPA, nei į FISA. EO 12333 ir FISA reglamentavimo apimtį ir skirtumus labai tiksliai iliustruoja 6 paveiksle pavaizduota J. Mayer schema[534]:



6 pav. *EO 12333 ir FISA reglamentavimo takoskyra pagal J. Mayer.*

Nors EO12333 pagrindu turėtų būti renkami tik už JAV teritorijos ribų esantys elektroniniai duomenys, o FISA atveju – tik JAV esantys elektroniniai duomenys, kaip pažymi J. Mayer, taip yra ne visada[535].

Trečioji JAV prezidento veiklos sritis, kurią išskyrė teisėjas Jakson – Kongreso uždrausta vykdomoji veikla. Veikiančio šioje srityje prezidento galia yra laikoma rizikinga (angl. „*power is at its lawest ebb*“) ir neturėtų būti pripažįstama teisėta[536], tačiau vykdomosios valdžios institucijoms yra privaloma, o tokios galios naudojimo veiksmams

[534] Jonathan Mayer, „Executive Order 12333 on American Soil, and Other Tales from the FISA Frontier“, *Web Policy*, žiūrėta 2020 m. rugsėjo 7 d., http://webpolicy.org/2014/12/03/eo-12333-on-american-soil/.

[535] Mayer, *supra note*, 534.

[536] „Youngstown Sheet & Tube Co. v. Sawyer, (Jackson., J. concurring)“, žiūrėta 2020 m. rugsėjo 7 d., https://www.law.cornell.edu/supremecourt/text/343/579.

neigiamų pasekmių nekyla. Tam tikrais atvejais, prezidento veikla EO 12333 pagrindu gali būti laikoma Kongreso jam uždrausta veikti veikla. Veikimo kongreso uždraustoje srityje EO 12333 pagrindu pavyzdžiu yra laikoma prezidento Klintono sprendimai dėl masinio asmens duomenų rinkimo po Rugsėjo 11-osios teroro aktų[537], kuriuos Teisingumo Departamentas (angl. *Departament of Justice*) laiko pažeidžiančiais teisės normas ir neteisėtais[538]. Prezidento Bušo vadovaujama administracija taip pat deklaravo prezidento negatyvią poziciją prezidento veikimo uždraustoje srityje atžvilgiu. Nepaisant to, Elektroninio teroristų sekimo programa (angl. *Terrorist Surveillance programm*) buvo vykdoma[539]. Yra manoma, kad ir šiandien EO 12333 pagrindu, prezidentui veikiant viršijant jam suteiktus įgaliojimus (angl. *„power is at its lawest ebb*“) yra vykdoma bent viena asmens duomenų rinkimo el. erdvėje programa[540]. Vykdomoji valdžia (angl. *Executive Branch*) ją įvardija kaip „Transit Authority“ programą[541]. Manoma, kad šia programa yra renkami tarptautinės telekomunikacijos, kertančios JAV, duomenys[542]. Apie šią programą nėra žinomos viešai skelbiamos informacijos[543].

Taigi, esminės EO 12333 savybės yra šios: 1) jis yra Konstitucijos 2 straipsnyje įtvirtintų prezidento įgaliojimų išraiška, 2) vadovaujantis EO 12333 yra renkami tie duomenys, kurie nepatenka į FISA reglamentavimo apimtį; 3) ekspertai mano, kad būtent EO 12333 pagrindu yra renkama didžioji dauguma asmens duomenų, esančių ne JAV, o didžiąja dauguma JAV žvalgybos institucijos asmens duomenis renka būtent ne JAV[544]. Juolab, kad ir žvalgybos tikslai pagal EO 12333 yra suprantami gerokai plačiau nei FISA: vadovaujantis EO 12333 1.2. straipsnį žvalgybos institucijos turi teisę rinkti informaciją, reikalingą prezidentui, Nacionalinio saugumo kancleriui (angl. *National Security Council*), Vidinio saugumo kancleriui (angl. *Homeland Security Council*) priimti sprendimus užsienio, gynybos ir ekonomikos politikos klausimais. Vadinasi, EO 12333 yra pagrindinis dokumentas, kurio pagrindu JAV žvalgybos institucijos elektroninėje erdvėje renka asmens duomenis. Kokios yra jame įtvirtintos asmens teisių apsaugos garantijos?

Nors ir jo vaidmuo yra tik formalus, tačiau FISA asmens teisių apsaugos garantu yra laikomas specialieji FISA teismai. Priklausomai nuo to, kokius duomenis JAV žvalgybos institucijos nori rinkti, FISA yra įtvirtinti skirtingi reikalavimai FISC teikiamų prašymų turiniui. EO 12333 pagrindu žvalgybos institucijos už JAV teritorijos ribų

---

537 Jonathan Mayer, „Executive Order 12333 (The President's Inherent Article II Power to Conduct Foreign Intelligence)“, *YouTube*, 2014, žiūrėta 2020 m. rugsėjo 7 d., https://www.youtube.com/watch?v=Hr36zslqQMU.

538 *Ibid.*

539 Adrienne LaFrance, „How Drug War Surveillance Turned Into Terrorism Surveillance“, *The Atlantic*, 2015, žiūrėta 2020 m. rugsėjo 7 d., https://www.theatlantic.com/technology/archive/2015/04/same-surveillance-state-different-war/389988/.

540 Patrick Toomey, „The NSA Continues to Violate Americans' Internet Privacy Rights“, *American Civil Liberties Union*, žiūrėta 2020 m. rugsėjo 7 d., https://www.aclu.org/blog/national-security/privacy-and-surveillance/nsa-continues-violate-americans-internet-privacy.

541 Mayer, *supra note,* 534.

542 Alan Z. Rozenshtein, „Surveillance Intermediaries“, *Stanford Law Review* 70, no. 1 (2018): 99–190.

543 Mayer, *op. cit.,* 537.

544 Mayer, *supra note,* 537.

elektroninėje esančius asmens duomenis apie ne JAV asmenis žvalgybos institucijos gali tiesiog rinkti bent kurio iš EO 12333 1.2 straipsnyje įvardintų asmenų iniciatyva, teisminio sankcionavimo mechanizmas jame nėra įtvirtintas. Nors EO 12333 pagrindu apie JAV asmenis teisėsaugos institucijos gali rinkti duomenis gali rinti tik atsitiktinai, tačiau 2007 m. Teismui pasisakius, kad IV JAV Konstitucijos pataisa galioja tik JAV teritorijoje ir tik JAV asmenims[545], galima preziumuoti, kad duomenis renkant pagal EO ir net ir JAV asmenims nėra suteikiamos jų teisių apsaugos garantijos. Nors yra teigiama, kad JAV asmenys negali būti žvalgybos pagal EO 12333 objektu, tačiau tai, kad, vadovaujantis Jungtinių Amerikos Valstijų signalų el. erdvėje rinkimo direktyva Nr. 18 (angl. *United States Signals Intelligence Directive 18*)[546] ir Gynybos departamento direktyva 5240 1-R (angl. *Departament of Defence Directive 5240 1-R)*[547] yra leidžiamas atsitiktinis JAV asmenų duomenų rinkimas, JAV mokslininkai laiko faktu, jog yra renkami duomenys ir apie JAV asmenis tuo pažeidžiant demokratinės valstybės principus[548]. Kaip paaiškėjo paviešinus 2011 m. medžiagą, EO 12333 pagrindu yra surenkama daugiau duomenų apie JAV asmenis nei atliekant žvalgybos veiksmus pagal FISA[549]. EO 12333 yra kritikuojamas ir dėl to, kad tapo lengvai apeinama FISA priemone. Manoma, kad dėl informacinių technologijų pažangos žvalgybos institucijos gali lengvai perdislokuoti asmens duomenų rinkimo operacijas už JAV teritorijos ribų ir tokiu būdu apeiti FISA reikalavimus. FISA suteikia tam tikrą apsaugą asmeniui, tačiau tik tuo atveju, jeigu transatlantiniai asmens duomenys yra renkami JAV. Informacinių technologijų pažangos dėka NSA bendradarbiaudama su Didžiosios Britanijos saugumo tarnybomis EO12333 pagrindu gali rinkti tuos pačius duomenis, kurie dar tik pakeliui į JAV ir kuriuos jau esančius JAV galėtų rinkti tik FISA įtvirtintais sankcionavimo būdais[550]. Pačiame EO 12333 nėra apribojimų jo pagrindu surinktų duomenų atskleidimui ir naudojimui kaip įrodymus teisme.

Labai ilgai informacija apie EO 12333 nebuvo skelbiama viešai[551], todėl šis teisės aktas nebuvo mokslininkų susidomėjimo objektu[552]. Pastaraisiais metais išaugus susidomėjimui EO 12333 kaip įrankiu, pažeidžiančiu JAV asmenų teises buvo prabilta ir apie šio teisės akto reformos poreikį [553]. Tačiau EO 12333 yra Konstitucijos

---

545 U. S. v. U. S. District Court (arba kitaip – *Keith byla*), žiūrėta 2020 m. rugsėjo 5 d., https://supreme.justia.com/cases/federal/us/407/297/.

546 „United States Signals Intelligence Directive“, žiūrėta 2020 m. rugpjūčio 14 d., https://www.dni.gov/files/documents/1118/CLEANEDFinal%20USSID%20SP0018.pdf.

547 *The Army Lawyer* (Judge Advocate General's School, 1997), 25.

548 Hans Born ir Marina Caparini, *Democratic Control of Intelligence Services: Containing Rogue Elephants* (Ashgate Publishing, Ltd., 2013), 119.

549 „United States Signals Intelligence Directive“, žiūrėta 2020 m. rugpjūčio 14 d., https://www.dni.gov/files/documents/1118/CLEANEDFinal%20USSID%20SP0018.pdf.

550 Mayer, *supra note,* 537.

551 „National security agency, memorandum: the national security agency: missions, authorities, oversight and partnerships at 2–3 (2013)“, žiūrėta 2017 m. liepos 13 d., www.nsa.gov/public_info/_files/speeches_testimonies/2013_08_09_the_nsa_story.pdf .

552 Arnbak ir Goldberg, *supra note,* 182: 333.

553 Timothy Edgar, „Surveillance Reform: Privacy Board Turns to E.O. 12,333“, *Lawfare*, 2015, žiūrėta 2020 m. rugsėjo 7 d., https://www.lawfareblog.com/surveillance-reform-privacy-board-turns-eo-12333.

2 straipsnyje įtvirtintų prezidento įgaliojimų išraiška, todėl tik pats prezidentas gali inicijuoti šio teisės akto reformą[554]. Nors prezidentui D. Trump viešai pasipiktinus tuo, kad žvalgybos institucijos rinko jo asmens duomenis rinkiminės kompanijos į prezidentus metu[555] buvo tikimasi teisės aktų, reglamentuojančių žvalgybos veiklą reformos, tačiau tapęs prezidentu D. Trump paskelbė nereformuosiąs JAV žvalgybos institucijų veiklos ir, kad tokia teisinė jų veiklos reglamentavimo sistema, kokia egzistuoja dabar, yra reikalinga JAV nacionalinio saugumo užtikrinimui[556].

***Apibendrinimas*:**

1. *JAV yra asmens duomenų rinkimo el. erdvėje teisėsaugos ir žvalgybos tikslais teisės (angl. Electronic Surveillance Law) pradininke. Nuo 1967 m. plėtojama sistema pasižymi tokiais ypatumais:*
   - *1.1. asmens duomenų rinkimą el. erdvėje teisėsaugos ir žvalgybos tikslais reglamentuoja keletas skirtingų teisės aktų: ECPA yra taikoma teisėsaugai, FISA – taikoma žvalgybai, EO 12 333 – taikoma žvalgybai, ir baudžiamojo proceso kodekso 41 straipsnis – taikoma ir teisėsaugai, ir žvalgybai. Kiekvienas iš šių teisės aktų nustato skirtingas asmens duomenų rinkimo procedūras priklausomai nuo to ar duomenys yra renkami esamuoju laiku ar istoriniai, turinio ar komunikacijos metaduomenys, JAV ar ne JAV asmenų atžvilgiu, JAV ar ne JAV teritorijoje. ECPA ir FISA atveju asmens duomenų rinkimas galimas tik jei yra JAV elementas (asmuo arba jo duomenys yra JAV arba keliauja per JAV), EO 12333 – tik tuo atveju, jei nei vienas elementas nėra JAV, o Baudžiamojo proceso kodekso 41 str. suteikia galimybę asmens duomenis rinkti prisijungus prie bent kurioje pasaulio vietoje esančio įrenginio. ECPA ir baudžiamojo proceso kodekso 41 str. teismo orderį išduoda bendrosios kompetencijos teismai, asmens duomenų rinkimą pagal FISA sankcionuoja specialūs FISA teismai, o EO 12333 asmens duomenų rinkimo pagrindas yra prezidento, nacionalinio saugumo kanclerio (angl. National Security Council), vidinio saugumo kanclerio (angl. Homeland Security Council) nurodymai;*
   - *1.2. išskiriami JAV ir ne JAV asmenys – tik JAV asmenų atžvilgiu galioja IV JAV Konstitucijos pataisa suteikianti teisę į privatumą bei asmens duomenų apsaugą. Ne JAV asmenys neturi jokios teisės aktų apsaugos nepriklausomai nuo to ar ją turi pagal savo nacionalinę teisę;*
   - *1.3. galioja trečiosios šalies doktrina, kurios esmė – el. paslaugų teikėjo turimi metaduomenys apie komunikaciją elektroninėje erdvėje nėra saugomi IV JAV Konstitucijos pataisa, kadangi paslaugos gavėjas žino, kad juos turi paslaugos teikėjas. Trečiosios šalies doktrina nepanaikina teisminio sankcionavimo privalomumo, tačiau sankcionavimo procedūra yra paprastesnė.*

---

[554] Kenneth R. Mayer, „Executive Orders and Presidential Power“, *The Journal of Politics* 61, no. 2 (1999): 445–66, doi:10.2307/2647511.

[555] Louis Nelson, „Trump Calls Unauthorized NSA Collection of Data ‘a Disgrace’“, *Politico*, žiūrėta 2020 m. rugsėjo 7 d., https://politi.co/2z3ykoU.

[556] Volz ir Holland, *supra note*, 505.

2. *JAV asmens duomenų rinkimo el. erdvėje modelis turi šiuos privalumus:*
   2.1. *ECPA, FISA ir EO 12333 yra aiškiai įtvirtinta, kad teisėsaugos ir žvalgybos institucijos asmens duomenis gali rinkti ne tik iš el. ryšių paslaugų teikėjų, bet ir iš visų el. paslaugų teikėjų;*
   2.2. *teisminis sankcionavimas yra privalomas ne tik turinio duomenų rinkimui, bet ir metaduomenų rinkimui, jeigu jie yra renkami JAV teisėsaugos ir kontržvalgybos tikslais;*
   2.3. *FISA teisme yra įsteigtas patariamasis ekspertinis organas Amicus Curiae. Šis patariamasis organas, susidedantis iš teisininkų ir technologijų srities ekspertų, papildo teisėjų kompetenciją apie asmens duomenų rinkimo technologijas ir jų poveikį teisei į asmens duomenų apsaugą.*
3. *JAV asmens duomenų rinkimo el. erdvėje modelis turi šiuos trūkumus:*
   3.1. *teisė į privatumą ir asmens duomenų apsaugą yra suteikiama tik JAV asmenims (angl. USA persons), todėl teisės aktų leidėjai ne JAV asmenų atžvilgiu gali priimti jų teisę į asmens duomenų apsaugą pažeidžiančius teisės aktus. Teisėsaugos ir ypač žvalgybos institucijų veiksmai, atlikti pagal teisės aktų nuostatas, nors ir pažeidžiantys ne JAV asmenų (angl. non USA persons) teisę į asmens duomenų apsaugą, nacionalinės JAV teisės prasme yra laikomi teisėtais. Todėl ir ne JAV asmenų atžvilgiu vykdomos masinio asmens duomenų rinkimo programos yra laikomos teisėtomis, jeigu vykdomos pagal galiojančių JAV teisės aktų nuostatas;*
   3.2. *paprastesnė metaduomenų sankcionavimo tvarka sąlygoja silpnesnę šios rūšies asmens duomenų apsaugą nors metaduomenys negali būti laikomi mažesnės vertės asmens duomenimis nei komunikacijos turinys;*
   3.3. *elektroninių laiškų privatumo akte (angl. Email Privacy Act) yra įtvirtintas labai sudėtingas duomenų apie komunikaciją el. laiškais rinkimo sankcionavimo bei teisės į privatumą užtikrinimo mechanizmas. Pati didžiausia apsauga galioja tik sekundės dalį, kol el. laiškas yra pakeliui pas jo gavėją, minimaliausia – jeigu el. laiškas yra pašto dėžutėje daugiau nei 180 dienų. Sankcionavimo procedūros skiriasi priklausomai nuo to el. laiško stadijos, kurios teisėsaugos institucija kreipdamasi į teismą gali nežinoti.*

3. ASMENS DUOMENŲ RINKIMO ELEKTRONINĖJE ERDVĖJE TEISĖSAUGOS IR ŽVALGYBOS TIKSLAIS REGLAMENTAVIMAS SUPRANACIONALINIAME LYGMENYJE (EUROPOS ATVEJO ANALIZĖ)

Po Antrojo pasaulinio karo Europos valstybės, norėdamos išvengti dar vieno karo ir siekdamos tarpusavio sąjungos ir bendros politikos formavimo, jungėsi į organizacijas: Europos Tarybą ir Europos Ekonominę Bendriją (Europos Sąjungą). Iškeldamos į pirmą vietą tai, kas pasaulinių karų metu neturėjo vertės – asmuo ir jo teisės – ir laikydamos, kad teisių apsauga yra demokratijos ir stabilumo Europoje užtikrinimo pagrindas ne tik valstybės individuliai, bet ir kolegialiai per ET bei ES, priėmė tai reglamentuojančius teisės aktus. Todėl Europos žemyne egzistuoja keli asmens teisių apsaugos lygiai: supranacionalinis – ET ir ES – bei valstybių nacionaliniai. „Jauniausia" iš visų asmens teisių yra teisė į asmens duomenų apsaugą[557], tiesiogiai teisės akte įtvirtinta tik 1981 m. Tiek šios teisės kilmė, tiek apsaugos apimtis yra skirtingos priklausomai nuo apsaugos lygio. Pavyzdžiui, ET asmens duomenų apsaugos teisinio reglamentavimo lygmenyje teisės į asmens privatumą ir į asmens duomenų apsaugą yra labai glaudžiai susijusios ir dažnai tapatinamos[558], tuo tarpu ES lygmenyje teisė asmens duomenų apsaugą yra laikoma savarankiška fundamentine teise[559, 560], kilusia iš asmens teisės į privatumą. Jauniausios teisės – teisės į asmens duomenų apsaugą – atsiradimą labiausiai įtakojo 1970 m. atsiradusi galimybė duomenis rinkti ir tvarkyti automatiniu būdu, arba kitaip – elektroninėje erdvėje. Elektroninė erdvė sąlygojo asmens privatumo sampratos[561] turinio išplėtimą nuo asmens ir asmens elgesio privatumo iki asmens duomenų ir asmens komunikacijos privatumo[562]. Reaguojant į tai, asmens privatumo apsaugos pagrindu, JAV 1968 m. ir vėliau Europoje 1981 – 1995 m. atsirado pirmieji nacionaliniai[563] bei regioniniai teisės aktai – Europos Tarybos 108

[557] Ovidiu Ungureanu ir Cornelia Munteanu, „The Right to Protection of Personal Data, an Autonomous Right II. Doctrine – Studies, Articles, Comments", *Romanian Review of Private Law* 2014, no. 1 (2014): 166–79.

[558] Michael D. Birnhack, „The EU Data Protection Directive: An Engine of a Global Regime", *Computer Law & Security Review* 24, no. 6 (January 1, 2008): 508–20, doi:10.1016/j.clsr.2008.09.001.

[559] „Data Protection, Privacy and New Technologies", *European Union Agency for Fundamental Rights*, žiūrėta 2020 m. rugsėjo 7 d., https://fra.europa.eu/en/themes/data-protection-privacy-and-new-technologies. „Surveillance by Intelligence Services: Fundamental Rights Safeguards and Remedies in the EU – Volume II: Field Perspectives and Legal Update, *European Union Agency for Fundamental Rights*, 2017, žiūrėta 2020 m. rugpjūčio 23 d., https://fra.europa.eu/sites/default/files/fra_uploads/fra-2017-surveillance-intelligence-services-vol-2_en.pdf.

[560] Todėl teisės į asmens duomenų apsaugą pažeidimas kartu gali būti ir teisės į privatumą pažeidimu . Tačiau galima situacija, kuomet teisės į asmens duomenų apsaugą pažeidimas nebus laikomas asmens teisės į privatumą pažeidimu.

[561] Mokslininkai vieningai sutinka, kad pateikti asmens privatumo sąvokos apibrėžimą yra neįmanoma. Todėl kaip alternatyva sąvokai yra pasirinktas asmens privatumo apibrėžimas per šios sąvokos galimus turinio komponentus.

[562] „Roger Clarke's 'Privacy Introduction and Definitions'", žiūrėta 2020 m. rugsėjo 7 d., http://www.rogerclarke.com/DV/Intro.html.

[563] Boehm, *supra note*, 76.

konvencija[564], 1995 m. spalio 24 d. Europos Parlamento ir Tarybos direktyva 95/46/EB dėl asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo (toliau – Direktyva Nr. 95/46)[565], kuriais buvo siekiama užtikrinti asmens privatumą ir duomenų apsaugą elektroninėje erdvėje. Nors dauguma Europos valstybių yra ET, ir ES narės – tačiau nacionalinis teisinis asmens duomenų apsaugos reglamentavimas iki ES asmens duomenų apsaugos reformos buvo skirtingas. Ir po ES reformos teisė į asmens duomenų apsaugą išliko neabsoliuti, o jos apribojimai teisėsaugos veikloje – iš dalies – bei žvalgybos veikloje – visiškai – liko kiekvienos ES valstybės narės reikalas. Europoje susidaro įdomi situacija dėl asmens duomenų rinkimo el. erdvėje teisėsaugos ir žvalgybos tikslais. Teisę į asmens duomenų apsaugą galima apriboti tik įstatymu, tačiau išskyrus Jungtinę Karalystę, ES valstybės narės neturi specialių teisės aktų, kurie reglamentuotų asmens duomenų rinkimą el. erdvėje. Kita vertus, manoma, kad teisėsaugos ir žvalgybos institucijos labai daug asmens duomenų surenka el. erdvėje[566]. Bet valstybių, neturinčių įstatymų, reglamentuojančių asmens duomenų rinkimą el. erdvėje teisėsaugos ir žvalgybos tikslais ir neturinčių visuomenei žinomos specialios tokių duomenų rinkimo tvarkos, nelaiko pažeidžiančiomis teisę į asmens duomenų apsaugą. Kodėl taip yra ir ar tikrai teisė į asmens duomenų apsaugą pati savaime yra pakankamas asmens duomenų apsaugos garantas bus analizuojama šiame disertacijos skyriuje.

3.1. Europos Tarybos lygmuo

Po Antrojo pasaulinio karo šalims supratus teisinės valstybės principo, demokratijos ir žmogaus teisių apsaugos svarbą šioms vertybėms Europoje ginti 1949 m. buvo įkurta Europos Taryba[567]. Siekdama įgyvendinti tikslą, kuriuo ji buvo įkurta, 1950 m. ET paskelbė Europos žmogaus teisių konvenciją (toliau – EŽTK), įsigaliojusią 1953 m. su nešališku tribunolu – Europos žmogaus teisių teismu (toliau – EŽTT). Šiandien visos 47 ET valstybės narės bei ES[568] yra įsipareigojusios laikytis EŽTK[569], kurioje yra įtvirtinta ir asmens teisė į privataus ir šeimos gyvenimo gerbimą. „Niekas neturi patirti savavališko kišimosi į jo privatumą, šeimos gyvenimą, buitį ar susirašinėjimą arba kėsinimosi į jo garbę ir reputaciją. Kiekvienas turi teisę į įstatymo apsaugą nuo tokio kišimosi arba kėsinimosi“ – būtent su šiais Europos žmogaus teisių konvencijoje 1948 m. įtvirtintais

---

564 „Konvencija dėl asmenų apsaugos ryšium su asmens duomenų automatizuotu tvarkymu (ETS Nr. 108)“, *eSeimas*, žiūrėta 2020 m. rugsėjo 7 d., https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/TAIS.129872.

565 „1995 m. spalio 24 d. Europos Parlamento ir Tarybos direktyva (95/46/EB) dėl asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo“, *EUR-Lex*, žiūrėta 2020 m. rugsėjo 7 d., https://eur-lex.europa.eu/legal-content/LT/TXT/?uri=CELEX%3A31995L0046.

566 Ava Kofman, „Digital Jail: How Electronic Monitoring Drives Defendants Into Debt“, *The New York Times*, 2019, žiūrėta 2020 m. rugsėjo 7 d., https://www.nytimes.com/2019/07/03/magazine/digital-jail-surveillance.html.

567 „Who We Are“, *The Council of Europe in Brief*, žiūrėta 2020 m. rugsėjo 7 d., https://www.coe.int/en/web/about-us/who-we-are.

568 Europos Sąjunga Europos Tarybos nare tapo 1999 m.

569 Jungtinės Amerikos Valstijos, Kanada, Meksika, Japonija, Izraelis ir Šventasis Sostas turi stebėtojų statusą Europos Tarybos tarpvyriausybinėse institucijose.

žodžiais yra siejamos tarptautinės teisinės asmens privatumo ir, kartu netiesiogiai, asmens duomenų apsaugos ištakos[570]. Visgi pažvelgę į EŽTK 8 straipsnį, pamatysime, kad tarp jame įtvirtintų pamatinių demokratinės visuomenės vertybių – asmens privatumo, šeimos gyvenimo, namų ir susirašinėjimo slaptumo – asmens duomenų apsauga tiesiogiai nėra įtvirtinta. Ankstyvosiose bylose ir EŽTT asmens duomenų apsaugos nelaikė sudėtine EŽTK 8 straipsnio dalimi[571]. Tačiau pripažindamas, kad EŽTK yra „gyvasis instrumentas", kurio turinys ir interpretacija kinta atsižvelgiant į šiuolaikinio gyvenimo aktualijas[572] ir atsiradus nenuginčijam asmens duomenų apsaugos poreikiui, EŽTT savo poziciją pakeitė[573]. Taigi dabar tiek mokslininkai, tiek EŽTT laikosi tos pozicijos, kad nors EŽTK 8 straipsnio formuluotėje tiesiogiai nėra kalbama apie asmens teisę į duomenų apsaugą, tačiau teisė į asmens duomenų apsaugą yra sudėtinė EŽTK 8 straipsnio dalis[574] [575]. Kokia yra EŽTK 8 str. apimtis, ar jis yra taikomas teisėsaugos ir žvalgybos asmens duomenų rinkimui vykdomam teisėsaugos ir žvalgybos institucijoms?

EŽTK 1 straipsnyje yra nurodyta, kad „Aukštosios Susitariančios Šalys kiekvienam jų jurisdikcijai priklausiančiam asmeniui garantuoja šios Konvencijos I skyriuje apibrėžtas teises bei laisves" ir joje, skirtingai nuo ES teisės aktų, nėra įtvirtinta taikymo išimčių nacionalinio saugumo užtikrinimo ar kovos su nusikalstamumu sričiai. Vadinasi, EŽTK 8 straipsnyje įtvirtinta teisė į asmens duomenų apsaugą galioja ir asmens duomenis renkant teisėsaugos ir žvalgybos institucijoms, įskaitant šių duomenų rinkimą el. erdvėje. Tačiau kitas niuansas yra tas, kad EŽTK 8 straipsnio nuostatų galiojimas nėra absoliutus[576]. Tai reiškia, kad tiek teisė į privatumą, tiek teisė į asmens duomenų apsaugą gali būti teisėtai suvaržytos aukštesnės vertybės apsaugos tikslais nepažeidžiant teisinės valstybės principų. Tačiau suvaržymas yra teisėtas tik tuo atveju, jeigu atitinka EŽTK 8 straipsnyje įtvirtintus principus. Visų pirma – asmens teisės gali būti ribojamos tik įstatymu. Antra, ribojama gali būti tik tiek, kiek tai būtina demokratinėje

---

570 „Handbook on European Data Protection Law – 2018 Edition", *European Union Agency for Fundamental Rights*, 2018, 14, žiūrėta 2020 m. rugsėjo 7 d., https://fra.europa.eu/en/publication/2018/handbook-european-data-protection-law-2018-edition.

571 Boehm, *supra note*, 76: 81.

572 „Europos Žmogaus Teisių Teismo 1978 m. balandžio 28 d. sprendimas byloje Tyrer prieš Jungtinę Karalystę (Nr. 5856/75)", *Hudoc*, žiūrėta 2020 m. rugsėjo 7 d., https://hudoc.echr.coe.int/fre#{%22itemid%22:[%22001-57587%22]}. „Europos Žmogaus Teisių Teismo 1995 m. kovo 23 d. sprendimas byloje Loizidou prieš Turkiją (Nr. 15318/89)", *Hudoc*, žiūrėta 2020 m. rugsėjo 7 d., https://hudoc.echr.coe.int/fre#{%22itemid%22:[%22001-57920%22]}. „Europos Žmogaus Teisių Teismo 2005 m. vasario 4 d. sprendimas byloje Mamatkulov ir Askarov prieš Turkiją (Nr. 46827/99 ir 46951/99)", *Hudoc,* žiūrėta 2020 m. rugsėjo 7 d., https://hudoc.echr.coe.int/fre#{%22itemid%22:[%22001-68183%22]}.

573 „Europos Žmogaus Teisių Teismo 2006 m. birželio 29 d. sprendimas byloje Panteleyenko prieš Ukrainą (11901/02)", *Hudoc*, žiūrėta 2020 m. rugsėjo 7 d., https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22002-3281%22]}. „Europos Žmogaus Teisių Teismo 2008 m. gruodžio 4 d. sprendimas byloje S. ir Marper prieš Jungtinę Karalystę (Nr. 30562/04 ir 30566/04)", *Hudoc*, žiūrėta 2020 m. rugsėjo 7 d., https://hudoc.echr.coe.int/fre#{%22itemid%22:[%22001-90051%22]}. „Europos Žmogaus Teisių Teismo 1997 m. sprendimas byloje Z. Prieš Suomiją (Nr. 22009/93)", *Hudoc*, žiūrėta 2020 m. rugsėjo 7 d., https://hudoc.echr.coe.int/rus#{%22itemid%22:[%22001-58033%22]}.

574 Boehm, *supra note,* 76: 81.

575 Todėl nors tik Europos Sąjungos pagrindinių teisių chartijoje yra nurodyta, kad „Kiekvienas turi teisę į savo asmens duomenų apsaugą", yra laikoma, kad teisė į asmens duomenų apsaugą Europoje visų pirma yra ET, o ne ES idėja ir jos apsauga visų pirma yra įtvirtinta ET ir tik paskui ES lygiu (pastarajai tapus ET nare) atsižvelgiant į EŽTT praktiką, kuri yra ypatingai svarbi teisės į asmens duomenų apsaugą plėtros ir tapimo sudėtine EŽTK 8 straipsnio dalimi kontekste.

576 „Handbook on European Data Protection Law – 2018 Edition", *supra note*, 570: 21.

visuomenėje valstybės saugumo, visuomenės saugos ar šalies ekonominės gerovės interesams, siekiant užkirsti kelią viešos tvarkos pažeidimams ar nusikaltimams, taip pat žmonių sveikatai ar moralei arba kitų asmenų teisėms ir laisvėms apsaugoti (EŽTK 8 str. 2 d.). Jei pirmoji teisės į asmens duomenų apsaugą apribojimo sąlyga yra konkreti ir aiški, tai antroji yra pakankamai abstrakti ir yra EŽTT ir valstybių narių interpretacijos objektu. EŽTT yra suformavęs tokius EŽTK 8 straipsnyje įtvirtintos teisės į asmens duomenų apsaugą apribojimo principus, kurie yra taikomi teisėsaugos ir žvalgybos institucijoms ir kurie atitinka demokratinės visuomenės santvarką:

1) asmens duomenų saugojimas nesant teisėto pagrindo pažeidžia EŽTK 8 str. (pvz. Leander v. Sweden[577], Kopp v. Switzerland[578], Amann v. Switzerland[579]). Vertindamas ar yra EŽTK 8 straipsnio pažeidimas teismas vertina aplinkybes dėl kurių asmens duomenys buvo renkami ir saugomi, duomenų pobūdį ir tikslą, kuriam tie duomenys naudojami[580];
2) šnipinėjimo ir terorizmo užkardymo bei kovos su juo tikslais valstybės narės turi plačią diskrecijos teisę dėl duomenų rinkimo ir slapto sekimo priemonių. Visgi slapto sekimo operacijų metu naudojami asmens duomenų gavimo ir panaudojimo būdai neturi būti priešingi demokratinės valstybės santvarkai (Klass and Others v. Germany[581]). Elektroninių laiškų, pašto ir telekomunikacijų kontrolę EŽTT laiko pateisinama ir nepažeidžiančia EŽTK 8 straipsnio kovos su terorizmu priemone[582];
3) modernios nusikaltimų tyrimo technologijos gali būti naudojamos jeigu yra laikomasi proporcingumo principo: EŽTK 8 straipsnio garantuojama apsauga bus pažeista, jeigu modernios technologijos nusikalstamų veikų tyrimui bus leidžiamos naudoti neatsižvelgiant į balansą tarp galimai gausimos naudos ir asmens privataus gyvenimo poreikio (S. and Marper v. the United Kingdom[583]).
4) policija[584] ir slaptos tarnybos[585] negali nevaržomai slaptai klausytis telefoninių pokalbių, o teisminės institucijos negali nevaržomai jų sankcionuoti[586];

---

577 „Europos Žmogaus Teisių Teismo 1987 m. kovo 26 d. sprendimas byloje Leander prieš Švediją (Nr. 9248/81)“, *Hudoc*, žiūrėta 2020 m. rugsėjo 7 d., https://hudoc.echr.coe.int/rus#{%22itemid%22:[%22001-57519%22]}.

578 „Europos Žmogaus Teisių Teismo 1998 m. kovo 25 d. sprendimas byloje Kopp prieš Šveicariją (Nr. 13/1997/797/1000)“, *Hudoc*, žiūrėta 2020 m. rugsėjo 7 d., https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-58144%22]}.

579 „Europos Žmogaus Teisių Teismo 2000 m. vasario 16 d. sprendimas byloje Amann prieš Šveicariją (Nr. 27798/95)“, *Hudoc*, žiūrėta 2020 m. rugsėjo 7 d., https://hudoc.echr.coe.int/tur#{%22itemid%22:[%22001-58497%22]}.

580 „Personal Data Protection,Fact Sheets on the European Union“, *European Parliament*, žiūrėta 2020 m. rugsėjo 10 d., https://www.europarl.europa.eu/factsheets/en/sheet/157/personal-data-protection.

581 „Europos Žmogaus Teisių Teismo 1978 m. rugsėjo 6 d. sprendimas byloje Klass ir kiti prieš Vokietiją (Nr. *5029/71*)“, *Hudoc*, žiūrėta 2020 m. rugsėjo 7 d., https://hudoc.echr.coe.int/rus#{%22itemid%22:[%22001-57510%22]}.

582 Boehm, *supra note,* 76: 73.

583 „Europos Žmogaus Teisių Teismo 2008 m. gruodžio 4 d. sprendimas byloje S. ir Marper prieš Jungtinę Karalystę (Nr. 30562/04 ir 30566/04)“, *Hudoc*, žiūrėta 2020 m. rugsėjo 7 d., https://hudoc.echr.coe.int/fre#{%22itemid%22:[%22001-90051%22]}.

584 „Europos Žmogaus Teisių Teismo 1984 m. rugpjūčio 2 d. sprendimas byloje Malone prieš Jungtinę Karalystę (Nr. 8691/79)“, *Hudoc*, žiūrėta 2020 m. rugsėjo 7 d., https://hudoc.echr.coe.int/rus#{%22itemid%22:[%22001-57533%22]}. „Europos Žmogaus Teisių Teismo 2000 m. gegužės 12 d. sprendimas byloje Khan prieš Jungtinę Karalystę (Nr. 35394/97)“, *Hudoc*, žiūrėta 2020 m. rugsėjo 7 d., https://hudoc.echr.coe.int/fre#{%22itemid%22:[%22001-58841%22]}.

585 Boehm, *supra note,* 76:73.

586 *Ibid.*

5) slapto sekimo metu surinktų asmens duomenų bazės sukūrimas vadovaujantis viešai neskelbtinu teisės aktu pažeidžia EŽTK 8 straipsnį, kadangi asmenims apribojama teisė sužinoti patekimo į šią duomenų bazę priežastis, tvarkomų asmens duomenų rūšis bei buvimo joje trukmę, informaciją kas ir kokiais tikslais duomenis tvarko[587]. Slaptu įstatymu yra pažeidžiama pati įstatymo esmė – jo turinio privalomas žinojimas asmenims, kurių visuomeninius santykius jis reguliuoja;
6) nacionaliniais teisės aktais tinkamai nereglamentuotas (neapibrėžtos institucijų diskrecijos ribos) pasiklausymo įrangos įmontavimas gyvenamosiose patalpose[588] bei su bylos nagrinėjimu nesusijusio asmens gyvenamosiose patalpose[589] pažeidžia EŽTK 8 straipsnį;
7) viešai paskelbta informacija apie asmenį taip pat gali patekti į EŽTK 8 straipsnio reglamentavimo apimtį, jei tokia informacija yra sistemiškai renkama valstybinių institucijų[590];
8) duomenys policijos, slaptųjų tarnybų ir teisminių institucijų duomenų bazėse turi būti renkami ir saugomi vadovaujantis EŽTK 8 straipsniu, tačiau valstybės nacionalinio saugumo ir kovos su terorizmu interesai yra pateisinama asmens duomenų tvarkymo pažeidžiant EŽTK 8 straipsnį priežastis[591]. Visgi nenuteistų asmenų duomenų bazėse įvardijimas pažeidėjais yra neleistinas[592] kaip ir neturėjimas teisės prašyti ištrinti tokiose duomenų bazėse esančią informaciją[593].

Taigi, EŽTK ir EŽTT aiškindamas EŽTK, laikosi pozicijos, teisę į asmens duomenų apsaugą galima apriboti tik įstatymu. Visgi, tai nereiškia, kad turi būti priimtas atskiras teisės aktas asmens duomenų rinkimo el. erdvėje reglamentavimui.

F. Boehm pastebi, kad EŽTT praktika pastaraisiais metais yra plėtojama valstybių narių diskrecijos mažinimo ir asmens teisės į asmens duomenų apsaugą iškėlimo virš valstybės interesų[594]. Tačiau nacionalinio saugumo ir kovos su terorizmu atvejais EŽTT yra linkęs palikti plačią valstybių narių diskreciją, patvirtindamas bendrąjį teisės principą, kad dėl savo pačių saugumo turime atsisakyti dalies savo teisių. Tik labai svarbu, jog valstybės neimtų piktnaudžiauti savo galia ir asmens teisės į duomenų

---

587 Boehm, *supra note,* 76:73.

588 *Ibid.*

589 „Europos Žmogaus Teisių Teismo 2001 m. rugsėjo 25 d., sprendimas byloje P. G. ir J. H. prieš Jungtinę Karalystę (Nr. 44787/98)“, *Hudoc*, žiūrėta 2020 m. rugsėjo 7 d., https://hudoc.echr.coe.int/eng-press#{%22itemid%22:[%22003-419654-419935%22]}.

590 *Ibid.*

591 „Europos Žmogaus Teisių Teismo 2006 m. birželio 6 d. sprendimas byloje Segerstedt-Wiberg ir kiti prieš Švediją (Nr. 62332/00)“, *Hudoc*, žiūrėta 2020 m. rugsėjo 7 d., https://hudoc.echr.coe.int/eng-press#{%22itemid%22:[%22003-1688388-1769677%22]}.

592 „Europos Žmogaus Teisių Teismo 2011 m. gegužės 10 d. sprendimas byloje Dimitrov-Kazakov prieš Bulgariją (Nr. 11379/03)“, *Hudoc*, žiūrėta 2020 m. rugsėjo 7 d., https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-103258%22]}. „Europos Žmogaus Teisių Teismo 2013 m. balandžio 29 d. sprendimas byloje M. M. prieš Jungtinę Karalystę (Nr. 24029/07)“, *Hudoc*, žiūrėta 2020 m. rugsėjo 7 d., https://hudoc.echr.coe.int/fre#{%22itemid%22:[%22001-114517%22]}.

593 „Europos Žmogaus Teisių Teismo 2014 m. balandžio 18 d. sprendimas byloje Brunet prieš Prancūziją (Nr. 21010/10)“, *Hudoc*, žiūrėta 2020 m. rugsėjo 7 d., https://hudoc.echr.coe.int/eng-press#{%22itemid%22:[%22003-4872410-5953858%22]}.

594 Boehm, *supra note,* 76: 73.

apsaugą atsisakymas netaptų absoliučiu kiek tai liečia nacionalinio saugumo užtikrinimą ir kovą su terorizmu[595]. Panaši tendencija atsispindi ir ES teisėkūroje: teisėsaugos institucijų veikla yra reglamentuojama Teisėsaugos tikslais tvarkomų asmens duomenų direktyva, tuo tarpu teisės akto, reglamentuojančio žvalgybos institucijų veiklą – nėra. Nėra visuotinai pripažįstamos tiek nacionalinio saugumo, tiek terorizmo sąvokos, todėl iškyla dar ir manipuliavimo visuomenės saugumo ir kovos su terorizmu sąvokomis siekiant kitų tikslų, kurie taip neveikia asmens pasąmonės kaip baimė tapti teroro akto auka[596].

EŽTK 8 straipsnis yra pirmoji, bet ne vienintelė teisinė ET asmens duomenų apsaugos priemonė. Kita priemone nuo 1981 m. yra Europos Tarybos 1981 m. Konvencija dėl asmenų apsaugos ryšium su asmens duomenų automatizuotu tvarkymu (toliau – 108 Konvencija). Iki priimant 108 Konvenciją, tik EŽTK 8 straipsnio pagrindu buvo ginama teisė į asmens duomenų apsaugą[597,598], o Europos Tarybos Ministrų Komitetas šio straipsnio pagrindu priėmė dokumentus dėl asmens duomenų apsaugos[599] nors ir neišskirdamas teisės į asmens duomenų apsaugą kaip savarankiškos teisės. Tačiau galiausiai 108 Konvencijoje, laikomoje EŽTK 8 straipsnio tąsa ir įgyvendinimo priemone[600], buvo tiesiogiai prabilta apie teisę į asmens duomenų apsaugą[601] įpareigojant valstybes nares imtis priemonių įteisinant pagrindinius 108 Konvencijoje nustatytus duomenų apsaugos principus (108 Konvencijos 4 str.). Šie principai skelbia, kad asmens duomenys privalo būti:

1) gauti ir tvarkomi sąžiningai ir teisėtai;
2) saugomi konkrečiam ir teisėtam tikslui ir nenaudojami kitu šiam tikslui prieštaraujančiu būdu;
3) tinkami, svarbūs ir ne pernelyg didelės apimties, kurie atitinka konkrečius tikslus;
4) tikslūs, prireikus papildomi nauja informacija;

---

595 Boehm, *supra note,* 76: 73.

596 Gary LaFree ir Laura Dugan, „Research on Terrorism and Countering Terrorism“, *Crime and Justice: A Review of Research* 38 (2009): 413–78.

597 EŽTK 5, 6, 10 ir 13 str. taip pat yra teisės į asmens duomenų apsaugą elementų (Boehm, *supra note*, 76: 84).

598 Žr., pvz., „Europos Žmogaus Teisių Teismo 1984 m. rugpjūčio 2 d. sprendimas byloje Malone prieš Jungtinę Karalystę (Nr. 8691/79)“, *Hudoc*, žiūrėta 2020 m. rugsėjo 7 d., https://hudoc.echr.coe.int/rus#{%22itemid%22:[%22001-57533%22]}. „Europos Žmogaus Teisių Teismo 1978 m. rugsėjo 6 d. sprendimas byloje Klass ir kiti prieš Vokietiją (Nr. *5029/71*)“, *Hudoc*, žiūrėta 2020 m. rugsėjo 7 d., https://hudoc.echr.coe.int/rus#{%22itemid%22:[%22001-57510%22]}. „Europos Žmogaus Teisių Teismo 1987 m. kovo 26 d. sprendimas byloje Leander prieš Švediją (Nr. 9248/81)“, Hudoc, žiūrėta 2020 m. rugsėjo 7 d., https://hudoc.echr.coe.int/rus#{%22itemid%22:[%22001-57519%22]} .

599 „Europos Tarybos Ministrų Komiteto 1973 m. rugsėjo 26 d. rezoliucija (73) 22 dėl asmenų privatumo apsaugos elektroninių duomenų bankų privačiame sektoriuje atžvilgiu“, *Council of Europe*, žiūrėta 2020 m. rugsėjo 7 d., https://rm.coe.int/1680502830. „Europos Tarybos Ministrų Komiteto 1974 m. rugsėjo 20 d. rezoliucija (74) 29 dėl asmenų privatumo apsaugos elektroninių duomenų bankų viešajame sektoriuje atžvilgiu“, *Council of Europe*, žiūrėta 2020 m. rugsėjo 7 d., https://rm.coe.int/16804d1c51.

600 Boehm, *supra note,* 76: 92.

601 „Konvencija dėl asmenų apsaugos ryšium su asmens duomenų automatizuotu tvarkymu (ETS Nr. 108) su Europos Tarybos Ministrų Komiteto priimtomis pataisomis“, *eSeimas*, žiūrėta 2020 m. rugsėjo 7 d. https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/TAIS.129872.

5) laikomi tokio pavidalo, kad duomenų subjektų tapatybes būtų galima nustatyti ne ilgiau, nei tai yra reikalinga tam tikslui, dėl kurių duomenys buvo saugomi[602];
6) tvarkomi atsižvelgiant į specifines nuostatas, taikomas duomenims, patenkantiems į „specialiųjų asmens duomenų“ kategoriją[603];
7) tvarkomi imantis tinkamų apsaugos priemonių, kurios neleistų jų netyčia ar neteisėtai sunaikinti, netyčia prarasti, neleistinai palikti juos prieinamus, keisti ar platinti[604].
8) patiems duomenų subjektams turi būti suteiktos papildomos garantijos: galimybes nustatyti, ar yra automatizuota asmens duomenų rinkmena, sužinoti ar jų asmens duomenys yra tvarkomi ir kieno, prašyti ištaisyti arba ištrinti jų asmens duomenis, turėti jų teisių gynimo priemonių savo pažeistoms teisėms apginti[605];
9) 108 Konvencijoje įtvirtintų principų taikymas nėra absoliutus: jie gali būti netaikomi[606].

Nepriklausomai nuo to ar jie traktuojami siauriau ar plečiamai, yra laikoma, kad 108 Konvencijoje įtvirtinti principai sudaro asmens duomenų apsaugos teisinio reglamentavimo pamatą Europoje[607] ir galioja automatizuotam asmens duomenų tvarkymui vykdomam visų subjektų: nepriklausomai nuo to ar duomenis tvarko viešas, ar privatus sektorius, įskaitant ir teisėsaugos bei žvalgybos institucijas[608].

2008 m. Europos Tarybai priėmus sprendimą dėl galimybės prie 108 Konvencijos prisijungti ir ne Europos Tarybos narėms[609] bei prie jos 2013 m. prisijungus Urugvajui[610] 108 Konvencija įgijo virš kontinentinį pobūdį, o joje įtvirtinti fundamentiniai principai ir nuostatos oficialiai pradėjo galioti ir už Europos ribų. Nors galima teigti, kad 108 Konvencija viršKontinentinį pobūdį įgijo šiek tiek anksčiau, kadangi ji kaip pavyzdys buvo naudojama Pietų Afrikos asmens duomenų apsaugos sistemos

602 „Konvencija dėl asmenų apsaugos ryšium su asmens duomenų automatizuotu tvarkymu (ETS Nr. 108) su Europos Tarybos Ministrų Komiteto priimtomis pataisomis“, 5 str., *eSeimas*, žiūrėta 2020 m. rugsėjo 7 d. https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/TAIS.129872.

603 „Konvencija dėl asmenų apsaugos ryšium su asmens duomenų automatizuotu tvarkymu (ETS Nr. 108) su Europos Tarybos Ministrų Komiteto priimtomis pataisomis“, 6, 8 ir 10 str., *eSeimas*, žiūrėta 2020 m. rugsėjo 7 d. https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/TAIS.129872.

604 „Konvencija dėl asmenų apsaugos ryšium su asmens duomenų automatizuotu tvarkymu (ETS Nr. 108) su Europos Tarybos Ministrų Komiteto priimtomis pataisomis“, 7 str., *eSeimas*, žiūrėta 2020 m. rugsėjo 7 d. https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/TAIS.129872.

605 „Konvencija dėl asmenų apsaugos ryšium su asmens duomenų automatizuotu tvarkymu (ETS Nr. 108) su Europos Tarybos Ministrų Komiteto priimtomis pataisomis“, 8 str., *eSeimas*, žiūrėta 2020 m. rugsėjo 7 d. https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/TAIS.129872.

606 Modernizuota 108 Konvencija šiuos asmens duomenų apsaugos principus išlaiko, tačiau juos laiko minimaliais, t. y. valstybės narės gali nustatyti griežtesnius asmens duomenų apsaugos standartus.

607 Boehm, *supra note,* 76: 93.

608 „Konvencija dėl asmenų apsaugos ryšium su asmens duomenų automatizuotu tvarkymu (ETS Nr. 108) su Europos Tarybos Ministrų Komiteto priimtomis pataisomis“, 33 str. 1 d., *eSeimas*, žiūrėta 2020 m. rugsėjo 7 d. https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/TAIS.129872.

609 „Accession by States which are not member States of the Council of Europe“, *Council of Europe*, žiūrėta 2015 m. lapkričio 18 d., https://rm.coe.int/16809028a4.

610 „Full List“, *Treaty Office*, žiūrėta 2015 m. lapkričio 18 d., https://www.coe.int/en/web/conventions/full-list.

kūrimui[611]. Tai, viena vertus, patvirtina universalių visam pasauliui asmens duomenų apsaugos principų įtvirtinimo poreikį, kita vertus – būtent Europos Tarybos 108 Konvencijoje įtvirtintų asmens duomenų apsaugos principų pripažinimą pasauliniu lygiu.

Mokslininkai mano, kad 108 Konvencijos tikslus ir kartu Europos pažangą asmens duomenų apsaugos srityje pristabdė tai, kad 108 Konvencija nėra tiesiogiai taikomas teisės aktas[612]. Tačiau tai, kad 108 Konvenciją pasirašė ir ratifikavo 47 Europos Tarybos narės bei ratifikavo 1 ne Europos Tarybos narė[613], rodo ne tik Europos Tarybos valstybių narių, bet ir ne valstybės narės sutikimą ne tik dėl 108 Konvencijos privalomumo, bet ir instrumento, tarptautiniu lygiu suvienodinančio asmens duomenų apsaugą, atsiradimo poreikį. Ilgai pagrindiniu 108 Konvencijos minusu buvo laikoma tai, kad ji nereglamentavo asmens duomenų perdavimo į trečiąsias šalis, nesančias 108 Konvencijos dalyvėmis. Tai iš dalies buvo ištaisyta 2001 m. lapkričio 8 d. ET priėmus papildomą protokolą dėl priežiūros institucijų ir valstybės sienas kertančių duomenų srautų[614] (toliau – 108 Konvencijos papildomas protokolas). Pasak Graham Greenleaf 108 Konvencijos papildomas protokolas buvo pirmasis Europos Tarybos žingsnis link 108 Konvencijos globalizacijos[615]. Atitinkamai tendencingai žiūrint antruoju ET žingsniu link globalizacijos reikėtų laikyti 2008 m. Europos Tarybos sprendimą, suteikiantį teisę prie 108 Konvencijos prisijungti ir ne Europos Tarybos valstybėms narėms[616], trečiuoju – 2012 m. parengtą 108 Konvencijos modernizacijos projektą[617], o ketvirtuoju – sprendimas į Europos Tarybos *ad hoc* asmens duomenų apsaugos komitetą (CAHDATA) stebėtojo teisėmis įtraukti tarptautines arba regionines ne Europoje veikiančias organizacijas: Jungtines Tautas, Amerikos Valstijų Organizaciją (angl. *Organization of American States*), Afrikos Uniją (angl. *African Union*), Vakarų Afrikos Valstybių Ekonominę Bendriją (angl. *Economic Community of West African States*), Šiaurės Azijos Tautų Asociaciją (angl. *Association of Southeast Asian Nations*) ir APEC dėl modernizuotos 108 Konvencijos 22 straipsnio, numatančio sąlygas dėl ne Europos Tarybos narių ir tarptautinių organizacijų prisijungimo prie 108 Konvencijos, svarstymo[618]. Tačiau pati 108 Konvencija yra pakankamai abstrakti, ji detaliai nereglamentuo-

---

611 Ciara Staunton ir kt., „Protection of Personal Information Act 2013 and Data Protection for Health Research in South Africa“, *International Data Privacy Law* 10, no. 2 (May 1, 2020): 160–79, doi:10.1093/idpl/ipz024.

612 Boehm, *supra note,* 76: 92.

613 Urugvajus 108 Konvenciją ratifikavo 2013 m. balandžio 10 d., įsigaliojo – 2013 m. rugpjūčio 1 d. Žr. „Details of Treaty No.108“, *Council of Europe*, žiūrėta 2020 m. rugsėjo 7 d., http://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108.

614 „Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, regarding supervisory authorities and transborder data flows“, *Council of Europe*, žiūrėta 2020 m. rugsėjo 7 d., https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/223.

615 Graham Greenleaf, „'Modernising' Data Protection Convention 108: A Safe Basis for a Global Privacy Treaty?“, *Computer Law & Security Review* 29, no. 4 (August 1, 2013): 2, doi:10.1016/j.clsr.2013.05.015.

616 „Accession by States which are not member States of the Council of Europe“, *Council of Europe*, žiūrėta 2015 m. lapkričio 18 d., https://rm.coe.int/16809028a4.

617 „Council of Europe Data Protection Website“, *Data Protection*, žiūrėta 2015 m. lapkričio 18 d., https://www.coe.int/en/web/data-protection/home.

618 „Convention 108 Bureau of the consultative committee of the convention for the protection of individuals with regard to automatic processing of personal data“, *Council of Europe*, žiūrėta 2020 m. rugpjūčio 14 d., https://rm.coe.int/the-consultative-committee-of-the-convention-for-the-protection-of-ind/168073e153.

ja visuomeninių santykių, suteikia prie jos prisijungusioms valstybėms narėms daug laisvės sprendžiant kaip taikyti ir ar išvis tam tikrais atvejais taikyti 108 Konvenciją ar atitinkamas jos nuostatas ir nebeatitinkanti šiuolaikinio pasaulio aktualijų, kadangi priimta 1981 m. ir pasaulyje labiau vertinama ne dėl jos nuostatų stiprumo, o dėl pačios asmens duomenų apsaugos idėjos teisinės formos suteikimo[619].

Apie 108 Konvencijos modernizavimą viešai buvo prabilta 2010 m.[620]. Modernizavimo priežastimis oficialiai buvo įvardintos dvi: iššūkių, susijusių su technologijų pažanga el. erdvėje sprendimas bei 108 Konvencijos nuostatų tolimesnis vystymasis (tąsa)[621]. 2015 m. balandžio mėn. susirinkęs Europos Tarybos *ad hoc* komitetas dėl asmens duomenų apsaugos (CAHDATA) pateikė Sekretoriatui 108 Konvencijos tekstą su pakeitimais atnaujinimui. Taigi, 2010 m. pradėtas ruošti modernizuotas 108 Konvencijos tekstas vis dar[622] yra svarstymo stadijoje. Tikimasi, kad naujoji 108 Konvencija bus orientuota į savo, kaip globalaus instrumento, statuso pavirtinimą tiek atsižvelgiant į numatytas naujų narių prisijungimo prie 108 Konvencijos procedūras, tiek poratifikacinę stadiją, užtikrinančią, kad naujos narės ne tik formaliai prisijungtų prie 108 Konvencijos, bet ir realiai vykdytų būsimus įsipareigojimus dar prieš prisijungiant prie modernizuotos 108 Konvencijos, tiek į išsamesnį ir griežtesnį asmens duomenų apsaugos visuomeninių santykių reglamentavimą. Manytina, kad realaus 108 Konvencijos įgyvendinimo reikalavimas, įtvirtintas pačiame modernizuotos konvencijos tekste, reikalaus ne tik formalaus jos nuostatų perkėlimo į nacionalinius teisės aktus, bet ir realaus tokių teisės aktų laikymosi[623]. Ar Konvencinio Komiteto, tikrinsiančio naujų narių įsipareigojimų pagal 108 Konvenciją vykdymą, funkcijos tai apims ar apsiribos tik formaliu teisės aktų tikrinu, galutinai paaiškės paskelbus modernizuotos 108 Konvencijos aiškinamąjį memorandumą. Modernizuota 108 Konvencija pasižymi daug išsamesniu nei jos pirmtakė asmens duomenų apsaugos teisinių santykių reglamentavimu, ką galimai įtakojo ne tik, kaip pati Europos Taryba teigia, technologinė pažanga[624], bet ir ES teisinis asmens duomenų apsaugos reglamentavimas bei įvykdyta reforma šioje srityje[625], kadangi tam tikri naujojo reglamentavimo aspektai supanašėjo su ES.

108 Konvencijos nuostatų taikymas užkardant ir tiriant nusikalstamas veikas pasižymi tam tikru specifiškumu, susijusiu su balansavimu tarp individo teisės į asmens duomenų apsaugą ir visuomenės interesų, nacionalinio saugumo užtikrinimu. Tiek

---

619 Alessandro Mantelero, „The Guidelines of the Council of Europe Data Protection Committee on the Protection of Individuals with Regard to the Processing of Personal Data in the Big Data Context Reports: Council of Europe", *European Data Protection Law Review (EDPL)* 3, no. 1 (2017): 88, 89.

620 „Speaking Points for the Deputy Secretary General Opening of the 21st t-PD Bureau Meeting", *Council of Europe*, žiūrėta 2020 m. rugpjūčio 14 d., https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016806869a9

621 *Ibid.,* 2.

622 Disertacijos rašymo metu.

623 Greenleaf, *supra note*, 615: 3.

624 „Convention 108+ : The Modernised Version of a Landmark Instrument", *Council of Europe*, žiūrėta 2020 m. rugsėjo 7 d., https://www.coe.int/en/web/data-protection/newsroom/-/asset_publisher/7oll6Oj8pbV8/content/modernisation-of-convention-108

625 Greenleaf, *supra note*, 615: 3.

iki priimant 108 Konvenciją, tiek vėlesnėje EŽTT praktikoje buvo laikomasi pozicijos, kad asmens teisė į privatumą ir į asmens duomenų apsaugą nėra absoliuti. Ši asmens teisė gali būti proporcingai ribojama siekiant apginti visuomenės interesus[626]. Dėl didėjančio terorizmo pavojaus, narkotikų verslo ir apskritai nusikalstamumo augimo bei galimybės rinkti asmens duomenis vis didesniais mastais nei iki atsirandant internetui pastaroji tapo priversta vis labiau skverbtis į asmens teisės į privatumą erdvę. Todėl, kad būtų užtikrintas balansas tarp atskirų individų teisių, visuomenės interesų ir policijos veiklos renkant ir tvarkant asmens duomenis Europos lygiu ir vienodą teisės į asmens duomenų apsaugą policijos veikloje aiškinimą[627], Europos Tarybos Ministrų Kabinetas priėmė rekomendacijas, kaip valstybės narės turėtų taikyti 108 Konvenciją asmens duomenims tvarkant policijai[628]. Tarybos dokumentu yra Europos Tarybos Ministrų Komiteto 1987 m. rugsėjo 17 d. Rekomendacijos Nr. R(87)15 valstybėms narėms dėl asmens duomenų naudojimo policijos sektoriuje (toliau – ET Rekomendacijos). Ir nors Rekomendacijos nėra privalomo pobūdžio bei priimtos ganėtinai seniai, tačiau jų svarbą Europos asmens duomenų apsaugos teisinėje sistemoje liudija tai, kad ET valstybės narės iki šiol deklaruoja Rekomendacijų laikymąsi[629] bei tai, kad jos tapo ES teisės aktų dėl asmens duomenų naudojimo teisėsaugos sektoriuje pagrindu (pvz. Priumo konvencija, Šengeno instrumentai, Sprendimas dėl Europolo įsteigimo, o mokslininkai šias Rekomendacijas laiko esant vienu iš pagrindinių EŽTK 8 str. įgyvendinimo ir 108 Konvencijos taikymo instrumentų[630] ir iki priimant ES teisėsaugos tikslais tvarkomų asmens duomenų apsaugos direktyvą, Rekomendacijos buvo vienintelis teisės aktu Europoje siekiančiu užtikrinti teisėsaugos vykdomo asmens duomenų rinkimo procedūrų teisėtumą nacionaliniu lygiu. Tačiau pats rekomendacijų pavadinimas kelia klausimą kokiems subjektams ir kokiais atvejais šios rekomendacijos yra taikomos?

Rekomendacijos yra taikomos valstybių narių policijai renkant, laikant, naudojant ir perduodant asmens duomenis[631]. „Policija“ Rekomendacijose yra suprantama kaip „policijos institucijos“, kurių pavadinimai priklausomai nuo valstybių narių nacionalinės teisės gali skirtis. Ne visada yra lengva atskirti ar konkreti institucija gali būti vadinama „policijos institucija“ Rekomendacijų prasme. Todėl Rekomendacijų aiškinamajame memorandume yra nurodoma, kad ar konkreti institucija gali būti laikoma

---

626 Žr. pvz. „Europos Sąjungos Teisingumo Teismo 2010 m. lapkričio 9 d. sprendimas byloje Volker und Markus Schecke GbR and Hartmut Eifert prieš Land Hessen (Nr. C-92/09 ir C-93/09)“, *EUR-Lex*, žiūrėta 2020 m. rugsėjo 7 d., https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62009CJ0092.

627 „Draft Explanatory Memorandum On The Draft Recommendation Regulating The Use Of Personal Data In The Police Sector“, Įžangos 4 p., *Council of Europe*, žiūrėta 2020 m. rugsėjo 7 d., https://rm.coe.int/168062dfd4.

628 „Council of Europe Committee of Ministers Recommendation No. R(87) 15 to the Member States on regulating the use of personal data in the police sector“, *Osce Polis*, žiūrėta 2020 m. rugsėjo 1 d., https://polis.osce.org/council-europe-committee-ministers-recommendation-no-r87-15-member-states-regulating-use-personal.

629 Joseph A. Cannataci ir Mireille M. Caruana, „Coe Report Data Privacy in the Police Sector“, žiūrėta 2020 m. rugsėjo 7 d., https://www.statewatch.org/media/documents/news/2013/oct/coe-report-data-privacy-in-the-police-sector.pdf.

630 Boehm, *supra note,* 76: 96.

631 „Council of Europe Committee of Ministers Recommendation No. R(87) 15 to the Member States on regulating the use of personal data in the police sector“, Scope and Definitios, *Osce Polis*, žiūrėta 2020 m. rugsėjo 1 d., https://polis.osce.org/council-europe-committee-ministers-recommendation-no-r87-15-member-states-regulating-use-personal.

„policija“ Rekomendacijų apimtyje, reikia žiūrėti į tai ar ta institucija atlieka policijos funkcijas renkant, laikant, naudojant ir perduodant asmens duomenis[632]. Ką apima policijos funkcijos Rekomendacijų aiškinamajame memorandume nėra nurodyta. Nors ET valstybės narės teikdamos ataskaitą apie Rekomendacijų įgyvendinimą ET ir nurodė, kad Rekomendacijos taikomos ne tik institucijoms, kurios tiesiogiai vadinamos policija, bet ir kitoms policijos funkcijas atliekančioms institucijoms, Joseph A. Cannataci bei Mireille M. Caruana nurodo, jog visgi nėra aišku kokia apimtimi ir kaip praktiškai Rekomendacijos yra taikomos kitoms valstybių narių institucijoms, atliekančioms policijos funkcijas[633]. Pavyzdžiui, Lietuvoje ikiteisminį tyrimą atlieka ne tik policija, bet ir Valstybės sienos apsaugos tarnyba, Specialiųjų tyrimų tarnyba, Karo policijai, Finansinių nusikaltimų tyrimo tarnyba, Lietuvos Respublikos muitinė, Priešgaisrinės apsaugos ir gelbėjimo departamentas[634]. Jeigu Rekomendacijos turėtų būti taikomos tik policijai, tuomet asmenys, apie kuriuos renkama informacija ikiteisminio tyrimo metu, būti diskriminuojami tuo pagrindu, kad jų teisių apsauga priklausytų nuo to, kokia institucija ikiteisminį tyrimą atlieka. Taigi Rekomendacijos turėtų reglamentuoti visą teisėsaugos institucijų sistemą.

Iš Rekomendacijų ir jų aiškinamojo memorandumo teksto neaišku yra ir ar Rekomendacijos turi būti taikomos žvalgybos institucijoms, tačiau buvo valstybių narių, kurios ataskaitoje ET teigė, kad Rekomendacijas taiko ir saugumo tarnyboms bei kriminalinės žvalgybos institucijoms[635, 636]. Visgi, Rekomendacijose nurodyti asmens duomenų rinkimo tikslai ir principai yra labiau susiję su teisėsaugos nei su žvalgybos veikla. Rekomendacijų priėmimo laikotarpiu – 1987 m. – asmens duomenų rinkimo el. erdvėje reglamentavimas taip pat nebuvo toks aktualus, kaip 2019 m. Todėl teoriškai valstybės gali deklaruoti jų laikymąsi, tačiau kaip praktiškai tas laikymasis užtikrinamas ir kaip yra interpretuojamos nuostatos renkant duomenis el. erdvėje, nėra aišku. Pavyzdžiui, Didžioji Britanija yra ET narė, ji deklaruoja ne tik EŽTK, 108 Konvencijos, bet ir Rekomendacijų laikymąsi. Tačiau 2013 m. E. Snowden atskleidus informaciją masinio asmens duomenų rinkimo programą JAV, paaiškėjo informacija, kad JAV partnere masinio asmens duomenų programoje buvo Didžioji Britanija. Ar tikrai Didžiosios Britanijos masiškai ir nediferencijuojant el. erdvėje surinktus asmens duomenis galime laikyti gautais sąžiningai ir teisėtai, yra retorinis klausimas, į kurį atsakymas yra labiau neigiamas nei teigiamas. Apskritai Rekomendacijose įtvirtinti principai nėra pakankami asmens teisės į asmens duomenų apsaugą užtikrinimui XXI a. egzistuojant

---

632 „Draft Explanatory Memorandum On The Draft Recommendation Regulating The Use Of Personal Data In The Police Sector“, *Council of Europe*, žiūrėta 2020 m. rugsėjo 7 d., https://rm.coe.int/168062dfd4.

633 Cannataci ir Caruana, *supra note*, 629.

634 Lietuvos Respublikos baudžiamojo proceso 165 str. yra numatyta, kad ikiteisminio tyrimo įstaiga yra policija. Ikiteisminio tyrimo įstaigomis taip pat yra Valstybės sienos apsaugos tarnyba, Specialiųjų tyrimų tarnyba, Karo policija, Finansinių nusikaltimų tyrimo tarnyba, Lietuvos Respublikos muitinė, Priešgaisrinės apsaugos ir gelbėjimo departamentas, kai tiriamos nusikalstamos veikos, išaiškėjusios šioms institucijoms atliekant tiesiogines funkcijas, numatytas jų veiklą reglamentuojančiuose įstatymus.

635 Tik kelios valstybės narės nurodė egzistuojant atskirus teisės aktus tokioms institucijoms. Žr. Cannataci ir Caruana, *supra note*, 629.

636 Cannataci ir Caruana, *supra note*, 629: 12.

masiniams asmens duomenų rinkimo mechanizmams ir netgi verslu tapusiomis asmens duomenų rinkimo el. erdvėje technologijoms[637].

Rekomendacijų priėmimo laikotarpiu pačiu svarbiausiu principu buvo laikomas reikalavimas turėti nepriklausomą ir į policijos sektorių neįeinančios priežiūros instituciją, užtikrinančią pamatinių asmens duomenų apsaugos principų laikymąsi[638]. Rekomendacijose numatyta, kad priežiūros institucija turėtų būti įgaliota ne tik kontroliuoti ir prižiūrėti kaip teisėsaugos institucijos tvarko asmens duomenis, bet ir leisti arba neleisti atlikti tam tikrus veiksmus su duomenimis, pavyzdžiui, perduoti asmens duomenis kitiems viešiems ir privatiems asmenims[639]. Priežiūros institucija taip pat gali būti ikiteisminiu duomenų subjektų ginčų su policija nagrinėjimo organu[640]. Tokios institucijos, kuri turėtų ypatingai stiprų vaidmenį ir įtaką teisėsaugos institucijų atžvilgiu ir sugebėtų kontroliuoti jų veiklą nei vienoje valstybėje įkurtos nebuvo. Nors šis principas aktualus ir šiandien, tačiau priežiūros institucija pati savaime, nesant aiškiai įtvirtintų gairių, kada asmens duomenų rinkimą, įskaitant asmens duomenų rinkimą el. erdvėje, galima laikyti teisėtu, nėra tas organas, kuris būtų pajėgus užtikrinti asmens teises. Teisėsaugos vykdomą asmens duomenų rinkimą el. erdvėje turi sankcionuoti teismas, kuris ir vykdo teisingumą. Įsigaliojęs teismo sprendimas negali būti skundžiamas ar kvestionuojamas. Taigi priežiūros institucija gali atsidurti dviprasmiškoje situacijoje, kai iš vienos pusės turėtų vertinti ne teisėsaugos, bet teismo sprendimo pagrįstumą, o iš kitos pusės negalėtų nieko padaryti, nes teismo sprendimo vertinimas būtų jos kompetencijos ribų peržengimas. Teismo sprendimo vykdymo priežiūra būtų įmanoma, bet abejotina asmens teisių užtikrinimo priemonė. Taip pat JAV pavyzdys su *Amicus Curiae* ir FISA teismais rodo, kad asmens duomenų rinkimo el. erdvėje atveju, reali priežiūra yra įmanoma tik tada, kai priežiūros organas turi specialiųjų žinių asmens duomenų rinkimo el. erdvėje technologijose[641]. Nesant šių žinių teisminė ar neteisminė kontrolė yra tik formali.

Rekomendacijų antrasis principas sako, kad policija rinkti gali tik tokius duomenis, kurie yra būtini nusikalstamų veikų prevencijai ir tyrimui bei viešosios tvarkos palaikymui, o ypatingi asmens duomenys gali būti tvarkomi tik jei tai yra būtina konkrečiam nusikalstamos veikos tyrimui. Rekomendacijų aiškinamajame memorandume nurodoma, kad šis principas apima kiekybinį ir kokybinį vertinimą drausdamas

---

[637] Simon Kuper, „Edward Snowden and the Millennial Conscience", *The Financial Times*, 2019, žiūrėta 2020 m. rugsėjo 7 d., https://medium.com/financial-times/edward-snowden-and-the-millennial-conscience-e399803e8323.

[638] „Council of Europe Committee of Ministers Recommendation No. R(87) 15 to the Member States on regulating the use of personal data in the police sector", 1 principas, *Osce Polis*, žiūrėta 2020 m. rugsėjo 1 d., https://polis.osce.org/council-europe-committee-ministers-recommendation-no-r87-15-member-states-regulating-use-personal.

[639] „Council of Europe Committee of Ministers Recommendation No. R(87) 15 to the Member States on regulating the use of personal data in the police sector", 5.2.1 i. a. p., 5.3.1. i. p., *Osce Polis*, žiūrėta 2020 m. rugsėjo 1 d., https://polis.osce.org/council-europe-committee-ministers-recommendation-no-r87-15-member-states-regulating-use-personal.

[640] „Council of Europe Committee of Ministers Recommendation No. R(87) 15 to the Member States on regulating the use of personal data in the police sector", 6.6. p., *Osce Polis*, žiūrėta 2020 m. rugsėjo 1 d., https://polis.osce.org/council-europe-committee-ministers-recommendation-no-r87-15-member-states-regulating-use-personal.

[641] Ben Cook, „The New FISA Court Amicus Should Be Able to Ignore Its Congressionally Imposed Duty", *American University Law Review* 66, no. 2 (January 1, 2017)., https://digitalcommons.wcl.american.edu/aulr/vol66/iss2/5.

neapribotą ir nediferencijuotą tarp objektų asmens duomenų rinkimą[642]. Kas iš esmės reiškia, jog yra draudžiamas masinis nediferencijuotas asmens duomenų rinkimas, kokį pvz. yra žinoma, kad vykdo ne tik JAV, bet ir ET narės. Bet esminis šio principo aspektas yra tai, kad jis, kaip ir Rekomendacijos, taikomas policijos veiklai. Masinis ir nediferencijuotas asmens duomenų rinkimas el. erdvėje paprastai yra vykdomas žvalgybos institucijų. Sudėtine šio principo dalimi yra ir pareiga informuoti to nežinančius asmenis, kad apie juos buvo renkami duomenys, suformuota EŽTT byloje *Leander prieš Švediją*[643]. Paminėtina ir EŽTT byla *S. ir Marper prieš Jungtinę Karalystę,* pateikianti Rekomendacijų antro principo taikymo išaiškinimą. EŽTT laikosi pozicijos, kad išteisintų asmenų tolimesnis duomenų (pirštų atspaudų, DNR profilių ir ląstelių mėginių) saugojimas policijos duomenų bazėse pažeidžia EŽTK 8 straipsnį ir reiškia neproporcingą pareiškėjo teisės į privataus gyvenimo gerbimą ribojimą[644]. Taigi, asmenų prieš kuriuos ikiteisminis tyrimas buvo nutrauktas tolimesnis asmens duomenų saugojimas reikštų neapribotą ir nediferencijuotą asmens duomenų rinkimą, kuris yra draudžiamas pagal Rekomendacijas.

Trečias Rekomendacijų principas numato asmens duomenų saugojimo sąlygas. Kaip nurodoma Rekomendacijų aiškinamajame memorandume, šis principas reikalauja duomenų, pagrįstų faktais atskyrimo nuo nuomone pagrįstų duomenų, bei duomenų, surinktų policijos tikslais, atskyrimo nuo duomenų, surinktų administraciniais tikslais[645]: administraciniais tikslais surinkti duomenys turi būti saugomi atskirame faile ir jiems negali būti taikomos tos taisyklės, kurios taikomos policijos tikslais surinktiems duomenims[646]. Administraciniais tikslais surinktais duomenimis yra laikomi ir komunikacijos el. erdvėje metaduomenys, renkami el. ryšių paslaugų. Ar tai reiškia, kad el. erdvėje surinktiems metaduomenims yra taikomas specialus, mažesnės teisinės apsaugos režimas? Pasak Francizkos Boehm nuo to momento, kai administraciniais tikslais surinkti duomenys (pvz. telekomunikacijų, migracijos) yra perduodami teisėsaugos institucijoms, jiems jau yra taikomos Rekomendacijos[647]. Tokiu pačiu principu buvo vadovaujamasi ir galiojant ES Duomenų saugojimo direktyvai[648], kuri įpareigojo el. ryšių paslaugų teikėjus rinkti ir saugoti duomenis su tikslu, kad tokių

---

642 „Draft Explanatory Memorandum On The Draft Recommendation Regulating The Use of Personal Data in The Police Sector“, 43 p., *Council of Europe*, žiūrėta 2020 m. rugsėjo 7 d., https://rm.coe.int/168062dfd4.

643 „Europos Žmogaus Teisių Teismo 1987 m. kovo 26 d. sprendimas byloje Leander prieš Švediją (Nr. 9248/81)“, *Hudoc*, žiūrėta 2020 m. rugsėjo 7 d., https://hudoc.echr.coe.int/rus#{%22itemid%22:[%22001-57519%22]}.

644 „Europos Žmogaus Teisių Teismo 2008 m. gruodžio 4 d. sprendimas byloje S. ir Marper prieš Jungtinę Karalystę (Nr. 30562/04 ir 30566/04)“, 119 ir 125 p., *Hudoc*, žiūrėta 2020 m. rugsėjo 7 d., https://hudoc.echr.coe.int/fre#{%22itemid%22:[%22001-90051%22]}.

645 „Draft Explanatory Memorandum On The Draft Recommendation Regulating The Use Of Personal Data In The Police Sector“, 53 p., *Council of Europe*, žiūrėta 2020 m. rugsėjo 7 d., https://rm.coe.int/168062dfd4.

646 „Council of Europe Committee of Ministers Recommendation No. R(87) 15 to the Member States on regulating the use of personal data in the police sector“, 3.3. p., *Osce Polis*, žiūrėta 2020 m. rugsėjo 1 d., https://polis.osce.org/council-europe-committee-ministers-recommendation-no-r87-15-member-states-regulating-use-personal.

647 Boehm, *supra note,* 76: 99.

648 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.

duomenų gali ateityje prireikti teisėsaugos ar žvalgybos tikslais, tačiau šių duomenų apsaugai nebuvo taikomi griežtesni reikalavimai.

Svarbu pabrėžti tai, kad Rekomendacijų egzistavimas pats savaime neužtikrina tinkamos asmens duomenų apsaugos tiriant nusikalstamas veikas bei dažnai valstybėms narėms suteikia diskrecijos teisę nuspręsti dėl atitinkamų nuostatų taikymo ribų[649]. EŽTT byloje *Leander prieš Švediją* konstatavo, kad EŽTK 8 straipsnio formuluotė reikalauja nacionalinių teisės aktų, kurie užtikrintų asmens teisę į privatumą[650]. Taigi, Rekomendacijos – tėra tik gairės. Valstybės pačios yra atsakingos, kad Rekomendacijų nuostatas tinkamai perkeltų į nacionalinius teisės aktus. Nesant tokių nacionalinių teisės aktų, jos nėra tiesiogiai taikomos, taigi ir negali būti pažeidžiamos. Tai dar vienas aspektas, įrodantis Rekomendacijų ribotumą ir valstybių galią spręsti kaip interpretuoti Rekomendacijas ir kaip bei kokia apimtimi perkelti į nacionalinius teisės aktus.

Nors ET lygmeniu nėra teisės akto reglamentuojančio žvalgybos vykdomą asmens duomenų rinkimą, po E. Snowden informacijos apie JAV ir jos partnerių vykdomą masinį nediferencijuotą asmens duomenų apie ne JAV asmenis rinkimą el. erdvėje, ET priėmė keletą politinio pobūdžio dokumentų, smerkiančių masinį asmens duomenų rinkimą:

1) 2013 m. Deklaraciją dėl rizikos fundamentinėms teisėms, atsirandančios dėl skaitmeninio sekimo ir kitų asmens duomenų rinkimo el. erdvėje technologijų (angl. *Declaration on Risks to Fundamental Rights stemming from Digital Tracking and other Surveillance Technologies of 2013*). Deklaracijoje ET nurodė, kad „masinio asmens duomenų rinkimo el. erdvėje galimybės ir praktika gali turėti „šaldantį" poveikį piliečių dalyvavimui socialiniame, kultūriniame ir politiniame gyvenime ir ilgalaikėje perspektyvoje – neigiamą poveikį demokratijai. Masinis asmens duomenų rinkimas el. erdvėje taip pat turi neigiamą įtaką konfidencialumui, kuris yra ypač svarbus tam tikrų profesijų atstovams (pvz. žurnalistams). Masinis asmens duomenų rinkimas informacijos šaltinio konfidencialumo užtikrinimą padaro neįmanomu ir sukelia pavojų tiek žurnalistams, tiek jų informacijos šaltiniams"[651];
2) Politinėje deklaracijoje, priimtoje 2013 m. ET Ministrų konferencijoje, atsakingoje už išraiškos laisvės skaitmeninėje visuomenėje užtikrinimą medijoje ir informacinėje visuomenėje (angl. *Political Declaration adopted at the Council of Europe Conference of Ministers responsible for media and information society on freedom of expression and democracy in the digital age (November 2013*) teigiama, kad „turi būti sukurtas adekvatus ir efektyvus žmogaus teisių užtikrinimo mechanizmas kaip atsvara augantiems technologiniams asmens duomenų rinkimo el. erdvėje pajėgumams, kurie gali pakenki ar netgi sunaikinti demokratiją".
3) ET Ministrų komiteto priimtoje 2013 m. Rezoliucijoje Nr. 1 „Dėl interneto saugumo" (angl. *Resolution No. 1 on Internet freedom*) CDMSI įpareigojama išana-

[649] „Council of Europe Committee of Ministers Recommendation No. R(87) 15 to the Member States on regulating the use of personal data in the police sector", 2.1, 3.1, 5.4. ir 5.6 p., *Osce Polis*, žiūrėta 2020 m. rugsėjo 1 d., https://polis.osce.org/council-europe-committee-ministers-recommendation-no-r87-15-member-states-regulating-use-personal.

[650] „Europos Žmogaus Teisių Teismo 1987 m. kovo 26 d. sprendimas byloje Leander prieš Švediją (Nr. 9248/81)", Hudoc, žiūrėta 2020 m. rugsėjo 7 d., 50 p. https://hudoc.echr.coe.int/rus#{%22itemid%22:[%22001-57519%22]}.

[651] „Reply to Recommendation: Recommendation 2067 (2015). Council of Europe Committee of Ministers", *Council of Europe*, žiūrėta 2020 m. rugpjūčio 14 d., http://assembly.coe.int/nw/xml/XRef/Xref-XML2HTML-en.asp?fileid=22234&lang=en.

lizuoti ar žvalgybos vykdomas elektroninės komunikacijos duomenų rinkimas atitinka EŽTK 8 straipsnio nuostatas.

4) 2015 m. Parlamentinės asamblėjos rezoliucija Nr. 2045 (2015), kuria masinį asmens duomenų rinkimą el. erdvėje ET įvardija neefektyvių ir prieštaraujančiu EŽTK 8 str. įtvirtintai teisei į asmens duomenų apsaugą ir demokratinės valstybės principams ir ragina ES ir valstybes nares imtis priemonių, kad būtų sukurtas mechanizmas demokratijos principus užtikrinantis asmens duomenų rinkimas el. erdvėje ir parengti Žvalgybos kodeksą (angl. *Intelligence codex*)[652].

Žvalgybos kodekso (angl. *Intelligence codex*), kaip dokumento, kuris turėtų būti pirmu ET žingsniu užtikrinant EŽTK 8 str. ir 108 Konvencijos nuostatų laikymąsi, vizija buvo išsakyta 2014 m. ET Parlamentinės Asamblėjos susirinkimo metu jame nuotoliniu būdu dalyvaujant ir E. Snowden. Žvalgybos kodeksas (angl. *Intelligence codex*), visų pirma, turėtų reglamentuoti žvalgybos santykius tarp ES ir NATO valstybių narių. Jame turėtų būti įtvirtintos keturios pagrindinės žvalgybos taisyklės:

1) bent kokios formos politinio ar ekonominio šnipinėjimo draudimas;
2) bent kokios formos žvalgybos veiksmai prieš kitą valstybę narę gali būti atliekami tik esant pastarosios sutikimui ir laikantis tos valstybės teritorijoje galiojančių teisės aktų;
3) prieiga prie tarptautinio pobūdžio duomenų judėjimo, nepriklausomai nuo to, kur duomenys būtų perimti, yra leidžiama tik iš anksto numatytiems tikslams (masinio naikinimo ginklų, terorizmo ar kitų sunkių nusikaltimų prevencija) ir turi būti labai griežtai ribojama; neaktualūs perimti duomenys privalo būti nedelsiant sunaikinti;
4) telekomunikacijos ir interneto paslaugų teikėjai negali būti verčiami žvalgybos institucijoms teikti masinių asmens duomenų nesant teismo sankcionavimo.

Tikimasi, kad ET Žvalgybos kodeksą (angl. *Intelligence codex*) taikančioms šalims ir jų piliečiams jis suteiktų užtikrinimą, kad jų duomenys būtų apsaugoti nuo neteisėto naudojimo ne tik pagal nacionalinę, bet ir pagal tarptautinę teisę[653]. Tačiau šis teiginys yra ne visiškai tikslus, kadangi Žvalgybos kodeksą (angl. *Intelligence codex*) taikančių šalių gyventojai būtų apsaugoti tik nuo tų šalių, kurios taip pat taikys Žvalgybos kodekso (angl. *Intelligence codex*) žvalgybos veiksmų el. erdvėje. Tuo tarpu, valstybės, tiek ET, tiek ne ET narės, kurios netaikys Žvalgybos kodekso (angl. *Intelligence codex*), ir toliau rinks duomenis el. erdvėje ir tai bus laikoma teisėta.

2015 m. ET Žvalgybos kodekso (angl. *Intelligence codex*) rengimo poreikiui pritarė ir Ministrų Taryba[654]. Tačiau ne visos valstybės narės sutiko su Žvalgybos kodekso

---

[652] Council of Europe Resolution 2045 (2015). Mass surveillance. 19.4 punktas, žiūrėta 2020 m. rugpjūčio 14 d., https://assembly.coe.int/nw/xml/XRef/Xref-XML2HTML-EN.asp?fileid=21692&lang=en.

[653] „Council of Europe Parliamentary Assembly. Extract from the minutes of the hearing of the Committee on Legal Affairs and Human Rights on Mass Surveillance", *Council of Europe*, žiūrėta 2020 m. rugpjūčio 14 d. https://assembly.coe.int/nw/xml/XRef/Xref-XML2HTML-en.asp?fileid=21583&lang=en.

[654] „Reply to Recommendation: Recommendation 2067 (2015). Council of Europe Committee of Ministers", *Council of Europe*, žiūrėta 2020 m. rugpjūčio 14 d., http://assembly.coe.int/nw/xml/XRef/Xref-XML2HTML-en.asp?fileid=22234&lang=en.

(angl. *Intelligence codex*) priėmimu. Pavyzdžiui, Olandijos vidaus reikalų ministras nurodė, kad toks kodeksas ir jame įtvirtintas draudimas ET valstybėms narėms šnipinėti viena apie kitą ribotų valstybių narių žvalgybos galimybes[655]. Tačiau, reikėtų pastebėti tai, kad būtent ir Olandija, ne vien tik Didžioji Britanija, yra JAV partnerės vykdant masinį asmens duomenų rinkimą[656]. Vadinasi, Olandijos prieštaravimas išryškina ne tik galbūt galimai dėl kodekso priėmimo kilsiančius neigiamus žvalgybos apribojimų padarinius, bet ir tai, kad masinį asmens duomenų rinkimą el. erdvėje vykdančios ET narės greičiausiai neinkorporuos šio kodekso į savo nacionalinę teisę. O jeigu jis nebus visuotinai taikomas, tuomet ir jo tikslas – užtikrinti teisę į asmens duomenų apsaugą kuomet teisėsaugos ir žvalgybos institucijos duomenis renka el. erdvėje – nebus pasiektas. Kol kas Žvalgybos kodekso (angl. *Intelligence codex*) rengimo klausimas ET yra sustabdytas ir masinį asmens duomenų rinkimo ribojimą užtikrinant žmogaus teises ET nori pasiekti bendradarbiaudama su ES[657].

3.2. Europos Sąjungos lygmuo iki asmens duomenų apsaugos reglamentavimo reformos

ES buvo įkurta 1993 m. Teisė į asmens duomenų apsaugą ES atsirado 1995 m. Labiausiai akcentuojama priežastis, dėl kurios ES į savo teisės aktus įtraukė ir teisę į asmens duomenų apsaugą, mokslininkų yra įvardijama informacinių technologijų pažanga[658], sudariusi sąlygas institucijoms tvarkyti asmens duomenis iki tol neregėta apimtimi bei kartu padidinusi ir piktnaudžiavimo asmens duomenų tvarkymu ar klaidų atsiradimo galimybes[659]. Kaip pažymėjo C. Simitis tvarkant duomenis automatiniu būdu, vienoje jų tvarkymo grandyje padaryta klaida nieko apie tą klaidą neįtariančiam ir tarkim vizos, banko paskolos ar darbo prašančiam asmeniui gali sukelti itin skaudžias pasekmes – dėl klaidingų duomenų gaunamą neigiamą atsakymą, o kartu ir ekonominę, politinę ar socialinę diskriminaciją[660]. Tačiau informacinių technologijų pažanga nėra vienintelė priežastis. Šios naujausios ES teisės kilmė siejama ir su viešosios tarptautinės teisės dokumentais[661] bei iš jų kylančiais

---

655 „Dutch government rejects idea of no-spy agreements between European countries“, *Policy Observatory*, žiūrėta 2020 m. rugsėjo 7 d., https://observatory.mappingtheinternet.eu/tags/intelligence%20codex.

656 „Council of Europe Parliamentary Assembly. Extract from the minutes of the hearing of the Committee on Legal Affairs and Human Rights on Mass Surveillance“, *Council of Europe*, žiūrėta 2020 m. rugpjūčio 14 d. https://assembly.coe.int/nw/xml/XRef/Xref-XML2HTML-en.asp?fileid=21583&lang=en.

657 „Reply to Recommendation: Recommendation 2067 (2015). Council of Europe Committee of Ministers“, *Council of Europe*, žiūrėta 2020 m. rugpjūčio 14 d., http://assembly.coe.int/nw/xml/XRef/Xref-XML2HTML-en.asp?fileid=22234&lang=en.
„Dutch government rejects idea of no-spy agreements between European countries“, *Policy Observatory*, žiūrėta 2020 m. rugsėjo 7 d., https://observatory.mappingtheinternet.eu/tags/intelligence%20codex.

658 Boehm, *supra note,* 76: 20.

659 *Ibid.*

660 *Ibid.*

661 „OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data“, *OECD*, žiūrėta 2020 m. rugsėjo 7 d., https://www.oecd.org/internet/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm.

įsipareigojimais[662], ir su pirmosiomis atskirų valstybių narių nacionalinėmis iniciatyvomis[663] leisti teisę į asmens duomenų apsaugą užtikrinančius aktus: Vokietija, Švedija ir Prancūzija buvo pirmosios Europos valstybės, priėmusios nacionalinius teisės aktus dėl asmens duomenų apsaugos dar iki atsirandant tarptautiniams šios teisės užtikrinimo instrumentams[664]. Kaip matome, priežasčių teisei į asmens duomenų apsaugą atsirasti ES buvo keletas, visgi svariausiu indėliu prof. dr. F. Boehm laiko Europos Tarybos indėlį[665], tiesiogiai ES pradėjusį veikti nuo pastarosios įstojimo į Europos Tarybą.

Visos ES valstybės narės būdamos ET narėmis privalėjo 108 Konvenciją perkelti į savo nacionalinius teisės aktus, tačiau kita vertus – 108 Konvencija paliko valstybėms didelę pasirinkimo laisvę dėl jos nuostatų apimties perkėlimo į nacionalinius teisės aktus. Baigdamas diskusijas apie tai ar egzistuojantis tik Europos Tarybos instrumentais grindžiamas asmens duomenų apsaugos režimas ES yra pakankamai efektyvus, o galbūt jį išviso galima laikyti neegzistuojančiu[666], Stokholmo veiksmų programos 2.3. skyrius skelbė, kad plataus pobūdžio nauja asmens duomenų apsaugos schema turi būti sukurta[667]. Iš tikrųjų, santykių tarp ES valstybių narių reglamentavimui asmens duomenų apsaugos srityje 108 Konvencijos nepakako, o ES vidaus rinka, pagrįsta laisvu prekių, paslaugų, asmenų ir kapitalo judėjimu nebūtų galėjusi tinkamai funkcionuoti, jeigu ES lygiu nebūtų imtasi priemonių užtikrinti XXI a. naftos – asmens duomenų – apsaugą. 108 Konvencijos 11 straipsnis, suteikė teisę Europos Tarybos narėms imtis priemonių, kurios sukurtų didesnę duomenų subjektų apsaugą nei ji numatyta 108 Konvencijoje. Priemonė, kuria ES siekė užtikrinti asmens duomenų apsaugą buvo valstybių narių asmens duomenų apsaugą reglamentuojančių teisės aktų harmonizavimas 1995 m. spalio 24 d. Europos Parlamento ir Tarybos direktyvos 95/46/EB dėl asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo (toliau – 1995 m. asmens duomenų apsaugos direktyva)[668] pagalba. Šios direktyvos atsiradimą sąlygojo ES suvokimas, kad nevienodas asmens duomenų apsaugos lygis valstybėse narėse bus kliūtis pamatinių ES laisvių įgyvendinimui. 1995 m. Asmens duomenų apsaugos direktyvos preambulėje buvo skelbiama, kad laisvas prekių, paslaugų, asmenų ir kapitalo judėjimas gali būti užtikrinamas esant galimybei asmens duomenims laisvai judėti iš vienos valstybės narės į kitą bei apsaugant pagrindines asmens teises. Atitinkamai

662 Boehm, *supra note,* 76:19.

663 Vokietijos, Švedijos ir Prancūzijos.

664 Boehm, *supra note,* 76: 20, 21.

665 *Ibid.,* 21.

666 Els De Busser, „EU Data Protection in Transatlantic Cooperation in Criminal Matters Will the EU Be Serving Its Citizens an American Meal?“, *Utrecht Law Review* 6 (January 25, 2010): 87, doi:10.18352/ulr.116.

667 „Europos Vadovų Taryba, Stokholmo veiksmų programa – Atvira ir saugi Europa piliečių labui ir saugumui“, *EUR-Lex,* žiūrėta 2020 m. rugpjūčio 14 d., https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2010:115:0001:0038:LT:PDF.

668 1995 m. spalio 24 d. Europos Parlamento ir Tarybos direktyva (95/46/EB) dėl asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo, 31 str., *EUR-Lex*, žiūrėta 2020 m. rugsėjo 7 d., https://eur-lex.europa.eu/legal-content/LT/TXT/?uri=CELEX%3A31995L0046.

nevienodas asmenų teisių ir laisvių tvarkant asmens duomenis lygis trukdys perduoti šiuos duomenis tarp valstybių narių, bus kliūtimi užsiimant kai kuriomis ekonominės veiklos rūšimis ES lygiu, netgi iškreips konkurenciją ar trukdys valdžios institucijoms vykdyti savo pareigas[669]. Teritoriniu atžvilgiu Asmens duomenų apsaugos direktyva galioja ne tik ES valstybėse narėse, bet ir Europos Ekonominės Bendrijos teritorijoje – Airijoje, Lichtenšteine ir Norvegijoje. Tačiau jeigu 108 Konvencija galioja asmens duomenis tvarkant automatiniu būdu visiems tiek fiziniams, tiek juridiniams asmenims, tiek valstybiniam sektoriui (įskaitant teisėsaugos institucijas)[670], o valstybės narės gali jos galiojimą išplėsti ir juridinio asmens statuso neturintiems subjektams[671] bei kad ji galiotų aukščiau išvardintiems subjektams duomenis tvarkant ir neautomatiniu būdu[672], tai Asmens apsaugos direktyvos galiojimo apimtis yra siauresnė[673]. Fizinių asmenų atžvilgiu ji negaliojo, jeigu fiziniai asmenys duomenis tvarko užsiimdami tik asmenine ar namų ūkio veikla. Ši direktyva taip pat nebuvo taikoma tose srityse kuri nepatenka į Bendrijos teisės taikymo sritį, kuri numatyta Europos Sąjungos sutarties V ir VI dalyse, taip pat kai atliekamos tvarkymo operacijos, susijusios su visuomenės saugumu, gynyba, valstybės saugumu (taip pat ir valstybės ekonomine gerove, kai tvarkymo operacija susijusi su valstybės saugumo klausimais) ir su valstybės veiksmais baudžiamosios teisės srityje[674] – t. y. ji neapėmė laisvės, saugumo ir teisingumo erdvės. Taigi, skirtingai nei 108 Konvencija, Asmens apsaugos direktyva nebuvo taikoma asmens duomenis tvarkant valstybių narių teisėsaugos, teisminėms ir žvalgybos institucijoms. Visgi ši nuostata nėra absoliuti: nedidelis ES valstybių narių skaičius Asmens duomenų apsaugos direktyvos galiojimą nacionaliniuose teisės aktuose buvo išplėtusios iki asmens duomenų apsaugos tiriant nusikalstamas veikas reglamentavimo[675], pati Asmens duomenų apsaugos direktyva nors ir tiesiogiai netaikoma laisvės, saugumo ir teisingumo erdvei, bet buvo laikoma galimu reglamentavimo pavyzdžiu[676], o Europos Sąjungos Teisingumo Teismo (toliau – ESTT) praktika dėl Asmens duomenų

---

669 1995 m. spalio 24 d. Europos Parlamento ir Tarybos direktyva (95/46/EB) dėl asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo, Preambulė, *EUR-Lex*, žiūrėta 2020 m. rugsėjo 7 d., https://eur-lex.europa.eu/legal-content/LT/TXT/?uri=CELEX%3A31995L0046.

670 1995 m. spalio 24 d. Europos Parlamento ir Tarybos direktyva (95/46/EB) dėl asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo, 3 str., *EUR-Lex*, žiūrėta 2020 m. rugsėjo 7 d., https://eur-lex.europa.eu/legal-content/LT/TXT/?uri=CELEX%3A31995L0046.

671 Cannataci ir Caruana, *supra note*, 629: 12.

672 *Ibid.*

673 Asmens duomenų apsaugos direktyva taikoma automatiniais būdais tvarkant asmens duomenis ištisai arba dalimis ir neautomatiniais būdais tvarkant asmens duomenis, kai tie duomenys sudaro arba yra skirti sudaryti rinkmenų sistemos dalį. (1995 m. spalio 24 d. Europos Parlamento ir Tarybos direktyva (95/46/EB) dėl asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo, 3 str. 1 d., *EUR-Lex*, žiūrėta 2020 m. rugsėjo 7 d., https://eur-lex.europa.eu/legal-content/LT/TXT/?uri=CELEX%3A31995L0046)

674 1995 m. spalio 24 d. Europos Parlamento ir Tarybos direktyva (95/46/EB) dėl asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo, 3 str. 2 d., *EUR-Lex*, žiūrėta 2020 m. rugsėjo 7 d., https://eur-lex.europa.eu/legal-content/LT/TXT/?uri=CELEX%3A31995L0046.

675 De Busser, *supra note*, 666: 90.

676 Boehm, *supra note*, 76: 127.

apsaugos taikymo laisvės, saugumo ir teisingumo erdvei buvo įvairi šiuo klausimu. Pavyzdžiui B. Lindqvist byloje [677, 678] ESTT pasisakė, kad Europos Sąjungos sutarties V ir VI antraštinėse dalyse nurodyta veikla bei tvarkymo operacijos, susijusios su visuomenės saugumu, gynyba, valstybės saugumu ir veikla baudžiamosios teisės srityje visais atvejais yra valstybių ar valstybės valdžios institucijų veikla ir tai nėra privačių asmenų veikla“[679]. Tačiau PNR byloje[680] ESTT savo poziciją pakeitė nurodydamas, kad privačių subjektų – oro vežėjų – vykdomas PNR duomenų perdavimas laikytinas tvarkymo operacija, susijusia su visuomenės saugumu ir su valstybės veiksmais baudžiamosios teisės srityje ir todėl patenka į Asmens duomenų apsaugos direktyvos netaikymo išimtį[681].

Asmens duomenų apsaugos direktyva buvo taikoma automatiniais būdais (pvz., informacinėje klientų duomenų bazėje) tvarkomiems asmens duomenims bei duomenims, kurie laikomi arba yra skirti laikyti neautomatinėse kartotekose (tradicinėse popierinėse bylose)[682]. Tačiau jeigu asmens duomenis tvarko ES institucijos, tuomet

---

677 Byloje ginčas kilo dėl to, kad B. Lindqvist, ėjusi rengiančio komunijai asmens pareigas Alsedos (Švedija) parapijoje, namuose savo asmeniniu kompiuteriu sukūrė interneto puslapius, kuriuose viešai skelbė asmens duomenis apie sutvirtinimo sakramentui besirengiančius parapijiečius. B. Lindqvist neinformavo puslapyje aprašytų asmenų apie jo egzistavimą, neprašė jų sutikimo viešai skelbti asmens duomenis ir apie savo veiksmus nepranešė *Datainspektion* (viešosios teisės reglamentuojama kompiuteriais perduodamų duomenų apsaugos įstaiga). Sužinojusi, kad kai kuriems asmenis jos interneto svetainė nepatiko, svetainės panaikino. Prieš B Lindqvist buvo pradėta baudžiamoji byla. Vienas iš klausimų, kurį kėlė nacionalinis Švedijos teismas nagrinėdamas baudžiamąją bylą: ar aplinkybė, kad tokie duomenys apie sakramentui besirengiančius asmenis pateikti privačiame pradiniame puslapyje, kuris prieinamas visiems žinantiems jo adresą, gali būti laikoma nepatenkančia į Asmens duomenų apsaugos direktyvos taikymo sritį pagal kurią nors iš 3 straipsnio 2 dalyje nustatytų išimčių? Atsakydamas dėl pirmosios Asmens duomenų apsaugos direktyvos 3 straipsnio 2 dalyje numatytos išimties, ESTT pasisakė, kad „pirmoje įtraukoje minėti veiklos pavyzdžiai (t. y. Europos Sąjungos sutarties V ir VI antraštinėse dalyse nurodyta veikla bei tvarkymo operacijos, susijusios su visuomenės saugumu, gynyba, valstybės saugumu ir veikla baudžiamosios teisės srityje) visais atvejais yra valstybių ar valstybės valdžios institucijų veikla ir tai nėra privačių asmenų veikla“

678 Europos Sąjungos Teisingumo Teismo 2003 m. lapkričio 3 d. sprendimas byloje C-101/01 Göta hovrätt prieš Bodil Lindqvist, 43 p., *Europa Curia*, žiūrėta 2020 m. rugsėjo 7 d., http://curia.europa.eu/juris/document/document.jsf;jsessionid=9ea7d0f130d59c4626168d7649759faacbd1410d3c1c.e34KaxiLc3eQc40LaxqMbN4Oc3uSe0?text=&docid=48382&pageIndex=0&doclang=LT&mode=lst&dir=&occ=first&part=1&cid=112030

679 *Ibid.*

680 Dėl 2001 m. rugsėjo 11 d. įvykdytų teroristinių išpuolių JAV tų pačių metų lapkričio mėnesį priėmė teisės aktus, nustatančius, kad visi oro vežėjai, vykdantys skrydžius į JAV ir iš jų arba per jų teritoriją tranzitu, turi leisti JAV muitinių įstaigoms elektroniniu būdu susipažinti su kompiuterinėse užsakymų ir išvykimo kontrolės sistemose laikomais duomenimis, vadinamais „passenger name records“ (PNR duomenys). Nors Europos Komisija kreipėsi į JAV teigdama, kad PNR duomenų perdavimas prieštarauja ES teisės aktams, JAV nuo 2003 m. ėmė taikyti sankcijas PNR duomenų neatskleidžiantiems oro vežėjams. ESTT, atsižvelgdamas į tai, kad PNR duomenys bus naudojami tik užkertant kelią terorizmui ir susijusiems nusikaltimams, kitiems tarpvalstybinio pobūdžio sunkiems nusikaltimams, įskaitant organizuotą nusikalstamumą, slėpimuisi nuo arešto ar įkalinimo už minėtus nusikaltimus bei kovai su jais, nusprendė, kad privačių subjektų – oro vežėjų – vykdomas PNR duomenų perdavimas laikytinas tvarkymo operacija, susijusia su visuomenės saugumu ir su valstybės veiksmais baudžiamosios teisės srityje ir todėl patenka į Asmens duomenų apsaugos direktyvos netaikymo išimtį.

681 Europos Sąjungos Teisingumo Teismo 2006 m. gegužės 30 d. sprendimas byloje C-317/04 ir C-318/04 Europos Parlamentas prieš Europos Sąjungos Tarybą ir Europos Bendrijų Komisiją, 55 ir 56 p., *Curia Europa*, žiūrėta 2020 m. rugsėjo 7 d., http://curia.europa.eu/juris/document/document.jsf?text=&docid=57549&pageIndex=0&doclang=LT&mode=lst&dir=&occ=first&part=1&cid=145330.

682 1995 m. spalio 24 d. Europos Parlamento ir Tarybos direktyva (95/46/EB) dėl asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo, *EUR-Lex*, žiūrėta 2020 m. rugsėjo 7 d., https://eur-lex.europa.eu/legal-content/LT/TXT/?uri=CELEX%3A31995L0046.

buvo[683] ir po asmens duomenų apsaugos reformos yra taikomos kitos asmens duomenų apsaugos taisyklės. Šalia bendrąjį asmens duomenų apsaugos reglamentavimą nustatančios Asmens duomenų apsaugos direktyvos bei Reglamento dėl asmenų apsaugos Bendrijos institucijoms ir įstaigoms tvarkant asmens duomenis ir laisvo tokių duomenų judėjimo paminėtinas ir kitas ES instrumentas, atsiradęs dėl masinio elektroninės erdvės naudojimo, t. y. dėl to, kad visuomenei tapo įperkami ir prieinami skaitmeniniai judrieji tinklai, turintys didžiulius pajėgumus ir galimybes tvarkyti asmens duomenis[684] – tai Europos Parlamento ir Tarybos 2002 m. liepos 12 d. 2002/58/EB Direktyva dėl asmens duomenų tvarkymo ir privatumo apsaugos elektroninių ryšių sektoriuje (toliau – Direktyva dėl privatumo ir elektroninių ryšių)[685], pakeičianti ir panaikinanti Direktyvą 97/66/EB[686]. Direktyva dėl privatumo ir elektroninių ryšių suderina valstybių narių nuostatas, užtikrinančias vienodą pagrindinių teisių ir laisvių apsaugos lygį, ypač teisę į privatumą, susijusį su asmens duomenų tvarkymu elektroninių ryšių sektoriuje, ir užtikrinančias laisvą tokių duomenų judėjimą ir laisvą elektroninių ryšių įrangos ir paslaugų judėjimą ES[687]. Direktyva dėl privatumo ir elektroninių ryšių yra ypatingai reikšmingu teisiniu instrumentu šių ryšių plėtrai, nes kaip skalbiama preambulėje, nuo naudotojų pasitikėjimo, kad nėra jokios rizikos jų privatumui, priklauso ir šių paslaugų sėkminga tarpvalstybinė plėtra[688]. Tačiau ji, kaip ir Asmens duomenų apsaugos direktyva, netaikoma veiklos rūšims, kurios neįeina į Europos bendrijos steigimo sutarties

---

683 Asmens duomenų tvarkymą visose ES institucijose reglamentuoja 2000 m. gruodžio 18 d. Europos Parlamento ir Tarybos reglamentas (EB) Nr. 45/2001 dėl asmenų apsaugos Bendrijos institucijoms ir įstaigoms tvarkant asmens duomenis ir laisvo tokių duomenų judėjimo (toliau – Reglamentas dėl asmenų apsaugos Bendrijos institucijoms ir įstaigoms tvarkant asmens duomenis ir laisvo tokių duomenų judėjimo). Šiuo reglamentu nustatomos taisyklės, kuriomis užtikrinamas privatumas ES institucijoms ir įstaigoms tvarkant asmens duomenis, bei apibrėžiamos susijusios piliečių teisės ir įsteigiama Europos asmens duomenų apsaugos priežiūros pareigūno institucija (EDAPP). Europos asmens duomenų priežiūros pareigūno institucija (EDAPP) – tai kontrolinę ir priežiūros funkciją atliekanti institucija stebinti, kaip ES institucijos ir įstaigos taiko asmens duomenų apsaugos taisykles, konsultuojanti rengiant privatumo užtikrinimo strategijas ir šios srities teisės aktus bei bendradarbiaujanti su kitomis panašaus pobūdžio institucijomis, kad būtų užtikrinta nuosekli duomenų apsauga. Tačiau nors Reglamentas dėl asmenų apsaugos Bendrijos institucijoms ir įstaigoms tvarkant asmens duomenis ir laisvo tokių duomenų judėjimo yra taikomas visoms ES institucijoms, t. y. ir veikiančioms laisvės, saugumo ir teisingumo erdvėje, pastarosioms jis taikomas tik tiek, kiek neprieštarauja specifiniam asmens duomenų apsaugos reglamentavimui šioje srityje.

684 1995 m. spalio 24 d. Europos Parlamento ir Tarybos direktyva (95/46/EB) dėl asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo, preambulės 5 p., *EUR-Lex*, žiūrėta 2020 m. rugsėjo 7 d., https://eur-lex.europa.eu/legal-content/LT/TXT/?uri=CELEX%3A31995L0046.

685 2002 m. liepos 12 d. Europos Parlamento ir Tarybos direktyva 2002/58/EB dėl asmens duomenų tvarkymo ir privatumo apsaugos elektroninių ryšių sektoriuje (Direktyva dėl privatumo ir elektroninių ryšių), *EUR-Lex,* https://eur-lex.europa.eu/legal-content/LT/TXT/?uri=CELEX%3A32002L0058.

686 Direktyva dėl privatumo ir elektroninių ryšių suderina valstybių narių nuostatas, užtikrinančias vienodą pagrindinių teisių ir laisvių apsaugos lygį, ypač teisę į privatumą, susijusį su asmens duomenų tvarkymu elektroninių ryšių sektoriuje, ir užtikrinančias laisvą tokių duomenų judėjimą ir laisvą elektroninių ryšių įrangos ir paslaugų judėjimą ES. Direktyva dėl privatumo ir elektroninių ryšių yra ypatingai reikšmingu teisiniu instrumentu šių ryšių plėtrai, nes kaip skalbiama preambulėje, nuo naudotojų pasitikėjimo, kad nėra jokios rizikos jų privatumui, priklauso ir šių paslaugų sėkminga tarpvalstybinė plėtra.

687 1995 m. spalio 24 d. Europos Parlamento ir Tarybos direktyva (95/46/EB) dėl asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo, 1 str. 1 d., *EUR-Lex*, žiūrėta 2020 m. rugsėjo 7 d., https://eur-lex.europa.eu/legal-content/LT/TXT/?uri=CELEX%3A31995L0046.

688 1995 m. spalio 24 d. Europos Parlamento ir Tarybos direktyva (95/46/EB) dėl asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo, preambulės 5 p., *EUR-Lex*, žiūrėta 2020 m. rugsėjo 7 d., https://eur-lex.europa.eu/legal-content/LT/TXT/?uri=CELEX%3A31995L0046.

taikymo sritį, tokioms, kurios nurodytos Europos Sąjungos steigimo sutarties V ir VI antraštinėse dalyse, ir visais atvejais veiklos rūšims, susijusioms su visuomenės saugumu, gynyba, valstybės saugumu (įskaitant valstybės ekonominę gerovę, kai atitinkamos veiklos rūšys yra susijusios su valstybės saugumo klausimais) bei valstybės veiksmais baudžiamosios teisės srityje[689], t. y. ji netaikoma laisvės, saugumo ir teisingumo erdvei.

Taigi, kaip matome, nei vienas iš aukščiau minėtų teisinių ES asmens duomenų apsaugos instrumentų nebuvo taikomas laisvės, saugumo ir teisingumo erdvėje. Kaip tuomet teisė į asmens duomenų apsaugą buvo užtikrinama laisvės, saugumo ir teisingumo erdvėje?

Pagrindinis asmens duomenų apsaugos reglamentavimo ES pagrindinis tikslas – ekonominis: buvusio pirmojo ramsčio ir vidinės rinkos tinkamo funkcionavimo užtikrinimas[690]. Tačiau duomenimis ES visada buvo keičiamasi ir jie yra tvarkomi ne tik buvusio pirmojo ramsčio apimtyje. Jie buvo ir yra tvarkomi ir laisvės, saugumo bei teisingumo erdvėje[691]. Todėl susiklostė dvilypė situacija: nors ES asmens duomenų apsaugos teisinis reglamentavimas yra laikomas vienu griežčiausiu pasaulyje, visgi mokslininkai iš šio teiginio buvo linkę išskirti ES laisvės, saugumo ir teisingumo erdvę, asmens duomenų apsaugos reglamentavimą joje laikydami silpnąja ES vieta[692], kadangi iki asmens duomenų apsaugos reformos asmens duomenų apsaugos reglamentavimas šioje sferoje buvo epizodinis, painus ir neturintis vieningų principų[693]. Pakankamai ilgai ES neturėjo jokio savo asmens duomenų keitimosi ir tvarkymo instrumento laisvės, saugumo ir teisingumo erdvėje, todėl jis buvo vykdomas vadovaujantis ET Rekomendacijomis[694]. Tačiau ET Rekomendacijos buvo neprivalomos ir taikomos tik ta

---

689 1995 m. spalio 24 d. Europos Parlamento ir Tarybos direktyva (95/46/EB) dėl asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo, 1 str. 3 d., *EUR-Lex*, žiūrėta 2020 m. rugsėjo 7 d., https://eur-lex.europa.eu/legal-content/LT/TXT/?uri=CELEX%3A31995L0046.

690 Hielke Hijmans ir Alfonso Scirocco, „Shortcomings in EU Data Protection in the Third and the Second Pillars. Can the Lisbon Treaty Be Expected to Help?“, *Common Market Law Review* 46 (October 1, 2009): 1485.

691 ES sutarties 3 str. 2 d. skelbia, kad „Sąjunga savo piliečiams siūlo vidaus sienų neturinčią laisvės, saugumo ir teisingumo erdvę, kurioje laisvas asmenų judėjimas užtikrinamas kartu taikant atitinkamas išorės sienų kontrolės, prieglobsčio suteikimo, imigracijos ir nusikalstamumo prevencijos bei kovos su juo priemones.“. Laisvės, saugumo ir teisingumo erdvė – tai politinio pobūdžio sąvoka, apimanti keturias sritis: sienų kontrolės, prieglobsčio ir imigracijos politiką, teisminį bendradarbiavimą civilinėse bylose, teisminį bendradarbiavimą baudžiamosiose bylose ir policijos bendradarbiavimą. Laisvės, saugumo ir teisingumo erdvę ES reguliuoja priimdama politinio pobūdžio dokumentus – daugiametes darbo programas. Nors programos nėra teisiškai valstybės narėms privalomi dokumentai, tačiau politiškai jos yra labai svarbios, kadangi jų pagrindu vėliau yra priimami jau valstybėms narėms teisiškai privalomi teisės aktai.

692 Georgia Miller ir Matthew Kearnes, „Nanotechnology, Ubiquitous Computing and The Internet of Things: Challenges to Rights to Privacy and Data Protection Draft Report to the Council of Europe“, 2013, žiūrėta 2020 m. rugpjūčio 14 d., https://rm.coe.int/168067f7f5.

693 Boehm, *supra note,* 76: 107.

694 „Opinion of the European Data Protection Supervisor OJ 2006, C-91/38 on the Proposal for a Council Decision on the establishment, operation and use of the Second Generation Schengen Information System (SIS II) (COM(2005)230 final)“, *EUR-Lex*, žiūrėta 2020 m. rugsėjo 7 d., https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52006XX0419%2801%29. „The Proposal for a Regulation of the European Parliament and of the Council on the establishment, operation and use of the Second Generation Schengen Information System (SIS II) (COM(2005)236 final)“, *EUR-Lex,* žiūrėta 2020 m. rugsėjo 7 d., https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52006XX0419%2802%29. „The Proposal for a Regulation of the European Parliament and of the Council regarding access to the Second Generation Schengen Information System (SIS II) by the services in the Member States responsible for issuing vehicle registration certificates (COM(2005)237 final)“, 6.1. p.., *EUR-Lex*, žiūrėta 2020 m. rugsėjo 7 d., https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52006XX0419(03).

apimtimi, kuria perkeltos į valstybių narių nacionalinius teisės aktus. Savarankiško ES reglamentavimo laisvės, saugumo ir teisingumo erdvėje pradžia tapo teisiškai neprivalomas dokumentas – darbo programa. 2004 m. Hagos programoje ES žengė žingsnį, kuris yra laikomas asmens duomenų apsaugos reglamentavimo ir laisvės, saugumo ir teisingumo erdvėje pradžia[695] ir įtvirtino „tinkamumo principo" privalomumą keičiantis duomenimis tarp valstybių narių teisėsaugos institucijų bei numatė dvišalių susitarimų būtinybę asmens duomenimis keičiantis tarp ES institucijų[696]. Laikotarpiu nuo 2005 m. iki 2008 m. pabaigos Hagos programoje įtvirtinto principo dėka vyko asmens duomenų dalijimasis tarp teisėsaugos institucijų bei sustiprėjo jų bendradarbiavimas[697]. Tačiau 2008 m. įvyko du esminiai reglamentavimo pokyčiai: 1) Lisabonos sutarties[698] 16 straipsnyje buvo tvirtinta teisė į asmens duomenų apsaugą, taikoma ir laisvės saugumo ir teisingumo erdvėje ir 2) buvo priimtas Europos Tarybos Pamatinis Sprendimas Nr. 2008/977/TVR „Dėl asmens duomenų, tvarkomų vykdant policijos ir teisminį bendradarbiavimą baudžiamosiose bylose, apsaugos" (toliau – Asmens duomenų apsaugos pamatinis sprendimas).

Nors Lisabonos sutartyje įtvirtintą teisę į asmens duomenų apsaugą galima laikyti labai abstrakčia, visgi vien tas faktas, kad ši teisė buvo įtvirtinta pirminiame ES teisės akte, taikomame ne tik ES institucijoms[699], bet jau ir jos valstybėms narėms, rodo jog jos reikšmė ES vidaus politikoje didėjo[700]. Prie Lisabonos sutarties pridėtoje 20 deklaracijoje dėl Sutarties dėl Europos Sąjungos veikimo 16 straipsnio yra numatyta pareiga laikytis Asmens duomenų apsaugos direktyvoje numatytų reglamentavimo išimčių nacionalinio saugumo srityje[701]. Žvelgiant dar toliau, 21 deklaracijoje dėl asmens duomenų apsaugos teisminio bendradarbiavimo baudžiamosiose bylose ir policijos bendradarbiavimo srityse buvo sutinkama, kad „dėl teisminio bendradarbiavimo baudžiamosiose bylose ir policijos bendradarbiavimo sričių ypatingo pobūdžio šiose srityse gali reikėti konkrečių taisyklių dėl asmens duomenų apsaugos ir laisvo šių duomenų judėjimo"[702]. Vadinasi, šiomis dvejomis deklaracijomis valstybės narės akivaizdžiai išsaugojo galimybę nacionalinio saugumo ir teisminio bei policijos bendradarbiavimo baudžiamosiose bylose atvejais pagrįstai tikėtis kitokio regla-

---

695 „The Hague Programme Ten priorities for the next five years", *European Commission*, žiūrėta 2020 m. rugsėjo 7 d., https://ec.europa.eu/commission/presscorner/detail/en/MEMO_05_153.

696 *Ibid.*

697 Boehm, *supra note,* 76: 8.

698 Priimta 2008 m.

699 Ankstesnis 286 straipsnis reikalavo asmens duomenų apsaugos tik ES institucijų lygiu.

700 Tai dar labiau patvirtina Lisabonos sutarties 16 straipsnio 2 dalyje numatytas nepriklausomų kontroliuojančių įstaigų buvimo reikalavimas ir bendra Europos Parlamento ir Tarybos teisės aktų priėmimo procedūra, pakeičianti iki tol numatytą taikyti parastą teisės aktų priėmimo procedūrą.

701 „20. Deklaracija dėl Sutarties dėl Europos Sąjungos veikimo 16 straipsnio", *EUR-Lex*, žiūrėta 2020 m. rugsėjo 7 d., https://eur-lex.europa.eu/legal-content/LT/TXT/?uri=CELEX:12016L/AFI/DCL/20.

702 „21.Deklaracija dėl asmens duomenų apsaugos teisminio bendradarbiavimo baudžiamosiose bylose ir policijos bendradarbiavimo srityse", *EUR-Lex*, žiūrėta 2020 m. rugpjūčio 14 d., https://eur-lex.europa.eu/legal-content/LT/TXT/?uri=CELEX:12016L/AFI/DCL/21.

mentavimo nei bendros rinkos, pinigų sąjungos, bendrosios žemės ūkio politikos, struktūrinės politikos ir kitos ekonominės integracijos tikslais. O trys ES valstybės narės – Jungtinė Karalystė, Airija ir Danija– pasirašė protokolus, kuriuose išreiškė savo poziciją, kad jos apskritai atsisako taikyti ES teisės aktus, priimtus laisvės, saugumo ir teisingumo erdvėje[703]. Todėl, šios valstybės narės galėjo nesaugoti asmens duomenų laisvės, saugumo ir teisingumo erdvėje arba turėti savitą reglamentavimą, kuris labai skyrėsi nuo ES reglamentavimo. Prie harmonizuoto ir vieningo asmens duomenų reglamentavimo neprisidėjo ir Lisabonos sutarties 36 protokolo 9 straipsnio nuostata, numatanti, jog ES institucijų, organų ir įstaigų aktai, priimti iki Lisabonos sutarties, išlieka galioti iki bus panaikinti, anuliuoti ar pakeisti[704]. Kaip pažymi P. Boehm iki Lisabonos sutarties priėmimo buvo priimta daugybė abejotinų teisės aktų dėl asmens duomenų apsaugos buvusio trečiojo ramsčio srityje[705], tame tarpe ir Europolo bei Eurojusto sprendimai (pvz. leidžiantys teisėsaugos institucijomis naudotis VIS duomenimis)[706]. Tokiu būdu, nesant vieningos ne tik valstybių narių, bet ir pačių ES institucijų pozicijos, tik iš dalies buvo įmanoma harmonizuoti asmens duomenų apsaugos reglamentavimą laisvės, saugumo ir teisingumo erdvėje. Pirmoji daugeliu aspektų dalinio harmonizavimo priemonė – tai Asmens duomenų apsaugos pamatinis sprendimas.

Asmens duomenų apsaugos pamatinio sprendimo tikslas – užtikrinti fizinių asmenų asmens duomenų apsaugą, kai jų asmens duomenys tvarkomi nusikalstamos veikos prevencijos, tyrimo, nustatymo ar patraukimo už šią veiką baudžiamojon atsakomybėn arba bausmių vykdymo tikslais[707]. Asmens duomenų apsaugos pamatinis sprendimas atitiko 108 Konvencijoje ir Asmens duomenų apsaugos direktyvoje įtvirtintas pamatines asmens duomenų apsaugos nuostatas. Juo buvo siekiama tiesiog detaliau reglamentuoti probleminius tarptautinio bendradarbiavimo perduodant asmens duomenis aspektus tokiu būdu didinant kompetentingų institucijų tarpusavio pasitikėjimą, užtikrinant informacijos apsaugą ir išvengiant diskriminacijos valstybių narių bendradarbiavimo atžvilgiu[708]. Asmens duomenų apsaugos pamatiniame sprendime buvo įtvirtinta ne tik asmens duomenų perdavimo ES viduje skirtingų valstybių narių

---

[703] „Protokolas (Nr. 21) dėl Jungtinės Karalystės ir Airijos pozicijos dėl laisvės, saugumo ir teisingumo erdvės“, *EUR-Lex*, žiūrėta 2020 m. rugpjūčio 14 d., https://eur-lex.europa.eu/legal-content/LT/TXT/?uri=CELEX%3A12012E%2FPRO%2F21. „Protokolas (Nr. 22) dėl Danijos pozicijos“, *EUR-Lex*, žiūrėta 2020 m. rugpjūčio 14 d., https://eur-lex.europa.eu/legal-content/LT/TXT/?uri=CELEX%3A12012E%2FPRO%2F22.

[704] „Protokolas (Nr. 36) dėl pereinamojo laikotarpio nuostatų“, *EUR-Lex*, žiūrėta 2020 m. rugpjūčio 14 d., https://eur-lex.europa.eu/legal-content/LT/TXT/?uri=CELEX:12008M/PRO/36.

[705] Boehm, *supra note,* 76: 119.

[706] „Regulation (EC) No 767/2008 of the European Parliament and of the Council of 9 July 2008 concerning the Visa Information System (VIS) and the exchange of data between Member States on short-stay visas (VIS Regulation)“, *EUR-Lex*, žiūrėta 2020 m. rugpjūčio 14 d., https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=celex%3A32008R0767.

[707] „2008 m. lapkričio 27 d. Tarybos pamatinis sprendimas 2008/977/TVR dėl asmens duomenų, tvarkomų vykdant policijos ir teisminį bendradarbiavimą baudžiamosiose bylose, apsaugos“, 6 p., *EUR-Lex*, žiūrėta 2020 m. rugpjūčio 14 d., https://eur-lex.europa.eu/legal-content/LT/ALL/?uri=celex%3A32008F0977.

[708] „2008 m. lapkričio 27 d. Tarybos pamatinis sprendimas 2008/977/TVR dėl asmens duomenų, tvarkomų vykdant policijos ir teisminį bendradarbiavimą baudžiamosiose bylose, apsaugos“, preambulės 5 p., *EUR-Lex,* žiūrėta 2020 m. rugpjūčio 14 d., https://eur-lex.europa.eu/legal-content/LT/ALL/?uri=celex%3A32008F0977.

kompetentingoms institucijoms arba informacinėms sistemoms, bet ir bendradarbiavimo su trečiosiomis šalimis principai[709].

Šis pamatinis sprendimas buvo priimtas įgyvendinant ES sutarties 30 (1) straipsnį (pakeistą 87 ir 88 straipsniais), reikalaujantį, kad teisėsaugos institucijos duomenis rinktų ir jais dalintųsi užtikrinant tinkamą jų apsaugą. Tačiau Asmens duomenų apsaugos pamatinis sprendimas nebuvo skirtas taikyti nacionaliniu lygiu. Jis buvo taikomas tik tarp valstybių narių persiųstų asmens duomenų ar duomenų, kuriais naudotis sudaryta galimybė, tvarkymui[710]. Tokiu būdu didžiausia ES asmens duomenų apsaugos teisinio reglamentavimo spraga buvo būtent tai, kad ES lygiu nebuvo galiojančių teisės aktų, reglamentuojančių asmens duomenų apsaugą teisėsaugos institucijoms užkardant ir tiriant nusikalstamas veikas valstybės lygmeniu. Iki asmens duomenų apsaugos reformos ES tai buvo palikusi spręsti kiekvienai valstybei narei savarankiškai, žinoma, nepažeidžiant 108 Konvencija prisiimtų įsipareigojimų. Taigi, atsižvelgiant į tai, kad Europos Tarybos asmens duomenų apsaugos instrumentai – 108 Konvencija ir Rekomendacijos – valstybėms narėms suteikia daug laisvės, iš būtent dėl šios suteiktos laisvės reglamentavimas yra pakankamai skirtingas, vadinasi ir valstybės narės nebuvo įpareigotos ir net neturėjo įrankio užtikrinti vieningos asmens duomenų apsaugos laisvės, saugumo ir teisingumo erdvėje. Tokiu būdu prie Asmens duomenų apsaugos pamatinio sprendimo ES asmens duomenų apsaugos laisvės, saugumo ir teisingumo srityje galiojo ir 27 skirtingi nacionaliniai reglamentavimai arba to reglamentavimo nebuvimas ir valstybėse narėse.

Kadangi rinkdamos ir tvarkydamos asmens duomenis valstybių narių teisėsaugos institucijos dažniausiai iš anksto nežinojo, kad iškils būtinybė jais keistis tarptautiniu lygiu, todėl H. Hijmans ir A. Scirocco kėlė klausimą, kaip ši Asmens duomenų apsaugos pamatinio sprendimo taikymo išimtis buvo taikoma praktikoje egzistuojant skirtingam nacionaliniam asmens duomenų tvarkymo, atliekamo teisėsaugos institucijų, reglamentavimui[711]. Antras Asmens duomenų apsaugos pamatinis sprendimo taikymo probleminis aspektas buvo tas, kad nuo 2005 m. jis nebuvo taikomas visam asmens duomenų keitimuisi ir tarp ne nacionalinių teisėsaugos institucijų. Jeigu keitimasis asmens duomenis vyksta vadovaujantis Priumo sprendimu, reglamentuojančiu tarptautinį keitimąsi DNR duomenimis, tuomet buvo vadovaujamasi Priumo sprendimo, o ne Asmens duomenų apsaugos pamatinio sprendimo nuostatos.

---

[709] Duomenų tvarkymo teisėtumo, proporcingumo ir tikslo, nuostatos dėl persiunčiamų duomenų kokybės patikrinimo, duomenų saugojimo terminų, registravimo ir dokumentavimo, nacionalinių asmens duomenų tvarkymo apribojimo laikymosi, duomenų subjekto informavimo, duomenų subjekto teisių, duomenų subjektų teisių apribojimo pagrindai, duomenų subjekto teisių gynimo priemonės, asmens duomenų tvarkymo konfidencialumo, saugumo, išankstinės konsultacijos su kompetentingomis nacionalinėmis priežiūros institucijomis prieš asmens duomenis įtraukiant į naują rinkmenų sistemą, sankcijų, taikomų pažeidus pagal Asmens duomenų apsaugos pamatinį sprendimą priimtų teisės aktų nuostatas ir nacionalinės priežiūros institucijų veiklos.

[710] „2008 m. lapkričio 27 d. Tarybos pamatinis sprendimas 2008/977/TVR dėl asmens duomenų, tvarkomų vykdant policijos ir teisminį bendradarbiavimą baudžiamosiose bylose, apsaugos“, 7 p., *EUR-Lex*, žiūrėta 2020 m. rugpjūčio 14 d., https://eur-lex.europa.eu/legal-content/LT/ALL/?uri=celex%3A32008F0977.

[711] „2008 m. lapkričio 27 d. Tarybos pamatinis sprendimas 2008/977/TVR dėl asmens duomenų, tvarkomų vykdant policijos ir teisminį bendradarbiavimą baudžiamosiose bylose, apsaugos“, 115 p. *EUR-Lex*, žiūrėta 2020 m. rugpjūčio 14 d., https://eur-lex.europa.eu/legal-content/LT/ALL/?uri=celex%3A32008F0977.

Nors ir įvairi, tačiau tai buvo ne vienintelė asmens duomenų apsaugos reglamentavimo laisvės, saugumo ir teisingumo erdvėje specifika. Šalia Asmens duomenų apsaugos pamatinio sprendimo, neharmonizuoto valstybinių narių vidinio asmens duomenų tvarkymo reglamentavimo, egzistavo ir atskiras, ir priešingai ES pozicijos valstybių narių atžvilgiu, ypatingai griežtas asmens duomenų apsaugos teisinis režimas, taikomas ES institucijoms, padedančioms užtikrinti tarpvalstybinį teisėsaugos institucijų bendradarbiavimą: Europos policijos biurui (toliau – Europolas), ES teisminio bendradarbiavimo padaliniui (toliau – Eurojustas).

Griežta asmens duomenų apsauga tokioms institucijoms, teigiama, yra svarbi dėl to, kad jos pačios neatlieka nusikalstamų veikų tyrimo[712], tačiau savo veikloje naudojasi valstybių narių perduotais duomenimis. Taigi ES siekė, jog valstybės narės visiškai pasitikėtų minėtomis institucijomis ir jaustųsi saugios perduodamos joms duomenis, būtinus šių institucijų veiklai[713]. Todėl tiek Europole, tiek Eurojuste yra įtvirtintas keliapakopio reglamentavimo asmens duomenų apsaugos teisinis režimas. Visų pirma, asmens duomenų perdavimas tarp Europolo ir Eurojusto ir valstybių narių vykdomas laikantis ES teisės aktų[714]. Antra, Į Europolo ir Eurojusto duomenų bazes patekusių asmens duomenų apsaugai yra taikomi 108 Konvencijoje ir Rekomendacijoje numatyti principai, susiję su automatiniu ir neautomatiniu asmens duomenų tvarkymu[715]. Galiausiai, specifiniai Europolo asmens duomenų apsaugos klausimai yra reglamentuojami tiesiogiai 2009 m. balandžio 6 d. Tarybos sprendime dėl Europos policijos biuro (Europolo) įsteigimo[716], Eurojusto – Asmens duomenų saugojimo ir tvarkymo taisyklėmis ir procedūromis (2005/C 68/01) ir Papildomomis taisyklėmis apibrėžiančius kai kuriuos specifinius asmens duomenų tvarkymo ir saugojimo aspektus dėl ne su Eurojusto veikla susijusių operacijų. Europolo asmens duomenų apsaugos sistema yra paremta nepriklausoma asmens duomenų apsaugos priežiūra, didelėmis Europolo saugios informacijos keitimosi galimybėmis, asmens duomenų apsaugos reikalavimų laikymosi reikalavimo iš privataus sektoriaus ir aiškiai apibrėžtomis asmens duomenų tvarkymo operacijomis[717]. Dėl ypatingo dėmesio asmens duomenų apsaugai, tiek Europolas, tiek Eurojustas savo asmens duomenų apsaugos sistemas laiko vienomis iš stipriausių teisėsaugos taikomų asmens duomenų apsaugos sistemų pasaulyje[718,719].

---

712 Daniel Drewer ir Jan Ellermann, „Europol's Data Protection Framework as an Asset in the Fight against Cybercrime", *ERA Forum* 13, no. 3 (November 1, 2012): 2, doi:10.1007/s12027-012-0268-6.

713 *Ibid.,* 3.

714 Frank Cali, „Europol's Data Protection Mechanisms: What Do They Know and Whom Are They Telling", *Touro International Law Review,* 10 (2000): 189–240.

715 „2009 m. balandžio 6 d. Tarybos sprendimas dėl Europos policijos biuro (Europolo) įsteigimo", *EUR-Lex*, žiūrėta 2020 m. rugpjūčio 14 d., https://eur-lex.europa.eu/legal-content/lt/TXT/?uri=CELEX%3A32009D0371.

716 *Ibid*.

717 „Europol Review 2013", 89, *European Police Office*, žiūrėta 2020 m. rugpjūčio 14 d., https://www.europol.europa.eu/activities-services/main-reports/europol-review-2013 .

718 *Ibid*.

719 „Data protection at Eurojust, *Eurojust*, žiūrėta 2020 m. rugsėjo 10 d., http://www.eurojust.europa.eu/Practitioners/Data-Protection/Pages/Data-protection-at-Eurojust.aspx.

Keitimasis valstybių narių turima informacija, apimančia asmens duomenis, specifinėse nusikalstamų veikų tyrimo srityse ES lygiu taip pat buvo reglamentuojamas ir kitais teisės aktais, papildančiais galiojančias bendrąsias asmens duomenų apsaugos taisykles, įtvirtintas aukščiau šiame skyriuje minėtuose ES teisės aktuose. Tarp šių teisės aktų – Tarybos pamatinis sprendimas 2009/315/TVR dėl valstybių narių keitimosi informacija iš nuosprendžių registro organizavimo ir turinio[720] ir Tarybos sprendimas 2000/642/TVR dėl valstybių narių finansinės žvalgybos padalinių bendradarbiavimo susitarimų dėl keitimosi informacija[721]. Pirmasis iš jų skirtas pagerinti keitimąsi informacija apie ES piliečiams priimtus apkaltinamuosius nuosprendžius ir apkaltinamuoju nuosprendžiu skirtos teisės dirbti tam tikrą darbą ar užsiimti tam tikra veikla atėmimą, jei tokia bausmė buvo skirta ir įregistruota apkaltinamąjį nuosprendį priėmusios valstybės narės nuosprendžių registre[722]. Antrasis – užtikrinti valstybių narių finansinės žvalgybos padalinių bendradarbiavimą renkant, analizuojant ir tiriant atitinkamą informaciją šiuose padaliniuose dėl kiekvieno fakto, kuris galėtų būti pinigų plovimo požymiu[723]. Kitas svarbus institucionalizuoto tarpvalstybinio bendradarbiavimo keičiantis nacionaliniais duomenimis pavyzdys yra Tarybos sprendimas 2008/615/TVR dėl tarpvalstybinio bendradarbiavimo gerinimo, visų pirma kovos su terorizmu ir tarpvalstybiniu nusikalstamumu srityje (toliau – Priumo sprendimas) [724], kuriuo į ES teisę 2008 m. įtraukta Priumo sutartis[725,726]. Priumo sprendimo tikslas – padėti valstybėms narėms pagerinti dalijimąsi informacija siekiant vykdyti nusikaltimų prevenciją ir kovoti su jais trijose srityse: terorizmo, tarpvalstybinio nusikalstamumo ir nelegalios migracijos. Šiuo tikslu sprendime įtvirtinamos nuostatos, susijusios su: 1) DNR profilių, pirštų atspaudų duomenų ir tam tikrų nacionalinių transporto priemonių registracijos duomenų automatinio perdavimo sąlygomis, 2) duomenų, susijusių su didelio masto tarpvalstybinio pobūdžio renginiais, teikimu, 3) informacijos teikimu teroristinių nu-

---

720 „2009 m. vasario 26 d. Tarybos pamatinis sprendimas 2009/315/TVR dėl valstybių narių keitimosi informacija iš nuosprendžių registro organizavimo ir turinio“, *EUR-Lex*, žiūrėta 2020 m. rugpjūčio 15 d., https://eur-lex.europa.eu/legal-content/LT/TXT/?uri=CELEX:32009F0315.

721 „2000 m. spalio 17 d. Tarybos sprendimas 2000/642/TVR dėl valstybių narių finansinės žvalgybos padalinių bendradarbiavimo susitarimų dėl keitimosi informacija“, *EUR-Lex*, žiūrėta 2020 m. rugpjūčio 15 d., https://eur-lex.europa.eu/legal-content/LT/TXT/HTML/?uri=CELEX:32000D0642&from=EN.

722 „2009 m. vasario 26 d. Tarybos pamatinis sprendimas 2009/315/TVR dėl valstybių narių keitimosi informacija iš nuosprendžių registro organizavimo ir turinio“, 6 p., *EUR-Lex*, žiūrėta 2020 m. rugpjūčio 15 d., https://eur-lex.europa.eu/legal-content/LT/TXT/?uri=CELEX:32009F0315.

723 „2000 m. spalio 17 d. Tarybos sprendimas 2000/642/TVR dėl valstybių narių finansinės žvalgybos padalinių bendradarbiavimo susitarimų dėl keitimosi informacija“, *EUR-Lex*, žiūrėta 2020 m. rugpjūčio 15 d., https://eur-lex.europa.eu/legal-content/LT/TXT/HTML/?uri=CELEX:32000D0642&from=EN.

724 „2008 m. birželio 23 d. Tarybos sprendimas 2008/615/TVR dėl tarpvalstybinio bendradarbiavimo gerinimo, visų pirma kovos su terorizmu ir tarpvalstybiniu nusikalstamumu srityje“, *EUR-Lex*, žiūrėta 2020 m. rugpjūčio 15 d., https://eur-lex.europa.eu/legal-content/LT/TXT/?uri=celex%3A32008D0615.

725 Belgijos Karalystės, Vokietijos Federacinės Respublikos, Ispanijos Karalystės, Prancūzijos Respublikos, Liuksemburgo Didžiosios Hercogystės, Nyderlandų Karalystės ir Austrijos Respublikos konvencija dėl tarpvalstybinio bendradarbiavimo gerinimo, visų pirma kovos su terorizmu, tarpvalstybiniu nusikalstamumu ir neteisėta migracija; galima rasti adresu http://register.consilium.europa.eu/pdf/en/05/st10/st10900.en05.pdf.

726 Priumo sutartis – 2005 m. Austrijos, Belgijos, Prancūzijos, Vokietijos, Liuksemburgo, Nyderlandų ir Ispanijos pasirašytas tarptautinis policijos bendradarbiavimo susitarimas.

sikaltimų tyrimo tikslais, 4) tarpvalstybinio policijos bendradarbiavimo gerinimu[727]. Duomenų bazėms, kuriomis galima pasinaudoti remiantis Priumo sprendimu, išimtinai taikoma nacionalinė teisė, tačiau keitimąsi duomenimis reglamentuoja Priumo sprendimas ir Duomenų apsaugos pamatinis sprendimas[728]. Už tokių duomenų srautų priežiūrą atsakingos yra nacionalinės duomenų apsaugos priežiūros institucijos[729].

ES valstybės narės ir ES institucijos, kovojančios su tarpvalstybiniu nusikalstamu gali ne tik keistis duomenimis tiesiogiai tarpusavyje, bet ir šiais duomenimis keistis per informacines sistemas. Konkrečiai, per Šengeno informacinę sistemą[730], Vizų nformacinę sistemą[731], EURODAC sistemą[732], EUROSUR sistemą[733] ir Muitinės

---

727 „2008 m. birželio 23 d. Tarybos sprendimas 2008/615/TVR dėl tarpvalstybinio bendradarbiavimo gerinimo, visų pirma kovos su terorizmu ir tarpvalstybiniu nusikalstamumu srityje“, 1 str., *EUR-Lex*, žiūrėta 2020 m. rugpjūčio 15 d., https://eur-lex.europa.eu/legal-content/LT/TXT/?uri=celex%3A32008D0615.

728 2008 m. birželio 23 d. Tarybos sprendimas 2008/615/TVR dėl tarpvalstybinio bendradarbiavimo gerinimo, visų pirma kovos su terorizmu ir tarpvalstybiniu nusikalstamumu srityje, 2 str., *EUR-Lex*, žiūrėta 2020 m. rugpjūčio 15 d., https://eur-lex.europa.eu/legal-content/LT/TXT/?uri=celex%3A32008D0615.

729 2008 m. birželio 23 d. Tarybos sprendimas 2008/615/TVR dėl tarpvalstybinio bendradarbiavimo gerinimo, visų pirma kovos su terorizmu ir tarpvalstybiniu nusikalstamumu srityje, 27 str., *EUR-Lex*, žiūrėta 2020 m. rugpjūčio 15 d., https://eur-lex.europa.eu/legal-content/LT/TXT/?uri=celex%3A32008D0615.

730 Šengeno informacinę sistemą – SIS II – sudaro centrinė sistema (C-SIS), nacionalinės sistemos (N-SIS) ir ryšių perdavimo tarp centrinės sistemos ir nacionalinių sistemų infrastruktūra. Šios sistemos tikslas yra aukšto lygio saugumo užtikrinimas ES laisvės, saugumo ir teisingumo erdvėje, įskaitant visuomenės saugumo ir viešosios tvarkos bei saugumo palaikymą valstybių narių teritorijose. Siekiant šio tikslo SIS II yra kaupiama informacija apie valstybių narių piliečius, dėl kurių yra pateiktas perspėjimas ir apie daiktus. Nuo 2007 m. šalia kitų asmens duomenų SIS II informacinėje sistemoje yra kaupiami ir tokie asmens duomenys kaip pirštų antspaudai ir nuotraukos. Tačiau jei iki 2007 m. Šengeno informacinėje sistemoje kaupiamų asmens duomenų apsauga buvo nereglamentuojama, tai nuo 2007 m. Tarybos sprendimu 2007/533/TVR dėl antrosios kartos Šengeno informacinės sistemos sukūrimo, veikimo ir naudojimo į SIS II įtraukiama 108 Konvencija bei Rekomendacijos tokiu būdu SIS II suteikiant Europos Tarybos nustatytą asmens duomenų apsaugos lygį.

731 Vizų informacinė sistema – VIS –, kurią kaip ir SIS II sudaro centrinė vizų sistema (CS VIS), nacionalinės sąsajos (NI-VIS) bei CS-VIS nei NI-VIS komunikacijų infrastruktūros buvo sukurta siekiant pagerinti ES vizų politikos įgyvendinimą. Ir jei SIS II yra tvarkomi valstybių narių piliečių asmens duomenys, tai VIS tvarkomi duomenys, susiję su trečiųjų šalių asmenų prašymais dėl trumpalaikių vizų apsilankymo Šengeno erdvėje arba šios erdvės kirtimo tikslais. Nors VIS esanti informacija visada buvo svarbi kovojant su terorizmu ir kitokio pobūdžio tarptautiniu nusikalstamumu, tačiau iki 2008 m. valstybių narių policijos institucijos ir ES institucijos, kovojančios su tarpvalstybiniu nusikalstamumu, neturėjo teisės naudotis VIS esančiais duomenimis. ES Tarybai nusprendus, kad „norint visiškai pasiekti tikslą didinti vidaus saugumą ir gerinti kovą su terorizmu“, už vidaus saugumą atsakingoms valstybės narės institucijoms bei Europolui, „vykdant savo pareigas, susijusias su baudžiamųjų nusikaltimų, įskaitant teroro aktus ir terorizmo grėsmę, prevencija, atskleidimu ir tyrimu“, turėtų būti suteikta teisė naudotis VIS, „griežtai laikantis asmens duomenų apsaugą reglamentuojančių taisyklių“. Taisyklės, kurias ES Taryba įpareigojo laikytis valstybes nares – analogiškai SIS II – 108 Konvencija bei Rekomendacijos, tokiu būdu VIS taip pat suteikiant Europos Tarybos nustatytą asmens duomenų apsaugos lygį.

732 EURODAC sistema – tai centralizuota sistema, kurioje pateikiami trečiųjų valstybių piliečių, teikiančių prašymus dėl prieglobsčio vienoje iš ES valstybių narių, pirštų atspaudų duomenys. EURODAC sistemos tikslas yra padėti nustatyti, kuri valstybė narė turėtų būti atsakinga už konkretaus prieglobsčio prašymo nagrinėjimą pagal Tarybos reglamentą (EB) Nr. 343/2003, nustatantį valstybės narės, atsakingos už trečiosios šalies piliečio vienoje iš valstybių narių pateikto prieglobsčio prašymo nagrinėjimą, nustatymo kriterijus ir mechanizmus (Dublino II reglamentas). Nors EURODAC buvo įsteigta 2003 m., tačiau net iki 2015 m. liepos mėn. nei valstybių narių teisėsaugos institucijos, nei Europolas neturėjo prieigos prie EURODAC sistemoje saugomų asmens duomenų. 2015 m. ES Taryba suteikė teisę valstybių narių teisėsaugos institucijoms ir Europolui išimtinai tik teroristinių ir sunkių nusikaltimų tyrimo tikslais naudotis EURODAC kartu nustatydama griežtesnį nei įprastai naudojamą asmens duomenų apsaugos lygį: Analogiškai aukščiau minėtiems atvejams teisėsaugos institucijos ir Europolas privalo vadovautis teisėsaugos institucijos ir Europolas privalo analogiškai aukščiau minėtiems atvejams vadovautis 108 Konvencija bei Rekomendacijomis.

733 Europos sienų stebėjimo sistema (toliau – EUROSUR) sukurta siekiant gerinti Šengeno išorės sienų kontrolę atskleidžiant ir kovojant su neteisėta migracija, tarptautinio pobūdžio nusikaltimais ir prisidedant prie migrantų gyvybių apsaugos ir išsaugojimo užtikrinimo. Ši sistema padeda gerinti keitimąsi informacija tarp nacionalinių koordinavimo

informacinę sistemą[734]. Šios informacinės sistemos taip pat turi savitą asmens duomenų apsaugos reglamentavimą.

3.3. Europos Sąjungos lygmuo po asmens duomenų apsaugos reformos

Asmens duomenų apsaugos direktyva įsigaliojo prieš 23 metus, kuomet internetu naudojosi mažiau nei 1 % ES gyventojų[735]. Ir tie, kurie juo naudojosi, naudojosi daugiausiai mokslinių tyrimų, bet ne asmeniniais tikslais[736]. Taigi, interneto ir modernių technologijų amžiuje galiojančio ES asmens duomenų apsaugos įrankio – Asmens duomenų apsaugos direktyvos – tekstas buvo parengtas kontekste, kuriame pasaulis asmens duomenis tvarkė nežinodamas, kas yra internetas ir, kad Asmens duomenų apsaugos direktyvos taikymo metu internetas ir moderniosios asmens duomenų apsaugos tvarkymo technologijos taps pagrindiniu asmens duomenų apsaugos iššūkiu. Visa informacinė-technologinė bazė, tapusi neatskiriama kiekvieno iš mūsų gyvenimo dalimi, žvelgiant iš 1995 m. perspektyvos, atrodė kaip kito žmonijos istorijos laikmečio atributai. Tuo, dabar jau kitu atrodančiu, žmonijos istorijos laikmečiu parengta Asmens duomenų apsaugos direktyva sugebėjo gyvuoti nepakeista taip ilgai ir netgi, technologiniu požiūriu, ir visiškai kitame amžiuje, tik dėka technologiškai neutralios terminijos, vartojamos jos tekste[737]. Visgi, debesų kompiuterija iškėlė tam tikrų problemų, kurios išsprendžiamos gali būti tik keičiant dabar iki 2018 m. galiojusį asmens duomenų apsaugos reglamentavimą ES[738]. Tačiau naujasis ES reglamentavimas turi

centrų ir FRONTEX (ES agentūros, atsakingos už naujos integruoto sienų valdymo koncepcijos kūrimą ir taikymą) bendradarbiavimą. Pagrindinis EUROSUR tinklas sudarytas iš nacionalinių koordinavimo centrų, kuriuose visos už sienų stebėjimą atsakingos nacionalinės institucijos (pvz., pasienio apsaugos tarnyba, policija, pakrančių apsaugos tarnyba, karinės jūrų pajėgos) turi bendradarbiauti ir koordinuoti savo veiksmus. Šios institucijos per nacionalinės padėties vaizdo sistemas dalinasi informacija apie incidentus prie išorės sausumos ir jūrų sienų, patrulių statusą ir poziciją, taip pat keisis analitinėmis ataskaitomis ir žvalgybos informacija. Tačiau keitimasis informacija Europos padėties vaizdo sistemoje ir bendroje pasienio žvalgybos sistemoje yra įmanomas tik išimtiniais atvejais. Ir informacija, kuria valstybių narų kompetentingos institucijos ir FRONTEX turi teisę keistis yra tik operacinio pobūdžio. Pagal bendrą taisyklę asmens duomenys negali būti šio keitimosi objektu. Jeigu išimtinais atvejais buvo apsikeista asmens duomenimis, tada asmens duomenų apsaugai yra taikomas ES asmens duomenų apsaugos teisinis režimas, numatytas, visų pirma, 2007/2004 reglamente. Asmens duomenų apsaugos direktyva, Tarybos pamatinis sprendimas, tik tuomet, jei visapusiškas duomenų apsaugos lygis neužtikrinamas 2007/2004 reglamentu arba kitomis konkrečiomis priemonėmis. Valstybių narių teisėsaugos institucijoms nėra suteiktos teisės naudotis EUROSUR duomenimis. Tik Europolas turi teisę bendradarbiauti su FRONTEX siekiant keistis į Europos padėties vaizdo sistemą įtrauktina informacija apie tarpvalstybinį nusikalstamumą.

[734] Kita su sienų apsauga susijusi ir ES lygmeniu sukurta bendra informacinė sistema yra Muitinės informacinė sistema (toliau – MIS). MIS tikslas – padėti valstybėms narėms užkirsti kelią nacionalinių ir ES muitinės ir žemės ūkio įstatymų pažeidimams, juos tirti ir patraukti už juos baudžiamojon atsakomybėn. Įgyvendinat šį tikslą į MIS gali būti tvarkomi ir asmens duomenys. Prieiga prie MIS suteikiama nacionalinėms muitinės, mokesčių, žemės ūkio, visuomenės sveikatos ir policijos institucijoms, taip pat Europolui ir Eurojustui. Tvarkant asmens duomenis būtina laikytis konkrečių Reglamente Nr. 515/97 ir MIS konvencijoje nustatytų taisyklių, taip pat Duomenų apsaugos direktyvos, ES institucijų duomenų apsaugos reglamento, Konvencijos Nr. 108 ir Rekomendacijos dėl policijos duomenų nuostatų.

[735] „Commission proposes a comprehensive reform of data protection rules to increase users' control of their data and to cut costs for businesses", *European Commission*, žiūrėta 2020 m. rugpjūčio 15 d., http://europa.eu/rapid/press-release_IP-12-46_en.htm?locale=en.

[736] Edward Lucas, *Cyberphobia: Identity, Trust, Security and the Internet* (Bloomsbury Publishing, 2015).

[737] Peter Blume, „It Is Time for Tomorrow: EU Data Protection Reform and the Internet", *Journal of Internet Law* 18, no. 8 (2015): 4.

[738] *Ibid*., 6, 7.

būti toks pat technologiškai neutralus, kad teisė sugebėtų prisitaikyti prieš pirma ją žengiančias inovatyvias technologijas ir asmens duomenų tvarkymo mechanizmus.

Technologinė pažanga, internetas ir debesų kompiuterija, kėlusi iššūkius teisinei asmens duomenų apsaugai[739] nebuvo vienintelė asmens duomenų apsaugos reformos ES priežastis. Antrąją priežastį[740] galime laikyti teisine – tai pokyčiai ES pirminės teisės sistemoje. Teisė į asmens duomenų apsaugą ES tiesiogiai buvo įtvirtinta 2000 m. Europos Sąjungos pagrindinių teisių chartijos 8 straipsnyje, o 2007 m. Lisabonos sutarties 16 straipsnyje buvo įtvirtintos nuostatos, užtikrinančios asmens duomenų apsaugą. Europos Sąjungos sutarties 6(1) straipsniu Chartijai buvo suteikta ES sutarčių galia reiškianti, kad ji tapo pirminiu ES teisės aktu. Taigi naujasis ES asmens duomenų apsaugos reglamentavimas nėra tik ES reakcija į technologinę pažangą. Tai, pasak, Peter Blume, kartu yra ES reakcija į fundamentinių jos piliečių teisių užtikrinimą[741] [742]. Tačiau EK pranešimas apie asmens duomenų apsaugos reformą rodo, kad piliečių teisių užtikrinimas, nebūtinai yra pirminis ES asmens duomenų apsaugos reformos tikslas, o tikėčiau, kad antrinis. EK savo pranešime nurodė, kad asmens duomenų apsaugos reforma ji siekia užtikrinti ne tik piliečių, bet ir verslo interesus. Skaitmeninės rinkos sukūrimas, esantis vienu iš ES ekonomikos prioritetų[743] ir kartu vienas verslo subjektų užtikrinimo asmens duomenų apsaugos reforma priežasčių[744]. Vadinasi, kaip ir 1995 m. asmens duomenų apsaugos direktyva atsirado dėl ekonominio ES siekio užtikrinti laisvą prekių, paslaugų ir kapitalo judėjimą[745], taip ir asmens duomenų apsaugos reforma visų pirma yra orientuota į skaitmeninės ekonomikos plėtrą ES per vieningos skaitmeninės rinkos sukūrimą[746], kuri, planuojama, ES biudžetą papildytų 415 bilijonų Eurų per metus[747]. Nors už bendrosios skaitmeninės rinkos sukūrimą atsakingas EK pirmininko pavaduotojas A. Ansipas tvirtino, kad „nustačius tvirtus bendrus duomenų apsaugos standartus, žmonės galės būti užtikrinti, kad kontroliuoja

---

739 „Commission proposes a comprehensive reform of data protection rules to increase users' control of their data and to cut costs for businesses", *European Commission*, žiūrėta 2020 m. rugpjūčio 15 d., http://europa.eu/rapid/press-release_IP-12-46_en.htm?locale=en.

740 Blume, *op. cit.,* 737: 5.

741 Blume, *supra note,* 737: 5.

742 EK skaitmeninio privatumo piliečių teisių užtikrinimą taip pat įvardijo tarp ES asmens duomenų apsaugos reformos priežasčių.

743 Marija Boban, „Digital Single Market and EU Data Protection Reform with Regard to the Processing of Personal Data as the Challenge of the Modern World The Legal Challenges of Modern World", *Economic and Social Development, 16th International Scientific Conference on Economic and Social Development: The Legal Challenges of Modern World* 16 (2016): 191–201.

744 „1995 m. spalio 24 d. Europos Parlamento ir Tarybos direktyva (95/46/EB) dėl asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo", preambulės 4,5 p., *EUR-Lex*, žiūrėta 2020 m. rugpjūčio 15 d., https://eur-lex.europa.eu/legal-content/lt/TXT/?uri=CELEX%3A31995L0046 .

745 Neil Robinson ir kt., „Review of the European Data Protection Directive", 24, žiūrėta 2020 m. rugpjūčio 15 d., https://ico.org.uk/media/about-the-ico/documents/1042349/review-of-eu-dp-directive.pdf.

746 „Agreement on Commission's EU Data Protection Reform Will Boost Digital Single Market", *European Commission,* žiūrėta 2020 m. rugpjūčio 15 d., https://ec.europa.eu/commission/presscorner/detail/en/IP_15_6321.

747 „Six Commission priorities for 2019–2023", *European Commission*, žiūrėta 2020 m. rugpjūčio 15 d., http://ec.europa.eu/priorities/digital-single-market/.

savo asmeninę informaciją“[748], tačiau bendrosios skaitmeninės rinkos sukūrimas yra paremtas didelių duomenų (angl. *big data*) vartojimu[749]. Ir deja, bet paprastai asmenys nesuvokia, kas didieji duomenys (angl. *big data*) yra ir kaip, ir kada jie yra renkami[750]. Asmens duomenų identifikavimo technologijos taip pat keičiasi. Pavyzdžiui, buvo manoma, kad dideli duomenys nesudaro galimybės identifikuoti konkretaus asmens, tačiau pastaruoju metu mokslininkai jau yra linkę su tuo nesutikti[751].

ES asmens duomenų apsaugos reformą sudaro 2018 m. įsigaliojęs dviejų dokumentų paketas: tiesiogiai taikomas Europos Parlamento ir Tarybos reglamentas dėl fizinių asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo (toliau – Bendrasis duomenų apsaugos reglamentas arba BDAR)[752] ir Europos Parlamento ir Tarybos direktyvos dėl fizinių asmenų apsaugos kompetentingoms institucijoms tvarkant asmens duomenis nusikalstamų veikų prevencijos, tyrimo, nustatymo ar traukimo baudžiamojon atsakomybėn už jas arba baudžiamųjų sankcijų vykdymo tikslais ir dėl laisvo tokių duomenų judėjimo (toliau – Teisėsaugos tikslais tvarkomų asmens duomenų apsaugos direktyva)[753]. Tiesiogiai valstybėse narėse taikomas Bendrasis asmens duomenų apsaugos reglamentas išpildė 2012 m. išreikštą 90% ES gyventojų norą turėti vienodą asmens duomenų apsaugos reglamentavimą visoje ES[754]. Bendruoju asmens duomenų apsaugos reglamentu yra atnaujinami ir modernizuojami 1995 m. Asmens duomenų apsaugos direktyvos principai. Direktyvos vaidmuo reformoje yra kitoks – ja siekiama bent iš dalies harmonizuoti asmens duomenų apsaugos taisykles valstybėse narėse, taikomas nusikalstamų veikų tyrimo, prevencijos, nustatymo ir baudžiamosios atsakomybės taikymo srityse ir ne tik duomenimis keičiantis tarp ES valstybių narių ir trečiųjų šalių teisėsaugos institucijų, bet ir nacionali-

---

748 „Agreement on Commission's EU data protection reform will boost Digital Single Market“, *European Commission*, žiūrėta 2020 m. rugpjūčio 15 d., http://europa.eu/rapid/press-release_IP-15-6321_en.htm.

749 „Big data“, *European Commission*, žiūrėta 2020 m. rugpjūčio 15 d., https://ec.europa.eu/digital-single-market/en/big-data.

750 „Big Data Has an 'I Don't Know' Problem“, *AgWeb*, žiūrėta 2020 m. rugpjūčio 15 d., https://www.agweb.com/article/big-data-has-an-i-dont-know-problem-NAA-ben-potter.

751 Natasha, Singer, „With a Few Bits of Data, Researchers Identify 'Anonymous' People“, *The New York Times*, žiūrėta 2020 m. rugpjūčio 15 d., https://bits.blogs.nytimes.com/2015/01/29/with-a-few-bits-of-data-researchers-identify-anonymous-people/. Scott Berinato, „There's No Such Thing as Anonymous Data“, *Harvard Business Review*, 2015, žiūrėta 2020 m. rugsėjo 7 d., https://hbr.org/2015/02/theres-no-such-thing-as-anonymous-data. Patrick Tucker, „Has Big Data Made Anonymity Impossible?“, *MIT Technology Review*, žiūrėta 2020 m. rugsėjo 7 d., https://www.technologyreview.com/2013/05/07/178542/has-big-data-made-anonymity-impossible/.

752 „2016 m. balandžio 27 d. Europos Parlamento ir Tarybos reglamentas (ES) 2016/679 dėl fizinių asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo ir kuriuo panaikinama Direktyva 95/46/EB (Bendrasis duomenų apsaugos reglamentas)“, *EUR-Lex*, žiūrėta 2020 m. rugpjūčio 15 d., https://eur-lex.europa.eu/legal-content/LT/TXT/?uri=CELEX%3A32016R0679.

753 „2016 m. balandžio 27 d. Europos Parlamento ir Tarybos direktyva (ES) 2016/680 dėl fizinių asmenų apsaugos kompetentingoms institucijoms tvarkant asmens duomenis nusikalstamų veikų prevencijos, tyrimo, atskleidimo ar baudžiamojo persekiojimo už jas arba bausmių vykdymo tikslais ir dėl laisvo tokių duomenų judėjimo, ir kuriuo panaikinamas Tarybos pamatinis sprendimas 2008/977/TVR“, *EUR-Lex*, žiūrėta 2020 m. rugpjūčio 15 d., https://eur-lex.europa.eu/legal-content/lt/TXT/?uri=CELEX%3A32016L0680.

754 „Attitudes on Data Protection and Electronic Identity in the European Union“, *Special Eurobarometer 359*, žiūrėta 2020 m. rugsėjo 10 d., https://ec.europa.eu/commfrontoffice/publicopinion/archives/ebs/ebs_359_en.pdf.
Viviane Reding „The European data protection framework for the twenty-first century“, *International Data Privacy Law*, Volume 2, Issue 3, 2012, 119–129.

niu lygiu[755]. Taigi direktyva, skirtingai nuo Pamatinio sprendimo, tikimasi, kad turėtų suvienodinti nacionalinę praktiką. Tačiau nors Bendrąjį asmens duomenų apsaugos reglamentą mokslininkai vertina teigiamai ir laiko sveikintinu[756], Teisėsaugos tikslais tvarkomų asmens duomenų apsaugos direktyva ne visuomet yra vertinama taip palankiai[757]. Nacionalinės asmens duomenų apsaugos tarnybos, taip pat daugiau dėmesio skiria Bendrajam asmens duomenų apsaugos reglamentui, nors tai ir yra tiesiogiai taikomas teisės aktas, nei Direktyvai. Pavyzdžiui Valstybinės asmens duomenų apsaugos inspekcijos tinklapyje yra atskira skiltis „Asmens duomenų apsaugos reforma", tačiau visa informacija yra pateikta tik dėl Reglamento taikymo. Dėl direktyvos taikymo ypatumų informacijos nėra[758].

3.3.1. Teisėsaugos tikslais tvarkomų asmens duomenų direktyva ir asmens duomenų rinkimas elektroninėje erdvėje

Kiekvieną dieną mes gyvename dvejuose pasauliuose – įprastiniame fiziniame ir elektroniniame. Per dieną tiesiogiai elektroninėje erdvėje mes praleidžiame iki 12 val., o netiesiogiai netgi 24 val. per parą[759], o joje absoliučiai kiekvienas mūsų veiksmas palieka pėdsakus, kurių mes negalime nei ištrinti, nei paslėpti ir, dažnai net nežinome, kad paliekame. Teisėsaugos ir žvalgybos tikslais elektroninėje erdvėje surenkamų asmens duomenų kiekis yra nepalyginamai didesnis nei įprastoje fizinėje aplinkoje[760] ne tik dėl labai didelio asmenų paliekamų elektroninių pėdsakų kiekio ir įvairovės, bet ir dėl technologinių galimybių tuos duomenis surinkti, o teisė neliudyti pačiam prieš save elektroninėje erdvėje negalioja. Todėl, kad nebūtų pažeisti teisinės valstybės principai turi būti pakankami asmens teisių el. erdvėje apsaugos garantai. Pavyzdžiui, kuo yra ypatinga JAV teisės sistema, kad ji turi specifinius teisės aktus, skirtus asmens duomenų rinkimo el. erdvėje reglamentavimui ir kartu asmens teisių užtikrinimui: teisėsaugos institucijų veikla reglamentuojama ECPA,

---

[755] „2016 m. balandžio 27 d. Europos Parlamento ir Tarybos direktyva (ES) 2016/680 dėl fizinių asmenų apsaugos kompetentingoms institucijoms tvarkant asmens duomenis nusikalstamų veikų prevencijos, tyrimo, atskleidimo ar baudžiamojo persekiojimo už jas arba bausmių vykdymo tikslais ir dėl laisvo tokių duomenų judėjimo, ir kuriuo panaikinamas Tarybos pamatinis sprendimas 2008/977/TVR", *EUR-Lex*, žiūrėta 2020 m. rugpjūčio 15 d., https://eur-lex.europa.eu/legal-content/lt/TXT/?uri=CELEX%3A32016L0680.

[756] „Opinion of the European Data Protection Supervisor on the data protection reform package", 4, *European Data Protection Supervisor*, žiūrėta 2020 m. rugpjūčio 15 d., https://edps.europa.eu/sites/edp/files/publication/12-03-07_edps_reform_package_en.pdf.

[757] „Opinion of the European Data Protection Supervisor on the data protection reform package", 4, *European Data Protection Supervisor*, žiūrėta 2020 m. rugpjūčio 15 d., https://edps.europa.eu/sites/edp/files/publication/12-03-07_edps_reform_package_en.pdf.

[758] „Reforma. Renginiai", *Valstybinė asmens duomenų inspekcija*, žiūrėta 2020 m. rugpjūčio 15 d., https://www.ada.lt/go.php/Renginiai975.

[759] Charles Hymas, „A Decade of Smartphones: We Now Spend an Entire Day Every Week Online", *The Telegraph*, 2018, žiūrėta 2020 m. rugsėjo 7 d., https://www.telegraph.co.uk/news/2018/08/01/decade-smartphones-now-spend-entire-day-every-week-online/. „How Much Time Do People Spend Online Each Day?", *UKOM*, 2018, žiūrėta 2020 m. rugsėjo 7 d., https://ukom.uk.net/insights/87-how-much-time-do-people-spend-online-each-day.php.

[760] „UK Surveillance Powers Explained", *BBC News*, 2015, žiūrėta 2020 m. rugsėjo 7 d., https://www.bbc.com/news/uk-34713435.

žvalgybos – FISA ir EO12333. ES lygiu tokie teisės aktai nėra priimti. Žvalgybos veikla iš viso ES lygiu nėra reglamentuojama, o Direktyva siekiama reglamentuoti apskritai visų teisėsaugos tikslais renkamų asmens duomenų tvarkymą. Vadinasi, Direktyva turėtų apimti ir el. erdvėje teisėsaugos tikslais renkamų asmens duomenų tvarkymą. Tačiau ar ji yra tam pritaikyta ir ar vadovaujantis Direktyva parengti nacionaliniai teisės aktai tinkamai užtikrins el. erdvėje renkamų asmens duomenų apsaugą? Atsakymo į šį klausimą ieškosime analizuodami Direktyvos objektą, subjektus ir taikymo teritoriją.

Direktyvos objektas. Direktyva yra taikoma teisėsaugos institucijoms tvarkant asmens duomenis nusikalstamų veikų prevencijos tyrimo, atskleidimo ar baudžiamojo persekiojimo už jas ar bausmių skyrimo, apsaugos nuo grėsmių visuomenės saugumui ir jų prevencijos tikslais. Direktyvos taikymo apimtis apima ir el. erdvę. Tačiau el. erdvėje gali būti renkami skirtingų kategorijų duomenys. Paprastai yra išskiriama dvi kategorijos duomenų, kurios gali būti renkamos el. erdvėje: komunikacijos turinys ir metaduomenys[761]. JAV, priklausomai nuo renkamų duomenų rūšies, yra taikomas skirtingas asmens duomenų tvarkymo reglamentavimas: komunikacijos turinys yra laikomas jautresne ir daugiau informacijos apie asmenis atskleidžiančia duomenų rūšimi, todėl tokio pobūdžio duomenų rinkimui yra taikomi griežtesni reikalavimai, o metaduomenų ir duomenų, kurie nėra nei komunikacijos turinys, nei metaduomenys, tvarkymui – paprastesni reikalavimai. Metaduomenys apima informaciją apie komunikacijos el. erdvėje gavėją, siuntėją, telefono numerį, IP adresą, laiko ir vietos informaciją ir kt. Nors atskirai komunikacijos el. erdvėje metaduomenys nėra informatyvūs, tačiau metaduomenų visuma gali ne tik atskleisti jautrią informaciją apie asmenį, bet ir sudaryti jo portretą, šiuolaikinių technologijų dėka meta duomenis yra lengva klasifikuoti, grupuoti ir analizuoti[762]. Jeigu komunikacijos turinys be jokios abejonės yra laikomas asmens duomenimis, tai pasaulyje nėra vieningos nuomonės ar metaduomenys yra laikomi asmens duomenimis[763]. Ar metaduomenys patenka į Direktyvos apimtį ir gali būti laikomi asmens duomenimis?

Direktyva, panašiai kaip ir Konvencija Nr. 108, asmens duomenis apibrėžia kaip bet kokią informaciją apie fizinį asmenį, kurio tapatybė nustatyta arba kurio tapatybę galima tiesiogiai ar netiesiogiai nustatyti[764]. Pasak J. Mayer ir Ch. Porter, visa el. erdvėje surinkta informacija yra asmens duomenimis, nes visuomet egzistuoja tech-

---

761 Graham Smith, „Content versus Metadata“, *Internet Newsletter for Lawyers*, 2017, žiūrėta 2020 m. rugsėjo 7 d., https://www.infolaw.co.uk/newsletter/2017/01/content-versus-metadata/.

762 „Briefing Note: Why Communications Data (Metadata) Matter“, *Big Brother Watch*, žiūrėta 2020 m. rugpjūčio 15 d., https://www.bigbrotherwatch.org.uk/wp-content/uploads/2014/07/Communications-Data-Briefing.pdf .

763 Campbell Simpson, „Your Metadata Isn't Private Personal Information, Federal Court Decides“, *Gizmodo Australia*, 2017, žiūrėta 2020 m. rugsėjo 7 d., https://www.gizmodo.com.au/2017/01/your-metadata-isnt-private-personal-information-federal-court-decides/.

764 Asmens duomenys – bet kokia informacija apie fizinį asmenį, kurio tapatybė nustatyta arba kurio tapatybę galima nustatyti (duomenų subjektas); fizinis asmuo, kurio tapatybę galima nustatyti, yra asmuo, kurio tapatybę tiesiogiai arba netiesiogiai galima nustatyti, visų pirma pagal identifikatorių, kaip antai vardą ir pavardę, asmens identifikavimo numerį, buvimo vietos duomenis ir interneto identifikatorių arba pagal vieną ar kelis to fizinio asmens fizinės, fiziologinės, genetinės, psichinės, ekonominės, kultūrinės ar socialinės tapatybės požymius.

nologinė galimybė nustatyti asmens tapatybę[765]. Teismų praktika[766] ir 29 darbo grupės pozicija jog tiek 108 Konvencija, tiek 1994 m. Direktyva metaduomenis laiko asmens duomenimis[767] tai patvirtina[768]. Metaduomenų laikymui asmens duomenimis 2015 m. pritarė ir Venecijos komisija[769]. ESTT Duomenų saugojimo direktyvos byloje pasisakydamas, kad telekomunikacijos meta duomenys kaip visuma gali suformuoti labai aiškų asmens privataus gyvenimo portretą[770], konstatavo, kad meta duomenų nuolatinis rinkimas ir saugojimas prieštarauja teisei į asmens duomenų apsaugą ir yra gali būti laikomas nuolatiniu asmenų stebėjimu[771]. Taigi meta duomenys patenka į Direktyvos reglamentavimo apimtį. Tačiau ar jų rinkimui ir kitokiam tvarkymui yra tikslinga taikyti tokias pačias procedūras kaip ir komunikacijos turiniui, ar geriau taikyti skirtingo lygio apsaugos reikalavimus, kaip tai yra daroma JAV.

Komunikacijos meta duomenų reikšmė ir galimybės identifikuojant asmenį bei jo veiksmus vis dar yra mokslinių diskusijų ir kartu technologijų pažangos klausimas. Komunikacijos turinį galime laikyti paties asmens liudijimu prieš save. Nors ateityje dėl dirbtinio intelekto pažangos, kad informacijos šaltiniu tikrai yra asmuo, gali tapti įrodinėjimo objektu[772]. Komunikacijos turinys visada tiksliai atspindės asmens komunikaciją ir tiesiogiai liudys prieš asmenį, t. y. dažniausiai tai bus tiesioginiais įrodymais. El. laiško turinys, jog asmuo A prisipažįsta asmeniui B ką tik nužudęs asmenį C bus vienu iš tiesioginių įrodymų. Tuo tarpu, komunikacijos meta duomenys paprastai neturėtų būti laikomi tiesioginiais įrodymais. Šie duomenys gali atskleisti informaciją, kad asmuo A. atitinkamu laiku iš atitinkamos vietos siuntė asmeniui B. el. laišką. Arba

---

765 C. Christine Porter, „De-Identified Data and Third Party Data Mining: The Risk of Re-Identification of Personal Information“, *University of Washington Shidler Journal of Law, Commerce & Technology*, 2008, žiūrėta 2020 m. rugjūčio 15 d., https://digitalcommons.law.uw.edu/cgi/viewcontent.cgi?article=1075&context=wjlta. „Big Data Analysis and Anonymisation Techniques under the EU General Data Protection Regulation“, *Financier Worldwide*, žiūrėta 2020 m. rugsėjo 7 d., https://www.financierworldwide.com/big-data-analysis-and-anonymisation-techniques-under-the-eu-general-data-protection-regulation.

766 Europos Sąjungos Teisingumo Teismo 2014 m. balandžio 8 d. sprendimas byloje Nr. C-293/12 ir C-594/12 Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others, EUR-Lex, žiūrėta 2020 m. rugsėjo 7 d., https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62012CJ0293.

767 „Article 29 Data Protection Working Party, Opinion 04/2014 on surveillance of electronic communications for intelligence and national security purposes, Nr. 819/14/EN WP 215“, 5, *European Commission*, žiūrėta 2020 m. rugpjūčio 16 d., https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp215_en.pdf.

768 „Bureau of Investigative Journalism and Alice Ross v. the United Kingdom, Written Submissions on Behalf of the International Commission of Jurists (ICJ)“, žiūrėta 2020 m. rugpjūčio 16 d., https://www.icj.org/wp-content/uploads/2016/02/UK-ICJ-AmicusBrief-BJURoss-ECtHR-legalsubmission-2016.pdf.

769 „European Commission for Democracy through Law (Venice Commission), Report on the Democratic Oversight of Signals Intelligence Agencies, adopted at its 102nd Plenary Session (Venice, 20-21 March 2015), Strasbourg, 15 December 2015 CDL-AD(2015)011, Study No. 719/2013“, 58-59 paragrafai, *Venice Commission*, žiūrėta 2020 m. rugpjūčio 16 d., https://www.venice.coe.int/webforms/documents/default.aspx?pdffile=CDL-AD(2015)011-e.

770 Europos Sąjungos Teisingumo teismo 2014 m. balandžio 8 d. sprendimas byloje Nr. C-293/12 ir C-594/12 Digital Rights Ireland Ltd v Ireland, EUR-Lex, žiūrėta 2020 m. rugsėjo 7 d., https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:62012CJ0293&rid=1.

771 *Ibid.*

772 Pvz. netikras JAV prezidento B. Obama balsas, žr. Will Knight, „This AI Lets You Deepfake Your Voice to Speak like Barack Obama“, *MIT Technology Review*, žiūrėta 2020 m. rugsėjo 7 d., https://www.technologyreview.com/2019/02/27/66005/this-ai-lets-you-deepfake-your-voice-to-speak-like-barack-obama/.

netgi tai, kad kažkas, naudodamasis asmens A mobiliąja paskyra iš atitinkamos vietos siuntė asmeniui B. el. laišką. Tačiau tai tiesiogiai neįrodys, jog asmuo A nužudė asmenį C, nors ir buvo šalia nužudymo vietos. Todėl JAV teismų praktikoje komunikacijos meta duomenys negali būti vieninteliais įrodymais byloje[773]. Nors tiesioginių ir netiesioginių duomenų rinkimui galioja tos pačios taisyklės, kaip ir netiesioginių, tačiau el. erdvėje tokių duomenų rinkimas labai supaprastėja, telekomunikacijų ir interneto paslaugų tiekėjai šiuos duomenis renka bent kokiu atveju ir gali be ypatingų papildomų pastangų juos suteikti teisėsaugai. Neabejotina, kad nediferencijuotas masinis meta duomenų rinkimas kelia rimtą pavojų teisės į asmens duomenų apsaugą pažeidimui[774], tačiau masinį asmens duomenų rinkimas paprastai yra vykdytinas žvalgybos, ne teisėsaugos tikslais. Todėl paprastesnės meta duomenų rinkimo procedūros galėtų sumažinti administracinę naštą ir padėtų teisėsaugos institucijoms pasinaudojant el. erdve greičiau ir efektyviau tirti nusikalstamas veikas. Kaip pažymi, M. Cierglowski, el. ryšių paslaugų ir el. paslaugų teikėjai renka asmens duomenis ir juos naudoja komerciniais tikslais daug didesniais mastais, nei tai daro teisėsaugos ar žvalgybos institucijos[775]. Paprastesnė teisėsaugos institucijų prieiga prie telekomunikacijų ir interneto paslaugų teikėjų jau surinktų meta duomenų iš esmės nereiškia tokių duomenų rinkimo inicijavimo. Tačiau minėti teiginiai nepaneigia metaduomenų svarbos. Metaduomenys yra skirtingų lygių (plačiau apie tai I disertacijos dalyje). Komunikacijos el. erdvėje turinys iš siuntėjo pas gavėją taip pat keliauja metaduomenų forma. Devynių pasaulio valstybių teisės aktuose yra įtvirtinta teisėsaugos institucijų teisė vykdyti prisijungimus prie elektroninės erdvės įrenginių. Daugumą komunikacijos šiandien vyksta ne per el. ryšių tinklų paslaugų teikėjus, bet per el. paslaugų teikėjus, o komunikacijos turinys yra užšifruotas ištisiniu šifravimu. Tokio komunikacijos el. erdvėje turinio teisėsaugos institucijos negali perskaityti. Metaduomenys lieka vieninteliu informacijos šaltiniu. Todėl metaduomenų svarba negali būti laikoma mažesne, o komunikacijos turinio ir metaduomenų rinkimo el. erdvėje taisyklės negali būti skirtingos.

Skirtingai nuo komunikacijos turinio, metaduomenys paprastai yra renkami iš elektroninių paslaugų teikėjų, kurie juos kaupia paslaugų teikimo tikslais, ir yra neužkoduoti ar papildomai neapsaugoti. Kadangi elektroninių paslaugų teikėjai paprastai veikia globaliu mastu ir tų pačių teikėjų paslaugomis naudojasi didžioji dauguma ES gyventojų[776], todėl didžioji dauguma teisėsaugos užklausų dėl el. komunikacijos metaduomenų rinkimo bus adresuotos tiems patiems teikėjams (Google, Facebook,

---

[773] Zachary W. Rosenberg, „Returning to Plato's Cave: Metadata's Shadows in the Courtroom", *Arizona State Law Journal*, 2016, žiūrėta 2020 m. rugpjūčio 16 d., http://arizonastatelawjournal.org/wp-content/uploads/2016/07/Rosenberg_Final.pdf.

[774] „Article 29 Data Protection Working Party, Opinion 04/2014 on surveillance of electronic communications for intelligence and national security purposes, Nr. 819/14/EN WP 215", 5, *European Commission*, žiūrėta 2020 m. rugpjūčio 16 d., https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp215_en.pdf.

[775] Charles Arthur, „Internet Regulation: Is It Time to Rein in the Tech Giants?", *The Observer*, 2017, žiūrėta 2020 m. rugsėjo 7 d., https://www.theguardian.com/technology/2017/jul/02/is-it-time-to-rein-in-the-power-of-the-internet-regulation.

[776] Olivia Solon, „Net Neutrality: 'father of Internet' Joins Tech Leaders in Condemning Repeal Plan", *The Guardian*, 2017, žiūrėta 2020 m. rugsėjo 7 d., https://www.theguardian.com/technology/2017/dec/11/net-neutrality-vint-cerf-tim-berners-lee-fcc-letter.

Twitter). Todėl užklausų teikimo procedūrų suvienodinimas bei teisėtų rinkimo pagrindų lygio bei valstybių narių vidinių baudžiamojo proceso procedūrų suvienodinimas užtikrintų ne tik, kad el. erdve ES besinaudojantys asmenys būtų vienodai traktuojami ir saugomi, bet ir pačioms elektroninių paslaugų teikėjoms tai supaprastintų procedūras ir administracinius išteklius. Identiška situacija yra ir su komunikacijos el. erdvėje turiniu. 2018 m. JAV priėmus *Claud Act* ne tik JAV, bet ir ES teisėsaugos institucijos turi galimybę gauti komunikacijos el. erdvėje turinį iš JAV[777]. Analogiškai komunikacijos meta duomenų rinkimui, komunikacijos el. erdvėje turinio rinkimo procedūrų suvienodinimas yra neišvengiamas visų pirma žiūrint iš pačių elektroninės paslaugas teikiančių įmonių pozicijų. Antra, ES gyventojai, besinaudojančių tomis pačiomis tų pačių įmonių paslaugomis (Facebook, Microsoft ir t. t.) neturėtų būti saistomi skirtingomis teisėsaugos institucijų procedūromis ir asmens duomenų apsaugos standartais. Ir galiausiai, teisėsaugos institucijoms asmens duomenų rinkimas el. erdvėje, visų pirma, debesyse, taip pat kelia problemų, kadangi ta tos pačios komunikacijos turinio (pvz. el. laiško) elementai gali būti laikomi skirtingose valstybėse esančiuose serveriuose. 2018 m. ES paskelbė apie planuojamą naują teisės aktą, skirtą teisėsaugos el. erdvėje renkamų asmens duomenų reglamentavimui, turintį pakeisti tarpusavio pagalbos sutartis[778]. Nors šio teisės aktu, planuojama, bus galima naudotis tik tuo atveju, kai asmeniui už nusikaltimo padarymą galės būti skiriama ne mažesnė nei 3 metų bausmė, tačiau pati teisės akto apimtis vis dar yra diskusijų objektu. Tai, kad pirminis teisės akto tikslas ir apimtis vis plečiasi, ir kad JAV jau įsigaliojo panašiais principais pagrįsto teisės akto projektas, tikėtina, kad ateityje galės būti sukurta universali asmens duomenų rinkimo el. erdvėje priemonė. Toks įrankis, supaprastinantis nusikalstamų veikų tyrimą, būtų aktualus teisėsaugos institucijoms, jeigu tik nepasikeis el. erdvės universalumas pasauliniu mastu, nes kai kurios valstybės (pvz. Rusija[779], Kinija[780]) jau planuoja kurti atskirą internetą. Tačiau kuriant universalią asmens duomenų rinkimo el. erdvėje priemonę, neišvengiamu taps jurisdikcijos sampratos pasikeitimas el. erdvės atžvilgiu.

Direktyvos taikymo teritorija. Technologiškai elektroninė erdvė dažniausiai yra apibrėžiama kaip globali decentralizuotų kompiuterių sistema, tinklų tinklas (angl. *network of networks*)[781]. Įrenginius vieną su kitu elektroninėje erdvėje gali jungti internetas, sklindantis vieliniu arba bevieliu ryšiu[782]. Taigi mūsų duomenys internetu

---

[777] Jennifer Daskal, „Microsoft Ireland, the CLOUD Act, and International Lawmaking 2.0 Essay", *Stanford Law Review Online* 71 (2019 2018): 9–16.

[778] Julia Fioretti, „Europe Seeks Power to Seize Overseas Data in Challenge to Tech Giants", *Reuters*, 2018, žiūrėta 2020 m. rugsėjo 7 d., https://www.reuters.com/article/us-eu-data-order-idUSKCN1GA0LP.

[779] Jane Wakefield Cellan-Jones Rory, „Russia 'successfully Tests' Its Unplugged Internet", *BBC News*, 2019, žiūrėta 2020 m. rugsėjo 7 d., https://www.bbc.com/news/technology-50902496.

[780] „China and Huawei Propose Reinvention of the Internet", žiūrėta 2020 m. rugsėjo 7 d., https://amp.ft.com/content/c78be2cf-a1a1-40b1-8ab7-904d7095e0f2?fbclid=IwAR3Ne3_yWeoJTCKtoDU2-n0uN9DkXZ038LYib4ORBaiXr35hmtk3_MtI8lw.

[781] Jackson Adams ir Mohamad Albakajai, „Cyberspace: A New Threat to the Sovereignty of the State", *Management Studies* 4, no. 6 (September 29, 2016): 1, doi:10.17265/2328-2185/2016.06.003.

[782] „How Does the Internet Work?", *Stanford University*, žiūrėta 2020 m. rugsėjo 7 d., https://web.stanford.edu/class/msande91si/www-spr04/readings/week1/InternetWhitepaper.htm.

keliauja arba žemėje esančiais kabeliais, išsiraizgiusiais tiek sausumoje, tiek vandenynų dugne, jeigu ryšys yra vielinis, arba oru – jeigu ryšys yra bevielis. Asmens duomenys internetu keliauja ne teritoriškai artimiausiu keliu tarp asmens duomenų siuntėjo ir gavėjo, bet pagal nustatytą duomenų perdavimo maršrutą, kuris gali kirsti kelių valstybių teritorijas ir teritorijas, nepriklausančias nei vienai valstybei, nors duomenų siuntėjas ir gavėjas fiziškai tuo metu yra tame pačiame kambaryje. Technologiškai yra įmanoma asmens duomenis rinkti visu asmens duomenų maršruto keliu[783].

Direktyva yra ES teisės aktas, taigi ji galioja tik ES valstybėms narėms, o Direktyvą įgyvendinantys teisės aktai galios valstybių narių teritorijoje. Teisės aktų galiojimas teritorijos atžvilgiu yra suvokiamas kaip galiojimas ne vien tik valstybės sienų ribojamoje teritorijoje, bet ir jos kontinentiniame šelfe, oro erdvėje ir jūrų laivuose ir orlaiviuose su skiriamaisiais valstybės ženklais[784]. Bet ar elektroninę erdvę galime laikyti valstybės teritorija? Dalis mokslininkų būtent tokios pozicijos ir laikosi. Pavyzdžiui, J. Sheldon mano, kad el. erdvės teritoriją galima apibrėžti panašiai kaip valstybės ar bent kurios kitos geografinės teritorijos kadangi visa el. erdvei reikalinga sukurti infrastruktūra (kompiuteriai, kabeliai, palydovai ir kt.) yra konkrečiose geografinėse teritorijose ir yra valdomi asmenų, priklausančių politinėms bendruomenėms[785]. Tačiau yra ir kitokią nuomonę turinčių mokslininkų. Pavyzdžiui, T. Schultz, teigia, kad internetas bei visa elektroninė erdvė yra tapusi kažkuo daugiau nei jungtimis tarp tinklo taškų, todėl, negali būti prilyginama juridiniams asmenims, kurių veikla bei jiems galiojantys teisės aktai yra aiškiai apibrėžti konkrečios valstybės ar konkrečių valstybių teritorija. Virtuali el. erdvės prigimtis komunikaciją joje padaro nematerialią (viskas yra elektroniška, kompiuterizuota), nepavaldžią laikui (angl. *detemporalization*), nepaisančią įprastinių teritorijų ir atstumų (angl. *detertorialization*). Todėl komunikacija trunka akimirksniu nepriklausomai nuo fizinio atstumo tarp asmenų. El. erdvėje mes galime būti visur tuo pačiu metu[786]. P. Bellanger apie valstybės jurisdikciją el. erdvėje yra pasakęs, kad valstybės yra vietos, o internetas yra ryšys. Valstybės yra apibrėžtos ir apribotos fizine teritorija, tuo tarpu elektroninė erdvė yra tas elementas, kuris jungia apribotas valstybių teritorijas. Ir nors yra daugybė valstybių, elektroninė erdvė – kol kas[787] – yra viena ir universali"[788]. El. erdvės ypatumas yra ir tas, kad joje veiksmai yra atliekami iš bent kur ir už realaus laiko suvokimo ribų.

---

783 *Ibid.*

784 Svarlien, Oscar, „Introduction to the Law of Nations", (New York: McGraw-Hill., 1955).

785 John B. Sheldon, „Geopolitics and Cyber Power: Why Geography Still Matters", *American Foreign Policy Interests* 36, no. 5 (September 3, 2014): 268, doi:10.1080/10803920.2014.969174.

786 Gabrielle Kaufmann-Kohler ir Thomas Schultz, *Online Dispute Resolution: Challenges for Contemporary Justice* (The Hague : Zürich: Kluwer Law International, 2004).

787 Pierre Bellanger, „De la souveraineté en général et de la souveraineté numérique en particulier", lesechos.fr, 2011, žiūrėta 2020 m. rugpjūčio 16 d., http://archives.lesechos.fr/archives/cercle/2011/08/30/cercle_37239.htm. Farid Gueham, „Digital sovereignty – steps towards a new system of internet governance", žiūrėta 2020 m. rugpjūčio 16 d., https://euagenda.eu/upload/publications/untitled-77045-ea.pdf. J. Adams ir M. Albakajai, „Cyberspace: A New Threat to the Sovereignty of the State", *Management Studies* 4, no. 6 (September 29, 2016), http://dx.doi.org/10.17265/2328-2185/2016.06.003.

788 *Ibid.,* 3.

Valstybės jurisdikcija pasireiškia vertikaliai –fizinių ir juridinių asmenų atžvilgiu, ir horizontaliai – santykių su kitomis valstybėmis atžvilgiu. Jeigu vertikalios jurisdikcijos atžvilgiu valstybė gali duoti privalomus vykdyti nurodymus fiziniams ir juridiniams asmenims, tai horizontaliosios jurisdikcijos atžvilgiu ji nėra pajėgi to padaryti[789]. El. erdvės ypatumas yra tas, kad ji yra tarsi tarp dviejų pasaulių: tradicinio, apriboto fizine teritorija ir valstybės jurisdikcija, ir virtualaus – technologinio, kuriame teritorija yra reikalinga tik techniniams įrenginiams ir valstybės jurisdikcija veikia tik tiek, kiek jos teritoriją apima technologiniai įrenginiai. Vis daugiau tiek teisės, tiek technologijų srities mokslininkų bei didžiosios paslaugas el. erdvėje teikiančios įmonės pasisako už atskirų teisės šakų, reglamentuojančių ne tik už elektroninės erdvės[790], bet ir dirbtinio intelekto[791] teisės kūrimą, yra netgi pateiktų elektroninės erdvės reglamentavimo modelių[792], o 2014 m. Kanadoje įsisteigė nevyriausybinė organizacija *Global commission on internet governance*[793]. Tai rodo, kad valstybės artimiausiu metu turės susitarti dėl jurisdikcijos el. erdvėje. Kol kas tokio susitarimo nėra, tačiau teisės aktų pavyzdžių, leidžiančių valstybėms peržengti savo jurisdikcijos teritoriją dėl klausimų, susijusių su elektronine erdve, yra.

Singapūro 2012 m. Asmens duomenų apsaugos akte (angl. *Personal data protection act 2012*) yra numatyta, kad jis yra taikomas ne tik Singapūre veikiančioms organizacijoms, bet ir bent kokioms kitoms organizacijoms, kurios vykdo asmens duomenų rinkimą, perdavimą arba atskleidimą per Singapūro teritoriją, net jei organizacija ir nėra įsisteigusi Singapūre[794]. Reglamente yra nuostatų, kurios taip pat tarsi išplečia ES valstybių jurisdikciją: pavyzdžiui jeigu ES neregistruoti paslaugų teikėjai nori paslaugas teikti ES, tai jiems galioja Reglamento nuostatos. Panašios, ES teisės aktų galiojimą išplečiančios už ES ribų nuostatos, yra įtvirtintos ir Direktyvoje. Jos pagrindu priimti teisės aktai galioja asmens duomenų perdavimui trečiosioms šalims ir tarptautinėms organizacijoms[795]. Kita vertus, Direktyva apima tik tradicinę

---

789 Jonathan Matusitz, „Cyberterrorism: Postmodern State of Chaos“, *Information Security Journal: A Global Perspective* 17, no. 4 (January 1, 2008): 179–187, doi:10.1080/19393550802397033. Jonathan Matusitz, „Intercultural Perspectives on Cyberspace: An Updated Examination“, *Journal of Human Behavior in the Social Environment* 24, no. 7 (October 3, 2014): 713–24, doi:10.1080/10911359.2013.849223.

790 Sandeep Mittal ir Priyanka Sharma, „Enough Law of Horses and Elephants Debatedd Letts Discuss the Cyber Law Seriously“, *SSRN Electronic Journal*, 2017, doi:10.2139/ssrn.2977374.

791 Dina Bass, „Microsoft Says AI Advances Will Require New Laws, Regulations“, *Bloomberg.Com*, 2018, žiūrėta 2020 m. rugsėjo 7 d., https://www.bloomberg.com/news/articles/2018-01-18/microsoft-says-ai-advances-will-require-new-laws-regulations.

792 Graham Greenleaf, „An Endnote on Regulating Cyberspace: Architecture vs Law?“, SSRN Scholarly Paper (Rochester, NY: Social Science Research Network, December 11, 1998), https://papers.ssrn.com/abstract=2188160.

793 „Global Commission on Internet Governance Paper Series“, *Centre for International Governance Innovation*, žiūrėta 2020 m. rugsėjo 7 d., https://www.cigionline.org/series/global-commission-internet-governance-paper-series.

794 Dan Jerker B. Svantesson, „Extraterritoriality in the Context of Data Privacy Regulation“, *Masaryk University Journal of Law and Technology* 7, no. 1 (2013): 90.

795 „2016 m. balandžio 27 d. Europos Parlamento ir Tarybos direktyva (ES) 2016/680 dėl fizinių asmenų apsaugos kompetentingoms institucijoms tvarkant asmens duomenis nusikalstamų veikų prevencijos, tyrimo, atskleidimo ar baudžiamojo persekiojimo už jas arba bausmių vykdymo tikslais ir dėl laisvo tokių duomenų judėjimo, ir kuriuo panaikinamas Tarybos pamatinis sprendimas 2008/977/TVR“, 35 str. 1 d., *EUR-Lex*, žiūrėta 2020 m. rugpjūčio 15 d., https://eur-lex.europa.eu/legal-content/lt/TXT/?uri=CELEX%3A32016L0680.

jurisdikcijos sampratą ta prasme, kad joje nėra įtvirtinta specifinių nuostatų dėl asmens duomenų rinkimo el. erdvėje. Vadovaujantis tradicine jurisdikcijos samprata, teisėsaugos institucijos asmens duomenis el. erdvėje pagal tradicines BPK įrodymų rinkimo procedūras, gali rinkti iš savo teritorijoje įregistruotų arba joje veikiančių ir joje duomenis laikančių elektroninių paslaugų teikėjų. Tai labiau pritaikytina komunikacijai mobiliuoju arba laidiniu telefonu. Tačiau internetu vykstanti komunikacija ir jos duomenys fiziškai gali būti kelių skirtingų valstybių teritorijose, keliauti per kelias skirtingas valstybes vienu metu. Todėl vadovaujantis tradicinės jurisdikcijos samprata tiesioginis tokių asmens duomenų rinkimas el. erdvėje yra negalimas. Tokiu atveju asmens duomenų rinkimas, vadovaujantis Direktyva, turėtų būti vykdomas pagal savitarpio pagalbos sutartis. Palikus tik tokį asmens duomenų el. erdvėje rinkimo variantą, ES būtų žingsniu atgal nuo *the Claud Act* priėmusios JAV ir iš esmės reikalaujančiu panašių veiksmų, visų pirma iš ES, bei visų kitų valstybių besinaudojančių JAV sukurtu internetu. Nors *the Claud Act* galima laikyti JAV jurisdikcijos viršijimu, kadangi jis sudaro sąlygas JAV rinkti asmens duomenis, esančius bent kurios valstybės teritorijoje, tačiau EO12333 pagrindu JAV nuo 1994 m. žvalgybos institucijos turi teisę rinkti ne JAV asmenų, tai reiškia likusių viso pasaulio gyventojų, asmens duomenis, kurie yra už JAV teritorijos ribų. Taigi, tokio reglamentavimo pavyzdys nebebūtų pirmasis, tačiau skirtųsi jo tikslas – ne žvalgybos, o teisėsaugos. Tam, kad nei JAV, nei ES priimdama teisės aktus, reglamentuojančius asmens duomenų rinkimą el. erdvėje[796] teisėsaugos tikslais, nepažeistų valstybių jurisdikcijų, sprendimu turėtų būti tarptautinis susitarimas ar tarptautinė sutartis. Kadangi žvalgybos technologijų rinka jau yra reglamentuojama tarptautiniu Wassenaro susitarimu , o valstybių teisės aktuose, reglamentuojančių asmens duomenų apsaugą, jau yra jų ekstrateriatorialumo pavyzdžių, tai rodo ne tik poreikio, bet ir tarptautinio susitarimo sudarymo galimybes. Kol tokio teisės projektas nėra rengiamas, o valstybės renka duomenis remdamosi arba tarpusavio pagalbos sutartimis arba savo nacionaliniais teisės aktais, leidžiančiais joms tai daryti. Tačiau tikėtina, kad nacionalinės jurisdikcijos viršijimas gali tapti teisminio ginčo objektu, o tokių veiksmų teisinis pagrįstumas yra labai diskutuotinas. Jeigu žvalgybos tikslais renkamos informacijos atžvilgiu jurisdikcijos viršijimą galima pagrįsti Lotus principu[797], tai teisėsaugos tikslais renkamai informacijai šis principas yra netaikomas.

Direktyvos subjektas. Direktyva yra taikoma kompetentingoms institucijoms tvarkant asmens duomenis:

1. nusikalstamų veikų prevencijos, tyrimo, atskleidimo ar baudžiamojo persekiojimo už jas;

---

[796] Tačiau teisėsaugai yra ypač aktualu tai, kad be el. erdvės, kurioje kiekvieną dieną naršo milijonai gyventojų, egzistuoja ir kita el. erdvė – tai dark web ir deep dark web. Yra paskaičiuota, kad mums įprasta el. erdvė sudaro tik 0,3% visos el erdvės. Likusi dalis – dark web ir deep dark web. Daugeliu atveju dark web ir deep dar k web yra naudojami nusikalstamais tikslais, nors yra galimas ir nenusikalstamas panaudojimas. Technologinių gigančių kaltinimas pagalba teroristams ir masinis asmens duomenų iš jų perėmimas atsirado neatsitiktinai. Pvz., Faceebook 2014 m. paskelbė, kad ji yra palaikoma ir TOR tinkle.

[797] Daniel Severson, „American Surveillance of Non-U.S. Persons: Why New Privacy Protections Offer Only Cosmetic Change Notes", *Harvard International Law Journal* 56, no. 2 (2015): 465–514.

2. bausmių vykdymo;
3. apsaugos nuo grėsmių visuomenės saugumui ir jų prevencijos, tikslais[798].

Visi šie tikslai sutrumpintai yra vadinami teisėsaugos tikslais.

Kompetentinga institucija Direktyvoje yra apibrėžiama kaip:

1) bet kokia valdžios institucija, kompetentinga nusikalstamų veikų prevencijos, tyrimo, atskleidimo ar baudžiamojo persekiojimo už jas arba bausmių vykdymo, be kita ko, apsaugos nuo grėsmių visuomenės saugumui ir jų prevencijos, tikslais; arba
2) bet kokia kita įstaiga arba subjektas, kuriems pagal valstybės narės teisę pavesta vykdyti viešosios valdžios funkcijas ir naudotis viešaisiais įgaliojimais nusikalstamų veikų prevencijos, tyrimo, atskleidimo ar baudžiamojo persekiojimo už jas arba bausmių vykdymo, be kita ko, apsaugos nuo grėsmių visuomenės saugumui ir jų prevencijos, tikslais.

Kokias institucijas ši sąvoka apima? Pirmasis papunktis labai aiškiai išskiria, jog ji apima visas institucijas, kurias mes paprastai laikome teisėsaugos institucijomis: policiją, STT, FNTT ir kt. Antrasis Teisėsaugos tikslais tvarkomų asmens duomenų direktyvos punktas praplečia kompetentingų institucijų sąvoką iki bent kokių įstaigų arba subjektų, kuriems pagal valstybės narės teisę pavesta vykdyti viešosios valdžios funkcijas ir naudotis viešaisiais įgaliojimais nusikalstamų veikų prevencijos, tyrimo, atskleidimo ar baudžiamojo persekiojimo už jas arba bausmių vykdymo, be kita ko, apsaugos nuo grėsmių visuomenės saugumui ir jų prevencijos, tikslais, tuo sukeldamas klausimų kas tokiomis įstaigomis ar subjektais gali būti. Lietuvos Respublikos Konstitucinis Teismas konstatavo, kad „Valstybė savo funkcijas vykdo per atitinkamų institucijų sistemą, apimančią visų pirma valstybės institucijas“. Tačiau, tęsdamas savo mintį, Konstitucinis Teismas taip pat konstatavo, kad valstybė savo funkcijas gali tam tikra apimtimi vykdyti ne vien tik per valstybės, bet ir ne per valstybės institucijas, jeigu tenkinamos tokios sąlygos:

1) joms pagal įstatymus yra pavesta (patikėta) vykdyti tam tikras valstybės funkcijas, arba
2) jos tam tikromis įstatymuose apibrėžtomis formomis ir būdais dalyvauja vykdant valstybės funkcijas[799, 800].

Pavyzdžiui, be teisėsaugos institucijų, viešosios valdžios funkcijas apsaugos nuo grėsmių visuomenės saugumui ir jų prevencijos, tikslais Lietuvoje vykdo ir vietos savivaldos

---

[798] „2016 m. balandžio 27 d. Europos Parlamento ir Tarybos direktyva (ES) 2016/680 dėl fizinių asmenų apsaugos kompetentingoms institucijoms tvarkant asmens duomenis nusikalstamų veikų prevencijos, tyrimo, atskleidimo ar baudžiamojo persekiojimo už jas arba bausmių vykdymo tikslais ir dėl laisvo tokių duomenų judėjimo, ir kuriuo panaikinamas Tarybos pamatinis sprendimas 2008/977/TVR“, 1 str. *EUR-Lex*, žiūrėta 2020 m. rugpjūčio 15 d., https://eur-lex.europa.eu/legal-content/lt/TXT/?uri=CELEX%3A32016L0680.

[799] „Lietuvos Respublikos Konstitucinio Teismo 2004 m. gruodžio 13 d. nutarimas „Dėl kai kurių teisės aktų, kuriais reguliuojami valstybės tarnybos ir su ja susiję santykiai, atitikties Lietuvos Respublikos konstitucijai ir įstatymams“, žiūrėta 2020 m. rugpjūčio 16 d., https://www.lrkt.lt/lt/teismo-aktai/paieska/135/ta275/content.

[800] *Ibid.*

subjektai[801]. A. Novikovas išskiria kelias viešosios tvarkos apsaugos funkcijos įgyvendinimo formas:

1) vietos savivalda pati savarankiškai įgyvendina šią funkciją per savivaldybių sukurtas viešosios tvarkos apsaugos tarnybas;
2) pasitelkiant savivaldybių teritoriją aptarnaujančią policiją;
3) pasitelkiant savivaldybių teritoriją aptarnaujančias privačias saugos tarnybas;
4) kuriant savanoriškas tarnybas, sudaromas iš vietos gyventojų[802].

Tačiau viešojo saugumo užtikrinimo funkcija savivaldybių privačioms saugos tarnyboms yra pavedama ne įstatymu, o sudarant paslaugų teikimo sutartis. Savanoriškos tarnybos taip pat negali būti laikomos kompetentingomis institucijomis, kadangi yra visuomeninės organizacijos, negalinčios savarankiškai taikyti administracinio poveikio priemonių ir valstybės funkcijų vykdymas joms nėra numatomas įstatymu. Taigi, tiek privačios saugos tarnybos, tiek savanoriškos viešosios tvarkos saugojimo visuomeninės organizacijos vadovaujantis Lietuvos Respublikos Konstitucinio Teismo doktrina neatitinka kompetentingų institucijų sąvokos pagal Lietuvos teisę. Tokiu atveju Lietuvoje gali susidaryti situacija, kad tuos pačius elektroninius asmens duomenis renkant teisėsaugos institucijoms galios vienoks teisinis režimas, o teisėsaugos užsakymus vykdantiems subjektams – kitoks. Kadangi, valstybės funkcijų vykdymas pagal kitų valstybių narių nacionalinę teisę ir doktriną gali būti aiškinamas skirtingai, tai skirtingose valstybėse narėse skirtingi subjektai gali būti laikomi kompetentingomis institucijomis Direktyvos prasme, tačiau jie visi asmens duomens rinks tų asmenų, kurie naudojasi tų pačių paslaugų el. erdvėje teikėjų paslaugomis ir, tikėtina, vėliau tais elektroniniais duomenimis galimai keisis tarpusavyje. Todėl gali susidaryti situacija, kai vienos valstybės narė gauna duomenis iš kitos valstybės narės institucijos, kuri pagal pirmosios nacionalinę teisę nėra laikoma kompetentinga institucija Direktyvos prasme. Tokiu atveju diskusiniu tampa asmens duomenų naudojimo klausimas. Tačiau tai nėra vienintelis klausimas. Dar vienas klausimas kyla ar privataus sektoriaus įmones, kurios iš esmės vykdo teisėsaugos institucijų funkcijas ir užsiima komercine žvalgyba, galime laikyti kompetentingu subjektu?

Oficialiai tokios įmonių veiklos šakos kaip komercinė žvalgyba nėra išskirtos, ir net ne visos šioje srityje veikiančios įmonės save iš karto tokiomis identifikuoja[803], tačiau tokia kategorija neoficialiai egzistuoja. Financial Times duomenimis ši įmonių kategorija ypač sustiprėjo 2008 m. dėl finansinės krizės, padažnėjusių kibernetinių atakų ir neišvengiamos globalizacijos. Gartner duomenimis, 2015 m. žvalgybą el. erdvėje vykdančių įmonių pajamos sudarė $76.9 milijardų per metus. Duomenų apie privačias sekimo paslaugas teisėsaugos ir žvalgybos institucijoms teikiančias įmones nėra daug. Pagrindiniai jų skiriamieji bruožai, manoma, yra, kad vadovais, įkūrėjais ir dar-

[801] Andrejus Novikovas, „Viešosios tvarkos apsauga savivaldybių teritorijoje: teisinis ir organizacinis aspektai“, *Jurisprudencija* 49, no. 41 (2003): 46–53.

[802] *Ibid.*

[803] Robert Tchenguiz, „A New Breed of Commercial Intelligence Company“, *Financial Times*, 2015, žiūrėta 2020 m. rugsėjo 7 d., https://www.ft.com/content/e0133cf6-cd66-11e4-9144-00144feab7de.

buotojais paprastai yra buvę saugumo tarnybų ar kariuomenės darbuotojai, padalinių vadai ir duomenis tokios institucijos renka būtent elektroninėje erdvėje[804]. Manoma, kad svarbiausiomis iš jų laikytinos AEGIS (Didžioji Britanija), Black Cube (Izraelis ir Didžioji Britanija), Booz Allen Hamilton (JAV), Control Risks Group (Didžioji Britanija), Groupe GEOS (Prancūzija), Fusion GPS (JAV), Hakluyt & Company (Didžioji Britanija), Kroll Inc. (JAV), Oxford Analytica, Pinkerton National Detective Agency (JAV įsteigusi, bet paslaugas teikianti visame pasaulyje) Smith Brandon International, Inc. (JAV), Stodacom (Afrika), Stratfor (JAV)[805]. Didžioji dauguma iš šių įmonių yra įsisteigusios UK arba JAV, todėl tiesiogiai joms ES teisės aktai nėra aktualūs. Apie ES reglamentavimą kalbėti negalime ir tuo atveju, kai tokias paslaugas teikia ne teisėsaugos, bet žvalgybos institucijoms, kadangi nacionalinis saugumas yra Direktyvos taikymo išimtis. Tačiau yra galimi keli tokio pobūdžio veiklą vykdančių institucijų bendradarbiavimo su teisėsaugos institucijomis ES scenarijai:

1) kuomet tokios įmonės yra įsisteigę ES ir teikia paslaugas ES teisėsaugos institucijoms, arba
2) jeigu tokios įmonės nors ir nėra įsisteigę ES, tačiau paslaugas teikia ES teisėsaugos institucijoms ir sutartyje su teisėsaugos institucija taikytina teisė yra numatyta ES valstybės narės, arba
3) jeigu tokios įmonės nors ir nėra įsisteigę ES, tačiau paslaugas teikia ES teisėsaugos institucijoms ir sutartyje su teisėsaugos institucija taikytina teisė yra numatyta ne ES valstybės narės.

Pirmuoju atveju, deleguotąsias teisėsaugos funkcijas vykdančioms privačioms žvalgybos įmonėms Direktyva nebūtų taikoma. Direktyva yra taikoma kompetentingoms institucijoms, kuriomis gali būti nebūtinai valdžios subjektas. Kompetentinga institucija gali būti laikoma ir privati įmonė (šiuo atveju žvalgybos el. erdvėje paslaugas teikianti įmonė), tačiau tik tuo atveju, jeigu jai tokios teisėsaugos funkcijos yra pavestos pagal valstybės narės teisę t. y. įtvirtintos įstatymuose. ES tokio atvejo, autorės žiniomis, nėra. Tačiau, pavyzdžiui, Naujosios Zelandijos Kratų ir elektroninės žvalgybos akte (angl. *Search and Surveillance Act*) yra tiesiogiai įtvirtinta galimybė privačioms įmonėms rinkti asmens duomenis el. erdvėje teisėsaugos tikslais[806]. Naujosios Zelandijos Žmogaus teisių komitetas tokią teisės akto nuostatą laikė kvestionuotina teisės į asmens duomenų apsaugą užtikrino atžvilgiu[807]. Taigi ES įsisteigusioms ir asmens duomenų rinkimo teisėsaugos tikslais paslaugas teikiančioms privačioms įmonėms galėtų būti taikomos Reglamento nuostatos, o asmens duomenų rinkimo pagrindu galėtų būti teisėtas interesas, jeigu Reglamente nebūtų nuostatos, jog jis nėra taikomas asmens duomenų tvarkymui teisėsaugos tikslais, kas iš esmės yra daroma šio tipo įmonių. Taigi, taip

---

804 Tchenguiz, *supra note*, 803.

805 Michael Smith, „Private Intelligence Companies How the Spooks Moved in on Big Business“, žiūrėta 2020 m. rugpjūčio 17 d., https://web.archive.org/web/20090205143528/http://michaelsmithwriter.com/pdf/intelligence_companies.pdf.

806 „Search and Surveillance Act 2012 No 24 (as at 12 April 2019), Public Act Contents – New Zealand Legislation“, žiūrėta 2020 m. rugsėjo 7 d., http://www.legislation.govt.nz/act/public/2012/0024/193.0/DLM2136536.html.

807 „Human Rights Commission: Intelligence and Security Bill Good Effort, but Scrutiny Needed“, žiūrėta 2020 m. rugsėjo 7 d., https://www.hrc.co.nz/news/intelligence-and-security-bill-good-effort-scrutiny-needed/.

vadinamos žvalgybos el. erdvėje paslaugas teikiančios ES įsisteigę įmonės netenkina sąlygų, kad joms būtų taikomi Direktyvos pagrindu priimti teisės aktai, nei kad būtų taikomas Reglamentas. Todėl vieninteliu asmens teisių apsaugos garantu galėtų būti sutartyje su tokia institucija įtvirtinti teisių į asmens duomenų apsaugą užtikrinimo garantai. Tačiau jų privalomas nėra imperatyvus ir yra abiejų šalių diskusijų objektu. Bet jeigu tokios įmonės paslaugas teikia žvalgyboms institucijoms, tikėtina, kad ES teisė joms yra netaikoma nepriklausomai nuo įsisteigimo vietos, kadangi Reglamente yra nuostata teigianti, kad asmens duomenų rinkimui nacionalinio saugumo užtikrinimo tikslais (kas sudaro žvalgybos tikslus) Reglamentas nėra taikomas[808].

Situacija yra labai panaši ir su ne ES įsisteigusiomis žvalgybos paslaugas teikiančiomis įmonėmis. Nors Direktyva reglamentuoja asmens duomenų perdavimą trečiosiose šalyse įsteigtiems asmens duomenų gavėjams, kuriais nėra numatyto privalomo reikalavimo, kad būtų teisėsaugos institucijos[809], tačiau ji nereikalauja, kad trečiose šalyse įsteigti asmens duomenų gavėjai, rinkdami asmens duomenis ir perduodami juos ES teisėsaugos institucijoms šiuos duomenis rinktų laikydamiesi ES ar ES valstybių narių teisės. Preziumuoti, kad tokiu atveju galiotų Reglamento nuostatos taip pat negalime, nes ne ES šalyse įsteigtiems asmenims jis galioja tik jeigu, jie teikia paslaugas duomenų subjektams. Teisėsaugos institucijos nėra asmens duomenų subjektai. Vadinasi, tik sutartyje įtvirtinti asmens duomenų apsaugos reikalavimai galėtų būti užtikrinimo garantu. Tačiau nėra niekur įtvirtinto reikalavimo, jog sutartims būtų taikoma valstybių narių ar ES teisė. Todėl jeigu taikytina teise pasirenkama ne EŽTK valstybių narių teisė, pvz. JAV teisė, tuomet asmenų teisių apsauga tampa labai minimalia, nes JAV ne JAV asmenims IV JAV Konstitucijos pataisa garantuojama teisė į asmens duomenų apsaugą negalioja. Be žvalgybos paslaugas teikiančių įmonių rinkos, asmens duomenų paslaugų teikimo rinką turi ir asmens duomenų apsaugos brokeriai, kurie asmens duomenis taip pat renka iš el. erdvės[810]. Santykių su jais reglamentavimo klausimai yra analogiški žvalgybos paslaugas teikiančių įmonių reglamentavimui. Taigi teisėsaugos institucijų santykiai su žvalgybos paslaugas el. erdvėje teikiančiomis įmonėmis taip pat yra silpnoji Direktyvos vieta, rodanti jos nevisišką pritaikomumą asmens duomenų rinkimui el. erdvėje.

Kaip Direktyva taptų pajėgi užtikrinti teisę į asmens duomenų apsaugą duomenis renkant el. erdvėje? Direktyvoje yra įtvirtinti bendrieji principai, tačiau nėra numatytų net minimalių asmens duomenų rinkimo el. erdvėje procedūrų. Ikiteisminių tyrimų procesų skirtumas buvo viena iš esminių nuolat kritikuojamų Pamatinio sprendimo

[808] „2016 m. balandžio 27 d. Europos Parlamento ir Tarybos reglamentas (ES) 2016/679 dėl fizinių asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo ir kuriuo panaikinama Direktyva 95/46/EB (Bendrasis duomenų apsaugos reglamentas)“, 23 str., *EUR-Lex*, žiūrėta 2020 m. rugpjūčio 15 d., https://eur-lex.europa.eu/legal-content/LT/TXT/?uri=CELEX%3A32016R0679.

[809] „2016 m. balandžio 27 d. Europos Parlamento ir Tarybos reglamentas (ES) 2016/679 dėl fizinių asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo ir kuriuo panaikinama Direktyva 95/46/EB (Bendrasis duomenų apsaugos reglamentas)“, 39 str., *EUR-Lex*, žiūrėta 2020 m. rugpjūčio 15 d., https://eur-lex.europa.eu/legal-content/LT/TXT/?uri=CELEX%3A32016R0679.

[810] Alexander Tsesis, „The Right to Erasure: Privacy, Data Brokers, and the Indefinite Retention of Data“, *Wake Forest Law Review* 49, no. 2 (2014): 433–84.

silpnybių[811]. Direktyva turėjo suvienodinti procedūras valstybėse narėse[812]. Tačiau kaip ir pamatiniame sprendime, taip ir Direktyvoje tėra numatytos tik keitimosi tarp valstybių narių ir trečiųjų šalių asmens duomenimis procedūros. Rinkimo procedūrų nėra numatyta. Suvienodintos iki tokio lygio, kad leistų vienoje valstybėje narėje surinktus įrodymus pripažinti kitoje valstybėje narėje procedūros yra svarbios renkant bent kuriuos duomenis. Bet dėl ypatingo asmens duomenų rinkimo ir pačių asmens duomenų pobūdžio el. erdvėje pobūdžio, jos yra ypač svarbios būtent renkant duomenis el. erdvėje. Nėra reikalinga, kad Direktyva standartizuotų visus asmens duomenų rinkimo veiksmus. Tai būtų sudėtinga padaryti jau įsisenėjusioms asmens duomenų rinkimo fizinėje el. erdvėje procedūroms. Tačiau asmens duomenų rinkimo el. erdvėje praktika dar tik formuojasi valstybėse narėse[813]. Ir ji formuojasi skirtingai. Todėl būtent besiformuojant praktikai, ES lygiu galėtų standartizuoti tam tikras asmens duomenų rinkimo el. erdvėje procedūras: sankcionavimo, meta ir turinio duomenų rinkimo iš ES ir ne ES esančių ICT paslaugų teikėjų procedūras, subjekto informavimo, privalomų sutartinių santykių su juridiniais asmenimis teisių į asmens duomenų apsaugą reikalavimų. Asmens duomenų rinkimas el. erdvėje yra vienas iš dažniausiai naudojamų tarptautinio pobūdžio nusikalstamų veikų tyrimo metodų[814], tačiau Jungtinės Tautos valstybių narių procedūrų skirtingumą laiko viena iš didžiausių problemų[815]. Dabartinės Direktyvos nuostatos šios problemos nesprendžia. Todėl arba Direktyva turėtų būti papildoma atskiru skyriumi dėl asmens duomenų rinkimo el. erdvėje, arba turėtų būti priimtas atskiras teisės aktas, reglamentuojantis asmens duomenų rinkimą el. erdvėje. Šią idėją disertacijos autorė pristatė mokslinėje publikacijoje[816]. Kiek vėliau 2018. EK paskelbė e. įrodymų direktyvos projektą, kurio idėja vertinama teigiamai, tačiau turinys toje srityje dirbančių įmonių – neigiamai[817].

---

811 Eleni Kosta, Fanny Coudert ir Jos Dumortier, „Data Protection in the Third Pillar: In the Aftermath of the ECJ Decision on PNR Data and the Data Retention Directive“, *International Review of Law, Computers & Technology* 21, no. 3 (2007): 347–62. „Green Paper on obtaining evidence in criminal matters from one Member State to another and securing its admissibility (COM/2009/0624 final)“, *EUR-Lex*, žiūrėta 2020 m. rugpjūčio 17 d. https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A52009DC0624 .

812 „2016 m. balandžio 27 d. Europos Parlamento ir Tarybos direktyva (ES) 2016/680 dėl fizinių asmenų apsaugos kompetentingoms institucijoms tvarkant asmens duomenis nusikalstamų veikų prevencijos, tyrimo, atskleidimo ar baudžiamojo persekiojimo už jas arba bausmių vykdymo tikslais ir dėl laisvo tokių duomenų judėjimo, ir kuriuo panaikinamas Tarybos pamatinis sprendimas 2008/977/TVR“, *EUR-Lex*, žiūrėta 2020 m. rugpjūčio 15 d., https://eur-lex.europa.eu/legal-content/lt/TXT/?uri=CELEX%3A32016L0680.

813 Natasha Lomas, „Mass Surveillance for National Security Does Conflict with EU Privacy Rights, Court Advisor Suggests“, *TechCrunch*, žiūrėta 2020 m. rugsėjo 7 d., https://social.techcrunch.com/2020/01/15/mass-surveillance-for-national-security-does-conflict-with-eu-privacy-rights-court-advisor-suggests/.

814 „Current Practices in Electronic Surveillance in the Investigation of Serious and Organized Crime“, *United Nations*, 2009, žiūrėta 2020 m. rugpjūčio 17 d., https://www.unodc.org/documents/organized-crime/Law-Enforcement/Electronic_surveillance.pdf.

815 *Ibid.*

816 International multidisciplinary scientific conference on social sciences and arts. SGEM 2015, Bulgaria.

817 Anastasiya Kazakova, „The EU's e-Evidence & the U.S. CLOUD Act: Race Only to Start“, *Kaspersky*, žiūrėta 2020 m. rugsėjo 7 d., https://www.kaspersky.com/about/policy-blog/privacy/e-evidence-and-cloud-act.

3.3.2. Tarpvalstybinio elektroninių įrodymų rinkimo baudžiamosiose bylose reglamentavimo projektas

EK duomenimis asmens duomenų rinkimas elektroninėje erdvėje yra atliekamas 85% ikiteisminių tyrimų. Du trečdaliai tyrimui reikalingų asmens duomenų būna kitoje nei ikiteisminį tyrimą atliekančios valstybės narės jurisdikcijoje[818]. Problemos dėl jurisdikcijos ir įrodymų rinkimo vadovaujantis tarpusavio pagalbos baudžiamosiose bylose sutartimis 2018 m. paskatino EK pateikti dvejų teisės aktų projektų siūlymus: 1) Reglamento dėl Europos elektroninių įrodymų baudžiamosiose bylose pateikimo ir saugojimo orderių[819], ir 2) Direktyvos, kuria nustatomos teisinių atstovų skyrimo įrodymams baudžiamosiose bylose rinkti suderintos taisyklės[820] bei 2019 m. pradėti derybas su JAV dėl bendradarbiavimo renkant elektroninius įrodymus[821]. Reglamento dėl Europos elektroninių įrodymų baudžiamosiose bylose pateikimo ir saugojimo orderių projektu nustatomi privalomi Europos įrodymų pateikimo (toliau – EĮPO) ir saugojimo orderiai (toliau – EĮSO). Abiejų rūšių orderius turi išduoti ar patvirtinti valstybės narės teisminė institucija. Orderis gali būti išduodamas siekiant išsaugoti (Saugojimo orderis) arba nurodyti pateikti duomenis (Pateikimo orderis), kuriuos saugo kitoje jurisdikcijoje esantis paslaugų teikėjas ir kurie yra būtini įrodymai atliekant baudžiamuosius tyrimus arba baudžiamajame procese. Tokie orderiai gali būti išduodami tik jeigu dėl tos pačios nusikalstamos veikos panašioje vidaus situacijoje išduodančiojoje valstybėje galima taikyti panašią priemonę. Abiejų rūšių orderiai gali būti įteikiami elektroninių ryšių paslaugų teikėjams, socialiniams tinklams, elektroninėms prekyvietėms, kitiems prieglobos paslaugų teikėjams ir interneto infrastruktūros, pvz., IP adresų ir domeno vardų registrų, teikėjams arba jų teisiniams atstovams, jei jie yra paskirti. Europos įrodymų saugojimo orderis, panašiai kaip ir Europos įrodymų pateikimo orderis, yra skirtas už išduodančiosios valstybės narės jurisdikcijos ribų esančiam teisiniam atstovui siekiant išsaugoti duomenis, kai vėliau numatoma prašyti pateikti tuos duomenis, pvz., savitarpio teisinės pagalbos kanalais, jei tai yra trečiosios šalys, arba dalyvaujančioms valstybėms narėms naudojant Europos tyrimo orderį (toliau – ETO). Pagal EĮSO leidžiama išsaugoti būsimus duomenis, prieiga prie duomenų vėliau nei buvo gautas Europos įrodymų saugojimo orderis (istorinio pobūdžio asmens duomenų) nesuteikiama. Europos įrodymų pateikimo orderio išdavimas priklausys nuo pra-

---

[818] „Frequently Asked Questions: New EU rules to obtain electronic evidence“, *European Commission*, 2018, žiūrėta 2020 m. rugpjūčio 25 d., https://ec.europa.eu/commission/presscorner/detail/en/MEMO_18_3345.

[819] „Proposal for a Regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal matters“, *EUR-Lex*, žiūrėta 2020 m. rugpjūčio 25 d., https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1524129181403&uri=COM:2018:225:FIN.

[820] „Proposal for a Directive of the European Parliament and of the Council laying down harmonised rules on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings“, *EUR-Lex*, žiūrėta 2020 m. rugpjūčio 25 d., https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1524129181403&uri=COM:2018:226:FIN.

[821] „Recommendation for a Council Decision authorising the opening of negotiations in view of an agreement between the European Union and the United States of America on cross-border access to electronic evidence for judicial cooperation in criminal matters“, *European Commission*, žiūrėta 2020 m. rugpjūčio 25 d., https://ec.europa.eu/info/sites/info/files/recommendation_council_decision_eu_us_e-evidence.pdf.

šomų suteikti asmens duomenų tipo: metaduomenys galės būti suteikiami dėl visų nusikalstamų veikų, turinio – tik dėl tokių nusikaltimų, už kuriuos valstybės narės, iš kurios prašoma suteikti duomenų, baudžiamajame įstatyme bus numatyta ne mažesnė nei 3 metų laisvės atėmimo bausmė[822].

Direktyva, kuria nustatomos teisinių atstovų skyrimo įrodymams baudžiamosiose bylose rinkti suderintos taisyklės paslaugų elektroninėje erdvėje teikėjams nustatomas įpareigojimas paskirti ES teisinį atstovą, kuris priimtų, vykdytų ir priverstinai vykdytų nurodymus, kuriais kompetentingos nacionalinės institucijos siekia surinkti įrodymus baudžiamosiose bylose. Projekto aiškinamajame memorandume teigiama, kad nustačius visiems ES veikiantiems paslaugų elektroninėje erdvėje teikėjams taikomą įpareigojimą paskirti teisinį atstovą būtų užtikrinta, kad visada bus aiškus adresatas, kuriam būtų galima teikti nurodymus, kuriais siekiama surinkti įrodymus baudžiamosiose bylose. Manoma, kad tokiu būdu paslaugų teikėjams būtų lengviau vykdyti šiuos nurodymus, nes teisinis atstovas būtų atsakingas už šių nurodymų priėmimą, vykdymą ir priverstinį vykdymą paslaugų teikėjo vardu[823].

Europos įrodymų pateikimo ir saugojimo orderiai yra trečia ES įtvirtintų orderių rūšis[824]. Kaip teigia R. Jurka, ES elektroninių įrodymų rinkimo reglamentavimo paketu yra sukuriamas tiesioginių ryšių principas, kildinamas iš Europos baudžiamojoje justicijoje taikomo abipusio pripažinimo maksimos. Vadovaujantis šiuo principu, skirtingai nei ETO atveju, EĮPO ir EĮSO išduodanti teisminė institucija, šiuos orderius ir juos lydinčius sertifikatus tiesiogiai perduoda paslaugų teikėjams arba jų paskirtiems teisiniams atstovams, o ne kitos valstybės narės teisėsaugos institucijai. Tokiu būdu šiomis teisėkūros idėjomis siekiama ne tik palengvinti, bet ir spartinti tarptautinio bendradarbiavimo baudžiamosiose bylose procesus aplenkiant kai kurias biurokratines procedūras[825]. Tačiau pagrindinis tikslas, kurio yra siekiama EĮPO ir EĮSO yra įspręsti elektroninių įrodymų rinkimo skirtingose jurisdikcijose problemas. Disertacijos tyrimo rezultatai rodo, kad pasiūlytas reglamentavimas negali išspręsti jurisdikcijos problemos, kadangi net jeigu paslaugos teikėjas yra įsisteigęs ES, asmens duomenys (elektroniniai įrodymai) yra saugomi ne juridiniame asmenyje, o serveriuose – duomenų saugojimo centruose. kurie dažniausiai yra ne ES. Didžiąją dalį paslaugas elektroninėje erdvėje ES gyventojams teikiančios rinkos valdo JAV kilmės įmonės: Google, kuriai taip pat priklauso YouTube, Facebook, kuriai taip pat priklauso WhatsApp ir Instagram, Microsoft, kuriai priklauso Skype, Apple ir Amazon. Nors šios įmonės turi dukterines įmones ES, bet serveriai, kuriuose jos saugo asmens duomenis neprivalo

---

[822] „Proposal for a Regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal matters“, *EUR-Lex*, žiūrėta 2020 m. rugpjūčio 25 d., https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1524129181403&uri=COM:2018:225:FIN.

[823] „Proposal for a Directive of the European Parliament and of the Council laying down harmonised rules on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings“, *EUR-Lex*, žiūrėta 2020 m. rugpjūčio 25 d., https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1524129181403&uri=COM:2018:226:FIN.

[824] Europos arešto orderis buvo įtvirtintas 2008, o Europos tyrimo orderis 2014 m.

[825] Raimondas Jurka, „Įrodymų perdavimo Europos Sąjungos valstybių narių baudžiamojoje justicijoje iššūkiai ir atradimai“, *Jurisprudencija,* (2019, 26(2)), 322.

būti ES arba gali būti keliose jurisdikcijose[826]. Pvz., Facebook dauguma serverių yra Švedijoje[827], kuri nėra ES valstybė narė. Apple daugumą duomenų saugo Microsoft ir Amazon serveriuose[828]. Microsoft turi 100 duomenų saugojimo centrų visame pasaulyje[829]. Didžioji jų dauguma – ne ES [830]. Oficialiame Microsoft tinklapyje tarp teikiamų paslaugų ir privalumų yra įvardijama ir „Apsauga nuo teismo orderių“[831]. Tai rodo, kad Microsoft yra orientuota į savo kliento, o ne ES teisėsaugos institucijų interesų interesus, todėl tikslingai gali asmens duomenis saugoti ne ES jurisdikcijose. Duomenų buvimo vietos jurisdikcijos problematika visuomet keliama privatumą debesų kompiuterijoje analizuojančių mokslininkų [832]. Kita vertus, kaip rodo disertacijos 5 skyriuje pateikta analizė, kai kurie paslaugų el. erdvėje teikėjai net ir nesant privalomo teisinio reglamentavimo teisėsaugos institucijoms tam tikrus duomenis suteikia savanoriškais pagrindais. Tačiau dabartiniu Reglamento projektu yra sukeliama problema dėl EĮPO imperatyvaus vykdymo reikalavimo vykdyti paslaugų teikėjui, kadangi atsižvelgiant į tai, kad yra didelė tikimybė, kad asmenų duomenys yra saugomi ne ES valstybėse narėse esančiuose serveriuose, paslaugos teikėjas dėl skirtingų jurisdikcijų teisinio reglamentavimo kolizijos ES teisėsaugos institucijoms dažnai negalės suteikti jų prašomų duomenų[833], o šiuos (nepaisant reglamentavimo kolizijos) suteikus – galės būti keliamas dėl tokių įrodymų teisėtumo ir priimtinumo. Taigi, Reglamentu yra sukuriama priemonė kitoje jurisdikcijoje esančių elektroninių įrodymų rinkimui, tačiau jame nėra įtvirtintas jurisdikcijos kolizijų sprendimo mechanizmas.

Reglamente yra numatyti apribojimai dėl asmens duomenų rinkimo pagal EĮRO bei EĮSO. Sandorių ir komunikacijos turinio duomenis pagal EĮRO ir EĮSO galės būti išduodami tik dėl nusikalstamų veikų, už kurias skiriama ne mažesnė nei 3 metų laisvės atėmimo bausmė, teroristinių nusikaltimų arba, kaip nurodyta pasiūlyme, už konkrečius kibernetinius, elektroninėmis priemonėmis daromus ar su terorizmu susiju-

---

826 S. A. Baset ir H. G. Schulzrinne, „An Analysis of the Skype Peer-to-Peer Internet Telephony Protocol“, in *Proceedings IEEE INFOCOM 2006. 25TH IEEE International Conference on Computer Communications* (Proceedings IEEE INFOCOM 2006. 25TH IEEE International Conference on Computer Communications, Barcelona, Spain: IEEE, 2006), 1–11, doi:10.1109/INFOCOM.2006.312.

827 „Facebook plans third data center in Luleå, Sweden“, *Data Center Dynamics,* žiūrėta 2020 m. rugpjūčio 29 d., https://www.datacenterdynamics.com/en/news/facebook-plans-third-data-center-in-lule%C3%A5-sweden/

828 Glenn Fleishman ir kt., „How to Find out Where Apple Stores Your ICloud Data (Spoiler: You Can't Exactly)“, *Macworld*, 2018, žiūrėta 2020 m. rugpjūčio 25 d., https://www.macworld.com/article/3274584/where-does-apple-stores-your-icloud-data.html.

829 „Azure facilities, premises, and physical security“, *Microsoft,* žiūrėta 2020 m. rugpjūčio 26 d., https://docs.microsoft.com/en-us/azure/security/fundamentals/physical-security.

830 „Microsoft“, *DataCenters*, žiūrėta 2020 m. rugpjūčio 26 d., https://www.datacenters.com/providers/microsoft.

831 Microsoft Privacy. Where is your data located?, *Microsoft*, žiūrėta 2020 m. rugpjūčio 26 d., https://www.microsoft.com/en-us/trust-center/privacy/data-location.

832 Žr. pvz. Dan Jerker B. Svantesson, *Solving the Internet Jurisdiction Puzzle*, *Solving the Internet Jurisdiction Puzzle* (Oxford University Press, 2017), žiūrėta 2020 m. rugpjūčio 29 d., https://oxford.universitypressscholarship.com/view/10.1093/oso/9780198795674.001.0001/oso-9780198795674. Stanislaw Tosza, „All Evidence Is Equal, but Electronic Evidence Is More Equal than Any Other: The Relationship between the European Investigation Order and the European Production Order“, *New Journal of European Criminal Law* 11, no. 2 (June 1, 2020): 161–83, doi:10.1177/2032284420919802.

833 Stanislaw Tosza, „All Evidence Is Equal, but Electronic Evidence Is More Equal than Any Other: The Relationship between the European Investigation Order and the European Production Order“, *New Journal of European Criminal Law* 11, no. 2 (June 1, 2020): 170, doi:10.1177/2032284420919802.

sius nusikaltimus. Duomenys apie abonentą ir prieigos duomenis galės būti suteikiami visais atvejais nepriklausomai nuo nusikalstamos veikos sunkumo[834]. Šios nuostatos kelia diskusijas dėl kelių aspektų:

1) Reglamente yra vartojamos netikslios asmens duomenų kategorijų sąvokos. Europos asmens duomenų priežiūros pareigūno institucija savo vertinime siūlo vartoti šiuo metu ES teisėje pradedamas vartoti komunikacijos turinio ir metaduomenų sąvokas[835]. Šias sąvokas disertacijos autorė taip pat siūlo perkelti į Lietuvos Respublikos BK (plačiau apie tai 1 disertacijos skyriuje).
2) ESTT 2018 m. byloje Nr. C-207/16 konstatavo, kad teisės į asmens duomenų apsaugą suvaržymas duomenis renkant iš elektroninių ryšių paslaugų teikėjų yra proporcingas, jeigu asmens duomenys yra renkami tiriant sunkius nusikaltimus[836]. EĮPO ir EĮSO galės būti išduodami tiriant visus nusikaltimus, už kuriuos numatyta ne mažesnė nei 3 metų laisvės atėmimo bausmė. Lietuvos Respublikos BK sunkiu nusikaltimu laikomas nusikaltimas už kurį numatyta didžiausia bausmė viršija 6 metus laisvės atėmimo (BK 11 str. 5 d.), o nusikaltimai, už kuriuos numatyta didžiausia bausmė viršija 3 metus laisvės atėmimo, bet neviršija 6 metų laisvės atėmimo yra laikomi apysunkiais (BK 11 str. 4 d.). Asmens duomenys, vadovaujantis BPK 154 str., Lietuvos teisėsaugos institucijų gali būti renkami ne tik sunkių, bet ir apysunkių nusikaltimų atveju. Todėl Reglamente įtvirtintų nusikaltimų apimtis atitiktų Lietuvos Respublikos BPK 154 str., tačiau Europos asmens duomenų apsaugos priežiūros institucija Reglamento projekto vertinime nurodo, kad 3 metų laisvės atėmimo bausmės reikalavimas yra per platus ir neatitinka teismų praktikos dėl teisės apribojimo proporcingumo[837].
3) Dauguma komunikacijos elektroninėje erdvėje turinio yra užšifruoti ištisiniu šifravimu (angl. *end to end encryption*), kas reiškia, kad daugumą komunikacijos paslaugų elektroninėje erdvėje sudarantys paslaugų teikėjai (pvz., WhatsApp, Google, Facebook ir kt.) teisėsaugos institucijoms negalės pateikti komunikacijos turinio. Tačiau komunikacijos metaduomenis paslaugų elektroninėje erdvėje teikėjai gali suteikti visais atvejais, įskaitant ištisiniu šifravimu užšifruotą komunikaciją. Kaip jau minėta disertacijoje, mokslininkai komunikacijos metaduomenis laiko lygiaverčiais komunikacijos turiniui[838]. EŽTT ir ESTT konkrečiai nėra pasisakęs dėl metaduomenų ir turinio duomenų tarpusavio santykio, tačiau abu teismai yra

[834] „Proposal for a Regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal matters", 5 str., *EUR-Lex*, žiūrėta 2020 m. rugpjūčio 25 d., https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1524129181403&uri=COM:2018:225:FIN.

[835] „Opinion on Proposals regarding European Production and Preservation Orders for electronic evidence in criminal matters No. 7/2019", *European Data Protection Supervisor*, 2019, 9, žiūrėta 2020 m. rugpjūčio 29 d., https://edps.europa.eu/sites/edp/files/publication/19-11-06_opinion_on_e_evidence_proposals_en.pdf.

[836] „European Court of Justice, case C-207/16 (Ministerio Fiscal)", *European Sources*, žiūrėta 2020 m. rugpjūčio 29 d., https://www.europeansources.info/record/case-c-207-16-ministerio-fiscal/.

[837] „Opinion on Proposals regarding European Production and Preservation Orders for electronic evidence in criminal matters No. 7/2019", *European Data Protection Supervisor*, 2019, 10, žiūrėta 2020 m. rugpjūčio 29 d., https://edps.europa.eu/sites/edp/files/publication/19-11-06_opinion_on_e_evidence_proposals_en.pdf.

[838] Žr. pvz., Frederik J. Zuiderveen Borgesius ir Wilfred Steenbruggen, „The Right to Communications Confidentiality in Europe: Protecting Privacy, Freedom of Expression, and Trust", *Theoretical Inquiries in Law* 20, no. 1 (March 16, 2019): 291–322, doi:10.1515/til-2019-0010.

pasisakę, jog metaduomenys yra saugomi atitinkamai EŽTK ir Europos Sąjungos pagrindinių teisių chartija. EŽTT bylose *Malone v. United Kingdom*[839], *P.G & J.H v. United Kingdom*[840] pasisakė, kad EŽTK 8 str. apima komunikacijos telefonu metaduomenis, *Copland v. United Kingdom* byloje – kad EŽTK 8 str. yra saugomi ir el. laiškų bei internetinio naudojimo metaduomenys[841]. ESTT *Digital Rights Ireland* byloje konstatavo, kad įpareigojimas elektroninių ryšių paslaugų teikėjams saugoti komunikacijos elektroninėje erdvėje metaduomenis teisėsaugos tikslais prieštarauja Europos Sąjungos pagrindinių teisių chartijos 8 str.[842]. *Tele2/Watson* byloje ESTT pakartotinai konstatavo, kad valstybės narės nepasydamos ankstesniojo sprendimo *Digital Rights Ireland* byloje ir nepanaikinusios įpareigojimo elektroninių ryšių paslaugų teikėjams saugoti asmens duomenis visus komunikacijos metaduomenis, nepaisant to, kad jie yra saugomi teisėsaugos ir kovos su terorizmu tikslais, pažeidžia Europos Sąjungos pagrindinių teisių chartijoje įtvirtintą teisę į asmens duomenų apsaugą[843]. *Schrems* byloje, kuria ESTT panaikino Saugos uosto principą ir 2020 m. liepos 16 d. byloje *Data Protection Commissioner v. Facebook Ireland and Maximillian Schrems*, kuria konstatavo, jog Saugaus uosto principą pakeitęs Privatumo skydas neužtikrina teisės į asmens duomenų apsaugos, kadangi komunikacijos elektroninėje erdvėje metaduomenys yra prieinami JAV žvalgybos institucijoms vadovaujantis JAV teisės aktais, komunikacijos elektroninėje erdvėje metaduomenų apsaugos neužtikrinimą laikė pagrindu panaikinti ES-JAV susitarimus dėl asmens duomenų judėjimo. Vadovaujantis mokslininkų ir teismų pozicija, darytina išvada, kad Reglamento dėl Europos elektroninių įrodymų baudžiamosiose bylose pateikimo ir saugojimo orderių projekte įtvirtintas didesnės teisinės apsaugos suteikimas komunikacijos turiniui yra teisiškai ir technologiškai nepagrįstas (apie tai plačiau 1 disertacijos skyriuje).

Ne visos ES valstybės narės pritarė 2018 m. elektroninių įrodymų rinkimo reglamentavimo pasiūlymų paketui motyvuodamos skirtingose valstybėse skirtingai įgyvendinamu teisinės valstybės principu ir dėl to atsirandančiu piktnaudžiavimo pasiūlytų teisės aktų projektais reglamentuojamų priemonių pavojumi[844]. 2019 m. gruodžio

---

[839] „Europos Žmogaus Teisių Teismo 1984 m. rugpjūčio 2 d. sprendimas byloje Malone prieš Jungtinę Karalystę (Nr. 8691/79)“, *Hudoc*, žiūrėta 2020 m. rugsėjo 7 d., https://hudoc.echr.coe.int/rus#{%22itemid%22:[%22001-57533%22]}.

[840] „Europos Žmogaus Teisių Teismo 2001 m. rugsėjo 25 d. sprendimas P.G & J.H v. United Kingdom (Nr. 44787/98)“, *Hudoc*, žiūrėta 2020 m. rugpjūčio 29 d., https://hudoc.echr.coe.int/eng-press#{%22itemid%22:[%22003-419654-419935%22]}

[841] „Europos Žmogaus Teisių Teismo 2007 m. liepos 3 d. sprendimas byloje Copland v. United Kingdom (Nr. 62617/00)“, *European Human Rights Court*, žiūrėta 2020 m. rugpjūčio 29 d., https://hudoc.echr.coe.int/rus#{%22itemid%22:[%22001-79996%22]}.

[842] „Europos Sąjungos Teisingumo Teismo 2014 m. balandžio 8 d. sprendimas byloje Nr. C-293/12 ir C-594/12 Digital Rights Ireland Ltd v. Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others“, *EUR-Lex*, žiūrėta 2020 m. rugsėjo 7 d., https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62012CJ0293.

[843] „Europos Sąjungos Teisingumo Teismo 2016 m. gruodžio 21 d. sprendimas bylose Nr. C-203/15 ir C-698/15 Tele2 Sverige AB prieš Post- och telestyrelsen ir Secretary of State for the Home Department prieš Tom Watson ir kt.“, *InfoCuria*, žiūrėta 2020 m. rugsėjo 10 d., http://curia.europa.eu/juris/document/document.jsf?text=&docid=186492&pageIndex=0&doclang=en&mode=lst&dir=&occ=first&part=1&cid=1319429.

[844] Mehreen Khan, „EU governments approve draft rules on sharing 'e-evidence'“, *Financial Times*, 2018, žiūrėta 2020 m. rugpjūčio 25 d., https://www.ft.com/content/63a6105a-fa24-11e8-af46-2022a0b02a6c.

mėnesį reglamento ir direktyvos projektams buvo pateikta 841 pastaba[845], yra kritikuojama Europos asmens duomenų apsaugos priežiūros institucijos[846] bei mokslininkų[847]. Sveikintina laikoma ES iniciatyva[848], reikalauja esminio joje įvirtinto teisinio asmens duomenų rinkimo teisėsaugos tikslais reglamentavimo peržiūrėjimo idant būtų pasiekti joje iškelti tikslai. ES elektroninių įrodymų rinkimo reglamentavimo paketo analogu laikomo JAV *the Cloud Act* projektas buvo paskelbtas ir įsigaliojo 2018 m. Todėl tikslinant Reglamento ir direktyvos projektus yra tikslinga atsižvelgti į *the Cloud Act* taikymo praktiką ir JAV atliktus mokslinius tyrimus.

3.3.3.Masinio asmens duomenų rinkimo problema Europos Sąjungoje dėl Duomenų saugojimo direktyvos

Rugsėjo 11-osios teroro aktai JAV įtakojo ne tik JAV priimti teisės aktus, leidžiančius masinį asmens duomenų rinkimą el. erdvėje, bet ir ES bei jos valstybes nares pradėti svarstyti apie elektroninės komunikacijos duomenų rinkimo naudą nusikalstamų veikų tyrimui ir už kardymui[849]. Labai greitai po 2004 m. teroristų atakų Madride ir Londone, Prancūzija, Airija, Švedija ir Didžioji Britanija parengė projektą „*Framework Decision on the retention of data of electronic communications service providers*“[850]. Ši valstybių narių iniciatyva sulaukė WP29 ir Europos asmens duomenų apsaugos pareigūno kritikos dėl potencialaus EŽTK 8 straipsnio ir ES Pagrindinių teisių chartijos 7 straipsnio pažeidimo[851, 852]. Tačiau Parlamentas, norėdamas parodyti savo indėlį

---

[845] „Draft Report. European Production and Preservation Orders for electronic evidence in criminal matters Proposal for a decision (COM(2018)0225 – C8-0155/2018 – 2018/0108(COD))“, *European Parlament*, žiūrėta 2020 m. rugpjūčio 25 d., https://www.europarl.europa.eu/doceo/document/LIBE-AM-644870_EN.pdf

[846] „Opinion on Proposals regarding European Production and Preservation Orders for electronic evidence in criminal matters No. 7/2019“, *European Data Protection Supervisor*, 2019, žiūrėta 2020 m. rugpjūčio 29 d., https://edps.europa.eu/sites/edp/files/publication/19-11-06_opinion_on_e_evidence_proposals_en.pdf.

[847] Žr. pvz., Dan Jerker B. Svantesson, „European Union Claims of Jurisdiction over the Internet – an Analysis of Three Recent Key Developments“, *Journal of Intellectual Property, Information Technology and E-Commerce Law* 9, no. 2 (2018), žiūrėta 2020 m. rugpjūčio 29 d., https://www.jipitec.eu/issues/jipitec-9-2-2018/4722. Tosza, *supra note*, 833: 170.

[848] Anastasiya Kazakova, „The EU's e-Evidence & the U.S. CLOUD Act: Race Only to Start“, *Kaspersky*, žiūrėta 2020 m. rugsėjo 8 d., https://www.kaspersky.com/about/policy-blog/privacy/e-evidence-and-cloud-act.

[849] Franziska Boehm ir Mark D. Cole, „Data Retention after the Judgement of the Court of Justice of the European Union“, 13, žiūrėta 2020 m. rugpjūčio 17 d., https://www.zar.kit.edu/DATA/veroeffentlichungen/237_237_Boehm_Cole-Data_Retention_Study-June_2014_1a1c2f6_9906a8c.pdf

[850] „Draft Framework Decision on the retention of data processed and stored in connection with the provision of publicly available electronic communications services or data on public communications networks for the purpose of prevention, investigation, detection and prosecution of crime and criminal offence including terrorism“, *Council of the European Union*, žiūrėta 2020 m. rugpjūčio 17 d., https://www.asser.nl/upload/eurowarrant-webroot/documents/cms_eaw_108_2_CouncilDoc.8356.05.pdf.

[851] „Article 29 Data Protection Working Party Opinion 9/2004 on a draft Framework Decision on the storage of data processed and retained for the purpose of providing electronic public communications services or data available in public communications networks with a view to the prevention, investigation, detection and prosecution of criminal acts, including terrorism“, *European Commission*, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2004/wp99_en.pdf .

[852] Michel Regnier, „The 'Moment of Truth' for the Data Retention Directive: EDPS Demands Clear Evidence of Necessity“, *European Data Protection Supervisor,* 2017, žiūrėta 2020 m. rugpjūčio 17 d., https://edps.europa.eu/press-publications/press-news/press-releases/2010/moment-truth-data-retention-directive-edps-demands_en.

į kovą su terorizmu ir veikiamas spaudimo, kad jei jis to nepadarys, analogišką dokumentą kaip pamatinį sprendimą priims Taryba, pirmininkaujant ypatingai asmens duomenų rinkimu suinteresuotai Didžiajai Britanijai, 2006 m. priėmė direktyvą, kuri buvo laikoma viena iš kontraversiškiausių ES kovos su terorizmu priemonių[853].

2006 m. kovo 15 d. Europos Parlamento ir Tarybos direktyva Nr. 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 (toliau – Duomenų saugojimo direktyva) buvo siekiama suderinti valstybių narių nuostatas, susijusias su viešai prieinamų elektroninių ryšių paslaugų ir viešųjų ryšių tinklų teikėjų pareigomis saugant fizinių ir juridinių asmenų srauto ir vietos nustatymo bei susijusius duomenis abonento ir paslaugų naudotojo nustatymui[854], kurie yra jų generuojami arba tvarkomi, tuo siekiant užtikrinti, kad duomenys būtų prieinami sunkių nusikaltimų, kaip jie apibrėžti kiekvienos valstybės narės nacionalinėje teisėje, tyrimo, atskleidimo ir baudžiamojo persekiojimo tikslu[855]. Duomenų saugojimo direktyva buvo netaikoma el. komunikacijos turiniui[856], tačiau labai plataus pobūdžio meta duomenis, būtinus ryšio šaltiniui nustatyti ir išsiaiškinti[857], ryšio paskirties taškui[858],

---

853 Chris Jones ir Ben Hayes, „The EU Data Retention Directive: a case study in the legitimacy and effectiveness of EU counter-terrorism policy, Securing Europe through Counter- Terrorism: Impact, Legitimacy and Effectiveness“, *Statewatch*, 2013, 4, žiūrėta 2020 m. rugpjūčio 17 d., https://www.statewatch.org/media/documents/news/2013/dec/seciledata-retention-directive-in-europe-a-case-study.pdf.

854 „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“, 2 str., *EUR-Lex*, žiūrėta 2020 m. rugpjūčio 17 d., https://eur-lex.europa.eu/legal-content/LT/TXT/?uri=CELEX%3A32006L0024.

855 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, 1 str., *EUR-Lex*, žiūrėta 2020 m. rugsėjo 8 d., https://eur-lex.europa.eu/legal-content/LT/TXT/?uri=CELEX%3A32006L0024.

856 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, 2 str., *EUR-Lex*, žiūrėta 2020 m. rugsėjo 8 d., https://eur-lex.europa.eu/legal-content/LT/TXT/?uri=CELEX%3A32006L0024.

857 a) duomenys, būtini ryšio šaltiniui išaiškinti ir nustatyti:
1) susiję su fiksuoto telefono ryšio tinklu ir judriuoju telefono ryšiu:
i) telefono numeris, iš kurio skambinta;
ii) abonento ar registruoto naudotojo vardas ir pavardė (pavadinimas) bei adresas;
2) susiję su interneto prieiga, interneto elektroniniu paštu ir interneto telefonija:
i) suteikti naudotojų atpažinimo kodai;
ii) naudotojo atpažinimo kodas ir telefono numeris, suteikti bet kokiam ryšiui, patenkančiam į viešąjį telefono tinklą;
iii) abonento ar registruoto naudotojo, kuriam ryšio metu buvo suteiktas interneto protokolo (IP) adresas, naudotojo atpažinimo kodas ar telefono numeris, vardas ir pavardė (pavadinimas) ir adresas;

858 1) susiję su fiksuoto telefono ryšio tinklu ir judriuoju telefono ryšiu:
i) rinktas telefono numeris ar numeriai (telefono numeris (-iai), į kurį (-iuos) skambinta), o papildomų paslaugų, pvz., skambučių peradresavimo ar skambučių persiuntimo atvejais – telefono numeris arba numeriai, į kuriuos nukreiptas skambutis;
ii) abonento (-ų) ar registruoto (-ų) naudotojo (-ų) vardas (-ai) ir pavardė (-s) (pavadinimas (-ai)) bei adresas (-ai);
2) susiję su internetu perduodamu elektroniniu paštu ir internetine telefonija:
i) telefono skambučių internetu numatomo (-ų) gavėjo (-ų) naudotojo atpažinimo kodas ar telefono numeris;
ii) abonento (-ų) ar registruoto (-ų) naudotojo (-ų) vardas (-i) ir adresas (-i) ir telefono skambučių internetu numatomo (-ų) gavėjo (-ų) naudotojo atpažinimo kodas;

ryšio datai, trukmei ir laikui[859], ryšio tipui[860], naudotojų ryšio įrangai ar tam, kas turėtų būti ryšio įranga[861], judriojo ryšio įrangos vietai[862] nustatyti komunikacijos paslaugų teikėjus ji įpareigojo tvarkyti ir saugoti nuo 6 iki 24 mėnesių laikotarpiui[863]. Duomenų saugojimo direktyva nenumatė duomenų teikimo kompetentingoms institucijoms tvarkos bei neapibrėžė, ką apima kompetentingų institucijų sąvoka, sudarant galimybes tiek teisėsaugos, tiek žvalgybos institucijoms teisę prieiti prie šių asmens duomenų. Pagal šią direktyvą saugomi duomenys kompetentingoms nacionalinėms institucijoms turėjo būti teikiami pagal nacionalinės teisės nuostatas laikantis ES ir tarptautinės viešosios teisės normų[864]. Elektroninių ryšių direktyva pasižymėjo tuo, kad perkeliant jos nuostatas į nacionalinę teisę valstybės narės turėjo daug laisvės pasirenkant reglamentavimo mechanizmą, o valstybių narių nacionaliniai teisės aktai sulaukė pasipriešinimo iš visuomenės ir politinių grupių[865] ir buvo nagrinėjami Bulgarijos, Rumunijos, Vokietijos, Kipro ir Čekijos[866] Konstituciniuose Teismuose. Visi minėti Konstituciniai teismai analizavo panašius klausimus dėl nacionalinių aktų

---

[859] c) duomenys, būtini ryšio datai, laikui ir trukmei nustatyti:
1) susiję su fiksuoto telefono ryšio tinklu ir judriuoju telefono ryšiu – ryšio pradžios ir pabaigos laikas bei data;
2) susiję su prieiga prie interneto, internetu perduodamu elektroniniu paštu ir internetine telefonija:
i) prisijungimo prie interneto ir atsijungimo nuo interneto prieigos paslaugų data ir laikas tam tikroje laiko juostoje ir dinamiškas ar statiškas interneto protokolo (IP) adresas, kurį ryšiui suteikė prieigos prie interneto paslaugos teikėjas, ir abonento ar registruoto naudotojo atpažinimo kodas;
ii) prisijungimo prie interneto ir atsijungimo nuo internetu perduodamo elektroninio pašto paslaugos ar internetinės telefonijos paslaugos data ir laikas tam tikroje laiko juostoje;

[860] 1) susiję su fiksuoto telefono ryšio tinklu ir judriuoju telefono ryšiu – telefoninio ryšio paslauga, kuria pasinaudota;
2) susiję su interneto prieiga, internetu perduodamu elektroniniu paštu ir internetine telefonija — interneto paslauga, kuria pasinaudota;

[861] 1) susiję su fiksuoto telefono ryšio tinklu – telefono numeriai, į kuriuos ir iš kurių skambinta;
2) susiję su judriuoju telefono ryšiu:
i) telefono numeriai, į kuriuos ir iš kurių skambinta;
ii) kviečiančiosios šalies tarptautinis judriojo ryšio abonento identifikatorius (IMSI);
iii) kviečiančiosios šalies tarptautinis judriojo ryšio įrangos identifikatorius (IMEI);
iv) kviečiamosios šalies tarptautinis judriojo ryšio abonento identifikatorius (IMSI);
v) kviečiamosios šalies tarptautinis judriojo ryšio įrangos identifikatorius (IMEI);
vi) iš anksto apmokėtų anoniminių paslaugų atveju paslaugos pirminio aktyvavimo data ir laikas bei žyma vietovės (Cell ID), iš kurios paslauga buvo aktyvuota;
3) susiję su interneto prieiga, internetu perduodamu elektroniniu paštu ir internetine telefonija:
i) telefono, iš kurio skambinama, numeris naudojamas tiesioginio rinkimo interneto ryšiu;
ii) skaitmeninė abonento linija (DSL) ar kiti pranešimo siuntėjo galiniai tinklo taškai;

[862] 1) vietovės žyma (Cell ID) ryšio pradžioje;
2) duomenys, padedantys nustatyti geografinę įrangos buvimo vietą pagal vietovės žymas (Cell ID) tuo laikotarpiu, kai ryšio duomenys išsaugomi.

[863] 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, 6 str., *EUR-Lex*, žiūrėta 2020 m. rugsėjo 8 d., https://eur-lex.europa.eu/legal-content/LT/TXT/?uri=CELEX%3A32006L0024.

[864] 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, 4 str., *EUR-Lex*, žiūrėta 2020 m. rugsėjo 8 d., https://eur-lex.europa.eu/legal-content/LT/TXT/?uri=CELEX%3A32006L0024.

[865] Boehm, *supra note,* 76:15.

[866] Christiana Markou, „The Cyprus and Other EU Court Rulings on Data Retention: The Directive as a Privacy Bomb", *Computer Law & Security Review* 28, no. 4 (August 1, 2012): 468–75, doi:10.1016/j.clsr.2012.05.003.

atitikimo EŽTK 8 str. ir Chartijos 8 str. įtvirtintai teisei į asmens duomenų apsaugą ir privatumą atsižvelgiant į tai, kad pagal El. ryšių direktyvą įgyvendinančius teisės aktus duomenys buvo renkami absoliučiai visų asmenų *a priori*, nors jie nebuvo susiję su jokiomis nusikalstamomis veikomis, o kompetentingos institucijos, galinčios prieiti prie tokių duomenų nebuvo konkrečiai įvardintos. Tačiau nei vienos valstybės Konstitucinis Teismas nesikreipė į ESTT dėl El. ryšių direktyvos atitikimo ES teisės aktuose įtvirtintoms fundamentinėms asmenų teisėms. ESTT klausimas dėl El. ryšių direktyvos teisėtumo pasiekė 2009 m., tačiau ir tuomet klausimas dėl El. ryšių direktyvos santykio su teise į asmens duomenų apsauga ESTT nebuvo keliamas. Airija ir Slovakija skundą pateikė tuo pagrindu, jog El. ryšių direktyva turėjo būti priimta ne I, o III ramstyje, nes jos tikslas yra kova su terorizmu ir kitais sunkiais nusikaltimais[867]. ESTT atmetė Airijos ir Slovakijos pareiškimą, motyvuodamas tuo, kad El. ryšių direktyva reglamentuojama telekomunikacijų ir interneto paslaugų teikėjų veikla nepriklausomai nuo to ar teisėsaugos institucijos kreipiasi dėl surinktų duomenų perdavimo, taigi Parlamentas turėjo teisę El. ryšių direktyvą priimti I, o ne III ramsčio pagrindu[868]. Tačiau debatams dėl nacionalinių teisės aktų atitikimo EŽTK ir ES teisių chartijai valstybėse narėse ir toliau nerimstant 2012 m. ESTT pasiekė antroji byla dėl El. ryšių direktyvos pagrįstumo[869]. ESTT antroji byla dėl El. ryšių direktyvos pasiekė dėl Airijoje veikiančios visuomeninės organizacijos Digital Rights Ireland skundo Airijos Aukščiausiajam teismui bei daugiau nei 11000 Austrijos gyventojų pateikto grupės ieškinio Austrijos Konstituciniam Teismui. Skundo pagrindas buvo į nacionalinę teisę perkeltos Duomenų saugojimo direktyvos atitikimas ES sutarties 4.3. straipsniui ir ES Pagrindinių teisių chartijai. 2014 m. balandžio 26 d. El. ryšių direktyva buvo panaikinta.

ESTT, vadovaudamasis EŽTT praktika panašiose bylose dėl teisės į asmens duomenų apsaugą užtikrinimu tiriant ir užkardant nusikalstamas veikas[870] nurodė, kad asmens duomenų rinkimas su tikslu, kad ateityje prireikus šiuos duomenis būtų galima perduoti kompetentingoms institucijoms tiesiogiai yra susijęs su asmenų privačiu gyvenimu[871] ir yra laikomas asmens duomenų tvarkymu Chartijos 7, 8 str. įtvirtinta prasme[872]. Tai, kad asmens duomenys yra nuolat renkami be asmens sutikimo sukūrė asmenims pojūtį lyg jie būtų nuolat sekami[873]. Visgi teisė į asmens duomenų apsaugą nėra absoliuti, todėl nustatęs, kad El. ryšių direktyva įtvirtintos nuostatos yra susiju-

---

867 „Europos Sąjungos Teisingumo Teismo 2009 m. vasario 10 d sprendimas byloje Nr. C-301/06 Airija prieš Europos Parlamentą ir Europos Sąjungos Tarybą“, *InfoCuria*, žiūrėta 2020 m. rugsėjo 8 d., http://curia.europa.eu/juris/liste.jsf?num=C-301/06

868 *Ibid.*

869 *Ibid.*

870 Boehm, *supra note,* 76: 20.

871 Europos Sąjungos Teisingumo Teismo 2014 m. balandžio 8 d. sprendimas byloje Nr. C-293/12 ir C-594/12 Digital Rights Ireland Ltd v. Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others, *EUR-Lex*, žiūrėta 2020 m. rugsėjo 7 d., https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62012CJ0293.

872 *Ibid.*

873 *Ibid.*

sios su asmens teise į asmens duomenų ir privatumo apsaugą, teismas turėjo patikrinti ar tos nuostatos atitinka Chartijoje įtvirtintas šios teisės išimties sąlygas.

Chartijos 52 straipsnio 1 d. yra įtvirtintos nuostatos, kuomet yra laikoma, kad Chartijoje įtvirtintų teisių nesilaikymas yra teisėtas tik tuo atveju, jeigu:

1) įvirtintas teisės akte;
2) nepažeidžia atitinkamos teisės esmės;
3) apribojimas yra proporcingas juo siekiamiems visuomenės interesams patenkinti: atitinka Sąjungos pripažintus bendrus interesus arba reikalingi kitų teisėms ir laisvėms apsaugoti.

Kadangi Duomenų saugojimo direktyva buvo perkelta į nacionalinius teisės aktus[874], todėl ESTT analizavo antrąjį ir trečiąjį teisių apribojimo pagrįstumo elementą. Kadangi El. ryšių direktyva buvo įpareigojama rinkti tik srauto ir vietos nustatymo duomenis, o komunikacijos turinys nebuvo renkamas, todėl teismas konstatavo, kad šios teisės į asmens duomenų apsaugą esmė nebuvo pažeista. Tačiau naujausios mokslinės studijos rodo, kad meta duomenys yra tokie patys svarbus kaip ir komunikacijos turinys, o kartais iš meta duomenų galima sužinoti daug daugiau informacijos apie asmenį negu iš komunikacijos turinio[875]. Meta duomenys gali suteikti informaciją apie asmens tapatybę, elgesį, socialinius ryšius, privačius pasirinkimus bei kitą informaciją[876]. Nors JAV teisės aktuose taip pat yra įtvirtinti griežtesni reikalavimai teisėsaugos institucijų prieigai prie komunikacijos turinio nei prie metaduomenų, tačiau informacijos, kurią metaduomenys atskleidžia apie asmenį pobūdis rodo, jog komunikacijos turinio laikymas privatesniu nei metaduomenų, yra nepagrįstas. Teiginį, kad ši apribojimo dalis nepažeidė teisės į asmens duomenų apsaugą esmės, teismas pagrindė ir tuo, kad direktyva ir nacionaliniai teisės aktai įpareigojo el. ryšių paslaugų ir el. paslaugų teikėjus imtis reikiamų surinktų asmens duomenų apsaugos priemonių[877]. Tačiau pavyzdžiui, tas faktas, kad hakeriai įsilaužė į vienos iš labiausiai pasaulyje saugomų JAV žvalgybos institucijų NSA, CIA duomenų bazes[878], o 2016 m. ir 2017 m. *Shadow Brokers* įsilaužė į vienos geriausių laikomos NSA Hakerių grupės duomenų bazes[879] rodo, jog praktiškai bent kokia asmens duomenų apsaugos sistema gali būti nulaužta,

---

874 Net ir neperkėlus yra įmanomas tiesioginis direktyvos taikymas.

875 Paul M. Schwartz, „Property, Privacy, and Personal Data", *Harvard Law Review* 117, no. 7 (2004 2003): 2070. Michael J. McCarthy, „Electronic Form of 'Invisible Ink' Inside Files May Reveal Secrets", *Wall Street Journal*, 2000, žiūrėta 2020 m. rugpjūčio 17 d., https://www.wsj.com/articles/SB972002214791170991.

876 „Report on the right to privacy in the digital age (A/HRC/27/37)", United Nations, 30 June 2014, 7, žiūrėta 2020 m. rugpjūčio 17 d., https://documents-dds-ny.un.org/doc/UNDOC/GEN/G18/239/58/PDF/G1823958.pdf?OpenElement.

877 Europos Sąjungos Teisingumo Teismo 2014 m. balandžio 8 d. sprendimas byloje Nr. C-293/12 ir C-594/12 Digital Rights Ireland Ltd v. Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others, *EUR-Lex*, žiūrėta 2020 m. rugsėjo 7 d., https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62012CJ0293.

878 Jamie Condliffe, „Security Experts Agree: The NSA Was Hacked", *MIT Technology Review*, žiūrėta 2020 m. rugsėjo 8 d., https://www.technologyreview.com/2016/08/18/70386/security-experts-agree-the-nsa-was-hacked/.

879 Rob Price, „'Shadow Brokers' Claims to Hack 'Equation Group,' Group Linked to NSA", *Business Insider*, žiūrėta 2020 m. rugsėjo 8 d., https://www.businessinsider.com/shadow-brokers-claims-to-hack-equation-group-group-linked-to-nsa-2016-8?international=true&r=US&IR=T.

sukurti tokią sistemą, kurios būtų neįmanoma nulaužti yra neįmanoma[880]. Vadovautis nuostata, įpareigojančia imtis pakankamų priemonių surinktiems duomenims apsaugoti, kaip pateisinančia teisės į asmens duomenų apsaugą suvaržymą, yra ydinga praktika. Apskritai, nors nuostata, reikalaujanti imtis techninių ir organizacinių priemonių surinktų duomenų apsaugojimui yra įtvirtinama visuose teisės aktuose, dėl anksčiau išvardintų priežasčių yra tik teorinė ir praktiškai neįgyvendinama, nes neįmanoma sukurti tokios sistemos, kurios nebūtų įmanoma nulaužti, o jeigu sistemą yra įmanoma nulaužti, vadinasi teisės akto prasme nebuvo imtasi reikiamų techninių ir organizacinių priemonių surinktų duomenų apsaugojimui. Todėl ši teismo sprendimo dalis yra diskutuotina dėl abiejų aspektų: dėl turininės informacijos didesnės svarbos nei metaduomenų ir dėl įpareigojimo imtis techninių ir organizacinių priemonių surinktų duomenų apsaugojimui.

Vertindamas ar visuotinis duomenų rinkimas atitiko Chartijos 52 straipsnyje įtvirtintą trečiąją sąlygą, teismas konstatavo, kad duomenų rinkimo tikslas – kova su sunkiais nusikaltimais – atitiko visuomenės interesus[881], o nustatydamas ar teisės į asmens duomenų apsaugą suvaržymas yra proporcingas siekiamiems tikslas, teismas vadovavosi EŽTT praktika. ESTT vertino vadovaudamasis dviguba proporcingumo taisykle: 1) ar suvaržymo apimtis yra būtina ja siekiamiems tikslams pasiekti ir 2) ar teisių suvaržymas neviršija reikiamų priemonių[882]. ESTT nurodė, kad jeigu yra suvaržomos fundamentinės teisės, tuomet įstatyme turi būti įtvirtintos griežtos šios teisės suvaržymo taisyklės[883], ko nebuvo padaryta Elektroninių ryšių direktyvoje ir būtent dėl šios priežasties ją pripažino negaliojančia nuo priėmimo momento[884]. Tačiau ESTT nepasisakė ar masinis asmens duomenų rinkimas yra būtina ir efektyvi kovos su nusikalstamumu priemonė tuo, mokslininkų manymu, savo motyvuojamą sprendimo dalį padarydamas silpnai argumentuota[885]. Tačiau tokiu būdu ESTT išvengė atsakomybės įvilkti į teisinį rūbą tai, ką JAV mokslininkai jau pradėjo įrodinėti – kad masinis asmens duomenų rinkimas nėra efektyvi kovos su nusikalstamumu priemonė ir jis labiau tarnauja kitiems, dažniausiai, politiniams tikslams[886]. Tačiau kaip Duomenų saugojimo direktyvos panaikinimas paveikė jos pagrindu valstybėse narėse priimtus įstatymus?

Panaikinus Duomenų saugojimo direktyvą valstybių narių nacionaliniai teisės aktai automatiškai nenustojo galioti. ESTT sprendimas teisiškai įpareigojo tik Austriją ir Airiją panaikinti savo nacionalinius aktus, kadangi šios valstybės kreipėsi į ESTT.

---

880 Yra tik laiko klausimas, kada ji bus nulaužta.

881 „Europos Sąjungos Teisingumo Teismo 2014 m. balandžio 8 d. sprendimas byloje Nr. C-293/12 ir C-594/12 Digital Rights Ireland Ltd v. Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others“, *EUR-Lex*, žiūrėta 2020 m. rugsėjo 7 d., https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62012CJ0293.

882 „Advocate General Opinion on Joint Cases C-293/12, C-594/12, 12 December 2013“, 46 paragrafas, *EUR-Lex*, žiūrėta 2020 m. rugpjūčio 17 d. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62012CC0293.

883 „Europos Žmogaus Teisių Teismo 2013 m. balandžio18 d. sprendimas byloje M. K. prieš Prancūziją (Nr. 19522/09)“, *Hudoc,* žiūrėta 2020 m. rugsėjo 8 d., https://hudoc.echr.coe.int/fre#{%22itemid%22:[%22001-119075%22]}.

884 *Ibid.*

885 Boehm, *supra note,* 76: 8.

886 Granick, *supra note*, 509.

Likusių valstybių narių Elektroninių ryšių direktyvą įgyvendinantys įstatymai turėtų būti panaikinti ar pakeisti nacionalinių parlamentų taip, kad nepažeistų asmenų teisės į asmens duomenų apsaugą[887]. Nors ES parlamentas nurodė, kad ESTT sprendimas „iš principo tiesiogiai neveikia nacionalinės teisės aktų leidybos[888], tačiau buvo nuspręsta Švedijai skirtą 3 000 000 Eur baudą už vėlavimą įgyvendinti Elektroninių ryšių direktyvą[889], grąžinti[890], o Vokietijai baudos skyrimo bylą dėl Elektroninių ryšių direktyvos neįgyvendinimo nutraukti[891].

Neigiama patirtis su Elektroninių ryšių direktyva, atrodo, nebuvo pakankama pamoka ES. Nuo 2018 m. gegužės 25 d. kartu su Asmens duomenų apsaugos paketu įsigaliojo kita direktyva, nors ir nukreipta ne į komunikacijos el. erdvėje paslaugų teikėjus, tačiau susijusi su masiniu nediferencijuotu asmens duomenų rinkimu el. erdvėje – PNR direktyva. Ar ši direktyva užtikrins asmenų teisę į asmens duomenų apsaugą?

3.3.4. Keleivių duomenų įrašo direktyva

PNR direktyvą galime laikyti teisine priemone, kuria reglamentuojamas asmens duomenų rinkimas el. erdvėje teisėsaugos tikslais, tačiau labai specifinėje ir siauroje srityje – renkant oro keleivių duomenų įrašus (PNR). Jei Teisėsaugos tikslais tvarkomų asmens duomenų direktyva apima visą asmens duomenų rinkimą ir el. erdvėje, tik, kaip jau išsiaiškinome, jos reglamentavimas yra nepakankamas, tai PNR direktyva reglamentuoja labai specifinę sritį. PNR direktyvos tikslas yra ES lygiu sureglamentuoti oro vežėjų atliekamą PNR duomenų tvarkymą ir panaudojimą teroristinių nusikaltimų ir sunkių nusikaltimų prevencijos, nustatymo, tyrimo ir patraukimo už juos baudžiamojon atsakomybėn tikslais. Skirtingai nuo Teisėsaugos tikslais tvarkomų asmens duomenų direktyvos, PNR direktyvoje įtvirtinti ne tik bendrieji deklaratyvūs principai, bet ir PNR duomenų rinkimo ir naudojimo mechanizmas. Direktyva nurodo, jog valstybės narės privalo tvarkyti PRN duomenis apie išorės skydžius, tačiau gali tvarkyti PNR duomenis ir apie vidaus skrydžius. Valstybės narės taip pat privalo įsteigti informacijos apie keleivius skyrių, kuriam oro vežėjai direktyvoje numatytais intervalais ir būdais privalo perduoti PNR duomenis ir API duomenis apie absoliučiai visus asmenis, kurie naudojasi ar ketina naudotis oro vežėjų paslaugomis, tačiau jomis

---

887 Xavier Tracol, „Legislative Genesis and Judicial Death of a Directive: The European Court of Justice Invalidated the Data Retention Directive (2006/24/EC) Thereby Creating a Sustained Period of Legal Uncertainty about the Validity of National Laws Which Enacted It", *Computer Law & Security Review* 30, no. 6 (December 1, 2014): 748, doi:10.1016/j.clsr.2014.09.008.

888 „Europos Sąjungos Teisingumo Teismo 2014 m. balandžio 30 d. sprendimas bylose Nr. C-390/12 iškeltose Robert Pfleger, Autoart a.s., Mladen Vucicevic, Maroxx Software GmbH, Ing. Hans-Jörg Zehetner", *InfoCuria*, žiūrėta 2020 m. rugsėjo 8 d., http://curia.europa.eu/juris/document/document.jsf?text=&docid=153472&pageIndex=0&doclang=LT&mode=req&dir=&occ=first&part=1&cid=778912.

889 Tracol, *op. cit.*, 887: 744.

890 „Europos Sąjungos Teisingumo Teismo 2013 m. gegužės 30 d. sprendimas byloje Nr. C-270/11 Europos Komisija prieš Švedijos Karalystę", *InfoCuria*, žiūrėta 2020 m. rugsėjo 8 d., http://curia.europa.eu/juris/liste.jsf?num=C-270/11&language=EN.

891 „Europos Sąjungos Teisingumo Teismo 2014 m. birželio 5 d. sprendimas byloje Nr. C-329/12 Europos Komisija prieš Vokietiją", žiūrėta 2020 m. rugsėjo 8 d. http://curia.europa.eu/juris/liste.jsf?language=en&num=C-329/12

nepasinaudoja (neatvyksta į skrydį, atšaukia skrydį ir kt.). 6 mėnesius informacijos apie keleivius skyriai saugo šiuos duomenis nepseudonimizuotus ir suteikia tiesiogiai į juos besikreipiančioms nacionalinėms kompetentingoms institucijoms arba kitų valstybių narių informacijos apie keleivius skyriams, o praėjus 6 mėn. laikotarpiui – pseudoanonimizuoja ir suteikia tik esant teismo ar kitos kompetentingos institucijos sankcionavimui. Taigi, tokie yra esminiai PNR direktyvos bruožai. Nors Direktyvoje yra nurodoma, jog ji yra suderinama ir su Chartija ir su 108 Konvencija, ir EŽTK, ir ja visiškai užtikrinama teisė į asmens duomenų apsaugą, tačiau esminės jos nuostatos kelia abejonių. Visų pirma, ar tikrai ES turėjo teisinį pagrindą priimti PNR direktyvą?

Vadovaujantis SESV 2(2) str., ES negali reglamentuoti sričių, kurios nepatinka į Bendrijos teisės reglamentavimo sritį. Viena iš tų sričių yra nacionalinio saugumo užtikrinimas. Terorizmas ir teroristiniai nusikaltimai yra laikomi nusikaltimais keliančiais pavojų nacionaliniam saugumui. EŽTT sprendimuose minimalūs asmens duomenų apsaugos standartai buvo pateisinami kova su terorizmu, kaip nacionalinio saugumo užtikrinimo priemone[892]. Kova su terorizmu kaip nacionalinio saugumo užtikrinimo priemone buvo pateisinamos ir JAV NSA vykdytos masinio asmens duomenų rinkimo programos[893]. Tačiau PNR direktyva sako, kad duomenys bus renkami ne kovos su terorizmu, o teroristinių ir sunkių nusikaltimų prevencijos, tyrimo, patraukimo baudžiamojon atsakomybėn tikslais. Ką tai reiškia?

PNR direktyvoje yra nurodyta, kad PNR duomenys yra renkami teroristinių ir sunkių nusikaltimų prevencijos, nustatymo, tyrimo ir patraukimo už juos baudžiamojon atsakomybėn tikslais. Nusikaltimų tyrimas ir patraukimas baudžiamojon atsakomybėn yra teisėsaugos institucijų kompetencija. Tačiau teroristinių nusikaltimų prevencija ir nustatymo priskyrimas teisėsaugos institucijų funkcijoms yra diskusinis klausimas. Klausimą dar aktualesniu padaro tai, kad PNR direktyva neapibrėžia, kas gi yra tos kompetentingos institucijos, kurios be teismo sankcionavimo 6 mėn. laikotarpiu gali gauti visus PNR duomenis. Kiekviena valstybė narė šių institucijų sąrašą. Nėra nurodyta, kad kompetentingų institucijų sąrašas privalo būti skelbiamas viešai. PNR direktyvos 7 str. 3 d., įpareigoja valstybes nares pateikti kompetentingų institucijų sąrašą EK, bet tik 9 str. 3 d. tikslais – kad vienas valstybės narės kompetentingos institucijos galėtų tiesiogiai prašyti kitų narių kompetentingų institucijų PNR duomenų esant ekstremalioms situacijoms. Tai reiškia, kad valstybės narės EK gali pateikti ne visą kompetentingų institucijų sąrašą, o tik tokių, į kurias būtų galima kreiptis kitoms valstybėms narėms, ir kurios būtų įgaliotos kreiptis į kitas valstybių narių kompetentingas institucijas ekstremalių situacijų atveju. Visa tai reiškia, kad nacionaliniuose PNR direktyvą įgyvendinančiuose įstatymuose oro vežėjai PNR duomenis gali būti įpareigojami ir greičiausiai bus įpareigojami teikti ne vien tik teisėsaugos, bet ir žvalgybos institucijoms. Tai dar labiau priartintų prie išvados, kad EK priimdama PNR direktyvą tiek, kiek tai liečia teroristinius nusikaltimus, galimai viršijo savo įgaliojimus ir veikė nacionalinio saugumo užtikrinimo srityje.

---

[892] Pvz., „Europos Žmogaus Teisių Teismo 1978 m. rugsėjo 6 d. sprendimas byloje Klass ir kiti prieš Vokietiją (Nr. 5029/71)“, *Hudoc*, žiūrėta 2020 m. rugsėjo 7 d., https://hudoc.echr.coe.int/rus#{%22itemid%22:[%22001-57510%22]}.

[893] James Carafano, „PRISM Is Essential to U.S. Security in War Against Terrorism“, *The Heritage Foundation*, žiūrėta 2020 m. rugpjūčio 17 d., https://www.heritage.org/defense/commentary/prism-essential-us-security-war-against-terrorism.

Antrasis PNR direktyvos pagrįstumą keliantis klausimas yra jos nuostatų neprieštaravimas teisei į asmens duomenų apsaugą. PRN direktyvoje įtvirtintas:

1) Analogiškai Elektroninių ryšių direktyvai absoliučiai visų besinaudojančių oro transportu asmenų asmens duomenų rinkimo mechanizmas – tai reiškia masinį ir nediferencijuotą asmens duomenų rinkimą ne tik apie keliaujančius asmenis, bet ir apie asmenis, kurie keliaujančių asmenų vardu užsako lėktuvo bilietus. Dar didesnį masinio asmens duomenų rinkimo įspūdį sudaro tai, kad visų asmenų PNR duomenis turės oro vežėjai privalės perduoti valstybės nustatytai valdžios institucijai, atsakingai už teroristinių ir sunkių nusikaltimų prevenciją. Kadangi konkrečiai nėra įvardinta, jog teisėsaugos institucijai, vadinasi tokia institucija gali būti ir žvalgybos institucija, jeigu ji atsakinga ir už teroristinių, ir už sunkių nusikaltimų prevenciją. Tai rodo, kad absoliučiai visų asmenų, net ir nei karto nepadariusių administracinės teisės pažeidimų, jau nekalbant apie baudžiamajai teisei priešingą veiką, PNR duomenys visais atvejais yra perduodami tai institucijai, kuri atsakinga už didžiausią pavojų keliančių nusikaltimų prevenciją. JAV vykdytas masinis ir nediferencijuotas asmens duomenų rinkimas buvo pasmerktas ET[894], Jungtinių Tautų[895] ir mokslininkų[896], kaip pažeidžiantis teisę į asmens duomenų apsaugą. ESTT pripažindamas Elektroninių ryšių direktyvą pažeidžiančią Chartiją konstatavo, kad masinis asmens duomenų rinkimas apie visus asmenis vien tik potencialiai ateityje vykdysiamų nusikaltimų prevencijos ir tyrimo atžvilgiu yra neproporcingas asmens teisės į asmens duomenų apsaugą suvaržymas.[897] Tačiau PNR direktyva ES tarsi paneigia Chartijoje įtvirtintą teisę į asmens duomenų apsaugą.
2) PNR duomenys privalės būti renkami ne oro vežėjo paslaugų teikimo tikslais, o sunkių nusikaltimų prevencijos, nustatymo, tyrimo ir patraukimo už juos baudžiamojon atsakomybėn tikslais.
3) 6 mėnesių laikotarpiu kompetentingos institucijos prie šių asmens duomenų turės teisę prieiti nesant teismo sankcionavimo – teisminis sankcionavimas yra vienu iš asmens teisių apsaugos garantų. Nors nei EŽTK, nei Chartijoje nėra įtvirtinto privalomo teisminio sankcionavimo norint apriboti teisę į asmens duomenų apsaugą, tačiau toks reikalavimas gali būti įtvirtintas valstybių narių

---

894 „Mass Surveillace“, *Council of Europe*, žiūrėta 2020 m. rugpjūčio 17 d. http://assembly.coe.int/nw/xml/XRef/Xref-XML2HTML-en.asp?fileid=21692.

895 „Online Mass-Surveillance: ‘Protect Right to Privacy Even When Countering Terrorism“, *United Nations*, žiūrėta 2020 m. rugpjūčio 17 d., https://www.ohchr.org/SP/NewsEvents/Pages/DisplayNews.aspx?NewsID=15200&LangID=E.

896 Anthony D. Romero, „Mass E-Mail Surveillance: The Next Battle“, *Sur – International Journal on Human Rights* 21 (2015): 1–3. Nadine Strossen, „Beyond the Fourth Amendment: Additional Constitutional Guarantees That Mass Surveillance Violates“, *Drake Law Review* 63, no. 4 (2015): 1143–70. A. Michael Froomkin, „Regulating Mass Surveillance as Privacy Pollution: Learning from Environemntal Impact Statements“, *University of Illinois Law Review* 2015, no. 5 (2015): 1713–90. Monika Žalnieriūtė, „An International Constitutional Moment for Data Privacy in the Times of Mass-Surveillance“, *International Journal of Law and Information Technology* 23, no. 2 (2015): 99–133.

897 „Europos Sąjungos Teisingumo Teismo 2014 m. balandžio 8 d. sprendimas byloje Nr. C-293/12 ir C-594/12 Digital Rights Ireland Ltd v. Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others“, *EUR-Lex*, žiūrėta 2020 m. rugsėjo 7 d., https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62012CJ0293.

Konstitucijose. Pavyzdžiui, Lietuvos Respublikos Konstitucijos 22 straipsnyje yra nurodyta, kad „informacija apie privatų asmens gyvenimą gali būti renkama tik motyvuotu teismo sprendimu ir tik pagal įstatymą“[898]. Laikantis EŽTT suformuoto principo, kad teisė į asmens duomenų apsaugą yra teisės į privatumą dalis[899] ir to, kad Konstitucinis Teismas mūsų Konstituciją laiko gyvu mechanizmu, kuris interpretuojamas atsižvelgiant į šiandieninio gyvenimo aplinkybes[900], todėl PNR duomenys turėtų būti laikomi Konstitucijos 22 str. įtvirtintos teisės į privatumą dalimi. Vadinasi, šių duomenų rinkimas be išankstinio teismo sankcionavimo pažeidžia Konstitucijos 22 straipsnyje įtvirtintą mūsų teisę į privatumą. Pažymėtina, kad JAV teismai nesankcionuotą asmens duomenų rinkimą antikonstituciniu pripažino 1967 m.

Apibendrinimas:

1. *Teisės į asmens duomenų apsaugą pagrindiniu šaltiniu Europoje yra EŽTK 8 str., kuris taikomas asmens duomenis renkant tiek teisėsaugos, tiek žvalgybos tikslais. Vėliau šios teisės apimtys buvo tikslinamos 108 Konvencija, Rekomendacijomis valstybėms narėms dėl asmens duomenų naudojimo policijos sektoriuje, o šiuo metu yra rengiamas 108 Konvencijos atnaujinimo projektas bei Elektroninės žvalgybos kodeksas. Tačiau valstybių narių teisiniam reglamentavimui ir nacionalinių teismų sprendimų motyvams didžiausią įtaką daro EŽTT jurisprudencija.*
2. *ES 2018 m. asmens duomenų reforma buvo siekiama modernizuoti ES asmens duomenų tvarkymo sistemą. Kartu su BDAR ES pirmą kartą priėmė direktyvą, kuri reglamentuotų asmens duomenų tvarkymą teisėsaugos tikslais. Tačiau šioje direktyvoje įtvirtintos nuostatos yra bendro pobūdžio ir nereglamentuoja specifinės asmens duomenų rinkimo elektroninėje erdvėje srities.*
3. *ES yra priėmusi Asmens duomenų saugojimo direktyvą ir PNR direktyvą, kurių nuostatos įtakoja ir teisėsaugos veiklą. Šiomis dvejomis direktyvomis ES, siekdama suvienodinti valstybių narių praktiką, išplečia teisėsaugos institucijų priėjimo prie asmens duomenų galimybes ir apimtis.*
4. *Valstybių narių nacionalinio saugumo klausimai neapima ES kompetencijos, todėl žvalgybos veikla nėra reglamentuojama ES teisės normomis.*

---

[898] „Lietuvos Respublikos Konstitucija“, 22 str., eSeimas, žiūrėta 2020 m. rugpjūčio 17 d. https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/TAIS.1890?positionInSearchResults=0&searchModelUUID=5138f54d-b9a1-45eb-b519-9011c0500362.

[899] Žr., pvz., „Europos Žmogaus Teisių Teismo 2008 m. liepos 17 d. sprendimas I. prieš Suomiją (Nr. 20511/03)“, *Hudoc*, žiūrėta 2020 m. rugsėjo 8 d., https://hudoc.echr.coe.int/eng#{%22fulltext%22:[%2220511/03%22],%22documentcollectionid2%22:[%22GRANDCHAMBER%22,%22CHAMBER%22],%22itemid%22:[%22001-87510%22]}, „Europos Žmogaus Teisių Teismo 2008 m. gruodžio 2 d. sprendimas K. U. prieš Suomiją (Nr. 2872/02)“, *Hudoc*, žiūrėta 2020 m. rugsėjo 8 d.,https://hudoc.echr.coe.int/eng#{%22fulltext%22:[%222872/02%22],%22documentcollectionid2%22:[%22GRANDCHAMBER%22,%22CHAMBER%22],%22itemid%22:[%22001-89964%22]}.

[900] Egidijus Jarašiūnas, „Jurisprudencinė konstitucija“, *Jurisprudencija : mokslo darbai*, no. 12 (2006): 24–33.

4. ASMENS DUOMENŲ RINKIMO ELEKTRONINĖJE ERDVĖJE TEISĖSAUGOS IR ŽVALGYBOS TIKSLAIS REGLAMENTAVIMAS KONTINENTINĖJE TEISĖJE (LIETUVOS RESPUBLIKOS ATVEJO ANALIZĖ)

Lietuvoje, skirtingai nei JAV, nėra teisės aktų, skirtų reglamentuoti išimtinai tik asmens duomenų rinkimą el. erdvėje, tačiau tokios nuostatos yra sudėtinėmis Kriminalinės žvalgybos įstatymo, Baudžiamojo proceso kodekso ir Žvalgybos įstatymo dalimis. Taisyklės, kuriomis vadovaujasi teisėsaugos ir žvalgybos institucijos, yra skirtingos, todėl toliau disertacijoje jos bus išskirtos į atskirus skirsnius. Asmens duomenų rinkimo teisėsaugos ir žvalgybos tikslais reglamentavimą el. erdvėje Lietuvoje apžvelgsiu pagal gerosios praktikos pavyzdį JAV.

4.1. Asmens duomenų rinkimas elektroninėje erdvėje teisėsaugos tikslais

4.1.1 Ikiteisminis tyrimas

Teisėsaugos institucijos Lietuvoje asmens duomenis elektroninėje erdvėje gali rinkti vykdydamos kriminalinę žvalgybą ir ikiteisminį tyrimą. BPK 154 str. pavadinimo formuluotė „Elektroninių ryšių tinklais perduodamos informacijos kontrolė, fiksavimas ir kaupimas“ leidžia daryti prielaidą, kad šis straipsnis yra išimtinai skirtas reglamentuoti asmens duomenų rinkimą elektroninėje erdvėje. Jame numatytus procesinius veiksmus ikiteisminio tyrimo pareigūnai gali atlikti tik tada, kai kitais būdais pasiekti proceso tikslų negalima. Pasiekus tikslus ar procesinei prievartos priemonei tapus nebereikalingai jos taikymas turi būti nutrauktas[901], o taikymo teisėtumas vertinamas pagal teisinius ir faktinius pagrindus[902]. Visgi Generalinio prokuroro 2012 m. gruodžio 31 d. rekomendacijų dėl Kriminalinės žvalgybos įstatymo, Baudžiamojo proceso kodekso normų taikymo ir kriminalinės žvalgybos informacijos panaudojimo baudžiamajame procese[903], mokslinės literatūros analizė bei interviu metu gauti duomenys rodo, asmens duomenys elektroninėje erdvėje ikiteisminio tyrimo metu gali būti renkami ir vadovaujantis BPK 97 str. „Daiktų ir dokumentų, turinčių reikšmės nusikalstamai veikai tirti ir nagrinėti, išreikalavimas“, 145 str. „Krata“, 147 str. „Poėmis“, 155 str. „Prokuroro teisė susipažinti su informacija“, 158 str. „Savo tapatybės neatskleidžiančių ikiteisminio tyrimo pareigūnų veiksmai“ ir 207 str. „Apžiūra“. Šiame disertacijos skyriuje poskyryje apžvelgsiu asmens duomenų rinkimo elektroninėje erdvėje

[901] „Lietuvos Aukščiausiojo Teismo 2014 m. vasario 11 d. nutartis Nr. 2K-49/2014“, *eTeismai*, žiūrėta 2020 m. rugsėjo 8 d., https://eteismai.lt/byla/3132987904756/2K-446/2014.

[902] „Procesinės prievartos priemonės – elektroninių ryšių tinklais perduodamos informacijos kontrolės, jos fiksavimo ir kaupimo – taikymas“, Lietuvos Aukščiausiojo Teismo Teisės tyrimų ir apibendrinimo departamentas, 2015, 2.

[903] „Rekomendacijos dėl Kriminalinės žvalgybos įstatymo, Baudžiamojo proceso kodekso normų taikymo ir kriminalinės žvalgybos informacijos panaudojimo baudžiamajame procese, patvirtintos Lietuvos Respublikos generalinio prokuroro 2012 m. gruodžio 31 d. įsakymu Nr. I-383“, *eSeimas*, žiūrėta 2020 m. rugpjūčio 17 d., https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/TAIS.440985?jfwid=-9dzqnu8af.

ikiteisminio tyrimo metu reglamentavimo ypatumus BPK analizę pradedant BPK 154 str., kuris reglamentuoja asmens duomenų rinkimą realiuoju laiku.

1. Asmens duomenų rinkimas elektroninėje erdvėje realiuoju laiku.

1.1. Renkamų asmens duomenų apimtys. BPK 154 str. yra išskiriamos dvi asmens duomenų el. erdvėje rūšys:

1) Pokalbiai, kurių galima klausytis;
2) Kita informacija.

JAV yra įprasta duomenis skirstyti į turinio ir metaduomenis. Kaip jau minėjau 1 disertacijos skyriuje, ši JAV praktika pamažu yra perimama ir ES, Reglamento dėl elektroninių ryšių ir privatumo projekte asmens duomenys jau yra skirstomi ne į turinio ir srauto bei vietos nustatymo, o į turinio ir metaduomenis. Palyginimui, Kriminalinės žvalgybos įstatyme yra išskiriami:

1) Turinio;
2) Srauto duomenys;
3) kita informacija.

Galima teigti, kad BPK 154 str. minima „kita informacija" apima kito nei telefoninių pokalbių turinio, srauto, vietos nustatymo ir kitus metaduomenis, tačiau turinio ir metaduomenų sąvokos yra skirtingų kategorijų, Elektroninių ryšių reguliavimo įstatyme yra vartojamos komunikacijos turinio, srauto ir vietos nustatymo duomenų sąvokos. Šios sąvokos yra perkeltos ir į Kriminalinės žvalgybos įstatymą. EP atlikta studija rodo telefoninių pokalbių mažėjimo tendenciją tarp vartotojų juos pakeičiant IP telefonija[904]. Bendravimo per elektroninę erdvę programėlės (pvz., WhatsApp, Viber, Messenger) naudoja ištisinį šifravimą (angl. *end to end encryption*), taigi ir pokalbių, kurių galima klausytis, skaičius turėtų būti ženkliai mažesnis lyginant su kitu komunikacijos turiniu. Atsižvelgiant į tai, kad BPK 154 str. įtvirtinti terminai turėtų būti suderinami su galiojančiu teisiniu reglamentavimu[905], įsigaliojus Reglamentui dėl elektroninių ryšių ir privatumo, pokalbių, kurių galima klausytis" ir „kitos informacijos" sąvokos turės būti pakeistos į turinio ir metaduomenų sąvokas. Struktūruoto interviu duomenys rodo, jog ikiteisminio tyrimo pareigūnams taip pat yra neaiški BPK 154 str. pagrindu renkamų asmens duomenų apimtis. 13 struktūruoto interviu respondentų nurodė, kad BPK 154 str. reglamentuoja ir turininio pobūdžio, ir metaduomenų rinkimą, 9 struktūruoto interviu respondentai mano, jog tik turininio pobūdžio duomenis, o 1 respondentas nurodė, jog tik metaduomenis.

BPK 154 str. 2 d. yra įtvirtinti reikalavimai teisėjo nutarčiai ar prokuroro nutarimui klausytis asmenų pokalbių, perduodamų elektroninių ryšių tinklais, daryti jų įrašus, kontroliuoti kitą elektroninių ryšių tinklais perduodamą informaciją ir ją fiksuoti bei kaupti. Nutartyje ar nutarime turi būti nurodyta turimi duomenys apie asmenį,

---

[904] „Regulating Electronic Communications: A Level Playing Field for Telecoms and OTTs?", *European Parlament*, žiūrėta 2020 m. rugpjūčio 17 d., https://www.europarl.europa.eu/thinktank/en/document.html?reference=EPRS_BRI%282016%29586641.

[905] Štitilis ir Laurinaitis, *supra note*, 26.

kurio atžvilgiu BPK 154 str. numatyta priemonė bus taikoma. Taigi nutartyje turi būti nurodytas asmens vardas ir pavardė, jo asmens kodas arba gimimo data. Generalinio prokuroro rekomendacijų 41 p. yra nurodyta, kad prokuroro prašyme ikiteisminio tyrimo teisėjui gali būti nenurodomas asmens naudojamas telefono ryšio numeris, elektroninių ryšių tinklų galinis įrenginys ar elektroninio pašto duomenys[906]. Tai reiškia, kad teismas, sankcionuodamas BPK 154 str. įtvirtintą procesinės prievartos priemonę, ne visais atvejais žino kokios bus jos naudojimo apimtys ir sankciją išduoda ne asmens duomenų, o asmens atžvilgiu. LAT atkreipia dėmesį, kad prokurorų prašymuose kartais nenurodomi duomenys apie asmenis, kuriems prašoma taikyti minėtą procesinės prievartos priemonę – nurodomas tik telefono abonentinis numeris, nors BPK 154 str. elektroninių ryšių tinklais perduodamos informacijos kontrolės ir įrašų darymo galimybė siejama ne su konkrečiais telefonų numeriais, o su konkrečiais asmenimis, kuriems prašomi veiksmai turi būti atlikti[907]. Struktūruoto interviu respondentai taip pat nurodė, kad teikdami prašymą prokurorui dėl BPK 154 str. taikymo, paprastai nedetalizuoja kokio pobūdžio duomenų jie prašo iš elektroninių ryšių paslaugų teikėjų[908], o pastarieji suteikia visą informaciją (ir turinį, ir metaduomenis) nors ir ikiteisminio tyrimo pareigūnas to neprašo[909]. Metaduomenys taip pat yra asmens duomenimis[910], todėl perteklinės informacijos pateikimas laikytinas teisės į asmens duomenų apsaugą pažeidimu.

Analizuojant BPK 154 str. nuostatas klausimas kyla ir dėl šiuo straipsniu reglamentuojamų renkamų asmens duomenų pobūdžio, t. y. ar ikiteisminio tyrimo metu tiek turinį, tiek metaduomenis vadovaujantis BPK 154 str. galima rinkti tiek esamuoju laiku, tiek jiems jau esant istorinio pobūdžio. Autorės nuomone, BPK 154 str. 1 d. reglamentuoja tik esamuoju laiku vykstančios komunikacijos duomenų rinkimą, kadangi jame yra tokios formuluotės: [...] klausytis asmenų pokalbių [...], [...] kontroliuoti kitą elektroninių ryšių tinklais perduodamą [...], (o ne perduotą) informaciją. BPK 154 str. 3 d. analogiškai 1 d. gali būti „kontroliuojama ir fiksuojama elektroninių ryšių tinklais perduodama informacija [...]“. Vadinasi, pagal įtvirtintą juridinę techniką istorinio pobūdžio asmens duomenų rinkimas nėra reglamentuojamas BPK 154 str. Šio straipsnio ypatumai yra išskirti 3 lentelėje. Istorinio pobūdžio asmens duomenys yra renkami vadovaujantis kitais BPK straipsniais, pvz. BPK 97, 147, 155, 158 str., kurie nėra skirti reglamentuoti išimtinai tik asmens duomenų rinkimo elektroninėje erdvėje.

---

906 „Rekomendacijos dėl Kriminalinės žvalgybos įstatymo, Baudžiamojo proceso kodekso normų taikymo ir kriminalinės žvalgybos informacijos panaudojimo baudžiamajame procese, patvirtintos Lietuvos Respublikos generalinio prokuroro 2012 m. gruodžio 31 d. įsakymu Nr. I-383“, 41 p., *eSeimas*, žiūrėta 2020 m. rugpjūčio 17 d., https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/TAIS.440985?jfwid=-9dzqnu8af.

907 „Lietuvos Aukščiausiojo Teismo Teisės tyrimų ir apibendrinimo departamento apibendrinimas „Procesinės prievartos priemonės – elektroninių ryšių tinklais perduodamos informacijos kontrolės, jos fiksavimo ir kaupimo – taikymas“.

908 Struktūruoto interviu rezultatai.

909 Struktūruoto interviu rezultatai.

910 „Bureau of Investigative Journalism and Alice Ross v. the United Kingdom, Written Submissions on Behalf of the International Commission of Jurists (ICJ)“, žiūrėta 2020 m. rugpjūčio 16 d., https://www.icj.org/wp-content/uploads/2016/02/UK-ICJ-AmicusBrief-BJURoss-ECtHR-legalsubmission-2016.pdf.

3 lentelė. *Asmens duomenų rinkimas elektroninėje erdvėje pagal BPK 154 str.*

El. asmens duomenys	Metaduomenys						Turinys				
	Rūšis					Teisminis sankcionavimas	Pokalbiai		Kt. turinys		Teisminis sankcionavimas
	tinklo	programos	paslaugos				Nešifruotas, arba užšifruotas kitu būdu nei ištisinis šifravimas		Užšifruotas ištisiniu šifravimu		
	Esam. l.	Esam. l.	Istorinis								
			Srauto	Vietos nustatymo	Kt.		Esamuoju laiku	Istorinis	Esamuoju laiku	Istorinis	
Ūkio subjektai, teikiantys el. ryšių tinklus[911]	Taip	Taip	–	–	–	Ikiteism. tyr. teisėjas	Taip	–	–	–	Ikiteism. tyr. teisėjas
Ūkio subjektai, teikiantys el. ryšių paslaugas[912]	Taip	Taip	–	–	–	Ikiteism. tyr. teisėjas	Taip	–			Ikiteism. tyr. teisėjas
Kiti juridiniai asmenys	–	–	–	–	–	–	–	–	–	–	–

1.2. Subjektai, iš kurių galima rinkti el. erdvės asmens duomenis vadovaujantis BPK 154 str. yra du (žr. 3 lentelę):

1) Ūkio subjektai, teikiantys el. ryšių tinklų paslaugas;
2) Ūkio subjektai, teikiantys el. ryšių tinklus.

Iki 2007 m. galiojusio BPK normos reglamentavo ne el. ryšių, o telekomunikacijų tinklais perduodamos informacijos kontrolę. Manoma, kad po 2007 m. atliktų BPK 154 str. pataisų, jo reguliavimas apima visą internetu perduodamų duomenų kontrolę, įskaitant IP telefoniją[913]. Visgi, ar tikrai paslaugų el. erdvėje teikėjai, šias paslaugas teikiantys naudojantis el. ryšių tinklais (pvz., Viber, WhatsApp, Facebook ir kt.

[911] **Elektroninių ryšių tinklas** – perdavimo sistemos ir (arba) komutavimo bei maršruto parinkimo įranga, kitos priemonės, įskaitant pasyviuosius tinklo elementus, leidžiančios perduoti signalus laidinėmis, radijo, optinėmis ar kitomis elektromagnetinėmis priemonėmis, įskaitant palydovinius tinklus, fiksuotuosius (kanalų ir paketų komutavimo, įskaitant internetą) ir judriuosius antžeminius tinklus, elektros perdavimo kabelines sistemas (kiek jos naudojamos signalams perduoti), tinklus, naudojamus radijo ir (arba) televizijos programoms transliuoti (retransliuoti), ir kabelinės televizijos bei mikrobangų daugiakanalės televizijos tinklus neatsižvelgiant į perduodamos informacijos pobūdį.

[912] **Elektroninių ryšių paslauga** – paprastai už atlygį teikiama paslauga, kurią visiškai ar daugiausia sudaro signalų perdavimas elektroninių ryšių tinklais, įskaitant telekomunikacijų paslaugas ir perdavimo (siuntimo) paslaugas transliavimui (retransliavimui) naudojamais tinklais. Elektroninių ryšių paslaugos neapima elektroninių ryšių tinklais ar naudojant elektroninių ryšių paslaugas perduodamos informacijos turinio teikimo ar redakcinės turinio kontrolės paslaugų, tarp jų informacinės visuomenės paslaugų, kurių visiškai ar daugiausia nesudaro signalų perdavimas elektroninių ryšių tinklais.

[913] Štitilis ir Laurinaitis, *supra note*, 26.

programėlių savininkai), yra priskiriami ūkio subjektams, teikiantiems el. ryšių tinklų paslaugas? Elektroninių ryšių reguliavimo įstatyme elektroninių ryšių paslauga apibrėžiama kaip *paprastai už atlygį teikiama paslauga, kurią visiškai ar daugiausia sudaro signalų perdavimas elektroninių ryšių tinklais, įskaitant telekomunikacijų paslaugas ir perdavimo (siuntimo) paslaugas transliavimui (retransliavimui) naudojamais tinklais*. Tačiau tai nėra absoliuti taisyklė. *Elektroninių ryšių paslaugos neapima elektroninių ryšių tinklais ar naudojant elektroninių ryšių paslaugas perduodamos informacijos turinio teikimo ar redakcinės turinio kontrolės paslaugų, tarp jų informacinės visuomenės paslaugų, kurių visiškai ar daugiausia nesudaro signalų perdavimas elektroninių ryšių tinklais*[914].

El. ryšių paslaugos apibrėžimą sudaro keli elementai:

a) signalų perdavimas elektroninių ryšių tinklais,
b) išskyrus:
   - turinio teikimo ir redakcinės kontrolės paslaugas,
   - informacinės visuomenės paslaugas.

Informacinė visuomenė yra apibrėžiama taip: paprastai už atlyginimą elektroninėmis priemonėmis ir per atstumą individualiu informacinės visuomenės paslaugos gavėjo prašymu teikiamos paslaugos[915]. Pagal Europos Parlamento ir Tarybos direktyvą 98/48/EB iš dalies keičiančią Direktyvą 98/34/EB, nustatančią informacijos apie techninius standartus ir reglamentus teikimo tvarką:

1) „teikimas per atstumą“ reiškia, kad paslauga, teikiama šalims nesant kartu vienoje vietoje;
2) „elektroninėmis priemonėmis“ – reiškia, kad iš pradžių paslauga elektronine įranga pasiunčiama ir priimama duomenims apdoroti (įskaitant skaitmeninį tankinimą) ir saugoti, o galutinai perduodama ir priimama laidais, radijo, optinėmis, kitomis elektromagnetinėmis priemonėmis;
3) „asmenišku paslaugų gavėjo prašymu“ reiškia, kad paslauga teikiama perduodant duomenis asmenišku prašymu.

Europos Parlamento studijoje *„Regulating electronic communications. A level playing field for telecoms and OTTs“* tradicines telekomunikacijų paslaugas pakeičiančias paslaugas, teikiamas naudojantis el. ryšių tinklais, vadinama „over the top services (arba OTT)“, kas reiškia paslaugomis teikiamomis kitų paslaugų dėka (šiuo atveju, interneto). Prie OTT yra priskiriama keletas rūšių paslaugų, tarp kurių yra ir socialinių tinklų paslaugų teikėjai, komunikacijos programėlės bei internetinės paieškos sistemos (pvz. Facebook, Google, WhatsApp, Viber, Instagram ir kt.). OTT paslaugos yra informacinės visuomenės paslaugos[916]. Vadinasi, nors BPK 154 str. buvo pakeistas subjektų

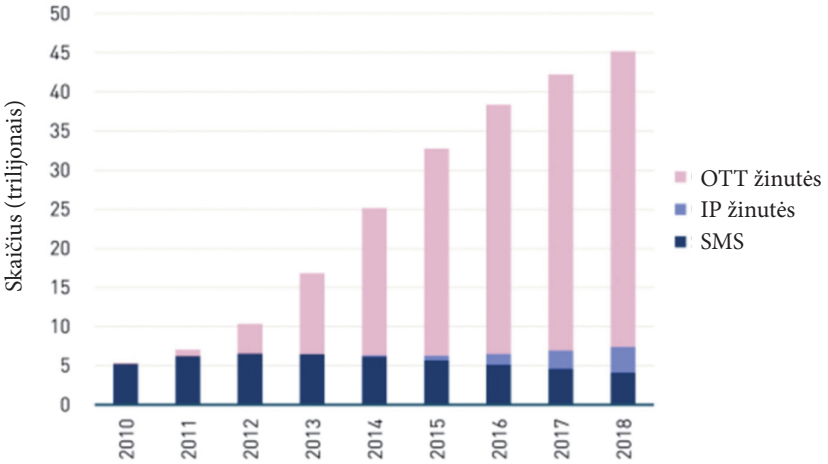
---

[914] „Lietuvos Respublikos elektroninių ryšių įstatymas“, 3 str. 15 d. *eTAR*, žiūrėta 2020 m. rugpjūčio 17 d., https://www.e-tar.lt/portal/lt/legalAct/TAR.82D8168D3049/asr.

[915] „Informacinės visuomenės paslaugų samprata“, *Informacinės visuomenės plėtros komitetas*, žiūrėta 2020 m. rugsėjo 8 d., http://ivpk.lrv.lt/lt/veiklos-sritys-1/informacines-visuomenes-paslaugos-1/informacines-visuomenes-paslaugu-samprata.

[916] „Regulating Electronic Communications: A Level Playing Field for Telecoms and OTTs?“, *European Parlament*, žiūrėta 2020 m. rugpjūčio 17 d., https://www.europarl.europa.eu/thinktank/en/document.html?reference=EPRS_BRI%282016%29586641.

pavadinimas iš telekomunikacijų tinklų paslaugų teikėjų į el. ryšio paslaugų teikėjus, tačiau šis pakeitimas nebuvo esminis, nes subjektų, iš kurių teisėsaugos institucijos gali prašyti asmens duomenų, ratas nepakito, kadangi el. paslaugų teikėjų sąvoka pagal dabar galiojantį Elektroninių ryšių įstatymą neapima socialinių tinklų paslaugų teikėjų, komunikacijos programėlių, internetinės paieškos sistemų teikėjų ir kitų paslaugas per el. erdvę teikiančių ūkio subjektų, nors jų naudojimo apimtys disertacijos rašymo metu, kaip pavaizduota 7 paveiksle, ženkliai viršija mobiliojo ir fiksuotojo ryšio telefonijos paslaugų naudojimą.



7 pav. *IP telefonijos naudojimo apimtys*[917].

Diskusijas dėl kitų nei telekomunikacijų paslaugų elektroninėje erdvėje teikėjų priskyrimo arba nepriskyrimo elektroninių ryšių paslaugų teikėjams 2018 m. sprendė ESTT[918]. *SkypeOut byloje* (C-142/18) ESTT konstatavo, kad Skype paslauga kuomet yra skambinama ne kitam Skype vartotojui, bet į fiksuoto ar mobiliojo ryšio telefono numerį turėtų būti laikoma elektroninių ryšių paslauga nors Skype elektroninių signalų perdavimą SkypeOut paslaugos funkcionavimui teikia ne pats, o sutarties su elektroninių ryšių tinklų tiekėju pagrindu, bet nesant šios sutarties *SkypeOut* paslaugos teikimas būtų negalimas[919]. *Gmail byloje* (C-193/18) ESTT priėjo prie išvados, kad

[917] „Regulating Electronic Communications: A Level Playing Field for Telecoms and OTTs?“, *European Parlament*, žiūrėta 2020 m. rugpjūčio 17 d., https://www.europarl.europa.eu/thinktank/en/document.html?reference=EPRS_BRI%282016%29586641.

[918] „ECJ Clarifies Scope of Telecoms Regulation for OTT Services“, *Technology's Legal Edge*, 2019, žiūrėta 2020 m. rugsėjo 8 d., https://www.technologyslegaledge.com/2019/07/ecj-clarifies-scope-of-telecoms-regulation-for-ott-services/.

[919] „Europos Sąjungos Teisingumo Teismo 2019 m. birželio 5 d. sprendimas byloje Nr. C-142/18 Skype Communications Sàrl prieš Institut belge des services postaux et des télécommunications (IBPT)“, *InfoCuria*, žiūrėta 2020 m. rugsėjo 8 d., http://curia.europa.eu/juris/document/document.jsf?text=&docid=214741&pageIndex=0&doclang=EN&mode=req&dir=&occ=first&part=1.

Gmail negali būti laikomas elektroninių ryšių paslaugų teikėju, kadangi teikdamas elektroninio pašto paslaugą pats *Gmail* nedalyvauja signalų perdavime, kuris yra vienas iš elektroninių ryšių paslaugos apibrėžimo elementų[920]. Tačiau 2018 m. gruodžio 11 d. Europos Parlamentas ir Taryba priėmė direktyvą (ES) 2018/1972, kuria nustatomas Europos elektroninių ryšių kodeksas[921]. Šiame kodekse yra pateikiamas naujas elektroninių ryšių paslaugų apibrėžimas, pagal kurį minėti du ESTT sprendimai tampa nebeaktualūs. Pagal naują apibrėžimą yra išplečiamas elektroninių ryšių paslaugų teikėjų ratas apimant beveik visas paslaugas per elektroninę erdvę teikiančios įmonės[922]. Taigi, nors pagal disertacijos rašymo metu ir iki 2020 m. gruodžio 11 d. galiojančius teisės aktus BPK 154 str. nurodyti ūkio subjektai, teikiantys elektroninių ryšių paslauga s turėtų būti aiškinami kaip neapimantys kitų nei telekomunikacijų įmonių, tačiau Elektroninių ryšių kodekso nuostatas perkėlus į Elektroninių ryšių reguliavimo įstatymą BPK 154 str. numatyti subjektai turės būti aiškinami kaip apimantys visus subjektus, teikiančius paslaugas per elektroninę erdvę.

Antroji subjektų grupė numatyta BPK 154 str. yra ūkio subjektai, įrengiantys el. ryšių tinklus. *Elektroninių ryšių tinklas yra apibrėžiamas kaip perdavimo sistemos ir (arba) komutavimo bei maršruto parinkimo įranga, kitos priemonės, įskaitant pasyviuosius tinklo elementus, leidžiančios perduoti signalus laidinėmis, radijo, optinėmis ar kitomis elektromagnetinėmis priemonėmis, įskaitant palydovinius tinklus, fiksuotuosius (kanalų ir paketų komutavimo, įskaitant internetą) ir judriuosius antžeminius tinklus, elektros perdavimo kabelines sistemas (kiek jos naudojamos signalams perduoti), tinklus, naudojamus radijo ir (arba) televizijos programoms transliuoti (retransliuoti), ir kabelinės televizijos bei mikrobangų daugiakanalės televizijos tinklus neatsižvelgiant į perduodamos informacijos pobūdį*[923]. Taigi, el. ryšių tinklų teikėjai paslaugų gyventojams tiesiogiai neteikia. Paslaugas jie teikia el. ryšių paslaugų teikėjams. Dažniausiai el. ryšių tinklų teikėjai yra naudojami žvalgybos tikslais[924], todėl šių subjektų, kaip asmens duomenų šaltinių, minėjimas BPK 154 str., yra nepagrįstas.

Vadinasi, iki Elektroninių ryšių kodekso nuostatas perkeliant į Elektroninių ryšių įstatymą turėtų būti traktuojama, kad BPK 154 str. vienintelis realus subjektas į kurį teisėsaugos institucijos turi teisę kreiptis dėl el. erdvės asmens duomenų rinkimo yra – el. ryšių paslaugų teikėjai prie kurių nėra priskiriami kiti juridiniai asmenys, teikiantys paslaugas elektroninėje erdvėje.

---

[920] „Europos Sąjungos Teisingumo Teismo 2019 m. birželio 13 d. sprendimas Nr. C-193/18 Google LLC prieš Vokietijos Federacinę Respubliką“, *InfoCuria*, žiūrėta 2020 m. rugsėjo 8 d., http://curia.europa.eu/juris/document/document.jsf?text=&docid=214944&pageIndex=0&doclang=EN&mode=req&dir=&occ=first&part=1.

[921] „2018 m. gruodžio 11 d. Europos Parlamento ir Tarybos direktyva (ES) 2018/1972, kuria nustatomas Europos elektroninių ryšių kodeksas“, *EUR-Lex*, žiūrėta 2020 m. rugpjūčio 17 d. https://eur-lex.europa.eu/legal-content/LT/TXT/?uri=CELEX:32018L1972

[922] Elena Gil Gonzalez, Paul De Hert ir Vagelis Papakonstantinou, „The Proposed ePrivacy Regulation: The Commission's and the Parliament's Draft s at a Crossroads?“, in D Hallinan, R Leenes, S Gutwirth and P De Hert (eds), *Data Protection and Privacy. Data Protection and Democracy.* Hart Publishing, 2020, 267–298.

[923] „Lietuvos Respublikos elektroninių ryšių įstatymas“, 3 str. 15 p., *eTAR*, žiūrėta 2020 m. rugpjūčio 17 d., https://www.e-tar.lt/portal/lt/legalAct/TAR.82D8168D3049/asr.

[924] „Russian Agents Plunge to New Ocean Depths in Ireland to Crack Transatlantic Cables“, *The Sunday Times,* žiūrėta 2020 m. rugsėjo 8 d., https://www.thetimes.co.uk/article/russian-agents-plunge-to-new-ocean-depths-in-ireland-to-crack-transatlantic-cables-fnqsmgncz.

1.3. Asmens duomenų rinkimo realiuoju laiku el. erdvėje teisiniai pagrindai. Kadangi el. erdvė sudaro galimybes asmens duomenis rinkti didesniais mastais nei naudojantis įprastinėmis nusikalstamų veikų tyrimo technikomis, todėl vienu iš pagrindinių teisėtumo užtikrinimo asmens duomenų rinkimo el. erdvėje teisėsaugos tikslais pamatų yra sankcionavimas[925]. Skirtingose pasaulio valstybėse egzistuoja skirtinga sankcionavimo praktika, bet apibendrintai sankcionuojančiu subjektu gali būti specialus (pvz., JAV FISA teismas) ar bendrosios kompetencijos teismas, prokuroras, specialus komisaras arba įgaliota institucija[926]. BPK yra įtvirtintas ne vienas, o keli asmens duomenų rinkimo el. erdvėje sankcionavimo modeliai, tačiau sankcionavimas yra privalomas ne visais atvejais:

1. Ikiteisminio tyrimo teisėjas sankcionuoja prokuroro prašymą (BPK 154 str. 1 d.). Tai yra pagrindinė taisyklė. Vadinasi, paprastai asmens duomenys el. erdvėje turėtų būti renkami tokių veiksmų sankcionavimą atlikus ikiteisminio tyrimo teisėjui. Ikiteisminio tyrimo pareigūnų struktūruoto interviu duomenys rodo, kad teismas prokurorų prašymus beveik visuomet sankcionuoja, o prokuroras atitinkamai labai retai atmeta pareigūnų prašymus kreipti į teismą dėl sankcionavimo[927]. Nors yra autorių manančių, kad teisminis procesinių veiksmų sankcionavimas yra tik formalumas[928], tačiau, kita vertus, institucijos, kuri vienintelė vykdo teisingumą, sankcionavimas suponuoja didesnę asmens teisių apsaugą. Vykdydamas ikiteisminio tyrimo teisėjo teisėtumo kontrolės funkciją, ikiteisminio tyrimo teisėjas užtikrina, kad nebūtų pažeisti procese dalyvaujančio asmens teisėti interesai, kad procese dalyvaujantys asmenys laikytųsi galiojančių įstatymų, t. y. užtikrina proceso teisėtumą. Jis konstatuoja, ar buvo (nebuvo) pažeistos asmens teisės, ar yra pakankamas pagrindas skirti procesines prievartos priemones arba nagrinėti bylą teisme, vertina pateiktą informaciją, remdamasis teisminė perspektyva, vykdo justicijos funkciją ikiteisminiame tyrime[929]. Tą iliustruoja pavyzdys JAV, kuomet asmens duomenų rinkimo el. erdvėje teisės aktai buvo teismų sprendimų rezultatas[930]. Nors Lietuva yra kontinentinės teisės tradicijų šalis, tačiau LAT praktika ir EŽTT jurisprudencija turi didelę reikšmę teisės į asmens duomenų apsaugą užtikrinime. Problema yra ta, kad ikiteisminio tyrimo pareigūnai ne visada laikosi LAT formuojamos gerosios praktikos. Pavyzdžiui, vadovaujantis BPK 11 str. 1 d. ir Lietuvos teismų praktika[931] ikiteisminio tyrimo

[925] „Current Practices in Electronic Surveillance in the Investigation of Serious and Organized Crime“, United Nations, 2009, 13, žiūrėta 2020 m. rugpjūčio 17 d., https://www.unodc.org/documents/organized-crime/Law-Enforcement/Electronic_surveillance.pdf.

[926] *Ibid.,* 15.

[927] Struktūruoto interviu duomenys.

[928] Walter F. Pratt, *Privacy in Britain* (Bucknell University Press, 1979), 59.

[929] Marina Gušauskienė, „Ikiteisminio tyrimo teisėjas – žmogaus teisių garantas“, *Jurisprudencija* 54, nr. 49 (2004): 129, 130.

[930] Stephen Rushin, „The Judicial Response to Mass Police Surveillance“, *University of Illinois Journal of Law, Technology & Policy* 2011, no. 2 (2011): 281–328.

[931] „Lietuvos Aukščiausiojo Teismo Elektroninių ryšių tinklais perduodamos informacijos kontrolės, jos fiksavimo ir kaupimo (Baudžiamojo proceso kodekso 154 straipsnis, Kriminalinės žvalgybos įstatymo 10 straipsnis) taikymo apžvalga“, *Lietuvos Aukščiausiasis Teismas*, žiūrėta 2020 m. rugpjūčio 17 d., https://www.lat.lt/lat-praktika/teismu-praktikos-apzvalgos/baudziamuju-bylu-apzvalgos/68.

pareigūnai prieš taikydami BPK 154 str. įtvirtintą procesinę prievartos priemonę privalo įsitikinti, kad kitais būdais tos informacijos surinkti nėra galimybės arba jos surinkimas būtų labai apsunkintas, tačiau 9 iš 22 struktūruoto interviu respondentų nurodė taip nedarantys[932].

2. Neatidėliotinais atvejais – prokuroro nutarimu, jeigu per tris dienas prokuroro nutarimą sankcionuoja ikiteisminio tyrimo teisėjas (BPK 160[1] str. 1 d.). Kriminalinės žvalgybos įstatyme yra pateiktas baigtinis neatidėliotinų atvejų sąrašas: kai iškyla pavojus žmogaus gyvybei, sveikatai, nuosavybei, visuomenės ar valstybės saugumui. Ką galima laikyti neatidėliotinus atvejus BPK 154 str. prasme nėra apibrėžta. Vadinasi, tai yra vertinamoji sąvoka ir ar atvejį galima laikyti neatidėliotinu, turėtų būti sprendžiama kiekvienu konkrečiu atveju individuliai. Struktūruoto interviu respondentai neatidėliotinus atvejus laiko duomenų rinkimą nusikalstamos veikos darymo metu, nusikalstamą veiką galimai padariusių asmenų persekiojimą „karštais pėdsakais", kai gresia pavojus asmens gyvybei ir (ar) sveikatai[933].
3. Nesankcionuotas asmens duomenų rinkimas. Jis yra galimas, kai yra duotas BPK 154 str. 6 d. įvardintų asmenų – nukentėjusiųjų, liudytojų ar kitų proceso dalyvių – sutikimas arba pateiktas jų prašymas, jei nesinaudojama ūkio subjektų, teikiančių elektroninių ryšių tinklus ir (ar) paslaugas, paslaugomis ir įrenginiais. Tokiu atveju nukentėjusiųjų, liudytojų ar kitų proceso dalyvių pokalbių perduodamų elektroninių ryšių tinklais, galima klausytis, daryti jų įrašus, kontroliuoti kitą šių asmenų elektroninių ryšių tinklais perduodamą informaciją, ją fiksuoti ir kaupti nors ir nėra tuo klausimu priimtos ikiteisminio tyrimo teisėjo nutarties ar prokuroro nutarimo. Šis asmens duomenų rinkimo el. erdvėje pagrindas yra diskutuotinas. Nors procedūrų skaidrumas ir tikslumas yra laikomas vienu iš asmens duomenų rinkimo el. erdvėje pagrindų[934], kokia tokiu atveju yra asmens duomenų rinkimo tvarka, BPK nereglamentuoja. Nėra aišku ar tokiu atveju yra reikalingas prokuroro patvirtinimas ar prašymas/sutikimas savaime yra leidimas ir ikiteisminio tyrimo pareigūnas gali rinkti asmens duomenis vien šio prašymo/sutikimo pagrindu. Svarbu atkreipti dėmesį ir į dar kelis probleminius aspektus. Visų pirma, nesankcionuoto asmens sutikimo pagrindu galima rinkti bent kada, nes BPK 154 str. 6 d. nėra specialių aplinkybių, kuomet asmens duomenų rinkimui turėtų pakakti sutikimo/leidimo. Atsižvelgiant į tai, kad tik neatidėliotinais atvejais asmens duomenis el. erdvėje galima rinkti prokuroro nutarimu ir vis tiek yra reikalingas teisminis sankcionavimas, tai sankcionavimo nebuvimas, ypatingų aplinkybių nenumatymas, asmens duomenų rinkimą BPK 154 str. 6 d. įtvirtinto asmens sutikimo/leidimo pagrindu padaro aukštesnės galios nei duomenų rinkimą neatidėliotinais atvejais sankcionavus prokurorui. Nors teisminis sankcionavimas ir nėra privalomas nei pagal EŽTK, nei pagal Chartiją,

[932] Struktūruoto interviu duomenys.

[933] Struktūruoto interviu duomenys.

[934] „Document on surveillance of electronic communications for intelligence and national security purposes", Article 29 Data Protection Working Party, 2014, žiūrėta 2020 m. rugpjūčio 17 d., https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp228_en.pdf

tačiau tai yra numatyta Lietuvos Respublikos Konstitucijos 22 str. , o arbitras turi būti nešališkas, kad galėtų nuspręsti ar konkretus asmens teisių suvaržymas yra būtinas demokratinėje visuomenėje. Kita BPK 154 str. 6 d. ypatybė yra ta, kad nėra nurodoma ir apie ką duomenis teisėsauga gali rinkti. Tėra nurodyta, kad „nukentėjusiųjų, liudytojų ar kitų proceso dalyvių pokalbių perduodamų elektroninių ryšių tinklais, galima klausytis, daryti jų įrašus, kontroliuoti kitą šių asmenų elektroninių ryšių tinklais perduodamą informaciją, ją fiksuoti ir kaupti". Vadinasi, nors informacijos šaltinis yra sutikimą davęs proceso dalyvis, tačiau informacijos subjektu gali būti bent kas, tame tarpe ir įtariamasis ar bent kuris kitas asmuo, kuris procesinės prievartos veiksmo atlikimo metu neturi procesinio statuso. Struktūruoto interviu rezultatai rodo, kad tyrėjai galimybe asmens duomenis rinkti asmens sutikimo pagrindu naudojasi retai[935]. Struktūruoto interviu respondentai nurodė, kad sutikimą duodantis subjektas dažniausiai yra nukentėjusysis, tačiau tokiu asmeniu, pasak respondentų, gali būti ir asmuo, neturintis procesinio statuso[936]. BPK taip pat nenumato kokia forma proceso dalyvis gali duoti susitikimą/leidimą. Kaip nurodo G. Goda procese dalyvaujančių asmenų prašymas ar sutikimas turėtų būti formuluojamas raštu ir pridedamas prie ikiteisminio tyrimo bylos[937]. Struktūruoto interviu respondentai nurodė, kad paprastai prašo rašytinio asmens sutikimo. Tačiau nevienodas yra prokuroro vaidmuo tokio sutikimo tvirtinimo procese. Daugiau nei pusė respondentų nurodė, kad jie nesikreipia į prokurorą dėl proceso dalyvio sutikimo tvirtinimo, likusieji teigė, jog sutikimas yra prokuroro tvirtinamas. Tai rodo, jog nėra susiklosčiusios praktikos kaip tokiu atveju ikiteisminio tyrimo pareigūnai turėtų elgtis, todėl nors BPK ir nereikalauja, ikiteisminio tyrimo pareigūnai yra linkę prašyti prokuroro sankcionavimo.

Lanksčios BPK 154 str. 6 d. nuostatos sudaro sąlygas piktnaudžiaujant proceso dalyvio sutikimu/leidimu rinkti asmens duomenis ir tais atvejais, kuomet galbūt ikiteisminio tyrimo teisėjas to nesankcionuotų. Įdomu yra tai, kad daugiau nei vienas BPK įtvirtintas procesinės prievartos veiksmas negali būti atliekamas bent kurio proceso dalyvio sutikimo pagrindu[938]. Todėl leisti asmens duomenis rinkti šiuo pagrindu taikant ypač jautrią teisės į asmens duomenų apsaugą pažeidimui techniką – rinkimą el. erdvėje – gali reikšti ES pagrindinių teisių chartijoje ir EŽTK įtvirtintos pamatinės asmens teisės pažeidimą. Tačiau įdomus šios nuostatos aspektas yra tas, kad esant sutikimui nesankcionuotai galima rinkti tik tuomet, kai tai daroma nesinaudojant ūkio subjektų, teikiančių elektroninių ryšių tinklus ir (ar) paslaugas, paslaugomis ir įrenginiais. Vadinasi, teisėsaugos institucijos nesankcionuotos elektroninius asmens duome-

[935] Struktūruoto interviu rezultatai.

[936] Struktūruoto interviu rezultatai.

[937] Gintaras Goda, „Procesinių prievartos priemonių Lietuvos Respublikos baudžiamojo proceso kodekso projekte samprata, klasifikacija ir turinys", Teisė. (2000): 17–27.

[938] Asmens būsto ar tarnybinių patalpų, kurios nėra įvykio vieta, tyrimas gali būti atliekamas esant būsto savininko ar įmonės, įstaigos, organizacijos atstovo sutikimui, tačiau šie asmenys nėra proceso dalyviais.

nis gali rinkti tik tuo atveju, jeigu jos pačios turi asmens duomenų rinkimo el. erdvėje įrankį ir jį įdiegia į sutikimą davusio asmens įrenginį, duomenis renka tiesiogiai iš sutikimą davusio asmens mobiliojo įrenginio neįrašę į jį specialios programinės įrangos arba duomenis renka iš kitų juridinių asmenų nei el. ryšių paslaugų teikėjai, perka iš kitų nei elektroninių ryšių tinklus ir paslaugas teikiančių subjektų – pvz. elektroninės žvalgybos paslaugas teikiančių įmonių. Kaip matysime tolimesniame disertacijos skyriuje, šiuo atveju santykiai tarp teisėsaugos bei elektroninės žvalgybos paslaugas teikiančių subjektų paprastai yra reglamentuojami tik sutartimi, kurios nuostatos gali priklausyti nuo pasirinktos taikytinos teisės. Yra galimas ir toks atvejis, kai pats asmuo į savo įrenginį įsirašo specialią asmens duomenų rinkimo programėlę (pvz. Call Recoder, Cube Call Recorder ACR ir kt.). Manytina, kad tokios programėlės pagrindu surinktų asmens duomenų naudojimo baudžiamajame procese teisėtumas ir pagrįstumas kiekvienu atveju turėtų būti vertinamas individualiai ir priklauso nuo programėlės įsirašymo, įrašo padarymo ir ikiteisminio tyrimo pradžios laiko. Vadovaujantis BPK 98 str. įtariamasis, kaltinamasis, atstovas pagal įstatymą, gynėjas, nukentėjusysis, civilinis ieškovas, civilinis atsakovas, jų atstovai, taip pat bet koks fizinis ar juridinis asmuo gali savo iniciatyva pateikti daiktus ir dokumentus, turinčius reikšmės nusikalstamai veikai tirti ir nagrinėti. BPK 98 str. skatinamas proceso dalyvių aktyvumas aiškinantis tiesą baudžiamajame procese ir šiame straipsnyje nėra numatyta, kad daiktų ir dokumentų data turi būti ankstesnė nei ikiteisminio tyrimo pradžios. Pokalbių įrašymo programėlės yra skirtos naudoti fizinių asmenų poreikių tenkinimui, todėl jų naudojimui nėra taikomi BDAR įtvirtinti teisėto asmens duomenų rinkimo pagrindai. Taigi nėra privaloma informuoti kitą asmenį apie tai, kad jo pokalbis yra įrašomas. Jeigu pokalbių programėlė yra naudojama iki pradedant ikiteisminį tyrimą, o ikiteisminio tyrimo metu įrašai, vadovaujantis BPK 98 str., yra pateikiami ikiteisminio tyrimo pareigūnui, jų teisėtumas neturėtų būti kvestionuojamas. Tačiau tokios programėlės tikslinis įsirašymas ir naudojimas pradėjus ikiteisminį siekiant įrašus pateikti ikiteisminio tyrimo institucijai nėra asmens duomenų tvarkymas fizinio asmens poreikių tenkinimo tikslais. Ikiteisminį tyrimą atlieka ikiteisminio tyrimo pareigūnai (BPK 164 str.), ne baudžiamojo proceso dalyviai ar kiti asmenys, todėl fiziniai asmenys neturi teisės vykdyti ikiteisminio tyrimo pareigūno funkcijų, iš neteisės negali atsirasti teisė[939]. Kaip jau minėta anksčiau disertacijoje ir yra įtvirtinta teismų praktikoje, teisė į asmens duomenų apsaugą gali būti suvaržyta slaptais asmens duomenų rinkimo veiksmais, tačiau suvaržymas yra teisėtas tik tada, kai atitinka EŽTK įtvirtintus teisėto suvaržymo principus, o sprendimą dėl to ar teisės į asmens duomenų apsaugą suvaržymas atitinka teisėtam suvaržymui keliamus reikalavimus ikiteisminio tyrimo metu turi priimti nešališkas arbitras – teismas[940]. Lietuvos Aukščiausiojo Teismo praktikoje

[939] „Klaipėdos apylinkės teismo Klaipėdos miesto rūmų 2020 m. vasario 19 d. nutarimas Nr. II-40-890/2020“, *Infolex praktika*, žiūrėta 2020 m. rugpjūčio 29 d., http://www.infolex.lt.skaitykla.mruni.eu/tp/1862389.

[940] „Europos Žmogaus Teisių Teismo 2015 m. gruodžio 4 d. sprendimas byloje Roman Zakharov prieš Rusiją (Nr. 47143/06)“, *Hudoc*, žiūrėta 2020 m. rugsėjo 9 d., https://hudoc.echr.coe.int/fre#{%22itemid%22:[%22001-159324%22]}. „Europos Žmogaus Teisių Teismo 2015 m. balandžio 15 d. sprendimas byloje Dragojević prieš Kroatiją (Nr. 68955/11)“, *Hudoc*, žiūrėta 2020 m. rugsėjo 9 d., https://hudoc.echr.coe.int/fre#{%22itemid%22:[%22001-150298%22]}.

yra akcentuojama, kad teismas – svarbi garantija nuo savivalės renkant duomenis elektroninėje erdvėje[941]. Todėl baudžiamojo proceso dalyvių savavališkas pokalbių įrašymo programėlės naudojimas ikiteisminio tyrimo tikslais negali būti laikomas teisėtu, o surinkti duomenys negali būti laikomi atitinkančiais įrodymų teisėtumo reikalavimus.

Tokios programėlės yra skirtos naudoti fiziniams asmenims jų asmeninių poreikių tenkinimui. Tokio pobūdžio asmens duomenų rinkimui nėra taikomas Bendrasis asmens duomenų apsaugos reglamentas. Kadangi asmens duomenis galima naudoti tik tais tikslais, kuriais jie yra surinkti.

Dar vienas klausimas, kylantis iš BPK 154 str. 6 d. formuluotės – kokius asmens duomenis ikiteisminio tyrimo pareigūnai gali rinkti. Siekiant nustatyti kokia apimti galima rinkti asmens duomenis esant asmens sutikimui reikia išsiaiškinti: 1) tų duomenų pobūdį; 2) komunikacijos šaltinį t. y. ar galima rinkti įeinančią ar tik išeinančią komunikaciją. BPK 154 str. 6 d. duomenys, kuriuos galima rinti asmens sutikimo pagrindu, yra įvardijami kaip elektroninių ryšių tinklais perduodami pokalbiai ir kita informacija. Vadinasi, asmens sutikimo pagrindu gali būti renkamas bent kokio pobūdžio komunikacijos el. erdvėje turinys. Tačiau to turinio šaltinis ikiteisminio tyrimo pareigūnams turėtų būti svarbus, kadangi BPK 154 str. 6 d. yra minima tik „šių asmenų < ... > perduodamos informacijos“ kontrolė. Yra du variantai kaip aiškinti pastarąją nuostatą:

1) kad galima rinkti tik išeinančią komunikaciją, t. y. tik tokį turinį, kurį siunčia sutikimą davęs asmuo, tačiau to asmens gaunamos komunikacijos turinio rinkimas yra negalimas;
2) kad galima rinkti ir išeinančią ir įeinančią komunikaciją, t. y. ir gaunamą ir siunčiamą, tačiau tik apie tuos asmenis, kurie turi procesinį statusą.

Kurį iš variantų omenyje turėjo įstatymo leidėjas nėra aišku, tačiau argumentų galima rasti tiek vieno, tiek kito varianto taikymui ar netaikymui. Sutikimas, kaip vienas iš teisėto asmens duomenų rinkimo pagrindų, yra naudojamas seniai. Jis taip pat yra įtvirtintas ir Bendrajame asmens duomenų apsaugos reglamente[942]. Tačiau vadovaujantis Reglamentu asmens duomenų subjektas gali duoti tik duomenų rinkimui apie patį save[943] arba nepilnametį asmenį[944]. Kadangi asmens duomenų rinkimas pagal Reglamentą yra galimas tik apie tą sutikimą davusį asmenį ir kadangi BPK 154 str. 6 d. kalba tik apie tų asmenų perduodamos, tačiau nekalba apie gaunamos informacijos kontrolę, todėl galima laikyti, jog BPK 154 str. 6 d. pagrindu galima rinkti tik sutikimą davusio proceso dalyvio išeinančią turininio pobūdžio informaciją. Iš kitos pusės BPK

---

941 „Lietuvos Aukščiausiojo Teismo 2019 m. gegužės 22 d. nutartis baudžiamojoje byloje Nr. 2K-90-303/2019“, *Infolex praktika*, žiūrėta 2020 m. rugpjūčio 29 d., http://www.infolex.lt.skaitykla.mruni.eu/tp/1727225#B_0.

942 „Bendrasis asmens duomenų apsaugos reglamentas“, *EUR-Lex*, 6 str. 1 p. a) d., žiūrėta 2020 m. rugsėjo 1 d., https://eur-lex.europa.eu/legal-content/LT/TXT/?uri=CELEX%3A32016R0679 .

943 Duomenų subjekto sutikimas – bet koks laisva valia duotas, konkretus ir nedviprasmiškas tinkamai informuoto duomenų subjekto valios išreiškimas pareiškimu arba vienareikšmiais veiksmais kuriais jis sutinka, kad būtų tvarkomi su juo susiję asmens duomenys;

944 „Bendrasis asmens duomenų apsaugos reglamentas“, *EUR-Lex*, 8 str., žiūrėta 2020 m. rugsėjo 1 d., https://eur-lex.europa.eu/legal-content/LT/TXT/?uri=CELEX%3A32016R0679 .

154 str. nėra vartojama elektroninių ryšių tinklais perduodamos informacijos sąvoka, pareigūnams rinkti tik sutikimą davusio asmens perduodamą informaciją, nerenkant gaunamos, nėra tikslinga. Struktūruoto interviu duomenys rodo, jog ir ikiteisminio tyrimo pareigūnams šios nuostatos taikymo praktika ikiteisminio tyrimo įstaigose skiriasi. 6 respondentai teigė, kad vadovaujantis BPK 154 str. 6 d. yra renkama informacija ne tik apie sutikimą davusį asmenį, bet ir apie visus kitus asmenis. 8 respondentai nurodė, kad yra renkama informacija tik apie sutikimą davusį asmenį.

BDAR taip pat yra įtvirtinti ir griežti reikalavimai sutikimo teisėtumui[945]. BPK, kaip matome, tokie reikalavimai nėra įtvirtinti. Teisėsaugos tikslais tvarkomų asmens duomenų apsaugos direktyvoje sutikimas nėra išskirtas teisėtu asmens duomenų rinkimo pagrindu, o kitose ES valstybėse nėra taikomas. Visgi, Lietuva nėra vienintelė valstybė, kurioje sutikimas gali būti asmens duomenų rinkimo el. erdvėje pagrindu. Tokia galimybė yra numatyta ir Kanadoje[946], JAV[947] bei seniau buvo numatyta Naujosios Zelandijos teisės aktuose[948]. Tačiau Naujojoje Zelandijoje, vienintelėje iš išvardintų valstybių, asmens duomenų rinkimo el. erdvėje procesas esant proceso dalyvio leidimui buvo panašus į BPK: praktiškai nereglamentuotos procedūros, nenumatytas vėlesnis sankcionavimas[949]. Kanados Baudžiamojo proceso kodekse nors ir numatyta galimybė asmens duomenų el. erdvėje rinkti esant proceso dalyvio sutikimui, tačiau yra numatytos ne tik asmens duomenų rinkimo el. erdvėje esant proceso dalyvio sutikimui procedūros bet ir privalomas teisėjo sankcionavimas[950]. Asmens sutikimas laikomas vienu iš Ketvirtosios JAV Konstitucijos pataisos, teigiančios kad krata ir poėmis gali būti atlikta tik esant teismo sankcionavimui, išimčių asmens duomenis renkant el. erdvėje[951]. JAV laikomasi pozicijos, kad sutikimą asmuo gali duoti tik dėl savo paties asmens duomenų rinkimo el. erdvėje. Nors sutikimas gali būti duotas bent kokia forma, tačiau JAV Elektroninių asmens duomenų rinkimo vadovas rekomenduoja teisėsaugos institucijoms prieš renkant duomenis gauti rašytinės formos sutikimą[952], kadangi teisėsaugos institucijos privalo

---

945 „Bendrasis asmens duomenų apsaugos reglamentas“, *EUR-Lex*, 7 str., žiūrėta 2020 m. rugsėjo 1 d., https://eur-lex.europa.eu/legal-content/LT/TXT/?uri=CELEX%3A32016R0679 .

946 Kanados baudžiamojo proceso kodekso 184(2) str., „Consolidated Federal Laws of Canada, Criminal Code“, *Legislative Services Branch*, 2020, žiūrėta 2020 m. rugpjūčio 17., https://laws-lois.justice.gc.ca/eng/acts/C-46/page-41.html#h-6.

947 „Section 2511(2)(c) of Title 18 „9-7.000 – Electronic Surveillance“, 2015, žiūrėta 2020 m. rugpjūčio 17 d., https://www.justice.gov/jm/jm-9-7000-electronic-surveillance.

948 „*Review of the Search and Surveillance Act 2012 =: Ko Te Arotake i Te Search and Surveillance Act 2012*, Unredacted version, Report 141 (Wellington, New Zealand: Law Commission, Te Aka Matua o te Ture : Ministry of Justice, Tāhū o te Ture, 2017), 58, žiūrėta 2020 m. rugpjūčio 17 d., https://www.lawcom.govt.nz/sites/default/files/projectAvailableFormats/NZLC-R141-Review-of-the-Search-and-Surveillance-Act-2012-final_0.pdf.

949 „Current Practices in Electronic Surveillance in the Investigation of Serious and Organized Crime“, *United Nations*, 2009, 16, žiūrėta 2020 m. rugpjūčio 17 d., https://www.unodc.org/documents/organized-crime/Law-Enforcement/Electronic_surveillance.pdf.

950 „Consolidated Federal Laws of Canada, Criminal Code“, *Legislative Services Branch*, 2020, žiūrėta 2020 m. rugpjūčio 17., https://laws-lois.justice.gc.ca/eng/acts/C-46/page-41.html#h-6.

951 „U.S. DOJ Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations“, *supra note*, 290: 15.

952 „U.S. DOJ Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations“, *supra note*, 290: 15.

įrodyti ne tik, kad gavo sutikimą, bet ir kad sutikimą gavo laisva valia bei to sutikimo apimtis[953, 954].

Taigi, nors Lietuva nėra vienintelė valstybė, kurioje asmens sutikimu, gali būti renkami asmens duomenys elektroninėje erdvėje, tačiau toks reglamentavimas, koks yra įtvirtintas BPK 154 str. 6 d. yra ydingas, todėl galimai pažeidžiantis teisę į asmens duomenų apsaugą. Todėl reikėtų arba atsisakyti baudžiamojo proceso dalyvio sutikimo/leidimo kaip elektroninių asmens duomenų rinkimo pagrindo, arba numatyti privalomą vėlesnį sankcionavimą ir tokio leidimo/sutikimo turinį bei jo gavimo procedūras. Nesant sankcionavimo procedūros asmens duomenų rinkimas elektroninėje erdvėje esant proceso dalyvio sutikimui tampa aukštesnės galios už prokuroro sankcionavimą, kadangi pastarąjį privalo patvirtinti ikiteisminio tyrimo teisėjas.

1.4. Elektroninių ryšių tinklais realiuoju laiku perduodamos informacijos kontrolės faktiniai pagrindai. BPK 154 straipsnyje įtvirtinta procesinės prievartos priemonė būti taikoma tik tada, jeigu:

1) yra pagrindas manyti, kad tokiu būdu galima gauti duomenų apie BPK 154 str. 1 d. nurodytus nusikaltimus ar šio straipsnio 3 d. nurodytus nesunkius nusikaltimus (esant šio straipsnio 3 d. nurodytoms sąlygoms), arba ar yra pavojus, kad nukentėjusiajam, liudytojui ar kitiems proceso dalyviams arba jų artimiesiems bus panaudotas smurtas, prievartavimas ar kitokios neteisėtos veikos; ir
2) nėra galimybės kitais būdais nustatyti faktus, ar šių faktų nustatymas kitais būdais būtų žymiai sudėtingesnis (BPK 11 str. 1 d.)[955].

Nors ES ir ET teisės aktuose nėra numatyta apribojimo, jog tik tam tikrų nusikalstamų veikų atžvilgiu baudžiamojo proceso metu galima asmens duomenis rinkti elektroninėje erdvėje, Lietuvos BPK tokį apribojimą nustato. Šis apribojimas gali sukelti painiavos, nes ikiteisminio tyrimo ar teisminio nagrinėjimo metu veikos gali būti perkvalifikuojamos į tas, kurios nėra numatytos BPK 154 str. LAT nuomone tai, kad nusikalstama veika, dėl kurios buvo sankcionuota elektroninių ryšių tinklais perduodamos informacijos kontrolė, vėliau (ikiteisminio tyrimo ar bylos nagrinėjimo metu) buvo perkvalifikuota pagal kitą BK normą, taip pat ir tokią, dėl kurios negalėjo būti atliekami BPK 154 straipsnyje įtvirtinti procesinės prievartos veiksmai, savaime nepaneigia šių duomenų reikšmės ir jų naudojimo baudžiamajame procese galimybių (leistinumo)[956]. Kasacinio teismo praktikoje yra konstatuota, kad nusikalstamos vei-

---

953 „U.S. DOJ Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations“, s*upra note,* 290: 16.

954 Įdomu yra tai, kad be asmens sutikimo, yra dar viena išimtis iš Ketvirtosios JAV Konstitucijos pataisos, kuomet nesankcionuotai galima rinkti duomenis – tai ypatingos aplinkybės: 1) įrodymams gresia sunaikinimas; 2) teisėsaugos pareigūnas arba visuomenė gali atsidurti pavojuje; 3) teisėsaugos institucijos seka „karštais įtariamojo pėdsakais“; 4) yra pagrindas manyti, kad įtariamasis pabėgs per tą laiką, kol teismas sankcionuos domenų rinkimą.

955 „Lietuvos Aukščiausiojo Teismo Elektroninių ryšių tinklais perduodamos informacijos kontrolės, jos fiksavimo ir kaupimo (Baudžiamojo proceso kodekso 154 straipsnis, Kriminalinės žvalgybos įstatymo 10 straipsnis) taikymo apžvalga“, *Lietuvos Aukščiausiasis Teismas*, žiūrėta 2020 m. rugpjūčio 17 d., https://www.lat.lt/lat-praktika/teismu-praktikos-apzvalgos/baudziamuju-bylu-apzvalgos/68.

956 „Lietuvos Aukščiausiojo Teismo Elektroninių ryšių tinklais perduodamos informacijos kontrolės, jos fiksavimo ir kaupimo (Baudžiamojo proceso kodekso 154 straipsnis, Kriminalinės žvalgybos įstatymo 10 straipsnis) taikymo apžvalga“, 8, *Lietuvos Aukščiausiasis Teismas*, žiūrėta 2020 m. rugpjūčio 17 d., https://www.lat.lt/lat-praktika/teismu-praktikos-apzvalgos/baudziamuju-bylu-apzvalgos/68.

kos kvalifikavimo pakeitimas baudžiamojo proceso metu negali nulemti teisėtai gautų duomenų neleistinumo[957]. Teismų pozicija el. erdvėje surinktus įrodymus pripažinti leistinais net ir tuo atveju, jeigu proceso eigoje paaiškėjo, jog pasikeičia nusikalstamos veikos kvalifikacija, ir pagal naują veikos kvalifikaciją asmens duomenų rinkimas buvo negalimas, yra diskutuotinos. 7 iš 22 struktūruoto interviu metu apklaustų ikiteisminio tyrimo pareigūnų nurodė, jog jie turi poreikį taikyti elektroninių ryšių tinklais perduodamos informacijos kontrolę ir kitais nei BPK 154 str. nurodytais atvejais. Nors EŽTT yra nurodęs vienintelį skirtumą tarp nusikalstamų veikų kuomet jų ištyrimui asmens teisės gali būti labiau varžomos nei kitų nusikalstamos veikų atžvilgių – tai pavojų nacionaliniam saugumui keliančios nusikalstamos veikos[958], tačiau teismų polinkis sankcionuoti beveik visus prokurorų prašymus dėl BPK 154 str. reikštų dar didesnius asmens duomenų rinkimo elektroninėje erdvėje mastus.

JAV asmens duomenų rinkimas elektroninėje erdvėje teisėsaugos tikslais nėra apribojamas konkrečių nusikaltimų sąrašu. Prisijungimai prie elektroninės erdvės įrenginių (angl. *Government hacking*) yra laikomi labiausiai teisę į asmens duomenų apsaugą suvaržančiomis procesinėmis prievartos priemonėmis (plačiau apie tai 4.1.3. disertacijos poskyryje). Tačiau, pavyzdžiui, Olandijoje net ir šios labiausiai teisę į asmens duomenų apsaugą suvaržančios priemonės taikymas nėra apribojamas konkrečių nusikalstamų veikų sąrašu. Vienintelis Olandijos baudžiamojo proceso kodekse numatytas apribojimas dėl prisijungimo prie elektroninės erdvės įrenginių yra, kad maksimali galima skirti bausmė už inkriminuojamą nusikaltimą būtų ne mažesnė nei 3 metų laisvės atėmimas. Lietuvoje tokie nusikaltimai yra laikomi nesunkiais. Manytina, kad teisę į asmens duomenų apsaugos užtikrinimui ne mažiau svarbus yra reikalavimas šią procesinės prievartos priemonę taikyti BPK 11 str. 1 d. įtvirtintą proporcingumo principą. BPK 11 str. 1 d. įtvirtintas reikalavimas asmens duomenų rinkimą el. erdvėje baudžiamajame procese taikyti tik tuo atveju, kai nėra galimybės kitais būdais nustatyti faktų arba tų faktų nustatymas būtų žymiai sudėtingesnis – būtent ir yra asmens teisės į asmens duomenų apsaugą garantas, kad asmens duomenų rinkimu el. erdvėje teisėsaugos institucijos nepiktnaudžiautų. LAT apžvalgoje yra nurodyta, kad teismai paprastai tikrina ar el. erdvėje surinktų duomenų nebuvo galima surinkti kitais būdais[959]. Visgi

---

[957] Pvz., Lietuvos Aukščiausiojo Teismo 2010 m. lapkričio 23 d. nutartis baudžiamojoje byloje Nr. 2K-504/2010, *eTeismai*, žiūrėta 2020 m. rugpjūčio 17 d., https://eteismai.lt/byla/235520032106674/2K-504/2010, Lietuvos Aukščiausiojo Teismo 2013 m. gegužės 21 d. nutartis baudžiamojoje byloje Nr. 2K-246/2013, *eTeismai*, žiūrėta 2020 m. rugpjūčio 17 d., https://eteismai.lt/byla/1343836724729 03/2K-246/2013, Lietuvos Aukščiausiojo Teismo 2014 m. balandžio 14 d. nutartis baudžiamojoje byloje Nr. 2K-194/2014, *eTeismai*, žiūrėta 2020 m. rugpjūčio 17 d., https://eteismai.lt/byla/9356367523030/2K-194/2014, Lietuvos Aukščiausiojo Teismo 2015 m. kovo 31 d. nutartis baudžiamojoje byloje Nr. 2K-168-139/2015, *eTeismai*, žiūrėta 2020 m. rugpjūčio 17 d., https://eteismai.lt/byla/141589214790674/2K-168-139/2015, Lietuvos Aukščiausiojo Teismo Baudžiamųjų bylų skyriaus plenarinės sesijos 2015 m. birželio 1 d. nutartis baudžiamojoje byloje 2K-P-94-895/2015, *eTeismai*, žiūrėta 2020 m. rugpjūčio 17 d., https://eteismai.lt/byla/44415389271611/2K-P-94-895/2015.

[958] „Europos Žmogaus Teisių Teismo 1987 m. kovo 26 d. sprendimas byloje Leander prieš Švediją (Nr. 9248/81)“, *Hudoc*, žiūrėta 2020 m. rugsėjo 7 d., https://hudoc.echr.coe.int/rus#{%22itemid%22:[%22001-57519%22]}.

[959] „Lietuvos Aukščiausiojo Teismo Elektroninių ryšių tinklais perduodamos informacijos kontrolės, jos fiksavimo ir kaupimo (Baudžiamojo proceso kodekso 154 straipsnis, Kriminalinės žvalgybos įstatymo 10 straipsnis) taikymo apžvalga“, 18, *Lietuvos Aukščiausiasis Teismas*, žiūrėta 2020 m. rugpjūčio 17 d., https://www.lat.lt/lat-praktika/teismu-praktikos-apzvalgos/baudziamuju-bylu-apzvalgos/68.

ne visi ikiteisminio tyrimo pareigūnai patvirtino, jog prieš taikydami BPK 154 str. vadovaujasi BPK 11 str. 1 d.[960]. Struktūruoto interviu metu 7 iš 22 ikiteisminio tyrimo pareigūnų nurodė, kad prieš taikydami BPK 154 str. įtvirtintą procesinės prievartos priemonę, jie neįsitikina ar nėra galimybės kitais būdais nustatyti faktų arba tų faktų nustatymas būtų žymiai sudėtingesnis. Kita vertus, tuo atveju, kai asmens duomenys yra renkami neatidėliotinais atvejais, tuomet atlikti papildomų procesinių veiksmų gali nebūti laiko arba nors ir gali būti galima tuos pačius duomenis surinkti ir kitais būdais, tačiau kitų būdų naudojimas apsunkintų tyrimą. BPK 11 str. 1 d. taip pat galioja ir duomenims, renkamiems asmens sutikimo pagrindu, tačiau kadangi tokiu atveju vadovaujantis BPK nei prokuroro, nei ikiteisminio tyrimo teisėjo sankcionavimas nėra reikalingas, todėl nėra ir subjekto, kuris įvertintų ar tikrai tie duomenys negalėjo būti surinkti kitais būdais.

2. Istorinio pobūdžio asmens duomenų rinkimas ikiteisminio tyrimo metu.

Generalinio prokuroro rekomendacijose slaptais ikiteisminio tyrimo veiksmais yra laikoma elektroninių ryšių tinklais perduodamos informacijos kontrolė, jos kaupimas ir fiksavimas, numatytas BPK 154 str., savo tapatybės neatskleidžiančių ikiteisminio tyrimo pareigūnų veiksmai, numatyti BPK 158 str., nusikalstamą veiką imituojantys veiksmai, numatyti BPK 159 str. ir slaptas sekimas, numatytas BPK 159 str.[961] BPK 154 str. reglamentuoja elektroninių ryšių tinklais perduodamų asmens duomenų rinkimą esamuoju laiku. Tyrimo rezultatai rodo, kad istorinio pobūdžio asmens duomenys ikiteisminio tyrimo metu yra renkami vadovaujantis keliais BPK straipsniais atsižvelgiant į subjektą, kuris tuos duomenis pateikia:

1) jeigu asmens duomenis pateikia paslaugas el. erdvėje teikiantys arba kiti juridiniai asmenys, tuomet vadovaujamasi BPK 97 str. „Daiktų ir dokumentų, turinčių reikšmės nusikalstamai veikai tirti ir nagrinėti, išreikalavimas“ arba BPK 155 str. „Prokuroro teisė susipažinti su informacija“.
2) jeigu asmens duomenys yra renkami paimant fiziniam ar juridiniam asmeniui priklausantį įrenginį – tuomet vadovaujamasi BPK 97 str. „Daiktų ir dokumentų, turinčių reikšmės nusikalstamai veikai tirti ir nagrinėti, išreikalavimas“, BPK 145 str. „Krata“, 147 sr. „Poėmis“ ir BPK 207 str. „Apžiūra“.
3) jeigu asmenys asmens duomenis pateikia savo iniciatyva, tuomet vadovaujamasi BPK 98 str.

Generalinio prokuroro rekomendacijose istorinio pobūdžio asmens duomenų rinkimas vadovaujantis BPK 97, 144, 147, 155 ir 207 str. nėra laikomas slaptais tyrimo veiksmais. Telekomunikacijų įmonės, vadovaujantis Elektroninių ryšių reguliavimo įstatymo 66 str., asmens metaduomenis privalo saugoti 6 mėnesius, kiti paslaugų

[960] Struktūruoto interviu duomenimis 31% neįsitikina.

[961] „Rekomendacijos dėl Kriminalinės žvalgybos įstatymo, Baudžiamojo proceso kodekso normų taikymo ir kriminalinės žvalgybos informacijos panaudojimo baudžiamajame procese, patvirtintos Lietuvos Respublikos generalinio prokuroro 2012 m. gruodžio 31 d. įsakymu Nr. I-383“, 2 p., *eSeimas*, žiūrėta 2020 m. rugpjūčio 17 d., https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/TAIS.440985?jfwid=-9dzqnu8af.

elektroninėje erdvėje tiekėjai tiek komunikacijos turinį, tiek metaduomenis gali saugoti neterminuotai[962]. Kita vertus, laidinio ir mobiliojo telefono ryšio naudojimo apimtys nuolat mažėja jas pakeičiant OTT paslaugas teikiančiais paslaugų teikėjais (žr. 7 paveikslą), o esant technologinėms galimybėmis paslaugų gavėjams neatlygintinai saugoti elektroninėje erdvėje asmens duomenis, didžioji dauguma asmens duomenų elektroninėje erdvėje yra istorinio pobūdžio[963] ir elektroninėje erdvėje yra saugomi neterminuotai[964]. Todėl atsižvelgiant į šiandieninį paslaugų elektroninėje erdvėje naudojimo pobūdį slaptais tyrimo veiksmais turėtų būti laikoma ne tik asmens duomenų rinkimas realiuoju laiku, vadovaujantis BPK 154 str., bet ir istorinio pobūdžio asmens duomenų rinkimas.

2.1. Renkamų asmens duomenų apimtys. BPK 97 str. „Daiktų ir dokumentų, turinčių reikšmės nusikalstamai veikai tirti ir nagrinėti, išreikalavimas“ yra įtvirtinta ikiteisminio tyrimo pareigūno, prokuroro ir teismo teisė reikalauti iš fizinių ir juridinių asmenų pateikti daiktus ir dokumentus, turinčius reikšmės nusikalstamai veikai tirti ir nagrinėti. Vadovaujantis BPK 95 str. dokumentais, turinčiais reikšmės nusikalstamai veikai tirti ir nagrinėti, yra laikomi objektai, kuriuose įmonė, įstaiga, organizacija, pareigūnas ar fizinis asmuo tam tikrais ženklais užfiksuoja informaciją, galinčią padėti atskleisti nusikalstamą veiką ir nustatyti su šia veika susijusias aplinkybes. BPK 95 str. pateikto dokumentų, turinčių reikšmės nusikalstamai veikai tirti ir nagrinėti, apibrėžimo lingvistinė analizė rodo, kad dokumentas nebūtinai turi egzistuoti prašymo pateikimo metu, jis gali būti parengtas jau gavus BPK 97 str. numatytą ikiteisminio tyrimo pareigūno, prokuroro arba teismo prašymą.

Istorinio pobūdžio asmens duomenys iš juridinių asmenų gali būti renkami ir vadovaujantis BPK 155 str. Skirtingai nuo BPK 97 str. duomenų rinkimas vadovaujantis BPK 155 str. tik prokuroras gali kreiptis į paslaugų el. erdvėje teikėjus su prašymu pateikti asmens duomenis. Vadovaujantis BPK 155 str. asmens duomenis galima rinkti ne vien tik iš elektroninių ryšių paslaugų teikėjų apie jų paslaugų vartotojus, bet ir iš kitų juridinių asmenų apie jų darbuotojus, pvz., darbuotojų el. laiškus ar kitokius susirašinėjimus.

BPK 97 ir 155 str. renkamų asmens duomenų apimtys nėra apibrėžtos, todėl jie galimai ne tik istorinio pobūdžio metaduomenis, bet ir istorinio pobūdžio komunikacijos turinį. Istorinio pobūdžio komunikacijos el. erdvėje turinio pavyzdžiais yra ne tik adresato gauti el. laiškai, WhatsApp, Viber ir kt. per OTT paslaugų teikėjus gautos žinutės, bet ir elektroninių ryšių tinklais į mobiliuosius telefonus perduotos SMS žinutės. Skirtingai nuo populiariųjų OTT paslaugų (WhatsApp, Gmail, Viber ir kt.), SMS žinučių turinys nėra užkoduotas (išskyrus Apple iMessage funkciją)[965] ir siuntimo

---

962 Ali E. Abbas, *Next-Generation Ethics: Engineering a Better Society* (Cambridge University Press, 2019), 451.

963 „How Much Data Is There In the World?“, *Bernard Marr*, žiūrėta 2020 m. rugsėjo 9 d., https://www.bernardmarr.com/default.asp?contentID=1846.

964 „Tech Firms Can't Keep Our Data Forever: We Need a Digital Expiry Date“, *The Guardian*, 2018, žiūrėta 2020 m. rugsėjo 9 d., http://www.theguardian.com/commentisfree/2018/may/19/online-privacy-digital-expiry-date. Rob Crossley, „Where in the World Is My Data and How Secure Is It?“, *BBC News*, 2016, žiūrėta 2020 m. rugsėjo 9 d., https://www.bbc.com/news/business-36854292.

965 Patrick Stump, „Are Text Messages Encrypted?“, *Rokacom*, 2018, žiūrėta 2020 m. rugpjūčio 17 d., https://www.rokacom.com/are-text-messages-encrypted/.

metu išsaugomas siunčiamų žinučių centre[966], todėl elektroninių ryšių paslaugų teikėjai turi galimybę teisėsaugos institucijoms pateikti ir žinučių turinį[967]. Elektroninių ryšių įstatymo 65 str. yra numatyta, kad viešųjų ryšių tinklų ir (ar) viešųjų elektroninių ryšių paslaugų teikėjai gali generuoti, kaupti ir tvarkyti tik tuos abonentų ir registruotų elektroninių ryšių paslaugų naudotojų asmens, srauto ir susijusius duomenis, kurie yra būtini abonentams ir paslaugų naudotojams identifikuoti, paslaugoms teikti, apskaitai ir atsiskaitymams. Elektroninių ryšių įstatymo 66 str. 4 d. yra numatyta, kad srauto duomenys yra saugomi 6 mėnesius, o duomenys, reikalingi nustatyti geografinei tinklo įrangos vietai, atitinkančiai vietovės žymų zoną (LAI), kaip tai apibrėžta telekomunikacijų standartuose, yra saugomi 2 mėnesius. SMS žinučių saugojimo terminų įstatymas nereglamentuoja. Pavyzdžiui, JAV pagrindinės telekomunikacijų įmonės SMS žinučių turinį saugo nuo 3 (Verizon) iki 90 (Virgin Mobile) dienų[968]. TELIA privatumo politikoje yra nurodoma, kad komunikacijos turinio duomenys yra tvarkomi tik siekiant perduoti komunikaciją elektroninių ryšių tinklu[969], tačiau nėra nurodyta, kiek laiko yra saugomas SMS žinutės turinys. Tele2 ir BITĖS privatumo politikose informacija apie komunikacijos turinio tvarkymą iš viso nėra pateikiama[970]. Kadangi siekiant SMS žinutę perduoti jos gavėjui jos turinys yra saugomas žinučių perdavimo centre[971] (išskyrus, jeigu žinutės yra siunčiamos tarp Apple telefonų naudojantis iMessage funkcija), todėl Lietuvos telekomunikacijų įmonės SMS žinučių turinį taip pat saugo, tačiau saugojimo trukmė nėra apibrėžta teisės aktais. Nors BPK 154 str. reglamentuoja asmens duomenų rinkimą iš elektroninių ryšių paslaugų teikėjų, tačiau šis straipsnis nereglamentuoja istorinio pobūdžio asmens duomenų rinkimo. Vadinasi, istorinio pobūdžio SMS žinučių turinio rinkimas turėtų būti vykdomas vadovaujantis BPK 155 arba 97 str. BPK 97 str. yra diskutuotinas asmens duomenų rinkimo pagrindas, kurio nerekomenduojama taikyti. Kaip jau minėta anksčiau disertacijoje ir yra įtvirtinta teismų praktikoje, teisė į asmens duomenų apsaugą gali būti suvaržyta, tačiau suvaržymas yra teisėtas tik tada, kai atitinka EŽTK įtvirtintus teisėto suvaržymo principus, o sprendimą dėl to ar teisės į asmens duomenų apsaugą suvaržymas atitinka teisėtam suvaržymui keliamus reikalavimus ikiteisminio tyrimo metu priima nešališkas arbitras – teismas[972]. Lietu-

---

966 Robert Triggs, „What is SMS and How Does it Work?“, *Android Authority*, 2013, žiūrėta 2020 m. rugpjūčio 17 d., https://www.androidauthority.com/what-is-sms-280988/.

967 Jacqueline R. Kanovitz and Michael I. Kanovitz, *Constitutional Law* (Routledge, 2010), 651.

968 Suzanne Choney, „How Long Do Wireless Carriers Keep Your Data?“, *NBC News*, žiūrėta 2020 m. rugpjūčio 17 d., http://www.nbcnews.com/technolog/how-long-do-wireless-carriers-keep-your-data-120367. „Smash It, Shred It, Wipe It: The Tom Brady Guide to Destroying Text Messages“, *The Guardian*, 2015., http://www.theguardian.com/technology/2015/jul/29/tom-brady-deflategate-destroy-text-messages-cellphone.
„Privatumas“, *Telia*, žiūrėta 2020 m. rugsėjo 9 d., https://www.telia.lt/privatumo-politika.

969 *Ibid.*

970 „Klientų duomenų tvarkymo bei privatumo politika“, *Tele2*, žiūrėta 2020 m. rugsėjo 9 d., https://tele2.lt/privatiems/apie-tele2/privatumo-politika. „Privatumo ir slapukų politika“, *Bitė Lietuva*, žiūrėta 2020 m. rugsėjo 9 d., https://www.bite.lt/privatumo-ir-slapuku-politika.

971 Triggs, *supra note*, 967.

972 „Europos Žmogaus Teisių Teismo 2015 m. gruodžio 4 d. sprendimas byloje Roman Zakharov prieš Rusiją (Nr. 47143/06)“, *Hudoc*, žiūrėta 2020 m. rugsėjo 9 d., https://hudoc.echr.coe.int/fre#{%22itemid%22:[%22001-159324%22]}. „Europos Žmogaus Teisių Teismo 2015 m. balandžio 15 d. sprendimas byloje Dragojević prieš Kroatiją (Nr. 68955/11)“, *Hudoc*, žiūrėta 2020 m. rugsėjo 9 d., https://hudoc.echr.coe.int/fre#{%22itemid%22:[%22001-150298%22]}.

vos Aukščiausiojo Teismo praktikoje yra akcentuojama, kad teismas – svarbi garantija nuo savivalės renkant duomenis elektroninėje erdvėje[973]. Vadovaujantis Lietuvos Respublikos Konstitucijos 22 str., teismo nesankcionuotas asmens duomenų rinkimas yra neteisėtas. Toliau disertacijoje yra pateikiami papildomi argumentai kodėl BPK 97 str. negali būti taikomas renkant asmens duomenis.

Skirtumas tarp BPK 97 ir 155 str. yra tas, kad BPK 97 str. yra įrodymų rinkimo būdas, o ne procesinės prievartos priemonė, todėl *„BPK 97 straipsnyje nustatyta ikiteisminio tyrimo pareigūnų (tik) teisė reikalauti iš fizinių ir juridinių asmenų pateikti daiktus, turinčius reikšmės nusikalstamai veikai tirti ir nagrinėti, ir nėra nustatyta, kokia konkreti pareiga atsiranda asmeniui, kuriam pateiktas ikiteisminio tyrimo pareigūno reikalavimas. [...] tokį reikalavimą šie asmenys gali įvykdyti tik savanoriškai ir neturi (neįgyja) pareigos perduoti daiktą. Atsisakymas įvykdyti reikalavimą savaime negali būti vertinamas kaip trukdymas ikiteisminio tyrimo pareigūnui atlikti su baudžiamosios bylos tyrimu susijusias pareigas, o kiekvienu konkrečiu atveju tai sprendžiama iš nustatytų bylos aplinkybių“*[974]. BPK 155 str. yra procesinės prievartos priemonė, todėl už prokuroro reikalavimų nevykdymą asmenys, vadovaujantis BPK 163 str., gali būti nubausti bauda (BPK 155 str. 2 p.). 4 lentelėje yra pateikiama istorinio pobūdžio asmens duomenų rinkimo el. erdvėje reglamentavimo BPK struktūra.

4 lentelė. *Istorinio pobūdžio asmens duomenų rinkimas pagal BPK.*

El. asmens duomenys	Metaduomenys							Turinys					
	Rūšis					Teisminis sankcionavimas		Pokalbiai		Kt. turinys		Teisminis sankcionavimas	
	tinklo	programos	paslaugos					Nešifruotas, arba užšifruotas kitu būdu nei ištisinis šifravimas		Užšifruotas ištisiniu šifravimu			
	Esam. l.	Esam. l.	Istorinis										
			Srauto	Vietos nustatymo	Kt.	BPK **97**	BPK **155**	Esamuoju laiku	Istorinis	Esamuoju laiku	Istorinis	BPK **97**	BPK **155**
Ūkio subjektai, teikiantys el. ryšių paslaugas	–	–	Taip	Taip	Taip	–	Taip	–	Taip	–	–	–	Taip
Kiti juridiniai asmenys	–	–	Taip	Taip	Taip	–	Taip	Taip	Taip	–	–	–	Taip

[973] „Lietuvos Aukščiausiojo Teismo 2019 m. gegužės 22 d. nutartis baudžiamojoje byloje Nr. 2K-90-303/2019“, Infolex praktika, žiūrėta 2020 m. rugpjūčio 29 d., http://www.infolex.lt.skaitykla.mruni.eu/tp/1727225#B_0

[974] Lietuvos Aukščiausiojo Teismo Baudžiamųjų bylų skyriaus 2019 m. gruodžio 30 d. nutartis baudžiamojoje byloje Nr. 2K-318-458/2019, *Infolex praktika*, žiūrėta 2020 m. birželio 15 d., https://www.infolex.lt/tp/1794194.

2.2. Istorinio pobūdžio asmens duomenų rinkimo teisiniai pagrindai. Istorinio pobūdžio asmens duomenys, apimantys komunikacijos turinį ir metaduomenis, vykdant ikiteisminį tyrimą gali būti renkami vadovaujantis BPK 97 str. ikiteisminio tyrimo pareigūno, prokuroro arba teismo reikalavimu. Klausimas ar teisminis sankcionavimas yra privalomas apribojant EŽTK 8 str. ir Europos žmogaus teisių chartijos 7 str. įtvirtintą teisę į asmens duomenų apsaugą yra iki šiol neatsakytas EŽTT ir ESTT praktikoje. G. Malgieri ir P. De Hert teigia, kad nei EŽTT, nei ESTT teisės į asmens duomenų apsaugą apribojimų nesieja su privalomu teisminiu sankcionavimu, nors sankcionavimo procedūra turėtų būti privaloma. Tačiau sankcionavimas gali būti ir qvazi teisminis arba neteisminis[975]. Visgi, ET ir ES valstybėse narėse gali būti įtvirtinti griežtesni apsaugos standartai. To pavyzdžiu gali būti Lietuvos Respublikos Konstitucijos 22 str. nuostata, kurioje yra įtvirtinta, kad teisė į privatumą gali būti apribota tik teismo sprendimu, todėl teisės akto nuostata leidžianti nesankcionuotai rinkti asmens duomenis turėtų būti laikoma pažeidžiančia Konstitucijos 22 str. Teismų praktikos analizė ir interviu duomenys rodo, kad vadovaujantis BPK 97 str. dažniausiai yra renkama informacija apie juridinius asmenis, pvz. buhalterinės apskaitos[976], juridinio asmens veiklos dokumentai[977]. Tačiau teismų praktikoje galima rasti pavyzdžių, kuomet asmens duomenys taip pat buvo renkami vadovaujantis BPK 97 str. Pvz., *„BPK 97 straipsnio nustatyta tvarka pateikta AB banko „Hansabankas" kompaktinė plokštelė su vaizdo įrašu, kur užfiksuotas D. P., gryninantis pinigus bankomatuose"*[978]. Asmens atvaizdas vaizdo įraše yra asmens duomenys[979]. *„Iš 2017-04-18 LR BPK 97 str. nustatyta tvarka VĮ „Regitra" Kauno filiale paimtuose dokumentuose, yra nurodyta, kad 2016-05-26 Transporto priemonės pirkimo-pardavimo sutarties pagrindu Ž. M., a.k. (duomenys neskelbtini) automobilį „BMW X", valstybinis numeris (duomenys neskelbtini) kėbulo numeris (duomenys neskelbtini), nusipirko iš S. Š., a.k. (duomenys neskelbtini) ir tą pačią 2016-05-26 pateikus prašymą dėl nurodytos transporto priemonės registracijos, pasikeitus jos valdytojui/savininkui, buvo išduotas transporto priemonės valstybinio numerio ženklas (duomenys neskelbtini) bei registravimo dokumentas (duomenys neskelbtini). Transporto priemonės pirkimo – pardavimo sutartyje nurodyta automobilio kaina – 11 000 Eur."*[980] Pirkimo-pardavimo sutarties informacija yra asmens duomenys, automobilio registracijos numeris yra asmens duomenys[981]. Vadovaujantis sistemine teisės aktų, teismų prak-

---

[975] Gianclaudio Malgieri ir Paul Hert, „European Human Rights, Criminal Surveillance, and Intelligence Surveillance: Towards 'Good Enough' Oversight, Preferably but Not Necessarily by Judges", in *The Cambridge Handbook of Surveillance Law*, 2017, 509–32, doi:10.1017/9781316481127.023.

[976] Žr. pvz., „Lietuvos Aukščiausiojo Teismo 2020 m. sausio 7 d. nutartis byloje Nr. 2K-52-942/2020", *Infolex praktika*, žiūrėta 2020 m. rugsėjo 10 d., http://www.infolex.lt.skaitykla.mruni.eu/tp/1819187.

[977] Lietuvos apeliacinio teismo 2019 m. balandžio 15 d. nuosprendis byloje Nr. 1A-1-449/2019", *Infolex Praktika*, žiūrėta 2020 m. rugsėjo 10 d., http://www.infolex.lt.skaitykla.mruni.eu/tp/1717089.

[978] Lietuvos apeliacinio teismo 2019 m. balandžio 15 d. nuosprendis baudžiamojoje byloje Nr. 1A-1-449/2019, *Infolex praktika*, žiūrėta 2020 m. rugpjūčio 22 d., https://www.infolex.lt/tp/1717089 .

[979] „Opinion 4/2007 on the concept of personal data", *Article 29 Working Party,* žiūrėta 2020 m. rugsėjo 1 d., https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_en.pdf

[980] Kauno apygardos teismo Baudžiamųjų bylų skyriaus 2018 m. gegužės 28 d. nuosprendis baudžiamojoje byloje Nr. 1-177-317/2018, *Infolex praktika*, žiūrėta 2020 m. birželio 15 d., https://www.infolex.lt/tp/1667265 .

[981] „Article 29 Working Party Opinion 4/2007 on the concept of personal data", *European Commission*, žiūrėta 2020 m. rugpjūčio 22 d., https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_en.pdf.

tikos ir mokslinės literatūros analize, darytina išvada, kad asmens duomenys neturėtų būti renkami vadovaujantis BPK 97 str., todėl vieninteliu istorinio pobūdžio asmens duomenų rinkimo pagrindu elektroninių ryšių paslaugų teikėjų ir kitų juridinių asmenų, įskaitant OTT teikėjus, galėtų būti BPK 155 str., tačiau ir šiame straipsnyje įtvirtinta teisminio sankcionavimo procedūra yra tobulintina.

BPK 154 str. yra numatyta, kad asmens duomenų rinkimas realiuoju laiku yra galimas tik ikiteisminio tyrimo teisėjui šiuo klausimu priėmus nutartį. Konkretūs reikalavimai ikiteisminio tyrimo teisėjo nutarties turiniui yra numatyti BPK 154 str. 2 d. Nutartyje privalo būti nurodomi turimi duomenys apie asmenį, prieš kurį veiksmai turi būti atlikti, duomenys, kuriais pagrindžiama būtinybė atlikti BPK 154 str. 1 d. numatytus veiksmus, konkretūs BPK 154 str. 1 d. numatyti veiksmai, kuriuos leidžiama atlikti ir veiksmų trukmė. Kad ikiteisminio tyrimo teisėjas sankcionuotų prokuroro prašymą, pastarasis turi pateikti tai pagrindžiančią informaciją. Tokiu būdu ikiteisminio tyrimo teisėjas gali įvertinti ar yra pagrindas taikyti procesinę prievartos priemonę ir savo sprendimą motyvuoti. Vykdydamas ikiteisminio tyrimo teisėjo teisėtumo kontrolės funkciją, ikiteisminio tyrimo teisėjas užtikrina, kad nebūtų pažeisti procese dalyvaujančio asmens teisėti interesai, kad procese dalyvaujantys asmenys laikytųsi galiojančių įstatymų, t. y. užtikrina proceso teisėtumą. Ikiteisminio tyrimo teisėjas vykdo justicijos funkciją ikiteisminiame tyrime[982]. Tačiau teikdamas prašymą sankcionuoti istorinio pobūdžio asmens duomenų rinkimą pagal BPK 155 str. prokuroras neprivalo motyvuoti prašymo pagrįstumo, o ikiteisminio tyrimo teisėjas – savo sprendimo. Ikiteisminio tyrimo teisėjas prokuroro prašymui pritaria jį vizuodamas. Motyvuota ikiteisminio tyrimo teisėjo nutartis šiuo klausimu nėra priimama. Lietuvos Respublikos Konstitucijos 22 str. yra numatyta, kad teisė į privatumą gali būti apribota tik motyvuotu teismo sprendimu. Ikiteisminio tyrimo teisėjo rezoliucija nėra motyvuojama, todėl BPK 155 str. nevisiškai atitinka teisėtam teisės į asmens duomenų apsaugą ir privatumą apribojimui keliamus reikalavimus ir kartu nesuteikia galimybės ikiteisminio tyrimo teisėjui įvertinti prašymo pagrįstumą ir proporcingumą.

Teismų praktikos analizė rodo, kad vadovaujantis BPK 155 str. yra renkama fiksuoto ir mobiliojo ryšio pokalbių išklotinės (metaduomenys) iš Lietuvos mobiliojo ryšio operatūrių[983]. Analogiškai, metaduomenys iš užsienio juridinių asmenų, teikiančių komunikacijos elektroninėje erdvėje paslaugas tarptautiniu mastu, pvz. WhatsApp, Messenger, Gmail, Instagram ir kt., taip pat gali būti renkama vadovaujantis šiuo straipsniu. Pagrindiniai JAV paslaugų el. erdvėje teikėjai (Apple, Facebook, Google ir Microsoft) informaciją ES ikiteisminio tyrimo institucijoms nesivadovaujant tarpusavio pagalbos sutarčių nuostatomis tiesiogiai teikia savanoriškais pagrindais (plačiau apie tai 5 disertacijos skyriuje)[984]. Kiekvienas jų turi skirtingą praktiką dėl teisėsaugos

---

[982] Gušauskienė, supra note, 929: 129, 130.

[983] Žr. pvz. „Lietuvos Aukščiausiojo Teismo 2014 m. sausio 14 d. nutartis byloje Nr. 2K-140/2014“, *eTeismai,* žiūrėta 2020 m. rugsėjo 9 d., https://eteismai.lt/byla/239334207577774/2K-140/2014.

[984] „Criminal justice access to data in the cloud: challenges“, *Council of Europe*, 4, žiūrėta 2020 m. rugpjūčio 22 d., https://rm.coe.int/1680304b59.

institucijų tiesioginių prašymų pateikimų būdų ir pateikiamų asmens duomenų kiekį, tačiau kaip rodo statistiniai duomenys, skirtingai nuo beveik absoliutaus teisminio sankcionavimo, tarptautinės paslaugas elektroninėje erdvėje teikiančios įmonės net ir teismo sankcionuotus teisėsaugos institucijų prašymus tenkina ne visais atvejais.

Apple skaidrumo ataskaitos duomenimis Lietuvos teisėsaugos institucijos į Apple iki 2020 m. birželio 15 d. tiesiogiai kreipėsi tik vieną kartą – 2017 m. liepos mėnesį. Apple Lietuvos teisėsaugos institucijos prašymą tenkino[985]. Kreipimosi pagrindas – skubios pagalbos situacija, kuomet pavojus gresia asmens gyvybei, valstybės arba valstybės strateginę reikšmę turintiems objektams[986]. Informacija kokius duomenis ir kokioje byloje Apple suteikė teisėsaugos institucijos nėra pateikiama.

Facebook skaidrumo ataskaitos duomenys apima Facebook, Messenger ir Instagram duomenis. Facebook skaidrumo duomenimis Lietuvos teisėsaugos institucijos į Facebook kreipiasi nuo 2013 m. Tuo metu Facebook buvo pateikti 6 prašymai, patenkintas 1 (17%). 2019 m. Facebook gavo 89 prašymus iš Lietuvos teisėsaugos institucijų, 77 iš jų buvo tenkinti (87%). Didžiausią kiekį prašymų Lietuvos teisėsaugos institucijos Facebook pateikė 2018 m. – 100, iš kurių 73 (73%) buvo patenkinti[987]. Teisėsaugos institucijos į Facebook taip pat gali kreiptis prašydamos apriboti viešą prieigą prie Facebook paskelbtos informacijos. Facebook skaidrumo ataskaitos duomenimis teisėsaugos institucijų prašymu Facebook 2017 m. apribojo viešą prieigą prie 2 viešų žinučių (angl. *post*), kurstančių neapykantą, 2018 m. – 1, 2019 m. – 4[988].

Google skaidrumo ataskaitos duomenimis Lietuvos teisėsaugos institucijos į Google kreipiasi nuo 2013 m. kuomet pateikė 11 užklausų (64% patenkino), 2019 m. – 164 užklausos (87% patenkintų)[989]. Google, skirtingai nei kitos JAV paslaugų el. erdvėje įmonės, „Gmail“, „Google Plus“, „Youtube“, „Google Blog“, „Google Drive“ informaciją teisėsaugos institucijoms teikia tik pagal tarpusavio pagalbos sutartis[990].

Microsoft skaidrumo ataskaitos duomenimis 2019 m. Lietuvos teisėsaugos institucijos Microsoft pateikė 28 prašymus dėl metaduomenų suteikimo. 23,80% prašymų Microsoft netenkino, 19,92% nerado prašomos informacijos, 58,29% prašymų tenkino[991].

---

985 „Privacy – Government Information Requests – Apple (LT)“, *Apple Legal*, žiūrėta 2020 m. rugpjūčio 22 d., https://www.apple.com/legal/transparency/lt.html.

986 „Apple Emergency Government / Law Enforcement Information Request“, *Apple Inc.*, žiūrėta 2020 m. rugpjūčio 22 d., https://www.apple.com/legal/privacy/le-emergencyrequest.pdf .

987 „Requests For User Data“, *Facebook Inc.,* žiūrėta 2020 m. rugpjūčio 22 d., https://transparency.facebook.com/government-data-requests/country/LT.

988 „Requests For User Data“, *Facebook Inc.*, žiūrėta 2020 m. rugpjūčio 22 d., https://transparency.facebook.com/content-restrictions/country/LT/jan-jun-2019.

989 „Naudotojų Informacijos Užklausos – „Google“ Skaidrumo Ataskaita“, *Google Inc.*, žiūrėta 2020 m. rugpjūčio 22 d., https://transparencyreport.google.com/user-data/overview?legal_process_breakdown=expanded:1,2&lu=legal_process_breakdown.

990 „Criminal justice access to data in the cloud: challenges“, *Council of Europe*, 8, žiūrėta 2020 m. rugpjūčio 22 d., https://rm.coe.int/1680304b59. Lietuvos policijos generalinio komisaro 2019 m. balandžio 11 d. nurodymas Nr. 5-N6 „Dėl bendradarbiavimo su bendrove „Google, Inc.“, *Lietuvos Respublikos generalinė prokuratūra*, žiūrėta 2020 m. rugpjūčio 22 d., https://www.prokuraturos.lt/data/public/uploads/2020/04/neapykantos_nusikaltimu_tyrimo_metodines_rekomendacijos.pdf

991 „Law Enforcement Requests Report – Microsoft CSR“, *Microsoft Inc.*, žiūrėta 2020 m. rugpjūčio 22 d., https://www.microsoft.com/en-us/corporate-responsibility/lerr.

Tai rodo, kad Lietuvos teisėsaugos institucijos į tarptautines paslaugų el. erdvėje teikėjas kreipiasi labai retai. Asmens duomenų el. erdvėje rinkimo tarpusavio pagalbos sutarčių pagrindu mechanizmas yra sudėtingas ir nepatrauklus taikyti praktikoje[992], tačiau savanoriško asmens duomenų (meta duomenų) teikimo procedūra yra paprasta: asmens duomenys yra teikiami per tarpusavio bendradarbiavimo platformą[993] arba elektroniniu paštu[994].

Nors metaduomenis ir komunikacijos turinį, kuris nėra užkoduotas ištisiniu šifravimu (angl. end to end ecryption), teisėsaugos institucijos tarpusavio pagalbos sutarčių pagrindu gali rinkti iš tų paslaugų teikėjų, kurie savanoriškais pagrindais su teisėsaugos institucijomis nebendradarbiauja, pvz., WhatsApp, Viber ir kt., tačiau teismų praktikos analizė rodo, kad ikiteisminio tyrimo institucijos susirašinėjimo per tarptautines komunikacijos el. erdvėje programėles informaciją gauna atrakinus įtariamųjų telefonus, pvz. „iš mobiliojo ryšio telefono Samsung apžiūros protokolo matyti, kad apžiūrimas juodos spalvos korpusu išmanusis mobiliojo ryšio telefonas Samsung, kurio IMEI (duomenys neskelbtini), su įdėta Sim kortele. Apžiūrėti susirašinėjimai programose: „WhatsApp“, „Viber“, „Messenger“, esantys mobiliojo ryšio telefone bei aplikacijose, nuotraukų galerija, interneto naršymo istorija, elektroniniu paštu gauti ir siųsti laiškai, kitos telefone esančios aplikacijos“[995] arba kitiems proceso dalyviams tokią informaciją pateikus savo noru, pvz. „2019-08-06 savanoriško daiktų, dokumentų pateikimo protokole nurodyta, kad liudytoja P. Y. sutiko savanoriškai pateikti iš savo mobiliojo ryšio telefone „iPhone 8“ (tel. Nr. (duomenys neskelbtini)) esančios programos „WhatsApp“ 2019-08-04 susirašinėjimą su savo vyru O. Y.“[996]. Šis asmens duomenų rinkimo būdas bus analizuojamas toliau disertacijoje.

2.3. Istorinio pobūdžio asmens duomenų rinkimo iš juridinių asmenų faktiniai pagrindai. Lietuvos Aukščiausias Teismas teismų praktikos apžvalgoje akcentuoja, kad BPK 154 str. gali būti taikomas tik tais atvejais, kai kitomis procesinės prievartos priemonėmis negalima pasiekti reikiamų rezultatų[997], o asmens duomenų rinkimu elektroninėje erdvėje teisė į privatumą ir asmens duomenų apsaugą yra labai apribojama[998]. BPK 11 str. 1 d. įtvirtintas proporcingumo principas yra taikomas visų procesinės prievartos priemonių atžvilgiu. Todėl proporcingumo reikalavimas turėtų būti

---

992 „Criminal justice access to data in the cloud: challenges“, *Council of Europe*, 8, žiūrėta 2020 m. rugpjūčio 22 d., https://rm.coe.int/1680304b59

993 Facebook atvejis.

994 Kiti atvejai.

995 „Kauno apygardos teismo 2019 m. spalio 29 d. baudžiamasis įsakymas baudžiamojoje byloje Nr. 1-336-966/2019“, *eTeismai*, žiūrėta 2020 m. rugsėjo 9 d., https://e-teismai.lt/byla/16094190275791/1-336-966/2019.

996 „Klaipėdos apygardos teismo 2020 m. vasario 11 d. nuosprendis baudžiamojoje byloje Nr. 1-27-380/2020“, *eTeismai*, žiūrėta 2020 m. rugsėjo 9 d., https://eteismai.lt/byla/187394242358099/1-27-380/2020?word=neringa%20zaicevait%C4%97.

997 „Lietuvos Aukščiausiojo Teismo Elektroninių ryšių tinklais perduodamos informacijos kontrolės, jos fiksavimo ir kaupimo (Baudžiamojo proceso kodekso 154 straipsnis, Kriminalinės žvalgybos įstatymo 10 straipsnis) taikymo apžvalga“, *Lietuvos Aukščiausiasis Teismas*, žiūrėta 2020 m. rugpjūčio 17 d., https://www.lat.lt/lat-praktika/teismu-praktikos-apzvalgos/baudziamuju-bylu-apzvalgos/68.

998 Lietuvos Aukščiausiojo Teismo Teisės tyrimų ir apibendrinimo departamento apibendrinimas „Procesinės prievartos priemonės – elektroninių ryšių tinklais perduodamos informacijos kontrolės, jos fiksavimo ir kaupimo – taikymas“.

taikomas ir istorinio pobūdžio asmens duomenų rinkimui pagal BPK 155 str. Pareiga užtikrinti proporcingumo reikalavimo laikymąsi tenka prokurorui, kadangi teismas neargumentuoja savo sprendimo apibrėždamas teisės į asmens duomenų apsaugą apribojimo ribas, o pritarimą/nepritarimą išreiškia rezoliucija. Tačiau proporcingumo principo reikalavimas nėra taikomas BPK 97 str. atžvilgiu, kadangi duomenų rinkimas pagal BPK 97 str. nėra procesinės prievartos priemonė. Tai yra antroji priežastis, kodėl asmens duomenys neturėtų būti renkami vadovaujantis BPK 97 str.

EŽTT byloje *Iordachi prieš Moldovą* neigiamai vertino tai, kad pagal Moldovos BPK taikyti elektroninių ryšių tinklais perduodamos informacijos kontrolę galima daugiau nei pusės BK įtvirtintų nusikalstamų veikų atžvilgiu[999]. Lietuvos Respublikos BPK 97 ir 155 str. taikymas nėra apribojamas konkrečių nusikalstamų veikų atžvilgiu. Vadinasi, skirtingai nei BPK 154 str., gali būti taikomas visų nusikalstamų veikų tyrime. Tai ne tik neatitinka EŽTT praktikos, bet ir sudaro teisines spragas apeiti BPK 154 str. numatytus apribojimus, jeigu yra renkami kiti duomenys nei realiuoju laiku vykstančių pokalbių turinys. Kaip jau minėta, esamasis laikas elektroninėje erdvėje trunka mikro sekundės dalis[1000], o paplitus 5G ryšiui asmens duomenų keliavimo el. erdve greitis dar labiau padidės[1001]. Vadinasi, realusis arba esamasis laikas elektroninėje erdvėja trunka tuo momentu kol asmens duomenys keliauja joje ir yra tik pas paslaugos teikėją, bet ne pas gavėją. Gavėjo gautos ir įrenginyje esančios žinutės ar atlikti veiksmai technologiškai yra istorinio pobūdžio duomenys. Taigi nuo momento, kai komunikacijos elektroninėje erdvėje turinys pasiekia gavėją, technologine prasme tampa istorinio pobūdžio duomenimis. Klausimas, kuris turėtų būti keliamas, jeigu istorinio ir esamojo laiko asmens duomenų rinkimas elektroninėje erdvėje yra reglamentuojamas skirtingai, yra ar gautą komunikacijos turinį automatiškai galima laikyti istorinio pobūdžio duomenimis? Ar asmens gautą, bet neperskaitytą el. laišką arba žinutę galime laikyti istorinio pobūdžio duomenimis? Disertacijos autorė diskusiją dėl šių klausimų yra iškėlusi 2 disertacijos dalyje, kurioje yra apžvelgiamas elektroninių laiškų turinio duomenų rinkimo reglamentavimas JAV. Technologiškai yra įmanoma atskirti ar komunikacijos elektroninėje erdvėje gavėjas perskaitė gautą žinutę, kadangi perskaityta žinutė yra saugoma skirtingoje vietoje nei neperskaityta. Bet problema yra ta, kad yra neįmanoma nustatyti ar asmuo ją perskaitė tol, kol neatlieka su gauta žinute veiksmų, t. y. neatidaro gauto el. laiško ar žinutės. Jeigu įrenginyje yra įjungta pranešimo apie gautus pranešimus ar el. laiškus kartu su turinio matymu funkcija, gavėjas trumpas žinutes gali perskaityti jų neatidaręs. Tokiu atveju elektroninė komunikacija yra pasiekusi gavėją ne tik technologiškai, bet ir faktiškai (t. y. asmuo perskaitė turinį ir jį žino), bet technologiškai kol kas to neįmanoma nustatyti. Bendravimas per el. erdvę yra susižinojimo tarp fizinių asmenų forma, todėl, autorės nuomone, gauta, bet technologiniu požiūriu neperskaityta komunikacija el. erdvėje (nors ir įrenginio darbalaukyje gali būti matoma dalis ar visas pranešimo

[999] „Europos Žmogaus Teisių Teismo 2009 m. rugsėjo 14 d. sprendimas byloje Iordachi ir kiti prieš Moldovą (Nr. 25198/02)“, *Hudoc*, žiūrėta 2020 m. rugsėjo 9 d., https://hudoc.echr.coe.int/fre#{%22itemid%22:[%22001-91245%22]}.

[1000] Jonathan Strickland, „How IP Convergence Works“, *HowStuffWorks*, žiūrėta 2020 m. rugpjūčio 22 d., https://computer.howstuffworks.com/ip-convergence.htm.

[1001] Joseph Migga Kizza, *Ethical and Secure Computing: A Concise Module*, Springer, 2019, 268.

turinys) turėtų būti laikoma realiuoju laiku vykstančia komunikacija, o perskaityta – istorinio pobūdžio. Kadangi istorinio pobūdžio elektroninius asmens duomenis vadovaujantis BPK 155 ir 97 str. (nors šio straipsnio taikymas asmens duomenų rinkimui yra ydinga praktika) galima rinkti dėl visų BK įtvirtintų nusikalstamų veikų, vadinasi pagal šiuo metu galiojantį reglamentavimą istorinio pobūdžio komunikacijos turinį teisėsaugos institucijos gali rinkti tirdamos visas nusikalstamas veikas. Toks asmens duomenų rinkimo reglamentavimas neatitinka EŽTT praktikos, galimai pažeidžia EŽTK 8 str., Europos žmogaus teisių chartijos 7 str. ir Konstitucijos 22 str. ir yra tobulintinas.

3. Asmens duomenų rinkimas iš juridinių ir fizinių asmenų paimant įrenginį.

3.1. Renkamų asmens duomenų apimtys. Asmens duomenys iš juridinių ir fizinių asmenų paimant įrenginį gali būti renkami vadovaujantis BPK 97 str., bet paprastai yra renkama vadovaujantis BPK 145 str. „Krata“, 147 sr. „Poėmis“ ir BPK 207 str. „Apžiūra“. 5 lentelėje yra pateikiama istorinio pobūdžio asmens duomenų rinkimo iš asmenų paimant įrenginį reglamentavimo BPK struktūra. Asmens duomenis renkant iš įrenginio, pvz., mobilaus telefono, kompiuterio, teisėsaugos institucija gauna visą jame esančią informaciją, įskaitant tą, kurios turinio negalima perimti jos keliavimo el. erdve metu, nes jis užšifruotas ištisiniu šifravimu (angl. *end to end encryption*). Taigi, renkant asmens duomenis tiesiogiai iš įrenginio yra gaunama platesnio pobūdžio informacija nei juos renkant iš paslaugas el. erdvėje teikiančių juridinių asmenų ir telekomunikacijų įmonių, įskaitant ištrintus duomenis.

5 lentelė. *Elektroninių asmens duomenų rinkimas iš įrenginio pagal BPK 97, 145 ir 147 str.*

El. asmens duomenys	Metaduomenys							Turinys					
	Rūšis					Teisminis sankcionavimas		Pokalbiai		Kt. turinys		Teisminis sankcionavimas	
	tinklo	programos	paslaugos					Nešifruotas, arba užšifruotas kitu būdu nei ištisinis šifravimas		Užšifruotas ištisiniu šifravimu			
	Esam. l.	Esam. l.	Istorinis										
			Srauto	Vietos nustatymo	Kt.	BPK **97**	BPK **145, 147**	Esamuoju laiku	Istorinis	Esamuoju laiku	Istorinis	BPK **97**	BPK **145, 147**
Ūkio subjektai, teikiantys el. ryšių paslaugas	–	–	Taip	Taip	Taip	–	Taip	Taip (?)	Taip	Taip (?)	Taip	–	Taip
Kiti juridiniai asmenys	–	–	Taip	Taip	Taip	–	Taip	Taip (?)	Taip	Taip (?)	Taip	–	Taip

3.2. Teisiniai pagrindai. BPK 97 str. yra numatyta, kad ikiteisminio tyrimo pareigūnas, prokuroras arba teismas turi teisę reikalauti pateikti fizinius ir juridinius asmenis ne tik dokumentus, bet ir daiktus. Tačiau, kaip jau analizuota anksčiau šiame skyriuje, įrenginių (daiktų) paėmimas vadovaujantis BPK 97 str. nuostatomis turėtų būti laikoma ydinga praktika dėl analogiškų anksčiau išvardintoms priežastims. Kadangi tyrimo veiksmų atlikimas vadovaujantis BPK 97 str. nėra sankcionuojamas teismo, todėl teismų praktikos dėl tokio pobūdžio veiksmų nepavyko rasti. Klaipėdos apygardos teismo 2017 m. vasario 3 d. nuosprendžio aprašymas iliustruoja kaip yra elektroniniai asmens duomenys yra renkami iš mobilaus telefono, kompiuterio ar kito įrenginio:

1. *„2016-04-18 Kratos protokolu nustatyta, kad kratos metu pas J. S., adresu (duomenys neskelbtini), Neringa, buvo paimtas mobiliojo ryšio telefonas „Huwei P8light", IMEI: (duomenys neskelbtini) su SIM kortele ir nešiojamasis kompiuteris „Asus N61J" (t. 1, b. l. 136–139).*
2. *2016-05-26 Lietuvos teismo ekspertizės centro specialisto išvadoje Nr. 11K-214(16) konstatuota, kad visa mobiliojo ryšio telefone „Huawei P8 light" bei jame esančioje microSD atminties kortelėje esanti informacija, kurią galima nuskaityti su LTEC turima aparatūrine ir programine įranga, įrašyta į prie specialisto išvados pridedamą DVD diską (t. 1, b. l. 151–152).*
3. *Remiantis 2016-06-17 Apžiūros protokolu nustatyta, kad DVD diske, ant kurio juodos spalvos rašikliu užrašyta „2016-05-26 specialisto išvada Nr. 11K-121(16) 1 priedas", yra du aplankai: „micro" ir „MRT". Kataloge „micro" – aplankai „Resources", „Webpages" ir „index". Aplanke „Recources", kuriame yra internetinių puslapių naršymo istorijos failai „Internet Exdplorer", „Firefox", paveikslėliai, vaizdo įrašai, dokumentiniai failai."*[1002]

Paprastai įrenginiai yra apsaugoti slaptažodžiu. Ne visada ir ne visus įrenginius galima atrakinti specialia programine įranga nulaužus slaptažodį. Vieningos nuomonės ar asmuo gali būti verčiamas ikiteisminio tyrimo pareigūnams pateikti savo mobiliojo įrenginio slaptažodį iki šiol nėra. Mokslinėje literatūroje ir teismų praktikoje yra pateikiamos skirtingi požiūriai[1003]. Reikalavimas pateikti slaptažodį gali būti traktuojamas kaip asmens liudijimas prieš patį save[1004]. Draudimo liudyti prieš save principas yra įtvirtintas Konstitucijos 31 str. Ši principas reiškia, kad nėra draudžiama apklausti asmenį dėl padarytos nusikalstamos veikos, jeigu šiam asmeniui yra tinkamai išaiškintos jo teisės atsisakyti duoti parodymus ir jeigu toks asmuo savo noru aiškiai sutinka duoti parodymus[1005]. Tačiau ne visada yra laikomasi nuomonės, kad slaptažodžio nurodymas yra asmens liudijimas prieš save. Yra teigiama, kad atskleisdamas įrenginio slap-

[1002] Klaipėdos apygardos teismo Baudžiamųjų bylų skyriaus 2017 m. vasario 3 d. nuosprendis baudžiamojoje byloje Nr. 1-33-462/2017, *eTeismai*, žiūrėta 2020 m. rugsėjo 9 d., https://eteismai.lt/byla/14843301723300/1-33-462/2017.

[1003] Joakim Kävrestad, *Fundamentals of Digital Forensics* (Springer Nature, n.d.), 11.

[1004] Sara Morrison, „The Police Want Your Phone Data. Here's What They Can Get – and What They Can't", *Vox*, 2020, žiūrėta 2020 m. rugpjūčio 23 d., https://www.vox.com/recode/2020/2/24/21133600/police-fbi-phone-search-protests-password-rights.

[1005] Raimondas Jurka, „Draudimas versti duoti parodymus prieš save kaip asmens konstitucinių teisių baudžiamajame procese garantas", *Jurisprudencija*, 1 2006 (79); 31–39.

tažodį asmuo ne liudija prieš save, o tik pagrindžia atitinkamo įrenginio nuosavybę. Pavyzdžiui, JAV Masačiusetso Aukščiausias Teismas 2019 m. byloje *Commonwealth v. Jones* įpareigojo įtariamąjį pasakyti savo mobiliojo įrenginio slaptažodį argumentuodamas tuo, kad teisėsaugos institucija turi įrodymų, kad kaltinamasis žino slaptažodį, todėl slaptažodžio pasakymas yra tik teisėsaugos institucijos žinojimo patvirtinimas, o ne asmens liudijimas prieš save[1006]. Nors tais pačiais metais kitoje JAV valstijoje – Pensilvanijoje – Aukščiausias teismas priėmė sprendimą byloje *Pennsylvania v. Davis*, kad teisėsaugos reikalavimas pateikti kompiuterio slaptažodį yra vertimas asmenį liudyti prieš save[1007]. JAV Apeliacinis teismas byloje *United States of America v. Apple Macpro Computer, Apple Mac Mini Computer, Apple I Phone 6 Plus, Ellular Telephone Western Digital My Book For Mac External Hard Drive, Western Digital My Book Velociraptor Duo External Hard Drive* konstatavo, kad asmuo negali būti verčiamas pasakyti savo slaptažodį, net jeigu jis teigia, kad neatsimena[1008] pakeisdamas 2012 m. Apeliacinio teismo praktiką, kad visgi tokiu atveju asmuo gali būti verčiamas pasakyti savo slaptažodį[1009]. Slaptažodis yra ne vienintelis telefono užrakinimo būdas. Biometrinių duomenų (pirštų antspaudų, veido atvaizdo) naudojimas pakeičia slaptažodžius, sudarytus iš ženklų kombinacijų. Ištisiniu šifravimu užšifruotus ženklų kombinacijų slaptažodžius asmeniui nesutinkant nulaužti yra beveik neįmanoma arba, kaip rodo pastarųjų metų Apple byla, yra labai brangu[1010]. Tačiau priverstinai atrakinti telefoną ar kompiuterį naudojant biometrinius asmens duomenis yra įmanoma. Disertacijos autorei nepavyko rasti duomenų, jog tokie veiksmai būtų teisminio nagrinėjimo objektu nei Lietuvoje, nei pasaulyje. Lietuvos Respublikos BPK 156 str. yra įtvirtinta ikiteisminio tyrimo pareigūno ir prokuroro teisė net ir asmeniui prieštaraujant, jį fotografuoti, filmuoti, matuoti, paimti rankų atspaudus ir pavydžius genetinei daktiloskopijai. Taigi sistemiškai vertinant BPK nuostatas galima teigti, kad prievartinis asmens įrenginio atrakinimas gali būti prilyginimas nusikalstamos veikos vietoje rastų pirštų antspaudų sulyginimui su prievarta paimtais įtariamojo pirštų antspaudais. Tokie ikiteisminio tyrimo veiksmai nėra laikomi asmens liudijimu prieš save. Tačiau teisės į asmens duomenų apsaugą atžvilgiu šios dvi situacijos skiriasi. Atrakinus asmens kompiuterį arba telefoną teisėsaugos institucijai tampa prieinama visi jame esantys duomenys, tam tikrais atvejais, ir ištrinti. Pvz., Klaipėdos apygardos teismo Baudžiamųjų bylų skyriaus 2017 m. vasario 3 d. nuosprendyje baudžiamojoje byloje Nr. 1-33-462/2017 yra nurodoma, kad apžiūros metu mobiliajame telefone tyrimui reikšmingos informacijos nerasta, tačiau ieškant tyrimui reikšmingos informacijos yra peržiūrimas visas

---

1006 „Commonwealth v. Jones“, *Justia Law*, žiūrėta 2020 m. rugpjūčio 22 d., https://law.justia.com/cases/massachusetts/supreme-court/2019/sjc-12564.html.

1007 „Pennsylvania v. Davis (Majority)“, *Justia Law*, žiūrėta 2020 m. rugpjūčio 22 d., https://law.justia.com/cases/pennsylvania/supreme-court/2019/56-map-2018.html.

1008 „United States of America v. Apple Macpro Computer, Apple Mac Mini Computer, Apple I Phone 6 Plus, Ellular Telephone Western Digital My Book For Mac External Hard Drive, Western Digital My Book Velociraptor Duo External Hard Drive“, *CaseLaw*, žiūrėta 2020 m. rugpjūčio 22 d., https://caselaw.findlaw.com/us-3rd-circuit/1853477.html.

1009 „United States of America v. John Doe“, *CaseLaw*, žiūrėta 2020 m. rugpjūčio 22 d., https://caselaw.findlaw.com/us-9th-circuit/1747358.html.

1010 Farivar, *supra note,* 22.

įrenginyje esantis turinys ir metaduomenys *„<...>socialiniame tinkle „Facebook“ žinutės asmeninio pobūdžio, apie laisvalaikį, atostogas, mokslus, tarpusavio santykius, siunčiamos įvairios nuotraukos, kuriuose matomi kasdieniniai darbai, maisto patiekalai ir pan. Panašios pokalbių temos vyrauja ir pokalbių programose „Skype“, „WhatsApp“, tik čia dažniau siunčiamos įvairių internetinių žaidimų nuorodos. Tarp trumpųjų SMS žinučių 2016-04-18 09.21 val. vienoje rašoma apie rūkymą: „O tas testas neparodo ar vakar, ar prieš savaitę rūkiau, tiesiog yra arba ne“. 2016-04-19 buvo išsiųsta SMS dėl elektroninio pašto(duomenys neskelbtini) slaptažodžio pakeitimo, nė viename iš anksčiau minėtų katalogų nerasta tyrimui reikšmingos informacijos*“[1011]. Visos įrenginyje esančios informacijos analizė yra diskutuotina proporcingumo principo atžvilgiu[1012]. Apžiūros metu suvedus ar nulaužus slaptažodį prisijungimą prie įrenginio galima prilyginti nuotoliniam prisijungimui prie įrenginių (angl. *law enforcement hacking*), kurį Europos Parlamentas laiko labiausiai teisę į asmens duomenų apsaugą ir privatumą varžančia procesinės prievartos priemone dėl turimos galimybės prieiti prie absoliučiai visų įrenginyje esančių asmens duomenų[1013], todėl prieiga prie tokių duomenų atitiks teisei į asmens duomenų apsaugą tik tuo atveju, jeigu ikiteisminio tyrimo teisėjo nutartyje bus aiškiai apibrėžta kokius ir kokio laikotarpio asmens duomenis ikiteisminio tyrimo pareigūnai gali rinkti iš asmens įrenginio (telefono arba kompiuterio). Šuo metu galiojančių BPK nuostatų analizė leidžia daryti išvadą, kad tai turėtų būti apibrėžta ikiteisminio tyrimo teisėjo nutartyje, kuria sankcionuojama krata arba poėmis. Jeigu asmens įrenginio slaptažodžio negalima nulaužti ir asmuo atsisako jį pateikti teisėsaugos institucijoms yra dar vienas subjektas, kuris gali slaptažodį pateikti – tai atitinkamo įrenginio gamintojas. Tačiau ištisiniu šifravimu užkoduoto įrenginio slaptažodžio gamintojai taip pat gali nesuteikti. Toks atvejis buvo teisminio ginčo objektu JAV 2016-2018 m. Apple byla dėl ištisiniu šifravimu užkoduoto slaptažodžio nulaužimo San Bernardino teroristinės atakos metu žuvusio teroristo iPhone mobilaus telefono yra aptariama 2 disertacijos skyriuje. Nors JAV Aukščiausias Teismas galutinio sprendimo byloje nepriėmė FTB atsiėmus savo skundą, tačiau galima laikyti, kad Apple ginčą laimėjo FTB nepavykus teisminiu būdu priversti Apple sukurti programos nulaužiančios šiuo metu saugiausią kodavimo būdą – ištisinį šifravimą[1014].

3.3. Faktiniai pagrindai. BPK 145 ir 147 str., priešingai nei BPK 154 str. gali būti taikomas visų BK įtvirtintų nusikalstamų veikų atžvilgiu. Kadangi analogiška situacija yra renkant asmens duomenis el. erdvėje BPK 97 ir 155 str. pagrindu, todėl aukščiau šiame skyriuje pateikti argumentai yra aktualūs ir BPK 145 bei 147 str. atžvilgiu.

[1011] Klaipėdos apygardos teismo Baudžiamųjų bylų skyriaus 2017 m. vasario 3 d. nuosprendis baudžiamojoje byloje Nr. 1-33-462/2017, *eTeismai*, žiūrėta 2020 m. rugsėjo 9 d., https://eteismai.lt/byla/14843301723300/1-33-462/2017.

[1012] Abelson, H. et al. 2015, „Keys Under Doormats: Mandating insecurity by requiring government access to all data and communications“, *Massachusetts Institute of Technology Computer Science and Artificial Intelligence Laboratory Technical Report*, 2015, žiūrėta 2020 m. rugpjūčio 22 d., https://dspace.mit.edu/bitstream/handle/1721.1/97690/MIT-CSAIL-TR-2015-026.pdf

[1013] Gutheil ir Liger, *supra note*, 144.

[1014] Farivar, *supra note,* 22.

Apibendrinimas:

1. *Asmens duomenų rinkimas dėl realiuoju laiku vykstančios komunikacijos elektroninėje erdvėje yra BPK yra reglamentuojama kaip speciali procesinės prievartos priemonė, įtvirtinta BPK 154 str. Istorinio pobūdžio asmens duomenys ikiteisminio tyrimo metu yra renkami vadovaujantis BPK 97 str., 145, 147 ir 155 str., kurie nepasižymi asmens duomenų rinkimo elektroninėje erdvėje reglamentavimo specifika, todėl nevisiškai atitinka pagrįstam teisės į asmens duomenų apsaugą suvaržymui keliamus reikalavimus.*
2. *Nors 2017 m. BPK 154 str. pataisomis buvo pakeistas subjektų pavadinimas iš telekomunikacijų tinklų paslaugų teikėjų į el. ryšio paslaugų teikėjus bei el. ryšių teikėjus, naujų sąvokų įvedimas nepakeitė BPK 154 str. apimties. El. ryšių paslaugų teikėjų sąvoka neapima socialinių tinklų paslaugų teikėjų, komunikacijos programėlių, internetinės paieškos sistemų teikėjų ir kitų paslaugas per el. erdvę teikiančių juridinių asmenų. Taip pat BPK 154 str. pataisomis yra įtvirtinta ydinga praktika suteikianti teisę ikiteisminio tyrimo institucijoms asmens duomenis rinkti iš el. ryšių tinklų teikėjų. El. ryšių tinklų teikėjai paslaugų gyventojams tiesiogiai neteikia. Paslaugas jie teikia el. ryšių paslaugų teikėjams. Dažniausiai el. ryšių tinklų teikėjai yra naudojami žvalgybos tikslais, todėl šių subjektų, kaip asmens duomenų šaltinių, minėjimas BPK 154 str., yra nepagrįstas. Vadinasi, BPK 154 str. vienintelis realus subjektas į kurį teisėsaugos institucijos turi teisę kreiptis dėl el. erdvės asmens duomenų rinkimo yra – el. ryšių paslaugų teikėjai.*
3. *BPK įtvirtinta asmens duomenų skirstymo ne į turinį ir metaduomenis, bet į pokalbius ir kitą informaciją sistema neturi loginio pagrindimo, neatitinka Reglamento dėl elektroninių tinklų ir privatumo projekte, Elektroninių ryšių įstatyme bei Kriminalinės žvalgybos įstatyme vartojamų sąvokų ir turėtų būti pakeista.*
4. *BPK 154 str. yra įtvirtinti trys asmens duomenų rinkimo pagrindai: teismo sankcionavimas, neatidėliotinais atvejais prokuroro nutarimas su įpareigojimu teisminiam sankcionavimui pateikti per 24 valandas ir nesankcionuotas asmens duomenų rinkimas. Tačiau:*
   – *Vadovaujantis Konstitucijos 22 str. ir EŽTT jurisprudencija, sankcionavimas yra pirmuoju teisėto teisės į asmens duomenų apsaugą suvaržymo reikalavimu. Ne visi asmens duomenų rinkimo elektroninėje erdvėje ikiteisminio tyrimo veiksmai yra sankcionuojami teismo. Ikiteisminio tyrimo metu istorinio pobūdžio asmens duomenys gali būti renkami vadovaujantis BPK 97, 145, 147, 155 str., kurie nėra skirti asmens duomenų rinkimo reglamentavimui, todėl neatitinka teisėtam ir proporcingam teisės į asmens duomenų apsaugą suvaržymui keliamų reikalavimų. Teisminis sankcionavimas nėra numatytas BPK 97 str., vadovaujantis BPK 155 str. asmens duomenys yra renkami ikiteisminio tyrimo teisėjo pritarimu, kuris neatitinka motyvuotam teismo sprendimui keliamų reikalavimų. Vadovaujantis JAV gerąja praktika siūlytina istorinio pobūdžio asmens duomenų rinkimą reglamentuoti ne bendromis, o specialiomis BPK nuostatomis išplečiant BPK 154 str. taikymo apimtis ir istorinio pobūdžio asmens duomenų rinkimui.*

– *BPK 154 str. 6 d. įtvirtinta galimybė nesankcionuotai rinkti asmens duomenis esant bent kurio proceso dalyvio sutikimui, jeigu nesinaudojama el. ryšių teikėjų paslaugomis ir įrenginiais, nereglamentuojant sutikimo gavimo procedūrų bei nenumačius vėlesnio teismo sankcionavimo tampa lygiaverčiu teismo sprendimui, o nesankcionuotas asmens duomenų rinkimas pažeidžia Lietuvos Respublikos Konstitucijos 22 str. Ši BPK nuostata turėtų būti panaikinta.*
– *Asmens duomenų rinkimas elektroninėje erdvėje turėtų būti vykdomas ne visų BK įtvirtintų nusikaltimų atžvilgiu, o tik keliančių didžiausią grėsmę. Asmens duomenų rinkimas realiuoju laiku yra apribotas BPK 154 str. 1 d. įtvirtintomis nusikalstamomis veikomis. Istorinio pobūdžio asmens duomenų rinkimas elektroninėje erdvėje yra galimas dėl visų BK nusikalstamų veikų. Tai neatitinka EŽTT jurisprudencijos dėl proporcingo EŽTK 8 str. įtvirtintos teisės apribojimo. Išplėtus BPK 154 str. reglamentaciją apimant istorinio pobūdžio asmens duomenų rinkimą istorinio pobūdžio asmens duomenų rinkimui galiotų tokios pačios nuostatos kaip ir realiuoju laiku renkamiems asmens duomenims.*

4.1.2. Kriminalinė žvalgyba

Kriminalinė žvalgyba (angl. *Law Enforcement Intelligent arba LAWINT*) kaip procedūra susiformavo vėliau nei ikiteisminis tyrimas ar žvalgyba. Kadangi jos atsiradimui įtakos turėjo tiek baudžiamasis procesas, tiek žvalgyba, todėl ir pavadinimas yra abiejų procesų junginys. Kriminalinės žvalgybos atsiradimo istorijos nėra aiškiai identifikuotos, tačiau, manoma, kad jos atsiradimą įtakojo prognozavimo poreikis ir galimybės tai padaryti dėl augančio kriminalistikos priemonių panaudojimo baudžiamajame procese bei žvalgybos metodų pritaikomumo prognostiniams procesams[1015]. Paprastai yra išskiriami du kriminalinės žvalgybos uždaviniai:

1) prevencinis – užkirsti kelią nusikalstamoms veikoms;
2) prognostinis – prognozuoti galimas nusikalstamumo tendencijas[1016].

Lietuvos Respublikos kriminalinės žvalgybos įstatyme yra įtvirtintas kiek kitoks kriminalinės žvalgybos suvokimas. Pirmasis – prevencinis – kriminalinės žvalgybos uždavinys išlieka, tačiau kiti uždaviniai skiriasi[1017].

Įgyvendindami kriminalinės žvalgybos uždavinius kriminalinės žvalgybos subjektai el. erdvėje generuojamus asmens duomenis gali rinkti vadovaudamiesi Kriminali-

[1015] David L. Carter, „Law Enforcement Intelligence Operations. Concept, issues, terms“, Michigan State University, 1990, 23, žiūrėta 2020 m. rugpjūčio 22 d., https://www.ncjrs.gov/pdffiles1/Photocopy/134434NCJRS.pdf.

[1016] *Ibid.*

[1017] Kriminalinės žvalgybos uždaviniai yra šie:
1) nusikalstamų veikų prevencija;
2) nusikalstamų veikų išaiškinimas, taip pat rengiančių, darančių ar padariusių nusikalstamas veikas asmenų nustatymas;
3) asmenų apsauga nuo nusikalstamo poveikio;
4) asmenų, kurie slapstosi nuo ikiteisminio tyrimo ar teismo, nuteistų, taip pat dingusių be žinios asmenų paieška;
5) daiktų, pinigų, vertybinių popierių, kito turto, susijusio su nusikalstamų veikų padarymu, paieška;
6) kriminalinės žvalgybos subjektų vidaus saugumo užtikrinimas.

nės Žvalgybos įstatymo 9 ir 10 str. Šiuose straipsniuose įtvirtintos toliau aptariamos el. erdvėje generuojamų asmens duomenų rinkimo taisyklės, schematiškai pavaizduotos 6 lentelėje.

6 lentelė. *Asmens duomenų rinkimas pagal Kriminalinės žvalgybos įstatymo 9 ir 10 str. nuostatas.*

El. asmens duomenys		Metaduomenys					Teisminis sankcionavimas	Turinys		Teisminis sankcionavimas
		tinklo	programos	paslaugos				Nešifruotas, arba užšifruotas kitu būdu nei ištisinis šifravimas	Užšifruotas ištisiniu šifravimu	
				Srauto	Vietos nustatymo	Kt.				
Ūkio subjektai, teikiantys el. ryšių tinklų paslaugas		–	–	Taip	Taip	–	Apylinkės teismas	Taip	–	Apygardos teismas, bet yra išimčių[1018]
Kiti juridiniai asmenys	9 str. 1 d. 3 p.	–	–	–	Taip	Taip	Apylinkės teismas	Taip	–	Apygardos teismas
	9 str. 8 p.	–	–	–	–	–	–	–	–	–

El. erdvėje renkamų asmens duomenų apimtys. Kriminalinės žvalgybos įstatymas išskiria tris asmens duomenų el. erdvėje rūšis:

1. Turinys.
2. Srauto duomenys.
3. Kita informacija.

Taip pat įstatyme yra išskiriami du subjektai, iš kurių renkami elektroniniai asmens duomenys:

1. Ūkio subjektai, teikiantys el. ryšių tinklų paslaugas.
2. Kiti juridiniai asmenys.

Kokius duomenis ir kokia tvarka kriminalinės žvalgybos subjektai gali rinkti priklauso nuo šių duomenų teikėjo kategorijos – ar tai yra el. ryšių tinklų paslaugas teikiantys ūkio subjektai, ar kiti juridiniai asmenys.

Kriminalinės žvalgybos subjektai iš el. ryšių paslaugų teikėjų gali rinkti tik komunikacijos turinį (10 str.) ir srauto duomenis (9 str.). Metaduomenys yra platesnė sąvoka,

[1018] Sutikimas ir nesinaudojimas įrenginiais.

apimanti tiek srauto, tiek lokacijos duomenis, tiek kitus duomenis apie komunikaciją el. erdvėje: istorinius ir perduodamus realiuoju laiku[1019]. Pastarųjų rinkimui paprastai yra naudojamos techninės priemonės. Kriminalinės žvalgybos įstatymo 9 str. 1 d. 1 p. yra minimi tik srauto duomenys. Vietos nustatymo duomenys gali būti renkami vadovaujantis Kriminalinės žvalgybos įstatymo 9 str. 1 d. 3 p. Taigi, kriminalinės žvalgybos įstatymas leidžia kriminalinės žvalgybos subjektams rinkti tik dalį visų ūkio subjektų, teikiančių el. ryšių paslaugas galimų prašyti rinkti metaduomenų neapimdamas realiuoju laiku vykstančios komunikacijos metaduomenų rinkimo. Turinio duomenų rinkimą reglamentuoja įstatymo 10 str. Jame numatyta, kad kriminalinės žvalgybos institucijos gali prašyti ūkio subjektus, teikiančius el. ryšių paslaugas, pateikti tik neužšifruotą arba užšifruotą ne ištisiniu šifru turinį, kadangi „atgalinių durų“ sukūrimo pareiga Lietuvos teisės aktuose nėra įtvirtinta.

Kriminalinės žvalgybos subjektai elektroninius asmens duomenis iš kitų juridinių asmenų gali rinkti vadovaudamiesi 9 ir 10 str.. Priešingai nei el. ryšių paslaugų teikėjų atveju, įstatymas konkrečiai neįvardija kokius duomenis kriminalinės žvalgybos subjektai gali rinkti iš juridinių asmenų. Tačiau 9 str. 1 d. 3 p. teiginys „kitą informaciją“ reiškia, kad galima prašyti pateikti tik tokią informaciją, kuri neapima paminėtos šio straipsnio 1 ir 2 p. Vadinasi vadovaujantis įstatymo 9 str. 1 d. 3 p. iš kitų juridinių asmenų galima prašyti pateikti tik tokius metaduomenis, kurie neapima srauto duomenų, nors srauto duomenis kiti juridiniai asmenys taip pat gali rinkti[1020]. Antra, šiame Kriminalinės žvalgybos įstatyme įtvirtinta sąlyga – kad tuos metaduomenis juridiniai asmenys turėtų. Tinklo ir programos lygio metaduomenys egzistuoja duomenų keliavo el. erdvėje metu, t. y. realiuoju laiku. Juridiniai asmenys paprastai jų neturi. Jie tvarko tik paslaugos naudojimo lygio metaduomenis – metaduomenis apie jau įvykusią komunikaciją. Visgi, tinklo ir programos lygio metaduomenis juridiniai asmenys gali rinkti, tačiau tam turi taikyti technologines priemones. Kadangi pagal straipsnio formuotę juridiniai asmenys duomenis jau turi turėti ir jie turi neapimti srauto duomenų, todėl darytina išvada, kad 9 str. 1 d. 3. d. apima tik vietos nustatymo duomenis ir kitus 3 lygio metaduomenis, kurie nėra srauto duomenimis. Vadinasi, vadovaujantis Kriminalinės žvalgybos įstatymo 9 str. yra renkami istorinio pobūdžio duomenys. Atsižvelgiant į tai, kad kaip jau minėta, dauguma komunikacijos elektroninėje erdvėje turinio yra istorinio pobūdžio asmens duomenys, darytina išvada, kad Kriminalinės žvalgybos įstatymo 9 str. 1 d. 3 p. teiginys „kita informacija“ apima ir komunikacijos turinį. Palyginimui BPK 154 str. „kita informacija“ reiškia srauto duomenis. Teisinio aiškumo tikslais Kriminalinės žvalgybos įstatyme ir BPK vartojamas „kitos informacijos“ sampratas reikėtų suvienodinti

Kriminalinės žvalgybos 9 str. 8 d. yra numatytas dar vienas atvejis, kuomet kriminalinės žvalgybos subjektai gali kreiptis į juridinius asmenis – norėdami kitos informacijos, kurios gavimui nėra reikalinga motyvuota teismo nutartis. Kokią informaciją ši dalis apima? Skirtingai nei 9 str. 1 d. p. informacijos rinkimui pagal 9 str. 8 d. nėra

[1019] Darius Štitilis, Rolandas Krikščiūnas ir Rimantas Pertauskas, „Kai kurie konvencijos dėl elektroninių nusikaltimų proceso teisės skirsnio įgyvendinimo Lietuvoje aspektai“, *Jurisprudencija: mokslo darbai* 67 (2005): 20–28.

[1020] Štitilis ir Laurinaitis, *supra note*, 26.

reikalinga, kad ją juridiniai asmenys turėtų. Vadinasi, ji gali apimti 1 ir 2 metaduomenų grupę, kadangi srauto duomenų ir vietos duomenų rinkimą reglamentuoja 9 str. 1 d. Tačiau antroji 9 str. 8 d. sąlyga yra, kad tokios informacijos rinkimui turi nereikėti teismo sankcionavimo. Vadovaujantis Lietuvos Respublikos Konstitucijos 22 str., teisė į privatumą gali būti apribojama tik teismo sprendimu. Taigi tam, kad asmuo nepatirtų savavališko ir nepagrįsto teisės į privatumą suvaržymo, slaptos informacijos apie rengiamą, daromą, padarytą nusikalstamą veiką rinkimo priemonės, kuriomis įsiterpiama į žmogaus privatų gyvenimą, gali būti skiriamos tik įstatyme nustatytais pagrindais, laikantis įstatyme nustatytos tvarkos, tik motyvuotu teismo sprendimu paisant proporcingumo reikalavimų[1021].

Įstatymo 2 str. 21 ir 22 d. yra apibrėžtos techninių priemonių naudojimo sąlygos. 2 str. 22 d. numatyta, kad technines priemones naudojant specialia tvarka yra renkama turinio duomenys (asmenų pokalbiai, kitoks susižinojimas ar veiksmai) ir toks duomenų rinkimas apriboja teisę į privataus gyvenimo neliečiamumą. Tinklo ir paslaugos naudojimo lygio metaduomenys nėra komunikacijos turiniu, programos lygio dalis metaduomenų gali tapti komunikacijos turiniu, tačiau rinkimo metu juo nėra. Todėl pirmoji (buvimo turiniu) sąlyga tiesiogiai yra netenkinama tik renkant tinklo ir paslaugos lygio metaduomenis. Galima būtų teigti, kad tinklo ir programos lygio metaduomenų rinkimas patenka į technologinių priemonių naudojimo bendra tvarka apimtį ir jie turi būti renkami pagal kriminalinės žvalgybos institucijų nustatytą tvarką nesankcionuojant teismui. Tačiau renkant tinklo ir programos lygio metaduomenis yra apribojama teisė į privatumą ir tai netenkina antrosios įstatyme įtvirtintos asmens duomenų rinkimo sąlygos. Taigi Kriminalinės žvalgybos įstatymo 9 str. 8 d. pagrindu teisėtai gali būti renkama tik ta informacija, kuri nėra asmens duomenimis. Asmens duomenimis yra bent kokia informacija apie asmenį. Kadangi 9 straipsnis reglamentuoja duomenų rinkimą iš el. ryšių tinklų ir paslaugų teikėjų, Lietuvos banko, finansinių įmonių ir kredito įstaigų bei kitų juridinių asmenų, todėl tikėtina, kad 9 str. 8 d. pagrindu yra renkama ir asmens duomenys. Ši Kriminalinės žvalgybos įstatymo nuostata gali būti laikoma atitinkančią BPK 97 str. nuostatas, todėl analogiškai gali būti taikoma iš Kriminalinės žvalgybos įstatymo 9 str. 8 d. nuostatų analizei (plačiau apie tai disertacijos 4.1.1. poskyryje).

Kriminalinės žvalgybos įstatymo 10 str. reglamentuoja turinio duomenų rinkimą. Turinys apima tik ištisiniu šifravimu (angl. *end to end encryption*) neužšifruotą turinį. Nors paslaugų el. erdvėje tiekėjai teoriškai gali sukurti priemones atšifruoti ištisiniu šifravimu užšifruotus duomenis, tačiau Kriminalinės žvalgybos įstatyme nėra numatyta įpareigojimo nei ūkio subjektams, teikiantiems el. ryšių paslaugas, nei kitiems juridiniams asmenims (el. paslaugų teikėjams) sukurti priemones turinio rinkimui, jeigu tokių nėra. Tai reiškia, kad įstatyme nėra numatyto įpareigojimo atšifruoti ištisiniu šifru (angl. *end to end encryption*) užšifruotus duomenis. Kriminalinės žvalgybos įstatymo 10 str. taip pat yra prisijungimo prie elektroninės erdvės įrenginių teisiniu pagrindu (plačiau apie tai disertacijos 4.1.3. poskyryje).

[1021] Lietuvos Aukščiausiojo Teismo Baudžiamųjų bylų skyriaus plenarinės sesijos 2015 m. birželio 1 d. nutartis baudžiamojoje byloje 2K-P-94-895/2015, *eTeismai*, žiūrėta 2020 m. rugpjūčio 17 d., https://eteismai.lt/byla/44415389271611/2K-P-94-895/2015.

Teismų praktikoje laikomasi nuostatos, kad teismas, nagrinėjantis bylą, kurioje kaltinimas grindžiamas duomenimis, gautais atliekant kriminalinės žvalgybos tyrimą, privalo patikrinti tris pagrindinius aspektus: 1) ar buvo teisinis ir faktinis pagrindas kriminalinės žvalgybos tyrimo veiksmams atlikti; 2) ar tyrimo veiksmai atlikti nepažeidžiant Lietuvos Respublikos kriminalinės žvalgybos įstatymo nustatytos tvarkos; 3) ar duomenis, gautus atliekant kriminalinės žvalgybos tyrimą, patvirtina duomenys, gauti BPK numatytais veiksmais[1022].

Teisiniai asmens duomenų rinkimo pagrindai. Kriminalinės žvalgybos institucijos asmens duomenis el. erdvėje gali rinkti:

1. sankcionavus apylinkės teismui – jeigu yra renkami srauto duomenys iš ūkio subjektų, teikiančių el. ryšių tinklų paslaugas arba jeigu vietos nustatymo arba paslaugos lygio metaduomenys, kurie nėra srauto duomenimis, yra renkami iš kitų juridinių asmenų (el. paslaugų teikėjų);
2. sankcionavus apygardos teismui – jeigu yra renkamas komunikacijos el. erdvėje turinys iš ūkio subjektų, teikiančių el. ryšių tinklų paslaugas arba iš kitų juridinių asmenų (el. paslaugų teikėjų);
3. neatidėliotinais atvejais – prokuroro nutarimu;
4. nesankcionuotai, jeigu:
   4.1. yra renkama asmens duomenimis nesanti informacija iš kitų nei el. ryšių paslaugų teikėjai juridinių asmenų (9 str. 8 d.);
   4.2. turinys yra renkamas asmens prašymu ar sutikimu nesinaudojant el. ryšių paslaugas teikiančių subjektų įranga ar paslaugomis.

Vadinasi, nors kriminalinės žvalgybos įstatymas nenumato skirtingų procedūrų turinio ir metaduomenų rinkimui, tačiau šiuos veiksmus sankcionuoja skirtingo lygio teismai. Reikalavimas turinio rinkimui gauti apygardos teismo leidimą rodo, kad komunikacijos el. erdvėje turiniui žvalgybos įstatymas suteikia didesnę apsaugą nei metaduomenims, kas šiuo metu mokslininkų yra laikoma technologiniu požiūriu jau nebepagrįsta praktika[1023].

Kita vertus, įstatyme yra įtvirtintos išimtys, kuomet duomenys gali būti renkami nesankcionuotai. Pirmoji išimtis yra įtvirtinta 9 str. 8 d. – tai informacijos rinkimas iš juridinių asmenų. Nors teoriškai tokiu būdu gali būti renkama tik asmens duomenimis nesanti informacija, manytina yra įmanomi atvejai, kuomet šio straipsnio pagrindu yra renkami ir asmens duomenys. Statistiniai duomenys apie įstatymo 9 str. 8 d. taikymą nėra skelbiami. Įstatyme nėra numatyta, kad tokius prašymus sankcionuotų prokuroras. O kriminalinės žvalgybos subjektui nusprendus baudžiamajame procese panaudoti informaciją, gautą atliekant kriminalinės žvalgybos veiksmus, paprastai surašomas kriminalinės žvalgybos veiksmų atlikimo protokolas, kuriame išdėstoma

[1022] Lietuvos Aukščiausiojo Teismo Baudžiamųjų bylų skyriaus plenarinės sesijos 2015 m. birželio 1 d. nutartis baudžiamojoje byloje 2K-P-94-895/2015, *eTeismai*, žiūrėta 2020 m. rugpjūčio 17 d., https://eteismai.lt/byla/44415389271611/2K-P-94-895/2015.

[1023] Žr. pvz., Štitilis, Krikščiūnas irmPetrauskas, *supra note*, 1020. Newell ir Tennis, *supra note*, 157. Stalla-Bourdillon, Papadaki ir Chown, *supra note*, 152. Mayer, Mutchler ir Mitchell, *supra note*, 132.

ne visa, o tik ikiteisminiam tyrimui reikšminga informacija[1024]. Vadinasi, kriminalinės žvalgybos subjektai gali rinkti tyrimui aktualią informaciją, tačiau jos nenaudoti baudžiamajame procese. Tokiu atveju, kriminalinės žvalgybos subjektų veiksmų teisėtumo klausimą turėtų kvestionuoti juridinis asmuo, į kurį kreipiamasi su prašymu pateikti informaciją, pateikdamas skundą apygardos teismo pirmininkui. Disertacijos autorei nepavyko rasti informacijos ar juridiniai asmenys tokia teise naudojasi.

Faktinis kriminalinės žvalgybos tyrimo veiksmų pagrindas yra įtvirtintas Kriminalinės žvalgybos įstatymo 8 str. Šiuo pagrindu yra:

1) informacija apie rengiamą, daromą ar padarytą labai sunkų ar sunkų nusikaltimą arba apie įstatyme išvardytus apysunkius nusikaltimus;
2) informacija apie minėtas veikas rengiančius, darančius ar padariusius asmenis;
3) įtariamojo, kaltinamojo arba nuteistojo pasislėpimas;
4) asmens dingimas be žinios;
5) asmenų apsaugos nuo nusikalstamo poveikio vykdymas.

Teismų praktikoje yra susiklosčiusi pozicija netikrinti faktinio kriminalinės žvalgybos veiksmų pagrindo tais atvejais, kai šiuos veiksmus sankcionavo apygardų teismų pirmininkai ar šių teismų Baudžiamųjų bylų skyrių pirmininkai[1025]. Teikdamas teismui prašymus prokuroras jame nurodo ne tik faktinį pagrindą, bet ir turi pagrįsti kriminalinės žvalgybos veiksmų būtinumą. Vertindami prašymo pagrįstumą teismai turėtų vadovautis EŽTT praktika dėl teisės į privatumą suvaržymo ir vertinti ar yra visi teisės į privatumą ir asmens duomenų apsaugą suvaržymo pagrindai:

1) teisių suvaržymo priemonės yra nustatytos įstatymu;
2) jos būtinos demokratinėje visuomenėje siekiant apsaugoti Konstitucijos ginamas ir saugomas vertybes;
3) jomis nėra paneigiama žmogaus teisės į privatumą prigimtis ir esmė;
4) jos yra proporcingos siekiamam tikslui.

Vienas iš nurodytų pagrindų – ar toks teisės apribojimas yra numatytas įstatyme. Todėl teismai privalo vertinti ir faktinį kriminalinės žvalgybos pagrindą tik jį vertindami neprivalo įsitinkinti turimos informacijos tikrumu.

Galimos tokios teisinės situacijos, kai atliekant slaptą telekomunikacijų tinklais perduodamos informacijos turinio kontrolę gaunami ir tam tikri duomenys, leidžiantys įtarti apie kitas asmens (asmenų) daromas nusikalstamas veikas ar nusižengimus. Kadangi šie atvejai nėra sureglamentuoti įstatymu, todėl paprastai teismai tampa teisės aiškintojais ir teisės spragų užpildytojais[1026]. Pavyzdžiui, iš įstatymo nuostatų nėra aišku ar kriminalinės žvalgybos būdu gauti faktiniai duomenys:

[1024] „Rekomendacijos dėl Kriminalinės žvalgybos įstatymo, Baudžiamojo proceso kodekso normų taikymo ir kriminalinės žvalgybos informacijos panaudojimo baudžiamajame procese, patvirtintos Lietuvos Respublikos generalinio prokuroro 2012 m. gruodžio 31 d. įsakymu Nr. I-383“, 22 punktas, *eSeimas*, žiūrėta 2020 m. rugpjūčio 17 d., https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/TAIS.440985?jfwid=-9dzqnu8af.

[1025] „Lietuvos Aukščiausiojo Teismo Baudžiamųjų bylų skyriaus plenarinės sesijos 2015 m. birželio 1 d. nutartis baudžiamojoje byloje 2K-P-94-895/2015“, *eTeismai*, žiūrėta 2020 m. rugpjūčio 17 d., https://eteismai.lt/byla/44415389271611/2K-P-94-895/2015.

[1026] Rima Ažubalytė, „Privataus asmens gyvenimo ribojimas slaptomis priemonėmis: (ne)kokybiško įstatymo problema“, *Jurisprudencija* 26, Nr. 2 (2019): 260–91, doi:10.13165/JUR-19-26-2-02.

1. Ar gali būti panaudoti kaip įrodymai baudžiamajame procese dėl kitų nusikalstamų veikų, kurių atžvilgiu asmens duomenų rinkimas el. erdvėje nebuvo sankcionuotas?

Teismų praktikoje yra išskiriami keturi tokių duomenų naudojimo baudžiamajame procese atvejai:

1.1. Kai nusikalstamos veikos patenka į kategoriją veikų, nurodytų įstatymo nuostatose ir sudarančių pagrindą pagal įstatymą atlikti operatyvinį veiksmą – tokiu atveju dėl jų gauta informacija gali būti kaip įrodymai naudojama ir kituose baudžiamuosiuose procesuose[1027].

1.2. Kai duomenys yra gauti apie asmens, dėl kurio buvo atliekama slapta elektroniniais ryšiais (telekomunikacijų tinklais) perduodamos informacijos turinio kontrolė, nusikalstamos veikos bendrininkus ar kitus su jo daroma nusikalstama veika susijusius asmenis (pvz., asmenis, kurie įgydavo, realizuodavo nusikalstamu būdu gautą turtą) ir tokie duomenys, vadovaujantis teismo praktika, yra laikomi įrodymais.

1.3. Kai nusikalstama veika, dėl kurios buvo sankcionuotas techninių priemonių panaudojimas specialia tvarka, vėliau (ikiteisminio tyrimo ar bylos nagrinėjimo metu) buvo perkvalifikuota pagal kitus BK straipsnius, taip pat ir tokius, kuriuose dėl numatytų nusikalstamų veikų negalėjo būti atliekami kriminalinės žvalgybos veiksmai. Kasacinės instancijos teismo praktikoje yra konstatuota, kad nusikalstamos veikos kvalifikavimo pakeitimas baudžiamojo proceso metu negali nulemti teisėtai gautų duomenų neleistinumo[1028].

1.4. Kai atliekant slaptą telekomunikacijų tinklais perduodamos informacijos turinio kontrolę gaunami ir tam tikri duomenys, leidžiantys įtarti apie kitas asmens (asmenų) daromas nusikalstamas veikas, kurios nepatenka į kategoriją nusikalstamų veikų, dėl kurių pagal įstatymą galėjo būti atliekamas minėtas kriminalinės žvalgybos veiksmas. Lietuvos Aukščiausias Teismas nusprendė, kad tokiu atveju duomenys, gauti atliekant slaptą telekomunikacijų tinklais perduodamos informacijos kontrolę ir leidžiantys įtarti apie kitas asmens (asmenų) daromas nusikalstamas veikas, kurios nepatenka į kategoriją nusikalstamų veikų, dėl kurių pagal Kriminalinės žvalgybos įstatymą galėjo būti atliekamas kriminalinės žvalgybos veiksmas, gali būti nepripažinti įrodymais pagal BPK ir jais gali būti nesiremiama nagrinėjant baudžiamąją bylą[1029].

[1027] Lietuvos Aukščiausiojo Teismo 2012 m. spalio 30 d. nutartis baudžiamojoje byloje Nr. 2K-P-178/2012, *eTeismai*, žiūrėta 2020 m. rugpjūčio 22 d., https://eteismai.lt/byla/21539073475107/2K-P-178/2012.

[1028] Lietuvos Aukščiausiojo Teismo 2010 m. lapkričio 23 d. nutartis baudžiamojoje byloje Nr. 2K-504/2010, *eTeismai*, žiūrėta 2020 m. rugpjūčio 17 d., https://eteismai.lt/byla/235520032106674/2K-504/2010, Lietuvos Aukščiausiojo Teismo 2013 m. gegužės 21 d. nutartis baudžiamojoje byloje Nr. 2K-246/2013, *eTeismai*, žiūrėta 2020 m. rugpjūčio 17 d., https://eteismai.lt/byla/134383672472903/2K-246/2013, Lietuvos Aukščiausiojo Teismo 2014 m. balandžio 14 d. nutartis baudžiamojoje byloje Nr. 2K-194/2014, *eTeismai*, žiūrėta 2020 m. rugpjūčio 17 d., https://eteismai.lt/byla/9356367523030/2K-194/2014, Lietuvos Aukščiausiojo Teismo 2015 m. kovo 31 d. nutartis baudžiamojoje byloje Nr. 2K-168-139/2015, *eTeismai*, žiūrėta 2020 m. rugpjūčio 17 d., https://eteismai.lt/byla/141589214790674/2K-168-139/2015.

[1029] Lietuvos Aukščiausiojo Teismo Baudžiamųjų bylų skyriaus plenarinės sesijos 2015 m. birželio 1 d. nutartis baudžiamojoje byloje 2K-P-94-895/2015, *eTeismai*, žiūrėta 2020 m. rugpjūčio 17 d., https://eteismai.lt/byla/44415389271611/2K-P-94-895/2015.

Minėtoje byloje teismas nesuformavo absoliučios taisyklės – nurodė, kad kriminalinės žvalgybos metu surinkta informacija gali būti nepripažinta įrodymais, tačiau, atsižvelgiant į bylos aplinkybes, gali būti ir pripažinta. EŽTK yra aiškiai numatyta, kad asmens teisių varžymas galimas tik įstatyme įtvirtintais atvejais. Kriminalinės žvalgybos įstatyme yra įtvirtintas baigtinis nusikalstamų veikų sąrašas, kurių atžvilgiu asmens duomenys gali būti renkami el. erdvėje. Todėl, autorės nuomone, kriminalinės žvalgybos informacijos kitų, nei įstatyme įtvirtintų nusikalstamų veikų arba asmenų, kurie daro kitas, nei įstatyme numatytas nusikalstamas veikas, atžvilgiu negali būti naudojama kriminalinės žvalgybos metu el. erdvėje surinkti asmens duomenys.

2. Ar gali tokie duomenys būti naudojami administraciniame procese skiriant tarnybines nuobaudas už korupcinio pobūdžio nusikalstamas veikas netgi tuo atveju, kai asmuo teismo nėra pripažintas kaltu už vykdymą ir kai duomenys yra surinkti ne apie tą asmenį, dėl kurio buvo sankcionuoti kriminalinės žvalgybos veiksmai?

Kriminalinės žvalgybos įstatymo 19 str. 3 d. yra įtvirtinta nuostata, kad kriminalinės žvalgybos informacija apie korupcinio pobūdžio nusikalstamos veikos požymių turinčią veiką, prokurorui sutikus, kriminalinės žvalgybos pagrindinės institucijos sprendimu vadovo sprendimu gali būti išslaptinta ir naudojama tiriant drausminius ir (ar) tarnybinius nusižengimus. Atsakymą į klausimą ar tai nepažeidžia teisės į asmens duomenų apsaugą ir Lietuvos Respublikos Konstitucijos nuostatų 2019 m. pateikė Lietuvos Respublikos Konstitucinis Teismas. Konstitucinis Teismas nutarime pažymėjo, kad Kriminalinės žvalgybos įstatymo 19 str. 3 d. nenurodyta, kad tik konkretaus asmens atžvilgiu, vykdant kriminalinės žvalgybos pagal Kriminalinės žvalgybos įstatymą tyrimą, surinkta kriminalinės žvalgybos informacija gali būti išslaptinama ir panaudojama tiriant būtent šio asmens galimai padarytą korupcinio pobūdžio tarnybinį nusižengimą[1030]. Taigi, kai atliekant kriminalinės žvalgybos tyrimą dėl vieno asmens surenkama informacija apie kitą asmenį ir iš jos matyti, kad tas kitas asmuo galimai padarė tarnybinį nusižengimą, turintį korupcinio pobūdžio nusikalstamos veikos požymių, tokia informacija pagal Kriminalinės žvalgybos įstatymo 19 str. 3 d. taip pat gali būti išslaptinama ir panaudojama to kito asmens korupcinio pobūdžio tarnybinio nusižengimo tyrimui[1031]. Vadinasi, el. erdvėj surinkta kriminalinės žvalgybos informacija apie korupcinio pobūdžio nusikalstamos veikos požymių turinčią veiką, prokurorui sutikus, kriminalinės žvalgybos pagrindinės institucijos sprendimu vadovo sprendimu gali būti išslaptinta ir naudojama tiriant drausminius ir (ar) tarnybinius nusižengimus nepriklausomai nuo to ar to asmens atžvilgiu buvo sankcionuotas asmens duomenų rinkimas el. erdvėje.

3. Ar gali būti plačiai naudojama ne vien tik baudžiamajame procese?

Lietuvos Respublikos Seime 2017 m. buvo įregistruotos Kriminalinės žvalgybos įstatymo pataisos, kuriomis visus kriminalinės žvalgybos metu surinktus duomenis, prokurorui sutikus, buvo ketinama leisti naudoti tiriant:

[1030] Lietuvos Respublikos Konstitucinio Teismo 2019 m. balandžio 18 d. nutarimas Nr. KT13-N5/2019 „Dėl kriminalinės žvalgybos informacijos panaudojimo tiriant korupcinio pobūdžio tarnybinius nusižengimus“, *Lietuvos Respublikos Konstitucinis Teismas*, žiūrėta 2020 m. rugpjūčio 22 d., https://www.lrkt.lt/lt/teismo-aktai/paieska/135/ta1927/content.

[1031] *Ibid.*

1) drausminius ir (ar) tarnybinius nusižengimus, turinčius korupcinio pobūdžio nusikalstamos veikos požymių (šiuo metu galiojančiame įstatyme minėtų nusižengimų tyrimui galima naudoti kriminalinės žvalgybos informaciją tik apie korupcinio pobūdžio nusikalstamos veikos požymių turinčią veiką);
2) teisės aktų, reglamentuojančių ūkinę, komercinę, finansinę ar profesinę veiklą, pažeidimus;
3) neteisėto labdaros, paramos, valstybės ir savivaldybių biudžetų lėšų ir Europos Sąjungos, užsienio valstybių ir tarptautinių organizacijų finansinės paramos lėšų panaudojimo atvejus;
4) viešųjų juridinių asmenų veiklą reglamentuojančių teisės aktų pažeidimus[1032].

Aiškinamajame rašte yra nurodoma, kad pažeidimai konkurencijos, viešųjų pirkimų, įvairios ūkinės, komercinės, finansinės ar profesinės veiklos srityse, neskaidrus fizinių ir juridinių asmenų veikimas stabdo Lietuvos Respublikos Konstitucijos preambulėje įtvirtintų tikslų siekimą, kenkia valstybės ekonomikos vystymuisi, sąžiningų verslo subjektų veiklos plėtrai, vartotojų interesams, valstybės ir savivaldybių biudžetui, demokratijos plėtrai[1033]. Konkrečių argumentų kodėl toks reglamentavimas turėtų būti įteisintas ar pagrindimo, kaip jis atitinka Konstitucijos 22 str., EŽTK 8 str. ar Europos žmogaus teisių chartijos 7 ir 8 str., jo rengėjai nepateikė. Įstatymo pataisoms nepritarė Lietuvos advokatūra[1034] ir Seimo Kanceliarijos Teisės departamentas[1035]. Nors ir neigiamai vertinamo, Seimas, šio Kriminalinės žvalgybos įstatymo pakeitimo projekto neatmetė, o nutarė daryti svarstymo pertrauką iki Lietuvos Respublikos Konstitucinis Teismas pateiks išaiškinimą dėl Kriminalinės žvalgybos įstatymo 19 str. 3 d. nuostatų konstitucingumo[1036]. Konstitucinis Teismas 2019 m. konstatavus, kad Kriminalinės žvalgybos įstatymo 19 str. 3 d. nepažeidžia Konstitucijos[1037] Kriminalinės žvalgybos įstatymo pakeitimo projekto svarstymas gali būti atnaujintas. Visgi minėtas Konstitucinio Teismo nutarimas negali būti pagrindu plačias teises naudoti kriminalinės žvalgybos informaciją suteikiančiam Kriminalinės žvalgybos įstatymo projektui. Konsti-

[1032] „Kriminalinės žvalgybos įstatymo Nr. XI-2234 19 straipsnio pakeitimo įstatymo projektas“, *eSeimas*, žiūrėta 2020 m. rugpjūčio 22 d., https://e-seimas.lrs.lt/portal/legalAct/lt/TAP/b058e9c0153011e7b6c9f69dc4ecf19f?positionInSearchResults=17&searchModelUUID=7e98340a-7523-43ce-80ca-fbec8cc68615

[1033] „Aiškinamasis raštas dėl Kriminalinės žvalgybos įstatymo Nr. XI-2234 19 straipsnio pakeitimo įstatymo projekto“, *eSeimas*, žiūrėta 2020 m. rugpjūčio 22 d., https://e-seimas.lrs.lt/portal/legalAct/lt/TAK/6700dca0153111e7b6c9f69dc4ecf19f?jfwid=1c1atz7irf

[1034] „Stabdomos itin plačias teises kriminalinei žvalgybai suteikiančios įstatymo pataisos“, *Lietuvos rytas*, žiūrėta 2020 m. rugpjūčio 22 d., https://lietuvosdiena.lrytas.lt/aktualijos/2017/06/21/news/stabdomos-itin-placias-teises-kriminalinei-zvalgybai-suteikiancios-istatymo-pataisos-1740598/.

[1035] „Teisės departamento išvada dėl Kriminalinės žvalgybos įstatymo Nr. XI-2234 19 straipsnio pakeitimo įstatymo projekto“, *eSeimas*, žiūrėta 2020 m. rugpjūčio 22 d., https://e-seimas.lrs.lt/portal/legalAct/lt/TAK/e67f7d5019fb11e79f4996496b137f39?jfwid=1c1atz7irf.

[1036] „Lietuvos Respublikos Seimo Teisės ir Teisėtvarkos komiteto išvada dėl Kriminalinės žvalgybos įstatymo Nr. XI-2234 19 straipsnio pakeitimo įstatymo projekto“, *eSeimas*, žiūrėta 2020 m. rugpjūčio 22 d., https://e-seimas.lrs.lt/portal/legalAct/lt/TAK/c2ed4380573211e78869ae36ddd5784f?jfwid=1c1atz7irf.

[1037] Lietuvos Respublikos Konstitucinio Teismo 2019 m. balandžio 18 d. nutarimas Nr. KT13-N5/2019 „Dėl kriminalinės žvalgybos informacijos panaudojimo tiriant korupcinio pobūdžio tarnybinius nusižengimus“, *Lietuvos Respublikos Konstitucinis Teismas*, žiūrėta 2020 m. rugpjūčio 22 d., https://www.lrkt.lt/lt/teismo-aktai/paieska/135/ta1927/content.

tucinis teismas nutarime akcentavo, kad Kriminalinės žvalgybos įstatymo 19 str. 3 d. neprieštarauja Konstitucijai nes:

1) korupcinio pobūdžio nusikalstamos veikos Kriminalinės žvalgybos įstatyme yra suprantamos plečiamai pagal Korupcijos prevencijos įstatymą;
2) kitokio pobūdžio tarnybinių nusižengimų (neturinčių korupcinio pobūdžio nusikalstamos veikos požymių) tyrimui Kriminalinės žvalgybos pagrindu surinkta informacija negali būti naudojama.

Terminai. KŽĮ 10 str. 5 ir 6 d. reglamentuojama susirašinėjimo ir kitokio susižinojimo slaptos kontrolės terminai ir jų pratęsimas – techninių priemonių panaudojimas specialia tvarka, slapta pašto siuntų ir jų dokumentų apžiūra, pašto siuntų kontrolė ir paėmimas, susirašinėjimo ir kitokio susižinojimo slapta kontrolė sankcionuojami ne ilgesniam kaip 3 mėn. laikotarpiui. Šis laikotarpis gali būti pratęstas. Bendras laikotarpis negali būti ilgesnis negu 12 mėn., išskyrus atvejus, kai kriminalinės žvalgybos tyrimas atliekamas dėl turimos informacijos apie rengiamą, daromą ar padarytą labai sunkų ar sunkų nusikaltimą arba kai yra kriminalinės žvalgybos tyrimo pagrindų, numatytų šio įstatymo 8 str. 1 d. 2, 3 ir 4 p. Kriminalinės žvalgybos veiksmus galima pratęsti. Pratęsimas sankcionuojamas ta pačia tvarka kaip ir šių veiksmų skyrimas. Pratęsimų skaičius neribojamas, tačiau kiekvienu atveju pratęsti galima ne ilgesniam negu šio straipsnio 5 d. nustatytam laikotarpiui. Vadovaujantis BPK 154 str., realiuoju laiku kontroliuoti elektroninių ryšių tinklais perduodamus asmens duomenis galima 6 mėn., šios procesinės prievartos priemonės taikymo terminą galima pratęsti vieną kartą 1 mėn. „*BPK įtvirtinti konkretūs minėtos procesinės prievartos priemonės taikymo terminai yra viena iš garantijų, kad nebūtų piktnaudžiaujama šia priemone ir taip nepagrįstai suvaržoma žmogaus teisė į privataus gyvenimo neliečiamumą*“[1038]. EŽTT byloje *Iordachi ir kiti prieš Moldovą* teisine spraga laikė tai, kad Moldovos BPK nenumatė aiškių pasiklausymo terminų. Moldovos BPK yra numatytas 6 mėn. terminas, tačiau jo pratęsimas, kaip ir Kriminalinės žvalgybos įstatyme, nėra ribojamas. Tokia Kriminalinės žvalgybos įstatymo nuostata turėtų būti tikslinama. LAT vertindamas Kriminalinės žvalgybos įstatymo 10 str. 5 p. nurodė, jog ydingas teisinis reguliavimas neatleidžia kriminalinės žvalgybos subjektų, prokurorų, teikiančių prašymus (teikimus) dėl šios kriminalinės žvalgybos priemonės taikymo, ir teisėjų, priimančių sprendimus sankcionuoti tokių priemonių skyrimą (pratęsti jų taikymą), nuo pareigos įvertinti jos taikymo trukmės pagrįstumą, tikslingumą ir proporcingumą[1039]. Lietuvos mokslininkų nuomonė dėl asmens duomenų rinkimo elektroninėje erdvėje trukmės išsiskyrė. G. Goda mano, kad elektroninių ryšių tinklais perduodamos informacijos kontrolė „*ilgesnį laiką keltų abejonių žmogaus teisių apsaugos požiūriu*“[1040]. P. Ancelis taip pat

---

[1038] „Lietuvos Aukščiausiojo Teismo Baudžiamųjų bylų skyriaus plenarinės sesijos 2015 m. birželio 1 d. nutartis baudžiamojoje byloje 2K-P-94-895/2015“, *eTeismai*, žiūrėta 2020 m. rugpjūčio 17 d., https://eteismai.lt/byla/44415389271611/2K-P-94-895/2015

[1039] „Lietuvos Aukščiausiojo Teismo 2007 m. birželio 28 d. Baudžiamojo proceso kodekso normų, reglamentuojančių įrodinėjimą, taikymo teismų praktikoje apžvalga“, *Teismų praktika*, 27 (2007).

[1040] Gintaras Goda, *Vertybiniai prioritetai baudžiamajame procese: monografija*, (Vilnius: Registrų centras, 2014).

mano, kad „*operatyvinis tyrimas neturi trukti labai ilgai*[1041]“. Tačiau D. Petrošius teigia, kad „*žmogau teisių apsaugos mechanizmą reikėtų numatyti ne ribojant terminus, bet nustatant institucines saugos galimybes*[1042]“. Visgi, EŽTT byloje *Iordachi ir kiti prieš Moldovą* teisine spraga laikė tai, kad Moldovos BPK nenumatė aiškių pasiklausymo terminų neribojant procesinės prievartos priemonės pratęsimo terminų. Atsižvelgiant į EŽTT praktiką, manytina, kad Kriminalinės žvalgybos įstatymo nuostata turėtų būti tikslinama nustatant maksimalius veiksmų atlikimo terminus.

Informavimas apie asmens duomenų rinkimą. BPK 161 str. numatyta, kad asmeniui, kuriam buvo taikoma bent viena šiame skyriuje numatyta priemonė jam nežinant (tarp jų ir BPK 154 str.), baigus tokią priemonę taikyti turi būti pranešta apie ją. Pranešti būtina iškart, kai tai įmanoma padaryti nepakenkiant tyrimo sėkmei. Tuo tarpu pagal KŽĮ 5 str. 8 d., jeigu įgyvendinant kriminalinės žvalgybos kontrolę nustatoma, kad kriminalinės žvalgybos metu buvo pažeistos žmogaus teisės ir laisvės, apie tai informuojamas kriminalinės žvalgybos pagrindinės institucijos vadovas. Kriminalinės žvalgybos pagrindinės institucijos vadovas privalo informuoti asmenį apie jo atžvilgiu kriminalinės žvalgybos metu padarytus pažeidimus, išskyrus atvejus, kai pateikus tokią informaciją gali būti padaryta žala nebaigtiems kriminalinės žvalgybos tyrimams ar atskleista kriminalinės žvalgybos slaptųjų dalyvių tapatybė. Jeigu tuo metu pateikta tokia informacija gali padaryti žalos nebaigtiems kriminalinės žvalgybos tyrimams, ji tuoj pat turi būti pateikta baigus kriminalinės žvalgybos tyrimą. Šios Kriminalinės žvalgybos įstatymo nuostatos leidžia daryti išvadą, kad asmenims apie jų atžvilgiu taikytą elektroninių ryšių tinklais perduodamos informacijos kontrolę paprastai yra nepranešama.

EŽTT byloje Klass prieš Vokietiją buvo keliamas klausimas, ar asmuo gali pateikti skundą dėl jo atžvilgiu taikytų slapto sekimo priemonių neturėdamas galimybės įvardinti konkrečios jį paveikusios priemonės. EŽTT konstatavo, kad EŽTK nuostatų efektyvumas reiškia, kad asmuo turi turėti galimybę kreiptis į Europos žmogaus teisių komisiją. Jeigu tokios galimybės nebūtų, tai EŽTK veikimas būtų neefektyvus. EŽTT atkreipia dėmesį, kad tais atvejais, kai valstybės institucijos slapto sekimo egzistavimą slepia nuo asmens, kurio atžvilgiu ši priemonė buvo taikoma, tokiu jam nesudarant galimybės kvestionuoti jos teisėtumo, tai EŽTK 8 str. numatytos teisės didžiąja dalimi yra paneigiamos. Nepaisant svarbaus sankcionuojančio teismo vaidmens užtikrinant asmens teisės, procesinės prievartos taikymo metu šios teisės vis tiek gali būti pažeidžiamos. Atsižvelgdamas į tai, kad asmuo turi teisę į teisminę gynybą, EŽTT konstatavo, kad susijusiems asmenims turi būti pranešta apie slaptą sekimą, kai tai įmanoma padaryti nepakenkus tyrimo tikslams[1043]. Be to, EŽTT byloje *Asociacija už Europos integraciją bei žmogaus teises ir Ekimdzhiev prieš Bulgariją* Bulgarijos teisės aktas, neįpareigojantis pranešti asmenims, kuriems buvo taikomas slaptas sekimas pažeidžia

[1041] Petras Ancelis, *Baudžiamojo proceso ikiteisminis etapas* (Vilnius: Mykolo Romerio universitetas, 2007), 16.

[1042] Darius Petrošius „Operatyvinės veiklos įstatymo raida žmogaus teisių apsaugos kontekste“, *Jurisprudencija* 63, Nr. 55 (2004): 133.

[1043] „Europos Žmogaus Teisių Teismo 1978 m. rugsėjo 6 d. sprendimas byloje Klass ir kiti prieš Vokietiją (Nr. *5029/71*)“, *Hudoc*, žiūrėta 2020 m. rugsėjo 7 d., https://hudoc.echr.coe.int/rus#{%22itemid%22:[%22001-57510%22]}.

EŽTK[1044]. Taigi darytina išvada, kad asmenims, kurių atžvilgiu buvo taikomi slapti veiksmai (tarp jų ir informacijos kontrolė), privalo būti pranešama apie tokių priemonių taikymą, nes kitu atveju yra paneigiamos EŽTK garantuojamos teisės.

Konstitucijos 30 str. 1 d. įtvirtinta, jog „*asmuo, kurio konstitucinės teisės ar laisvės pažeidžiamos, turi teisę kreiptis į teismą*“. Teisė kreiptis į teismą yra absoliuti, šios teisės negalima apriboti ar paneigti, kad pagal Konstituciją įstatymų leidėjas turi pareigą nustatyti tokį teisinį reguliavimą, kad visus ginčus dėl asmens teisių ir laisvių pažeidimo būtų galima spręsti teisme, kad teisės aktais gali būti nustatyta ir ikiteisminė ginčų sprendimo tvarka, tačiau negalima nustatyti tokio teisinio reguliavimo, kuriuo būtų paneigta asmens, manančio, kad jo teisės ar laisvės pažeistos, teisė ginti savo teises ar laisves teisme.[1045] Taigi Konstitucijoje yra įtvirtinta besąlygiška teisė asmeniui kreiptis į teismą. Todėl teisinis reglamentavimas, kai asmeniui nėra pranešama apie jo atžvilgiu taikytą elektroninių ryšių tinklais perduodamos informacijos kontrolę (susirašinėjimo ir kitokio susižinojimo slaptą kontrolę) neatitinka EŽTT formuojamos praktikos ir Konstitucinio Teismo išaiškinimų. Asmuo turėtų būti informuojamas ne tik dėl esamuoju laiku vykdyto asmens duomenų rinkimo, bet ir dėl istorinio pobūdžio asmens duomenų rinkimo.

Apibendrinimas:

1. *Kriminalinės žvalgybos įstatymo 10 str. yra reglamentuojamas asmens duomenų rinkimas realiuoju laiku, 9 str. – istorinio pobūdžio asmens duomenų rinkimas.*
2. *Kriminalinės žvalgybos įstatyme įtvirtintos dvi galimybės teismo nesankcionuotai rinkti asmens duomenis: 1) iš juridinių asmenų ir 2) esant asmens sutikimui, kai nesinaudojama el. ryšių paslaugų teikėjų įrenginiais ar paslaugomis. Pirmuoju atveju iš juridinių asmenų turėtų būti renkama tik asmens duomenų neapimanti informacija, tačiau, tikėtina, jog vadovaujantis Kriminalinės žvalgybos įstatymo 9 str. 8 d. pagrindu gali būti renkami ir asmens duomenys. Todėl šią įstatymo formuluotę reikėtų tikslinti. Antrąjį atvejį teismo nesankcionuoto asmens duomenų rinkimo atvejį reikėtų panaikinti, kadangi asmens sutikimo pagrindu asmens duomenys yra renkami ne tik apie sutikimą davusį asmenį, nėra numatyta neatitinka Konstitucijos 22 str.*
3. *Kriminalinės žvalgybos įstatymo 9 ir 10 str. pagrindu el. erdve perduodami asmens duomenys gali būti renkami įstatymo 8 str. 1 d. numatytais pagrindais ir plečiamai gali būti naudojam tik 19 str. 3 d. įtvirtintu atveju.*
4. *Kriminalinės žvalgybos įstatymo nuostatos įpareigojančios pranešti asmeniui apie jo atžvilgiu taikytą elektroninių ryšių tinklais perduodamų asmens duomenų kontrolę tik tuo atveju, kai buvo pažeistos to asmens teisės neatitinka EŽTT formuojamos praktikos ir Konstitucinio Teismo doktrinos. Asmuo turėtų būti informuojamas ne tik dėl esamuoju laiku vykdyto asmens duomenų rinkimo, bet ir dėl istorinio pobūdžio asmens duomenų rinkimo.*

[1044] „Europos Žmogaus Teisių Teismo 2008 m. sausio 30 d. sprendimas byloje The Association for European Integration and Human Rights ir Ekimdzhiev prieš Bulgariją (Nr. 62540/00)“, *Hudoc*, žiūrėta 2020 m. rugpjūčio 22 d., https://hudoc.echr.coe.int/fre#{%22itemid%22:[%22001-81323%22]}.

[1045] „Lietuvos Respublikos Konstitucinio Teismo 2004 m. gruodžio 29 d. nutarimas „Dėl organizuoto nusikalstamumo užkardymo“, *Lietuvos Respublikos Konstitucinis Teismas*, žiūrėta 2020 m. rugpjūčio 22 d., https://www.lrkt.lt/lt/teismo-aktai/paieska/135/ta277/content.

4.1.3. Teisėsaugos institucijų prisijungimas prie elektroninės erdvės įrenginių

Ištisinio šifravimo (angl. *end to end encryption*) atsiradimas paskatino teisėsaugą galvoti apie būdus kaip rinkti komunikacijos el. erdvėje turinį. Nors yra keletas variantų kaip gauti prieigą prie el. turinio, teisėsaugos ir žvalgybos institucijų labiausiai akcentuojami būdai yra šie – arba priversti paslaugų el. erdvėje tiekėjus palikti spragą programoje vadinamą „atgalinėmis durimis" (angl. *backdoor*), arba įteisinti teisėsaugos institucijų hakeriavimo (prisijungimų prie elektroninės erdvės įrenginių, paprastai kompiuterius, telefonus ar kitus mobiliuosius įrenginius) galimybę[1046]. „Atgalinių durų" sukūrimui sulaukus didelio pasipriešinimo iš paslaugų el. erdvėje teikėjų bei neigiamo mokslininkų vertinimo[1047], teisėsaugos institucijos prisijungimus prie elektroninės erdvės įrenginių pradėjo laikyti ištisinio šifravimo problemos sprendimu. Tačiau šis ištisinio šifravimo (angl. *end to end encryption*) apėjimo būdas lyginant su kitomis asmens duomenų rinkimo el. erdvėje formomis, kelia didžiausią grėsmę:

1) teisei į privatumą ir asmens duomenų apsaugą. Tokio prisijungimo prie elektroninės erdvės įrenginių metu teisėsaugos institucijos gauna prieigą prie absoliučiai visų atitinkamam el. erdvės komponente esančių asmens duomenų. Pavyzdžiui, prisijungimo prie mobilaus telefono atveju tai būtų visos žinutės, el. laiškai, adresatų knyga su skambučių informacija, nuotraukos, lokacijos duomenys ir visa kita informacija, kurios asmenys net nežino, kad telefonas žino apie juos[1048]. Pavyzdžiui, Olandijos teisėsaugai prisijungus prie į pinigų plovimu įtariamo asmens Blackberry telefoną buvo surinkta 7 terabaitai asmens duomenų, kas sudarytų 86 milijonus Microsoft Word lapų[1049]. Dažniausiai yra minimas prisijungimas prie kompiuterio arba kito mobilaus įrenginio, tačiau technologiškai prisijungti galima į bent kurį el. erdvės elementą[1050], įskaitant el. ryšių tinklus. Prisijungus prie el. ryšių tinklo įrenginio, asmens duomenų apimtis būtų daug kartų didesnė nei prisijungus prie fizinio asmens įrenginio (pvz. išmanaus telefono, kompiuterio).
2) interneto saugumui. ENISA ir EUROPOLO nuomone, prisijungimų prie elektroninės erdvės įrenginių įteisinimas padidina piktnaudžiavimo teisėsaugos galiomis riziką tuo sumažindamas interneto patikimumą[1051]. Problemos spren-

[1046] Gutheil ir Liger, *supra note*, 144: 8.

[1047] Amitai Etzioni, „End to End Encryption, the Wrong End", *South Carolina Law Review* 67, no. 3 (2016 2015): 561–84. Tarcisio Teixeira, Paulo Henrique Sabo ir Isabela Cristina Sabo, „Whatsapp and End-to-End Encryption: Legal Trend and the Conflict Privacy vs. Public Interest", *Revista Da Faculdade de Direito Da Universidade Federal de Minas Gerais* 71 (2017): 607–40.

[1048] Victor Immanuel Oloo, „Here's What Your Phone Knows about You", *Dignited*, 2019, žiūrėta 2020 m. rugpjūčio 22 d., https://www.dignited.com/49959/heres-what-your-phone-knows-about-you/.

[1049] Pierluigi Paganini, „Ennetcom – Dutch Police confirmed to have decrypted BlackBerry PGP messages in a criminal case", *Security Affairs*, žiūrėta 2020 m. rugpjūčio 22 d., https://securityaffairs.co/wordpress/57036/cyber-crime/blackberry-pgp-messages.html .

[1050] Pierluigi Paganini, „Hacking a network, using an 'invisibility cloak' – Is it that simple?", *Security Affairs*, žiūrėta 2020 m. rugpjūčio 22 d., https://securityaffairs.co/wordpress/99465/hacking/hacking-a-network-invisibility-cloak.html.

[1051] „On Lawful Criminal Investigation That Respects 21st Century Data Protection – Europol and ENISA Joint Statement", *Europol*, žiūrėta 2020 m. rugpjūčio 22 d., https://www.europol.europa.eu/publications-documents/lawful-criminal-investigation-respects-21st-century-data-protection-europol-and-enisa-joint-statement-0 .

dimu netolimoje ateityje gali tapti šiuo metu Olandijoje kuriamas kvantinio interneto prototipas. Jo kūrėjų teigimu, įsilaužimo į kvantinį internetą galimybių nebuvimas eliminuos asmens duomenų perėmimo jų keliavimo el. erdve grėsmę[1052]. Kvantinio interneto prototipui pasitvirtinus ne tik nelegalūs, bet ir teisėti įsilaužimai, tikėtina, taps neįmanomi. Todėl teisėsaugos institucijos turės ieškoti kitų užšifruotų elektroninių asmens duomenų rinkimo būdų.

3) valstybių suverenitetui. Teisėsaugos institucijos gali nežinoti tikslios mobiliojo įrenginio buvimo vietos, todėl prisijungimo prie elektroninės erdvės įrenginių sankcionavus vienos valstybės teismui, jis gali vykti asmeniui, jo mobiliajam telefonui, kompiuteriui ar kitam įrenginiui būnant kitoje valstybėje, kurioje galioja kitos nei prisijungimą prie elektroninės erdvės įrenginių sankcionavusios valstybės jurisdikcija. JAV baudžiamojo proceso kodekso 41 straipsnyje nuo 2018 m. įtvirtinta teisė per el. erdvę prisijungti prie elektroninės erdvės įrenginių nepriklausomai nuo jo buvimo vietos mokslininkų buvo kritikuojama[1053], tačiau būtent ši nuostata įteisina kitoje nei sankcionavusio teismo valstybėje įsibrovimo metu surinktus duomenis. Priežastis kodėl ši nuostata atsirado JAV baudžiamojo proceso kodekse buvo situacija Šilko kelio byloje, kuomet teisėsaugos surinkti duomenys buvo nepripažinti įrodymais būtent dėl to, kad prisijungimo metu mobilusis įrenginys buvo kitoje valstybėje nei prisijungimą sankcionavęs JAV teismas[1054]. Tarp šešių ES valstybių narių, kuriose yra įtvirtinta galimybė teisėsaugos institucijoms vykdyti prisijungimą prie elektroninės erdvės įrenginių, tik Olandijoje tai nėra ribojama teritorija. Tačiau tokiu atveju Olandijos teisėsaugos turi kreiptis į kitos valstybės teisėsaugos institucijas pagal savitarpio pagalbos sutartis[1055].
4) Nekontroliuojamam įsilaužimo priemonių kūrimui. Tai ypač opia problema gali tapti nedemokratinėse šalyse[1056]. Apie tai plačiau bus rašoma paskutiniame disertacijos skyriuje.

Europos Parlamento užsakyto mokslinio tyrimo duomenimis, prisijungimai prie elektroninės erdvės yra reglamentuojami šešiose ES valstybėse narėse: Lenkijoje, Prancūzijoje, Vokietijoje, Olandijoje, Italijoje ir Didžiojoje Britanijoje. Disertacijos autorės

---

[1052] Gideon Lichfield, „Inside the Race to Build the Best Quantum Computer on Earth", *MIT Technology Review*, žiūrėta 2020 m. rugpjūčio 22 d., https://www.technologyreview.com/2020/02/26/916744/quantum-computer-race-ibm-google/.

[1053] Dyane L. O'Leary, „License to Hack", *New York University Law Review Online* 94 (2019): 56–95. Zach Lerner, „A Warrant to Hack: An Analysis of the Proposed Amendments to Rule 41 of the Federal Ruled of Criminal Procedure", *Yale Journal of Law and Technology* 18 (2016): 26–69. Devin M. Adams, „The 2016 Amendments to Criminal Rule 41: National Search Warrants to Seize Cyberspace, Particularly Speaking National Security in the Information Age: Are We Heading toward Big Brother: Symposium Issue 2017: Data Collection and Advancements in Surveillance Techniques", *University of Richmond Law Review* 51, no. 3 (2017 2016): 727–72.

[1054] „Man Behind Silk Road Website Is Convicted on All Counts", *The New York Times*, žiūrėta 2020 m. rugsėjo 9 d., https://www.nytimes.com/2015/02/05/nyregion/man-behind-silk-road-website-is-convicted-on-all-counts.html. Alice Salles, „Silk Road Case Sets Dangerous Precedents", 2016, žiūrėta 2020 m. rugpjūčio 22 d., https://fee.org/articles/silk-road-case-sets-dangerous-precedents/.

[1055] Gutheil ir Liger, *supra note*, 145: 11.

[1056] *Ibid.*, 9.

nuomone, nors teisėsaugos vykdomi prisijungimai prie elektroninės erdvės kelia didelę grėsmę teisei į asmens duomenų apsaugą, tačiau tam tikrų kovos su nusikalstamumu arba nacionalinio saugumo užtikrinimo įrankių buvimas vienose valstybėse ir nebuvimas kitose, kelia dar didesnę grėsmę, ypač nacionaliniam saugumui, ir kartu sąlygoja valstybių atsilikimą. Svarbu yra ne uždrausti teisę į asmens duomenų apsaugą galinčius pažeisti tiek teisėsaugos, tiek žvalgybos veiksmus, o sukurti teisines priemones, užtikrinančias šios teisės suvaržymo pagrįstumą ir proporcingumą.

Teisėsaugos prisijungimai prie elektroninės erdvės įrenginių nėra vienintelis ištisinio šifravimo apėjimo būdas, tačiau tarptautinėse ir ES lygio diskusijose nebekeliamas alternatyvaus būdo paieškos klausimas[1057]. Europos Parlamento užsakymu 2017 m. buvo atlikta mokslinė studija apie teisėsaugos institucijų prisijungimo prie elektroninės erdvės įrenginių reglamentavimą[1058]. Visose šešiose aukščiau minėtose tuometinėse ES valstybėse narėse[1059] teisėsaugos prisijungimų prie elektroninės erdvės reglamentavimas skiriasi, tačiau visų jų teisės aktuose yra įtvirtinta tiek *ex ante*, tiek *ex post* kontrolės mechanizmai turintys padėti užtikrinti teisės į asmens duomenų apsaugą apribojimo teisėtumą.

Ex ante kontrolė apima:

1) teisminį sankcionavimą, nors kai kuriose ES valstybėse narėse (Vokietijoje, Lenkijoje ir Didžiojoje Britanijoje) skubiais atvejais yra leidžiamas ir teismo nesankcionuotas prisijungimas su sąlyga, kad teismas vėliau (per 3 dienas Vokietijoje, per 5 dienas Lenkijoje[1060]) autorizuos;
2) nusikalstamų veikų, kurių atžvilgiu galima vykdyti prisijungimą prie elektroninės erdvės įrenginių, išskyrimu. Valstybėse narėse nusikalstamos veikos pasirenkamos skirtingais pagrindais: arba sudarant jų sąrašą, arba apsiribojant bausmės griežtumu;
3) prisijungimo prie elektroninės erdvės įrenginių trukmės ribojimu. Pavyzdžiui, Prancūzijoje ir Olandijoje teismas gali sankcionuoti tokius teisėsaugos veiksmus iki 1 mėn. laikotarpiui, Didžiojoje Britanijoje – iki 6 mėn.

Ex post kontrolė apima:

1) asmens, kurio atžvilgiu buvo vykdomas prisijungimo prie elektroninės erdvės įrenginių, informavimą apie šiuos teisėsaugos veiksmus;
2) informacijos apie prisijungimo prie elektroninės erdvės įrenginių veiksmus teikimą išoriniam, teisėsaugos institucijai nepriklausančiam, organui.

Nepaisant kritikos prisijungimo prie elektroninės erdvės įrenginių reglamentavimui, Europos Parlamento užsakymu atliktos studijos autoriai teigiama laiko Vokietijos

[1057] „On Lawful Criminal Investigation That Respects 21st Century Data Protection – Europol and ENISA Joint Statement“, *Europol*, žiūrėta 2020 m. rugpjūčio 22 d., https://www.europol.europa.eu/publications-documents/lawful-criminal-investigation-respects-21st-century-data-protection-europol-and-enisa-joint-statement-0 .

[1058] Gutheil ir Liger, *supra note*, 145.

[1059] Nors Didžioji Britanija nebėra ES valstybe nare, tačiau tyrimo atlikimo ir disertacijos rašymo metu ja dar buvo, todėl disertacijoje ji yra įvardijama kaip ES valstybė narė.

[1060] „Europos Taryba 5 dienų autorizavimo terminą laiko nepagrįstai ilgu. „Venice Commission Opinion No. 839/ 2016, Poland: On the Act of 15 January 2016 Amending the Police Act and Certain Other Acts“, *Council of Europe*, žiūrėta 2020 m. rugpjūčio 22 d., https://www.venice.coe.int/webforms/documents/default.aspx?pdffile=CDL-AD(2016)012-e.

praktiką nedelsiant sunaikinti prisijungimo prie elektroninės erdvės įrenginių metu surinktą, tačiau su tiriama byla nesusijusią informaciją, Italijos įstatymo rengėjų poziciją į teisėkūros procedūras įtraukti šias technologijas išmanančius asmenis bei Olandijoje numatytą privalomą proporcingumo vertinimą prieš teismui sankcionuojant prisijungimo prie elektroninės erdvės įrenginių veiksmus[1061].

Teisės aktuose įtvirtinti griežti kontrolės mechanizmai turėtų būti teisinėmis asmens duomenų apsaugos priemonėmis. Tačiau problema yra tokia pati kaip ir renkant asmens duomenis el. erdvėje įprastiniais būdais – kad el. erdvė yra viena, apimanti visą pasaulį, prisijungimo prie elektroninės erdvės įrenginių būdai taip pat gali būti naudojami tokie patys visose valstybėse, bet valstybės narės tiek *ex ante*, tiek *ex post* kontrolę reglamentuoja skirtingai, todėl teisė į asmens duomenų apsaugą skirtingose valstybėse įgyvendinama skirtingai. Kol kas oficialiai dar tik šešiose valstybėse narėse yra teisėsaugos prisijungimo prie elektroninės erdvės įrenginių galimybė reglamentuojama atskira nuostata. Tačiau ir jose teisėsaugos institucijų teisės bei duomenų rinkimo apimtys yra skirtingos. Vienintelis būdas suvienodinti praktiką bent ES lygiu yra ES lygio teisės akto priėmimas. Tačiau kol tokio teisės akto nėra priimto, valstybės narės yra tiek laisvos nustatyti nacionalinį reglamentavimą, kiek tai nepažeidžia EŽTK ir Europos žmogaus teisių chartijos. Vėlgi, ar reglamentavimas atitinka EŽTK ir Europos žmogaus teisių chartiją sprendžia pačios valstybės narės prieš priimdamos teisės aktus. Ir nors ne visi teisės aktai yra teisė, tačiau jie galioja ir reglamentuoja visuomeninius santykius tol, kol nėra panaikinami[1062].

Reglamentavimas Lietuvoje. Lietuvoje nei Kriminalinės žvalgybos įstatyme, nei BPK teisėsaugos institucijoms prisijungimo prie elektroninės erdvės įrenginių galimybės tiesiogiai nėra įtvirtintos. Netiesiogiai tokia galimybe galime laikyti Kriminalinės žvalgybos įstatymo 10 str. 1 d. kriminalinės žvalgybos subjektams leidžiančią atlikti slaptą susižinojimo kontrolę nesinaudojant ūkio subjektų, teikiančių el. ryšius ir (ar) paslaugas paslaugomis ir BPK 158 str., kuriuo reglamentuojami savo tapatybės neatskleidžiančių ikiteisminio tyrimo pareigūnų veiksmai. Nors, pvz. Italijos baudžiamojo proceso kodekse prisijungimų prie elektroninės erdvės teisiniu pagrindu yra labai panaši nuostata, kuri yra įtvirtinta BPK 154 str. 6 d., leidžianti ikiteisminio tyrimo institucijoms klausytis asmenų pokalbių, daryti jų įrašus ir kontroliuoti kitą el. ryšių tinklais perduodamą informaciją nesinaudojant el. ryšių tinklų ir paslaugų teikėjų įrenginiais ir paslaugomis esant asmens sutikimui.. Šios nuostatos pagrindu Italijos teisėsaugos institucijos naudoja kenkėjiškas programas (angl. *malware*)[1063], paprastai Trojos arklius[1064]. Asmens duomenys kenkėjiškų programų dėka yra renkami prisijungus prie

---

[1061] Gutheil ir Liger, *supra note*, 145.

[1062] Vaišvila, *supra note*, 52.

[1063] Giuseppe Vaciago ir David Silva Ramalho, „Online Searches and Online Surveillance: The Use of Trojans and Other Types of Malware as Means of Obtaining Evidence in Criminal Proceedings", *Digital Evidence and Electronic Signature Law Review*, žiūrėta 2020 m. rugpjūčio 22 d., https://journals.sas.ac.uk/deeslr/article/view/2299.

[1064] Trojos arkliai – kenkėjiškos programos, turinčios kenkėjiškų funkcijų ir besislepiančios kitose programose. Trojos arkliai patenka į sistemą per spragas naršyklėse ar juos pateikiant kaip naudingą programą. Kenkėjiška programa įveda kodą operacinėje sistemoje, todėl piratas gali pasiekti užkrėstą kompiuterį. Trojos arkliai paprastai nesidaugina – juos paskleidžia virusai, kirminai arba atsisiųsta programinė įranga. Tipinio Trojos arklio funkcionalumas yra klaviatūros paspaudimų registravimas, procesų valdymas, bylų išsiuntimas, galimybė stebėti naudotoją ir kt

asmens kompiuterio ar kito mobiliojo įrenginį. Tarkim, Trojos arkliai patenka į sistemą per spragas naršyklėse ar juos pateikiant kaip naudingą programą. Kenkėjiška programa įveda kodą operacinėje sistemoje ir tokiu būdu hakeris gali pasiekti užkrėstą kompiuterį[1065]. Kenkėjiškų programų naudojimas yra tik vienas iš prisijungimo prie elektroninės erdvės įrenginių būdų.

EŽTT bylose *Klass and others v. Germany, Malone v. UK ir Huvig v. France*, *Association for European Integration and Human Rights and Ekimdzhiev v. Bulgaria*, *Dragojević v. Croatia* suformavo šiuos principus, kuriuos turi atitikti teisę į privatumą suvaržantis teisės aktas:

1) teisės akto išraiškos forma gali būti įstatymas arba poįstatyminis aktas, atitinkamai pagal nacionalinės teisės reikalavimus;
2) teisės aktas turi būti viešai paskelbtas, visiems prieinamas ir aiškus;
3) teisės aktas turi nepažeisti teisinės valstybės principo.

Huvig v. France ir *Rotaru v. Romania* bylose EŽTT išskyrė elementus, kurie privalo būti numatyti teisę į privatumą suvaržančiose teisės akto nuostatose, reglamentuojančiuose asmens duomenų rinkimą elektroninėje erdvėje, kad būtų išvengta teisėsaugos institucijų piktnaudžiavimo. Teisės akte privalo būti:

1) išskirtos asmenų kategorijos, kurių atžvilgiu gali būti taikomos teisę į privatumą ribojančios prievartos priemonės;
2) išskirtos nusikalstamų veikų, dėl kurių gali būti nuspręsta taikyti slapto sekimo priemones, kategorijos;
3) aiškiai nustatytos tokio stebėjimo trukmės ribos;
4) numatyta procedūra, pagal kurią tiriami, naudojami ir laikomi gauti duomenys;
5) numatytos atsargumo priemonės, kurių imamasi perduodant šiuos duomenis kitiems subjektams;
6) numatytos aplinkybės, kuriomis gauti duomenys gali ar privalo būti sunaikinti;
7) numatytas teisminis sankcionavimas[1066].

EŽTK 8 str. nėra aiškiai įvardyta ar apribojant asmens teisę į privatumą teisminis sankcionavimas yra privalomas. Byloje *Huvig v. France*, EŽTT pasisakė netiesiogiai, kad teisminis asmens duomenų rinkimo el. erdvėje sankcionavimas yra privalomas[1067]. G. Malgieri ir P. De Hert teigia, kad pagal EŽTT praktiką EŽTK 8 str. įtvirtintos teisės į privatumą apribojimo atvejais *ex ante* sankcionavimas yra privalomas, tačiau jis ne

---

[1065] „Kenkėjiškos programinės įrangos tipai“, *Esaugumas*, žiūrėta 2020 m. rugpjūčio 22 d., https://www.esaugumas.lt/lt/kompiuteriu-virusai/kenkejiskos-programines-irangos-tipai/92

[1066] „Europos Žmogaus Teisių Teismo 1978 m. rugsėjo 6 d. sprendimas byloje Klass ir kiti prieš Vokietiją (Nr. *5029/71*)“, *Hudoc*, žiūrėta 2020 m. rugsėjo 7 d., https://hudoc.echr.coe.int/rus#{%22itemid%22:[%22001-57510%22]}. „Europos Žmogaus Teisių Teismo 1984 m. rugpjūčio 2 d. sprendimas byloje Malone prieš Jungtinę Karalystę (Nr. 8691/79)“, *Hudoc*, žiūrėta 2020 m. rugsėjo 7 d., https://hudoc.echr.coe.int/rus#{%22itemid%22:[%22001-57533%22]}. ir Huvig v. France, European Human Rights Court, žiūrėta 2020 m. rugpjūčio 22 d., https://hudoc.echr.coe.int/eng#{%22fulltext%22:[%22\%22CASE%20OF%20HUVIG%20v.%20FRANCE\%22%22],%22documentcollectionid2%22:[%22GRANDCHAMBER%22,%22CHAMBER%22],%22itemid%22:[%22001-57627%22]}.

[1067] Gianclaudio Malgieri ir Paul de Hert, „European Human Rights, Criminal Surveillance, and Intelligence Surveillance: Towards 'Good Enough' Oversight, Preferably but Not Necessarily by Judges“, in *The Cambridge Handbook of Surveillance Law*, 2017, 8, doi:10.1017/9781316481127.023.

visais atvejais privalo būti teisminis. Sankcionuojantis subjektas priklauso nuo asmens duomenų rinkimo tikslo: asmens duomenis renkant teisėsaugos tikslais sankcionuojančiu subjektu turėtų būti teismas, žvalgybos tikslais – sankcionavimą gali vykdyti ir neteisminio pobūdžio institucija[1068].

Jeigu Kriminalinės žvalgybos įstatymo 10 str. 1 d. bei BPK 158 str. laikysime nuostatomis, leidžiančiomis Lietuvos teisėsaugos institucijoms prisijungti prie elektroninės erdvės, tai atsižvelgiant į EŽTT praktiką ir Europos Parlemento mokslinėje studijoje išskirtus *ex ante* bei *ex post* piktnaudžiavimo galimybe prisijungus prie elektroninės erdvės renkant duomenis elektroninėje erdvėje kontrolės mechanizmus, galime daryti prielaidas, kad:

1) BPK 158 str ir KŽĮ 10 str. 1 d. nėra aiškiai įtvirtinta, kad šie straipsniai apima ikiteisminio tyrimo pareigūnų ir kriminalinės žvalgybos subjektų teisę prisijungti prie elektroninės erdvės, nors įstatymo aiškumas yra vienas iš kertinių teisės į privatumą ir asmens duomenų apsaugą apribojimo pagrindų. BPK 158 str. reglamentuoja ikiteisminio tyrimo vykdymą pareigūnams neatskleidžiant savo tapatybės. Kokius veiksmus gali atlikti savo tapatybės neatskleidžiantys pareigūnai gali atlikti BPK 158 str. tiesiogiai nėra įtvirtinta, tačiau jame nurodoma, kad procesinės prievartos priemones taikyti galima tik teismui jas atskirai sankcionavus (BPK 158 str. 5 d.). Kad BPK 158 str. apima ir teisę prisijungti prie elektroninės erdvės įrenginio tampa aišku tik iš Generalinio prokuroro rekomendacijų 52 p., kuriame yra nurodyta, kad pareigūnai gali *„slapta naudoti technines priemones, kontroliuojant ar fiksuojant asmenų pokalbius, kitokį susižinojimą ar veiksmus, kai nė vienam pokalbio, kitokio susižinojimo ar veiksmų dalyviui apie tokią kontrolę nėra žinoma (išskyrus elektroninių ryšių tinklais perduodamos informacijos kontrolę)“.* Nors EŽTK 8 str. įtvirtinta asmens teisė į privatumą ir asmens duomenų apsaugą vadovaujantis EŽTT sprendimu *Huvig v. France* gali būti apribota ir poįstatyminiu teisės aktu, tačiau teisinis reglamentavimas ir poįstatyminiame teisės akte turi būti aiškus. Generalinio prokuroro rekomendacijose prisijungimo prie elektroninės erdvės nuostatos taip pat nėra aiškiai apibrėžtos, pvz. nėra nurodyta prie kokių įrenginių galima prisijungti, nėra aišku ar prisijungus yra galimas asmens duomenų rinkimas realiuoju laiku, kadangi nereglamentuojama prisijungimo trukmė. EŽTK 8 str. sąlyga, kad teisė į privatumą ir duomenų apsaugą gali būti apribojama įstatymu yra laikoma išpildyta tik tada, kai įstatymas yra aiškus ir tikslus. BPK 158 str. net ir aiškintinas kartu su Generalinio prokuroro rekomendacijomis neatitinka tikslaus ir aiškaus prisijungimo prie elektroninės erdvės įrenginių reikalavimų. Galimai todėl 2017 m. Europos Parlamento studijoje Lietuva nėra minima tarp valstybių narių, kuriose yra reglamentuojamas prisijungimas prie elektroninės erdvės įrenginių[1069].
2) Prisijungimas prie elektroninės erdvės įrenginių nėra įtvirtintas kaip atskira procesinės prievartos priemonė, nors remdamasi tarptautine praktika ir

[1068] Malgieri ir de Hert, *supra note,* 1067: 11.

[1069] Gutheil ir Liger, *supra note*, 145.

tyrimo rezultatais, autorė mano, kad būtent taip turėtų būti. Todėl, skirtingai nei kitų procesinės prievartos priemonių atžvilgiu, teismas sankcionuodamas slaptų tyrimo veiksmų atlikimą prisijungimo prie elektroninės erdvės įrenginių atskirai nesankcionuoja. Tačiau vadovaujantis BPK 158 str. 3 d. 4 p. nutartyje privalo nurodyti konkrečius veiksmus, kuriuos leidžia atlikti. Tokiu būdu teismas tampa pagrindiniu ir vieninteliu teisės į asmens duomenų apsaugą proporcingo suvaržymo garantu. Teisės į asmens duomenų apsaugą teisėto užtikrinimo sąlygas perkėlus iš įstatymo į teismą iškyla dvi problemos: 1) sankcionavimo apimtis priklauso nuo subjektyvaus elemento – ikiteisminio tyrimo teisėjo ankstesnės patirties ir kompetencijos konkrečiai asmens duomenų rinkimo elektroninėje erdvėje sankcionavime. Dauguma teisėjų neturi itin specifinės praktinės asmens duomenų rinkimo elektroninėje erdvėje, IT ir telekomunikacijų srityje patirties, todėl įvertinti asmens duomenų rinkimo mastus ir poveikį privatumui yra sudėtingiau nesant kokybiško įstatymo, kuris nustatytų teisės į asmens duomenų apsaugą proporcingo apribojimo svertus. Tai, kad beveik visi teisėsaugos institucijų prašymai rinkti duomenis elektroninėje erdvėje yra sankcionuojami ne vien tik Lietuvoje, bet ir visame pasaulyje, visų pirma rodo ne teisėjų praktinių žinių apie asmens duomenų rinkimą el. erdvėje trūkumą, bet kokybiško įstatymo trūkumą. Įstatyme turi būti labai aiškūs teisės į privatumą suvaržymo kriterijai tam, kad teisėjas galėtų priimti mažiausiai subjektyvų ir labiausiai asmens teises apsaugantį sprendimą; 2) įstatymai yra skirti visuomeninių santykių reguliavimui. Jie privalo būti viešai skelbiami tam, kad abi visuomeninių santykių pusės būtų informuotos apie tai, kaip tie santykiai yra reguliuojami ir kokios pasekmės laukia nesilaikant nustatytų visuomenės elgesio normų. BPK 158 str. nėra aiškiai nurodoma, kad savo tapatybės neatskleidžiančių pareigūnų veiksmais gali būti atliekami prisijungimai prie elektroninės erdvės įrenginių (mobiliųjų telefonų, kompiuterių ir kt.) asmeniui to nežinant.

3) Vadovaujantis BPK 158 str. 6 d, kriminalinės žvalgybos subjektai ir ikiteisminio tyrimo institucijos prisijungti prie elektroninės erdvės įrenginio gali pačios arba paslaugų sutarties pagrindu samdydamos fizinius ar juridinius asmenis (plačiau apie bendradarbiavimą IV disertacijos skyriuje) – tai atitinka pasaulinę praktiką, pvz, FTB turi savo vidines hakerių komandas, tačiau taip pat paslaugų sutarčių pagrindu samdo ir išorinius hakerius. Olandijoje konfidencialumo sutartis su prisijungimą prie elektroninės erdvės įrenginių vykdančiu fiziniu ar juridiniu asmeniu yra naudojama kaip pretekstas neinformuoti asmenų apie tai, kad į jų įrenginį buvo įsilaužta[1070] . Taigi, prisijungimo prie elektroninės erdvės įrenginio slaptumas pasireiškia per tai, kad asmuo, kuris naudojasi įrenginiu, nežino, kad prie to įrenginio prisijungė teisėsaugos institucijos. Italijos teisėsaugos institucijos naudoja kenkėjiškas programas (angl. *malware*)[1071], paprastai Trojos ark-

[1070] Gutheil ir Liger, *supra note*, 145: 56.

[1071] Vaciago ir Ramalho, *supra note*, 1064.

lius[1072]. Asmens duomenys kenkėjiškų programų dėka yra renkami prisijungimus prie elektroninės erdvės įrenginių. Tarkim, Trojos arkliai patenka į sistemą per spragas naršyklėse ar juos pateikiant kaip naudingą programą. Kenkėjiška programa įveda kodą operacinėje sistemoje ir tokiu būdu teisėsaugos institucijos pareigūnas gali pasiekti užkrėstą kompiuterį[1073]. Kenkėjiškų programų naudojimas yra tik vienas iš prisijungimo prie elektroninės erdvės įrenginių būdų[1074]. Prisijungimo prie elektroninės erdvės įrenginio procese pareigūno tapatybės slaptumas yra nereikalingas, kadangi prisijungimas vyksta pareigūnui fiziškai nesąveikaujant su įtariamuoju[1075].

4) Kriminalinės žvalgybos atveju prisijungimus prie elektroninės erdvės įrenginių galima vykdyti visais atvejais dėl kurių galima atlikti kriminalinę žvalgybą, baudžiamojo proceso metu – kurių atžvilgiu galima taikyti 158 str. įtvirtintą procesinę prievartos priemonę. BPK 158 str. yra įtvirtinta ir Generalinio prokuroro rekomendacijose atkartota ydinga nuostata dėl nusikaltimų, kurių atžvilgiu gali būti slaptai kontroliuojamas susižinojimas tarp asmenų: jeigu savo tapatybės neatskleidžiančių ikiteisminio tyrimo pareigūnų atliekamais veiksmais gali būti varžoma <...> susirašinėjimo ar kitokio susižinojimo ne elektroninių ryšių tinklais slaptumas, tokie veiksmai gali būti atliekami tiriant tik labai sunkius, sunkius ir apysunkius nusikaltimus. Susirašinėjimo ar kitokio susižinojimo ne elektroninių ryšių tinklais slaptu sekimu teisėsaugos institucijos gali sužinoti tik tą informaciją, kuri yra įrašoma arba kitokiu būdu perimama nuo įrašymo ar kito pasiklausymo įrenginio slapto įmontavimo ar kt. Prisijungimu prie elektroninės erdvės įrenginio teisėsaugos institucijoms tampa prieinama visa tame įrenginyje arba per tą įrenginį keliaujanti informacija, todėl mokslininkai laiko labiausiai teisę į privatumą ir asmens duomenų apsaugą pažeidžiančia teisėsaugos taikoma asmens duomenų rinkimo priemone[1076]. EŽTT byloje *Iordachi ir kiti prieš Moldovą* proporcingumo principo pažeidimu laikė tai, kad Moldovos BPK numatyta galimybė elektroninių ryšių tinklais perduodamą informaciją rinkti dėl daugiau nei pusės Moldovos BK įtvirtintų nusikalstamų veikų. Europos Parlamento užsakymu mokslininkų atliktoje studijoje teigiama, kad

[1072] Trojos arkliai – kenkėjiškos programos, turinčios kenkėjiškų funkcijų ir besislepiančios kitose programose. Trojos arkliai patenka į sistemą per spragas naršyklėse ar juos pateikiant kaip naudingą programą. Kenkėjiška programa įveda kodą operacinėje sistemoje, todėl piratas gali pasiekti užkrėstą kompiuterį. Trojos arkliai paprastai nesidaugina – juos paskleidžia virusai, kirminai arba atsisiųsta programinė įranga. Tipinio Trojos arklio funkcionalumas yra klaviatūros paspaudimų registravimas, procesų valdymas, bylų išsiuntimas, galimybė stebėti naudotoją ir kt

[1073] „Kenkėjiškos programinės įrangos tipai“, *Esaugumas*, žiūrėta 2020 m. rugpjūčio 22 d., https://www.esaugumas.lt/lt/kompiuteriu-virusai/kenkejiskos-programines-irangos-tipai/92

[1074] I. C. T. ICT School, *Computer Hacking: This Book Includes: Hacking Tools for Computers with Linux Mint, Linux for Beginners and Kali Linux Tools and Hacking with Kali Linux with Basic Security Testing* (Amazon Digital Services LLC – KDP Print US, 2019).

[1075] Gediminas Bučiūnas, „Slaptas sekimas – tinkamos pusiausvyros paieška tarp visuomenės teisės būti saugia ir asmens teisės į privatumą“ (Vytauto Didžiojo universitetasPrieiga per eLABa – nacionalinė Lietuvos akademinė elektroninė biblioteka, 2014), 71.

[1076] Giovanni Ziccardi, „The GDPR and the LIBE Study on the Use of Hacking Tools by Law Enforcement Agencies Essays“, *Italian Law Journal* 4, no. 1 (2018): 220.

prisijungimai prie elektroninės erdvės turėtų būti įstatymiškai leidžiami tik sunkių ir labai sunkių nusikaltimų atveju[1077]. Šis teisės į asmens duomenų apsaugą suvaržymo būdas pasižymi ne tik tuo, kad teisėsaugos institucijos įgyja prieigą prie visų įrenginyje esančių asmens duomenų ir tokiu būdu labiausiai suvaržo asmens privatumą[1078], bet ir todėl, kad prisijungęs asmuo gali faktiškai valdyti įrenginį, pvz. išsiųsti žinutę įtariamojo vardu, ištrinti dalį duomenų, juos pakeisti ir kt.[1079]. Nutraukus prisijungimo prie įrenginio veiksmus paprastai jame lieka prisijungimu padarytos spragos operacinėje sistemoje, kurių ištaisyti dažnai nebeįmanoma, tokiu būdu sumažinant įrenginio saugumą arba funkcionalumą[1080] .

5) EŽTT nagrinėdamas bylą *Iordachi ir kiti prieš Moldovą* nustatė kaip trūkumą tai, kad įstatyme nėra įtvirtintų aiškių elektroninių ryšių tinklais perduodamos informacijos kontrolės terminų. BPK 154 str. reglamentuoja mažiau teisę į asmens duomenų apsaugą ribojančią priemonę nei BPK 158 str. Tačiau BPK 154 str. 4 d. yra aiškiai įtvirtinti maksimalūs elektroninių ryšių tinklais perduodamos informacijos kontrolės terminai. Ši procesinės prievartos priemonė negali trukti ilgiau nei 6 mėnesius, o tiriant sudėtingą ar didelio masto nusikalstamą veiką jos taikymas gali būti vieną kartą pratęstas, bet ne ilgiau nei 3 mėnesiams. Konkrečių terminų nenustatymas gali būti aiškinamas taip, kad BPK 158 str. yra galimas tik vienkartiniam prisijungimui prie elektroninės erdvės įrenginio ir visų jame esančių asmens duomenų nukopijavimui. Bet viena iš pagrindinių priežasčių kodėl teisėsaugos institucijos vis dažniau taiko šį asmens duomenų rinkimo būdą yra negalėjimas kontroliuoti ištisiniu šifravimu užšifruotos tiek istorinio pobūdžio, tiek esamuoju laiku vykstančios komunikacijos elektroninėje erdvėje (pvz. per WhatsApp, Viber ir kt.)[1081], tiriant nusikaltimus tamsiajame internete[1082]. BPK 158 str. nėra įtvirtinti slaptų veiksmų taikymo terminai, tačiau ikiteisminio tyrimo teisėjo nutarčiai yra keliamas reikalavimas nurodyti slaptų veiksmų trukmę (BPK 158 str. 3 d. 6 p.). Vadovaujantis šiuo ikiteisminio tyrimo teisėjo nutarčiai ir kartu prokuroro prašymui keliamu reikalavimu galime daryti prielaidą, kad vadovaujantis BPK 158 str. galima sankcionuoti realiuoju laiku vykstančios komunikacijos duomenų rinkimą. Tačiau tai yra tik prielaida ir kartu BPK 158 str. trūkumas, kadangi asmens duomenų rinkimas realiuoju laiku prisijungus prie elektroninės erdvės įrenginio tiesiogiai nėra įtvirtintas. G. Bučiūnas disertacijoje „Slaptas sekimas“ daro išvadą, kad elektroninių ryšių tinklais perduodamos

---

[1077] Gutheil ir Liger, *supra note*, 145.

[1078] Nash Haynes, *Cyber Crime.* (London: ED Tech Press, 2018), 92.

[1079] Kim Zetter, „Hackers Can Control Your Phone Using a Tool That's Already Built Into It“, *WIRED*, žiūrėta 2020 m. rugpjūčio 22 d., https://www.wired.com/2014/07/hackers-can-control-your-phone-using-a-tool-thats-already-built-into-it/.

[1080] Ziccardi, *supra note*, 1077: 221.

[1081] Nash Haynes, *Cyber Crime.* (London: ED Tech Press, 2018), 92.

[1082] Eduardo R. Mendoza, „Network Investigation Techniques: Government Hacking and the Need for Adjustment in the Third-Party Doctrine Comment“, *St. Mary's Law Journal* 49, no. 1 (2018 2017): 237–68. Orin S. Kerr and Sean D. Murphy, „Government Hacking to Light the Dark Web: What Risks to International Relations and International Law Essay“, *Stanford Law Review Online* 70 (2018 2017): 58–69.

informacijos kontrolė paprastai vyksta esamuoju laiku[1083]. Iš visų asmens duomenų rinkimą elektroninėje erdvėje reglamentuojančių BPK straipsnių tik BPK 154 str. reglamentuoja realiuoju laiku vykstančios komunikacijos elektroninėje erdvėje duomenų rinkimą. Tačiau jame yra įtvirtinti du subjektai iš kurių asmens duomenys gali būti renkami – elektroninių ryšių ir paslaugų teikėjai. Prisijungus prie asmeniui priklausančio įrenginio asmens duomenys yra renkami tiesiogiai iš įrenginio, ne iš elektroninių ryšių ar paslaugų teikėjų. Kaip jau minėta, prisijungimu prie elektroninės erdvės yra siekiama „apeiti" ištisiniu šifravimu užšifruotą ir todėl negalimą surinkti iš elektroninių ryšių ir paslaugų teikėjų asmenų komunikaciją elektroninėje erdvėje. Todėl BPK 158 str. sankcionavimas kartu su BPK 154 str. neturėtų būti laikomas teisiškai pagrįstu sprendimu asmens duomenis renkant prisijungus prie elektroninės erdvės įrenginių.

Siūlomas reglamentavimas Lietuvoje. Prisijungimas prie elektroninės erdvės įrenginių vadovaujantis minėtomis Kriminalinės žvalgybos įstatymo ir BPK nuostatomis gali būti laikomas teisėsaugos institucijų veikimu „pilkojoje zonoje" dėl neaiškaus reglamentavimo. Veikimas „pilkojoje zonoje" pats savaime nėra neteisėtas, tačiau asmens teisių užtikrinimo klausimas tokiu atveju lieka atviras. Jungtinės Tautos kritikuoja asmens duomenų rinkimą veikiant „pilkojoje zonoje"[1084]. Autorės nuomone, siekiant išvengti galimo Lietuvos teisėsaugos institucijų veikimo „pilkojoje zonoje", kuomet veiksmai yra atliekami balansuojant tarp teisėtumo ir neteisėtumo ribos, ir atsižvelgiant į tarptautinę asmens duomenų rinkimo el. erdvėje praktiką bei į tai, kad Lietuvos teisėsaugos institucijos dalyvauja tarptautinėse operacijose[1085], Lietuvos teisės aktuose turėtų atsirasti aiški ir atskirai išskirta nuostata, atskira procesinės prievartos priemonė ir kriminalinės žvalgybos informacijos rinkimo būdas, reglamentuojantis teisėsaugos institucijų prisijungimą prie elektroninės erdvės įrenginių. Tačiau kaip tai padaryti, kad nebūtų pažeista teisė į asmens duomenų apsaugą, o teisėsaugos institucijų galios nebūtų nei per daug išplėstos, nei apribotos?

Visų pirma reikėtų apsispręsti kuriame teisės akte tokią galimybę įtvirtinti: Kriminalinės žvalgybos įstatyme, BPK, abejuose teisės aktuose ar priimti atskirą tai reglamentuojantį teisės aktą. Pavyzdžiui, Prancūzijoje teisėsaugos institucijų prisijungimai prie elektroninės erdvės įrenginių yra reglamentuojami Prancūzijos baudžiamojo proceso kodeksu[1086], Vokietijoje – Vokietijos baudžiamojo proceso kodeksu ir Vokietijos federaliniu kriminalinės policijos aktu[1087], Olandijoje – El. nusikaltimų III aktu[1088],

[1083] Bučiūnas, *supra note*, 1076: 72.

[1084] David Kaye, „Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, A/HRC/29/32", 2015, žiūrėta 2020 m. rugsėjo 1 d., https://ap.ohchr.org/documents/dpage_e.aspx?si=A/HRC/29/32

[1085] „Tarptautinės policijos operacijos", *Lietuvos policija*, žiūrėta 2020 m. rugpjūčio 22 d., https://policija.lrv.lt/lt/veiklos-sritys/nusikalstamu-veiklu-atskleidimas-ir-tyrimas/tarptautines-policijos-operacijos

[1086] Gutheil ir Liger, *supra note*, 145: 72.

[1087] *Ibid.,* 77.

[1088] *Ibid.,* 90.

Lenkijoje – Policijos aktu[1089], Didžiojoje Britanijoje – Tyrimo galių aktu[1090]. Teisės akto pasirinkimas priklauso nuo nacionalinių ikiteisminio tyrimo, kriminalinės žvalgybos ir asmens duomenų rinkimo el. erdvėje teisėsaugos tikslais reglamentavimo ypatumų. Kadangi Lietuvoje asmens duomenų rinkimas el. erdvėje nėra reglamentuojamas atskiru teisės aktu, tačiau atskiros nuostatos yra įtvirtintos tiek Kriminalinės žvalgybos įstatyme, tiek BPK, todėl abejais teisės aktais prisijungimo prie elektroninės erdvės įrenginių galėtų būti reglamentuojami. Tokiu atveju visos teisėsaugos institucijos, esant poreikiui, turėtų galimybę atlikti prisijungimo prie elektroninės erdvės įrenginių veiksmus.

Sankcionavimas. Teisminis sankcionavimas yra laikomas viena iš pagrindinių teisės į asmens duomenų apsaugą suvaržymo teisėtumą užtikrinančių priemonių. Visose ES valstybėse narėse, taip pat JAV, Izraelyje ir Australijoje, teisėsaugos institucijų vykdomus prisijungimus prie elektroninės erdvės įrenginių privalo sankcionuoti teismai[1091]. Skirtumai yra tik pačiose sankcionavimo procedūrose bei galimybėje vykdyti prisijungimus prie elektroninės erdvės įrenginių neturint išankstinio teismo sankcionavimo, tačiau privalomai jį gaunant vėliau. Prancūzijoje, Vokietijoje, Italijoje ir Olandijoje kreiptis į teismą dėl prisijungimo prie elektroninės erdvės įrenginių sankcionavimo gali prokuroras. Lenkijoje kreiptis į teismą dėl sankcionavimo gali teisėsaugos institucijos pareigūnas, gavęs prokuroro leidimą. Didžiojoje Britanijoje – teisėsaugos institucijos vadovui sankcionavus pareigūno prašymą, šis gali kreiptis į specialų organą – *Judicial Commissionier* – kuris nepriklauso bendrosios kompetencijos teismui, tačiau yra specialiąja teismine institucija, kurioje pareigas užimti gali tik aukščiausios kvalifikacijos teisėjai[1092]. Lietuvoje prašymus perimti el. ryšių tinklais perduodamą informaciją bendrosios kompetencijos teismui teikia prokuroras. Autorės nuomone, analogiškai turėtų būti reglamentuojama ir prisijungimo prie elektroninės erdvės įrenginių sankcionavimo atveju. Specialiosios kompetencijos teismo, kaip tai yra pvz., JAV, steigti Lietuvoje nėra tikslinga. Siekiant išvengti kritikuojamos situacijos bendrosios kompetencijos teismuose, kad teisėjai neturi kompetencijos įvertinti teisėsaugos institucijų prašymų sankcionuoti el. ryšių tinklais perduodamų asmens duomenų kontrolę[1093]JAV yra įsteigtas patariamasis teismo organas *Amici Curiae*[1094], kurio struktūra pavaizduota 7 lentelėje.

[1089] *Ibid.,* 97.

[1090] Gutheil ir Liger, *supra note*, 145: 103.

[1091] *Ibid.,* 48, 49.

[1092] „Investigatory Powers Act 2016“, 229 str. 9 p., žiūrėta 2020 m. rugpjūčio 22 d., https://www.legislation.gov.uk/ukpga/2016/25/part/8/chapter/1/crossheading/main-functions-of-commissioners/enacted?view=plain . https://www.judiciary.uk/wp-content/uploads/2017/10/jc-announcement-13-new-commissioners-oct2017.pdf

[1093] Gutheil ir Liger, *supra note*, 145: 73.

[1094] „Individuals Designated as Eligible to Serve as an Amicus Curiae Pursuant to 50 U.S.C. § 1803(i)(1)“, *US Courts*, žiūrėta 2020 m. rugpjūčio 22 d., https://www.fisc.uscourts.gov/amici-curiae.

7 lentelė. *JAV FISA teismo patariamojo organo narių struktūra.*

Vardas, pavardė	Pareigos	Organizacija
Paskirti nuo 2015 m.		
Jonathan G. Cedarbaum	Partneris	WilmerHale advokatų kontora
Laura Donohue	Profesorė (teisė)	Georgetown teisės universitetas
Amy Jeffress	Partneris	Arnold & Porter advokatų kontora
Marc Zwillinger	Vadovaujantis partneris	ZwillGen PLLC advokatų kontora
Paskirti nuo 2016 m.		
David S. Kris	Įkūrėjas	Culper Partners LLC advokatų kontora
Paskirti nuo 2018 m.		
Ana I. Anton	Profesorė (IT)	School of Interactive Computing, Georgia Institute of Technology
Ben Johnson	Įkūrėjas ir vadovas	Obsidian Security
Robert T. Lee	Skaitmeninė kriminalistikos ir saugumo pažeidimų diagnostikų vadovas	SANS Institutas

Tokio patariamojo organo steigimas Lietuvoje nėra tikslingas, juolab, kad ir su elektroninių asmens duomenų rinkimu susijusių bylų skaičiai Lietuvoje yra mažesni nei JAV. Tačiau disertacijos autorė, vadovaudamasi Europos Parlamento užsakymu atliktos mokslinės studijos įžvalgomis ir mokslinėje literatūroje keliamoms abejonėms dėl labai specifinės informacinių ir komunikacijos technologijų srities kompetencijos nepakankamumo teisinį išsilavinimą turintiems teisėjams[1095], mano, jog teisėsaugos institucija, teikdama teismui prašymą dėl prisijungimo prie elektroninės erdvės (angl. *law enforcement hacking*) sankcionavimo kartu turėtų pateikti *poveikio privatumui vertinimą*. Vadovaujantis Lietuvos Respublikos asmens duomenų, tvarkomų nusikalstamų veikų prevencijos, tyrimo, atskleidimo ar baudžiamojo persekiojimo už jas, bausmių vykdymo arba nacionalinio saugumo ar gynybos tikslais, teisinės apsaugos įstatymo 25 str. poveikio privatumui vertinimą teisėsaugos institucijos privalo atlikti visais atvejais, kai dėl duomenų tvarkymo rūšies, visų pirma naudojant naujas technologijas, ir atsižvelgiant į duomenų tvarkymo pobūdį, aprėptį, kontekstą ir tikslus žmogaus teisėms ir laisvėms gali kilti didelis pavojus[1096]. Teisėti prisijungimai prie el. erdvės yra teisėsaugos institucijų veiksmai, keliantys didelį pavojų teisei į privatumą ir asmens

[1095] Gutheil ir Liger, *supra note*, 145: 73.

[1096] „Lietuvos Respublikos asmens duomenų, tvarkomų nusikalstamų veikų prevencijos, tyrimo, atskleidimo ar baudžiamojo persekiojimo už jas, bausmių vykdymo arba nacionalinio saugumo ar gynybos tikslais, teisinės apsaugos įstatymas“, *eSeimas*, žiūrėta 2020 m. rugsėjo 27 d., https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/TAIS.397419/asr.

duomenų apsaugą[1097], todėl toks vertinimas turėtų būti atliekamas prieš kreipiantis į teismą dėl prisijungimo prie el. erdvės įrenginių sankcionavimo. Teisėsaugos institucijos, vadovaujantis įstatymo 31 str., privalo turėti asmens duomenų apsaugos pareigūnus, kurių viena iš funkcijų yra pagalba atliekant poveikio privatumui vertinimą[1098]. Duomenų apsaugos pareigūnas taip pat turėtų stebėti kaip laikomasi asmens duomenų apsaugos reikalavimų ir gali atlikti auditus[1099]. Todėl galima teigti, kad duomenų apsaugos pareigūnų vaidmuo turėtų būti aktyvus ir jie, vadovaujantis įstatymu, gali atlikti dalį *ex post* kontrolės funkcijų pačioje teisėsaugos institucijoje ir tikrinti kaip teisėsaugos institucijos tyrimo metu tvarko asmens duomenis. Poveikio privatumui vertinimas būtų informacijos šaltinis teisėjui vertinant procesinės prievartos priemonės taikymo tikslingumą ir įtariamojo bei kitų su juo bendraujančių asmenų teisės į privatumą ir asmens duomenų apsaugą apribojimo proporcingumą. Teisėjams žinių technologinėje srityje įgyti padėtų, jeigu Lietuvos teismo ekspertizės centras kartu su asmens duomenų apsaugos srityje mokslinius tyrimus vykdančiais mokslininkais, reguliariai vestų mokymus ikiteisminio tyrimo teisėjams asmens duomenų rinkimo elektroninėje erdvėje naujoves ir pateiktų mokslinius technologinius ir teisnius vertinimus.

Teisinis ir faktinis pagrindas. Teismas prokuroro prašymus sankcionuoti turėtų tik tuo atveju, jeigu tam yra teisinis ir faktinis pagrindas vykdyti prisijungimus prie elektroninės erdvės įrenginių. Olandijos praktika, kuomet teikiantis prašymą prokuroras jame turi įrodyti, kad prisijungimas prie elektroninės erdvės įrenginių yra proporcinga teisės į asmens duomenų apsaugą suvaržymo priemonė šiuo suvaržymu siekiamų tikslų atžvilgiu[1100], iš vienos pusės turėtų palengvinti teismui sprendimo priėmimą, iš kitos pusės, ir pačiai teisėsaugos institucijai toks privalomas pagrindimas padėtų įsivertint ar tikrai tokia asmens duomenų rinkimo priemonė yra reikalinga ir proporcinga siekiamiems tikslams. Kitas probleminis klausimas į kurį reikėtų atsakyti – ar prisijungimus prie elektroninės erdvės įrenginių leisti visais Kriminalinės žvalgybos įstatyme ir BPK įtvirtintais atvejais, kuomet yra leidžiamas el. ryšių tinklais perduodamų asmens duomenų rinkimas. Atsakymui į šį klausimą yra svarbi tarptautinė praktika ir pats duomenų rinkimo pobūdis. Kriminalinės žvalgybos įstatymas el. asmens duomenis leidžia rinkti iš el. ryšių tinklų paslaugų teikėjų bei kitų juridinių asmenų, BPK – tik iš el. ryšių tinklų ir paslaugų teikėjų. Bendras abejus atvejus siejantis bruožas yra, kad nepriklausomai iš kokių paslaugų el. erdvėje teikėjų asmens duomenys renkami, jie renkami iš tų juridinių asmenų, kurie juos turi arba gali turėti. Prisijungimo prie elektroninės erdvės įrenginių gali vykdyti pačios institucijos arba sutarties su teisėsaugos institucija pagrindu kiti fiziniai ir juridiniais asmenys, turintys

[1097] Gutheil ir Liger, *supra note*, 145.

[1098] „Lietuvos Respublikos asmens duomenų, tvarkomų nusikalstamų veikų prevencijos, tyrimo, atskleidimo ar baudžiamojo persekiojimo už jas, bausmių vykdymo arba nacionalinio saugumo ar gynybos tikslais, teisinės apsaugos įstatymas“, 33 str. 1 d. 3 p., *eSeimas*, žiūrėta 2020 m. rugsėjo 27 d., https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/TAIS.397419/asr.

[1099] „Lietuvos Respublikos asmens duomenų, tvarkomų nusikalstamų veikų prevencijos, tyrimo, atskleidimo ar baudžiamojo persekiojimo už jas, bausmių vykdymo arba nacionalinio saugumo ar gynybos tikslais, teisinės apsaugos įstatymas“, 33 str. 1 d. 2 p., *eSeimas*, žiūrėta 2020 m. rugsėjo 27 d., https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/TAIS.397419/asr.

[1100] Gutheil ir Liger, *supra note*, 145: 12.

tam kompetencijos ir priemonių. Nei vienas iš šių subjektų – teisėsaugos institucija arba prisijungimo prie elektroninės erdvės įrenginių teikiantys fiziniai ar juridiniai asmenys – asmens duomenų neturi. Visus atitinkamoje prisijungimo prie elektroninės erdvės įrenginių vietoje esančius asmens duomenis subjektas perima tik prie jo prisijungus. Prisijungimo prie elektroninės erdvės įrenginių metu perimamų asmens duomenų kiekis yra labai didelis[1101]. Pavyzdžiui, prisijungus prie elektroninės erdvės įrenginių į mobilųjį telefoną gaunama visa (įskaitant ištrintą) jame esanti informacija, apimanti visų, kuriais konkretus asmuo naudojasi, paslaugų el. erdvėje teikėjų turimus duomenis. Pavyzdžiui, SMS žinutes (tarkim paslaugų teikėjas Telia), neužkoduotas Viber žinutes (paslaugų teikėjas Viber), neužkoduotas WhatsApp žinutes (paslaugų teikėjas WhatsApp), neužkoduotus el. laiškus (tarkim, paslaugų teikėjas Gmail), nuotraukas (tarkim, paslaugų teikėjas Samsung), adresatų sąrašą ir informaciją apie juos (tarkim, paslaugos teikėjas Samsung) ir kt. Minėti asmens duomenys yra istorinio pobūdžio. Tačiau, priklausomai nuo įrenginio prie kurio prisijungiama, prisijungus galima tą įrenginį valdyti, rinkti realiuoju metu per įrenginį gaunamus asmens duomenis ir netgi tuos asmens duomenis ištrinti ar pakeisti[1102]. Dėl didelio istorinio pobūdžio ir esamuoju laiku perimamų asmens duomenų (ypač turinio pobūdžio asmens duomenų) kiekio Lietuvos teisėsaugos institucijos prisijungimus prie elektroninės erdvės įrenginių turėtų būti leidžiama vykdyti ne visais dabartiniuose Kriminalinės žvalgybos įstatymo 10 str. 1 d. ir BPK 158 str. įtvirtintais atvejais. ES valstybių narių praktika šiuo klausimu yra skirtinga. Pavyzdžiui, Italijoje teisėsaugos institucijos teisę prisijungti prie elektroninės erdvės įrenginių turi tik tirdamos su organizuotu nusikalstamumu susijusius nusikaltimus[1103]. Visiškai priešingas yra Olandijos pavyzdys. Čia teisėsaugos institucijos turi teisę prisijungti prie elektroninės erdvės įrenginių į el. erdvę tirdamos nusikaltimus įtvirtintus Olandijos baudžiamojo proceso kodekso 67 str. 1 d. t. y. visus nusikaltimus, kurių bausmė yra ne trumpesnė nei 3 metai laisvės atėmimo bei kitas nusikalstamas veikas numatytas tame straipsnyje[1104]. Pirmasis variantas – Italijos – yra labai siauras, Olandijos – pernelyg platus. Tačiau abiem jiems bendras bruožas yra tas, kad prisijungimus prie elektroninės erdvės įrenginių vykdyti galima tik nusikalstamų veikų tyrimo ir prevencijos tikslais. Šis asmens duomenų rinkimo el. erdvėje būdas nėra taikomas asmenų, nusikalstamu būdu įgyto turto legalizavimo paieškai ir kitiems Kriminalinės žvalgybos įstatyme ir BPK įtvirtintiems tikslams, išskyrus grėsmę žmogaus gyvybei, laisvei ir nacionaliniam saugumui. Toks atvejis yra įtvirtintas Vokietijos Federal Criminal Police Office Act[1105]. Tačiau minėtame Vokietijos teisės akte nėra

[1101] Pierluigi Paganini, „Ennetcom – Dutch Police confirmed to have decrypted BlackBerry PGP messages in a criminal case", *Security Affairs*, žiūrėta 2020 m. rugpjūčio 22 d., https://securityaffairs.co/wordpress/57036/cyber-crime/blackberry-pgp-messages.html.

[1102] „Pay No Attention to That Man Behind the Curtain – Exposing and Challenging Government Hacking for Surveillance, žiūrėta 2020 m. rugsėjo 9 d., https://privacyinternational.org/sites/default/files/2018-06/Pay%20No%20Attention%20to%20That%20Man%20Behind%20the%20Curtain%20-%20Exposing%20and%20Challenging%20Government%20Hacking%20for%20Surveillance.pdf .

[1103] Gutheil ir Liger, *supra note*, 145: 50.

[1104] *Ibid.*, 93.

[1105] Gutheil ir Liger, *supra note*, 145: 79.

įtvirtintos nuostatos, kad teisėsaugos institucijos prisijungimus prie elektroninės erdvės įrenginių gali vykdyti be išankstinio teisminio sankcionavimo, kas būtų aktualu grėsmės asmens gyvybei atveju. Autorės nuomone, Prancūzijos baudžiamojo proceso kodekse yra įtvirtintas optimaliausias nusikalstamų veikų sąrašas, kurių atžvilgiu galima vykdyti prisijungimo prie elektroninės erdvės įrenginių veiksmus – tai sunkūs ir labai sunkūs nusikaltimai bei su organizuotu nusikalstamumu ir terorizmu susiję nusikaltimai. Lygiai taip pat, kaip ir masiniam asmens duomenų rinkimui iš el. ryšių paslaugų ir paslaugų el. erdvėje teikėjų terorizmas buvo pateisinimo priemone, tokia pačia priemone jis yra laikomas ir el. prisijungimo prie elektroninės erdvės įrenginių reikalingumo pateisinimui[1106]. Autorės nuomone, Kriminalinės žvalgybos įstatyme bei BPK taip pat galėtų būti įtvirtinta nuostata prisijungimus prie elektroninės erdvės įrenginių leidžianti vykdyti tik sunkių ir labai sunkių nusikaltimų, su organizuotu nusikalstamumu ir terorizmu susijusių nusikalstamų veikų atveju. Siekiant neužkirsti kelio pasinaudoti galimybe prisijungti prie elektroninės erdvės įrenginių tuo atveju, kai gresia pavojus žmogaus gyvybei ar sveikatai, visuomenės ar valstybės saugumui, tokią nuostatą taip pat reikėtų įtvirtinti ir Kriminalinės žvalgybos įstatyme bei BPK. Kadangi minėtais atvejais operatyvumas ir laikas įgyja ypatingą svarbą, šiuo vieninteliu atveju turėtų būti sudaryta galimybė vykdyti prisijungimus prie elektroninės erdvės įrenginių neturint išankstinio teismo sankcionavimo[1107]. Tačiau jis turėtų būti gautas, analogiškai Kriminalinė žvalgybos įstatyme ir BPK įtvirtintiems atvejams – per 24 val.

El. erdvės apibrėžimo ir jos elementų apimties aktualumas labiausiai išryškėja būtent prisijungimo prie elektroninės erdvės įrenginių reglamentavime. Šiuo atveju nebeužtenka el. erdvę apibrėžti kaip tinklų tinklą, nes tokiu atveju yra neaišku ar kas tą tinklų tinklą sudaro ir prie ko teisėsaugos institucijos gali prisijungt. Todėl analizuojant prisijungimus prie elektroninės erdvės įrenginių svarbia tampa pirmoji disertacijos dalis, kurioje yra pateikiamas el. erdvės apibrėžimas ir jos apimtis. Šiame disertacijos poskyryje reikia apibrėžti prie kokių elektroninės erdvės įrenginių teisėsaugos institucijos gali prisijungti: visą el. erdvę ar tik į tam tikras jos dalis. Prancūzijos BPK suteikia teisę prisijungti prie asmenų kompiuterių. Vokietijos teisėsaugos institucijos turi teisę prisijungti prie informacinių technologijų sistemos, Lenkijos – prie asmens duomenų saugojimo įrenginių (angl. data storage media), telekomunikacijų įrenginius, informacijos perdavimo ir komunikacijos sistemas. Didžiojoje Britanijoje bei JAV yra leidžiama rinkti duomenis iš įrenginių, nedetalizuojant jų tipo[1108]. Prancūzijos BPK atrodo esantis siauriausios apimties. Tačiau, tikėtina, kam kompiuterio sąvoka yra suprantamai plečiamai, pvz., kaip tai suprantama Talino vadove[1109] ir apima ir kitus el. erdvės įrenginius ne vien tik asmeninius kompiuterius. Pvz. išmaniajame

[1106] *Ibid.,* 46.

[1107] „Venice Commission Opinion No. 839/ 2016, Poland: On the Act of 15 January 2016 Amending the Police Act and Certain Other Acts“, *Council of Europe*, žiūrėta 2020 m. rugpjūčio 22 d., https://www.venice.coe.int/webforms/documents/default.aspx?pdffile=CDL-AD(2016)012-e.

[1108] Gutheil ir Liger, *supra note*, 145: 45.

[1109] „Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations | Humanitarian Law“, *Cambridge University Press.*

šaldytuve taip pat yra integruotas kompiuteris, prie kurio galima prisijungti[1110]. Lenkijoje pasirinktas el. erdvės komponentų sąrašas taip pat yra apimantis beveik visą ar netgi visą el. erdvę. Autorės nuomone, siekiant išvengti dviprasmybių sąvokose, nėra tikslo Lietuvos teisės aktuose detalizuoti el. erdvės komponentų į kuriuos teisėsaugos institucijoms būtų suteikta teisė prisijungti prie elektroninės erdvės įrenginių. Pakanka tai įvardinti įrenginiais.

Prisijungus prie atitinkamo el. erdvės komponento galima perimti ne tik tuo metu jame esančius asmens duomenis (istorinio pobūdžio asmens duomenys), bet ir toliau rinkti duomenis realiuoju laiku bei, priklausomai nuo el. erdvės komponentą prie kurio prisijungiama, jį gali fiziškai valdyti, pvz. įjungti kamerą ir tokiu būdu per mobilųjį įrenginį stebėti aplinką, daryti garso įrašus ir t. t.[1111]. Įrenginys prie kurio prisijungiama, yra užvaldomas ir gali būti paverčiamas šnipinėjimo įrankiu. Iš visų asmens duomenų rinkimo el. erdvėje būdų, prisijungimai prie elektroninės erdvės įrenginių, yra labiausiai pažeidžiantys teisę į asmens duomenų apsaugą, o asmens duomenų apimtys ir pobūdis gerokai viršija tuos asmens duomenis, kuriuos teisėsaugos institucijos galėtų surinkti turėdamos ištisinio šifravimo kodą. Todėl prisijungimai prie elektroninės erdvės įrenginių turėtų būti leidžiami tik tada, kai teismui yra pagrindžiama, kad kitais būdais surinkti informacijos neįmanoma, o trukmė kiek leisti vykdyti prisijungimus prie elektroninės erdvės įrenginių, turi būti ypač griežtai teismo kontroliuojama. Laikotarpiai, kurių metu teisėsaugos institucijos gali likti prisijungę prie elektroninės erdvės įrenginių, yra skirtingi skirtingose Valstybėse. Pavyzdžiui, Prancūzijoje teismas prisijungimus prie elektroninės erdvės įrenginių gali sankcionuoti iki 4 mėn. laikotarpiui. Šis laikotarpis, esant pagrindui ir poreikiui, gali būti pratęstas net iki 2 metų. Vokietijoje teismas gali sankcionuoti 3 mėn. laikotarpiui. Šis laikotarpis gali būti pratęstas vieną kartą ne ilgesniam nei dar 3 mėn. laikotarpiui. Skirtumai tarp laikotarpių yra labai dideli. Tačiau tai galima pateisinti skirtinga prisijungimų prie elektroninės erdvės įrenginių apimtimi. Prisiminkime, kad Vokietijoje teisėsaugos institucijos gali prisijungti prie visos informacinių technologijų sistemo, Prancūzijoje – tik prie kompiuterių. Tikėtina, kad kompiuteriai Prancūzijos PBK prasme yra aiškinami plačiąja prasme analogiškai Talino vadovui[1112], tačiau net ir tokiu atveju, kompiuterio sąvoka neapima visos informacinių technologijų sistemos. Vokietijoje maksimali prisijungimo prie elektroninės erdvės įrenginių sankcionavimo trukmė yra 6 mėn., tačiau apimtys yra didesnės. Kriminalinės žvalgybos įstatyme nėra įtvirtintas terminas meta duomenų rinkimui. Jis yra įtvirtintas tik turinio duomenų rinkimui – 3 mėn. su galimybe pratęsti iki 12 mėn., o esant tam tikroms aplinkybėms ir iki 2 metų. BPK 154 str. 4 d. yra įtvirtinta, kad el. ryšių tinklais perduodamos informacijos kontrolė gali trukti iki

[1110] Colin Neagle, „Smart Refrigerator Hack Exposes Gmail Account Credentials“, *Network World*, , 2015, žiūrėta 2020 m. rugpjūčio 22 d., https://www.networkworld.com/article/2976270/smart-refrigerator-hack-exposes-gmail-login-credentials.html.

[1111] „„Bulk hacking‘ by UK spy agencies is illegal, high court told“, *The Guardian*, žiūrėta 2020 m. rugpjūčio 22 d., https://www.theguardian.com/technology/2019/jun/17/liberty-mounts-latest-court-challenge-to-snoopers-charter-mi5-gchq.

[1112] „Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations | Humanitarian Law“, *Cambridge University Press*.

6 mėn. Šis terminas gali būti pratęstas dar 3 mėn. laikotarpiui. Lietuvos teisės aktuose prisijungimo prie elektroninės erdvės įrenginių reglamentavimo kaip prisijungimo prie bent kurio įrenginio t. y. visą el. erdvės sistemą atveju šių veiksmų trukmę reikėtų abejuose teisės aktuose, vadovaujantis Vokietijos pavyzdžiu, reikėtų apriboti iki 3 mėn. su galimybe pratęsti dar maksimaliam 3 mėn. laikotarpiui.

Paprastai labiausiai baiminamasi, kad asmens duomenis el. erdvėje teisėsaugos institucijas renka apie visus asmenis, t. y. kad teismai sankcionuoja masinį asmens duomenų rinkimą. Pvz., teigiama, kad Didžiosios Britanijos Investigatory Powers Act įteisdamas prisijungimus prie elektroninės erdvės įrenginių, kartu įteisino ir masinius prisijungimus prie elektroninės erdvės įrenginių ne Didžiojoje Britanijoje esančių asmenų atžvilgiu bei prisijungimus prie elektroninės erdvės įrenginių neturint tikslo rinkti konkretaus asmens duomenis (angl. *bulk hacking*)[1113]. Kita vertus būtent minėto teisės akto pagrindu įsteigtai specialiajai teisminei institucijai pradėjus tikrinti Didžiosios Britanijos žvalgybos institucijos MI5 veiklą, konkrečiai prisijungimus prie elektroninės erdvės įrenginių, buvo nustatyta, jog duomenys yra renkami neteisėtai[1114]. Išvados yra dvi: 1) MI5 yra žvalgybos, ne teisėsaugos institucija. Žvalgybos objektas ir yra užsienyje esantys asmenys. Paprastai žvalgybos, ne teisėsaugos institucijos, vykdo masinio asmens duomenų rinkimo programas. Didžiojoje Britanijoje, skirtingai nuo likusios Europos, šis teisės aktas yra taikomas tiek teisėsaugos, tiek žvalgybos institucijoms; 2) ir iki Investigatory Powers Act veikdama „pilkojoje zonoje“ MI5 vykdė prisijungimus prie elektroninės erdvės įrenginių. Šiuo teisės aktu tai reglamentavus sugriežtėjo kontrolė ir įtvirtintos aiškios procedūros. Kad procedūros būtų aiškios ir nekiltų klausimų dėl masinio asmens duomenų rinkimo įteisinimo, teisės akte turi būti aiškiai apibrėžta, kad tik asmenų ir kartu nustatyta kurių asmenų atžvilgiu teisėsaugos institucijos gali vykdyti prisijungimus prie elektroninės erdvės įrenginių. Tik tokių asmenų atžvilgiu vykdomi prisijungimai prie elektroninės erdvės įrenginių yra laikomi teisėti. Nors piktnaudžiavimo įgaliojimais galimybė negali būti atmetama, tačiau renkant duomenis apie kitus asmenis nei kad buvo sankcionuota teismo, tokių duomenų rinkimas bus laikomas neteisėtu su visomis iš to išplaukiančiomis pasekmėmis teisėsaugos institucijai.

Paprastai prisijungimai prie elektroninės erdvės įrenginių yra galimi tik įtariamųjų atžvilgiu. Tačiau yra šios bendrosios taisyklės išimčių. Pvz. Vokietijoje, prisijungimai prie elektroninės erdvės įrenginių galimi ne tik įtariamojo, bet ir su juo susijusių asmenų atžvilgiu[1115]. Teismo sankcija galioja asmens, o ne atitinkamo el. erdvės komponento atžvilgiu. Pvz., jei prisijungimas prie elektroninės erdvės įrenginių yra sankcionuojamas asmens A atžvilgiu, tai teisėsaugos institucija gali prisijungti ne prie asmens kompiuterio, bet ir į asmens B kompiuterį, jeigu asmuo A asmens B kompiuteriu naudojasi atitinkamu dažnumu, o ne atsitiktinai[1116]. Prisijungiant prie kito, nei asmens

[1113] Natasha Lomas, „UK faces Human Rights challenge to state's bulk hacking abroad“, *TechRunch*, žiūrėta 2020 m. rugpjūčio 22 d., https://techcrunch.com/2016/08/08/uk-faces-human-rights-challenge-to-states-bulk-hacking-abroad/

[1114] „MI5's use of personal data was ‚unlawful', says watchdog“, *BBC News*, žiūrėta 2020 m. rugpjūčio 22 d., https://www.bbc.com/news/uk-48597111.

[1115] Gutheil ir Liger, *supra note*, 145: 50.

[1116] *Ibid.*, 94.

mobilusis įrenginys el. erdvės elementą, pvz. serverį[1117], jo priklausomybės įtariamam asmeniui klausimas negali būti keliamas, nes serveris, priklausomai nuo jo pobūdžio, gali priklausyti paslaugų el. erdvėje teikėjui. Nors prisijungimas prie serverio teoriškai ir bus teisėtas, tačiau serveryje, priklausomai nuo jo pobūdžio, skirtingai nei asmens kompiuteryje ar telefone, paprastai yra saugomi ne vieno asmens duomenys. Prisijungus prie serverio identifikuoti kurie duomenys yra konkretaus įtariamojo ir rinkti tik įtariamojo duomenis, yra neįmanoma arba beveik neįmanoma. Taip pat tokiu atveju yra pažeidžiama ir paslaugų el. erdvėje teikėjo bei juridinio asmens, kuriam priklauso serveris, nuosavybės teisė. Todėl, autorės nuomone, prisijungimai prie kitų nei įtariamajam ar kitam su juo susijusiam fiziniam asmeniui priklausančius įrenginiu, turėtų būti leidžiami tik tuo atveju, kai teisėsaugos institucija kreipėsi į atitinkamus duomenis turintį juridinį asmenį, tačiau šis informacijos nepateikė arba atsisakė ją pateikti. Lietuvos teisės aktuose – Kriminalinės žvalgybos įstatyme ir BPK – reikėtų įtvirtinti analogiškas nuostatas, nors BPK procesines prievartos priemones leidžia taikyti ir nuteistųjų atžvilgiu, o Kriminalinės žvalgybos objektu gali būti nusikalstama veika pati savaime.

Teritorija. Jurisdikcijos internete tematika susilaukia didelio mokslininkų dėmesio[1118]. Šiam klausimui spręsti netgi yra įsteigtas Tarptautinis Jurisdikcijos internete politikos forumas[1119]. Tačiau jurisdikcijos internete ribų klausimas iki šiol lieka atviras. Supaprastintai problema yra ta, kad asmens duomenys fiziškai gali būti bent kurioje pasaulio šalyje, o teismai ir teisėsaugos institucijos jurisdikciją turi tik savo šalyje. Konvencijoje dėl elektroninių nusikaltimų yra įtvirtintas teritorialumo principas, reiškiantis, kad teisėsaugos institucijos kitoje valstybėje esančius asmens duomenis gali rinkti vadovaudamiesi Tarptautinėmis sutartimis arba tarpusavio pagalbos susitarimais. Tokios praktikos laikosi ir Lietuvos Aukščiausiasis Teismas 2019 m. gegužės 22 d. nutartyje Nr. 2K-90-303/2019[1120]. Šioje byloje teismas konstatavo, kad teisėsaugos institucijos privalo pranešti kitai valstybei narei apie elektroninių ryšių tinklais perduodamos informacijos perėmimą, kai asmuo yra pastarosios valstybės teritorijoje. Asmens duomenų rinkimas per tarpusavio pagalbos sutartis ir susitarimus yra neefektyvus[1121]. Efektyviausia būtų, jeigu teisėsaugos institucijos turėtų teisę peržengti savo valstybių ribas rinkdamos asmens duomenis el. erdvėje. Didžiosios pasaulio paslaugų el. erdvėje tiekėjos – Google, Facebook, Apple ir Microsoft – tam tikrus metaduomenis ES teisėsaugos institucijoms išduoda tiesiogiai, šioms nesinaudojant tarpusavio pagalbos sutartimis ir susitarimais (plačiau apie tai IV disertacijos skyriuje[1122]). Tačiau

---

[1117] „Ethical Hacking: How To Hack A Web Server“, *Infosec Resources*, žiūrėta 2020 m. rugpjūčio 22 d., https://resources.infosecinstitute.com/category/certifications-training/ethical-hacking/attacking-web-servers-and-applications/#gref.

[1118] Pvz. Steverson, Koops, BJ & Goodwin, MEA. 2014. *Cyberspace, the cloud, and cross-border criminal investigation. The limits and possibilities of international law*, The Hague/Tilburg: WODC/TILT, available at https://ssrn.com/abstract=2698263.

[1119] „Internet and Jurisdiction Policy Network“, žiūrėta 2020 m. rugpjūčio 22 d. https://www.internetjurisdiction.net/.

[1120] „Lietuvos Aukščiausiojo Teismo 2019 m. gegužės 22 d. nutartis Nr. 2K-90-303/2019“, *eTeismai*, žiūrėta 2020 m. rugsėjo 9 d., https://eteismai.lt/byla/39877772051198/2K-90-303/2019.

[1121] Bert-Jaap Koops ir Morag Goodwin, „Cyberspace, the Cloud, and Cross-Border Criminal Investigation. The Limits and Possibilities of International Law“, *SSRN Electronic Journal*, 2014, doi:10.2139/ssrn.2698263.

[1122] Gutheil ir Liger, *supra note*, 145: 29.

el. komunikacijos turinį iš minėtų paslaugų teikėjų galima gauti tik vadovaujantis tarpusavio pagalbos sutartimis ir susitarimais.

Teigiama, kad teisėsaugos institucijos paprastai nežino kur atitinkamas įrenginys fiziškai yra, ypatingai tais atvejais, kai prisijungiama prie tamsiojo interneto[1123]. Tarkim, naudojantis VPN galima pakeisti informaciją apie įrenginio, pvz. kompiuterio ar mobilaus telefono, IP adresą, kuris parodo fizinio buvimo vietą. Tikroji įrenginio vieta sužinoma tik į prie jo prisijungus. Prisijungimo prie elektroninės erdvės įrenginių metu, priklausomai nuo naudojamos atakos pobūdžio, gali būti renkami tiek metaduomenys, tiek turinys. Prisijungimo prie elektroninės erdvės įrenginių atveju asmens duomenys yra renkami iš įrenginio arba naudojantis įrenginiu, prie kurio prisijungiama, ne iš paslaugų el. erdvėje teikėjo. Atitinkamo įrenginio buvimo vieta paprastai sužinoma tik prie jo prisijungus, tačiau net ir žinant įrenginio vietą, asmens duomenų buvimo vieta gali išlikti nežinoma. Asmens duomenų buvimo vieta gali būti ne įrenginyje, prie kurio prisijungiama (pavyzdžiui, tuo atveju, jeigu duomenys yra laikomi debesyje (angl. *the cloud*) ir kitoje valstybėje, nei ta, kurioje fiziškai yra įrenginys. Nevisais atvejais ir paslaugų el. erdvėje teikėjai gali žinoti, kur yra asmens duomenų buvimo vieta[1124]. Asmens duomenų judėjimo el. erdvėje technologiniai ypatumai ir JAV patirtis (plačiau apie tai I disertacijos skyriuje) rodo, kad apriboti prisijungimo prie elektroninės erdvės įrenginių reglamentavimą tik savo šalies teritorija yra netikslinga[1125]. Pavyzdžiui, Olandijos įstatymo, reglamentuojančio prisijungimą prie elektroninės erdvės įrenginių, aiškinamajame akte yra nurodyta, kad teisėsaugos institucija gali prisijungti ir prie kitoje valstybėje esantį serverį, jeigu prieš prisijungdama ji nežino to serverio buvimo vietos. Visgi, jeigu serverio buvimo vieta teisėsaugos institucijai yra žinoma, tuomet ji privalo kreiptis į atitinkamos valstybės teisėsaugos instituciją pagal tarpusavio pagalbos sutartis. Tačiau jeigu kitos valstybės teisėsaugos institucija negali suteikti pagalbos pagal tarpusavio pagalbos prašymą arba į jį nereaguoja, tuomet net ir žinodamos serverio buvimo vietą, kuri yra užsienyje, teisėsaugos institucijos gali prie jo prisijungti[1126]. Tiek JAV, tiek Europos mokslininkai baiminasi, kad galimybė prisijungti prie elektroninės erdvės įrenginių, kurių buvimo vieta yra nežinoma, sudaro sąlygas piktnaudžiauti šia teise ir neteisėtai stebėti užsienyje esančius asmenis[1127]. Tačiau užkirsti kelią teisėsaugos institucijų piktnaudžiavimui vykdant prisijungimus prie elektroninės erdvės įrenginių yra kitų priemonių (*ex ante, ex post* kontrolė). Apribojimas teritorija nėra proporcinga teisių apsaugojimo priemone. Todėl atsižvelgdama į asmens duomenų judėjimo el. erdvėje ypatumus, autorė mano, kad Kriminalinės žvalgybos įstatymas ir BPK neturėtų prisijungimo prie elektroninės erdvės įrenginių

[1123] Mendoza, *supra note*,1083.

[1124] „Cloud Computing and cybercrime investigations: Territoriality vs. the power of disposal? Discussion paper", *Council of Europe*, 5, žiūrėta 2020 m. rugsėjo 9 d., https://rm.coe.int/16802fa3df. Bert-Jaap Koops ir Morag Goodwin, *Cyberspace, the cloud, and cross-border criminal investigation. The limits and possibilities of international law*, The Hague/Tilburg: WODC/TILT, 2014, žiūrėta 2020 m. rugsėjo 9 d., https://www.wodc.nl/binaries/2326-summary_tcm28-73008.pdf.

[1125] Salles, *supra note*, 1055.

[1126] Gutheil ir Liger, *supra note*, 145: 94.

[1127] Lerner, *supra note*, 1054. O'Leary, *supra note*, 1054. Vaciago ir Ramalho, *supra note*, 1064. Salles, *supra note*, 1055.

į el. erdvę riboti tik Lietuvos Respublikos teritorija, tačiau teisėsaugos institucija per prokurorą teikdama prašymą teismui, privalo įrodyti, kad įrenginio buvimo vietos nustatyti neįmanoma.

***Ex post* kontrolė.** Prisijungimai prie elektroninės erdvės įrenginių yra labiausiai teisę į asmens duomenų apsaugą ribojanti priemonė iš visų teisėsaugos taikomų. Tam kad išlaikyti balansą tarp teisės į asmens duomenų apsaugą užtikrinimo ir teisėto bei be pagrindo nevykdomo prisijungimo prie elektroninės erdvės įrenginių, ne mažiau nei išankstinė yra svarbi ir po prisijungimo prie elektroninės erdvės įrenginių veiksmų pabaigos vykdoma teisėsaugos institucijų kontrolė. Šiuo metu visose ES valstybėse yra naudojami du *ex post* kontrolės mechanizmai:

1) asmenų informavimas – asmuo apie jo atžvilgiu vykdytus prisijungimo prie elektroninės erdvės įrenginių veiksmus privalo būti informuotas nepriklausomai nuo to ar jo atžvilgiu yra pradėtas ikiteisminis procesas ir byla perduodama teisminiam nagrinėjimui. Toks asmuo taip turi būti informuotas apie jo teisę apskųsti teisėsaugos institucijos veiksmus. Tai ne tik skatintų juridinius asmenis bendradarbiauti su teisėsaugos institucija teikiant teisėsaugos institucijos prašomą informaciją tokiu būdu išvengiant teisėsaugos institucijos prisijungimų prie elektroninės erdvės įrenginių, bet ir kartu juridiniai asmenys būtų informuoti apie jų turimas įrenginių spragas.
2) specialios priežiūros institucijos informavimas – informacija apie vykdytus prisijungimus prie elektroninės erdvės įrenginių, jų metu rinktų asmens duomenų apimtis ir panaudojimą privalo būti teikiama išoriniam kontrolės organui. Lenkijoje yra suformuotas specialus Seimo narių organas ir vykdoma Parlamentinė kontrolė. Vokietijoje generalinis prokuroras informaciją apie prisijungimus prie elektroninės erdvės įrenginių privalo teikti Federalinei teisingumo įstaigai. Įstaigai pateiktos ataskaitos yra viešos[1128]. Lietuvoje kriminalinę žvalgybą ir ikiteisminį tyrimą kontroliuoja prokuratūra. Parlamentinė kontrolė yra taikoma žvalgybai. Kaip jau minėta anksčiau, iš dalies *ex post* kontrolę turėtų atlikti institucijų asmens duomenų apsaugos pareigūnai. Kita institucija, kurios funkcijos teisėsaugos srityje buvo sustiprintos Teisėsaugos tikslais tvarkomų asmens duomenų apsaugos direktyva ir šios direktyvos pagrindu priimtu įstatymu yra Valstybinės asmens duomenų apsaugos inspekcija (toliau – VDAI). VDAI nuostatų 2 p. yra įtvirtinta, kad inspekcijos paskirtis yra prižiūrėti, kad būtų apsaugotos fizinių asmenų pagrindinės teisės ir laisvės tvarkant asmens duomenis bei sudarytos palankesnės sąlygos laisvam asmens duomenų judėjimui Europos Sąjungoje. Nuostatų 10.2. p. numatyta, kad vienas iš VDAI veiklos tikslų yra stebėti ir užtikrinti Asmens duomenų, tvarkomų nusikalstamų veikų prevencijos, tyrimo, atskleidimo ar baudžiamojo persekiojimo už jas, bausmių vykdymo arba nacionalinio saugumo ar gynybos tikslais, teisinės apsaugos įstatymo (į kurį buvo perkeltos Teisėsaugos tikslais tvarkomų asmens duomenų apsaugos direktyvos nuostatos) taikymą. Siekdama šio tikslo VDAI nagrinėja asmenų skundus ir, remdamasi

[1128] Gutheil ir Liger, *supra note*, 145: 53.

skunduose pateikta informacija, tikrina asmens duomenų tvarkymo teisėtumą bei priima sprendimus dėl asmens duomenų tvarkymo pažeidimų (Nuostatų 12.1 p.) . Asmens duomenų, tvarkomų nusikalstamų veikų prevencijos, tyrimo, atskleidimo ar baudžiamojo persekiojimo už jas, bausmių vykdymo arba nacionalinio saugumo ar gynybos tikslais, teisinės apsaugos įstatymo 15 str. yra įtvirtinta VDAI teisė, gavus asmens skundą, atlikti patikrinimus ir teisėsaugos institucijų priimtų sprendimų. Todėl vadovaujantis galiojančiu teisiniu reglamentavimu galima teigti, kad dalį ex post kontrolės funkcijų VDAI šiuo metu atlieka. Nuomonė, kad valstybinės asmens duomenų apsaugos institucijos galėtų atlikti kontrolės institucijos funkcijas vietoje parlamentinės ar kitos taikomos yra išsakyta ir vieno iš žymiausių Europoje asmens duomenų apsaugos teisėsaugos ir žvalgybos srityje mokslininkų – Paul de Hert[1129]. Šiuo metu Lietuvoje pagrindinis ikiteisminio tyrimo kontrolę po procesinių veiksmų atlikimo atliekantis subjektas yra prokuroras bei teismas[1130], kriminalinės žvalgybos – Kriminalinės žvalgybos parlamentinės kontrolės komisija[1131]. Visgi jei kriminalinės žvalgybos parlamentinė kontrolė pasireiškia atliktų kriminalinės žvalgybos veiksmų vertinimu, tai ikiteisminio tyrimo metu teismo funkcijos vertinant ar teisėtai buvo taikomos procesinės prievartos priemonės pasireiškia tik gavus skundą dėl ikiteisminio tyrimo įstaigos veiksmų. BPK įtvirtintos prokuroro kontrolės funkcijos taip pat neapima atliktų procesinių veiksmų vertinimo. A. Panomariovas teigia, tai, kad tada, kai ikiteisminį tyrimą atlieka kuri nors iš BPK 165 str. įvardintų ikiteisminio tyrimo institucijų, jokiam šioje ikiteisminio tyrimo institucijoje dirbančiam asmeniui nesuteikta procesinė teisė kontroliuoti asmens, atliekančio toje institucijoje ikiteisminį tyrimą, procesinių veiksmų ir jo priimamų procesinių sprendimų yra ydinga[1132]. Disertacijos autorės nuomone, teisėsaugos institucijos asmens duomenų apsaugos pareigūnas turėtų būti tas asmuo, kuris turi teisę kontroliuoti, kaip konkrečių ikiteisminių tyrimų metu yra užtikrinama teisė į asmens duomenų apsaugą, o prisijungimų prie el. erdvės įrenginių metu tokia kontrolė turėtų būti privaloma kiekvienam iš šios procesinės prievartos priemonės taikymo atvejų. Svarstytinas yra ir VDAI *ex post* kontrolės funkcijų išplėtimas ikiteisminio tyrimo metu, tačiau pačios teisėsaugos institucijos asmens duomenų apsaugos pareigūno aktyvus įtraukimas būtų paprastesnis ir keliantis mažiau diskusijų dėl konfidencialumo įsipareigojimo užtikrinimo. Juolab, kad Lietuvos Respublikos asmens duomenų, tvarkomų nusikalstamų veikų prevencijos, tyrimo, atskleidimo ar baudžiamojo persekiojimo už jas, bausmių vykdymo arba nacionalinio saugumo ar gynybos tikslais, teisinės apsaugos įstatymo 33 str. tokią teisę netiesiogiai suteikia.

[1129] Malgieri ir de Hert, *supra note*, 976.

[1130] Artūras *Panomariovas,* „Ikiteisminio tyrimo procesinės kontrolės teoriniai-diskusiniai aspektai“, *Jurisprudencija,* t. 59, Nr.51, 2004, 34.

[1131] „Parlamentinė kontrolė“, *Lietuvos Respublikos Seimas*, žiūrėta 2020 m. rugsėjo 27 d., https://www.lrs.lt/sip/portal.show?p_r=36421&p_k=1.

[1132] Panomariovas, *op. cit.*, 1130: 31.

Techninių prisijungimo prie elektroninės erdvės įrenginių įrankių pašalinimas iš įrenginio baigus vykdyti prisijungimo prie elektroninės erdvės įrenginių operaciją taip pat turėtų būti vienas teisėsaugai keliamų privalomų reikalavimų. Olandijos, Vokietijos, Prancūzijos ir Italijos teisės aktuose yra įtvirtintos panašios nuostatos, kad techninės prisijungimo prie elektroninės erdvės įrenginių priemonės privalo būti pašalintos iš įrenginio, prie kurio buvo prisijungta, iškart po prisijungimo operacijos veiksmų pabaigos. Jeigu techninių priemonių visiškai ar iš dalies neįmanoma pašalinti arba jeigu pašalinimas keltų grėsmę renginio ar jame esančių asmens duomenų saugumui, tuomet teisėsaugos institucija privalo apie tai informuoti įrenginio savininką ar administratorių bei pateikti jam informaciją, kaip jam pačiam teisėsaugos institucijos naudotas technines priemones pašalinti iš savo įrenginio[1133].

Apibendrinimas:

1. *Prisijungimo prie elektroninės erdvės įrenginių galimybė yra įtvirtinta šešiose ES valstybėse narėse: Lenkijoje, Prancūzijoje, Vokietijoje, Olandijoje, Italijoje ir Didžiojoje Britanijoje. Disertacijos autorės nuomone, nors teisėsaugos vykdomi prisijungimai prie elektroninės erdvės įrenginių kelia didelę grėsmę teisei į asmens duomenų apsaugą, tačiau tam tikrų kovos su nusikalstamumu arba nacionalinio saugumo užtikrinimo įrankių buvimas vienose valstybėse ir nebuvimas kitose, kelia dar didesnę grėsmę, ypač nacionaliniam saugumui, ir kartu sąlygoja valstybių atsilikimą. Svarbu yra ne uždrausti teisę į asmens duomenų apsaugą galinčius pažeisti tiek teisėsaugos, tiek žvalgybos veiksmus, o sukurti teisines priemones, užtikrinančias šios teisės suvaržymo pagrįstumą ir proporcingumą.*
2. *Teisės į asmens duomenų apsaugą suvaržymo pagrįstumas ir proporcingumas prisijungimus prie elektroninės erdvės įrenginių reglamentavusiose valstybėse yra užtikrinamas ex ante ir ex post kontrolės mechanizmais. Ex antre kontrolė apima teisminį sankcionavimą, nusikaltimų, kurių atžvilgiu galima vykdyti prisijungimą prie elektroninės erdvės įrenginių, ribojimą bei prisijungimo prie elektroninės erdvės įrenginių trukmės ribojimą. Ex post kontrolė apima asmens, kurio atžvilgiu buvo vykdomas prisijungimas, informavimą apie šiuos teisėsaugos veiksmus bei informacijos apie prisijungimo veiksmus teikimą išoriniam, teisėsaugos institucijai nepriklausančiam, kontrolės organui.*
3. *Lietuvos teisės aktuose teisėsaugos institucijų galimybės prisijungti prie elektroninės erdvės įrenginių tiesiogiai nėra įtvirtintos. Netiesiogiai tokia galimybe galime laikyti Kriminalinės žvalgybos įstatymo 10 str. 1 d. kriminalinės žvalgybos subjektams leidžiančią atlikti slaptą susižinojimo kontrolę nesinaudojant ūkio subjektų, teikiančių el. ryšius ir (ar) paslaugas paslaugomis ir BPK 154 str. 6 d. nuostatą, leidžiančią ikiteisminio tyrimo institucijoms klausytis asmenų pokalbių, daryti jų įrašus ir kontroliuoti kitą el. ryšių tinklais perduodamą informaciją nesinaudojant el. ryšių tinklų ir paslaugų teikėjų įrenginiais ir paslaugomis. Tačiau prisijungimų prie elektroninės erdvės įrenginių vykdymas vadovaujantis minėtomis teisės aktų nuostatomis galėtų būti laikomas veikimu „pilkojoje zonoje" ir jo teisėtumas yra*

[1133] Gutheil ir Liger, *supra note*, 145: 53.

abejotinas ypač atsižvelgiant į tai, kad Kriminalinės žvalgybos įstatymo 10 str. 1 d. ir BPK 154 str. 6 d. nėra įtvirtintų jokių ex ante ir ex post kontrolės nuostatų, padedančių užtikrinti teisės į asmens duomenų apsaugą suvaržymo pagrįstumą ir proporcingumą. Vadinasi, jeigu Lietuvos kriminalinės žvalgybos įstatymo 10 str. 1 d. ir BPK 154 str. 6 d. pagrindu Lietuvos kriminalinės žvalgybos subjektai arba atitinkamai ikiteisminio tyrimo institucijos vykdytų prisijungimo prie elektroninės erdvės įrenginių, tai tokie institucijų veiksmai galėtų būti kvestionuojami kaip pažeidžiantys teisę į asmens duomenų apsaugą.

4. *Siekiant Lietuvos kriminalinės žvalgybos subjektų ir ikiteisminio tyrimo institucijų galimų teisės į asmens duomenų apsaugą pažeidimų Kriminalinės žvalgybos įstatyme ir BPK turėtų atsirasti atskiras prisijungimo prie elektroninės erdvės įrenginių operacijų reglamentavimas, kurioje turėtų būti įtvirtinti tokie principai*
   - *4.1. privalomas teisminis sankcionavimas:*
     - *4.1.1. prašymą teismui teikia prokuroras pagrįsdamas būtinumą vykdyti prisijungimo prie elektroninės erdvės operaciją ir šių priemonių proporcingumą siekiamiems tikslams bei nurodydamas kokio asmens atžvilgiu tai bus vykdoma, įrenginio, prie kurio ketinama prisijungti buvimo vietą arba pagrindimą, kad buvimo vieta yra nežinoma ir jos neįmanoma nustatyti, planuojamas naudoti technines prisijungimo priemones bei asmens duomenų, kuriuos ketinama perimti pobūdį ir rūšį(is).*
     - *4.1.2. su teikiamu prašymu pateikiamas poveikio privatumui vertinimas;*
     - *4.1.3. Neatidėliotinais atvejais, kai gresia pavojus žmogaus gyvybei, sveikatai visuomenės ar nacionaliniam saugumui, prisijungimus prie elektroninės erdvės įrenginių galima vykdyti be išankstinio teismo sankcionavimo.*
   - *4.2. pavojingų nusikaltimų išskyrimas:*
     - *4.2.1. sunkūs ir labai sunkūs nusikaltimai;*
     - *4.2.2. grėsmė žmogaus gyvybei, sveikatai, visuomenės ar nacionaliniam saugumui.*
   - *4.3. Prisijungimo operacijų terminas turėtų būti apribotas iki 3 mėn. su galimybe pratęsti papildomam 3 mėn. laikotarpiui.*
   - *4.4. Apie prisijungimo prie elektroninės erdvės įrenginių operaciją jai pasibaigus privalo būti informuotas fizinis asmuo, kurio atžvilgiu buvo vykdytas prisijungimas bei juridinis asmuo, jeigu renkant įtariamojo asmens duomenis buvo prsijungta į juridiniam asmeniui priklausantį ar jo administruojamą įrenginį. Tai ne tik skatintų juridinius asmenis bendradarbiauti su teisėsaugos institucija teikiant teisėsaugos institucijos prašomą informaciją tokiu būdu išvengiant teisėsaugos institucijos prisijungimų prie elektroninės erdvės įrenginių, bet ir kartu juridiniai asmenys būtų informuoti apie jų turimas įrenginių spragas.*
   - *4.5. privaloma teisėsaugos institucijos duomenų apsaugos pareigūno kontrolė dėl asmens duomenų apsaugos reikalavimų laikymosi procesinės prievartos taikymo metu surinktų asmens duomenų tvarkymo;*
   - *4.6. Techninės prisijungimo prie elektroninės erdvės įrenginių priemonės privalo būti pašalintos iš įrenginio, prie kurio buvo prisijungta, iškart po įsilaužimo operacijos veiksmų pabaigos. Jeigu techninių priemonių visiškai ar iš dalies neįmanoma*

pašalinti arba jeigu pašalinimas keltų grėsmę renginio ar jame esančių asmens duomenų saugumui, tuomet teisėsaugos institucija privalo apie tai informuoti įrenginio savininką ar administratorių bei pateikti jam informaciją, kaip jam pačiam teisėsaugos institucijos naudotas technines priemones pašalinti iš savo įrenginio.

4.2. Asmens duomenų rinkimas elektroninėje erdvėje žvalgybos tikslais

Nacionalinio saugumo pagrindų įstatymas išskiria dvi nacionalinio saugumo užtikrinimo subjektų kategorijas:

1) valstybė, jos nacionalinio saugumo bei gynybos ir kitos institucijos;
2) piliečiai, jų bendrijos ir organizacijos[1134].

Nors nacionalinį saugumą užtikrinančių institucijų Nacionalinio saugumo pagrindų įstatyme yra įvardinta keletas[1135], žvalgybos ir kontržvalgybos veiklą iš jų vykdo tik dvi: Valstybės saugumo departamentas (toliau – VSD)[1136] ir Antrasis operatyvinių tarnybų departamentas prie Krašto apsaugos ministerijos (toliau – AOTD)[1137].

VSD veiklos tikslas yra apsaugoti valstybę nuo pasikėsinimų, jos suverenitetą ir konstitucinę santvarką[1138], o AOTD – stiprinti krašto apsaugos sistemos saugumą ir šalies gynybinę galią[1139].

VSD žvalgybą ir kontržvalgybą vykdo, kiek tai neapima AOTD veiklos:

1) visuomeninėje politinėje, ekonominėje, mokslo, technologijų, informacinės veiklos srityse;
2) Lietuvos Respublikos valstybės diplomatinės tarnybos ir kitų Lietuvos Respublikos institucijų, veikiančių užsienyje, saugumo srityje;
3) valstybės ir tarnybos paslaptį sudarančios informacijos apsaugos srityje;
4) valstybės valdymui skirtų elektroninių ryšių tinklų įrengimo, eksploatavimo ir jų kriptografinės ir kitos apsaugos srityje[1140].

AOTD žvalgybos ir kontržvalgybos veiklą vykdo:

1) gynybos, karinėje-politinėje, karinėje-ekonominėje, karinėje-technologinėje, karinėje-informacinėje srityse;

[1134] „Lietuvos Respublikos nacionalinio saugumo pagrindų įstatymas“, Antrasis skirsnis, *eSeimas*, žiūrėta 2020 m. rugpjūčio 22 d., https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/TAIS.34169/asr.

[1135] „Lietuvos Respublikos nacionalinio saugumo pagrindų įstatymas“, III dalis, *eSeimas*, žiūrėta 2020 m. rugpjūčio 22 d., https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/TAIS.34169/asr.

[1136] „Lietuvos Respublikos nacionalinio saugumo pagrindų įstatymas“, 20 skyrius *eSeimas*, žiūrėta 2020 m. rugpjūčio 22 d., https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/TAIS.34169/asr.

[1137] „Lietuvos Respublikos nacionalinio saugumo pagrindų įstatymas“, 18 skyrius, *eSeimas*, žiūrėta 2020 m. rugpjūčio 22 d., https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/TAIS.34169/asr.

[1138] „Lietuvos Respublikos nacionalinio saugumo pagrindų įstatymas“, 20 skirsnis, *eSeimas*, žiūrėta 2020 m. rugpjūčio 22 d., https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/TAIS.34169/asr.

[1139] „Antrasis operatyvinių tarnybų departamentas“, *Lietuvos Respublikos krašto apsaugos ministerija*, žiūrėta 2020 m. rugpjūčio 22 d., https://kam.lt/lt/struktura_ir_kontaktai_563/kas_institucijos_567/aotd.html.

[1140] „Lietuvos Respublikos žvalgybos įstatymas“, 8 str. 2 d., *eSeimas*, žiūrėta 2020 m. rugpjūčio 22 d., https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/TAIS.106097/asr.

2) Lietuvos Respublikos krašto apsaugos sistemos institucijų veiklos užsienyje srityje;
3) Lietuvos Respublikos krašto apsaugos sistemos institucijų valstybės ir tarnybos paslaptį sudarančios informacijos apsaugos srityje[1141].

Tiesiogiai pavojų nacionaliniam saugumui keliančių nusikaltimų, pvz. tokių kaip teroro aktų ir kitų nusikaltimų visuomenės saugumui, nusikaltimų žmogiškumui ir karo nusikaltimų, nusikaltimų elektroninių duomenų ir informacinių sistemų saugumui, prevencija nėra žvalgybos objektu. Tačiau VSD ir AOTD turi kriminalinės žvalgybos institucijų teises ir pareigas, kai jų padaliniai atlieka kriminalinės žvalgybos tyrimą[1142]. Kas reiškia, kad VSD ir AOTD gali vykdyti žvalgybą ir nacionalinį grėsmę nacionaliniam saugumui keliančių nusikaltimų prevencijos ir užkardymo tikslais ir kad kriminalinę žvalgybą galima pradėti žvalgybos metu surinktų duomenų pagrindu. Tačiau tai nėra pagrindinis žvalgybos institucijų tikslas ir pagrindinė jų funkcija. Visgi nepriklausomai nuo to ar vykdo žvalgybą, kontržvalgybą ar kriminalinę žvalgybą, EŽTK 8 str. įtvirtinta teisė į asmens duomenų apsaugą galioja. Kaip ji įgyvendinama žvalgybos institucijoms renkant duomenis elektroninėje erdvėje?

Žvalgybos įstatyme yra numatyta, kad įgyvendindamos savo funkcijas žvalgybos institucijos gali:
1) taikyti žvalgybos metodus;
2) Žvalgybos įstatymo nustatyta tvarka atlikti teismo sankcionuojamus veiksmus;
3) gauti iš institucijų, įmonių, įstaigų ir organizacijų žvalgybos institucijų veiklai reikalingą informaciją[1143].

Vadovaujantis Žvalgybos įstatymo 13 str. 1 d. 1 p. bent kuris apygardos teismas sankcionuoja elektroninių ryšių tinklais perduodamos informacijos turinio, susirašinėjimo ir kitokio asmens susižinojimo stebėjimą ir fiksavimą. Įstatyme yra įtvirtinta ir sankcionavimo tvarka: žvalgybos institucijos vadovas ar jo įgaliotas pavaduotojas turi pateikti apygardos teismui:
1) duomenis apie fizinius asmenis (vardas ir pavardė, asmens kodas) arba juridinius asmenis (buveinė, kodas), arba objektus (jų apibūdinimas), kuriems bus taikomi veiksmai;
2) duomenis (motyvus), pagrindžiančius būtinumą taikyti sankcionuojamus veiksmus;
3) duomenys apie galinį įrenginį, kurį naudojant bus perduodama informacija (identifikacinis numeris, pavadinimas ir (arba) galinio įrenginio buvimo adresas), kai numatoma kontroliuoti elektroninių ryšių tinklais perduodamos informacijos turinį;
4) veiksmai, kuriuos prašoma leisti atlikti;
5) prašomų taikyti veiksmų trukmė arba prašomos pateikti informacijos apimtis ir periodas, kai prašoma taikyti šio straipsnio 1 dalies 6 punkte nurodytą veiksmą.

[1141] „Lietuvos Respublikos žvalgybos įstatymas“, 8 str. 3 d., *eSeimas*, žiūrėta 2020 m. rugpjūčio 22 d., https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/TAIS.106097/asr

[1142] „Kriminalinė žvalgyba“, *Lietuvos Respublikos prokuratūra*, žiūrėta 2020 m. rugpjūčio 22 d., https://www.prokuraturos.lt/lt/veiklos-sritys/baudziamasis-persekiojimas/kriminaline-zvalgyba/186.

[1143] „Lietuvos Respublikos žvalgybos įstatymas“, 9 str. 1 d., *eSeimas*, žiūrėta 2020 m. rugpjūčio 22 d., https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/TAIS.106097/asr

Teisiniai asmens duomenų rinkimo pagrindai. Žvalgybos įstatyme yra numatyta, kad duomenis žvalgybos institucijos gali rinti:

1) teismui sankcionavus[1144],
2) vadovaujantis tiesiogiai Žvalgybos įstatyme įtvirtintomis nuostatomis, pavyzdžiui, vadovaudamosi Žvalgybos įstatymo 9 str. 1 d. 4 p. turi teisę gauti iš institucijų, įmonių, įstaigų ir organizacijų žvalgybos institucijų veiklai reikalingą informaciją be teismo sankcionavimo;
3) taip pat, tikėtina, kad žvalgybos institucijos asmens duomenis el. erdvėje gali rinkti vadovaudamosi slaptais žvalgybos metodais, kurių klausimas dėl teisminio sankcionavimo yra valstybės paslaptis kaip ir patys metodai.

Taigi teisinių asmens duomenų rinkimo pagrindų prasme Žvalgybos įstatymas yra lankstus. ES teisė žvalgybos institucijoms yra netaikoma, tačiau EŽTK nuostatos lieka galioti ir žvalgybos institucijų veiklos reglamentavimui. Ar lanksčios Žvalgybos įstatymo nuostatos atitinka EŽTK 8 str. 2 d. įtvirtintus teisės į asmens duomenų apsaugą apribojimo principus? EŽTK 8 str. 2 d. yra nurodyta, kad valstybės institucijos neturi teisės apriboti naudojimosi teise į privatumą, išskyrus įstatymų nustatytus atvejus. EŽTK 8 str. 2 d. nėra minimas privalomas įstatyme įtvirtintų teisės į privatumą suvaržymo atvejų teisminis sankcionavimas, privalomas tik įstatyminis reglamentavimas. Tačiau tai nėra vienintelė sąlyga. Tolimesnė EŽTK 8 str. 2 d. formuluotėje yra įtvirtinta vertinamoji sąlyga – „ir, kai tai būtina demokratinėje visuomenėje valstybės saugumo, visuomenės saugos ar šalies ekonominės gerovės interesams, siekiant užkirsti kelią viešos tvarkos pažeidimams ar nusikaltimams, taip pat žmonių sveikatai ar moralei arba kitų asmenų teisėms ir laisvėms apsaugoti“. Ši EŽTK 8 str. 2 d. formuluotė suponuoja, jog turėtų būti nešališkas arbitras, kuris įvertintų ar įstatyme numatytas teisės į privatumą suvaržymas yra būtinas demokratinėje visuomenėje. Tačiau tiesiogiai nėra pasakyta, kad tas nešališkas arbitras visuomet turėtų būti teismas[1145]. Vadinasi galima daryti prielaidą, kad išimtinai tik teisminis žvalgybos institucijų veiklos el. erdvėje sankcionavimas nėra privalomas. Žvalgybos institucijų veiklai ir jos reglamentavimui galioja ne vien tik EŽTK, bet ir Konstitucija. Konstitucijos 22 str. yra įtvirtinta, kad „informacija apie privatų asmens gyvenimą gali būti renkama tik motyvuotu teismo sprendimu“. Konstitucija galioja Lietuvos Respublikos teritorijoje. Todėl vadovaujantis Konstitucijos 22 str. kontržvalgybos atveju teisminis sankcionavimas yra privalomas, žvalgybos – ne, nes Konstitucijos nuostatų veikimas ir teismų jurisdikcija yra apribota Lietuvos Respublikos teritorija, nors teismo jurisdikcija el. erdvėje yra diskutuotinas klausimas[1146] (plačiau apie tai, kituose disertacijos poskyriuose).

Asmens duomenų rinkimo el. erdvėje atveju, vadovaujantis Žvalgybos įstatymu, teisminio sankcionavimo Lietuvoje nereikia galimai dviem atvejais: 1) kai duomenys

---

[1144] „Lietuvos Respublikos žvalgybos įstatymas“, 9 str. 1 d. 2 p., *eSeimas*, žiūrėta 2020 m. rugpjūčio 22 d., https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/TAIS.106097/asr.

[1145] Europos Žmogaus Teisių Teismo 2013 m. spalio 21 d. sprendimas byloje Janowiec ir kiti prieš Rusiją (Nr. 55508/07 ir 29520/09), žiūrėta 2020 m. rugpjūčio 22 d., https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-110513%22]} .

[1146] Davidson, *supra note*,118.

yra renkami tiesiogiai iš įmonių, įstaigų ir institucijų, ir 2) kai yra taikomi slapti žvalgybos metodai. Informacijos rinkimas iš asmenų yra vykdomas vadovaujantis žvalgybos institucijų vadovų ar įgaliotų žvalgybos pareigūnų raštu. Taigi nešališko arbitro, kuris sankcionuotų žvalgybos institucijų veiksmus, šiuo atveju nėra. Apygardos teismas vaidmenį įgyja tik tada, kai asmuo atsisako suteikti informaciją. Tačiau net ir tokiu atveju, vadovaujantis Žvalgybos įstatymu, jis nekvestionuoja žvalgybos institucijų veiksmų teisėtumo, o tik įpareigoja asmenį atlikti žvalgybos institucijos prašomus veiksmus[1147]. Ir tik tada, jeigu asmuo nesutinka ir su Apygardos teismo įpareigojimu, jo skundas yra nagrinėjamas Apeliaciniame teisme[1148]. Žvalgybos įstatymo 15 straipsnio analizė rodo ne vien tik tai, kad žvalgybos institucijos iš fizinių ir juridinių asmenų duomenis gali rinkti nesankcionuotos jokio nešališko arbitro, bet ir tai, kad asmeniui yra apsunkinama teisės į teisminę gynybą pasinaudojimo galimybė, kadangi žvalgybos institucijų veiksmų teisėtumas yra analizuojamas tik tada, jeigu apskundžiamas Apeliaciniam teismui. Asmens duomenų rinkimo elektroninėje erdvėje atveju turėtų būti taikoma Žvalgybos įstatymo 15 str. 3 d. numatanti, kad duomenys yra renkami pagal su juridiniais asmenimis sudaromas sutartis. Kokio pobūdžio tos sutartys yra – vienkartinio ar nuolatinio – Žvalgybos įstatymas atsakymo nepateikia. Tačiau ši formuluotė primena E. Snowden paviešintą informaciją apie masinį asmens duomenų rinkimą el. erdvėje, kuomet JAV žvalgybos institucija šiuos duomenis rinko sutarčių su įmonėmis pagrindu[1149]. Todėl tam, kad Žvalgybos įstatymo 15 str. nekeltų klausimų dėl atitikimo EŽTK 8 str. reikėtų ją patikslinti numatant, kad Apygardos teismo sankcionavimas yra privalomas visais atvejais, o sutartys su fiziniais asmenimis gali būti pasirašomos taip pat tik jei tokį duomenų rinkimą prieš tai sankcionavo teismas. Tačiau teisminį sankcionavimą numatyti reikėtų tik tuo atveju, jeigu duomenys yra renkami apie tuos asmenis, kurie arba kurių asmens duomenys patenka į Lietuvos Respublikos teismų jurisdikciją.

Be ką tik minėto asmens duomenų rinkimo tiesiogiai iš įmonių, įstaigų ir organizacijų atvejo, manytina, kad žvalgybos institucijos nesankcionuotos asmens duomenis elektroninėje erdvėje gali rinkti taikydamos žvalgybos metodus. Žvalgybos metodas yra apibrėžiamas kaip būdas gauti žvalgybos informaciją[1150]. Žvalgybos įstatyme yra numatyta, kad žvalgybos institucijų veiklos metodai yra nevieši ir jie negali būti atskleidžiami asmenims, nevykdantiems žvalgybos ir kontržvalgybos arba šios veiklos kontrolės ar koordinavimo[1151]. Žvalgybos metodus, jų taikymo tvarką, terminus ir

---

[1147] Jeigu asmuo per žvalgybos institucijos nurodytą terminą nepateikia prašomų duomenų arba atsisako juos pateikti, žvalgybos institucijos turi teisę kreiptis į bet kurį apygardos teismą su prašymu įpareigoti pateikti duomenis, reikalingus žvalgybos institucijų uždaviniams įgyvendinti.

[1148] Apygardos teismo nutartis per 7 dienas nuo nutarties gavimo gali būti skundžiama Lietuvos apeliaciniam teismui. Lietuvos apeliacinis teismas privalo skundą išnagrinėti ir priimti nutartį dėl skundo ne vėliau kaip per 7 dienas nuo skundo gavimo šiame teisme dienos. Lietuvos apeliacinio teismo nutartis įsigalioja jos priėmimo dieną ir yra neskundžiama.

[1149] „How the US Spy Scandal Unravelled“, *BBC News*, 2014, žiūrėta 2020 m. rugsėjo 9 d., https://www.bbc.com/news/world-us-canada-23123964.

[1150] „Lietuvos Respublikos žvalgybos įstatymas“, 9 str. 11 d., *eSeimas*, žiūrėta 2020 m. rugpjūčio 22 d., https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/TAIS.106097/asr.

[1151] „Lietuvos Respublikos žvalgybos įstatymas“, 5 str., *eSeimas*, žiūrėta 2020 m. rugpjūčio 22 d., https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/TAIS.106097/asr.

sąlygas nustato Vyriausybė[1152]. Kadangi VDS yra atskaitinga ir pavaldi Prezidentui, AOTD – Krašto apsaugos ministrui, o Vyriausybinė žvalgybos institucijų kontrolė pasireiškia tik labai epizodiškai[1153], vadinasi, Vyriausybė tiesiogiai turėdama palyginus nedaug sąryšių su žvalgybos institucijų veikla, nustato slaptus žvalgybos metodus ir jų taikymo tvarką, ją tvirtindama priimdama poįstatyminį teisės aktą – Vyriausybės nutarimą. Lietuvos mokslininkai šią įstatymo nuostatą kritikuoja ir vienabalsiai ją vadina pažeidžiančia EŽTK 8 str. nuostatas[1154]. Aš siūlau šiek tiek kitokį požiūrį. EŽTT savo jurisprudencijoje susilaiko nuo griežtesnių žvalgybos veiklų vertinimo pasisakydamas, kad ji yra laisva veikti tiek, kiek tai neprieštarauja demokratinės visuomenės principams[1155]. Todėl EŽTK vertindamas žvalgybos institucijų veiklą 8 str. atžvilgiu yra ne kartą pasisakęs, kad teisė į privatumą bei, vadovaujantis EŽTK 8 str. gali būti suvaržyta, tačiau tik aukščiausios galios teisės aktu – įstatymu. Ar pakanka abstraktaus žvalgybos metodų, kaip tokių egzistuojančių, taikymo galimybės įvardijimo, nors patys metodai ir jų taikymo tvarka reglamentuojama poįstatyminiu teisės aktu, kad laikytumėme, jog teisė į asmens duomenų apsaugą yra varžoma įstatymu, o ne poįstatyminiu slaptu teisės aktu? Žvalgybos srityje slaptos teisės aktų interpretacijos ir aiškinimai, įtakos žvalgybos veiklai turi tiek pat kaip ir įstatymas. Teisinės valstybės principo sudėtinė dalis yra teisės aktų viešo skelbimo reikalavimas, o vadovaujantis jurisprudencija, slapti teisės aktai yra arba blogi, arba negali iš viso tokiais būti laikomi[1156].

Realiai Žvalgybos įstatyme yra įtvirtinti tik trys faktai apie žvalgybos metodus: kad egzistuoja slapti žvalgybos informacijos rinkimo būdai, jie yra valstybės paslaptis, jie nesankcionuojami teismo, patys būdai ir jų taikymo tvarka reglamentuojama Vyriausybės priimtu poįstatyminiu teisės aktu. Taigi, iš esmės įstatymas nereglamentuoja pačių žvalgybos metodų, nenustato net minimaliausių reikalavimų jų reglamentavimui, o tik informuoja, jog tokie egzistuoja. Tai gali būti laikoma nesuderinama su EŽTK 8 str. įtvirtinta teise į asmens duomenų apsaugą. Būtent tokią savo poziciją yra pateikęs Lietuvos ambasados Jungtinėse Valstijose gynybos patarėjas V. Urbelis[1157]. Bet apie elektroninės žvalgybos taikomus metodus galima rasti informacijos tiek moksliniuose straipsniuose[1158], tiek internete – netgi tokiame primityviame informacijos šaltinyje

---

[1152] „Lietuvos Respublikos žvalgybos įstatymas“, 12 str., *eSeimas*, žiūrėta 2020 m. rugpjūčio 22 d., https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/TAIS.106097/asr.

[1153] „Lietuvos Respublikos žvalgybos įstatymas“, 22 str., *eSeimas*, žiūrėta 2020 m. rugpjūčio 22 d., https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/TAIS.106097/asr.

[1154] Vaidotas Urbelis, „Lietuvos žvalgybos sistema“, *Lietuvos metinė strateginė apžvalga 2008, 2009*, 215–245.

[1155] Antonella Galetta ir Paul De Hert, „Complementing the Surveillance Law Principles of the ECtHR with Its Environmental Law Principles: An Integrated Technology Approach to a Human Rights Framework for Surveillance“, *Utrecht Law Review* 10, no. 1 (2014): 55–75.

[1156] Graham Smith, „Illuminating the Investigatory Powers Act“, *Cyberleagle*, žiūrėta 2020 m. rugpjūčio 22 d., http://www.cyberleagle.com/2018/02/illuminating-investigatory-powers-act.html?utm_source=feedburner&utm_medium=email&utm_campaign=Feed%3A+Cyberleagle+%28Cyberleagle%29.

[1157] Urbelis, *op. cit.*, 1149.

[1158] Steven A. Stottlemyre, „HUMINT, OSINT, or Something New? Defining Crowdsourced Intelligence“, *International Journal of Intelligence and CounterIntelligence* 28, no. 3 (2015): 578–89, doi:10.1080/08850607.2015.992760. United Nations Office on Drugs and Crime, *Current Practices in Electronic Surveillance in the Investigation of Serious and Organized Crime* (New York: United Nations, 2009). „Electronic Surveillance – an Overview“, *ScienceDirect*, žiūrėta 2020 m. rugsėjo

kaip Vikipedija[1159], taip pat yra rengiami vieši mokymai, kurie vyksta ir Lietuvoje[1160]. Todėl pagrįstai galėtų kilti klausimas – ar tikrai žvalgybos metodai yra slapti. Veikiau slapti yra konkretūs žvalgybos veiksmai kai taikomi žvalgybos metodai arba objektai, kurių atžvilgiu jie taikomi. Atitinkamai Vyriausybė, tikėtina, ne slaptus žvalgybos metodus nustato, nes metodai, patys savaime mažai tikėtina, kad yra slapti, o tvirtina konkrečius veiksmus ar tikslus, kurių atžvilgiu taikomi žvalgybos metodai, ir veikia ne kaip „įstatymo leidėja", o kaip sankcionuotoja. Todėl, autorės nuomone, reikėtų ne akcentuoti, kad Lietuva pažeidžia EŽTK 8 str. žvalgybos metodus numatydama poįstatyminiame teisės akte, o tiesiog patikslinti Žvalgybos įstatymo formuluotę, numatant, kad Vyriausybė ne nustato slaptus žvalgybos metodus, o tvirtina žvalgybos veiksmus, ir būtent pastarieji iš tikrųjų ir yra slapti.

Metaduomenų ir turinio duomenų rinkimo tvarka. Žvalgybos įstatymo formuluotė suponuoja tai, kad Apygardos teismas asmens duomenų rinkimą el. erdvėje sankcionuoja tik tuo atveju, kai žvalgybos institucijos renka ir fiksuoja elektroninėje erdvėje perduodamos informacijos turinį. Susirašinėjimas ir kitoks asmens susižinojimas būtent ir yra laikyti turininio pobūdžio informacija. Vadinasi, metaduomenų rinkimui teismo sankcionavimas yra nereikalingas. Jau minėtame Žvalgybos įstatymo 15 str. yra įtvirtinta, kad žvalgybos institucijos teismo nesankcionuotos gali gauti iš institucijų, įmonių, įstaigų ir organizacijų žvalgybos institucijų veiklai reikalingą informaciją. Reikalingos informacijos sąvoka, tikėtina, apima ir asmens duomenis, kurie yra komunikacijos elektroninėje erdvėje metaduomenys. Dėl nesankcionuoto meta duomenų rinkimo kyla dvi problemos. Pirma, tai gali sudaryti sąlygas Lietuvos žvalgybos institucijoms vykdyti masinį nediferencijuotą asmens duomenų rinkimą, kuris yra laikomas grėsme teisės į asmens duomenų apsaugą užtikrinimui[1161]. Antra, metaduomenys jau nebėra laikomais mažesnės svarbos nei komunikacijos el. erdvėje turinio duomenys[1162] ir priklausomai nuo jų tipo gali apimti ir komunikacijos turinį, todėl įstatyme nustatant tvarką turinio duomenų rinkimui, bet analogiškos tvarkos neįtvirtinant metaduomenų rinkimo atveju, gali kilti klausimas ar tai atitinka EŽTK 8 str. reikalavimus dėl teisės į asmens duomenų apsaugą apribojimo pagrindų. Tikėtina, kad šiuo atveju galioja bendra nuostata, kad elektroninių ryšių tinklų teikėja arba paslaugų el. erdvėje teikėja komunikacijos el. erdvėje meta duomenis žvalgybos institucijoms teikia pagal

9 d., https://www.sciencedirect.com/topics/computer-science/electronic-surveillance. Colin Shaff, „Is the Court Allergic to Katz – Problems Posed By New Methods of Electronic Surveillance to the Reasonable-Expectation-of-Privacy Test Note", *Southern California Interdisciplinary Law Journal* 23, no. 2 (2014): 409–50. Urbelis, *supra note*, 1149.

[1159] „Open-Source Intelligence", *Wikipedia*, žiūrėta 2020 m. rugpjūčio 22 d., https://en.wikipedia.org/w/index.php?title=Open-source_intelligence&oldid=970364598. „Human Intelligence (Intelligence Gathering)", *Wikipedia*, žiūrėta 2020 m. rugpjūčio 22 d., https://en.wikipedia.org/w/index.php?title=Human_intelligence_(intelligence_gathering)&oldid=965753709.

[1160] „Mokymai „Atvirųjų šaltinių žvalgyba", *NRD Cyber Security*, žiūrėta 2020 m. rugpjūčio 22 d., https://www.nrdcs.lt/lt/Renginiai/-mokymai-atviruju-saltiniu-zvalgyba-/61.

[1161] „Document on surveillance of electronic communications for intelligence and national security purposes", *Article 29 Data Protection Working Party*, 2014, žiūrėta 2020 m. rugpjūčio 17 d., https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp228_en.pdf.

[1162] Christopher Kuner ir kt., „An Unstoppable Force and an Immoveable Object? EU Data Protection Law and National Security", *International Data Privacy Law* 8, no. 1 (February 1, 2018): 1–3, doi:10.1093/idpl/ipy003.

atskiras sutartis[1163]. Nors vadovaujantis EŽTK asmens teisės gali būti apribojamos tik įstatyme nustatyta tvarka[1164], Lietuvoje tokia tvarka yra numatyta tik komunikacijos el. erdvėje turinio rinkimui. Metaduomenų rinkimo teismas nesankcionuoja, o įstatymas nenumato rinkimo tvarkos ir procedūrų. Galima būtų teigti, kad metaduomenys nėra asmens duomenys, tačiau tokia pozicija mokslininkų jau yra paneigta[1165]. JAV NSA masinio asmens duomenų rinkimo programos būtent ir buvo vykdomos renkant ne komunikacijos el. erdvėje turinį, bet metaduomenis. Tiek ES WP29[1166], tiek asmens duomenų apsaugos ekspertai komunikacijos metaduomenis po NSA skandalo pradėjo laikyti tiek pat svarbiais asmens duomenimis, kaip ir turinys, todėl reikalavimas sankcionuoti komunikacijos turinio rinkimą ir tokio paties reikalavimo metaduomenų rinkimui nebuvimas yra neproporcingas teisės į asmens duomenų užtikrinimo atžvilgiu.

Panašia logika, kad tam tikrai asmens duomenų kategorijai rinkti teisminis sankcionavimas yra nereikalingas iki 1967 m. buvo vadovaujasi ir JAV, kur teismas byloje *Katz v. United States* IV JAV Konstitucijos pataisos, o ne teisės akto pagrindu, pripažino, kad nesankcionuotas asmens duomenų rinkimas el. erdvėje yra negalimas. Iki šio teismo sprendimo net ir komunikacijos el. erdvėje turinį buvo galima rinkti teismui nesankcionavus. Visgi vėlesni teismo sprendimai bylose *United States v. Miller*[1167] ir *Smith v. Maryland*[1168] įteisino trečios šalies doktriną, kurios esmė tokia pati, kaip Lietuvos žvalgybos įstatymo nuostatų – komunikacijos el. erdvėje meta duomenys nėra saugomi IV JAV Konstitucijos pataisa. Tačiau, kaip jau išsiaiškinome I skyriuje, tai nereiškia, kad JAV įstatymo leidėjai numatė galimybę metaduomenis rinkti iš viso nesankcionuotai. JAV meta duomenys yra renkami sankcionuotai, skiriasi tik prašymo teismui sankcionuoti turinys, teisminio sankcionavimo forma ir teismo įgaliojimai. Analogiškai JAV, Lietuvos Respublikos Konstitucijos 22 str. 2 d. yra nurodyta, kad „informacija apie privatų asmens gyvenimą gali būti renkama tik motyvuotu teismo sprendimu ir tik pagal įstatymą“. Todėl tokia, kokia dabar yra įtvirtinta, Žvalgybos įstatymo nuostata galėtų būti pripažinta prieštaraujančia Lietuvos Respublikos Konstitucijos 22 str. 2 d., kadangi metaduomenys taip pat yra asmens duomenys. Atsižvelgiant į tai, Žvalgybos įstatyme turėtų būti įtvirtintas meta duomenų sankcionavimas ir jo tvarka.

Atlikus Žvalgybos įstatymo nuostatų analizę galime kelti tokius klausimus:

1. Ar Žvalgybos įstatymas sudaro sąlygas Lietuvos žvalgybos institucijoms rinkti asmens duomenis nediferencijuojant asmenų, t. y. vykdyti masinį asmens duomenų

[1163] „Lietuvos Respublikos žvalgybos įstatymas“, 15 str. 3 d., *eSeimas*, žiūrėta 2020 m. rugpjūčio 22 d., https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/TAIS.106097/asr.

[1164] „Europos žmogaus teisių ir pagrindinių laisvių apsaugos konvencija“, 8 str. 2 d., *eSeimas*, žiūrėta 2020 m. rugsėjo 9 d., https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/TAIS.19841 ir Europos Sąjungos pagrindinių teisių chartija“, 52 str. 1 d., *EUR-Lex*, žiūrėta 2020 m. rugsėjo 9 d., https://eur-lex.europa.eu/legal-content/LT/TXT/PDF/?uri=CELEX:12016P/TXT&from=EN

[1165] Stalla-Bourdillon, Papadaki ir Chown, *supra note*, 152.

[1166] „Document on surveillance of electronic communications for intelligence and national security purposes“, *Article 29 Data Protection Working Party*, 2014, žiūrėta 2020 m. rugpjūčio 17 d., https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp228_en.pdf

[1167] United States v. Miller, *supra note*, 222.

[1168] Smith v. Maryland, *supra note*, 212.

rinkimą? Atsakymas, teoriškai taip. Pirma, metaduomenų rinkimas nėra teismo sankcionuojamas. Antra, prašydamos apygardos teismo sankcionuoti komunikacijos el. erdvėje turinio rinkimą, žvalgybos institucijos turi teisę rinktis kokią informaciją pateikti teismui ir kieno atžvilgiu rinkti asmens duomenis: konkrečių fizinių asmenų (tokiu atveju pateikiama vardas ir pavardė, asmens kodas), konkrečių juridinių asmenų (pateikiama buveinė, kodas), arba objektų (pateikiamas jų apibūdinimas). Jeigu informacija renkama konkrečių juridinių asmenų atžvilgiu, tuomet tikėtina, kad gali būti renkama visų konkrečiuose juridiniuose asmenyse esančių, dirbančių ar juose apsilankiusių fizinių asmenų atžvilgiu, jeigu tik žvalgybos institucijos turi technologines galimybes tai padaryti. Žvalgybos institucijos gali prašyti teismo sankcionuoti komunikacijos turinio rinkimą ir neapsiribodamos konkrečiu juridiniu asmeniu. Žvalgybos įstatymas numato galimybę rinkti asmenų komunikacijos el. erdvėje turinį, kurie komunikacijos metu yra arba buvo atitinkamame objekte. Kas yra laikytina objektu Žvalgybos įstatymas nepateikia aiškinimo. Kadangi prašymui sankcionuoti komunikacijos turinio rinkimą pakanka objekto apibūdinimo, darytina išvada, kad tai yra labai plati sąvoka, galinti apimti ir visą Lietuvos teritoriją.

2. Ar teisminis sankcionavimas gali būti laikomas pakankamu ir realiai teisę į asmens duomenų apsaugą užtikrinančiu pagrindu? Principas, kad teisingumą vykdo tik teismas yra nekvestionuojamas. Todėl dažnai teismas yra tapatinamas su žmogaus teisių apsaugos garantu. Teisių apsaugoje esminis elementas yra žmogus. Žvalgyboje ir kontržvalgyboje objektu nėra konkretus žmogus, išskyrus jeigu jis gali kelti pavojų nacionaliniam saugumui. Tačiau net ir šiuo atveju, jis labiau veikia ne kaip fizinis asmuo, bet kitos valstybės, organizacijos ar pan. atstovas. Žvalgybos objektu yra kitos valstybės, organizacijos ir pan. politinė, ekonominė, mokslo, technologijų, informacinė, karinė veikla. Todėl tiesiogiai pasekmės žmogui, veikiančiam kaip fiziniam asmeniui, dėl žvalgybos ir kontržvalgybos veiklos paprastai nekyla. Aišku pasekmės nekyla tik tada, jeigu kalbame apie demokratines valstybės. Netiesiogiai asmeniui pasekmės visgi gali kilti, kadangi surinktos žvalgybinės informacijos pagrindu valstybė gali formuoti savo politiką, priimti sprendimus[1169]. Todėl be to, kad konkretus žmogus nėra žvalgybos ir kontržvalgybos objektu reikėtų išskirti ir kelias kitas ypatybes, kodėl teismas negali būti laikomas absoliučiu asmens teisių apsaugos garantu. Pirma, teismas jurisdikciją turi tik Lietuvos teritorijoje esančių asmenų atžvilgiu. Antra, nesuderinti su kita valstybe žvalgybos veiksmai jos atžvilgiu yra laikomi nusikaltimais. Kaip jau žinome iš II disertacijos skyriaus, JAV FISA akte yra numatytas FISA teismo vykdomas elektroninės žvalgybos sankcionavimas, tačiau FISA teismas asmens duomenų rinkimą el. erdvėje sankcionuoja tik tuo atveju jeigu asmuo yra už JAV teritorijos ribų, tačiau bent vienas elementas yra JAV – tai jo asmens duomenys. Kas gali būti keliais atvejais – jie keliauja per

[1169] „The Ethics (or Not) of Massive Government Surveillance", *Stanford University*, žiūrėta 2020 m. rugpjūčio 23 d., https://cs.stanford.edu/people/eroberts/cs181/projects/ethics-of-surveillance/ethics.html. H Akın Ünver, „Politics of Digital Surveillance, National Security and Privacy", n.d., 23.

JAV teritoriją į kitose valstybėse esančius serverius, yra JAV esančiuose serveriuose arba el. paslaugų teikėjai yra JAV įmonės ir jos techniškai gali suteikti informaciją žvalgybos institucijoms. Nors FISA tikslas yra rinkti ne JAV asmenų duomenis, tačiau manoma, kad atsitiktinis JAV asmenų asmens duomenų rinkimas yra labai dažnas[1170]. Todėl iš tikrųjų FISA teismo paskirtis yra užtikrinti JAV asmenų teisę į asmens duomenų apsaugą, o ne viso likusio pasaulio gyventojų teisių apsaugą. Nors skirtingai nuo JAV, EŽTK 8 str. asmenys nėra suprantami tik kaip Konvencijos šalių piliečiai, t. y. šalys negali jų skirstyti į savo ir ne savo asmenis, tačiau EŽTT žvalgybos veiklai el. erdvėje suteikia daug laisvės, svarbu tik, kad tai nežeistų demokratinės visuomenės principų[1171]. O tarptautinėje teisėje egzistuoja vadinamasis Lotus principas suteikiantis teisę valstybėms vykdyti žvalgybą viena kitos atžvilgiu[1172] patvirtina, kad tai yra neišvengiama. Klausimas ar teisminis sankcionavimas yra privalomas apribojant EŽTK 8 str. ir Europos žmogaus teisių chartijos 7 str. įtvirtintą teisę į asmens duomenų apsaugą yra iki šiol aiškiai neatsakytas EŽTT ir ESTT praktikoje. G. Malgieri ir P. De Hert teigia, kad nei EŽTT, nei ESTT teisės į asmens duomenų apsaugą apribojimų nesieja su privalomu teisminiu sankcionavimu, nors sankcionavimo procedūra turėtų būti privaloma. Tačiau žvalgybos veiksmų sankcionavimas dėl pačios žvalgybos veiklos politinio pobūdžio gali būti ir qvazi teisminis arba neteisminis[1173]. Todėl galima daryti išvadą, kad tiek turininio, tiek neturininio pobūdžio asmens duomenų rinkimas elektroninėje erdvėje žvalgybos tikslais teismų negali būti sankcionuojamas, tačiau kito organo sankcionavimo procedūra yra būtina tam, kad nebūtų pažeisti demokratinės valstybės principai. Tuo kitu organu Lietuvoje galėtų būti Valstybės gynimo taryba. Tokia Valstybės gynybos tarybos veikla atitiktų Lietuvos Respublikos valstybės gynimo tarybos įstatymo 4 str. įtvirtintas Valstybės gynimo tarybos funkcijas.

Visgi, asmens duomenų rinkimas elektroninėje erdvėje, nepriklausomai nuo to ar renkami elektroninės komunikacijos turinio duomenys ar metaduomenys, jeigu tai daroma kontržvalgybos tikslais turėtų būti sankcionuojamas teismo. Ir tai turėtų būti aiškiai įvardijama Žvalgybos įstatyme bei nustatoma tokių duomenų rinkimo tvarka.

3. Ar Bendrajame asmens duomenų apsaugos reglamente įtvirtinta informavimo pareiga ir teisė susipažinti su informacija apie savo asmens duomenų rinkimą yra realizuojama atsižvelgiant į Žvalgybos įstatymo nuostatas? Reglamente yra numatyta, kad nepriklausomai nuo to ar asmens duomenys yra renkami iš duomenų subjekto ar ne iš duomenų subjekto, duomenų valdytojas privalo asmens duomenų gavimo metu duomenų subjektui pateikti informaciją apie asmens

[1170] Elizabeth Goitein, „Another Bite out of Katz: Foreign Intelligence Surveillance and the Incidental Overhear Doctrine Symposium: Katz @ 50: The Fourth Amendment in the Digital Age“, *American Criminal Law Review* 55, no. 1 (2018): 105–26.

[1171] „Guide on Article 8 of the European Convention on Human Rights“, *European Court of Human Rights*, žiūrėta 2020 m. rugpjūčio 23 d., https://www.echr.coe.int/Documents/Guide_Art_8_ENG.pdf.

[1172] Daniel Severson, „American Surveillance of Non-U.S. Persons: Why New Privacy Protections Offer Only Cosmetic Change Notes“, *Harvard International Law Journal* 56, no. 2 (2015): 465–514.

[1173] Malgieri and Hert, „European Human Rights, Criminal Surveillance, and Intelligence Surveillance.“

duomenų gavėjus arba asmens duomenų gavėjų kategorijas taip pat duomenų subjektas turi kitas su tuo susijusias teises[1174]. Žvalgybos įstatymo 14 str. yra įtvirtinta visiškai priešinga nuostata – kad informacija apie duomenų pateikimą žvalgybos institucijoms iš valstybės ir žinybinių registrų, informacinių sistemų ir duomenų bazių tretiesiems asmenims neteikiama. Tačiau tokia Žvalgybos įstatymo nuostata negali būti laikoma prieštaraujančia Reglamente įtvirtintai informavimo pareigai ir teisei į informaciją. Ne tik kad Reglamentas, kaip ir Direktyva, nėra taikomi valstybių nacionalinio saugumo sričiai, bet ir Reglamente yra papildomai įtvirtinta, kad informavimo pareiga ir teisė į informaciją nėra absoliuti ir gali būti ribojama nacionalinio saugumo tikslais[1175]. Taigi tai, kad asmenys nėra informuojami, jog žvalgybos institucijos renka, rinko informaciją apie juos negali būti laikoma prieštaraujančia pareigai informuoti ir teisei žinoti. Visgi nors Chartijoje įtvirtinta teisė į asmens duomenų apsaugą negalioja žvalgybos atžvilgiu, EŽTK galioja. Kaip yra pažymėjęs EŽTT, nacionalinio saugumo tikslai nėra tapatūs įprastinių nusikaltimų užkardymui[1176]. Tai suteikia laisvės valstybėms spęsti kiek būti atviromis su savo piliečiais. Ne visos valstybės narės naudojasi galimybe absoliučiai neteikti informacijos asmenims apie tai, kad žvalgybos institucijos rinko jų duomenis. Net 23 ES valstybėse narėse tokia informacija gali būti teikiama[1177]. Tik Lietuvoje, Lenkijoje, Čekijoje, Airijoje ir Slovakijoje nėra jokių galimybių asmenims susižinoti apie tai, kad jų asmens duomenys buvo žvalgybos institucijų tyrimo objektu[1178]. Tai reiškia, kad:

1) asmenys patys negali žinoti ar jų teisės ir teisėti interesai nebuvo pažeisti;
2) tuo atveju, jei asmenų teisės ir ar teisėti interesai buvo pažeisti jie netenka teisės į teisminę gynybą;
3) tuo atveju, kai asmenų teisės ir teisėti interesai buvo pažeisti, jie netenka teisės į žalos, atsiradusios dėl neteisėtų valdžios institucijų veiksmų kompensavimą.

Vadinasi, nors ir Žvalgybos įstatymas šiuo atveju atitinka ET ir ES teisės aktų reikalavimus, kitų ES valstybių narių praktika rodo, jog informacijos suteikimo nuostatos Lietuvoje galėtų būti švelnesnės. Nežinojimas, kad apie asmenį buvo renkami asmens duomenys užkerta kelią į teisminę gynybą. Ypač turint omenyje tai, kad net ir teisminio proceso metu kaltinamoji šalis gali neturėti galimybės susipažinti su VSD ir AOTD surinkta bylos medžiaga, kurios pagrindu ne tik formuojamas kaltinimas, bet ir priimamas sprendimas, sukeliantis pasekmes konkrečiam asmeniui. Kita vertus, net ir turėdamos pareigą informuoti, valstybių institucijos randa būdą kaip šią pareigą

[1174] BDAR, 13 str. 1-e ir 14-1-e, EUR-Lex, žiūrėta 2020 m. rugpjūčio 23 d., https://eur-lex.europa.eu/legal-content/LT/TXT/?uri=CELEX%3A32016R0679.

[1175] BDAR 23 str. 1 d., EUR-Lex, žiūrėta 2020 m. rugpjūčio 23 d., https://eur-lex.europa.eu/legal-content/LT/TXT/?uri=CELEX%3A32016R0679.

[1176] „Surveillance by Intelligence Services: Fundamental Rights Safeguards and Remedies in the EU – Volume II: Field Perspectives and Legal Update", *European Union Agency for Fundamental Rights*, 2017, žiūrėta 2020 m. rugpjūčio 23 d., https://fra.europa.eu/sites/default/files/fra_uploads/fra-2017-surveillance-intelligence-services-vol-2_en.pdf.

[1177] *Ibid.*, 62.

[1178] *Ibid.*

apeiti. Pavyzdžiui, Olandijoje su asmens duomenų teikėju teisėsaugos institucijos pasirašo neatskleidimo sutartį (angl. *non disclosure agreement*). Teisėsaugos institucijoms ši sutartis tampa pagrindu neinformuoti asmens apie jo asmens duomenų rinkimą[1179].

4. Ar teismas, sankcionuodamas asmens duomenų rinkimą el. erdvėje, žino kokiu tikslu tie duomenys bus renkami? Atsakymas – ne. Kodėl svarbu tai yra žinoti? Viena vertus, asmens duomenų rinkimo tikslas yra vienas iš kertinių teisėto asmens duomenų rinkimo pagrindų, įtvirtintų tiek EŽTK, tiek Europos žmogaus teisių chartijoje, tiek Reglamente. Kita vertus, žvalgybos vykdomo asmens duomenų elektroninėje erdvėje rinkimo tikslai yra vienas iš dažniausiai diskutuojamų ir labiausiai prieštaringai vertinamų klausimų literatūroje kalbant apie žvalgybą[1180]. Tiek Reglamente, tiek Direktyvoje yra numatyta, kad nacionalinio saugumo tikslais šių teisės aktų nuostatos yra netaikomos. EŽTT taip pat stengiasi kuo mažiau kištis į nacionalinio saugumo klausimus palikdamas tai kiekvienos valstybės kompetencijai. Tačiau EŽTT yra suformavęs bendrąjį principą, kuris sako, kad žvalgybos veikla nacionalinio saugumo užtikrinimo atveju privalo būti suderinta su demokratinės valstybės principais ir pagrindais. Kas apima nacionalinį saugumą EŽTT nėra įvardijęs, tačiau yra pasisakęs, jog žvalgybos veikla įprastinių nusikalstamų veikų užkardymo atveju nors ir yra jų kompetencijos srityje, tačiau tai nėra veikimas nacionalinio saugumo tikslais[1181]. Vadinasi, teismas turėtų taikyti skirtingus standartus ir būti lakstesnis, kuomet asmens duomenys yra renkami nacionalinio saugumo užtikrinimo tikslais ir griežčiau vertinti tuomet, kai jie renkami kitais tikslais. Lietuvos BK yra labai aiškiai įtvirtinta, kokie nusikaltimai kelia grėsmę visuomenės saugumui, tačiau nacionalinio saugumo, kaip BK ginamos vertybės, nėra įtvirtintos. BK saugoma vertybė – visuomenės saugumas – yra pažeidžiama tik tada, kai yra vykdomi su nusikalstamu susivienijimu ir terorizmu susiję nusikaltimai. Ir iš tikrųjų elektroninės žvalgybos tikslu, kaip kovos su nusikalstamu tikslu, paprastai yra įvardijama tik kova su terorizmu ir paprastai terorizmas ir yra įvardijamas grėsme nacionaliniam saugumui[1182]. Išviešintų žinomų JAV, Didžiosios Britanijos, Vokietijos ir kitų valstybių masinio asmens duomenų rinkimo el. erdvėje programų viešai skelbiamas tikslas yra kova su terorizmu. Bet vis dažniau yra keliamas klausimas apie tai, kad ne tik kad kova su terorizmu nėra pagrindinis elektroninė žvalgybos tikslas, bet ir kad masinis asmens duomenų rinkimas el. erdvėje neužkardo terorizmo. Manytina, kad terorizmas yra pasirinktas kaip labiausiai visuomenę veikiančiu, gąsdinančiu ir skatinančiu savo teisę į asmens duomenų apsaugą išmainyti į apsaugą nuo teroro aktų įrankiu iš tikrųjų elektronine žvalgyba siekiant

---

[1179] Gutheil ir Liger, *supra note*, 145: 56.

[1180] „The Ethics (or Not) of Massive Government Surveillance", *Stanford University*, žiūrėta 2020 m. rugpjūčio 23 d., https://cs.stanford.edu/people/eroberts/cs181/projects/ethics-of-surveillance/ethics.html.

[1181] „Europos Žmogaus Teisių Teismo 1987 m. kovo 26 d. sprendimas byloje Leander prieš Švediją (Nr. 9248/81)", *Hudoc*, žiūrėta 2020 m. rugsėjo 7 d., https://hudoc.echr.coe.int/rus#{%22itemid%22:[%22001-57519%22]}.

[1182] Rodolfo G. Biazon, „Terrorism and National Security. Special Issue on International Crimes: Section II: Roundtable Discussion", *World Bulletin: Bulletin of the International Studies of the Philippines* 14, no. 3–4 (1998): 57–61.

kitų tikslų[1183]. Pavyzdžiui, Šveicarijoje 2017 m. priimant žvalgybos įstatymai piliečiai pasisakė, kad jie balsavo[1184] už apsaugą nuo teroro aktų[1185]. Tačiau apsiriboti terorizmu, kaip pagrindine grėsme nacionaliniam saugumui, automatiškai žvalgybos institucijoms suteikiančia žalią šviesą nevaržomam asmens duomenų rinkimui el. erdvėje yra nelogiška dar ir todėl, kad ne visose ES ar EŽTK valstybėse narėse egzistuoja vienodo dydžio tiesioginė terorizmo grėsmė. Todėl grėsmė nacionaliniam saugumui kiekvienoje valstybėje turėtų būti vertinama individualiai neapsiribojant vien tik kova su terorizmu. Pavyzdžiui, Lietuvoje, vadovaujantis VSD ir AOTD ataskaita, terorizmo grėsmės nėra[1186]. Tačiau neabejotina, kad nacionaliniam saugumui grėsmę kelia grėsminga Rusijos politika. Tikėtina, kad ir Lietuvos gyventojai labiau sutiktų savo teisių atsisakyti vardan apsaugos nuo Rusijos ar kitos valstybės agresijos tikslais nei kovos su terorizmu tikslu. Nacionalinio saugumo sąvokos kilmė nėra siejama su terorizmu. Pirminė nacionalinio saugumo sąvokos reikšmė buvo apsauga nuo karinių veiksmų[1187]. Todėl, autorės nuomone, nors Lietuvos BK koncepcija su terorizmu ir nusikalstamumu susivienijimu susijusius nusikaltimus laikyti nusikaltimus visuomenės saugumui atitinka pasaulines tendencijas, tačiau atsižvelgiant į situaciją Lietuvoje, BK XVI skyriuje įtvirtinti nusikaltimai valstybės nepriklausomybei, teritorijos vientisumui ir konstituciniai santvarkai turėtų būti laikomi nusikaltimais nacionaliniam saugumui bent jau žvalgybos, kiek tai yra susiję su žvalgybos teisėmis renkant duomenis el. erdvėje, prasme. Tai atitinka ir Žvalgybos įstatymo nuostatoms, kurios žvalgybos uždavinius sieja su grėsmėmis valstybės suverenitetui, teritorijos neliečiamybei ir vientisumui, konstitucinei santvarkai, valstybės interesams, gynybinei ir ekonominei galiai[1188]. Nacionalinio saugumo pagrindų saugumo įstatymas nacionalinį saugumą sieja su dar platesne apimtimi[1189]. Todėl žvalgybos institucijos prašydamos teismui sankcionuoti asmens duomenų rinkimą el. erdvėje privalo nurodyti ir tikslą, kuriam tie duomenys yra renkami, tačiau ne tam, kad teismas griežčiau vertintų tuos prašymus, kurie nėra susiję su terorizmu, o todėl, kad teismas galėtų įvertinti ar asmens duomenys yra renkami nacionalinio saugumo užtikrinimo tikslais ir atitinka žvalgybai ir kontržvalgybai keliamus uždavinius ir ar tai nėra kriminalinės žvalgybos objektas.

[1183] Charlie Savage, *Power Wars: The Relentless Rise of Presidential Authority and Secrecy*, Revised edition (New York: Back Bay Books, 2017)

[1184] Balsavimas yra įstatymų priėmimo dalis.

[1185] „Swiss Approve New Surveillance Law“, *BBC News*, 2016, žiūrėta 2020 m. rugpjūčio 23 d., https://www.bbc.com/news/world-europe-37465853.

[1186] „Grėsmių nacionaliniam saugumui vertinimas“, *Lietuvos Respublikos valstybės saugumo departamentas, Antrasis operatyvinių tarnybų departamentas prie Krašto apsaugos ministerijos*, žiūrėta 2020 m. rugpjūčio 23 d., https://www.vsd.lt/wp-content/uploads/2019/02/2019-Gresmes-internetui-LT.pdf.

[1187] „National Security versus Global Security“, *United Nations*, žiūrėta 2020 m. rugpjūčio 23 d., https://www.un.org/en/chronicle/article/national-security-versus-global-security.

[1188] „Lietuvos Respublikos žvalgybos įstatymas“, 7 str., *eSeimas*, žiūrėta 2020 m. rugpjūčio 22 d., https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/TAIS.106097/asr.

[1189] „Nacionalinio saugumo pagrindų įstatymas“, 1 str. 2 p., *eSeimas*, žiūrėta 2020 m. rugpjūčio 22 d., https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/TAIS.34169/asr.

5. Kaip žvalgybos ir kontržvalgybos veikla yra susijusi su kriminaline žvalgyba? Pagrindinis žvalgybos ir kontržvalgybos tikslas yra nacionalinio saugumo užtikrinimas[1190], kurį žvalgybos institucijos įgyvendina prognozuodamos ir nustatydamos rizikos veiksnius, pavojus ir grėsmes, galinčius turėti reikšmės valstybės suverenitetui, teritorijos neliečiamybei ir vientisumui, konstitucinei santvarkai, valstybės interesams, gynybinei ir ekonominei galiai[1191]. Pagrindiniai kriminalinės žvalgybos uždaviniai yra nusikalstamų veikų prevencija ir išaiškinimas. Žvalgybos institucijos gali vykdyti kriminalinę žvalgybą tik konkrečiai Kriminalinės žvalgybos įstatyme įvardintų nusikalstamų veikų atžvilgiu. Žvalgybos institucijos gautos žvalgybos informacijos pagrindu gali pradėti kriminalinės žvalgybos tyrimą, jeigu gauna duomenų apie BK 114 str. „Valstybės perversmas“, 118 str. „Padėjimas kitai valstybei veikti prieš Lietuvos Respubliką“, 119 str. „Šnipinėjimas“, 121 str. „Antikonstitucinių grupių ar organizacijų kūrimas ir veikla“, 122 str. „Vieši raginimai smurtu pažeisti Lietuvos Respublikos suverenitetą“, 124 str. „Neteisėtas disponavimas informacija, kuri yra valstybės paslaptis“, 125 str. „Valstybės paslapties atskleidimas“, 126 str. „Valstybės paslapties praradimas“, 296 str. „Tarnybos paslapties pagrobimas ar kitoks neteisėtas įgijimas“ ir 297 str. „Tarnybos paslapties atskleidimas“ numatytas nusikalstamas veikas ir šių duomenų nepakanka pradėti ikiteisminį tyrimą. Pradėjus kriminalinės žvalgybos tyrimą, žvalgybos informacijos rinkimas apie tą fizinį ar juridinį asmenį nedelsiant nutraukiamas, o kriminalinės žvalgybos tyrimai atliekami Lietuvos Respublikos kriminalinės žvalgybos įstatymo nustatyta tvarka[1192]. Tokios yra bendrosios nuostatos iš kurių išplaukia kelios diskusinės įžvalgos. Pats pirmas klausimas, kuris pažvelgus į nusikalstamų veikų, kurių atžvilgiu VSD ir AOTD turi teisę vykdyti kriminalinę žvalgybą, sąrašą galėtų kilti – o kurgi jame yra terorizmas?

Nacionalinio saugumo sąvoka yra abstrakti. Abstrakti ir kiekvieno suvokiama skirtingai yra ir terorizmo sąvoka[1193]. Terorizmas – tai socialinis fenomenas. Baudžiamąją teisinę reikšmę turi tik baudžiamuosiuose įstatymuose įtvirtintas teroro aktas ir kiti teroristiniai nusikaltimai, bet ne pats terorizmas. ES teroro akto ir teroristinių nusikaltimų sąvoką buvo bandyta suvienodinti 2002 m. birželio 13 d. Tarybos pamatiniu sprendimu dėl kovos su terorizmu Nr. 2002/475/TVR[1194]. Terorizmas yra pasauliniu mastu yra laikomas grėsme nacionaliniam valstybių saugumui[1195]. Jau žinome, kad

---

[1190] „Lietuvos Respublikos žvalgybos įstatymas“, 6 str., *eSeimas*, žiūrėta 2020 m. rugpjūčio 22 d., https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/TAIS.106097/asr.

[1191] „Lietuvos Respublikos žvalgybos įstatymas“, 7 str. 1 d., *eSeimas*, žiūrėta 2020 m. rugpjūčio 22 d., https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/TAIS.106097/asr.

[1192] „Lietuvos Respublikos žvalgybos įstatymas“, 17 str., *eSeimas*, žiūrėta 2020 m. rugpjūčio 22 d., https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/TAIS.106097/asr.

[1193] David C. Rapoport, „The Four Waves of Rebel Terror and September 11“, *Anthropoetics*, 8, Nr. 1 (2002), žiūrėta 2020 m. rugpjūčio 23 d., http://anthropoetics.ucla.edu/ap0801/terror/.

[1194] 2002 m. birželio 13 d. Tarybos pamatinis sprendimas dėl kovos su terorizmu Nr. 2002/475/TVR, *EUR-Lex*, žiūrėta 2020 m. rugpjūčio 23 d., https://eur-lex.europa.eu/legal-content/LT/TXT/HTML/?uri=CELEX:02002F0475-20081209&from=EN.

[1195] Alexandra Doncea, „Tackling Terrorism as a Threat to National Security“, *European Journal of Public Order and National Security* 2015, no. 3 (2015): [i]-47.

JAV masinio asmens duomenų rinkimo el. erdvėje programų pagrindas buvo terorizmas. Teroristinių nusikaltimų užkardymą kaip teisės į privatumą ribojimo pagrindą laiko ir EŽTT[1196]. Kadangi nacionalinio saugumo užtikrinimas visų pirma yra žvalgybos institucijų funkcija, ir teroristinių nusikaltimų užkardymas paprastai patenka į valstybių žvalgybos institucijų veiklos apimtį, todėl logiška būtų, kad tokias funkcijas atliktų ir VSD bei AOTD. Tačiau įdomu yra tai, kad žvalgybos institucijų kriminalinės žvalgybos funkcijos neapima tų nusikaltimų kurie tiesiogiai BK yra siejami su pavojumi visuomenės saugumui – tai nusikalstamas susivienijimas (BK 249), teroro aktas (BK 250), teroristinių nusikaltimų kurstymas (BK 250[1]), verbavimas teroristinei veiklai (BK 250[2]), grasinimas padaryti teroristinį nusikaltimą (BK 250[3]), teroristinės veiklos finansavimas ir rėmimas (BK 250[4]), teroristų rengimas ir mokymasis teroristiniais tikslais (BK 250[5]), vykimas teroristiniais tikslais (BK 250[6]). Vadovaujantis Kriminalinės įstatymu nei VSD, nei AOTP nevykdo kriminalinės žvalgybos šių nusikaltimų atveju. Tai kelia klausimus 1) ar BK XXXV skyriuje įtvirtintų nusikaltimų prevencijos ir išaiškinimo tikslais kriminalinės žvalgybos įstatymas nėra taikomas ir žvalgybos institucijos tokiu atveju taiko labiau asmens teises varžančius tyrimo veiksmus, įtvirtintus Žvalgybos įstatyme; 2) ar VSD ir AOTP neturi teisės tirti šių nusikaltimų ir jų prevenciją bei išaiškinimą privalo atlikti kitos Kriminalinės žvalgybos įstatyme įtvirtintos institucijos.

Nors Lietuvoje sąvokos „visuomenės saugumas“ išaiškinimas įstatyminiu lygiu nėra pateiktas ir gali atrodyti, kad ši sąvoka yra siauresnė arba mažiau svarbi už Lietuvos Respublikos nacionalinio saugumo pagrindų įstatymo 1 str. 2 d. pateiktą nacionalinio saugumo apibūdinimą ir būtent nepatenka į kriminalinės žvalgybos objektų apimtį, tačiau BK XXXV skyriuje įtvirtintų nusikalstamų veikų pobūdis ir jų vykdymo ypatumai rodo, kad kalbant apie visuomenės saugumą BK XXXV skyrius omenyje turi ne tik Lietuvos visuomenės saugumą, o ir tarptautinį saugumą[1197]. Žiūrint iš teroristinių nusikaltimų reglamentavimo pusės, galima išskirti dvi grupes baudžiamųjų įstatymų: vienų valstybių baudžiamieji įstatymai baudžiamąją atsakomybę už tarptautinį terorizmą numato atskiruose straipsniuose[1198], o kitų valstybių baudžiamieji įstatymai tarptautinio terorizmo atskirai nereglamentuoja[1199]. Taigi, pirmoji reikšminga BK ypatybė yra ta, kad jame nėra atskiro straipsnio, reglamentuojančio atsakomybę už tarptautinį terorizmą. Tačiau nederėtų skubėti daryti išvados, kad vadovaujantis BK atsakomybė už tarptautinio pobūdžio nusikalstamas veikas yra negalima, kadangi vadovaujantis BK 7 str. baudžiamoji atsakomybė už jų padarymą visgi kyla. Tik, jei kai kurių valstybių baudžiamieji įstatymai išskiria į atskirus straipsnius atsakomybę už vidaus ir išorės terorizmą, tai pagal Lietuvos baudžiamąjį įstatymą asmuo už tarptautinio pobūdžio teroro aktą baudžiamojon atsakomybėn patraukiamas vadovaujantis tuo pačiu straipsniu: BK 250 str. Antroji, nagrinėjant šį klausimą mums aktuali BK ypatybė yra

[1196] „Guide on Article 8 of the Convention – Right to respect for private and family life“, *European Court of Human Rights*, žiūrėta 2020 m. rugpjūčio 23 d., https://www.echr.coe.int/Documents/Guide_Art_8_ENG.pdf.

[1197] Egidijus Vareikis, *Nacionalinis ir tarptautinis saugumas*, (Kaunas: Vytauto Didžiojo universiteto leidykla, 2005).

[1198] Pavyzdžiui, Slovėnijos, Slovakijos ir Baltarusijos.

[1199] Pavyzdžiui, Rusijos Federacijos, Kanados ir daugumos ES valstybių.

ta, kad už teroro aktą asmenys pagal Lietuvos BK atsako „nesvarbu, kokia jų pilietybė ir gyvenamoji vieta, taip pat nusikaltimo padarymo vieta bei tai, ar už padarytą veiką baudžiama pagal nusikaltimo padarymo vietos įstatymus“. Vadinasi, galime pagrįstai daryti išvadą, kad BK gina viso pasaulio visuomenės saugumą nuo nusikalstamų veikų, numatytų BK 250 str. padarymo. JAV Aukščiausias teismas taip pat yra pažymėjęs, kad „už terorizmą asmuo atsako remiantis universalios baudžiamosios jurisdikcijos principu“[1200] [1201]. Nusikaltimai visuomenės saugumui yra ne vienintelė išimtis, kuomet žvalgybos institucijos negali vykdyti kriminalinės žvalgybos veiksmų nors gali vykdyti žvalgybą. BK XVI skyriuje yra įtvirtintos 16 nusikalstamų veikų nukreiptų prieš valstybės nepriklausomybę, teritorijos vientisumą ir konstitucinę santvarką. Tačiau tik 10 iš jų Kriminalinės žvalgybos įstatyme yra priskirta žvalgybos institucijų kompetencijai vykdyti kriminalinį tyrimą. Kitų net ir sunkių nusikaltimų atveju (pvz. BK 115 str. „Kėsinimasis į Lietuvos Respublikos Prezidento gyvybę“) žvalgybos institucijos neturi kompetencijos vykdyti kriminalinę žvalgybą, nors minėto pavyzdžio atveju, tai gali būti laikoma teroro aktu[1202]. Kokiu pagrindu yra atrinkta nusikalstamos veikos nėra aišku, kadangi net tarp tų nusikalstamų veikų dėl kurių VDS ir AOTD gali vykdyti kriminalinę žvalgybą – BK 114[1203], 118[1204], 119[1205], 121[1206], 122[1207], 124[1208], 125[1209], 126[1210], 296[1211] ir 297[1212] surasime ne tik sunkius nusikaltimus (pvz. BK 114 str.), bet ir baudžiamuosius nusižengimus (pvz. BK 297 str.). Kitų institucijų kompetencijos ribose patenka ir tiesiogiai BK grėsmę ne visuomenės, o jau nacionaliniam saugumui keliantis 198 str. 2 d. įtvirtintas nusikaltimas, už kurį yra baudžiamas tas, kas neteisėtai stebėjo, fiksavo, perėmė, įgijo, laikė, pasisavino, paskleidė ar kitaip panaudojo strateginę reikšmę nacionaliniam saugumui arba didelę reikšmę valstybės valdymui, ūkiui ar finansų sistemai turinčius neviešus elektroninius duomenis. Šiame BK straipsnyje įtvirtintas nusikaltimas savo išraiškos forma gali būti būdas įvykdyti BK 118 str. įtvirtintą nusikaltimą „Padėjimas kitai valstybei veikti prieš Lietuvos Respubliką“ arba BK 119 str. įtvirtintą nusikaltimą „Šnipinėjimas“. BK 198 str. 2 d. ne tik kelia grėsmę

[1200] „Flatow v. Islamic Republic of Iran and Others“, *FindLaw*, žiūrėta 2020 m. rugpjūčio 23 d., https://caselaw.findlaw.com/us-dc-circuit/1002995.html.

[1201] Tačiau čia pat galime pastebėti ir BK trūkumą: BK 7 straipsnyje nėra nustatyta universali baudžiamoji jurisdikcija visiems teroristiniams nusikaltimams, kaip to reikalauja Tarybos pamatinis sprendimas. Tai laikytina baudžiamojo įstatymo trūkumu, kuris turėtų būti ištaisytas.

[1202] „Terrorism and Assassination“, *Oxford Reference*, žiūrėta 2020 m. rugsėjo 9 d., https://www.oxfordreference.com/view/10.1093/acref/9780191737190.timeline.0001.

[1203] Valstybės perversmas.

[1204] Padėjimas kitai valstybei veikti prieš Lietuvos Respubliką.

[1205] Šnipinėjimas.

[1206] Antikonstitucinių grupių ar organizacijų kūrimas ir veikla.

[1207] Vieši raginimai smurtu pažeisti Lietuvos Respublikos suverenitetą.

[1208] Neteisėtas disponavimas informacija, kuri yra valstybės paslaptis.

[1209] Valstybės paslapties atskleidimas.

[1210] Valstybės paslapties praradimas.

[1211] Tarnybos paslapties pagrobimas ar kitoks neteisėtas įgijimas.

[1212] Tarnybos paslapties atskleidimas.

nacionaliniam saugumui, bet ir yra vykdomas Lietuvos atžvilgiu nelegalios elektroninės žvalgybos būdu, todėl kriminalinė žvalgyba šiuo atveju turėtų būti išimtinai VSD ir AOTD kompetencija.

6. Ar VSD ir AOTD vykdomai kriminalinei žvalgybai yra taikoma ES teisė? Kriminalinę žvalgybą gali vykdyti daug platesnis institucijų ratas nei žvalgybą ir kontržvalgybą: Policijos departamentas ir jam pavaldžios policijos įstaigos, VSAT, Vadovybės apsaugos departamentas, FNTT, Muitinės departamentas ir Muitinės kriminalinės žvalgybos įgalioti padaliniai, STT, Kalėjimų departamentas ir laisvės atėmimo vietų įgalioti padaliniai[1213]. Vykdant kriminalinės žvalgybos veiksmus kriminalinės žvalgybos subjektai gali rinkti asmens duomenis elektroninėje erdvėje. Ir čia susiduriame su situacija, kuomet tokius pačius veiksmus gali atlikti ir žvalgybos, ir teisėsaugos institucijos. Iš esmės kriminalinę žvalgybą galima pradėti dėl sunkių ir labai sunkių nusikaltimų bei kitų nusikalstamų veikų, tiesiogiai įtvirtintų Kriminalinės žvalgybos įstatyme. Dalis tų nusikalstamų veikų yra susiję su nacionalinio saugumo užtikrinimu ir todėl patenka į žvalgybos institucijų kompetenciją. Kita vertus ne visos ir su nacionalinio saugumo užtikrinimu susijusios nusikalstamos veikos patenka į žvalgybos institucijų kompetenciją. Todėl lieka neaišku ar žvalgybos institucijoms, renkančioms duomenis pagal Kriminalinės žvalgybos įstatymą turėtų būti taikoma ES teisė, BDAR ir Teisėsaugos tikslais tvarkomų asmens duomenų apsaugos direktyva, ar jos išsaugo savo imunitetą nuo ES teisės ne tik žvalgybai, bet ir kriminalinei žvalgybai. Jeigu žvalgybos institucijos vykdamos kriminalinę žvalgybą išsaugo savo imunitetą nuo ES teisės, ar tą imunitetą taip pat turi ir likusios kriminalinės žvalgybos institucijos tirdamos nusikalstamas veikas, kuriomis kėsinamasi į nacionalinį saugumą, pvz. teroro aktą?

Kadangi pagal Kriminalinės žvalgybos įstatymą asmens duomenys yra renkami nusikalstamų veikų prevencijos, tyrimo, atskleidimo ar baudžiamojo persekiojimo už jas tikslais, todėl tokiam asmens duomenų tvarkymui turėtų būti taikoma Teisėsaugos tikslais tvarkomų asmens duomenų direktyva. Tačiau ESTT nuomone, terorizmo prevencijos tikslais institucijos gali labiau riboti asmens teises nei įprastų nusikalstamų veikų atžvilgiu. Tačiau Lietuvoje pagal tą patį įstatymą, vadovaudamosi tokiomis pačiomis procedūromis, turėdamos tokias pačias teises, atlikdamos tokius pačius veiksmus, asmens duomenis renka ir žvalgybos, ir teisėsaugos institucijos, ir dėl nusikaltimų, susijusių su nacionalinio saugumo užtikrinimu, ir dėl didesnę žalą visuomenei keliančių, bet įprastų, t. y. nesusijusių su nacionalinio saugumo užtikrinimu, nusikaltimų[1214] .

[1213] „Lietuvos Respublikos Vyriausybės 2013 m. vasario 6 d. nutarimas Nr. 108 „Dėl kriminalinės žvalgybos subjektų sąrašo patvirtinimo ir jų kriminalinės žvalgybos masto nustatymo“, *eTar*, žiūrėta 2020 m. rugpjūčio 23 d., https://www.e-tar.lt/portal/lt/legalAct/TAR.2B88BD021FCB/asr.

[1214] turima informacijos apie rengiamą, daromą ar padarytą labai sunkų ar sunkų nusikaltimą arba apie apysunkius nusikaltimus, numatytus Lietuvos Respublikos baudžiamojo kodekso 131 straipsnyje (naujagimio nužudymas), 145 straipsnio 2 dalyje (žmogaus terorizavimas), 146 straipsnio 2 ir 3 dalyse (**Neteisėtas laisvės atėmimas**), 151 straipsnio 2 dalyje (nepilnamečio **Privertimas lytiškai santykiauti**), 151[1] straipsnio 3 dalyje (Tėvo, motinos, globėjo, rūpintojo l**ytinės aistros tenkinimas pažeidžiant nepilnamečio asmens seksualinio apsisprendimo laisvę ir (ar) neliečiamumą**), 153 (**Jaunesnio negu šešiolikos metų asmens tvirkinimas**) ir 162 straipsniuose (**Vaiko išnaudojimas pornografijai**),

Pačiame įstatyme nėra nurodyta ar jis yra parengtas atsižvelgiant į bent vieną ES teisės aktą. Ir atsakymo ar jo atžvilgiu galioja išimtis iš ES teisės nėra įtvirtinto. Siekiant išvengti šios dviprasmybės reikėtų pačiame Kriminalinės žvalgybos teisės akte įtvirtinti grėsmę nacionaliniam saugumui keliančių nusikalstamų veikų apibrėžimą arba sąrašą, numatyti, kad kompetenciją jų tyrimo atžvilgiu turi VSD ir AOTD bei paprastesnes nei likusių nusikalstamų veikų atžvilgiu asmens duomenų rinkimo taisykles. Visoms kitoms kriminalinės žvalgybos institucijoms renkant asmens duomenis, įskaitant duomenis el. erdvėje, turi būti taikoma Teisėsaugos tikslais tvarkomų asmens duomenų apsaugos direktyva ir ES teisė.

Apibendrinimas:

1. *Lietuvoje žvalgybos institucijos asmens duomenis elektroninėje erdvėje gali rinkti žvalgybos ir kontržvalgybos tikslais. Šie tikslai reiškia, kad žvalgybos institucijos veikia arba Lietuvoje arba už Lietuvos teritorijos. Lietuvos Respublikos Konstitucija garantuojama teisė į privatumą, teismų jurisdikcija galioja tik Lietuvoje arba tik Lietuvos piliečiams, tačiau asmens duomenų rinkimas žvalgyba ir kontržvalgybos tikslais Žvalgybos įstatyme yra reglamentuojama vienodai.*
2. *Asmens duomenis el. erdvėje žvalgybos institucijos renka: 1) sankcionuotos teismo, jeigu yra renkami turininio pobūdžio duomenys, arba 2) nesankcionuotos teismo – jeigu metaduomenys gaunami iš institucijų, įmonių, įstaigų ir organizacijų bei taikydamos slaptus žvalgybos metodus. Taigi Žvalgybos įstatymas teisminio sankcionavimo poreikį skirsto ne pagal veiklos tikslą – žvalgybą ar kontržvalgyba – o pagal tai ar yra renkama meta duomenys ar turininio pobūdžio informacija. Tai neatitinka EŽTK 8 str. ir Konstitucijos 22 str. dėl to, kad metaduomenys yra asmens duomenys, o asmenų, kuriems galioja Lietuvos Respublikos Konstitucijos 22 str. atžvilgiu jie turi būti renkami teismui sankcionavus.*

---

178 straipsnio 2 dalyje (**Vagystė**), 180 straipsnio 1 dalyje (**Plėšimas**) , 181 straipsnio 1 dalyje (**Turto prievartavimas**), 187 straipsnio 2 dalyje (**Turto sunaikinimas ar sugadinimas**), 189 straipsnio 2 dalyje (**Nusikalstamu būdu gauto turto įgijimas arba realizavimas**), 189[1] straipsnyje (**Neteisėtas praturtėjimas**), 198 straipsnio 2 dalyje (2. Tas, kas neteisėtai stebėjo, fiksavo, perėmė, įgijo, laikė, pasisavino, paskleidė ar kitaip panaudojo strateginę reikšmę nacionaliniam saugumui arba didelę reikšmę valstybės valdymui, ūkiui ar finansų sistemai turinčius neviešus elektroninius duomenis,), 213 straipsnio 1 dalyje (**Netikrų pinigų ar vertybinių popierių gaminimas, laikymas arba realizavimas**), 214 (**Netikros elektroninės mokėjimo priemonės gaminimas, tikros elektroninės mokėjimo priemonės klastojimas ar neteisėtas disponavimas elektronine mokėjimo priemone arba jos duomenimis**) ir 215 straipsniuose (**Neteisėtas elektroninės mokėjimo priemonės ar jos duomenų panaudojimas**), 225 straipsnio 1 dalyje (**Kyšininkavimas**), 226 straipsnio 1 ir 2 dalyse (**Prekyba poveikiu**), 227 straipsnio 1 ir 2 dalyse (**Papirkimas**), 228 straipsnio 1 dalyje (**Piktnaudžiavimas**), 228[1] (**Neteisėtas teisių į daiktą įregistravimas**) ir 240 straipsniuose (**Kalinio išlaisvinimas**), 253 straipsnio 1 dalyje (**Neteisėtas disponavimas šaunamaisiais ginklais, šaudmenimis, sprogmenimis ar sprogstamosiomis medžiagomis**), 256 straipsnio 1 dalyje (**Neteisėtas disponavimas branduolinėmis ar radioaktyviosiomis medžiagomis arba kitais jonizuojančiosios spinduliuotės šaltiniais**), 266 straipsnio 2 dalyje (**Neteisėtas disponavimas pirmos kategorijos narkotinių ar psichotropinių medžiagų pirmtakais (prekursoriais)**) 300 straipsnio 2 ir 3 dalyse (**Dokumento suklastojimas ar disponavimas suklastotu dokumentu0**, 301 straipsnio 2 dalyje (**Antspaudo, spaudo ar blanko suklastojimas**), 302 straipsnio 2 dalyje (**Antspaudo, spaudo ar dokumento pagrobimas arba pagrobtojo panaudojimas**), 307 straipsnio 1 ir 2 dalyse (**Pelnymasis iš kito asmens prostitucijos**), 309 straipsnio 3 dalyje (**Disponavimas pornografinio turinio dalykais**), arba apie šias veikas rengiančius, darančius ar padariusius asmenis;

2) pasislepia įtariamasis, kaltinamasis arba nuteistasis;

3) dingsta be žinios asmuo;

4) vykdoma asmenų apsauga nuo nusikalstamo poveikio.

3. *EŽTK 8 str. nereikalauja, kad visais atvejais asmens duomenų rinkimą sankcionuotų teismas, tačiau turi būti nešališkas subjektas, kuris galėtų įvertinti ar duomenų rinkimas neprieštarauja demokratinės visuomenės principams. Vadovaujantis Konstitucija, kontržvalgybos atveju renkant duomenis elektroninėje erdvėje tas subjektas privalo būti teismas, žvalgybos atveju gali būti Valstybės gynybos taryba, Pavyzdžiui JAV taip pat žvalgybos, kai bent vienas elementas yra JAV – asmuo arba jo duomenys – galioja FISA, visais kitais atvejais EO 12 333. Pastarasis teisės aktas yra labai trumpos 1 puslapio apimties ir tiesiog apibrėžia taikymo sritį ir subjektus sankcionuojančius žvalgybą. Nors vadovaujantis Leono principu valstybės gali vykdyti žvalgybą taikos metu, tačiau nesuderinti žvalgybos veiksmai yra neteisėti pagal kitos valstybės teisę.*
4. *Žvalgybos įstatyme įtvirtintus žvalgybos metodus Lietuvos autoriai laiko potencialiu EŽTK 8 str. pažeidimu, kadangi jie yra įtvirtinami ne įstatyme, o viešai neskelbiamame Vyriausybės priimame poįstatyminiame teisės akte. Autorės nuomone, patys žvalgybos metodai nėra slapti, slapti yra konkretūs žvalgybos veiksmai kai taikomi žvalgybos metodai arba objektai, kurių atžvilgiu jie taikomi. Atitinkamai Vyriausybė, tikėtina, tvirtina konkrečius veiksmus ar tikslus, kurių atžvilgiu taikomi žvalgybos metodai, ir veikia ne kaip „įstatymo leidėja", o kaip sankcionuotoja. Todėl, autorės nuomone, reikėtų ne akcentuoti, kad Lietuva pažeidžia EŽTK 8 str. žvalgybos metodus numatydama poįstatyminiame teisės akte, o tiesiog patikslinti Žvalgybos įstatymo formuluotę, numatant, kad Vyriausybė ne nustato slaptus žvalgybos metodus, o tvirtina žvalgybos veiksmus, ir būtent pastarieji iš tikrųjų ir yra slapti.*
5. *Neaiškus kriminalinės žvalgybos teisinis statusas: ar ji patenka į nacionalinio saugumo išimtį, ir ES teisė jos atžvilgiu negalioja, ar visgi nepatenka. Autorė nuomone, nacionalinio saugumo išimtis gali būti taikoma tik daliai kriminalinės žvalgybos veiklų. ESTT savo praktikoje nusikaltimus skirto į keliančius grėsmę nacionaliniam saugumui ir kitus. Nacionaliniam saugumui grėsmę keliančių nusikaltimų tyrimas patenka į valstybės veikimą nacionalinio saugumo užtikrinimo tikslais, todėl EŽTK 8 str. yra taikomi griežtesni apribojimai, kadangi nusikaltimai kelia grėsmę ne atskiram individui ar jų grupei, o visai valstybei. Kitų nusikaltimų tyrimo atžvilgiu EŽTK 8 str. netaikymui turi būti taikomi griežtesni apribojimai, kadangi grėsmės mastas yra siauresnės apimties. Kriminalinė žvalgyba Lietuvoje yra atliekama tiek grėsmę nacionaliniam saugumui keliančių nusikalstamų veikų atžvilgiu, tiek ir nekeliančių, pagal tas pačias taisykles. Tai neatitinka EŽTT praktikos. Todėl šiame įstatyme reikėtų išskirti keliančius grėsmę nacionaliniam saugumui ir jų tyrimą pavesti žvalgybos institucijoms. Kitų nusikaltimų tyrimo atveju, kaip ir ikiteisminio tyrimo metu, įtraukti prokurorą kaip koordinuojančią grandį.*

5. TEISĖSAUGOS IR ŽVALGYBOS INSTITUCIJŲ BENDRADARBIAVIMAS SU PRIVAČIAIS JURIDINIAIS ASMENIMIS DĖL ASMENS DUOMENŲ RINKIMO ELEKTRONINĖJE ERDVĖJE

Skirtingai nuo dažno pirminio įsivaizdavimo, teisėsaugos ir žvalgybos institucijos elektroninius asmens duomenis daugeliu atvejų renka ne pačios, o bendradarbiaudamos su verslo ir mokslo subjektais. Ir skirtingai nuo dažno įsivaizdavimo, nors fiziniai asmenys ir yra duomenų subjektai, tačiau mūsų asmens duomenys priklauso ne mums. Elektroninė erdvė iš esmės yra valdoma elektronines paslaugas teikiančių įmonių. Jos kuria asmens duomenų rinkimo ir tvarkymo įrankius tam, kad suteiktų savo klientams paslaugas. Paprastai gali susidaryti įspūdis, kad žvalgybos ir teisėsaugos institucijose yra naudojamos naujausios technologijos, kurias šios institucijos pačios ir kuria. Tačiau 2016 m. San Franciske vykusioje RSA konferencijoje NSA direktorius Rogers oficialiai kreipėsi į Silico slėnio įmones, kad šios padėtų kovoti su kibernetinėmis grėsmėmis ir terorizmu kurdamos kovos su šiomis grėsmėmis įrankius NSA ir kitoms žvalgybos institucijoms[1215]. Tokiu būdu žvalgybos institucijos prisipažino, kad technologine prasme jos atsilieka nuo visuomenei gerai žinomų IT ir telekomunikacijos paslaugų teikėjų. Pažangiausios IT įmonės yra žingsniu toliau inovacijose negu žvalgybos ar teisėsaugos institucijos, kadangi jos inovacijų kūrimą ir inovatyvių produktų ar inovatyviais produktais grįstų paslaugų teikimą į rinką laiko konkurencingumą didinančia priemone ir į tai orientuojasi[1216]. Žvalgybos ir teisėsaugos institucijoms be bendradarbiavimo su IT ir telekomunikacijų paslaugų teikėjais rinkti asmens duomenis elektroninėje erdvėje nors ir būtų įmanoma[1217], bet nepalyginamai sudėtingiau. Todėl teisėsaugos ir žvalgybos institucijoms yra naudinga užmegzti santykius su privačiomis įmonėmis[1218]. Tačiau mokslinių diskusijų, kaip ir šios disertacijos, tyrimo objektu paprastai yra teisės normose įtvirtinti santykiai tarp teisėsaugos, žvalgybos institucijų ir verslo – įpareigojimas suteikti el. ryšių paslaugų teikėjų iš kitų verslo subjektų jau renkamus asmens duomenis, arba juos rinkti teisėsaugos ir žvalgybos institucijų nurodymu[1219]. Tokio pobūdžio santykius galime laikyti imperatyviais. Disertacijoje iki šiol buvo rašoma apie imperatyvų bendradarbiavimą tarp teisėsaugos, žvalgybos ir verslo. Tačiau be imperatyvių santykių gali susiklostyti ir dispozityvūs teisėsaugos ir žvalgybos institucijų santykiai su verslo ir mokslo subjektais, sudarantys

[1215] Tim Greene, „NSA Asks Silicon Valley to Help Fight Cybercrime, Terrorism", *Network World*, 2016, žiūrėta 2020 m. rugpjūčio 23 d., http://www.networkworld.com/article/3040175/security/nsa-asks-silicon-valley-to-help-fight-cybercrime-terrorism.html.

[1216] Sarah Spiekermann, *Ethical IT Innovation: A Value-Based System Design Approach* (CRC Press, 2015).

[1217] „U.S. Says It Has Unlocked IPhone Without Apple", *The New York Times*, žiūrėta 2020 m. rugsėjo 9 d., https://www.nytimes.com/2016/03/29/technology/apple-iphone-fbi-justice-department-case.html.

[1218] Aukštesnis inovacijų poreikis yra labiau sietinas su itin sunkiais nusikaltimais ir nacionalinio saugumo užtikrinimo tikslais, todėl labiau tikėtinas yra žvalgybos, o ne teisėsaugos institucijų, ir IT bei kitų technologinių įmonių bendradarbiavimas, tačiau įmanomas ir teisėsaugos bei IT technologijas kuriančių bei telekomunikacijų institucijų bendradarbiavimas

[1219] Carr ir Bellia, *supra note,* 21.

elektroninės žvalgybos paslaugų rinką. Viešai prieinamos informacijos apie tokio pobūdžio bendradarbiavimą nėra daug.

Pasiūla atsiranda visuomet, jei tik atsiranda paklausa. Todėl šiandien ne tik kad oficialiai egzistuoja elektroninės žvalgybos paslaugų teikimo rinka (angl. *electronic surveillance market*), bet ši rinka ir sparčiai auga. Manoma, kad el. žvalgybos paslaugų teikimo rinkos užuomazgos atsirado prasidėjus Šaltajam karui, o sparčiai ši rinka pradėjo formuotis 1990 m. kuomet, iš vienos, pusės teisėsaugos ir žvalgybos institucijos suprato asmens duomenų rinkimo el. erdvėje kuriamą pridėtinę vertę ir, iš kitos pusės, vis labiau augo el. erdve besinaudojančių asmenų skaičius[1220]. Prie el. žvalgybos paslaugų rinkos priskiriamos ne tik paslaugas el. erdvėje teikiančios įmonės, bet ir visos kitos įmonės, kurios gali padėti asmens duomenis rinkti el. erdvėje, pavyzdžiui, jūros kabelių tiekėjų įmonės, įmonės, kurios specializuojasi tik žvalgybos technologijų kūrime, ir pan. Privacy International yra atlikusi tyrimą apie el. žvalgybos paslaugų teikimo rinką. Tyrime įvardinti paslaugų teikėjų tipai, teikiamos paslaugos ir pateikti įmonių pavyzdžiai pateikiami 8 lentelėje.

8 lentelė. *Žvalgybos rinka pagal Privacy International 2016 m. tyrimą*[1221].

Veiklos sritis	**Technologija, paslaugos**	**Paslaugas teikiančių įmonių pavyzdžiai**
ISPs/Telekomunikacijų operatorius	Interneto ir telefoninio ryšio paslaugos. Valstybinė arba privati, turinti įvairių akcininkų	AT&T, Vodafone, Comcast, Orange, Telecom Egypt, Uzbektelecom
Povandeninių kabelių tiekėjai	Povandeninių kabelių operatoriai / Pakrovimo taškų operatoriai. Paprastai finansuojamas iš operatorių konsorciumų	TATA-3, China Unicom, Hibernia, Level 3, Atlantic Crossing, Huawei Marine
Telekomunikacijų tinklo įrangos pardavėjai	Standartiniai tinklo mazgai (angl. *network nodes*), tokie kaip jungikliai (angl. *switches*) ir tinklų sąsajos (angl. *gateways*), kai kurie iš jų yra suprojektuoti taip, kad būtų galima perimti informaciją arba skirti tinklo stebėjimui	Ericsson, Nokia, Huawei, ZTE, Cisco, Bluecoat
Žvalgybos technologijų kūrimo ir žvalgybos paslaugas teikiančios įmonės	Valstybinių organizacijų arba valstybiniais tikslais telekomunikacijų įmonių užsakymu teikiančios žvalgybos technologijų	Verint, NICE Systems, Qosmos, Trovicor, Hacking Team, NeoSoft, VasTech, Palantir
Rangovai ir PMSCs	Konsultacinės paslaugos ir personalas	Booz Allen Hamilton, BAE, SAIC, Chertoff Group, ManTech
Platintojai	Partneriai ir žvalgybos technologijų perpardavinėtojai	Elamen, Ezzy Group

[1220] „The Global Surveillance Industry“, *Privacy International,* 16, žiūrėta 2020 m. rugpjūčio 23 d., https://www.privacyinternational.org/sites/default/files/2017-12/global_surveillance_0.pdf.

[1221] *Ibid.,* 17.

Didžiausia žvalgybos paslaugų tiekėjų rinka yra JAV (122 žvalgybos paslaugas teikiančios įmonės), Didžiojoje Britanijoje (104 žvalgybos paslaugų tiekėjos), Prancūzijoje (45 žvalgybos paslaugų tiekėjos), Vokietijoje (41 žvalgybos paslaugų tiekėja) ir Izraelyje (27 žvalgybos paslaugas teikiančios įmonės). Iš 28 ES valstybių narių 23-jose veikia žvalgybos paslaugas teikiančių įmonių. Daugiausiai žvalgybos įmonių yra Didžiojoje Britanijoje (104 žvalgybos paslaugų tiekėjos), Prancūzijoje (45 žvalgybos paslaugų tiekėjos), Vokietijoje (41 žvalgybos paslaugų tiekėja), Italijoje (18 žvalgybos paslaugų tiekėjos) ir Švedijoje (9 žvalgybos paslaugų tiekėjos). Lietuvoje taip yra bent 3 el. žvalgybos paslaugas teikiančios įmonės. Galima pastebėti paraleles tarp kiek oficialiai žinoma, pirmaujančių žvalgybos el. erdvėje programas vykdančių šalių ir didžiausias žvalgybos paslaugų rinkas turinčių valstybių. Tiek JAV, tiek Didžioji Britanija yra laikomos daugiausiai el. žvalgybos programų vykdančiomis valstybėmis. Šiose šalyse el. žvalgybos industrija taip pat yra stipriausia. Teiginiai priklausomybės ryšiai egzistuoja ir tarp valstybių, kurių teisės aktuose yra įtvirtinta prisijungimo prie elektroninės erdvės įrenginių galimybės, ir žvalgybos rinkos jose.

Žvalgybos technologijos ir žvalgybos paslaugų teikimas yra ypatingos svarbos klausimai kiekvienai valstybei ne vien tik dėl nacionalinio saugumo užtikrinimo tikslų, bet ir dėl piktnaudžiavimo žmogaus teisėmis prevencijos bei stabilumo pasaulyje užtikrinimo. Jei demokratinėse valstybėse diskutuotina dėl asmens surinktų asmens duomenų naudojimo tikslų ir suderinamumo su asmens teise į privatumą ir duomenų apsaugą[1222], tai nedemokratinėse valstybėse pažangios žvalgybos technologijos gali tapti ypatingai galingu susidorojimo įrankiu[1223]. Siekiant to išvengti el. žvalgybos technologijų ir paslaugų rinka yra reglamentuojama 1996 m. Wassenaaro susitarimu dėl įprastinės ginkluotės ir dvejopo naudojimo prekių ir technologijų[1224] eksporto kontrolės (Angl. *The Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies*)[1225]. Wassenaaro susitarimo narėmis yra tik tos valstybės, kurios gamina minėtus produktus ir gali kontroliuoti jų eksportą, o šio susitarimo tikslas yra skatinat skaidrumą ir didesnę atsakomybę dėl įprastinės ginkluotės ir dvejopo naudojimo prekių ir technologijų eksporto užtikrinti regioninį ir tarptautinį saugumą ir stabilumą. Nors Wassenaro susitarime dalyvauja iš viso 43 šalys, įskaitant Lietuvą, tačiau tai nėra sutartis, todėl šis susitarimas neturi privalomos teisinės galios. Taip pat Wasenaro susitarimas nėra eksporto draudimo įrankis. Įmonės gali eksportuoti savo kuriamą produkciją, tačiau turi gauti atitinkamos valstybinės institucijos leidimą.

[1222] Schwartz, „Property, Privacy, and Personal Data“, 2004 2003.

[1223] Sari Horwitz, Shyamantha Asokan ir Julie Tate, „Trade in Surveillance Technology Raises Worries“, *Washington Post*, 2011, žiūrėta 2020 m. rugpjūčio 23 d., https://www.washingtonpost.com/world/national-security/trade-in-surveillance-technology-raises-worries/2011/11/22/gIQAFFZOGO_story.html?utm_term=.f1d6995119ae.

[1224] Dvejopo naudojimo objektai (įskaitant programinę įrangą ir technologijas) yra civiliniai objektai, kurie gali būti naudojami kariniams tikslams. Juos eksportuojant iš Europos Sąjungos, jiems taikoma kontrolė. Šiomis kontrolės priemonėmis ypač siekiama užkirsti kelią masinio naikinimo ginklų platinimui. Visų pirma, jos atitinka tikslus, nustatytus 2004 m. balandžio mėn. priimtoje Jungtinių Tautų Saugumo Tarybos rezoliucijoje Nr. 1540.

[1225] „The Wassenaar Agreement On Export Controls for Conventional Arms and Dual-Use Goods and Technologies“, žiūrėta 2020 m. rugpjūčio 23 d., http://www.wassenaar.org/ .

Iki 2013 m. Wassenaro susitarimas neapėmė žvalgybos elektroninėje erdvėje technologijų eksporto kontrolės. Tačiau Arabų pavasaris[1226] buvo aiškiausias įrodymas, jog nekontroliuojamas elektroninės žvalgybos technologijų eksportas gali sunkiai pažeisti asmenų teises[1227]. Todėl 2013 m. Wassenaro susitarimas buvo atnaujintas objektų sąrašą papildant interneto pagrindu veikiančiomis žvalgybos technologijomis[1228]. Nuo 2013 m. eksporto kontrolė yra taikoma įsilaužimo programinei įrangai (angl. *intrusion software*) ir IP ryšio komunikacijų žvalgybos technologijoms (angl. *IP network communications surveillance systems*). Tačiau labai greitai JAV administracija ir kai kurios įsilaužimo programinės įrangos (angl. *intrusion software*) technologijų kūrėjos pastebėjo, kad Wasenaro suistarime įsilaužimo programinė įranga (angl. *intrussion software*) apima bent kokią programą, kodą ar programinės įrangos įrankį, susijusį su įsilaužimo programine įranga (angl. *intrusion software*), o tai trukdo ne tik tolimesnius mokslinius tyrimus, bet ir pačios programinės įrangos naudojimui[1229]. 2017 m. pabaigoje JAV iniciatyvos dėka buvo pritarta Wasenaro susitarimo keitimui, kuriame numatyta išimtis dėl eksporto kontrolės įsilaužimo programinės įrangos (angl. *intrusion software*) pažeidžiamumo moksliniams tyrimams[1230]. Kokios bus 2017 m. pabaigoje sulygtos Wasenaro susitarimo išimčių pasekmės mokslininkai kol kas yra nelinkę prognozuoti ir yra linkę palaukti kol bus oficialiai patvirtinta naujoji išimtis bei numatytos jos taikymo procedūros[1231]. Todėl debatai dėl el. žvalgybos technologijų eksporto ir jų naudojimo, tikėtina, dar yra tik priešaky.

Wasenaro susitarimas yra eksporto – santykių su išorės valstybėmis – kontrolės mechanizmas. Jis neapima valstybės vidaus politikos ir elektroninės žvalgybos technologijų naudojimo pačios valstybės poreikių tenkinimui. Nors yra mokslininkų elektroninės žvalgybos technologijas laikančių kaip galinčias tapti masinio naikinimo ginklu[1232] ir nors egzistuoja tarptautinis susitarimas dėl masinio naikinimo ginklų kūrimo ir naudojimo draudimo[1233], valstybės savo viduje yra nekontroliuojamos nei dėl elektroninės žvalgybos technologijų kūrimo, nei dėl tokių paslaugų naudojimo. Teisėsaugos ir žvalgybos institucijų santykiai su verslo subjektais bei mokslo ir studijų institucijomis valstybės viduje gali pasireikšti keleriopai. Verslo subjektai bei mokslo ir studijų institucijos gali asmens duomenis rinkti ar asmens duomenų tvarkymo programas teisėsaugos ir žvalgybos institucijoms kurti vykdydamos sutartinius santykius, įstaty-

---

[1226] Rob Dickinson, „Responsibility to Protect: Arab Spring Perspectives“, *Buffalo Human Rights Law Review* 20 (2014 2013): 91–124.

[1227] Horwitz, Asokan ir Tate, *op. cit.*, 1218.

[1228] „The Wassenaar Agreement On Export Controls for Conventional Arms and Dual-Use Goods and Technologies“, žiūrėta 2020 m. rugpjūčio 23 d., https://www.wassenaar.org/?s=List-of-DU-Goods-and-Technologies-and-Munitions-List.

[1229] Garrett Hinck, „Wassenaar Export Controls on Surveillance Tools: New Exemptions for Vulnerability Research“, *LawFare*, žiūrėta 2020 m. rugpjūčio 23 d., https://www.lawfareblog.com/wassenaar-export-controls-surveillance-tools-new-exemptions-vulnerability-research.

[1230] Hinck, *supra note,* 1229.

[1231] *Ibid.*

[1232] J. K. Petersen, *Handbook of Surveillance Technologies, Third Edition* (CRC Press, 2012).

[1233] „List of Weapons of Mass Destruction Treaties“, i*Wikipedia*, žiūrėta 2020 m. rugsėjo 9 d., https://en.wikipedia.org/w/index.php?title=List_of_weapons_of_mass_destruction_treaties&oldid=946037660.

mo įpareigotos, vykdydamos mokslinius projektus bei ikiprekybinius pirkimus. Kurį iš bendradarbiavimo variantų teisėsaugos ir žvalgybos institucijos pasirinks, priklauso nuo žvalgybos ar teisėsaugos institucijos poreikio ir norimo vaidinti vaidmens el. žvalgybos paslaugų rinkos kūrime. Imperatyvaus reglamentavimo analize iš esmės yra paremta visa disertacija. Nepaminėtas tik JAV CALEA aktas, kuris pasižymi tuo, kad visos JAV kuriamos technologijos, vadovaujantis CALEA aktu, privalo būti kuriamos taip, kad atsiradus teisėsaugos ar žvalgybos institucijų poreikiui, joms būtų sudaryta galimybė rinti duomenis per tas technologijas[1234]. Todėl disertacijos pabaigai norėčiau paminėti teisės į asmens duomenų apsaugą ypatumus esant dispozityvioms bendradarbiavimo tarp teisėsaugos, žvalgybos bei verslo ir mokslo formoms bei išankstiniam technologijų pritaikymui galimam teisėsaugos poreikių tenkinimui.

Privalomas kuriamų technologijų pritaikymas potencialiems elektroninės žvalgybos poreikiams. 2018 m. pradžioje JAV apkaltino Kinijos įmonę Huawei, kad šios įrenginiuose yra iš anksto įdiegti šnipinėjimo įrenginiai[1235]. Tai sukėlė didelį atgarsį pasaulyje. Tačiau pačiose JAV yra teisės aktas, kuris įpareigoja įmones labai panašiems veiksmams, kokiais buvo apkaltinta Kinija ir Huawei. Dar 1994 m. JAV Senatas veikiamas FTB lobizmo[1236] priėmė Pagalbos teisėsaugos institucijoms dėl komunikacijos prėmomo (angl, *The Communications Assistance for Law Enforcement Act (CALEA))*. CALEA tikslas yra sudaryti sąlygas teisėsaugos ir žvalgybos institucijoms, nepriklausomai nuo nuolat besivystančių technologijų, visada turėti galimybę esant poreikiui rinkti asmens duomenis elektroninėje erdvėje. Į CALEA apimtį patenkančios įmonės privalo savo įrenginius kurti taip, kad šie būtų iš anksto pritaikyti rinkti asmens duomenis, jei tik atsirastų toks poreikis teisėsaugos institucijoms. CALEA 103 (b) str. yra nurodyta, kad teisėsaugos institucijos neturi teisės nurodyti privačiam sektoriui nurodyti kaip projektuoti specializuotus kompiuterių tinklus (angl. *specific network design*) arba kaip fonfiguruoti sistemą (angl. *system configurations*), kaip ir uždrausti. Tačiau teisėsaugos sektorius gali konsultuotis su privačiu sektoriumi tam, kad įsitikintų, jog privataus sektoriaus naudojami techniniai sprendimai atitinka CALEA keliamus reikalavimus[1237].

CALEA veikimo mechanizmas nėra paprastas ir yra paremtas etapų sistema. Pirmasis etapas prasideda nuo to, kad privatus sektorius privalo pasiūlyti tokį techninį standartą Federaliniai komunikacijų komisijai (angl. *Federal Communications Commision (FCC))*[1238], kuris užtikrintų teisėsaugai asmens duomenų rinkimo el. erdvėje galimybes. Vadinasi, privatus sektorius pirmiausia turi ne tik sukurti atitinkamą techninį sprendimą, bet ir susitarti tarpusavyje. Tuo atveju, jeigu privatus sektorius nesugeba susitarti tarpusavyje ir parengti standarto, tuomet standartą turi parengti pati FCC.

[1234] Constance L. Martin, „Exalted Technology: Should CALEA Be Expanded to Authorize Internet Wiretapping Notes and Comments“, *Rutgers Computer & Technology Law Journal* 32, no. 1 (2006 2005): 140–82.

[1235] „Huawei Security Scandal: Everything You Need to Know“, *Forbes*, žiūrėta 2020 m. rugsėjo 9 d., https://www.forbes.com/sites/kateoflahertyuk/2019/02/26/huawei-security-scandal-everything-you-need-to-know/#7e440b1673a5.

[1236] Patricia Moloney Figliola, „Digital Surveillance: The Communications Assistance for Law Enforcement Act“, 17, žiūrėta 2020 m. rugpjūčio 23 d. https://fas.org/sgp/crs/intel/RL30677.pdf.

[1237] Ian Walden, *Telecommunications Law and Regulation* (OUP Oxford, 2012).

[1238] „FAQ on the CALEA Expansion by the FCC“, *Electronic Frontier Foundation*, 2007, žiūrėta 2020 m. rugpjūčio 23 d., https://www.eff.org/pages/calea-faq.

Tačiau iki šiol tokio atvejo praktikoje nebuvo. Pirmasis privataus sektoriaus pasiūlytas standartas – J-STD-025 (arba J standartas)[1239] yra skirtas telefoninių pokalbių turinio ir skambinančio buvimo vietą identifikuojančių duomenų (angl. *call identifying information*) rinkimui. Standarte yra įtvirtinti reikalavimai, kurie užtikrintų technines galimybes esant poreikiui teisėsaugos institucijoms ir telekomunikacijų bendrovės prašyti aukščiau minėtų duomenų. J standartas buvo pirmasis, tačiau ne vienintelis. Šiuo metu yra 25 standartai. Visi jie skelbiami FTB tinklapyje http://www.askcalea.net/[1240]. Antrasis etapas vyksta FCC. Gavusi standartą FCC jį patikrina, kad įsitikintų atitikimu CALEA reikalavimams[1241]. Procesas FCC gali užtukti ilgai. Pavyzdžiui, pirmojo standarto priėmimas užtruko apie dešimtmetį[1242]. Pastabas dėl privataus sektoriaus pasiūlyto standarto FCC gali teikti teisėsaugos institucijos, socialinė visuomenės grupė arba paslaugų el. erdvėje teikėjai, motyvuodamos, kad arba standartas yra per platus ir išeina už CALEA reglamentavimo ribų, arba, kad standartas yra per siauras ir neatitinka CALEA reikalavimų. Vertindama ar privataus sektoriaus pasiūlytas standartas atitinka CALEA reikalavimus, FCC turi teisę plečiamai interpretuoti CALEA nuostatas. Paskutinis etapas yra CALEA standarto įgyvendinimas. Jeigu FCC išvada yra teigiama, tuomet standartas tampa privalomu privačiam sektoriui ir privatus sektorius privalo jį įdiegti į savo technologijas[1243].

Iš pradžių CALEA buvo taikoma tik telefoninei komunikacijai, tačiau vėliau į šio teisės akto galiojimo apimtį buvo įtraukti ir interneto bei IP telefonijos paslaugų bei įrenginių teikėjai[1244]. Nepaisant diskusijų dėl teisėsaugos galių išplėtimo[1245], oficialiai yra laikoma, kad CALEA nėra teisės aktas, išplečiantis teisėsaugos galias. Tai yra teisės, kuris sudaro sąlygas technologiškai teisėsaugos institucijoms turėti galimybę vykdyti asmens duomenų rinkimą el. erdvėje[1246]. Nors CALEA turi sudaryti sąlygas asmens duomenis rinkti tik konkrečių asmenų atžvilgiu[1247], yra manančių, kad CALEA gali sudaryti sąlygas ir masiniam asmens duomenų rinkimui[1248]. Prieš priimant šį teisės

---

[1239] „FCC Adopts CALEA Technical Standards", *Federal Communications Commission*, žiūrėta 2020 m. rugpjūčio 23 d., https://transition.fcc.gov/Bureaus/Engineering_Technology/News_Releases/1999/nret9003.html

[1240] „Communications Assistance for Law Enforcement Act (CALEA)", *TiaOnline*, žiūrėta 2020 m. rugpjūčio 23 d., http://standards.tiaonline.org/standards/technology/calea/index.cfm.

[1241] „CALEA Flexible Deployment Assistance Guide", *TiaOnline*, žiūrėta 2020 m. rugpjūčio 23 d., http://standards.tiaonline.org/standards/technology/calea/documents/flexgide2.pdf .

[1242] Larry Chaffin, *Building a VoIP Network with Nortel's Multimedia Communication Server 5100* (Elsevier, 2006), 431.

[1243] „CALEA Flexible Deployment Assistance Guide", *TiaOnline,* žiūrėta 2020 m. rugpjūčio 23 d., http://standards.tiaonline.org/standards/technology/calea/documents/flexgide2.pdf .

[1244] Chaffin, *Building a VoIP Network with Nortel's Multimedia Communication Server 5100*, 431.

[1245] Sara E. Dirvianskis, „American Council on Education v. FCC: Proper Outcome, Lack of Clarity in the Interpretation of CALEA Developments in Science and Technology Law – Part I: Law and Technology", *Jurimetrics* 47, no. 4 (2007 2006): 463–78. Steven R. Morrison, „Breaking IPhones under CALEA and the All Writs Act: Why the Government Was (Mostly) Right", *Cardozo Law Review* 38, no. 6 (2017 2016): 2039–82.

[1246] Patricia Moloney Figliola, „Digital Surveillance: The Communications Assistance for Law Enforcement Act", 6, žiūrėta 2020 m. rugpjūčio 23 d. https://fas.org/sgp/crs/intel/RL30677.pdf.

[1247] „CALEA Flexible Deployment Assistance Guide", *TiaOnline,* žiūrėta 2020 m. rugpjūčio 23 d., http://standards.tiaonline.org/standards/technology/calea/documents/flexgide2.pdf .

[1248] „Communications Assistance for Law Enforcement Act", *Wikipedia*, žiūrėta 2020 m. rugsėjo 9 d., https://en.wikipedia.org/w/index.php?title=Communications_Assistance_for_Law_Enforcement_Act&oldid=949624418.

aktą Electronic Frontier Foundation (EFF) perspėjo, kad CALEA sumažins JAV programinės ir techninės įrangos (angl. *software and hardware*) patrauklumą užsienio vartotojams, paskatins MTEP migraciją iš JAV ir dirbtinai sukurs šešėlinę ekonomiką tų įrenginių, kurie yra nesuderinami su CALEA reikalavimais, gamybai ir naudojimui[1249]. Tai neįvyko, kadangi užsienio naudotojai neišmano JAV teisės aktų ir nežino koks teisinis režimas galioja jų asmens duomenų atžvilgiu.

JAV taip pat yra numatytos tiek teisinės prievartos, tiek skatinamosios priemonės, kaip verslo subjektus priversti bendradarbiauti su teisėsaugos institucijomis. Pavyzdžiui, FCC patvirtintų standartų privalomumas privačiam sektoriui yra užtikrinamas CALEA numatytomis sankcijomis (pavyzdžiui, Teisingumo departamentas (angl. *Department of Justice*) turi teisę pareikšti civilinį ieškinį privačiam sektoriui[1250])[1251], [1252]. Tačiau be sankcijų CALEA yra numatyta ir skatinamoji standartų įdiegimo priemonė – piniginės kompensacijos (angl. *reimbursement*). Įsigaliojus CALEA JAV Kongresas alokavo 0,5 milijardo JAV dolerių kompensacijoms už standartų įdiegimą[1253].

Sutartinis bendradarbiavimas – tai teisėsaugos ir žvalgybos institucijų bendradarbiavimas su el. ryšių ir paslaugų el. erdvėje teikėjais ir kitomis įmonėmis sutarties pagrindu. *Privacy International* duomenimis 2016 m. duomenimis pasaulyje sutartiniu pagrindu su žvalgybos ir teisėsaugos institucijomis bendradarbiavo 528 įmonės[1254]. Nuo įstatyminio bendradarbiavimo ši bendradarbiavimo forma skiriasi tuo, kad yra sudaroma ir vykdoma laisva valia pagal sutartyje įtvirtintas sąlygas. Šiuos sutartinius santykius reglamentuoja civilinės teisės normos su teisės aktuose įtvirtintomis išimtimis. Sutartinis teisėsaugos ir žvalgybos institucijų bendradarbiavimas su el. ryšių ir paslaugų el. erdvėje teikėjais yra labiau paplitęs JAV[1255], kadangi dauguma paslaugų el. erdvėje teikėjų yra JAV įmonės. Ir nors EOS duomenimis tai yra reta praktika Europoje[1256], tačiau jis vis labiau populiarėja. Didėjantį privataus sektoriaus bendradarbiavimo su žvalgybos ir teisėsaugos institucijomis patvirtina ir ENISA, kuri 2017 metais kreipdamasi į EK išsakė institucijos, koordinuojančios tokį bendradarbiavimą,

---

[1249] „FAQ on the CALEA Expansion by the FCC“, *Electronic Frontier Foundation*, žiūrėta 2020 m. rugpjūčio 23 d., https://www.eff.org/pages/calea-faq.

[1250] 18 U.S. Code § 2522(b), *Legal Information Institute*, žiūrėta 2020 m. rugpjūčio 23 d., https://www.law.cornell.edu/uscode/text/18/2522.

[1251] 18 U.S. Code § 2522(a), *Legal Information Institute*, žiūrėta 2020 m. rugpjūčio 23 d., https://www.law.cornell.edu/uscode/text/18/2522.

[1252] 47 U.S. Code § 229, *Legal Information Institute*, žiūrėta 2020 m. rugpjūčio 23 d., https://www.law.cornell.edu/uscode/text/47/229.

[1253] United States Office of Management and Budget, *Budget of the United States Government: Appendix* (U.S. Government Printing Office, 2004), 666.

[1254] „Privacy International launches the Surveillance Industry Index & New Accompanying Report“, *Privacy International*, žiūrėta 2020 m. rugpjūčio 23 d., https://privacyinternational.org/sites/default/files/global_surveillance.pdf.

[1255] „CIA Front Companies“, žiūrėta 2020 m. rugpjūčio 23 d., http://www.jar2.com/2/Intel/CIA/CIA%20Fronts.htm Rodney Stich, *Explosive Secrets of Covert CIA Companies* (Silverpeak Enterprises, 2006).

[1256] „Study on pre-commercial procurement in the field of Security Within the Framework Contract of Security Studies – ENTR/09/050, *ECORYS*, 9, žiūrėta 2020 m. rugpjūčio 23 d., https://ec.europa.eu/home-affairs/sites/homeaffairs/files/e-library/documents/policies/security/pdf/pcp_sec_finalreport_en.pdf.

sukūrimo poreikį[1257]. Sutartinis bendradarbiavimas yra galimas ir dėl asmens duomenų rinkimo elektroninėje erdvėje[1258], tačiau jis labiau tikėtinas dėl mokslinių tyrimų ir eksperimentinės plėtros kuriant arba perkant parduodant asmens duomenų rinkimo, slaptos žvalgybos elektroninėje erdvėje technologijas. Pažymėtina, kad sutartinis bendradarbiavimas nebūtinai vyksta valstybės viduje, galimas ir tarptautinis bendradarbiavimas. Pavyzdžiui, 2012 m. Ugandos žvalgybos institucijos iš įvairių Didžiosios Britanijos įmonių pirko žvalgybos priemonių stebėti opozicijai, aktyvistams, išriktajai vyriausybei, žurnalistams[1259], o 2015 m. iš Izraelio įmonės pirko interneto srautų stebėjimo technologiją[1260]. Europoje sukurtos žvalgybos technologijos dažnai yra perkamos ne demokratinio režimo ir arba trečiojo pasaulio šalių[1261], todėl *Amnesty International* išreiškusi susirūpinimą, kad ES sukurtų technologijų dėka netiesiogiai yra remiami nedemokratiniai režimai ir sudaromos sąlygos žmogaus teisių pažeidimams, prašė Europos Komisijos ir valstybių narių imtis prevencinių priemonių[1262]. Tačiau tiek identifikuoti pačias priemones, kurių galimai buvo imtasi, tiek jų poveikį yra sudėtinga.

Sutartinis reglamentavimas pasižymi tuo, kad sutarčiai gali būti taikoma bent kurios iš šalių teisė arba pasirinkta kita teisė. Kas reiškia tai, kad jeigu sutartis yra sudaroma su JAV įmone, tai sutarčiai gali būti taikoma JAV teisė, kurioje teisė į asmens duomenų apsaugą negalioja ne JAV asmenų atžvilgiu. Todėl sutartinio bendradarbiavimo atveju teisės į asmens duomenų apsaugą užtikrinimas priklauso nuo to, kiek į tai nori atsižvelgti teisėsaugos ir žvalgybos institucijos.

Moksliniai projektai. Sutartys su įmonėmis ir mokslo bei studijų institucijomis gali būti sudaromos ne tik tiesiogiai, bet ir netiesiogiai. Pavyzdžiui, JAV yra įkurta speciali agentūra, atsakinga už kariniais ir nacionalinio saugumo užtikrinimo tikslais vykdomų mokslinių tyrimų skatinimą ir finansavimo tokiems projektams skyrimą– DARPA[1263]. DARPA programos ir technologijų poreikis atsiranda arba pačios DARPA programų vadovų, arba karinių ir nacionalinio saugumo užtikrinimo struktūrų iniciatyva, o jų kūrėjais gali būti tiek mokslo institucijos, tiek mažos ir vidutinės, tiek ir didelės įmonės[1264]. DARPA skiriamo finansavimo dėka kuriamos įvairiausios technologijos, kurios taip pat gali būti pritaikytos ir ne kariniais tikslais. Pvz. internetas yra DARPA finan-

---

[1257] Catherine Stupp, „EU agency asks Commission to 'avoid fragmentation' in new cyber security plans", *Euractiv*, žiūrėta 2020 m. rugpjūčio 23 d., http://www.euractiv.com/section/cybersecurity/news/eu-agency-asks-commission-to-avoid-fragmentation-in-new-cybersecurity-plans/

[1258] „Privacy International launches the Surveillance Industry Index & New Accompanying Report", *Privacy International*, žiūrėta 2020 m. rugpjūčio 23 d., https://privacyinternational.org/sites/default/files/global_surveillance.pdf.

[1259] „Privacy International's Briefing On The Data Protection Bill For The Committee Stage In The House of Lords", *Privacy International*, žiūrėta 2020 m. rugpjūčio 23 d., http://www.privacyinternational.org/advocacy/656/privacy-internationals-briefing-data-protection-bill-committee-stage-house-lords.

[1260] „Africa Intelligence: Exclusive News on Africa", žiūrėta 2020 m. rugpjūčio 23 d., https://www.africaintelligence.com/.

[1261] „Privacy International launches the Surveillance Industry Index & New Accompanying Report", *Privacy International*, žiūrėta 2020 m. rugpjūčio 23 d., https://privacyinternational.org/sites/default/files/global_surveillance.pdf.

[1262] „Undermining Global Security: The European Union's Global Arms Exports", *Amnesty International*, 2004, žiūrėta 2020 m. rugpjūčio 23 d., http://www.amnesty.eu/static/documents/Text_ACT300032004.pdf .

[1263] „Our Reseach", *Defense Advanced Research Projects Agency*, žiūrėta 2020 m. rugpjūčio 23 d., https://www.darpa.mil/our-research.

[1264] „Defense Advanced Research Projects Agency", žiūrėta 2020 m. rugpjūčio 23 d., https://www.darpa.mil/.

suoto projekto rezultatas[1265]. DARPA tikslas nėra asmens duomenų rinkimo technologijų kūrimas, jos tikslas yra apskritai visų technologijų, skirtų nacionaliniam saugumui ir karinei pramonei kūrimo skatinimas ir finansavimas. Tačiau rugsėjo 11 teroro aktų DARPA buvo gavusi nurodymą inicijuoti projektą „Total Information Awareness (TIA)"[1266], skirtą būtent asmens duomenų rinkimo žvalgybos ir nacionalinio saugumo tikslais el. erdvėje technologijų kūrimui[1267]. TIA tikslas buvo integruojant prieš tai JAV naudotų asmens duomenų rinkimo programų, pvz. Genoa, Genoa II, Genisys, SSNA, EELD, WAE, TIDES, Communicator, HumanID and Bio-Surveillance, komponentus su privataus sektoriaus turimonis kompetencijos duomenų gavybos srityje (angl. *data mining*) sukurti priemonę vykdyti žvalgybą, kontržvalgybą ir teisėsaugos užduotis[1268]. Kuriant TIA sutarties pagrindu bendradarbiavo 9 valstybinės institucijos INSCOM, NSA, DIA, CIA, CIFA, STRATCOM, SOCOM, JFCOM, JWAC[1269] su privačiom įmonėm Science Applications International Corporation[1270], Booz Allen Hamilton, Lockheed Martin Corporation, Schafer Corporation, SRS Technologies, Adroit Systems, CACI Dynamic Systems, ASI Systems International, and Syntek Technologies[1271] ir mokslo bei studijų institucijom Berkeley, Colorado State, Carnegie Mellon, Columbia, Cornell, Dallas, GeorgiaTech, Maryland, MIT ir Southampton[1272]

ES lygiu teisėsaugos ir žvalgybos sektorių bendradarbiavimas su mokslo ir studijų institucijomis bei verslu taip pat yra skatinamas finansuojant mokslinių tyrimų projektus. ES skyrė 1,7 milijardo eurų 2014-2020 periodo H2020 projektų, skirtų saugumo klausimams spręsti, finansavimui[1273]. Taigi, nors nacionalinis saugumas yra išimtis iš ES teisės taikymo srities, tačiau finansuodama mokslinių tyrimų projektus ES skatina mokslą ir verslą kurti technologijas, skirtas saugumo sričiai. ES mokslinių tyrimų ir eksperimentinės plėtros projektų finansavimo vienas iš bruožų – specifinės nuostatos dėl projekto metu sukurtos intelektinės nuosavybės. Paprastai ji atitenka ją sukūrusiai šaliai, tačiau

---

[1265] Evan Andrews, „Who Invented the Internet?", Corbis, žiūrėta 2020 m. rugpjūčio 23 d., https://www.history.com/news/who-invented-the-internet.

[1266] „Total Information Awareness (TIA) System", *Defense Advanced Research Projects Agency,* žiūrėta 2020 m. rugpjūčio 23 d., https://web.archive.org/web/20021003053651/http://www.darpa.mil/iao/tiasystems.htm.

[1267] „More about Department of Defense/NSA Spying", *ACLU*, žiūrėta 2020 m. rugpjūčio 23 d., https://www.aclu.org/other/more-about-department-defensensa-spying

[1268] „*Overview of the Information Awareness Office", Defense Advanced Research Projects Agency*, žiūrėta 2020 m. rugpjūčio 23 d., https://fas.org/irp/agency/dod/poindexter.html. Gina Marie Stevens, *Privacy: Total Information Awareness Programs and Latest Developments* (New York: Novinka Books, 2003).

[1269] „Report to Congress Regarding the Terrorism Information Awareness Program: In response to Consolidated Appropriations Resolution", 2003, žiūrėta 2020 m. rugpjūčio 23 d., https://epic.org/privacy/profiling/tia/may03_report.pdf.

[1270] Shane Harris, „TIA Lives On", *National Journal*, 2016, žiūrėta 2020 m. rugpjūčio 23 d., http://shaneharris.com/magazinestories/tia-lives-on/.

[1271] *Mayle, Adam ir Knott, Alex,* „Outsourcing Big Brother: Office of Total Information Awareness relies on private sector to track Americans", *The Center for Public Integrity*, žiūrėta 2020 m. rugpjūčio 23 d., https://publicintegrity.org/2002/12/17/3164/outsourcing-big-brother.

[1272] Amos Y. Johnson ir kt., „Human Identification at a Distance", *Georgia Institute of Technology College of Computing, žiūrėta 2020 m. rugpjūčio 23 d.*, https://www.cc.gatech.edu/cpl/projects/hid/.

[1273] Chris Jones, „The visible hand: the European Union's Security Industrial Policy", *Statewatch*, 2016, 12, žiūrėta 2020 m. rugpjūčio 23 d., http://www.statewatch.org/analyses/no-297-security-industrial-policy.pdf .

gali būti perduodamos kitiems už rinkos kainą[1274]. Šios nuostatos yra netaikomos saugumo srities projektams. Saugumo projektų ypatybė yra ta, kad sutartyse dėl jų vykdymo ir finansavimo gali būti įtvirtinta nuostata jog intelektinę nuosavybę į sukurtą produktą jį sukūrusios šalys gali naudoti tik tolimesnių tyrimų ir nekomercinio naudojimo tikslais. Mokslinis bendradarbiavimas gali būti skatinamas ir pačių teisėsaugos institucijų iniciatyva. Pavyzdžiui, Europoje veikia Europos teisėsaugos institucijų technologinių paslaugų tinklas (angl. *European Network of Law Enforcement Technology Services*)[1275].

Pagal 7BP EK finansavimą yra skyrusi ir labai kontraversiškai vertinam INDECT projektui[1276]. Šio projekto tikslas buvo sukurti pažangų ir inovatyvų algoritmą, kuris padėtų kovoti su terorizmu it kitais nusikaltimais (prekyba žmonėmis, vaikų pornografija), aptiktų pavojingas realiuoju laiku viešojoje erdvėje vykstančias situacijas (pvz. vykdomus plėšimus) ir atsiradusius grėsmę keliančius daiktus (pvz., peilius, ginklus) bei apie tai praneštų. Skirtingai nuo įprastinių vaizdo stebėjimo technologijų, kuomet asmuo turi pats stebėti ir vertinti situacijas, INDECT projekto metu buvo kuriama technologija, kuri turėjo asmens stebėjimui ir vertinimui pateikti tik, algoritmo „manymu", realiuoju laiku vykstančias pavojingas situacijas. Kadangi technologija neišvengiamai turėjo vykdyti masinį asmens duomenų rinkimą, todėl jos kūrimo proceso dalimi turėjo būti ir modernios asmens duomenų ir privatumo apsaugos technologijos sukūrimas. Kritikai teigė, kad INDECT projekto metu buvo sukurtas masinio asmens duomenų rinkimo įrankis, paremtas apskritai visos visuomenės nuolatiniu stebėjimu, kas pats savaime yra teisės į asmens duomenų apsaugą ir privatumą pažeidimas*[1277]*. *Open Europe* darė prielaidą, kad šį įrankį naudos mažai kam žinoma, tačiau ES lygiu veikianti, kontraversišku pagrindu įsteigta ES žvalgybos institucija – ES bendrų situacijų centras (angl. *EU Joint Situation Centre (SitCen))*[1278], galimai tapsianti Europos CŽV atitikmeniu[1279]. Reaguodamas į visuomenės aktyvistų pasipiktinimą projektu kelios valstybės narės Europos Parlamente kėlė projekto atitikimo demokratinės visuomenės principams klausimą[1280], tačiau fi-

---

1274 „Komisijos komunikatas – Valstybės pagalbos moksliniams tyrimams, technologinei plėtrai ir inovacijoms sistema", *EUR-Lex,* žiūrėta 2020 m. rugpjūčio 23 d., https://eur-lex.europa.eu/legal-content/LT/TXT/?uri=celex:52014XC0627(01)

1275 „European Network of Law Enforcement Technology Services", žiūrėta 2020 m. rugpjūčio 23 d., http://www.enlets.eu/.

1276 „Intelligent Information System Supporting Observation, Searching and Detection for Security of Citizens in Urban Environment", *CORDIS*, žiūrėta 2020 m. rugpjūčio 23 d., https://cordis.europa.eu/project/id/218086.

1277 Ian Johnston, „EU Funding 'Orwellian' Artificial Intelligence Plan to Monitor Public for 'Abnormal Behaviour'", 2009, žiūrėta 2020 m. rugpjūčio 23 d., https://www.telegraph.co.uk/news/uknews/6210255/EU-funding-Orwellian-artificial-intelligence-plan-to-monitor-public-for-abnormal-behaviour.html.

1278 „EU funding ‚Orwellian' artificial intelligence plan to monitor public for „abnormal behaviour", PrivacyFirst, žiūrėta 2020 m. rugpjūčio 23 d., https://www.privacyfirst.eu/images/stories/PDFs/Telegraph20090919_EU-funding-Orwel.pdf.

1279 Ian Johnston, „EU Funding 'Orwellian' Artificial Intelligence Plan to Monitor Public for 'Abnormal Behaviour'", 2009, žiūrėta 2020 m. rugpjūčio 23 d., https://www.telegraph.co.uk/news/uknews/6210255/EU-funding-Orwellian-artificial-intelligence-plan-to-monitor-public-for-abnormal-behaviour.html.

1280 Alexander Alvaro ir kt., „Written Declaration pursuant to Rule 123 of the Rules of Procedure on INDECT (intelligent information system supporting observation, searching and detection for security of citizens in urban environment)", *European Parlament*, žiūrėta 2020 m. rugpjūčio 23 d. http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+WDECL+P7-DCL-2010-0082+0+DOC+PDF+V0//EN&language=EN. „Parliamentary questions", *European Parlament*, žiūrėta 2020 m. rugpjūčio 23 d., https://www.europarl.europa.eu/sides/getAllAnswers.do?reference=E-2010-7521&language=EN.

nansavimas projektui nebuvo sustabdytas. Kalbos, jog projekto metu sukurta technologija buvo bandoma 2012 UEFA Futbolo Čempionate, taip pat buvo paneigtos Europos Parlamento. Tačiau Europos Parlamentui atskleidus, kad projekto metu sukurta technologija bus testuojama Lenkijos Gdansko Rebiechowo oro uoste ir Baltijos Arenoje[1281], nesukėlė nei valstybių narių, nei visuomenės tolimesnio pasipriešinimo. IDECT projektas pasibaigė 2014 m. liepą. Nuo to laiko informacijos apie sukurtos technologijos naudojimą, jos testavimą Lenkijoje, diskusijų dėl atitikimo demokratinės visuomenės principams, viešojoje erdvėje nėra.

Bendrų mokslinių projektų vykdymas galimas ir nacionaliniu lygius. Lietuvoje taip pat yra projektų pagrindu vykdomo žvalgybos ir teisėsaugos institucijų bei įmonių bendradarbiavimo pavyzdžių. Mokslo, inovacijų ir technologijų agentūra (toliau – MITA) bendradarbiaudama su Lietuvos Respublikos krašto apsaugos ministerija 2015 m paskelbė konkursą kuriuo siekiama vykdyti mokslo tiriamuosius darbus ir plėsti jų taikymą gynybos srityje, skatinti bendradarbiavimą su verslo ir pramonės sektoriumi[1282]. Kita mokslinius tyrimus finansuojanti institucija – Lietuvos mokslo taryba – tiesiogiai neturi mokslinių tyrimų programos, skirtos saugumo srities moksliniams projektams, tačiau saugumo srities projektus gali finansuoti per „Valstybės užsakymų programą“[1283]. Projektų finansavimo sąlygose nėra įtvirtinta reikalavimo tais atvejais, kai renkami asmens duomenys, atlikti poveikio privatumui vertinimą. Autorės nuomone, toks reikalavimas turėtų būti privalomas.

3. Ikiprekybiniai pirkimai – tai viešųjų pirkimų būdas kai perkančioji organizacija gali netaikydama Viešųjų pirkimų įstatymo įsigyti rinkoje nesančių prekių ir paslaugų sukūrimą vykdant mokslinius tyrimus ir eksperimentinę plėtrą (toliau – MTEP)[1284]. Ikiprekybinių pirkimų schema yra analogiška natūraliai vykstančiam inovatyviojo produkto pateikimo į rinką procesui[1285]. ESRIF savo ataskaitoje pabrėžia, kad ikiprekybiniai pirkimai – tai mokslinių tyrimų priartinimo prie rinkos mechanizmas[1286]. 8 paveiksle pavaizduota ikiprekybinių

[1281] „Parliamentary questions“, *European Parlament*, žiūrėta 2020 m. rugpjūčio 23 d., http://www.europarl.europa.eu/sides/getAllAnswers.do?reference=E-2010-6912&language=EN

[1282] Kvietimai teikti paraiškas projektų finansavimui yra skelbiami pagal tematikas. 2015 m. buvo paskelbtas kvietimas teikti projektų, skirtų mini klasės bepiločio orlaivio sukūrimui, paraiškas. 2016 km buvo paskelbtas kvietimas teikti projektų, skirtų sunkiai aptinkamo radijo ryšio technologijos sukūrimui, paraiškas. Nors kvietimas teikti projektų paraiškas dėl asmens duomenų rinkimo ir elektroninės žvalgybos nebuvo paskelbtas, tačiau sunkiai aptinkamo radijo ryšio technologijos sukūrimą galima laikyti kontržvalgybos priemone.

[1283] „Valstybės užsakymai“, Lietuvos mokslo taryba, žiūrėta 2020 m. rugpjūčio 23 d., https://www.lmt.lt/lt/mokslo-finansavimas/vykdytos-mokslo-finansavimo-priemones/valstybes-uzsakymai/2295.

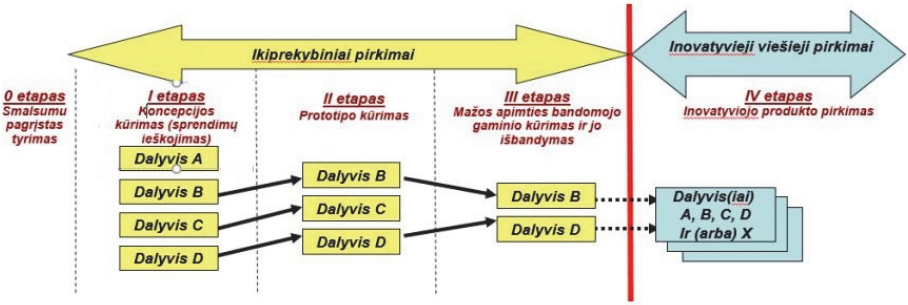
[1284] „Mokslinių tyrimų ir eksperimentinės plėtros paslaugų pirkimų vykdymo tvarkos aprašas, patvirtintas Lietuvos Respublikos Vyriausybės 2020 m. sausio 15 d. nutarimu Nr. 22“, *eSeimas,* žiūrėta 2020 m. rugpjūčio 23 d., https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/48ae1cf0391811eabd71c05e81f09716?jfwid=mmceokxwi.

[1285] „Komisijos komunikatas Europos parlamentui, Tarybai, Europos ekonomikos ir socialinių reikalų komitetui ir Regionų komitetui – Ikiprekybiniai viešieji pirkimai. Naujovių skatinimas siekiant užtikrinti ilgalaikes kokybiškas viešąsias paslaugas Europoje {SEC(2007) 1668}/* KOM/2007/0799 galutinis */“, *EUR-Lex*, žiūrėta 2020 m. rugpjūčio 23 d., https://eur-lex.europa.eu/legal-content/LT/TXT/?uri=CELEX%3A52007DC0799.

[1286] Chris Jones, „The visible hand: the European Union's Security Industrial Policy“, *Statewatch*, 2016, 13, žiūrėta 2020 m. rugpjūčio 23 d., http://www.statewatch.org/analyses/no-297-security-industrial-policy.pdf .

pirkimų vykymo schema Europos Komisijos buvo paskelbta 2007 m.[1287], tačiau teisiniai mechanizmai juos vykdyti Lietuvoje atsirado tik 2015 m.[1288] Nuo įprastų viešųjų pirkimų ikiprekybiniai pirkimai skiriasi tuo, kad:

1) ikiprekybiniai pirkimai vykdomi skirtingais etapais: pirmojo etapo metu yra kuriama koncepcija, antrojo – prototipas, trečioji – bandomoji partija, kuri išbandoma maža apimtimi;
2) juose dalyvauja ne vienas dalyvis, o mažiausiai trys pirmame etape, du – antrame etape, kurie tarpusavyje konkuruoja ir varžosi norėdami perkančiajai organizacijai pasiūlyti kuo geresnį produktą. Vienas dalyvis gali būti tik paskutiniame etape, nors yra rekomenduotina ir paskutiniame etape numatyti ne mažesnį bei 2 dalyvių skaičių, kad nebūtų monopolizuojama rinka;
3) ikiprekybinių pirkimų būdu perkančioji organizacija gali įsigyti tik tokio produkto sukūrimą, kurio nėra rinkoje, ir kurio sukūrimui yra reikalingi moksliniai tyrimai ir eksperimentinė plėtra;



8 pav. *Ikiprekybinių pirkimų vykdymo schema.*

Teisėsaugos ir žvalgybos institucijos, kaip perkančiosios organizacijos, ikiprekybinius pirkimus gali organizuoti, kai jų turimos problemos reikalauja sprendinių, kurie gali būti pateikti tik atlikus MTEP[1289]. Ikiprekybinių pirkimų dalyviai teisėsaugos ir žvalgybos institucijai kaip perkančiajai organizacijai pateikdami ne vieną, o kiekvienas po skirtingą inovatyvų jos problemos sprendimą kartu sudaro sąlygas jai matyti atitinkamų siūlomų inovatyvių sprendinių privalumus ir trūkumus bei palyginus tarpusavyje išsirinkti geriausią variantą. SIP nurodo, kad ikiprekybinių pirkimų dėka

[1287] „Komisijos komunikatas Europos parlamentui, Tarybai, Europos ekonomikos ir socialinių reikalų komitetui ir Regionų komitetui – Ikiprekybiniai viešieji pirkimai. Naujovių skatinimas siekiant užtikrinti ilgalaikes kokybiškas viešąsias paslaugas Europoje {SEC(2007) 1668}/* KOM/2007/0799 galutinis */“, *EUR-Lex*, žiūrėta 2020 m. rugpjūčio 23 d., https://eur-lex.europa.eu/legal-content/LT/TXT/?uri=CELEX%3A52007DC0799.

[1288] „Mokslinių tyrimų ir eksperimentinės plėtros paslaugų pirkimų vykdymo tvarkos aprašas, patvirtintas Lietuvos Respublikos Vyriausybės 2020 m. sausio 15 d. nutarimu Nr. 22“, *eSeimas,* žiūrėta 2020 m. rugpjūčio 23 d., https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/48ae1cf0391811eabd71c05e81f09716?jfwid=mmceokxwi.

[1289] Chris Jones, „The visible hand: the European Union's Security Industrial Policy“, *Statewatch*, 2016, 13, žiūrėta 2020 m. rugpjūčio 23 d., http://www.statewatch.org/analyses/no-297-security-industrial-policy.pdf .

saugumo technologijų sektorius iki 2020 m. turėjo sugeneruoti apie 2 bilijonus eurų papildomų pajamų[1290]. Prognozės buvo tokios optimistiškos todėl, kad ikiprekybinių pirkimų idėja yra labai artima nuo 1977 m. JAV veikiančiai Smulkių ir vidutinių įmonių inovatyvumo skatinimo programai (angl. *The Small Business Innovation Research (SBIR) program*)[1291]. SBIR programoje dalyvauja 12 JAV institucijų, tarp kurių yra ir Gynybos departamentas ir Vidaus saugumo departamentas. Todėl dalis SBIR finansuojamų projektų yra skirti nacionalinės žvalgybos priemonių kūrimui. Analogiškai ikiprekybiniams pirkimams pagal SBIR programą projektai vykdomi trimis stadijomis: 1 stadija – techninės galimybių studijos rengimas, 2 stadija – prototipo kūrimas, 3 stadija – bandomosios partijos testavimas[1292]. Tačiau, skirtingai nuo ikiprekybinių pirkimų, ši stadija nėra finansuojami pagal SBIR programą ir gali būti finansuojama arba kitų agentūrų, saugumo srities atveju, pavyzdžiui, DARPA[1293] lėšomis, arba pačios įmonės lėšomis[1294]. JAV Vidaus saugumo departamentas (angl. *Departament of Homeland security*) 2015 m. paleido naują programą „*Homeland security Sillicon Valley programm*“, kurios tikslas yra įmonių skatinimas kurti produktus, skirtus nacionalinio saugumo užtikrinimui. Ši programa yra orientuota tik į didžiausią technologinį centrą JAV – Silicio slėnį ir, nors ir sudaryta iš 4 etapų, savo esme labai panaši į ikiprekybinių pirkimų schemą. Pagal šią programą jau yra finansuojami 32 projektai ir paskelbtas kvietimas teikti paraiškas dar pagal 4 tematikas[1295]. Taigi, ikiprekybinių pirkimų schema nors ir su tam tikrais slaptumo elementais, tačiau gali būti laikoma efektyvia teisėsaugos ar žvalgybos sektoriaus bendradarbiavimo su mokslo ir studijų institucijomis bei įmonėmis forma.

Lietuvoje ikiprekybinių pirkimų vykdymas yra unikalus tuo, kad visos perkančiosios organizacijos, įskaitant teisėsaugos ir žvalgybos institucijas, privalo gauti MITA leidimą vykdyti ikiprekybinį pirkimą. Leidimas vykdyti ikiprekybinį pirkimą duodamas tik tuo atveju, jeigu atlikus ekspertinį vertinimą prieinama išvada, kad pirkimo objektas atitinka ikiprekybiniam pirkimui keliamus reikalavimus[1296]. Tarp perkančiųjų organizacijų, kurios teikė dokumentus MITA ekspertiniam vertinimui yra VSD bei Generolo Jono Žemaičio Lietuvos karo akademija. Abiejų institucijų planuoti ikiprekybiniai

---

[1290] „Communication from the Commission to the European Parliament, the Council and the European Economic and Social Committee „Security Industrial Policy Action Plan for an innovative and competitive Security Industry“ /* COM/2012/0417 final */, *EUR-Lex,* 10, https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:52012DC0417.

[1291] „The SBIR and STTR Programs“, *America's Seed Fund*, žiūrėta 2020 m. rugpjūčio 23 d., https://www.sbir.gov/about/about-sbir .

[1292] „Three-Phase Program“, *America's Seed Fund*, žiūrėta 2020 m. rugpjūčio 23 d., https://sbir.nih.gov/about/three-phase-program

[1293] „The leading nonprofit defending digital privacy, free speech, and innovation for 30 years and counting!“, *Electronic Frontier Foundation*, žiūrėta 2020 m. rugpjūčio 23 d., https://w2.eff.org/Privacy/TIA/TIA-report.pdf .

[1294] „The SBIR and STTR Programs“, *America's Seed Fund*, žiūrėta 2020 m. rugpjūčio 23 d., https://www.sbir.gov/about/about-sbir .

[1295] „Silicon Valley Innovation Program“, *U. S. Department of Homeland Security,* žiūrėta 2020 m. rugpjūčio 23 d., https://www.dhs.gov/science-and-technology/hsip.

[1296] „Mokslinių tyrimų ir eksperimentinės plėtros paslaugų pirkimų vykdymo tvarkos aprašas, patvirtintas Lietuvos Respublikos Vyriausybės 2020 m. sausio 15 d. nutarimu Nr. 22“, *eSeimas,* žiūrėta 2020 m. rugpjūčio 23 d., https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/48ae1cf0391811eabd71c05e81f09716?jfwid=mmceokxwi.

pirkimai panašūs ir yra susiję su elektroninės erdvės stebėjimo sistemos sukūrimu[1297], tačiau leidimą vykdyti ikiprekybinį pirkmą disertacijos rašymo metu gavo tik Generolo Jono Žemaičio Lietuvos karo akademija. Ikiprekybinis pirkimas galėtų būti sprendimas ir technologijos, kuri padėtų minimalizuoti el. erdvėje teisėsaugos tikslais surenkamus asmens duomenis juos išfiltruojant dar rinkimo metu. Tai leistų apsaugoti su ikiteisminiu tyrimu nesusijusių asmenų interesus, kurie gali tapti ikiteisminio tyrimo medžiaga tik todėl, kad bendravo su įtariamuoju. Taip pat ir įtariamojo bei kitų proceso dalyvių interesus neįtraukti į ikiteisminio tyrimo medžiagą su ja nesusijusių asmeninių duomenų (pvz., privačios nuotraukos, žinutės, el. laiškai). Nors yra įpareigojimas sunaikinti su bylos medžiaga nesusius duomenis, tačiau tokie duomenys yra sunaikinami tik tuomet kai baudžiamoji byla yra perduodama nagrinėti teismui. Vadinasi, ikiteisminio tyrimo metu pareigūnai gali matyti surinktą su byla nesusijusią privačią asmens informaciją. Inicijuoti ikiprekybinį pirkimą, kurio metu būtų sukurtas šią problemą sprendžiantis produktas Lietuvoje šiuo metu yra labai tikslinga dėl struktūrinių fondų priemone „Ikiprekybiniai pirkimai LT“ skiriamo iki 2 mln. Eur finansavimo. Taigi, tiek JAV, tiek ES lygiu, tiek nacionaliniu Lietuvos lygiu yra priemonių kaip paskatinti el. paslaugas teikiančio privataus žvalgybos sektoriaus plėtrą.

Žvalgybos technologijų ir paslaugų rinka yra ypatingai jautri ir tiesiogiai įtakojama ne tik valstybės vidaus, užsienio, bet ir tarptautinės politikos. Dabartinės pasaulinės tendencijos rodo, ne tik Rusijos bei Kinijos ginklavimąsi tradicine karine amunicija, bet ir kibernetine: Rusija paskelbė netrukus atsijungsianti nuo pasaulinio interneto tinklo[1298] bei planuojanti išstoti iš EŽTK[1299]. Tai reikštų, jog Rusija teisiškai nebebūtų įpareigota gerbti pasaulio gyventojų teisės į privatumą ir asmens duomenų apsaugą ir tai suponuotų nevaržomą elektroninę žvalgybą ir atitinkamai elektroninės žvalgybos technologijų paklausos šalyje padidėjimą. Kinija taip pat skelbia, kad iki 2021 m. jau bus sukūrusi savo saugesnį internetą. Tačiau viskas gali vykti ir iš kitos pusės – elektroninės žvalgybos technologijos bei IT bei telekomunikacijų paslaugų teikėjai gali įtakoti valstybės politiką. Microsoft byloje, teismui nusprendus, kad teisėsaugos ir žvalgybos institucijos neturi galios rinkti kitos valstybės serveryje esančių duomenų apie savo piliečius, iškiltų grėsmė debesų kompiuterijai, o jos pagrindu šiandien veikia didžioji dauguma IT ir telekomunikacijų įmonių. Microsoft byloje technologijų gigantei Microsoft nepalankus sprendimas reikštų įmonės, kuri yra vienu iš JAV ekonomikos variklių, sužlugdymu ir jau išsivysčiusių šiuolaikinių technologijų nepaisymu. Todėl teismas iš esmės yra technologijų įkaitu ir bylą nagrinėti turi atsižvelgdamas ir į jo sprendimo poveikį technologinei plėtrai bei inovacijų skatinimui. Arba 2018 m. *Apple v United States* byla, kurioje buvo laukiama teismo sprendimo, kaip manoma, turėjusio turėti lemiamą

[1297] Ikiprekybinis pirkimas „Nacionalinė informacinio poveikio atpažinimo ir analizės ekosistema (NAAS)“, plačiau žr. http://www.lka.lt/lt/moksline-veikla/mokslo-projektine-veikla/naas.html.

[1298] „V. Putino patarėjas: Rusija pasirengusi atsijungti nuo tarptautinio interneto“, *DELFI,* žiūrėta 2020 m. rugpjūčio 23 d., https://www.delfi.lt/mokslas/technologijos/v-putino-patarejas-rusija-pasirengusi-atsijungti-nuo-tarptautinio-interneto.d?id=77336711.

[1299] „Russia may end cooperation with European Court of Human Rights: RIA“, *Reuters*, 2018, žiūrėta 2020 m. rugpjūčio 23 d., https://www.reuters.com/article/us-russia-court-echr-withdrawal/russia-may-end-cooperation-with-european-court-of-human-rights-ria-idUSKCN1GD47U

įtaką sprendžiant kas yra aukščiau: teisė į asmens duomenų apsaugą, JAV technologijų gigante laikomos Apple prestižas ar žvalgybos institucijų interesai nacionalinio saugumo užtikinimo kontekste. Nors žemesnės instancijos teismai ir tenkino FTB prašymą įpareigoti Apple sukurti programinę įrangą, kuri sudarytų jiems iki tol technologiškai neįmanomą galimybę – nesėkmingai bandyti atrakinti teroro akto vykdymu įtariamo mirusio asmens telefoną – koks būtų buvęs Aukščiausiojo teismo sprendimas nėra aišku. FTB atsiėmė prašymą prieš pat teismo posėdį ir rado kitą būdą kaip apeiti Apple telefono apsaugą – paslaugų teikimo sutartį su hakeriu, kuris sukūrė programinę įrangą telefono atrakinimui. Spėjama, kad FTB hakerio paslauga kainavo 4 mln. dolerių. Manoma, kad Apple buvo paruošusi tokius argumentus, kurie visiškai nepaliko vilties FTB šią bylą laimėti. Tai rodo, kad technologiškai labai stiprios įmonės gali įtakoti valstybes netgi žvalgybos srityje. Scott J. Shackelford teiginys, kad ne vien tik valstybės, bet ir įmonės yra įpareigotos laikytis asmens duomenų apsaugos reikalavimų, net ir šioms vykdant valstybės užsakymus[1300] reiškia, kad nors ir kaltinamos asmens duomenų apsaugos reikalavimų nesilaikymu didžiosios el. paslaugų teikėjos dėl savo įtakos pasaulio ekonomikai gali įtakoti valstybes ir tapti asmens teisių apsaugos ambasadoriais.

Savanoriškas bendradarbiavimas. Microsoft, Facebook, Google ir Apple yra JAV įmonės. Todėl JAV teisėsaugos ir žvalgybos institucijos šių įmonių turimus asmens duomenis gali tiesiogiai rinkti iš tiesiogiai iš jų. Likusio pasaulio teisėsaugos institucijos – tik pagal savitarpio pagalbos sutartis su JAV. Reaguodamos į susidariusią situaciją didžiąją dalį paslaugų el. erdvėje pasaulio rinkos valdančios Microsoft, Facebook, Google ir Apple įmonės yra savanoriško bendradarbiavimo tarp teisėsaugos ir kadangi tam tikrus metaduomenis teisėsaugos institucijoms jos suteikia tiesiogiai, ne per tarpusavio pagalbos sutartis. Apple įmonė jos turimus metaduomenis viso pasaulio teisėsaugos institucijoms suteiks pastarosioms prašymą atsiuntus tiesiogiai Apple el. paštu iš oficialaus teisėsaugos institucijos el. pašto adreso. Analogišką praktiką taiko ir Microsoft. Kitoms nei JAV ir Kanados teisėsaugos institucijoms Facebook prašomą informaciją suteikia per Facebook Ireland padalinį, kuriame veikia specialus bendradarbiavimo su teisėsauga padalinys. Google skelbia, kad viso pasaulio teisėsaugos institucijoms jie suteikia tokios pačios apimties informaciją kaip ir JAV teisėsaugos institucijoms[1301]. Šios iniciatyvos minėtos įmonės ėmėsi pačios dar prieš JAV priimant CLOUD aktą bei ES paskelbus El. įrodymų direktyvos projektą. Tai rodo, kad įmonės, teikdamos paslaugas pasauliniu mastu, supranta, kad viso pasaulio teisėsaugos institucijos turėtų turėti vienodas galimybes gauti tyrimui reikalingus asmens duomenis. Didžiausių paslaugų el. erdvėje teikėjų palaikymas būtų esminiu ir inicijuojant naujos tarptautinės sutarties dėl asmens duomenų apsaugos el. erdvėje projektą, padedant užtikrinti ET parengto Žvalgybos kodekso laikymąsi bei modernizuotos 108 Konvencijos nuostatų įgyvendinimą.

[1300] „The „State of Play" of Human Rights Due Diligence Anticipating the next five years", *Institute for Human Rights and Business,* žiūrėta 2020 m. rugpjūčio 23 d., https://www.ihrb.org/pdf/The_State_of_Play_of_Human_Rights_Due_Diligence.pdf. Scott Shackelford, „Human Rights and Cybersecurity Due Diligence: A Comparative Study", *University of Michigan Journal of Law Reform* 50, no. 4 (2017): 859–85.

[1301] „Criminal justice access to data in the cloud: challenges", *Council of Europe*, žiūrėta 2020 m. rugpjūčio 22 d., https://rm.coe.int/1680304b59.

IŠVADOS

1. Asmens duomenims elektroninėje erdvėje galiojančią teisę apsprendžia ne fizinio asmens buvimo vietos teisė, o asmens duomenų maršrutas el. erdvėje, serverių, kuriuose saugomi asmens duomenys lokacija ir teisėsaugos bei žvalgybos institucijų imperatyviu ar dispozityviu pagrindu paslaugas joms teikiančių įmonių galimybė asmens duomenis saugoti, perimti ir pateikti bei tokio pobūdžio asmens duomenų tvarkymui galiojančios teisės normos ar sutarties nuostatos. Teisės į asmens duomenų apsaugą galiojimas pagal dabartinius teisinio reglamentavimo modelius priklauso nuo kitų parametrų– fizinio asmens buvimo vietos teisės ir valstybėse galiojančių supranacionalinių ir nacionalinių teisės aktų nuostatų. Taigi problema dėl teisės į asmens duomenų apsaugą užtikrinimo atsiranda dėl to, kad asmeniui ir jo elektroniniams asmens duomenims gali galioti skirtingi teisiniai režimai, kurie keičiasi asmens duomenims keliaujant elektronine erdve.
2. Šiuo metu egzistuoja trys teisės į asmens duomenų apsaugą suvaržymo modeliai: 1) supranacionalinis, 2) bendrosios teisės tradicijų ir 3) kontinentinės teisės modeliai. Šie modeliai egzistuoja skirtinguose lygmenyse: *macro* lygmenyje yra ES ir ET supranacionalinis reglamentavimas, *micro* – JAV (kaip bendrosios teisės tradicijų valstybės) ir Lietuvos (kaip kontinentinės teisės tradicijų valstybės) reglamentavimas. Tik atsiradus *meta* lygmens (pasauliniam) reglamentavimui (tarptautinės sutarties ar susitarimo forma), yra įmanoma užtikrinti teisę į asmens duomenų apsaugą, kadangi elektroninė erdvė yra globali (*meta* lygmens).
3. Bendrosios teisės tradicijų, kurio pavyzdžiu yra reglamentavimas JAV, modeliui būdinga detali reglamentacija ir diferenciacija:
   3.1. asmenys yra skirstomi į JAV ir ne JAV, o IV JAV Konstitucijos pataisa garantuojama teisė į privatumą ir kartu asmens duomenų apsaugą galioja tik JAV asmenų, esančių JAV teritorijoje atžvilgiu. Vadinasi, visi likę pasaulio gyventojai JAV teisinėje sistemoje neturi teisės į asmens duomenų apsaugą, nepriklausomai nuo to, kad ją turi pagal nacionalinius ar virš nacionalinius teisės aktus;
   3.2. asmens duomenų rinkimas el. erdvėje teisėsaugos tikslais yra reglamentuojamas ECPA, kurioje numatytos skirtingos asmens duomenų rinkimo el. erdvėje procedūros ir apsaugos lygiai priklausomai nuo to ar yra renkama turinio ar neturininio pobūdžio duomenys (metaduomenys) bei nuo to ar jie yra renkami realiuoju laiku, ar yra istorinio pobūdžio;
   3.3. teisminis asmens duomenų rinkimo sankcionavimas yra privalomas, tačiau reikalavimai teisminio sankcionavimo pagrįstumui skiriasi priklausomai nuo asmens duomenų tipo ir pobūdžio;
   3.4. asmens duomenų rinkimas el. erdvėje žvalgybos tikslais reglamentavimas priklauso nuo asmens ir jo asmens duomenų buvimo vietos. FISA yra taikomas tuo atveju, jeigu bent vienas užsienio subjektas yra JAV arba keliauja pro JAV teritoriją – asmuo (užsienio valstybės pilietis) arba jo duomenys. EO 12 333 taikomas tuo atveju, jeigu nei vienas užsienio subjektas nėra JAV.

Taigi, nors bendrosios teisės šalyse teisminės praktikos vaidmuo yra labai svarbus, tačiau aktyvus teismo galimybės užtikrinti teisės į asmens duomenų apsaugą juos renkant teisėsaugos ir žvalgybos tikslais elektroninėje erdvėje yra ribojamos diferencijuotu teisiniu reglamentavimu.

4. Europos kontinentiniam asmens duomenų rinkimo elektroninėje erdvėje teisėsaugos ir žvalgybos tikslais modeliui turėtų būti būdinga integracija, tačiau:
   4.1. nors EŽTK ir Europos Sąjungos teisių Chartija ir galioja visų asmenų ne tik valstybių narių piliečių atžvilgiu, integracija vyksta ne per supranacionalinį teisinį reglamentavimą, o EŽTT ir ESTT plėtojamą jurisprudenciją;
   4.2. nors ET rodo iniciatyvą, kad teisė į asmens duomenų apsaugą būtų užtikrinta asmens duomenis renkant el. erdvėje teisėsaugos ir žvalgybos tikslais ir šiuo metu rengia Elektroninės žvalgybos kodeksą, tačiau faktinio, o ne deklaratyvaus, mechanizmo ji nėra pajėgi parengti ir užtikrinti, jeigu planuojamas Elektroninės žvalgybos kodeksas neturės tarptautinės sutarties statuso ir jam nepritars didžiosios valstybės, kurios žvalgybą elektroninėje erdvėje vykdo plačiausiu mastu;
   4.3. ES lygmeniu asmens duomenų rinkimas el. erdvėje teisėsaugos ir žvalgybos tikslais specialiaisiais aktais nėra reglamentuojamas. ES teisė yra netaikoma žvalgybai, taigi valstybės narės pačios sprendžia kaip reglamentuoti asmens duomenų rinkimą el. erdvėje žvalgybos tikslais. Asmens duomenų rinkimas el. erdvėje teisėsaugos tikslais disertacijos rašymo metu taip pat nėra reglamentuojamas, nors yra pradėtas rengti elektroninių įrodymų direktyvos projektas. 2018 m. įsigaliojusios Asmens duomenų tvarkymo teisėsaugos tikslais direktyvoje specialiųjų nuostatų dėl asmens duomenų rinkimo el. erdvėje nėra.
5. Asmens duomenų rinkimo elektroninėje erdvėje teisėsaugos ir žvalgybos tikslais reglamentavimas Lietuvoje yra nestruktūruotas. Specialiomis normomis reglamentuojamas tik asmens duomenų rinkimas realiuoju laiku iš elektroninių ryšių paslaugų teikėjų, kurie iki 2018 m. paskelbto Elektroninių ryšių kodekso, vadovaujantis ESTT išaiškinimu, neapėmė kitų nei telekomunikacijų paslaugų teikėjų. Istorinio pobūdžio asmens duomenų rinkimas yra vykdomas vadovaujantis BPK ir Kriminalinės žvalgybos įstatymo nuostatomis, skirtoms rinkti bendro pobūdžio duomenis (t. y. ne asmens duomenis) ne elektroninėje aplinkoje. Toks reglamentavimas tik iš dalies atitinka EŽTT jurisprudenciją dėl teisėtų EŽTK 8 str. įtvirtintos teisės į asmens duomenų apsaugą apribojimo pagrindų ir nepakankamai užtikrina teisę į asmens duomenų apsaugą. Asmens duomenų rinkimo elektroninėje erdvėje reglamentavimas Lietuvoje papildytas gerosios reglamentavimo JAV praktikos pavyzdžiais, visiškai atitiktų teisėto teisės į asmens duomenų apsaugą suvaržymui keliamus reikalavimus.
6. Vadovaujantis Konstitucijos 22 str. ir EŽTT jurisprudencija, sankcionavimas yra pirmuoju teisėto teisės į asmens duomenų apsaugą suvaržymo reikalavimu. Tačiau ne visi asmens duomenų rinkimo elektroninėje erdvėje ikiteisminio tyrimo veiksmai yra sankcionuojami teismo. Teisminis sankcionavimas nėra numatytas

BPK 97 str., vadovaujantis BPK 155 str. asmens duomenys yra renkami ikiteisminio tyrimo teisėjo pritarimu, kuris neatitinka motyvuotam teismo sprendimui keliamų reikalavimų.

7. Ikiteisminio tyrimo metu istorinio pobūdžio asmens duomenys gali būti renkami vadovaujantis BPK 97, 145, 147, 155 str., kurie nėra skirti asmens duomenų rinkimo reglamentavimui, todėl neatitinka teisėtam ir proporcingam teisės į asmens duomenų apsaugą suvaržymui keliamų reikalavimų. Adaptuojant gerąją JAV praktiką siūlytina istorinio pobūdžio asmens duomenų rinkimą reglamentuoti ne bendromis, o specialiomis BPK nuostatomis išplečiant BPK 154 str. taikymo apimtis ir istorinio pobūdžio asmens duomenų rinkimui.
8. Asmens duomenų rinkimas realiuoju laiku yra apribotas BPK 154 str. 1 d. įtvirtintomis nusikalstamomis veikomis. Istorinio pobūdžio asmens duomenų rinkimas elektroninėje erdvėje, vadovaujantis BPK 97, 145, 147, 155 str., yra galimas dėl visų BK nusikalstamų veikų. Tai neatitinka EŽTT jurisprudencijos dėl proporcingo EŽTK 8 str. įtvirtintos teisės apribojimo. Išplėtus BPK 154 str. reglamentaciją apimant istorinio pobūdžio asmens duomenų rinkimą tokiam duomenų rinkimui galiotų tokios pačios nuostatos kaip ir realiuoju laiku renkamiems asmens duomenims.
9. BPK 154 str. 6 d. ir Kriminalinės žvalgybos įstatymo 9 str. 7 d. įtvirtinta galimybė nesankcionuotai rinkti asmens duomenis esant asmens sutikimui, jeigu nesinaudojama el. ryšių teikėjų paslaugomis ir įrenginiais. Nereglamentuojant sutikimo gavimo procedūrų, asmens duomenų rinkimo apimties bei nenumačius vėlesnio teismo sankcionavimo tampa lygiaverčiu teismo sprendimui. Tai reiškia, kad vieno asmens sutikimo pagrindu yra renkama ne tik sutikimą davusio asmens, bet ir visų kitų asmenų (įskaitant ne proceso dalyvių), kurie tokio sutikimo nedavė, tačiau el. erdvėje komunikuoja su sutikimą davusiu asmeniu, asmens duomenys. Toks nesankcionuotas asmens duomenų rinkimas pažeidžia Lietuvos Respublikos Konstitucijos 22 str. Ši BPK ir Kriminalinės žvalgybos įstatymo nuostata turėtų būti panaikinta.
10. Siekiant įvesti teisinio aiškumo ir sureglamentuoti BPK 158 str. ir Kriminalinės žvalgybos įstatymo 10 str. 1 d. tiesiogiai nereglamentuojamą prisijungimo prie elektroninės erdvės specifiką, prisijungimas prie elektroninės erdvės BPK turėtų būti įtvirtintas kaip atskira procesinė prievartos priemonė, o Kriminalinės žvalgybos įstatyme atskiras kriminalinės žvalgybos informacijos rinkimo būdas.
11. Kriminalinės žvalgybos įstatyme įtvirtintos dvi galimybės teismo nesankcionuotai rinkti asmens duomenis: 1) iš juridinių asmenų ir 2) esant asmens sutikimui, kai nesinaudojama el. ryšių paslaugų teikėjų įrenginiais ar paslaugomis. Toks nesankcionuotas asmens duomenų rinkimas neatitinka Konstitucijos 22 str. nuostatų.
12. Lietuvoje žvalgybos institucijos asmens duomenis elektroninėje erdvėje gali rinkti žvalgybos ir kontržvalgybos tikslais. Šie tikslai reiškia, kad žvalgybos institucijos veikia arba Lietuvoje arba už Lietuvos teritorijos. Lietuvos Respublikos Konstitucija garantuojama teisė į privatumą, teismų jurisdikcija galioja tik

Lietuvoje arba tik Lietuvos piliečiams, tačiau asmens duomenų rinkimas žvalgybos ir kontržvalgybos tikslais Žvalgybos įstatyme yra reglamentuojamas vienodai.

13. Žvalgybos įstatymas teisminio sankcionavimo poreikį skirsto ne pagal veiklos tikslą – žvalgybą ar kontržvalgyba – o pagal tai ar yra renkama meta duomenys ar turininio pobūdžio informacija. Tai neatitinka EŽTK 8 str. ir Konstitucijos 22 str. dėl to, kad meta duomenys taip pat yra asmens duomenys, o asmenų, kuriems galioja Lietuvos Respublikos Konstitucija atžvilgiu jie, vadovaujantis Žvalgybos įstatymu, yra renkami teismui nesankcionavus. Todėl asmens duomenų rinkimas kontržvalgybos tikslais turėtų būti sankcionuojamas teismo, žvalgybos tikslais – Valstybės gynimo tarybos.
14. Teisėsaugos ir žvalgybos institucijų bendradarbiavimo su privačiais juridiniais asmenimis dėl asmens duomenų rinkimo įtaka teisės į asmens duomenų apsaugą įgyvendinimui priklauso nuo šių subjektų bendradarbiavimo formos ir tikslo: 1) sutartinio bendradarbiavimo atveju teisės į asmens duomenų apsaugą užtikrinimas tampa susitarimo ir susitarimui taikytinos teisės objektu, todėl asmens duomenų apsaugos garantijos tampa minimalios arba tokių iš viso nelieka; 2) savanoriško bendradarbiavimo atveju teisėsaugos pagal nacionalinės teisės nuostatas pateikti prašymai yra pakartotinai vertinami privataus juridinio asmens ir nevisais atvejais yra tenkinami.

PASIŪLYMAI

1. Prokuratūra, bendradarbiaudama su teisininkais, informacijų technologijų specialistais ir elektroninių ryšių tinklų teikėjais turėtų parengti ir patvirtinti asmens duomenų rinkimo elektroninėje erdvėje vadovą, kuriame būtų paaiškinama kokie asmens duomenys gali būti renkami elektroninėje erdvėje, jų skirtumai, nauda ikiteisminiam tyrimui, detalizuotos rinkimo procedūros.

2. BPK ir Kriminalinės žvalgybos įstatymą turėtų būti patikslintas atsižvelgiant į disertacijoje suformuotas išvadas.

1. Autorė BPK 154 str. siūlo tikslinti taip:

154 straipsnis. Elektronine erdve perduodamos informacijos kontrolė, jos fiksavimas ir kaupimas

1. Kai pagal prokuroro prašymą yra priimta ikiteisminio tyrimo teisėjo nutartis, ikiteisminio tyrimo pareigūnas gali ~~klausytis asmenų pokalbių, perduodamų elektroninių ryšių tinklais, daryti jų įrašus,~~ kontroliuoti ~~kitą~~ *baudžiamojo proceso dalyvių* ~~elektroninių ryšių tinklais~~ *elektronine erdve perduodamos ir perduotos* informacijos turinį ir meta duomenis, fiksuoti bei kaupti, jeigu yra pagrindas manyti, kad tokiu būdu galima gauti duomenų apie rengiamą, daromą ar padarytą labai sunkų, sunkų ar apysunkį nusikaltimą arba apie nesunkius nusikaltimus, numatytus Lietuvos Respublikos baudžiamojo kodekso 152[1] straipsnyje, 162 straipsnio 2 dalyje, 170 straipsnyje, 198[2] straipsnio 1 dalyje, 309 straipsnio 2 dalyje *nusikalstamą veiką*, arba jeigu yra ~~pavojus~~ pagrindas manyti, kad nukentėjusiajam, liudytojui ar kitiems proceso dalyviams arba jų artimiesiems *gresia pavojus gyvybei ar sveikatai* ~~bus panaudotas smurtas, prievartavimas ar kitokios neteisėtos veikos.~~

2. Prašyme ikiteisminio tyrimo teisėjui ~~klausytis asmenų pokalbi~~ leisti rinkti ~~elektroninių ryšių tinklais~~ *elektronine erdve* perduodamos informacijos *turinį ir meta duomenis* turi būti nurodyta:

1) turimi duomenys apie baudžiamojo proceso dalyvį, prieš kurį veiksmai turi būti atlikti;

2) pagrindimas, kad yra pagrindas manyti, kad tokiu būdu galima gauti duomenų apie rengiamą, daromą ar padarytą nusikalstamą veiką arba pagrindimas, kad yra pagrindas manyti, kad nukentėjusiajam, liudytojui ar kitiems proceso dalyviams arba jų artimiesiems *gresia pavojus gyvybei ar sveikatai*;

3) konkretūs šio straipsnio 1 dalyje numatyti veiksmai, kuriuos leisti atlikti;

4) veiksmų trukmė;

5) *pagrindimas, jog duomenų negalima gauti kitais būdais* arba, kad taikant kitus būdus jų gavimas apsunkėtų;

3. Ikiteisminio tyrimo teisėjo nutartyje ar prokuroro nutarime ~~klausytis asmenų pokalbių~~, perimti ~~elektroninių ryšių tinklais~~ *elektronine erdve* perduodamos informacijos *turinį ir meta duomenis*, daryti įrašus~~, kontroliuoti kitą elektroninių ryšių tinklais perduodamą informaciją~~ ir fiksuoti bei kaupti turi būti nurodyta:

1) turimi duomenys apie asmenį, prieš kurį veiksmai turi būti atlikti;

2) duomenys, kuriais pagrindžiama būtinybė atlikti šio straipsnio 1 dalyje numatytus veiksmus;

3) konkretūs šio straipsnio 1 dalyje numatyti veiksmai, kuriuos leidžiama atlikti;

4) veiksmų trukmė.

3. ~~Šio straipsnio 1 dalyje nustatyta tvarka gali būti kontroliuojama ir fiksuojama elektroninių ryšių tinklais perduodama informacija, išskyrus jos turinį, jeigu yra pagrindas manyti, kad tokiu būdu galima gauti duomenų apie nesunkius nusikaltimus, numatytus Lietuvos Respublikos baudžiamojo kodekso 166, 198[1] straipsniuose, 309 straipsnio 1 dalyje.~~

4. ~~Asmenų pokalbių, perduodamų elektroninių ryšių tinklais, klausymas, įrašų darymas ar kitos elektroninių ryšių tinklais perduodamos informacijos kontrolė, jos fiksavimas ir kaupimas~~ *Šiame straispnyje tvirtinta procesinė prievartos priemonė* negali ~~trukti~~ *būti taikoma* ilgiau kaip šešis mėnesius. Tiriant sudėtingą ar didelio masto nusikalstamą veiką, šios priemonės taikymas gali būti vieną kartą pratęstas trims mėnesiams.

5. *Elektroninių ryšių paslaugų teikėjai ir kiti juridiniai asmenys, teikiantys paslaugas elektroninėje erdvėje* ~~Ūkio subjektai, teikiantys elektroninių ryšių tinklus ir (ar) paslaugas~~, privalo sudaryti sąlygas ~~klausytis asmenų pokalbių, perduoti~~ *perimti* elektroninių ryšių tinklais perduodamos, ~~ir~~ gaunamos *ir saugomos* informacijos *turinį ir (arba) meta duomenis*. ~~Ūkio subjekto, teikiančio elektroninių ryšių tinklus ir (ar) paslaugas, darbuotojai, nevykdantys šios pareigos ar trukdantys atlikti šiame straipsnyje nurodytus veiksmus, gali būti remiantis šio Kodekso 163 straipsniu nubausti bauda.~~ *Elektroninių ryšių paslaugų teikėjai ir kiti juridiniai asmenys, teikiantys paslaugas elektroninėje erdvėje, turi teisę apskųsti ikiteisminio tyrimo pareigūno, prokuroro veiksmus ir (arba) ikiteisminio tyrimo teisėjo nutartį Apygardos teismui, jeigu turi pakankamą pagrindą manyti, kad tai pažeidžia asmens teisę į asmens duomenų apsaugą.*

~~6. Nukentėjusiųjų, liudytojų ar kitų proceso dalyvių pokalbių, perduodamų elektroninių ryšių tinklais, galima klausytis, daryti jų įrašus, kontroliuoti kitą šių asmenų elektroninių ryšių tinklais perduodamą informaciją, ją fiksuoti ir kaupti šių asmenų prašymu arba jų sutikimu, nors ir nėra tuo reikalu priimtos ikiteisminio tyrimo teisėjo nutarties, jei nesinaudojama ūkio subjektų, teikiančių elektroninių ryšių tinklus ir (ar) paslaugas, paslaugomis ir įrenginiais.~~

7. Draudžiama ~~klausytis~~ perimti ~~elektroninių ryšių tinklų komunikacijos~~ *elektronine erdve perduodamos komunikacijos* tarp gynėjo ir ~~su~~ įtariamojo ar kaltinamojo turinį ir meta duomenis, ~~perduodamų elektroninių ryšių tinklais, daryti jų įrašus, kontroliuoti kitą elektroninių ryšių tinklais tarp jų perduodamą informaciją, ją fiksuoti ir kaupti.~~

8. ~~Dėl pokalbių, perduodamų elektroninių ryšių tinklais, ar kitos elektroninių ryšių tinklais perduodamos informacijos turinio kontrolės fakto~~ Ikiteisminio tyrimo pareigūno surašytame protokole *dėl asmens duomenų rinkimo elektroninėje erdvėje* išdėstomas tik tyrimui reikšmingas duomenų ~~bei garso įrašo~~ turinys. Tyrimui reikšmės neturintys duomenys ~~ir garso įrašai, kurie nėra bendroje laikmenoje su reikšmingais bylai duomenimis ir įrašais,~~ prie bylos nepridedami ir tuoj pat prokuroro nutarimu sunaikinami surašius atitinkamą aktą.

154[1] straipsnis. Asmens duomenų rinkimas prisijungus prie elektroninės erdvės įrenginių

1. Kai pagal prokuroro prašymą ikiteisminio tyrimo teisėjas priima nutartį, ikiteisminio tyrimo institucija ar kitas asmuo, su kuriuo ikiteisminio tyrimo institucija yra sudariusi sutartį, gali prisijungti baudžiamojo proceso dalyvio įrenginio, jeigu yra pagrindas manyti, kad tokiu būdu galima gauti duomenų apie rengiamą, daromą ar padarytą labai sunkų, sunkų nusikaltimą arba yra pagrindas manyti, kad nukentėjusiajam, liudytojui ar kitiems proceso dalyviams arba jų artimiesiems gresia pavojus gyvybei ar sveikatai.

2. Prašyme ikiteisminio tyrimo teisėjui leisti prisijungti prie baudžiamojo proceso dalyvio įrenginio turi būti nurodyta:

1) turimi duomenys apie baudžiamojo proceso dalyvį, prieš kurį veiksmai turi būti atlikti;

2) pagrindimas, kad yra pagrindas manyti, kad tokiu būdu galima gauti duomenų apie rengiamą, daromą ar padarytą labai sunkų ar sunkų nusikaltimą arba pagrindimas, kad yra pagrindas manyti, kad nukentėjusiajam, liudytojui ar kitiems proceso dalyviams arba jų artimiesiems gresia pavojus gyvybei ar sveikatai;

3) informacija apie įrenginį(ius), prie kurio(ų) prašoma leisti prisijungti ir įrenginio(ų) vietas iš kurių prašoma leisti rinkti informaciją;

4) prisijungimo priemonės veikimo ir žalos įrenginiui, prie kurio prisijungiama aprašymas;

5) asmens duomenys, kuriuos prašoma leisti rinkti;

7) veiksmų trukmė;

8) pagrindimas, kad duomenų negalima gauti kitais būdais arba, kad taikant kitus būdus jų gavimas apsunkėtų;

9) pagrindimas, kad šiuo tyrimo būdu siekiami tikslai yra proporcingi teisės į asmens duomenų apsaugą suvaržymui;

10) informacija kas atliks prisijungimo ir asmens duomenų rinkimo veiksmus.

3. Kartu su prašymu turi būti pateikiamas poveikio privatumui vertinimas.

4. Ikiteisminio tyrimo teisėjo nutartyje leisti prisijungti prie baudžiamojo proceso dalyvio įrenginio turi būti nurodyta:

1) turimi duomenys apie asmenį, prieš kurį veiksmai turi būti atlikti;

2) duomenys, kuriais pagrindžiama būtinybė atlikti šio straipsnio 1 dalyje numatytus veiksmus;

3) pagrindimas, kad prisijungimu prie asmens įrenginio siekiami tikslai yra proporcingi teisės į asmens duomenų apsaugą suvaržymui;

4) konkretus(ūs) įrenginys(iai) prie kurių leidžiama prisijungti, ir įrenginio(ių) vietos iš kurių leidžiama rinkti informaciją;

5) asmens duomenys, kuriuos leidžiama rinkti;

6) veiksmų trukmė;

7) subjektas(i), kuriam(iems) leidžiama atlikti prisijungimo ir asmens duomenų rinkimo veiksmus;

8) įpareigojimas informuoti asmenį, prie kurio įrenginio buvo prisijungta, pabaigus ikiteisminį tyrimą ir bylą perdavus teisminiam nagrinėjimui arba nutraukus ikiteisminį tyrimą.

5. Šiame straipsnyje tvirtinta procesinė prievartos priemonė negali būti taikoma ilgiau kaip šešis mėnesius. Tiriant sudėtingą ar didelio masto nusikalstamą veiką, šios priemonės taikymas gali būti vieną kartą pratęstas trims mėnesiams.

6. Tuo atveju, jeigu prisijungimo prie elektroninės erdvės įrenginio(ų) veiksmus atlieka ne pati ikiteisminio tyrimo institucija, privalo būti sudaryta sutartis su paslaugą teikiančiu fiziniu ar juridiniu asmeniu. Sutartyje privalo būti nuostatos, užtikrinančios asmens, prie kurio įrenginio prisijungiama, teisės į asmens duomenų apsaugą užtikrinimą.

7. Draudžiama prisijungti prie gynėjui priklausančių įrenginių.

8. Ikiteisminio tyrimo pareigūno surašytame protokole dėl prisijungimo prie įrenginio (ių)išdėstomas tik tyrimui reikšmingas duomenų turinys. Tyrimui reikšmės neturintys duomenys prie bylos nepridedami ir tuoj pat prokuroro nutarimu sunaikinami surašius atitinkamą aktą.

2. Atsižvelgiant į disertacijoje suformuotas išvadas dėl asmens duomenų rinkimo žvalgybos ir kontržvalgybos tikslais reglamentavimo, disertacijos autorė siūlo tokius Žvalgybos įstatymo pakeitimus:

11 straipsnis. Žvalgybos informacijos rinkimo bendrosios nuostatos

Žvalgybos informacija renkama:

1) ~~taikant žvalgybos metodus~~ *atliekant Valstybės gynimo tarybos sankcionuojamus veiksmus*;

2) atliekant teismo sankcionuojamus veiksmus;

3) gaunant duomenis iš valstybės ir žinybinių registrų, informacinių sistemų ir duomenų bazių;

4) gaunant duomenis iš juridinių ir (ar) fizinių asmenų, *išskyrus tuos duomenis, kurie yra renkami atliekant teismo sankcionuotus veiksmus.*

12 straipsnis. Žvalgybos informacijos rinkimas ~~taikant žvalgybos metodus~~ *atliekant Vyriausybės arba Valstybės gynimo tarybos sankcionuotus veiksmus.*

Žvalgybos informacijos rinkimo ~~metodus, jų taikymo~~ tvarką, terminus ir sąlygas nustato Vyriausybė arba Valstybės gynimo taryba.

13 straipsnis. ~~Žvalgybos~~ Kontržvalgybos informacijos rinkimas atliekant teismo sankcionuojamus veiksmus

1. Pagal motyvuotą apygardos teismo nutartį gali būti atliekami šie veiksmai:

1) ~~elektroninių ryšių tinklais~~ elektronine erdve perduodamos informacijos *turinio ir meta duomenų,* ~~susirašinėjimo ir kitokio asmens susižinojimo~~ stebėjimas ir fiksavimas.

< ...>.

15 straipsnis. Duomenų gavimas iš asmenų

1. Žvalgybos institucijos, įgyvendindamos joms pavestus uždavinius, gali motyvuotu jų vadovų ar įgaliotų žvalgybos pareigūnų raštu kreiptis į asmenis su prašymu pateikti jų veiklai vykdyti reikalingus duomenis. *Tuo atveju, jeigu prašoma pateikti asmens duomenis kontržvalgybos tikslais – toks prašymas privalo būti sankcionuotas teismo, žvalgybos tikslais – Valstybės gynimo tarybos.*

2. Asmuo turi teisę atsisakyti pateikti prašomus duomenis, jeigu turi pakankamą pagrindą matyti, jog duomenų pateikimas pažeistų asmens ar asmenų teisę į asmens duomenų apsaugą. Motyvuotą sprendimą nesuteikti prašomos informacijos asmuo žvalgytos institucijai privalo pateikti ne vėliau nei per 7 dienas nuo nutarties gavimo.

2. Jeigu asmuo per žvalgybos institucijos nurodytą terminą nepateikia prašomų duomenų arba atsisako juos pateikti, žvalgybos institucijos turi teisę kreiptis į bet kurį apygardos teismą su prašymu įpareigoti pateikti duomenis, reikalingus žvalgybos institucijų uždaviniams įgyvendinti. Apygardos teismo nutartis per 7 dienas nuo nutarties gavimo gali būti skundžiama Lietuvos apeliaciniam teismui. Lietuvos apeliacinis teismas privalo skundą išnagrinėti ir priimti nutartį dėl skundo ne vėliau kaip per 7 dienas nuo skundo gavimo šiame teisme dienos. Lietuvos apeliacinio teismo nutartis įsigalioja jos priėmimo dieną ir yra neskundžiama.

3. Privatūs juridiniai asmenys informaciją, kuri kaupiama, saugoma ir (ar) tvarkoma jų duomenų bazėse, žvalgybos institucijoms teikia pagal atskiras sutartis. *Tuo atveju, jeigu prašoma pateikti asmens duomenis kontržvalgybos tikslais – toks prašymas privalo būti sankcionuotas teismo, žvalgybos tikslais – Valstybės gynimo tarybos, prezidento arba Vyriausybės.*

LITERATŪROS SĄRAŠAS

1. TEISĖS AKTAI

Europos Tarybos ir kiti tarptautiniai teisės aktai

1. „Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, regarding supervisory authorities and transborder data flows“, *Council of Europe*, žiūrėta 2020 m. rugsėjo 7 d., https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/223.
2. „Convention on Cybercrime“, *Council of Europe*, žiūrėta 2020 m. rugsėjo 10 d., https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185.
3. „Council of Europe Committee of Ministers Recommendation No. R(87) 15 to the Member States on regulating the use of personal data in the police sector“, *Osce Polis*, žiūrėta 2020 m. rugsėjo 1 d., https://polis.osce.org/council-europe-committee-ministers-recommendation-no-r87-15-member-states-regulating-use-personal.
4. „Council of Europe Parliamentary Assembly. Extract from the minutes of the hearing of the Committee on Legal Affairs and Human Rights on Mass Surveillance“, *Council of Europe*, žiūrėta 2020 m. rugpjūčio 14 d. https://assembly.coe.int/nw/xml/XRef/Xref-XML2HTML-en.asp?fileid=21583&lang=en.
5. „Draft Explanatory Memorandum On The Draft Recommendation Regulating The Use Of Personal Data In The Police Sector“, Įžangos 4 p., *Council of Europe*, žiūrėta 2020 m. rugsėjo 7 d., https://rm.coe.int/168062dfd4.
6. „Draft Explanatory Memorandum On The Draft Recommendation Regulating The Use Of Personal Data In The Police Sector“, *Council of Europe*, žiūrėta 2020 m. rugsėjo 7 d., https://rm.coe.int/168062dfd4..
7. „European Commission for Democracy through Law (Venice Commission), Report on the Democratic Oversight of Signals Intelligence Agencies, adopted at its 102nd Plenary Session (Venice, 20-21 March 2015), Strasbourg, 15 December 2015 CDL-AD(2015)011, Study No. 719/2013“, 58-59 paragrafai, *Venice Commission*, žiūrėta 2020 m. rugpjūčio 16 d., https://www.venice.coe.int/webforms/documents/default.aspx?pdffile=CDL-AD(2015)011-e.
8. „Europos Tarybos Ministrų Komiteto 1973 m. rugsėjo 26 d. rezoliucija (73) 22 dėl asmenų privatumo apsaugos elektroninių duomenų bankų privačiame sektoriuje atžvilgiu“, *Council of Europe*, žiūrėta 2020 m. rugsėjo 7 d., https://rm.coe.int/1680502830.
9. „Europos Tarybos Ministrų Komiteto 1974 m. rugsėjo 20 d. rezoliucija (74) 29 dėl asmenų privatumo apsaugos elektroninių duomenų bankų viešajame sektoriuje atžvilgiu“, *Council of Europe*, žiūrėta 2020 m. rugsėjo 7 d., https://rm.coe.int/16804d1c51.

10. „Europos žmogaus teisių ir pagrindinių laisvių apsaugos konvencija“, *eSeimas*, žiūrėta 2020 m. rugsėjo 9 d., https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/TAIS.19841.
11. „Konvencija dėl asmenų apsaugos ryšium su asmens duomenų automatizuotu tvarkymu (ETS Nr. 108)“, *eSeimas*, žiūrėta 2020 m. rugsėjo 7 d., https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/TAIS.129872.
12. „Konvencija dėl elektroninių nusikaltimų“, *eSeimas*, žiūrėta 2020 m. rugsėjo 10 d., https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/TAIS.228195. „Proposal for a Directive of the European Parliament and of the Council laying down harmonised rules on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings“, *EUR-Lex*, žiūrėta 2020 m. rugpjūčio 25 d., https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1524129181403&uri=COM:2018:226:FIN.
13. „The Wassenaar Agreement On Export Controls for Conventional Arms and Dual-Use Goods and Technologies“, žiūrėta 2020 m. rugpjūčio 23 d., http://www.wassenaar.org/ .
14. „Council of Europe Resolution 2045 (2015). Mass surveillance.“ žiūrėta 2020 m. rugpjūčio 14 d., https://assembly.coe.int/nw/xml/XRef/Xref-XML2HTML-EN.asp?fileid=21692&lang=en.

Europos Sąjungos teisės aktai

15. „1995 m. spalio 24 d. Europos Parlamento ir Tarybos direktyva (95/46/EB) dėl asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo, 31 str., *EUR-Lex*, žiūrėta 2020 m. rugsėjo 7 d., https://eur-lex.europa.eu/legal-content/LT/TXT/?uri=CELEX%3A31995L0046.
16. „20. Deklaracija dėl Sutarties dėl Europos Sąjungos veikimo 16 straipsnio“, *EUR-Lex*, žiūrėta 2020 m. rugsėjo 7 d., https://eur-lex.europa.eu/legal-content/LT/TXT/?uri=CELEX:12016L/AFI/DCL/20.
17. „2000 m. spalio 17 d. Tarybos sprendimas 2000/642/TVR dėl valstybių narių finansinės žvalgybos padalinių bendradarbiavimo susitarimų dėl keitimosi informacija“, *EUR-Lex*, žiūrėta 2020 m. rugpjūčio 15 d., https://eur-lex.europa.eu/legal-content/LT/TXT/HTML/?uri=CELEX:32000D0642&from=EN.
18. „2002 m. birželio 13 d. Tarybos pamatinis sprendimas dėl kovos su terorizmu Nr. 2002/475/TVR“, *EUR-Lex*, žiūrėta 2020 m. rugpjūčio 23 d., https://eur-lex.europa.eu/legal-content/LT/TXT/HTML/?uri=CELEX:02002F0475-20081209&from=EN
19. „2002 m. liepos 12 d. Europos Parlamento ir Tarybos direktyva 2002/58/EB dėl asmens duomenų tvarkymo ir privatumo apsaugos elektroninių ryšių sektoriuje (Direktyva dėl privatumo ir elektroninių ryšių)“, *EUR-Lex,* https://eur-lex.europa.eu/legal-content/LT/TXT/?uri=CELEX%3A32002L0058.
20. „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“, 2 str., *EUR-Lex*, žiūrėta 2020 m. rugpjūčio 17 d., https://eur-lex.europa.eu/legal-content/LT/TXT/?uri=CELEX%3A32006L0024.
21. „2008 m. birželio 23 d. Tarybos sprendimas 2008/615/TVR dėl tarpvalstybinio bendradarbiavimo gerinimo, visų pirma kovos su terorizmu ir tarpvalstybiniu nusikalstamumu srityje“, *EUR-Lex*, žiūrėta 2020 m. rugpjūčio 15 d., https://eur-lex.europa.eu/legal-content/LT/TXT/?uri=celex%3A32008D0615.
22. „2008 m. lapkričio 27 d. Tarybos pamatinis sprendimas 2008/977/TVR dėl asmens duomenų, tvarkomų vykdant policijos ir teisminį bendradarbiavimą baudžiamosiose bylose, apsaugos“, 6 p., *EUR-Lex*, žiūrėta 2020 m. rugpjūčio 14 d., https://eur-lex.europa.eu/legal-content/LT/ALL/?uri=celex%3A32008F0977.
23. „2009 m. vasario 26 d. Tarybos pamatinis sprendimas 2009/315/TVR dėl valstybių narių keitimosi informacija iš nuosprendžių registro organizavimo ir turinio“, *EUR-Lex*, žiūrėta 2020 m. rugpjūčio 15 d., https://eur-lex.europa.eu/legal-content/LT/TXT/?uri=CELEX:32009F0315.
24. „2009 m. balandžio 6 d. Tarybos sprendimas dėl Europos policijos biuro (Europolo) įsteigimo“, *EUR-Lex*, žiūrėta 2020 m. rugpjūčio 14 d., https://eur-lex.europa.eu/legal-content/lt/TXT/?uri=CELEX%3A32009D0371.
25. „2016 m. balandžio 27 d. Europos Parlamento ir Tarybos reglamentas (ES) 2016/679 dėl fizinių asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo ir kuriuo panaikinama Direktyva 95/46/EB (Bendrasis duomenų apsaugos reglamentas)“, *EUR-Lex*, žiūrėta 2020 m. rugpjūčio 15 d., https://eur-lex.europa.eu/legal-content/LT/TXT/?uri=CELEX%3A32016R0679.
26. „2018 m. gruodžio 11 d. Europos Parlamento ir Tarybos direktyva (ES) 2018/1972, kuria nustatomas Europos elektroninių ryšių kodeksas“, *EUR-Lex*, žiūrėta 2020 m. rugsėjo 1 d., https://eur-lex.europa.eu/legal-content/LT/TXT/?uri=CELEX:32018L1972.
27. „21.Deklaracija dėl asmens duomenų apsaugos teisminio bendradarbiavimo baudžiamosiose bylose ir policijos bendradarbiavimo srityse“, *EUR-Lex*, žiūrėta 2020 m. rugpjūčio 14 d., https://eur-lex.europa.eu/legal-content/LT/TXT/?uri=CELEX:12016L/AFI/DCL/21.
28. „Bendrasis asmens duomenų apsaugos reglamentas“, EUR-Lex, 4 str. 1 p., žiūrėta 2020 m. rugsėjo 1 d., https://eur-lex.europa.eu/legal-content/LT/TXT/?uri=CELEX%3A32016R0679 .
29. „Draft Framework Decision on the retention of data processed and stored in connection with the provision of publicly available electronic communications services or data on public communications networks for the purpose of prevention, investigation, detection and prosecution of crime and criminal offence including terrorism“, *Council of the European Union*, žiūrėta 2020 m. rugpjūčio 17 d., https://www.asser.nl/upload/eurowarrant-webroot/documents/cms_eaw_108_2_CouncilDoc.8356.05.pdf.
30. „Europos Sąjungos pagrindinių teisių chartija“, *EUR-Lex*, žiūrėta 2020 m. rugsėjo 9 d., https://eur-lex.europa.eu/legal-content/LT/TXT/PDF/?uri=CELEX:12016P/TXT&from=EN

31. „Europos Vadovų Taryba, Stokholmo veiksmų programa – Atvira ir saugi Europa piliečių labui ir saugumui“, *EUR-Lex,* žiūrėta 2020 m. rugpjūčio 14 d., https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2010:115:0001:0038:LT:PDF.
32. „Pasiūlymas dėl Europos Parlamento ir Tarybos reglamento dėl teisės į privatų gyvenimą ir asmens duomenų apsaugos elektroninių ryšių sektoriuje, kuriuo panaikinama Direktyva 2002/58/EB (Reglamentas dėl privatumo ir elektroninių ryšių), COM/2017/010 final – 2017/03 (COD)“, *EUR-Lex*, žiūrėta 2020 m. rugsėjo 4 d., https://eur-lex.europa.eu/legal-content/LT/TXT/?uri=CELEX%3A52017PC0010 .
33. „Proposal for a Directive of the European Parliament and of the Council laying down harmonised rules on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings“, *EUR-Lex*, žiūrėta 2020 m. rugpjūčio 25 d., https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1524129181403&uri=COM:2018:226:FIN.
34. „Proposal for a Regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal matters“, *EUR-Lex*, žiūrėta 2020 m. rugpjūčio 25 d., https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1524129181403&uri=COM:2018:225:FIN.
35. „Proposal for a Regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal matters“, *EUR-Lex*, žiūrėta 2020 m. rugpjūčio 25 d., https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1524129181403&uri=COM:2018:225:FIN.
36. „Protokolas (Nr. 21) dėl Jungtinės Karalystės ir Airijos pozicijos dėl laisvės, saugumo ir teisingumo erdvės“, *EUR-Lex*, žiūrėta 2020 m. rugpjūčio 14 d., https://eur-lex.europa.eu/legal-content/LT/TXT/?uri=CELEX%3A12012E%2FPRO%2F21.
37. „Protokolas (Nr. 22) dėl Danijos pozicijos“, *EUR-Lex*, žiūrėta 2020 m. rugpjūčio 14 d., https://eur-lex.europa.eu/legal-content/LT/TXT/?uri=CELEX%3A12012E%2FPRO%2F22.
38. „Protokolas (Nr. 36) dėl pereinamojo laikotarpio nuostatų“, *EUR-Lex*, žiūrėta 2020 m. rugpjūčio 14 d., https://eur-lex.europa.eu/legal-content/LT/TXT/?uri=CELEX:12008M/PRO/36.
39. „Regulation (EC) No 767/2008 of the European Parliament and of the Council of 9 July 2008 concerning the Visa Information System (VIS) and the exchange of data between Member States on short-stay visas (VIS Regulation)“, *EUR-Lex*, žiūrėta 2020 m. rugpjūčio 14 d., https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=celex%3A32008R0767.
40. „The Proposal for a Regulation of the European Parliament and of the Council on the establishment, operation and use of the Second Generation Schengen Information System (SIS II) (COM(2005)236 final)“, *EUR-Lex,* žiūrėta 2020 m. rugsėjo 7 d., https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52006XX0419%2802%29.

41. 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.

Lietuvos Respublikos įstatymai ir poįstatyminiai teisės aktai

42. „Aiškinamasis raštas dėl Kriminalinės žvalgybos įstatymo Nr. XI-2234 19 straipsnio pakeitimo įstatymo projekto“, *eSeimas*, žiūrėta 2020 m. rugpjūčio 22 d., https://e-seimas.lrs.lt/portal/legalAct/lt/TAK/6700dca0153111e7b6c9f69dc4ecf19f?jfwid=1c1atz7irf.
43. Lietuvos Respublikos baudžiamojo proceso kodeksas, *eTar,* žiūrėta 2020 m. rugsėjo 11 d., https://www.e-tar.lt/portal/lt/legalAct/TAR.EC588C321777/asr.
44. „Lietuvos Respublikos baudžiamasis kodeksas“, *eTar,* žiūrėta 2020 m. rugsėjo 11 d., https://www.e-tar.lt/portal/lt/legalAct/TAR.2B866DFF7D43/asr.
45. „Kriminalinės žvalgybos įstatymo Nr. XI-2234 19 straipsnio pakeitimo įstatymo projektas“, *eSeimas*, žiūrėta 2020 m. rugpjūčio 22 d., https://e-seimas.lrs.lt/portal/legalAct/lt/TAP/b058e9c0153011e7b6c9f69dc4ecf19f?positionInSearchResults=17&searchModelUUID=7e98340a-7523-43ce-80ca-fbec8cc68615
46. „Lietuvos policijos generalinio komisaro 2019 m. balandžio 11 d. nurodymas Nr. 5-N6 „Dėl bendradarbiavimo su bendrove „Google, Inc.“, *Lietuvos Respublikos generalinė prokuratūra*, žiūrėta 2020 m. rugpjūčio 22 d., https://www.prokuraturos.lt/data/public/uploads/2020/04/neapykantos_nusikaltimu_tyrimo_metodines_rekomendacijos.pdf.
47. „Lietuvos Respublikos elektroninių ryšių įstatymas“, 3 str. 15 d. *eTAR*, žiūrėta 2020 m. rugpjūčio 17 d., https://www.e-tar.lt/portal/lt/legalAct/TAR.82D8168D3049/asr.
48. „Lietuvos Respublikos kibernetinio saugumo įstatymas“, *eTar*, žiūrėta 2020 m. rugsėjo 10 d., https://www.e-tar.lt/portal/lt/legalAct/5468a25089ef11e4a98a9f2247652cf4/asr.
49. „Lietuvos Respublikos Konstitucija“, eSeimas, žiūrėta 2020 m. rugpjūčio 17 d. https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/TAIS.1890?positionInSearchResults=0&searchModelUUID=5138f54d-b9a1-45eb-b519-9011c0500362.
50. „Lietuvos Respublikos nacionalinio saugumo pagrindų įstatymas“, 18 skyrius, *eSeimas*, žiūrėta 2020 m. rugpjūčio 22 d., https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/TAIS.34169/asr.
51. „Lietuvos Respublikos Seimo Teisės ir teisėtvarkos komiteto išvada dėl Kriminalinės žvalgybos įstatymo Nr. XI-2234 19 straipsnio pakeitimo įstatymo projekto“, *eSeimas*, žiūrėta 2020 m. rugpjūčio 22 d., https://e-seimas.lrs.lt/portal/legalAct/lt/TAK/c2ed4380573211e78869ae36ddd5784f?jfwid=1c1atz7irf.
52. „Lietuvos Respublikos Vyriausybės 2013 m. vasario 6 d. nutarimas Nr. 108 „Dėl kriminalinės žvalgybos subjektų sąrašo patvirtinimo ir jų kriminalinės žvalgybos masto nustatymo“, *eTar*, žiūrėta 2020 m. rugpjūčio 23 d., https://www.e-tar.lt/portal/lt/legalAct/TAR.2B88BD021FCB/asr.

53. „Lietuvos Respublikos žvalgybos įstatymas“, *eSeimas*, žiūrėta 2020 m. rugpjūčio 22 d., https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/TAIS.106097/asr.
54. „Mokslinių tyrimų ir eksperimentinės plėtros paslaugų pirkimų vykdymo tvarkos aprašas, patvirtintas Lietuvos Respublikos Vyriausybės 2020 m. sausio 15 d. nutarimu Nr. 22“, *eSeimas,* žiūrėta 2020 m. rugpjūčio 23 d., https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/48ae1cf0391811eabd71c05e81f09716?jfwid=mmceokxwi
55. „Rekomendacijos dėl Kriminalinės žvalgybos įstatymo, Baudžiamojo proceso kodekso normų taikymo ir kriminalinės žvalgybos informacijos panaudojimo baudžiamajame procese, patvirtintos Lietuvos Respublikos generalinio prokuroro 2012 m. gruodžio 31 d. įsakymu Nr. I-383“, *eSeimas*, žiūrėta 2020 m. rugpjūčio 17 d., https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/TAIS.440985?jfwid=-9dzqnu8af.
56. „Teisės departamento išvada dėl Kriminalinės žvalgybos įstatymo Nr. XI-2234 19 straipsnio pakeitimo įstatymo projekto“, *eSeimas*, žiūrėta 2020 m. rugpjūčio 22 d., https://e-seimas.lrs.lt/portal/legalAct/lt/TAK/e67f7d5019fb11e79f4996496b137f39?jfwid=1c1atz7irf.

Jungtinių Amerikos Valstijų teisės aktai

57. „50 U.S. Code § 1801 – Definitions“, *LII / Legal Information Institute*, žiūrėta 2020 m. rugsėjo 4 d., https://www.law.cornell.edu/uscode/text/50/1801 .
58. „18 U.S. Code § 2511 – Interception and Disclosure of Wire, Oral, or Electronic Communications Prohibited“, *Legal Information Institute*, žiūrėta 2020 m. rugsėjo 4 d., https://www.law.cornell.edu/uscode/text/18/2511.
59. „18 U.S. Code § 2518 – Procedure for Interception of Wire, Oral, or Electronic Communications“, *Legal Information Institute*, žiūrėta 2020 m. rugsėjo 4 d., https://www.law.cornell.edu/uscode/text/18/2518.
60. „18 U.S. Code Chapter 119 – Wire and Electronic Communications Interception and Interception of Oral Communications“, *Legal Information Institute*, žiūrėta 2020 m. rugsėjo 4 d., https://www.law.cornell.edu/uscode/text/18/part-I/chapter-119
61. „2015 USA Freedom Act“, *U. S. Congress*, žiūrėta 2020 m. rugsėjo 5 d., https://www.congress.gov/bill/114th-congress/house-bill/2048 .
62. „Electronic Communications Privacy Act of 1986“, žiūrėta 2020 m. rugsėjo 4 d., https://it.ojp.gov/PrivacyLiberty/authorities/statutes/1285.
63. „FISA Amendments Reauthorization Act of 2017“, *U. S. Congress*, žiūrėta 2020 m. rugsėjo 5 d., https://www.congress.gov/bill/115th-congress/house-bill/4478.
64. „Foreign Intelligence Surveillance Act of 1978 Amendments Act of 2008“, *U. S. Congress*, žiūrėta 2020 m. rugsėjo 5 d., https://www.congress.gov/bill/110th-congress/house-bill/6304 .
65. „Investigatory Powers Act 2016“, 229 str. 9 p., žiūrėta 2020 m. rugpjūčio 22 d., https://www.legislation.gov.uk/ukpga/2016/25/part/8/chapter/1/crossheading/main-functions-of-commissioners/enacted?view=plain

66. „Protect America Act of 2007“, *U. S. Congress*, žiūrėta 2020 m. rugsėjo 5 d., https://www.congress.gov/110/plaws/publ55/PLAW-110publ55.pdf.
67. „Section 214 of USA PATRIOT ACT“, *US Congress*, žiūrėta 2020 m. rugsėjo 6 d., https://www.congress.gov/109/plaws/publ177/PLAW-109publ177.htm.
68. „Section 2511(2)(c) of Title 18 „9-7.000 - Electronic Surveillance“, 2015, žiūrėta 2020 m. rugpjūčio 17 d., https://www.justice.gov/jm/jm-9-7000-electronic-surveillance.
69. „Terrorist Surveillance Act of 2006“, *U. S. Congress*, žiūrėta 2020 m. rugsėjo 5 d., https://www.congress.gov/bill/109th-congress/senate-bill/3931?s=1&r=9.
70. „United States Signals Intelligence Directive“, žiūrėta 2020 m. rugpjūčio 14 d., https://www.dni.gov/files/documents/1118/CLEANEDFinal%20USSID%20SP0018.pdf.
71. 18 U. S. Code §3121-3127, *Legal Information Institute*, žiūrėta 2020 m. rugsėjo 4 d., https://www.law.cornell.edu/uscode/text/18/3121.
72. 18 U.S. Code § 2522, *Legal Information Institute*, žiūrėta 2020 m. rugpjūčio 23 d., https://www.law.cornell.edu/uscode/text/18/2522.
73. 18 U.S. Code §2510, *Legal Information Institute*, žiūrėta 2020 m. rugsėjo 4 d., https://www.law.cornell.edu/uscode/text/18/2510.
74. 18 U.S. Code §2703, *Legal Information Institute*, žiūrėta 2020 m. rugsėjo 4 d., https://www.law.cornell.edu/uscode/text/18/2703.
75. 18 U.S.C. § 2818, *Legal Information Institute*, žiūrėta 2020 m. rugsėjo 4 d., https://www.law.cornell.edu/uscode/text/18/1028.
76. 18 U.S.C. Chapter 121 §§ 2701–2712, *Legal Information Institute*, žiūrėta 2020 m. rugsėjo 4 d., https://www.law.cornell.edu/uscode/text/18/part-I/chapter-121.
77. 18 U.S.C. § 2518, *Legal Information Institute*, žiūrėta 2020 m. rugsėjo 4 d., https://www.law.cornell.edu/uscode/text/18/2518.
78. 22 U.S.C. § 2656(f), *Legal Information Institute*, žiūrėta 2020 m. rugsėjo 6 d., https://www.law.cornell.edu/uscode/text/22/2656f.
79. 47 U.S. Code § 229, *Legal Information Institute*, žiūrėta 2020 m. rugpjūčio 23 d., https://www.law.cornell.edu/uscode/text/47/229.
80. 47 U.S.C. § 1841-46, *Legal Information Institute*, žiūrėta 2020 m. rugsėjo 6 d., https://www.law.cornell.edu/uscode/text/47/227.
81. 47 U.S.C. § 1801-12, *Legal Information Institute*, žiūrėta 2020 m. rugsėjo 6 d., https://www.law.cornell.edu/uscode/text/50/1801.
82. 47 U.S.C. § 1821-29, *Legal Information Institute*, žiūrėta 2020 m. rugsėjo 6 d., https://www.law.cornell.edu/uscode/text/12/1821
83. 47 U.S.C. § 1861-62, *Legal Information Institute*, žiūrėta 2020 m. rugsėjo 6 d., https://www.law.cornell.edu/uscode/text/28/1861.
84. 47 U.S.C. § 1881-81, *Legal Information Institute*, žiūrėta 2020 m. rugsėjo 6 d., https://www.law.cornell.edu/uscode/text/50/1881.
85. 50 U.S. Code § 1801, *Legal Information Institute*, žiūrėta 2020 m. rugsėjo 5 d., https://www.law.cornell.edu/uscode/text/50/1801.

86. 50 U.S.C. § 1802, *Legal Information Institute*, žiūrėta 2020 m. rugsėjo 6 d., https://www.law.cornell.edu/uscode/text/50/1802
87. 50 U.S.C. § 1805, *Legal Information Institute*, žiūrėta 2020 m. rugsėjo 6 d., https://www.law.cornell.edu/uscode/text/50/1805.
88. 50 U.S.C. § 1806, *Legal Information Institute*, žiūrėta 2020 m. rugsėjo 6 d., https://www.law.cornell.edu/uscode/text/50/1806.
89. 50 U.S.C. §1861*Legal Information Institute*, žiūrėta 2020 m. rugsėjo 6 d., https://www.law.cornell.edu/uscode/text/50/1861.
90. United States Office of Management and Budget, *Budget of the United States Government: Appendix* (U.S. Government Printing Office, 2004), 666.

Rekomendacinio pobūdžio dokumentai

91. „Article 29 Data Protection Working Party Opinion 9/2004 on a draft Framework Decision on the storage of data processed and retained for the purpose of providing electronic public communications services or data available in public communications networks with a view to the prevention, investigation, detection and prosecution of criminal acts, including terrorism", *European Commission*, žiūrėta 2020 m. rugpjūčio 16 d., https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2004/wp99_en.pdf
92. „Article 29 Data Protection Working Party, Opinion 04/2014 on surveillance of electronic communications for intelligence and national security purposes, Nr. 819/14/EN WP 215", 5, *European Commission*, žiūrėta 2020 m. rugpjūčio 16 d., https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp215_en.pdf.
93. „Communication from the Commission to the European Parliament, the Council and the European Economic and Social Committee „Security Industrial Policy Action Plan for an innovative and competitive Security Industry" /* COM/2012/0417 final */, *EUR-Lex,* 10, https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:52012DC0417.
94. „Council of Europe Committee of Ministers Recommendation No. R(87) 15 to the Member States on regulating the use of personal data in the police sector", *Osce Polis*, žiūrėta 2020 m. rugsėjo 1 d., https://polis.osce.org/council-europe-committee-ministers-recommendation-no-r87-15-member-states-regulating-use-personal.
95. „Document on surveillance of electronic communications for intelligence and national security purposes", *Article 29 Data Protection Working Party*, 2014, žiūrėta 2020 m. rugpjūčio 17 d., https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp228_en.pdf
96. „Green Paper on obtaining evidence in criminal matters from one Member State to another and securing its admissibility (COM/2009/0624 final)", *EUR-Lex*, žiūrėta 2020 m. rugpjūčio 17 d. https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A52009DC0624

97. „Grėsmių nacionaliniam saugumui vertinimas“, *Lietuvos Respublikos valstybės saugumo departamentas, Antrasis operatyvinių tarnybų departamentas prie Krašto apsaugos ministerijos*, žiūrėta 2020 m. rugpjūčio 23 d., https://www.vsd.lt/wp-content/uploads/2019/02/2019-Gresmes-internetui-LT.pdf.
98. „Guide on Article 8 of the Convention – Right to respect for private and family life“, *European Court of Human Rights*, 7, žiūrėta 2020 m. rugpjūčio 23 d., https://www.echr.coe.int/Documents/Guide_Art_8_ENG.pdf.
99. „Komisijos komunikatas – Valstybės pagalbos moksliniams tyrimams, technologinei plėtrai ir inovacijoms sistema“, *EUR-Lex,* žiūrėta 2020 m. rugpjūčio 23 d., https://eur-lex.europa.eu/legal-content/LT/TXT/?uri=celex:52014XC0627(01)
100. „OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data“, *OECD*, žiūrėta 2020 m. rugsėjo 7 d., https://www.oecd.org/internet/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm.
101. „Opinion 4/2007 on the concept of personal data“, *Article 29 Working Party,* žiūrėta 2020 m. rugsėjo 1 d., https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_en.pdf.
102. „Opinion of the European Data Protection Supervisor OJ 2006, C-91/38 on the Proposal for a Council Decision on the establishment, operation and use of the Second Generation Schengen Information System (SIS II) (COM(2005)230 final)“, *EUR-Lex*, žiūrėta 2020 m. rugsėjo 7 d., https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52006XX0419%2801%29.
103. „Opinion of the European Data Protection Supervisor on the data protection reform package“, 4, *European Data Protection Supervisor*, žiūrėta 2020 m. rugpjūčio 15 d., https://edps.europa.eu/sites/edp/files/publication/12-03-07_edps_reform_package_en.pdf.
104. „Opinion of the European Economic and Social Committee on the Communication from the Commission to the European Parliament and the Council on the Use of Security Scanners at EU airports, COM(2010) 311 final“, *European Economic and Social Committee,* 2011, 49–52, žiūrėta https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52011AE0361 .
105. „Opinion on Proposals regarding European Production and Preservation Orders for electronic evidence in criminal matters No. 7/2019“, *European Data Protection Supervisor*, 2019, 9, žiūrėta 2020 m. rugpjūčio 29 d., https://edps.europa.eu/sites/edp/files/publication/19-11-06_opinion_on_e_evidence_proposals_en.pdf.
106. „Reply to Recommendation: Recommendation 2067 (2015). Council of Europe Committee of Ministers“, *Council of Europe*, žiūrėta 2020 m. rugpjūčio 14 d., http://assembly.coe.int/nw/xml/XRef/Xref-XML2HTML-en.asp?fileid=22234&lang=en.

107. „Report on the right to privacy in the digital age (A/HRC/27/37)“, United Nations, 30 June 2014, 7, žiūrėta 2020 m. rugpjūčio 17 d., https://documents-dds-ny.un.org/doc/UNDOC/GEN/G18/239/58/PDF/G1823958.pdf?OpenElement.
108. „The Impact of the Use of Body Scanners in the Field of Aviation Security on Human Rights, Privacy, Personal Dignity, Health and Data Protection“, *European Commission*, 2016, žiūrėta 2020 m. rugsėjo 1 d., https://ec.europa.eu/transport/modes/air/consultations/2009_02_19_body_scanners_en.
109. „Venice Commission Opinion No. 839/ 2016, Poland: On the Act of 15 January 2016 Amending the Police Act and Certain Other Acts“, *Council of Europe*, žiūrėta 2020 m. rugpjūčio 22 d., https://www.venice.coe.int/webforms/documents/default.aspx?pdffile=CDL-AD(2016)012-e.
110. David Kaye, „Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, A/HRC/29/32“, 2015, žiūrėta 2020 m. rugsėjo 1 d., https://ap.ohchr.org/documents/dpage_e.aspx?si=A/HRC/29/32.
111. Komisijos komunikatas Europos parlamentui, Tarybai, Europos ekonomikos ir socialinių reikalų komitetui ir Regionų komitetui – Ikiprekybiniai viešieji pirkimai. Naujovių skatinimas siekiant užtikrinti ilgalaikes kokybiškas viešąsias paslaugas Europoje {SEC(2007) 1668}/* KOM/2007/0799 galutinis */“, *EUR-Lex*, žiūrėta 2020 m. rugpjūčio 23 d., https://eur-lex.europa.eu/legal-content/LT/TXT/?uri=CELEX%3A52007DC0799.

TEISMŲ PRAKTIKA

Europos žmogaus teisių teismo praktika

112. „Europos Žmogaus Teisių Teismo 1978 m. balandžio 28 d. sprendimas byloje Tyrer prieš Jungtinę Karalystę (Nr. 5856/75)“, *Hudoc*, žiūrėta 2020 m. rugsėjo 7 d., https://hudoc.echr.coe.int/fre#{%22itemid%22:[%22001-57587%22]}.
113. „Europos Žmogaus Teisių Teismo 1978 m. rugsėjo 6 d. sprendimas byloje Klass ir kiti prieš Vokietiją (Nr. *5029/71*)“, *Hudoc*, žiūrėta 2020 m. rugsėjo 7 d., https://hudoc.echr.coe.int/rus#{%22itemid%22:[%22001-57510%22]}.
114. „Europos Žmogaus Teisių Teismo 1984 m. rugpjūčio 2 d. sprendimas byloje Malone prieš Jungtinę Karalystę (Nr. 8691/79)“, *Hudoc*, žiūrėta 2020 m. rugsėjo 7 d., https://hudoc.echr.coe.int/rus#{%22itemid%22:[%22001-57533%22]}.
115. „Europos Žmogaus Teisių Teismo 1987 m. kovo 26 d. sprendimas byloje Leander prieš Švediją (Nr. 9248/81)“, *Hudoc*, žiūrėta 2020 m. rugsėjo 7 d., https://hudoc.echr.coe.int/rus#{%22itemid%22:[%22001-57519%22]}.
116. „Europos Žmogaus Teisių Teismo 1995 m. kovo 23 d. sprendimas byloje Loizidou prieš Turkiją (Nr. 15318/89)“, *Hudoc*, žiūrėta 2020 m. rugsėjo 7 d., https://hudoc.echr.coe.int/fre#{%22itemid%22:[%22001-57920%22]}.

117. „Europos Žmogaus Teisių Teismo 1997 m. sprendimas byloje Z. prieš Suomiją (Nr. 22009/93)“, *Hudoc*, žiūrėta 2020 m. rugsėjo 7 d., https://hudoc.echr.coe.int/rus#{%22itemid%22:[%22001-58033%22]}.
118. „Europos Žmogaus Teisių Teismo 1998 m. kovo 25 d. sprendimas byloje Kopp prieš Šveicariją (Nr. 13/1997/797/1000)“, *Hudoc*, žiūrėta 2020 m. rugsėjo 7 d., https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-58144%22]}.
119. „Europos Žmogaus Teisių Teismo 2000 m. gegužės 12 d. sprendimas byloje Khan prieš Jungtinę Karalystę (Nr. 35394/97)“, *Hudoc*, žiūrėta 2020 m. rugsėjo 7 d., https://hudoc.echr.coe.int/fre#{%22itemid%22:[%22001-58841%22]}.
120. „Europos Žmogaus Teisių Teismo 2000 m. vasario 16 d. sprendimas byloje Amann prieš Šveicariją (Nr. 27798/95)“, *Hudoc*, žiūrėta 2020 m. rugsėjo 7 d., https://hudoc.echr.coe.int/tur#{%22itemid%22:[%22001-58497%22]}.
121. „Europos Žmogaus Teisių Teismo 2001 m. rugsėjo 25 d. sprendimas P.G & J.H v. United Kingdom (Nr. 44787/98)“, *Hudoc*, žiūrėta 2020 m. rugpjūčio 29 d., https://hudoc.echr.coe.int/eng-press#{%22itemid%22:[%22003-419654-419935%22]}
122. „Europos Žmogaus Teisių Teismo 2001 m. rugsėjo 25 d., sprendimas byloje P. G. ir J. H. prieš Jungtinę Karalystę (Nr. 44787/98)“, *Hudoc*, žiūrėta 2020 m. rugsėjo 7 d., https://hudoc.echr.coe.int/eng-press#{%22itemid%22:[%22003-419654-419935%22]}.
123. „Europos Žmogaus Teisių Teismo 2005 m. vasario 4 d. sprendimas byloje Mamatkulov ir Askarov prieš Turkiją (Nr. 46827/99 ir 46951/99)“, *Hudoc,* žiūrėta 2020 m. rugsėjo 7 d., https://hudoc.echr.coe.int/fre#{%22itemid%22:[%22001-68183%22]}.
124. „Europos Žmogaus Teisių Teismo 2006 m. birželio 29 d. sprendimas byloje Panteleyenko prieš Ukrainą (11901/02)“, *Hudoc*, žiūrėta 2020 m. rugsėjo 7 d., https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22002-3281%22]}.
125. „Europos Žmogaus Teisių Teismo 2006 m. birželio 6 d. sprendimas byloje Segerstedt-Wiberg ir kiti prieš Švediją (Nr. 62332/00)“, *Hudoc*, žiūrėta 2020 m. rugsėjo 7 d., https://hudoc.echr.coe.int/eng-press#{%22itemid%22:[%22003-1688388-1769677%22]}.
126. „Europos Žmogaus Teisių Teismo 2007 m. liepos 3 d. sprendimas byloje Copland v. United Kingdom (Nr. 62617/00)“, *European Human Rights Court*, žiūrėta 2020 m. rugpjūčio 29 d., https://hudoc.echr.coe.int/rus#{%22itemid%22:[%22001-79996%22]}.
127. „Europos Žmogaus Teisių Teismo 2008 m. gruodžio 2 d. sprendimas K. U. prieš Suomiją (Nr. 2872/02)“, *Hudoc*, žiūrėta 2020 m. rugsėjo 8 d.,https://hudoc.echr.coe.int/eng#{%22fulltext%22:[%222872/02%22],%22documentcollectionid2%22:[%22GRANDCHAMBER%22,%22CHAMBER%22],%22itemid%22:[%22001-89964%22]}.
128. „Europos Žmogaus Teisių Teismo 2008 m. gruodžio 4 d. sprendimas byloje S. ir Marper prieš Jungtinę Karalystę (Nr. 30562/04 ir 30566/04)“, *Hudoc*, žiūrėta 2020 m. rugsėjo 7 d., https://hudoc.echr.coe.int/fre#{%22itemid%22:[%22001-90051%22]}.

129. „Europos Žmogaus Teisių Teismo 2008 m. liepos 17 d. sprendimas I. prieš Suomiją (Nr. 20511/03)“, *Hudoc*, žiūrėta 2020 m. rugsėjo 8 d., https://hudoc.echr.coe.int/eng#{%22fulltext%22:[%2220511/03%22],%22documentcollectionid2%22:[%22GRANDCHAMBER%22,%22CHAMBER%22],%22itemid%22:[%22001-87510%22]},
130. „Europos Žmogaus Teisių Teismo 2008 m. sausio 30 d. sprendimas byloje The Association for European Integration and Human Rights ir Ekimdzhiev prieš Bulgariją (Nr. 62540/00)“, *Hudoc*, žiūrėta 2020 m. rugpjūčio 22 d., https://hudoc.echr.coe.int/fre#{%22itemid%22:[%22001-81323%22]}.
131. „Europos Žmogaus Teisių Teismo 2009 m. rugsėjo 14 d. sprendimas byloje Iordachi ir kiti prieš Moldovą (Nr. 25198/02)“, *Hudoc*, žiūrėta 2020 m. rugsėjo 9 d., https://hudoc.echr.coe.int/fre#{%22itemid%22:[%22001-91245%22]}.
132. „Europos žmogaus teisių teismo 2010 m. gruodžio 16 d. sprendimas byloje Aleksey Ovchinnikov v. Russia“, *Hudoc*, žiūrėta 2020 m. rugsėjo 1 d., https://hudoc.echr.coe.int/eng#{%22fulltext%22:[%22Aleksey%20Ovchinnikov%20v.%20Russia%22],%22documentcollectionid2%22:[%22GRANDCHAMBER%22,%22CHAMBER%22],%22itemid%22:[%22001-102322%22]}.
133. „Europos Žmogaus Teisių Teismo 2011 m. gegužės 10 d. sprendimas byloje Dimitrov-Kazakov prieš Bulgariją (Nr. 11379/03)“, *Hudoc*, žiūrėta 2020 m. rugsėjo 7 d., https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-103258%22]}.
134. „Europos Žmogaus Teisių Teismo 2013 m. balandžio 29 d. sprendimas byloje M. M. prieš Jungtinę Karalystę (Nr. 24029/07)“, *Hudoc*, žiūrėta 2020 m. rugsėjo 7 d., https://hudoc.echr.coe.int/fre#{%22itemid%22:[%22001-114517%22]}.
135. „Europos Žmogaus Teisių Teismo 2014 m. balandžio 18 d. sprendimas byloje Brunet prieš Prancūziją (Nr. 21010/10)“, *Hudoc*, žiūrėta 2020 m. rugsėjo 7 d., https://hudoc.echr.coe.int/eng-press#{%22itemid%22:[%22003-4872410-5953858%22]}.
136. „Europos Žmogaus Teisių Teismo 2015 m. balandžio 15 d. sprendimas byloje Dragojević prieš Kroatiją (Nr. 68955/11)“, *Hudoc*, žiūrėta 2020 m. rugsėjo 9 d., https://hudoc.echr.coe.int/fre#{%22itemid%22:[%22001-150298%22]}.
137. „Europos Žmogaus Teisių Teismo 2015 m. gruodžio 4 d. sprendimas byloje Roman Zakharov prieš Rusiją (Nr. 47143/06)“, *Hudoc*, žiūrėta 2020 m. rugsėjo 9 d., https://hudoc.echr.coe.int/fre#{%22itemid%22:[%22001-159324%22]}.

Europos Sąjungos teisingumo teismo praktika

138. „Advocate General Opinion on Joint Cases C-293/12, C-594/12, 12 December 2013“, 46 paragrafas, *EUR-Lex*, žiūrėta 2020 m. rugpjūčio 17 d. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62012CC0293.
139. „Bureau of Investigative Journalism and Alice Ross v. the United Kingdom, Written Submissions on Behalf of the International Commission of Jurists (ICJ)“, žiūrėta 2020 m. rugpjūčio 16 d., https://www.icj.org/wp-content/

uploads/2016/02/UK-ICJ-AmicusBrief-BJURoss-ECtHR-legalsubmission-2016.pdf.
140. „European Court of Justice, case C-207/16 (Ministerio Fiscal)“, *European Sources*, žiūrėta 2020 m. rugpjūčio 29 d., https://www.europeansources.info/record/case-c-207-16-ministerio-fiscal/.
141. „Europos Sąjungos Teisingumo Teismo 2003 m. lapkričio 3 d. sprendimas byloje C-101/01 Göta hovrätt prieš Bodil Lindqvist, 43 p., *Europa Curia*, žiūrėta 2020 m. rugsėjo 7 d., http://curia.europa.eu/juris/document/document.jsf;jsessionid=9ea7d0f130d59c4626168d7649759faacbd1410d3c1c.e34KaxiLc3eQc40LaxqMbN4Oc3uSe0?text=&docid=48382&pageIndex=0&doclang=LT&mode=lst&dir=&occ=first&part=1&cid=112030
142. „Europos Sąjungos Teisingumo Teismo 2006 m. gegužės 30 d. sprendimas byloje C-317/04 ir C-318/04 Europos Parlamentas prieš Europos Sąjungos Tarybą ir Europos Bendrijų Komisiją, 55 ir 56 p., *Curia Europa*, žiūrėta 2020 m. rugsėjo 7 d., http://curia.europa.eu/juris/document/document.jsf?text=&docid=57549&pageIndex=0&doclang=LT&mode=lst&dir=&occ=first&part=1&cid=145330
143. „Europos Sąjungos Teisingumo Teismo 2009 m. vasario 10 d sprendimas byloje Nr. C-301/06 Airija prieš Europos Parlamentą ir Europos Sąjungos Tarybą“, *InfoCuria*, žiūrėta 2020 m. rugsėjo 8 d., http://curia.europa.eu/juris/liste.jsf?num=C-301/06
144. „Europos Sąjungos Teisingumo Teismo 2010 m. lapkričio 9 d. sprendimas byloje Volker und Markus Schecke GbR and Hartmut Eifert prieš Land Hessen (Nr. C-92/09 ir C-93/09)“, *EUR-Lex*, žiūrėta 2020 m. rugsėjo 7 d., https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62009CJ0092.
145. „Europos Sąjungos Teisingumo Teismo 2013 m. gegužės 30 d. sprendimas byloje Nr. C-270/11 Europos Komisija prieš Švedijos Karalystę“, *InfoCuria*, žiūrėta 2020 m. rugsėjo 8 d., http://curia.europa.eu/juris/liste.jsf?num=C-270/11&language=EN.
146. „Europos Sąjungos Teisingumo Teismo 2014 m. balandžio 30 d. sprendimas bylose Nr. C-390/12 iškeltose Robert Pfleger, Autoart a.s., Mladen Vucicevic, Maroxx Software GmbH, Ing. Hans-Jörg Zehetner“, *InfoCuria*, žiūrėta 2020 m. rugsėjo 8 d., http://curia.europa.eu/juris/document/document.jsf?text=&docid=153472&pageIndex=0&doclang=LT&mode=req&dir=&occ=first&part=1&cid=778912.
147. „Europos Sąjungos Teisingumo Teismo 2014 m. balandžio 8 d. sprendimas byloje Nr. C-293/12 ir C-594/12 Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others, EUR-Lex, žiūrėta 2020 m. rugsėjo 7 d., https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62012CJ0293.
148. „Europos Sąjungos Teisingumo Teismo 2014 m. birželio 5 d. sprendimas byloje Nr. C-329/12 Europos Komisija prieš Vokietiją“, žiūrėta 2020 m. rugsėjo 8 d. http://curia.europa.eu/juris/liste.jsf?language=en&num=C-329/12

149. „Europos Sąjungos Teisingumo Teismo 2016 m. gruodžio 21 d. sprendimas bylose Nr. C-203/15 ir C-698/15 Tele2 Sverige AB prieš Post- och telestyrelsen ir Secretary of State for the Home Department prieš Tom Watson ir kt.“, *InfoCuria*, žiūrėta 2020 m. rugsėjo 10 d., http://curia.europa.eu/juris/document/document.jsf?text=&docid=186492&pageIndex=0&doclang=en&mode=lst&dir=&occ=first&part=1&cid=1319429.
150. „Europos Sąjungos Teisingumo Teismo 2019 m. birželio 13 d. sprendimas Nr. C-193/18 Google LLC prieš Vokietijos Federacinę Respubliką“, *InfoCuria*, žiūrėta 2020 m. rugsėjo 8 d., http://curia.europa.eu/juris/document/document.jsf?text=&docid=214944&pageIndex=0&doclang=EN&mode=req&dir=&occ=first&part=1.
151. „Europos Sąjungos Teisingumo Teismo 2019 m. birželio 5 d. sprendimas byloje Nr. C-142/18 Skype Communications Sàrl prieš Institut belge des services postaux et des télécommunications (IBPT)“, *InfoCuria*, žiūrėta 2020 m. rugsėjo 8 d., http://curia.europa.eu/juris/document/document.jsf?text=&docid=214741&pageIndex=0&doclang=EN&mode=req&dir=&occ=first&part=1.
152. „Europos Sąjungos Teisingumo Teismo sprendimas byloje Éditions Plon v. France“, *Hudoc* žiūrėta 2020 m. rugsėjo 1 d., https://hudoc.echr.coe.int/eng#{%22fulltext%22:[%22%C3%89ditions%20Plon%20v.%20France%22],%22documentcollectionid2%22:[%22GRANDCHAMBER%22,%22CHAMBER%22],%22itemid%22:[%22001-61760%22]} .
153. „Europos Sąjungos Teisingumo Teismo sprendimas byloje Google LLC v Bundesrepublik Deutschland“, *Curia*, žiūrėta 2020 m. rugsėjo 1 d., http://curia.europa.eu/juris/document/document.jsf?text=&docid=214944&pageIndex=0&doclang=EN&mode=req&dir=&occ=first&part=1.
154. „Europos Sąjungos Teisingumo Teismo sprendimas byloje Skype Communications Sàrl v Institut belge des services postaux et des télécommunications (IBPT)“, *Curia*, žiūrėta 2020 m. rugsėjo 1 d., http://curia.europa.eu/juris/document/document.jsf?text=&docid=214741&pageIndex=0&doclang=EN&mode=req&dir=&occ=first&part=1.
155. Europos Sąjungos Teisingumo Teismo 2014 m. balandžio 8 d. sprendimas byloje Nr. C-293/12 ir C-594/12 Digital Rights Ireland Ltd v. Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others, *EUR-Lex*, žiūrėta 2020 m. rugsėjo 7 d., https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62012CJ0293.

Lietuvos Respublikos teismų praktika

156. „Lietuvos Aukščiausiojo Teismo 2014 m. balandžio 14 d. nutartis baudžiamojoje byloje Nr. 2K-194/2014“, *eTeismai*, žiūrėta 2020 m. rugpjūčio 17 d., https://eteismai.lt/byla/9356367523030/2K-194/2014,
157. „Kauno apygardos teismo 2019 m. spalio 29 d. baudžiamasis įsakymas baudžiamojoje byloje Nr. 1-336-966/2019“, *eTeismai*, žiūrėta 2020 m. rugsėjo 9 d., https://e-teismai.lt/byla/16094190275791/1-336-966/2019.

158. „Kauno apygardos teismo Baudžiamųjų bylų skyriaus 2018 m. gegužės 28 d. nuosprendis baudžiamojoje byloje Nr. 1-177-317/2018“, *Infolex praktika*, žiūrėta 2020 m. birželio 15 d., https://www.infolex.lt/tp/1667265 .
159. „Kauno apylinkės teismo 2013 m. birželio 7 d. nuosprendis baudžiamojoje byloje Nr. 1-680-530/2013“, eTeismai, žiūrėta 2020 m. rugsėjo 1 d., https://eteismai.lt/byla/128140400772250/1-680-530/2013.
160. „Klaipėdos apygardos teismo 2020 m. vasario 11 d. nuosprendis baudžiamojoje byloje Nr. 1-27-380/2020“, *eTeismai*, žiūrėta 2020 m. rugsėjo 9 d., https://eteismai.lt/byla/187394242358099/1-27-380/2020?word=neringa%20zaicevait%C4%97.
161. „Klaipėdos apygardos teismo Baudžiamųjų bylų skyriaus 2017 m. vasario 3 d. nuosprendis baudžiamojoje byloje Nr. 1-33-462/2017“, *eTeismai*, žiūrėta 2020 m. rugsėjo 9 d., https://eteismai.lt/byla/14843301723300/1-33-462/2017.
162. „Klaipėdos apylinkės teismo Klaipėdos miesto rūmų 2020 m. vasario 19 d. nutarimas Nr. II-40-890/2020“, *Infolex praktika*, žiūrėta 2020 m. rugpjūčio 29 d., http://www.infolex.lt.skaitykla.mruni.eu/tp/1862389.
163. „Lietuvos apeliacinio teismo 2019 m. balandžio 15 d. nuosprendis baudžiamojoje byloje Nr. 1A-1-449/2019“, *Infolex praktika*, žiūrėta 2020 m. rugpjūčio 22 d., https://www.infolex.lt/tp/1717089 .
164. „Lietuvos Aukščiausiojo Teismo 2010 m. lapkričio 23 d. nutartis baudžiamojoje byloje Nr. 2K-504/2010“, *eTeismai*, žiūrėta 2020 m. rugpjūčio 17 d., https://eteismai.lt/byla/235520032106674/2K-504/2010,
165. „Lietuvos Aukščiausiojo Teismo 2012 m. spalio 30 d. nutartis baudžiamojoje byloje Nr. 2K-P-178/2012“, *eTeismai*, žiūrėta 2020 m. rugpjūčio 22 d., https://eteismai.lt/byla/21539073475107/2K-P-178/2012.
166. „Lietuvos Aukščiausiojo Teismo 2013 m. gegužės 21 d. nutartis baudžiamojoje byloje Nr. 2K-246/2013“, *eTeismai*, žiūrėta 2020 m. rugpjūčio 17 d., https://eteismai.lt/byla/134383672472903/2K-246/2013,
167. „Lietuvos Aukščiausiojo Teismo 2014 m. balandžio 14 d. nutartis baudžiamojoje byloje Nr. 2K-194/2014“, *eTeismai*, žiūrėta 2020 m. rugpjūčio 17 d., https://eteismai.lt/byla/9356367523030/2K-194/2014,
168. „Lietuvos Aukščiausiojo Teismo 2014 m. sausio 14 d. nutartis byloje Nr. 2K-140/2014“, *eTeismai,* žiūrėta 2020 m. rugsėjo 9 d., https://eteismai.lt/byla/239334207577774/2K-140/2014.
169. „Lietuvos Aukščiausiojo Teismo 2014 m. vasario 11 d. nutartis Nr. 2K-49/2014“, *eTeismai*, žiūrėta 2020 m. rugsėjo 8 d., https://eteismai.lt/byla/3132987904756/2K-446/2014.
170. „Lietuvos Aukščiausiojo Teismo 2019 m. gegužės 22 d. nutartis baudžiamojoje byloje Nr. 2K-90-303/2019“, *Infolex praktika*, žiūrėta 2020 m. rugpjūčio 29 d., http://www.infolex.lt.skaitykla.mruni.eu/tp/1727225#B_0
171. „Lietuvos Aukščiausiojo Teismo 2019 m. gegužės 22 d. nutartis baudžiamojoje byloje Nr. 2K-90-303/2019“, Infolex praktika, žiūrėta 2020 m. rugpjūčio 29 d., http://www.infolex.lt.skaitykla.mruni.eu/tp/1727225#B_0

172. „Lietuvos Aukščiausiojo Teismo 2020 m. sausio 7 d. nutartis byloje Nr. 2K-52-942/2020“, *Infolex praktika*, žiūrėta 2020 m. rugsėjo 10 d., http://www.infolex.lt.skaitykla.mruni.eu/tp/1819187.
173. „Lietuvos Aukščiausiojo Teismo Baudžiamųjų bylų skyriaus 2019 m. gruodžio 30 d. nutartis baudžiamojoje byloje Nr. 2K-318-458/2019“, *Infolex praktika*, žiūrėta 2020 m. birželio 15 d., https://www.infolex.lt/tp/1794194.
174. „Lietuvos Aukščiausiojo Teismo Baudžiamųjų bylų skyriaus plenarinės sesijos 2015 m. birželio 1 d. nutartis baudžiamojoje byloje 2K-P-94-895/2015“, *eTeismai*, žiūrėta 2020 m. rugpjūčio 17 d., https://eteismai.lt/byla/44415389271611/2K-P-94-895/2015.
175. „Lietuvos Aukščiausiojo Teismo Elektroninių ryšių tinklais perduodamos informacijos kontrolės, jos fiksavimo ir kaupimo (Baudžiamojo proceso kodekso 154 straipsnis, Kriminalinės žvalgybos įstatymo 10 straipsnis) taikymo apžvalga“, *Lietuvos Aukščiausiasis Teismas*, žiūrėta 2020 m. rugpjūčio 17 d., https://www.lat.lt/lat-praktika/teismu-praktikos-apzvalgos/baudziamuju-bylu-apzvalgos/68.
176. „Lietuvos Aukščiausiojo Teismo Teisės tyrimų ir apibendrinimo departamento apibendrinimas „Procesinės prievartos priemonės – elektroninių ryšių tinklais perduodamos informacijos kontrolės, jos fiksavimo ir kaupimo – taikymas“.
177. „Lietuvos Respublikos Konstitucinio Teismo 2004 m. gruodžio 13 d. nutarimas „Dėl kai kurių teisės aktų, kuriais reguliuojami valstybės tarnybos ir su ja susiję santykiai, atitikties Lietuvos Respublikos konstitucijai ir įstatymams“, žiūrėta 2020 m. rugpjūčio 16 d., https://www.lrkt.lt/lt/teismo-aktai/paieska/135/ta275/content.
178. „Lietuvos Respublikos Konstitucinio Teismo 2004 m. gruodžio 29 d. nutarimas „Dėl organizuoto nusikalstamumo užkardymo“, *Lietuvos Respublikos Konstitucinis Teismas*, žiūrėta 2020 m. rugpjūčio 22 d., https://www.lrkt.lt/lt/teismo-aktai/paieska/135/ta277/content.
179. „Lietuvos Respublikos Konstitucinio Teismo 2019 m. balandžio 18 d. nutarimas Nr. KT13-N5/2019 „Dėl kriminalinės žvalgybos informacijos panaudojimo tiriant korupcinio pobūdžio tarnybinius nusižengimus“, *Lietuvos Respublikos Konstitucinis Teismas*, žiūrėta 2020 m. rugpjūčio 22 d., https://www.lrkt.lt/lt/teismo-aktai/paieska/135/ta1927/content.
180. „Procesinės prievartos priemonės – elektroninių ryšių tinklais perduodamos informacijos kontrolės, jos fiksavimo ir kaupimo –taikymas“, Lietuvos Aukščiausiojo Teismo Teisės tyrimų ir apibendrinimo departamentas, 2015.
181. Lietuvos Aukščiausiojo Teismo 2015 m. kovo 31 d. nutartis baudžiamojoje byloje Nr. 2K-168-139/2015, *eTeismai*, žiūrėta 2020 m. rugpjūčio 17 d., https://eteismai.lt/byla/141589214790674/2K-168-139/2015.

182. „Pennsylvania v. Davis (Majority)“, *Justia Law*, žiūrėta 2020 m. rugpjūčio 22 d., https://law.justia.com/cases/pennsylvania/supreme-court/2019/56-map-2018.html.
183. „Berger v. New York“, *FindLaw*, žiūrėta 2020 m. rugsėjo 4 d., https://caselaw.findlaw.com/us-supreme-court/388/41.html.
184. „*Cf.* SEC v. Jerry T. O'Brien, Inc.“, *FindLAw*, žiūrėta 2020 m. rugsėjo 4 d., https://caselaw.findlaw.com/us-supreme-court/467/735.html.
185. „Commonwealth v. Jones“, *Justia Law*, žiūrėta 2020 m. rugpjūčio 22 d., https://law.justia.com/cases/massachusetts/supreme-court/2019/sjc-12564.html.
186. „Crispin v. Christian Audigier“, *CaseTex*, žiūrėta 2020 m. rugsėjo 4 d., https://casetext.com/case/crispin-v-christian-audigier.
187. „Flatow v. Islamic Republic of Iran and Others“, *FindLaw*, žiūrėta 2020 m. rugpjūčio 23 d., https://caselaw.findlaw.com/us-dc-circuit/1002995.html.
188. „Hester v. United States“, *Legal Information Institute*, žiūrėta 2020 m. rugsėjo 4 d., https://www.law.cornell.edu/supremecourt/text/265/57 .
189. „Hoffa v. United States“, *FindLaw*, žiūrėta 2020 m. rugsėjo 4 d., https://caselaw.findlaw.com/us-supreme-court/385/293.html.
190. „In Re applications of U. S. for orders Pursuant to title 18, U. S. Code Section 2703(d)“, *CaseLaw*, žiūrėta 2020 m. rugsėjo 4 d., https://casetext.com/case/in-re-application-of-us-2. Kaufman v Nest Seekers“, *CaseLaw*, žiūrėta 2020 m. rugsėjo 4 d., https://casetext.com/case/kaufman-v-nest-seekers.
191. „In Re Yahoo Mail Litig., Case No. 13-CV-04980-LHK“, žiūrėta 2020 m. rugsėjo 4 d., https://casetext.com/case/in-re-yahoo-mail-litig-1.
192. „In Re of the United States for Historical Cell Site Data, 747 F. Supp. 2d 827“, *CaseText*, žiūrėta 2020 m. rugsėjo 4 d., https://casetext.com/case/in-re-us-for-historical-cell-site-data.
193. „Katz v. United States“, *FindLaw*, žiūrėta 2020 m. rugsėjo 4 d., https://caselaw.findlaw.com/us-supreme-court/389/347.html.
194. „Kyllo v. United States“, *FindLaw*, žiūrėta 2020 m. rugsėjo 4 d., https://caselaw.findlaw.com/us-supreme-court/533/27.html
195. „Lewis v. United States“, *FindLaw*, žiūrėta 2020 m. rugsėjo 4 d., https://caselaw.findlaw.com/dc-court-of-appeals/1048783.html.
196. „Loop AI Labs Inc v. Gatti“, *CaseText*, žiūrėta 2020 m. rugsėjo 4 d., https://casetext.com/case/loop-ai-labs-inc-v-gatti-13.
197. „Lopez v. United States“, *FindLaw*, žiūrėta 2020 m. rugsėjo 4 d., https://caselaw.findlaw.com/dc-court-of-appeals/1123691.html.
198. „Maryland v. King“, *FindLaw*, žiūrėta 2020 m. rugsėjo 4 d., https://caselaw.findlaw.com/us-supreme-court/12-207.html.
199. „Microsoft Corp. v. United States“, *Harvard Law Review,* žiūrėta 2020 m. rugsėjo 4 d., https://harvardlawreview.org/2016/12/microsoft-corp-v-united-states/.

200. „Mintz v. Mark Bartelstein & Associates, Inc.“, *CaseText*, žiūrėta 2020 m. rugsėjo 4 d., https://casetext.com/case/mintz-v-mark-bartelstein-assocs-1?q=Mintz%20v%20Mark%20Bartelstein%20%26%20Associates,%20Inc.%20&PHONE_NUMBER_GROUP=C&sort=relevance&p=1&type=case.
201. „Oliver v. United States“, *FindLaw*, žiūrėta 2020 m. rugsėjo 4 d., https://caselaw.findlaw.com/dc-court-of-appeals/1318002.html.
202. „Olmstead v. United States“, *FindLaw*, žiūrėta 2020 m. rugsėjo 4 d., https://caselaw.findlaw.com/us-supreme-court/277/438.html Paul Jr. Larkin, „The Fourth Amendment and New Technologies“, *The Heritage Foundation*, žiūrėta 2020 m. rugsėjo 4 d., https://www.heritage.org/report/the-fourth-amendment-and-new-technologies.
203. „On Lee v. United States“, *FindLaw*, žiūrėta 2020 m. rugsėjo 4 d., https://caselaw.findlaw.com/us-supreme-court/343/747.html.
204. „Optiver Australia Pty. Ltd. & Anor v. Tilbra Trading Pty. Ltd. & Ors.“, *CaseText*, žiūrėta 2020 m. rugsėjo 4 d., https://casetext.com/case/optiver-australia-pty-ltd-v-tibra-trading-pty-ltd.
205. „Pascal Pour Elle, Ltd. v. Jin“, *CaseLaw*, žiūrėta 2020 m. rugsėjo 4 d., https://casetext.com/case/pascal-pour-elle-ltd-v-jin.
206. „Quon v. Arch Wireless Operating Co., Inc.“, *FindLaw*, žiūrėta 2020 m. rugsėjo 4 d., https://caselaw.findlaw.com/us-9th-circuit/1144813.html.
207. „Smith v. Maryland“, *FindLaw*, žiūrėta 2020 m. rugsėjo 4 d., https://caselaw.findlaw.com/us-supreme-court/442/735.html.
208. „Steve Jackson Games, Inc. v. United States Secret Service“, *US Supreme Court*, žiūrėta 2020 m. rugsėjo 4 d., https://law.justia.com/cases/federal/district-courts/FSupp/816/432/1976489/.
209. „Suzlon Energy Ltd v. Microsoft Corp.“, *US Supreme Court*, žiūrėta 2020 m. rugsėjo 4 d., https://law.justia.com/cases/federal/appellate-courts/ca9/10-35793/10-35793-2011-10-03.html.
210. „Teisėjo Andrew J. Guilford atskiroji nuomonė byloje Suzlon Energy Ltd. v. Microsoft Corp., No. 10-35793 (9th Cir. 2011)“, US courts, žiūrėta 2020 m. rugsėjo 8 d., http://cdn.ca9.uscourts.gov/datastore/opinions/2011/10/03/10-35793.pdf.
211. „Theofel v. Farey-Jones“, *FindLaw*, žiūrėta 2020 m. rugsėjo 4 d., https://caselaw.findlaw.com/us-9th-circuit/1419886.html.
212. „U. S. v Buck“, CaseLaw, žiūrėta 2020 m. rugsėjo 5 d., https://caselaw.findlaw.com/us-5th-circuit/1054668.html. „Zweibon v. Mitchell“, *US Supreme Court*, žiūrėta 2020 m. rugsėjo 5 d., https://law.justia.com/cases/federal/district-courts/FSupp/444/1296/2149063/.
213. „U. S. v U. S. District Court for Eastern District of Michigan, Southern Division“, *US Supreme Court*, žiūrėta 2020 m. rugsėjo 5 d., https://supreme.justia.com/cases/federal/us/407/297/.
214. „United States of America v. Apple Macpro Computer, Apple Mac Mini Computer, Apple I Phone 6 Plus, Ellular Telephone Western Digital My Book For

Mac External Hard Drive, Western Digital My Book Velociraptor Duo External Hard Drive“, *CaseLaw*, žiūrėta 2020 m. rugpjūčio 22 d., https://caselaw.findlaw.com/us-3rd-circuit/1853477.html.
215. „United States of America v. John Doe“, *CaseLaw*, žiūrėta 2020 m. rugpjūčio 22 d., https://caselaw.findlaw.com/us-9th-circuit/1747358.html.
216. „United States v. Apple Inc.“, *CaseLaw*, žiūrėta 2020 m. rugsėjo 4 d., https://caselaw.findlaw.com/us-2nd-circuit/1702133.html.
217. „United States v. Biasucci“, *CaseText*, žiūrėta 2020 m. rugsėjo 5 d., https://casetext.com/case/united-states-v-biasucci.
218. „United States v. Councilman“, *CaseLaw*, žiūrėta 2020 m. rugsėjo 4 d., https://caselaw.findlaw.com/us-1st-circuit/1290871.html.
219. „United States v. Cuevas-Sanchez“, *CaseText*, žiūrėta 2020 m. rugsėjo 5 d., https://casetext.com/case/us-v-cuevas-sanchez.
220. „United States v. Dunn“, *FindLaw*, žiūrėta 2020 m. rugsėjo 4 d., https://caselaw.findlaw.com/us-9th-circuit/1266164.html.
221. „United States v. Falls“, *CaseLaw*, žiūrėta 2020 m. rugsėjo 5 d., https://caselaw.findlaw.com/us-2nd-circuit/1207287.html.
222. „United States v. Jones“, FindLaw, žiūrėta 2020 m. rugsėjo 4 d., https://caselaw.findlaw.com/us-5th-circuit/1364966.html
223. „United States v. Koyomejian“, *CaseText*, žiūrėta 2020 m. rugsėjo 5 d., https://casetext.com/case/us-v-koyomejian.
224. „United States v. Mesa-Rincon“, *CaseText*, žiūrėta 2020 m. rugsėjo 5 d., https://casetext.com/case/us-v-mesa-rincon.
225. „United States v. Miller“, *FindLAw*, žiūrėta 2020 m. rugsėjo 4 d., https://caselaw.findlaw.com/us-3rd-circuit/1177040.html.
226. „United States v. New York Telephone Company“, *US Supreme Court*, žiūrėta 2020 m. rugsėjo 5 d., https://supreme.justia.com/cases/federal/us/434/159/.
227. „United States v. Torres“, *CaseLaw*, žiūrėta 2020 m. rugsėjo 5 d., https://caselaw.findlaw.com/us-8th-circuit/1214998.html.
228. „United States v. United States District Court“, *FindLaw*, žiūrėta 2020 m. rugsėjo 4 d., https://caselaw.findlaw.com/us-supreme-court/407/297.html
229. „United States v. White“, *FindLaw*, žiūrėta 2020 m. rugsėjo 4 d., https://caselaw.findlaw.com/us-5th-circuit/1278977.html.
230. „United States v. Williams“, *CaseLaw*, žiūrėta 2020 m. rugsėjo 5 d., https://caselaw.findlaw.com/dc-court-of-appeals/1191178.html.
231. „Viacom Intern. Inc. v. YouTube Inc.“, *FindLaw*, žiūrėta 2020 m. rugsėjo 4 d., https://caselaw.findlaw.com/us-2nd-circuit/1597925.html.

Specialioji literatūra

232. „Cloud Computing and cybercrime investigations: Territoriality vs. the power of disposal? Discussion paper“, *Council of Europe*, 5, žiūrėta 2020 m. rugsėjo 9 d., https://rm.coe.int/16802fa3df.

233. „Developments in the Law: The Law of Cyberspace“, *Harvard Law Review* 112, no. 7 (1999): 1579, doi:10.2307/1342414.
234. „Electronic Surveillance Recent Legislation“, *Harvard Law Review* 122, no. 4 (2009 2008): 1271–78.
235. „Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations“, *Cambridge University Press*, 211.
236. „The Ethics (or Not) of Massive Government Surveillance“, *Stanford University*, žiūrėta 2020 m. rugpjūčio 23 d., https://cs.stanford.edu/people/eroberts/cs181/projects/ethics-of-surveillance/ethics.html.
237. A. Michael Froomkin, „Regulating Mass Surveillance as Privacy Pollution: Learning from Environemntal Impact Statements“, *University of Illinois Law Review* 2015, no. 5 (2015): 1713–90.
238. Aaron Nance, „Taking the Fear Out of Electronic Surveillance in the New Age of Terror Note“, *UMKC Law Review* 70, Nr. 3 (2002 2001): 751–80.
239. Ahmed Ghappour, „Searching Places Unknown: Law Enforcement Jurisdiction on the Dark Web“, *Stanford Law Review* 69, no. 4 (2017): 1075–1136.
240. Alan Davidson, „Jurisdiction in Cyberspace“, *The Law of Electronic Commerce* (Cambridge University Press, 2009), doi:10.1017/CBO9780511818400.011.
241. Alan Z. Rozenshtein, „Surveillance Intermediaries“, *Stanford Law Review* 70, no. 1 (2018): 99–190.
242. Alessandro Mantelero, „The Guidelines of the Council of Europe Data Protection Committee on the Protection of Individuals with Regard to the Processing of Personal Data in the Big Data Context Reports: Council of Europe“, *European Data Protection Law Review (EDPL)* 3, no. 1 (2017): 88, 89.
243. Alex Kimata, „Section 702 Malfisance“, *Colorado Technology Law Journal* 16, no. 2 (2018 2017): 455–80.
244. Alexander Tsesis, „The Right to Erasure: Privacy, Data Brokers, and the Indefinite Retention of Data“, *Wake Forest Law Review* 49, no. 2 (2014): 433–84.
245. Alexandra Doncea, „Tackling Terrorism as a Threat to National Security“, *European Journal of Public Order and National Security* 2015, no. 3 (2015): [i]-47.
246. Alfonsas Vaišvila, *Teisės teorija: vadovėlis*, 4-asis leid ed. (Vilnius: Justitia, 2014).
247. Alfred Korzybski, *A Non-Aristotelian System and Its Necessity for Rigour in Mathematics and Physics: Abstract*, 1931, 745.
248. Ali E. Abbas, *Next-Generation Ethics: Engineering a Better Society* (Cambridge University Press, 2019), 451.
249. Amitai Etzioni, „End to End Encryption, the Wrong End“, *South Carolina Law Review* 67, no. 3 (2016 2015): 561–84.
250. Andreas Wolkenstein, Ralf J. Jox ir Orsolya Friedrich, „Brain–Computer Interfaces: Lessons to Be Learned from the Ethics of Algorithms“, *Cambridge Quarterly of Healthcare Ethics* 27, no. 4 (2018): 635–46, doi:10.1017/S0963180118000130.

251. Andrejus Novikovas, „Viešosios tvarkos apsauga savivaldybių teritorijoje: teisinis ir organizacinis aspektai“, *Jurisprudencija* 49, no. 41 (2003): 46–53.
252. Anthony D. Romero, „Mass E-Mail Surveillance: The Next Battle“, *Sur - International Journal on Human Rights* 21 (2015): 1–3.
253. Antonella Galetta ir Paul De Hert, „Complementing the Surveillance Law Principles of the ECtHR with Its Environmental Law Principles: An Integrated Technology Approach to a Human Rights Framework for Surveillance“, *Utrecht Law Review* 10, no. 1 (2014): 55–75.
254. Ariana R. Levinson, „Toward a Cohesive Interpretation of the Electronic Communications Privacy Act for the Electronic Monitoring of Employees“, *West Virginia Law Review* 114, no. 2 (2012 2011): 461–530.
255. Artūras Panomariovas ir Ramūnas Ramanauskas, „Slaptumas – tiesos baudžiamajame procese nustatymo priemonė“, *Jurisprudencija: mokslo darbai*, no. 75 (2005): 50–57.
256. Aurelijus Gutauskas, „Kriminalinė žvalgyba ir privatus žmogaus gyvenimas“, *Teisė* 113 (2019): 8–26, doi:10.15388/Teise.2019.113.1.
257. Axel Arnbak ir Sharon Goldberg, „Loopholes for Circumventing the Constitution: Unrestricted Bulk Surveillance on Americans by Collecting Network Traffic Abroad“, *Michigan Telecommunications and Technology Law Review* 21, no. 2 (2015 2014): 317–62.
258. Ben Cook, „The New FISA Court Amicus Should Be Able to Ignore Its Congressionally Imposed Duty“, *American University Law Review* 66, no. 2 (January 1, 2017)., https://digitalcommons.wcl.american.edu/aulr/vol66/iss2/5.
259. Bert-Jaap Koops ir Morag Goodwin, „Cyberspace, the Cloud, and Cross-Border Criminal Investigation. The Limits and Possibilities of International Law“, *SSRN Electronic Journal*, 2014, doi:10.2139/ssrn.2698263.
260. Bert-Jaap Koops ir Morag Goodwin, *Cyberspace, the cloud, and cross-border criminal investigation. The limits and possibilities of international law*, The Hague/Tilburg: WODC/TILT, 2014, žiūrėta 2020 m. rugsėjo 9 d., https://www.wodc.nl/binaries/2326-summary_tcm28-73008.pdf.
261. Bryce Newell ir Joseph Tennis, „Me, My Metadata, and the NSA: Privacy and Government Metadata Surveillance Programs“, 2014, doi:10.9776/14109.
262. C. Raj Kumar, „Human Rights Implications of National Security Laws in India: Combating Terrorism While Perserving Civil Liberties“, *Denver Journal of International Law and Policy* 33, no. 2 (2005 2004): 195–222.
263. Chaffin, *Building a VoIP Network with Nortel's Multimedia Communication Server 5100*, 431.
264. Charlie Savage, *Power Wars: The Relentless Rise of Presidential Authority and Secrecy*, Revised edition (New York: Back Bay Books, 2017).
265. Cheryl Niemeier, „Rolling in the Deep Not Dark Web“, *AALL Spectrum* 20, no. 6 (2016 2015): 23–25.
266. Christian Oggolder, „From Virtual to Social: Transforming Concepts and Images of the Internet“, *Information & Culture: A Journal of History* 50, no. 2 (2015): 181, doi:10.1353/lac.2015.0008.

267. Christiana Markou, „The Cyprus and Other EU Court Rulings on Data Retention: The Directive as a Privacy Bomb“, *Computer Law & Security Review* 28, no. 4 (August 1, 2012): 468–75, doi:10.1016/j.clsr.2012.05.003.
268. Christopher Cooke, „Note: Securing Liberty: A Response to Debates on Section 215 of the Patriot Act Symposium Comments and Notes: Phone Records and the NSA: Protecting America vs. Protecting Americans' Privacy“, *Georgetown Journal of Law & Public Policy* 12, no. 2 (2014): 889–96.
269. Christopher Kuner ir kt., „An Unstoppable Force and an Immoveable Object? EU Data Protection Law and National Security“, *International Data Privacy Law* 8, no. 1 (February 1, 2018): 1–3, doi:10.1093/idpl/ipy003.
270. Ciara Staunton ir kt., „Protection of Personal Information Act 2013 and Data Protection for Health Research in South Africa“, *International Data Privacy Law* 10, no. 2 (May 1, 2020): 160–79, doi:10.1093/idpl/ipz024.
271. Cyrus Farivar, *Habeas Data: Privacy vs. the Rise of Surveillance Tech* (Brooklyn: Melville House, 2018).
272. Clive Norris ir kt., *The Unaccountable State of Surveillance: Exercising Access Rights in Europe*, Issues in Privacy and Data Protection (Springer International Publishing, 2017), doi:10.1007/978-3-319-47573-8.
273. Colin J Bennett, *Regulating Privacy: Data Protection and Public Policy in Europe and the United States*, (Cornell University Press, 1992).
274. Constance L. Martin, „Exalted Technology: Should CALEA Be Expanded to Authorize Internet Wiretapping Notes and Comments“, *Rutgers Computer & Technology Law Journal* 32, no. 1 (2006 2005): 140–82.
275. Dan Jerker B. Svantesson, „Cross-Border Data Transfers after the CJEU's Safe Harbour Decision: A Tale of Gordian Knots“, *Alternative Law Journal* 41, no. 1 (2016): 39–42.
276. Dan Jerker B. Svantesson, „European Union Claims of Jurisdiction over the Internet – an Analysis of Three Recent Key Developments“, *Journal of Intellectual Property, Information Technology and E-Commerce Law* 9, no. 2 (2018), žiūrėta 2020 m. rugpjūčio 29 d., https://www.jipitec.eu/issues/jipitec-9-2-2018/4722.
277. Dan Jerker B. Svantesson, „Extraterritoriality in the Context of Data Privacy Regulation“, *Masaryk University Journal of Law and Technology* 7, no. 1 (2013): 90.
278. Dan Jerker B. Svantesson, *Solving the Internet Jurisdiction Puzzle*, *Solving the Internet Jurisdiction Puzzle* (Oxford University Press, 2017), žiūrėta 2020 m. rugpjūčio 29 d., https://oxford.universitypressscholarship.com/view/10.1093/oso/9780198795674.001.0001/oso-9780198795674.
279. Daniel Drewer ir Jan Ellermann, „Europol's Data Protection Framework as an Asset in the Fight against Cybercrime“, *ERA Forum* 13, no. 3 (November 1, 2012): 2, doi:10.1007/s12027-012-0268-6.
280. Daniel J. Solove, „I've Got Nothing to Hide and Other Misunderstandings of Privacy“, *San Diego Law Review* 44, no. 4 (2007): 745–72.

281. Daniel Severson, „American Surveillance of Non-U.S. Persons: Why New Privacy Protections Offer Only Cosmetic Change Notes“, *Harvard International Law Journal* 56, no. 2 (2015): 465–514.
282. Dara Hallinan ir kt., „Neurodata and Neuroprivacy: Data Protection Outdated?“, *Surveillance & Society* 12, no. 1 (November 20, 2013): 55–72, doi:10.24908/ss.v12i1.4500.
283. Darius Petrošius „Operatyvinės veiklos įstatymo raida žmogaus teisių apsaugos kontekste“, *Jurisprudencija* 63, Nr. 55 (2004): 133.
284. Darius Štitilis ir kt., *Interneto ir technologijų teisė: vadovėlis*, Teisinė literatūra (Vilnius: Registrų centras, 2016).
285. Darius Štitilis ir Marius Laurinaitis, „IP telefonija – iššūkis elektroninių ryšių kontrolės, siekiant ištirti nusikaltimus, teisiniam reguliavimui“, *Socialinių mokslų studijos*, no. 1 (2009): 205–221.
286. Darius Štitilis, „Elektroninių ryšių kontrolės nusikaltimų tyrimo tikslias teisiniai aspektai“, *Informacijos mokslai : mokslo darbai* 34 (2005): 103–110.
287. Darius Štitilis, Rolandas Krikščiūnas ir Rimantas Pertauskas, „Kai kurie konvencijos dėl elektroninių nusikaltimų proceso teisės skirsnio įgyvendinimo Lietuvoje aspektai“, *Jurisprudencija: mokslo darbai* 67 (2005): 20–28.
288. David Lyon, „Surveillance after September 11“, *Sociological Research Online*, November 7, 2017, doi:10.5153/sro.643.
289. David S. Kris, „The Rise and Fall of the FISA Wall Symposium – Spies, Secrets, and Security: The New Law of Intelligence: The Foreign Intelligence Surveillance Act“, *Stanford Law & Policy Review* 17, no. 2 (2006): 487–530.
290. Debbie V. S. Kasper, „The Evolution (or Devolution) of Privacy“, *Sociological Forum* 20, no. 1 (2005): 76, doi:10.1007/s11206-005-1898-z.
291. Deborah Pearlstein, „Before Privacy, Power: The Structural Constitution“, *Journal of National Security Law and Policy* 9, no. 2 (2018 2017): 159–210.
292. Deirdre K. Mulligan, „Reasonable Expectations in Electronic Communications: A Critical Perspective on the Electronic Communications Privacy Act The Future of Internet Surveillance Law: A Symposium to Discuss Internet Surveillance, Privacy & (and) the USA Patriot Act: Surveillance, Records & (and) Computers“, *George Washington Law Review* 72, no. 6 (2004 2003): 1557–98.
293. Demetrius Klitou, „Backscatter Body Scanners – A Strip Search by Other Means“, *Computer Law & Security Review* 24, no. 4 (January 1, 2008): 317, doi:10.1016/j.clsr.2008.05.005.
294. Dennis J. McFarland ir Jonathan R. Wolpaw, „Brain-Computer Interfaces for Communication and Control“, *Communications of the ACM* 54, no. 5 (2011): 63, doi:10.1145/1941487.1941506.
295. Devin M. Adams, „The 2016 Amendments to Criminal Rule 41: National Search Warrants to Seize Cyberspace, Particularly Speaking National Security in the Information Age: Are We Heading toward Big Brother: Symposium Issue 2017: Data Collection and Advancements in Surveillance Techniques“, *University of Richmond Law Review* 51, no. 3 (2017 2016): 727–72.

296. Dyane L. O'Leary, „License to Hack", *New York University Law Review Online* 94 (2019): 56–95.
297. Eduardo R. Mendoza, „Network Investigation Techniques: Government Hacking and the Need for Adjustment in the Third-Party Doctrine Comment", *St. Mary's Law Journal* 49, no. 1 (2018 2017): 237–68.
298. Edward Lucas, *Cyberphobia: Identity, Trust, Security and the Internet* (Bloomsbury Publishing, 2015).
299. Egidijus Jarašiūnas, „Jurisprudencinė konstitucija", *Jurisprudencija : mokslo darbai*, no. 12 (2006): 24–33.
300. Egidijus Vareikis, *Nacionalinis ir tarptautinis saugumas*, (Kaunas: Vytauto Didžiojo universiteto leidykla, 2005).
301. Elena Gil Gonzalez, Paul De Hert ir Vagelis Papakonstantinou, „The Proposed ePrivacy Regulation: The Commission's and the Parliament's Draft s at a Crossroads?", in D Hallinan, R Leenes, S Gutwirth and P De Hert (eds), *Data Protection and Privacy. Data Protection and Democracy.* Hart Publishing, 2020, 267-298.
302. Eleni Kosta, Fanny Coudert ir Jos Dumortier, „Data Protection in the Third Pillar: In the Aftermath of the ECJ Decision on PNR Data and the Data Retention Directive", *International Review of Law, Computers & Technology* 21, no. 3 (2007): 347–62.
303. Elizabeth Goitein, „Another Bite out of Katz: Foreign Intelligence Surveillance and the Incidental Overhear Doctrine Symposium: Katz @ 50: The Fourth Amendment in the Digital Age", *American Criminal Law Review* 55, no. 1 (2018): 105–26.
304. Els De Busser, „EU Data Protection in Transatlantic Cooperation in Criminal Matters Will the EU Be Serving Its Citizens an American Meal?", *Utrecht Law Review* 6 (January 25, 2010): 87, doi:10.18352/ulr.116.
305. Francesca Bignami, „European Versus American Liberty: A Comparative Privacy Analysis of Anti-Terrorism Data-Mining", 48 (GW Law Faculty Publications & Other Works, 2007): 91.
306. Francesca Bignami, „The US legal system on data protection in the field of law enforcement. Safeguards, rights and remedies for EU citizens", *European Parlament*, žiūrėta 2020 m. rugsėjo 10 d., https://www.europarl.europa.eu/thinktank/en/document.html?reference=IPOL_STU(2015)519215.
307. Frank Cali, „Europol's Data Protection Mechanisms: What Do They Know and Whom Are They Telling", *Touro International Law Review,* 10 (2000): 189–240.
308. Franziska Boehm, *Information Sharing and Data Protection in the Area of Freedom, Security and Justice: Towards Harmonised Data Protection Principles for Information Exchange at EU-Level* (Berlin Heidelberg: Springer-Verlag, 2012), 81, doi:10.1007/978-3-642-22392-1.
309. Frederik J. Zuiderveen Borgesius ir Wilfred Steenbruggen, „The Right to Communications Confidentiality in Europe: Protecting Privacy, Freedom

of Expression, and Trust", *Theoretical Inquiries in Law* 20, no. 1 (March 16, 2019): 291–322, doi:10.1515/til-2019-0010.
310. Gabrielle Kaufmann-Kohler ir Thomas Schultz, *Online Dispute Resolution: Challenges for Contemporary Justice* (The Hague : Zürich: Kluwer Law International, 2004).
311. Gary LaFree ir Laura Dugan, „Research on Terrorism and Countering Terrorism", *Crime and Justice: A Review of Research* 38 (2009): 413–78.
312. Gediminas Bučiūnas, „Slaptas sekimas – tinkamos pusiausvyros paieška tarp visuomenės teisės būti saugia ir asmens teisės į privatumą" (Vytauto Didžiojo universitetas. Prieiga per eLABa – nacionalinė Lietuvos akademinė elektroninė biblioteka, 2014), 71.
313. Gianclaudio Malgieri ir Paul Hert, „European Human Rights, Criminal Surveillance, and Intelligence Surveillance: Towards 'Good Enough' Oversight, Preferably but Not Necessarily by Judges", in *The Cambridge Handbook of Surveillance Law*, 2017, 509–32, doi:10.1017/9781316481127.023.
314. Gina Marie Stevens, *Privacy: Total Information Awareness Programs and Latest Developments* (New York: Novinka Books, 2003).
315. Gintaras Goda, „Procesinių prievartos priemonių Lietuvos Respublikos baudžiamojo proceso kodekso projekte samprata, klasifikacija ir turinys", Teisė. (2000): 17–27.
316. Gintaras Goda, *Vertybiniai prioritetai baudžiamajame procese: monografija*, (Vilnius: Registrų centras, 2014).
317. Giovanni Ziccardi, „The GDPR and the LIBE Study on the Use of Hacking Tools by Law Enforcement Agencies Essays", *Italian Law Journal* 4, no. 1 (2018): 220.
318. Giuseppe Vaciago ir David Silva Ramalho, „Online Searches and Online Surveillance: The Use of Trojans and Other Types of Malware as Means of Obtaining Evidence in Criminal Proceedings", *Digital Evidence and Electronic Signature Law Review*, žiūrėta 2020 m. rugpjūčio 22 d., https://journals.sas.ac.uk/deeslr/article/view/2299.
319. Glenn Greenwald, Ewen MacAskill ir Laura Poitras, „Edward Snowden: The Whistleblower behind the NSA
320. Gloria Gonzalez Fuster, „Un-Mapping Personal Data Transfers", *European Data Protection Law Review (EDPL)* 2, no. 2 (2016): 160–68.
321. Graham Greenleaf, „'Modernising' Data Protection Convention 108: A Safe Basis for a Global Privacy Treaty?", *Computer Law & Security Review* 29, no. 4 (August 1, 2013): 2, doi:10.1016/j.clsr.2013.05.015.
322. Graham Greenleaf, „An Endnote on Regulating Cyberspace: Architecture vs Law?", SSRN Scholarly Paper (Rochester, NY: Social Science Research Network, December 11, 1998), https://papers.ssrn.com/abstract=2188160.
323. H Akın Ünver, „Politics of Digital Surveillance, National Security and Privacy", n.d., 23.

324. Hamza S. Dawood, „Understanding Privacy, by Daniel J. Solove Book Note“, *Osgoode Hall Law Journal* 47, no. 4 (2009): 819–20.
325. Hans Born ir Marina Caparini, *Democratic Control of Intelligence Services: Containing Rogue Elephants* (Ashgate Publishing, Ltd., 2013), 119.
326. Helen Nissenbaum, „Privacy as Contextual Integrity Symposium – Technology, Values, and the Justice System“, *Washington Law Review* 79, no. 1 (2004): 119–58.
327. Hielke Hijmans ir Alfonso Scirocco, „Shortcomings in EU Data Protection in the Third and the Second Pillars. Can the Lisbon Treaty Be Expected to Help?“, *Common Market Law Review* 46 (October 1, 2009): 1485.
328. I. C. T. ICT School, *Computer Hacking: This Book Includes: Hacking Tools for Computers with Linux Mint, Linux for Beginners and Kali Linux Tools and Hacking with Kali Linux with Basic Security Testing* (Amazon Digital Services LLC – KDP Print US, 2019).
329. Ian Walden, *Telecommunications Law and Regulation* (OUP Oxford, 2012).
330. Yanan Wang ir kt., „Probe Computing Model Based on Small Molecular Switch“, *BMC Bioinformatics* 20, no. 8 (June 10, 2019): 285, doi:10.1186/s12859-019-2767-8.
331. Ida Lindren ir Gabriella Jansson, „Electronic services in the public sector: A conceptual framework“, *Government Information Quarterly*, 30(2) (2013):163–172.
332. Yi-Hsuan Chen, „EU Data Protection Law Reform: Challenges for Service Trade Liberalization and Possible Approaches for Harmonizing Privacy Standards into the Context of GATS, The“, *Spanish Yearbook of International Law* 19 (2015): 211–20.
333. Irmantas Jarukaitis, *Elektroninių ryšių teisė* (Vilnius: Eugrimas, 2005).
334. J. Adams ir M. Albakajai, „Cyberspace: A New Threat to the Sovereignty of the State“, *Management Studies* 4, no. 6 (September 29, 2016), http://dx.doi.org/10.17265/2328-2185/2016.06.003.
335. J. K. Petersen, *Handbook of Surveillance Technologies, Third Edition* (CRC Press, 2012).
336. Jackson Adams ir Mohamad Albakajai, „Cyberspace: A New Threat to the Sovereignty of the State“, *Management Studies* 4, no. 6 (September 29, 2016): 1, doi:10.17265/2328-2185/2016.06.003.
337. Jacob G. Oakley, „Cyber Collection“, in *Waging Cyber War: Technical Challenges and Operational Constraints*, ed. Jacob G. Oakley (Berkeley, CA: Apress, 2019), 57–70, doi:10.1007/978-1-4842-4950-5_5.
338. Jacob Sommer, „FISA Authority and Blanket Surveillance; A Gatekeeper without Opposition“, *Litigation* 40, no. 4 (2014 2013): 40–46.
339. Jacqueline R. Kanovitz and Michael I. Kanovitz, *Constitutional Law* (Routledge, 2010).
340. Jaffer, *op. cit.,* 422: 8. Gerald H. Robinson, „We're Listening – Electronic Eavesdropping, Fisa, and the Secret Court“, *Willamette Law Review* 36, no. 1 (2000): 51–82.

341. Jameel Jaffer, „Secret Evidence in the Investigative State: FISA, Administrative Subpoenas, and Privacy Symposium: Secret Evidence and the Courts in the Age of National Security: Panel Report“, *Cardozo Public Law, Policy, and Ethics Journal* 5, no. 1 (2007 2006): 7–26.
342. James Carr ir Patricia Bellia, *The Law of Electronic Surveillance, 2017-2 Ed.*, 1 dalis, (Clark Boardman Callaghan, 2017).
343. James Carr ir Patricia Bellia, *The Law of Electronic Surveillance, 2017-2 Ed.*, 2 dalis, (Clark Boardman Callaghan, 2017), 443.
344. Jeffrey Pomerantz, *Metadata*, The MIT Press Essential Knowledge Series (Cambridge, Massachusetts; London, England: The MIT Press, 2015).
345. Jemima Stratford ir Tim Johnston, „The Snowden ‘Revelations’: Is GCHQ Breaking the Law?“, *European Human Rights Law Review* 2014, no. 2 (2014): 129–41.
346. Jennifer Daskal, „Microsoft Ireland, the CLOUD Act, and International Lawmaking 2.0 Essay“, *Stanford Law Review Online* 71 (2019 2018): 9–16.
347. Jennifer Stisa Granick, *American Spies: Modern Surveillance, Why You Should Care, and What to Do About It* (Cambridge UK New York: Cambridge University Press, 2017), 5.
348. Jing Ran, „Striking the Balance between Privacy and Governance in the Age of Technology“, 11 (2016): 20.
349. Joakim Kävrestad, *Fundamentals of Digital Forensics* (Springer Nature, n.d.), 11.
350. Joanna Kulesza, „USA Cyber Surveillance and EU Personal Data Reform: PRISM’s Silver Lining?“, SSRN Scholarly Paper (Rochester, NY: Social Science Research Network, 2014), 4, https://papers.ssrn.com/abstract=2599274.
351. John B. Sheldon, „Geopolitics and Cyber Power: Why Geography Still Matters“, *American Foreign Policy Interests* 36, no. 5 (September 3, 2014): 268, doi:10.1080/10803920.2014.969174.
352. John R. Vacca, *Computer and Information Security Handbook* (Morgan Kaufmann, 2009).
353. Jonathan Mayer, „Government Hacking“, *Yale Law Journal* 127, no. 3 (2018 2017): 570–663.
354. Jonathan Mayer, Patrick Mutchler ir John C. Mitchell, „Evaluating the Privacy Properties of Telephone Metadata“, *Proceedings of the National Academy of Sciences* 113, no. 20 (May 17, 2016): 5536–41, doi:10.1073/pnas.1508081113.
355. Jonathan Matusitz, „Cyberterrorism: Postmodern State of Chaos“, *Information Security Journal: A Global Perspective* 17, no. 4 (January 1, 2008): 179–187, doi:10.1080/19393550802397033.
356. Jonathan Matusitz, „Intercultural Perspectives on Cyberspace: An Updated Examination“, *Journal of Human Behavior in the Social Environment* 24, no. 7 (October 3, 2014): 713–24, doi:10.1080/10911359.2013.849223.
357. Joseph Migga Kizza, *Ethical and Secure Computing: A Concise Module*, Springer, 2019.

358. Julius Zaleskis, *Europos Sąjungos bendrasis duomenų apsaugos reglamentas ir asmens duomenų apsaugos teisė: monografija*, Teisinė literatūra (Vilnius: Registrų centras, 2019).
359. Justina Dešriūtė, „Esminiai asmens duomenų apsaugos baudžiamajame procese reformos Europos Sąjungoje aspektai ir jų įtaka nacionaliniam teisiniam reguliavimui“, *Teisės problemos*, 1 (91), (2016): 25–51.
360. Kenneth R. Mayer, „Executive Orders and Presidential Power“, *The Journal of Politics* 61, no. 2 (1999): 445–66, doi:10.2307/2647511.
361. Larry Chaffin, *Building a VoIP Network with Nortel's Multimedia Communication Server 5100* (Elsevier, 2006), 431.
362. Laura K. Donohue, „FISA Reform“, *I/S: A Journal of Law and Policy for the Information Society* 10, no. 2 (2015 2014): 599–640.
363. Laura K. Donohue, „Section 702 and the Collection of International Telephone and Internet Content“, *Harvard Journal of Law & Public Policy* 38, no. 1 (2015): 117–266.
364. Laura K. Donohue, *The Future of Foreign Intelligence: Privacy and Surveillance in a Digital Age*, 1 edition (New York: Oxford University Press, 2016), 76.
365. Laura L. Clukey, „The Electronic Communications Privacy Act of 1986: The Impact on Software Communication Technologies Comment“, *Software Law Journal* 2, no. 2 (1988 1987): 243–64.
366. Liane Colonna, „Prism and the European Union's Data Protection Directive“, *John Marshall Journal of Information Technology and Privacy Law* 30, no. 2 (2014 2013): 227–52.
367. Linas Belevičius, „Techninių priemonių panaudojimo tiriant nusikaltimus teisinis reglamentavimas“, *Jurisprudencija : mokslo darbai* 29 (2002): 72–85.
368. Lois A. Chiarella ir Michael A. Newton, „So Judge, How Do I Get That FISA Warrant: The Policy and Procedure for Conducting Electronic Surveillance“, *Army Lawyer* 1997, no. 10 (1997): 25–73.
369. Marija Boban, „Digital Single Market and EU Data Protection Reform with Regard to the Processing of Personal Data as the Challenge of the Modern World The Legal Challenges of Modern World“, *Economic and Social Development, 16th International Scientific Conference on Economic and Social Development: The Legal Challenges of Modern World* 16 (2016): 191–201.
370. Marina Gušauskienė, „Ikiteisminio tyrimo teisėjas – žmogaus teisių garantas“, *Jurisprudencija* 54, nr. 49 (2004): 129, 130.
371. Marina Skrinjar Vidovic, „EU Data Protection Reform: Challenges for Cloud Computing Notes“, *Croatian Yearbook of European Law and Policy* 12 (2016): 171–206.
372. Michael D. Birnhack, „The EU Data Protection Directive: An Engine of a Global Regime“, *Computer Law & Security Review* 24, no. 6 (January 1, 2008): 508–20, doi:10.1016/j.clsr.2008.09.001.
373. Michael Friedewald, Rachel Finn, ir David Wright, *Seven Types of Privacy*, 2013, 3–32, doi:10.1007/978-94-.

374. Michael P. O'Connor ir Celia M. Rumann, „Into the Fire: How to Avoid Getting Burned by the Same Mistakes Made Fighting Terrorism in Northern Ireland", *Cardozo Law Review* 24, no. 4 (2003 2002): 1657–1752.
375. Michael Paul Falzone, „Search and Seizure-Limitations on Closed Container Searches in Open Fields-United States v. Ramapuram Notes", *Wake Forest Law Review* 17, no. 3 (1981): 478–96.
376. Michael W. Price, „Rethinking Privacy: Fourth Amendment Papers and the Third-Party Doctrine", *Journal of National Security Law and Policy* 8, no. 2 (2016 2015): 247–300.
377. Milan Babic, Jan Fichtner ir Eelke M. Heemskerk, „States versus Corporations: Rethinking the Power of Business in International Politics", *The International Spectator* 52, no. 4 (2017): 20–43, doi:10.1080/03932729.2017.1389151.
378. Mindaugas Civilka ir Lina Šlapimaitė, „Asmens duomenų samprata elektroninėje erdvėje", *Teisė*, 96 (2015): 126-148.
379. Mindaugas Kiškis ir kt., *Teisės informatika ir informatikos teisė: vadovėlis*, (Vilnius: Mykolo Romerio universitetas, 2006), 11.
380. Monika Žalnieriūtė, „An International Constitutional Moment for Data Privacy in the Times of Mass-Surveillance", *International Journal of Law and Information Technology* 23, no. 2 (2015): 99–133.
381. Nadine Strossen, „Beyond the Fourth Amendment: Additional Constitutional Guarantees That Mass Surveillance Violates", *Drake Law Review* 63, no. 4 (2015): 1143–70.
382. Nash Haynes, *Cyber Crime.* (London: ED Tech Press, 2018), 92.
383. Nick Harper, „FISA's Fuzzy Line between Domestic and International Terrorism Comment", *University of Chicago Law Review* 81, no. 3 (2014): 1123–64.
384. Orin Kerr, „The Case for the Third-Party Doctrine", *Michigan Law Review* 107, no. 4 (2009): 563.
385. Orin S. Kerr and Sean D. Murphy, „Government Hacking to Light the Dark Web: What Risks to International Relations and International Law Essay", *Stanford Law Review Online* 70 (2018 2017): 58–69.
386. Ovidiu Ungureanu ir Cornelia Munteanu, „The Right to Protection of Personal Data, an Autonomous Right II. Doctrine – Studies, Articles, Comments", *Romanian Review of Private Law* 2014, no. 1 (2014): 166–79.
387. Patrick Walsh, „Stepping on (or over) the Constitution's Line: Evaluating FISA Section 702 in a World of Changing Resonableness under the Fourth Amendment", *New York University Journal of Legislation and Public Policy* 18, no. 4 (2015): 741–94.
388. Paul M. Schwartz and Daniel J. Solove, „Reconciling Personal Information in the United States and European Union Essay", *California Law Review* 102, no. 4 (2014): 877–916.
389. Paul M. Schwartz ir Daniel J. Solove, „Reconciling Personal Information in the United States and European Union", 102 California. Law. Review. 877 (2014), 1.

390. Paul M. Schwartz, „Property, Privacy, and Personal Data“, *Harvard Law Review* 117, no. 7 (2004 2003): 2056–2128.
391. Paulius Pakutinskas, „Elektroninių komunikacijų teisinio reguliavimo modeliai“, (daktaro disertacija, Mykolo Romerio universitetas, 2009).
392. Peter Blume, „It Is Time for Tomorrow: EU Data Protection Reform and the Internet“, *Journal of Internet Law* 18, no. 8 (2015): 4.
393. Peter Margulies, „The NSA in Global Perspective: Surveillance, Human Rights, and International Counterterrorism Symposium: Citizenship, Immigration, and National Security after 9/11“, *Fordham Law Review* 82, no. 5 (2014 2013): 2137–68.
394. Petras Ancelis, *Baudžiamojo proceso ikiteisminis etapas* (Vilnius: Mykolo Romerio universitetas, 2007), 16.
395. Petras Tarasevičius, „Techninių priemonių naudojimo kriminalinėje žvalgyboje teisėtumo problemos“, *Teisė*, 2017, 84–99, doi:10.15388/Teise.2017.105.11114.
396. Philip Schütz ir Michael Friedewald, „Technologies for Human Enhancement and their impact on privacy“, *Privacy, data protection and ethical issues in new and emerging technologies: Five case studies*, eds. Rachel Finn and David Wright..
397. Phillip B. K. Potter, „Terrorism in China: Growing Threats with Global Implications“, *Strategic Studies Quarterly* 7, no. 4 (2013): 70–92.
398. Privacy and Civil Liberties Oversight Board, *Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act* (CreateSpace Independent Publishing Platform, 2015).
399. Quirine Eijkman ir Daan Weggemans, „Open Source Intelligence and Privacy Dilemmas: Is It Time to Reassess State Accountability Special Section: Security versus Privacy: What Is Europe Heading For“, *Security and Human Rights* 23, no. 4 (2012): 285–96.
400. Rachel L. Finn, David Wright ir Michael Friedewald, „Seven Types of Privacy“, in *European Data Protection: Coming of Age*, ed. Serge Gutwirth et al. (Dordrecht: Springer Netherlands, 2013), 3–32, doi:10.1007/978-94-007-5170-5_1.
401. Raimondas Jurka, „Draudimas versti duoti parodymus prieš save kaip asmens konstitucinių teisių baudžiamajame procese garantas“, *Jurisprudencija*, 1 2006 (79); 31–39.
402. Raimondas Jurka, „Įrodymų perdavimo Europos Sąjungos valstybių narių baudžiamojoje justicijoje iššūkiai ir atradimai“, *Jurisprudencija,* (2019, 26(2)), 322.
403. Renata Marcinauskaitė, „Nusikalstamos veikos elektroninėje erdvėje“, (daktaro disertacija, Mykolo Romerio universitetas).
404. Richard M Thompson Ii, „The Fourth Amendment Third-Party Doctrine“, (Congressional Research Service, 2014), 17.
405. Richard M. Thompson II ir Jared P. Cole, „Stored Communications Act: Reform of the Electronic Communications Privacy Act (ECPA)“, (Congressional Research Service, 2015), 12.

406. Rima Ažubalytė, „Baudžiamojo proceso principai: teisės spragų šalinimas“, *Lietuvos Respublikos baudžiamojo proceso kodeksui – 10 metų : recenzuotų mokslinių straipsnių, skirtų Lietuvos ir užsienio šalių baudžiamojo proceso, baudžiamosios teisės ir kriminalistikos aktualijoms ir problematikai, rinkinys*, 2012, 13–34
407. Rima Ažubalytė, „Privataus asmens gyvenimo ribojimas slaptomis priemonėmis: (ne)kokybiško įstatymo problema“, *Jurisprudencija* 26, no. 2 (2019): 260–291, doi:10.13165/JUR-19-26-2-02.
408. Rimantas Alfonsas Petrauskas ir Darius Štitilis, „Monitoring Electronic Communications: Privacy Issues“, *Monitoring, Supervision and Information Technology : Proceedings of the First International Seminar of the Legal Framework for the Information Society (LEFIS) on Monitoring, Supervision and Information Technology, 15 June 2006, Rotterdam*, 2006, 5–20.
409. Rob Dickinson, „Responsibility to Protect: Arab Spring Perspectives“, *Buffalo Human Rights Law Review* 20 (2014 2013): 91–124.
410. Robert A. Fiatal, „The Electronic Communications Privacy Act: Addressing Today's Technology (Part 1) Legal Digest“, *FBI Law Enforcement Bulletin* 57, no. 2 (1988): 25–30.
411. Rodolfo G. Biazon, „Terrorism and National Security. Special Issue on International Crimes: Section II: Roundtable Discussion“, *World Bulletin: Bulletin of the International Studies of the Philippines* 14, no. 3–4 (1998): 57–61.
412. Russell A. Miller, *Privacy and Power: A Transatlantic Dialogue in the Shadow of the NSA-Affair* (Cambridge University Press, 2017), 369.
413. S. A. Baset ir H. G. Schulzrinne, „An Analysis of the Skype Peer-to-Peer Internet Telephony Protocol“, in *Proceedings IEEE INFOCOM 2006. 25TH IEEE International Conference on Computer Communications* (Proceedings IEEE INFOCOM 2006. 25TH IEEE International Conference on Computer Communications, Barcelona, Spain: IEEE, 2006), 1–11, doi:10.1109/INFOCOM.2006.312.
414. Samuel D. Warren ir Louis D. Brandeis, „The Right to Privacy“, *Harvard Law Review* 4, no. 5 (1890): 193–220, doi:10.2307/1321160.
415. Sandeep Mittal ir Priyanka Sharma, „Enough Law of Horses and Elephants Debatedd Letts Discuss the Cyber Law Seriously“, *SSRN Electronic Journal*, 2017, doi:10.2139/ssrn.2977374.
416. Sara E. Dirvianskis, „American Council on Education v. FCC: Proper Outcome, Lack of Clarity in the Interpretation of CALEA Developments in Science and Technology Law – Part I: Law and Technology“, *Jurimetrics* 47, no. 4 (2007 2006): 463–78.
417. Sarah Spiekermann, *Ethical IT Innovation: A Value-Based System Design Approach* (CRC Press, 2015).
418. Saskia Sassen (1997) Electronic space and power, Journal of Urban Technology, 4:1, 1-17, DOI: 10.1080/10630739708724545.

419. Scott Shackelford, „Human Rights and Cybersecurity Due Diligence: A Comparative Study“, *University of Michigan Journal of Law Reform* 50, no. 4 (2017): 859–85.
420. Serge Gutwirth, Ronald Leenes ir Paul de Hert, eds., *Reforming European Data Protection Law*, Issues in Privacy and Data Protection (Springer Netherlands, 2015), 16, doi:10.1007/978-94-017-9385-8.
421. Serge Gutwirth, Ronald Leenes, Paul de Hert ir kt, eds., *European Data Protection: Coming of Age* (Dordrecht: Springer Netherlands, 2013), doi:10.1007/978-94-007-5170-5,
422. Serge Gutwirth, Ronald Leenes, Paul de Hert, ir kt, *European Data Protection: Coming of Age* (Springer
423. Serge Gutwirth, Ronald Leenes, Paul de Hert, ir kt., eds., *European Data Protection: Coming of Age* (Springer Netherlands, 2013), 16, doi:10.1007/978-94-007-5170-5.
424. Shawn Marie Boyne, „Data Protection in the United States: U.S. National Report“, SSRN Scholarly Paper (Rochester, NY: Social Science Research Network, 2017), doi:10.2139/ssrn.3089004.
425. Sherri J. Conrad, „Executive Order 12,333: Unleashing the CIA Violates the Leash Law Notes“, *Cornell Law Review* 70, no. 5 (1985 1984): 968–90.
426. Silvia Venier ir Emilio Mordini, „Second-generation biometrics“, in *Privacy, data protection and ethical issues in new and emerging technologies: Five case studies*, eds. Rachel Finn and David Wright, 25 November 2011.
427. Sophie Stalla-Bourdillon, Evangelia Papadaki ir Tim Chown, „Metadata, Traffic Data, Communications Data, Service Use Information... What Is the Difference? Does the Difference Matter? An Interdisciplinary View from the UK“, SSRN Scholarly Paper (Rochester, NY: Social Science Research Network, 2015), 1, https://papers.ssrn.com/abstract=2625181.
428. Stanislaw Tosza, „All Evidence Is Equal, but Electronic Evidence Is More Equal than Any Other: The Relationship between the European Investigation Order and the European Production Order“, *New Journal of European Criminal Law* 11, no. 2 (June 1, 2020): 161–83, doi:10.1177/2032284420919802.
429. Stephen E. Henderson, „Learning from All Fifty States: How to Apply the Fourth Amendment and Its State Analogs to Protect Third Party Information from Unreasonable Search“, *Catholic University Law Review* 55, no. 2 (2006 2005): 373–438.
430. Stephen I. Vladeck, "The FISA Court and Article III Cybersurveillance in the Post-Snowden Age“, *Washington and Lee Law Review* 72, no. 3 (2015): 1161–80.
431. Stephen I. Vladeck, „The FISA Court and Article III Cybersurveillance in the Post-Snowden Age“, *Washington and Lee Law Review* 72, no. 3 (2015): 1161–80.
432. Stephen Rushin, „The Judicial Response to Mass Police Surveillance“, *University of Illinois Journal of Law, Technology & Policy* 2011, no. 2 (2011): 281–328.

433. Steven A. Stottlemyre, „HUMINT, OSINT, or Something New? Defining Crowdsourced Intelligence“, *International Journal of Intelligence and CounterIntelligence* 28, no. 3 (2015): 578–89, doi:10.1080/08850607.2015.992760.
434. Steven M. Bellovin ir kt., „It's Too Complicated: How the Internet Upends Katz, Smith, and Electronic Surveillance Law“, *Harvard Journal of Law & Technology (Harvard JOLT)* 30, no. 1 (2017 2016): 1–102.
435. Steven R. Morrison, „Breaking IPhones under CALEA and the All Writs Act: Why the Government Was (Mostly) Right“, *Cardozo Law Review* 38, no. 6 (2017 2016): 2039–82.
436. Steverson, Koops, BJ & Goodwin, MEA. 2014. *Cyberspace, the cloud, and cross-border criminal investigation. The limits and possibilities of international law*, The Hague/Tilburg: WODC/TILT, available at https://ssrn.com/abstract=2698263.
437. Susan Freiwald, „A First Principles Approach to Communications' Privacy“, SSRN Scholarly Paper (Rochester, NY: Social Science Research Network, 2008), https://papers.ssrn.com/abstract=1132421.
438. Svarlien, Oscar, „Introduction to the Law of Nations“, (New York: McGraw-Hill., 1955).
439. Tarcisio Teixeira, Paulo Henrique Sabo ir Isabela Cristina Sabo, „Whatsapp and End-to-End Encryption: Legal Trend and the Conflict Privacy vs. Public Interest“, *Revista Da Faculdade de Direito Da Universidade Federal de Minas Gerais* 71 (2017): 607–40.
440. *The Army Lawyer* (Judge Advocate General's School, 1997), 25.
441. United Nations Office on Drugs and Crime, *Current Practices in Electronic Surveillance in the Investigation of Serious and Organized Crime* (New York: United Nations, 2009).
442. Vaidotas Urbelis, „Lietuvos žvalgybos sistema“, *Lietuvos metinė strateginė apžvalga 2008, 2009*, 215–245.
443. Viet D. Dinh ir Wendy J. Keefer, „FISA and the Patriot Act: A Look Back and a Look Forward Note“, *Annual Review of Criminal Procedure* 35 (2006): iii–xxxiv.
444. Vilius Stakėnas. *Internetas*. Visuotinė lietuvių enciklopedija, T. VIII (Imhof-Junusas). – Vilnius: Mokslo ir enciklopedijų leidybos institutas, 2005. 177.
445. Viviane Reding „The European data protection framework for the twenty-first century“, *International Data Privacy Law*, Volume 2, Issue 3, 2012, 119–129.
446. Wayne R. LaFave, *Search and Seizure, A Treatise on the Fourth Amendment, Fourth Edition, 6 Volume Set*, 5th edition (Thomson West, 2004), 747.
447. Walter F. Pratt, *Privacy in Britain* (Bucknell University Press, 1979), 59.
448. Whitfield Diffie ir Martin E. Hellman, „New Directions in Cryptography“, *IEEE Transactions on Information Theory* 22, no. 6 (1976): 644–54, žiūrėta 2020 m. rugsėjo 1 d., https://ee.stanford.edu/~hellman/publications/24.pdf.
449. William C. Banks ir M. E. Bowman, „Executive Authority for National Security Surveillance“, *American University Law Review* 50, no. 1 (2001 2001): 1–130.

450. William C. Banks, „Next Generation Foreign Intelligence Surveillance Law: Renewing 702 National Security in the Information Age: Are We Heading toward Big Brother: Symposium Issue 2017: Data Collection and Advancements in Surveillance Techniques“, *University of Richmond Law Review* 51, no. 3 (2017-2016): 675.
451. William C. Banks, „The Death of FISA Symposium – 9/11 Five Years On: A Look at the Global Response to Terrorism“, *Minnesota Law Review* 91, no. 5 (2007 2006): 1209–1301.
452. Xavier Tracol, „Legislative Genesis and Judicial Death of a Directive: The European Court of Justice Invalidated the Data Retention Directive (2006/24/EC) Thereby Creating a Sustained Period of Legal Uncertainty about the Validity of National Laws Which Enacted It“, *Computer Law & Security Review* 30, no. 6 (December 1, 2014): 748, doi:10.1016/j.clsr.2014.09.008.
453. Zach Lerner, „A Warrant to Hack: An Analysis of the Proposed Amendments to Rule 41 of the Federal Ruled of Criminal Procedure“, *Yale Journal of Law and Technology* 18 (2016): 26–69.

Mokslinės studijos

454. „Criminal justice access to data in the cloud: challenges“, *Council of Europe*, 4, žiūrėta 2020 m. rugpjūčio 22 d., https://rm.coe.int/1680304b59.
455. „Current Practices in Electronic Surveillance in the Investigation of Serious and Organized Crime“, *United Nations*, 2009, 16, žiūrėta 2020 m. rugpjūčio 17 d., https://www.unodc.org/documents/organized-crime/Law-Enforcement/Electronic_surveillance.pdf.
456. „Guide on Article 8 of the European Convention on Human Rights“, *European Court of Human Rights*, žiūrėta 2020 m. rugpjūčio 23 d., https://www.echr.coe.int/Documents/Guide_Art_8_ENG.pdf.
457. „Regulating Electronic Communications: A Level Playing Field for Telecoms and OTTs?“, *European Parlament*, žiūrėta 2020 m. rugpjūčio 17 d., https://www.europarl.europa.eu/thinktank/en/document.html?reference=EPRS_BRI%282016%29586641.
458. „Study on pre-commercial procurement in the field of Security Within the Framework Contract of Security Studies – ENTR/09/050, *ECORYS*, 9, žiūrėta 2020 m. rugpjūčio 23 d., https://ec.europa.eu/home-affairs/sites/homeaffairs/files/e-library/documents/policies/security/pdf/pcp_sec_finalreport_en.pdf.
459. „Surveillance by Intelligence Services: Fundamental Rights Safeguards and Remedies in the EU – Volume II: Field Perspectives and Legal Update“, *European Union Agency for Fundamental Rights*, 2017, žiūrėta 2020 m. rugpjūčio 23 d., https://fra.europa.eu/sites/default/files/fra_uploads/fra-2017-surveillance-intelligence-services-vol-2_en.pdf.
460. „The Global Surveillance Industry“, *Privacy International,* 16, žiūrėta 2020 m. rugpjūčio 23 d., https://www.privacyinternational.org/sites/default/files/2017-12/global_surveillance_0.pdf.

461. „The Impact of the Use of Body Scanners in the Field of Aviation Security on Human Rights, Privacy, Personal Dignity, Health and Data Protection“, *European Commission*, 2016, žiūrėta 2020 m. rugsėjo 1 d., https://ec.europa.eu/transport/modes/air/consultations/2009_02_19_body_scanners_en.
462. Abelson, H. ir kt. „Keys Under Doormats: Mandating insecurity by requiring government access to all data and communications“, *Massachusetts Institute of Technology Computer Science and Artificial Intelligence Laboratory Technical Report*, 2015, žiūrėta 2020 m. rugpjūčio 22 d., https://dspace.mit.edu/bitstream/handle/1721.1/97690/MIT-CSAIL-TR-2015-026.pdf
463. Franziska Boehm ir Mark D. Cole, „Data Retention after the Judgement of the Court of Justice of the European Union“, 13, žiūrėta 2020 m. rugpjūčio 17 d., https://www.zar.kit.edu/DATA/veroeffentlichungen/237_237_Boehm_Cole-Data_Retention_Study-June_2014_1a1c2f6_9906a8c.pdf
464. Georgia Miller ir Matthew Kearnes, „Nanotechnology, Ubiquitous Computing and The Internet of Things: Challenges to Rights to Privacy and Data Protection Draft Report to the Council of Europe“, 2013, žiūrėta 2020 m. rugpjūčio 14 d., https://rm.coe.int/168067f7f5.
465. Joseph A. Cannataci ir Mireille M. Caruana, „Coe Report Data Privacy in the Police Sector“, žiūrėta 2020 m. rugsėjo 7 d., https://www.statewatch.org/media/documents/news/2013/oct/coe-report-data-privacy-in-the-police-sector.pdf.
466. Mirja Gutheil ir Quentin Liger, „Legal Frameworks for Hacking by Law Enforcement: Identification, Evaluation and Comparison of Practices“, *European Parlament,* 2017, 18, žiūrėta 2020 m. rugpjūčio 22 d., https://www.europarl.europa.eu/RegData/etudes/STUD/2017/583137/IPOL_STU(2017)583137_EN.pdf.

Kiti šaltiniai

467. „NSA Collecting Phone Records of Millions of Verizon Customers Daily“, *The Guardian*, žiūrėta 2020 m. rugpjūčio 30 d., https://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order.
468. „Reagan-Era Order on Surveillance Violates Rights, Says Departing Aide“, *The New York Times*, žiūrėta 2020 m. rugsėjo 1 d., https://www.nytimes.com/2014/08/14/us/politics/reagan-era-order-on-surveillance-violates-rights-says-departing-aide.html.
469. „Supporting fundamental rights, PrIvacy and Ethics in surveillaNce Technologies“, *Cordis*, žiūrėta 2020 m. rugpjūčio 30 d., https://cordis.europa.eu/project/id/261698.
470. „The Price Of Covid-19 Freedom May Be Eternal Spying“, Bloomberg, žiūrėta 2020 m. rugpjūčio 30 d., https://www.bloombergquint.com/view/coronavirus-contact-tracing-apps-mean-spying-end-to-data-privacy.
471. „The World's Most Valuable Resource Is No Longer Oil, but Data“, *The Economist*, žiūrėta 2020 m. rugpjūčio 30 d., https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data.

472. „The World's Most Valuable Resource Is No Longer Oil, but Data", *The Economist*, žiūrėta 2020 m. rugpjūčio 30 d., https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data.
473. Barton Gellman ir Ashkan Soltani, „NSA Surveillance Program Reaches 'into the Past' to Retrieve, Replay Phone Calls", *Washington Post*, 2014, žiūrėta 2020 m. rugsėjo 11 d., https://www.washingtonpost.com/world/national-security/nsa-surveillance-program-reaches-into-the-past-to-retrieve-replay-phone-calls/2014/03/18/226d2646-ade9-11e3-a49e-76adc9210f19_story.html.
474. Darius Mikutavičius, „„Microsoft" vertė pirmą kartą pasiekė trilijono dolerių ribą", *lrt.lt*, žiūrėta 2020 m. rugpjūčio 30 d., https://www.lrt.lt/naujienos/mokslas-ir-it/11/1052527/microsoft-verte-pirma-karta-pasieke-trilijono-doleriu-riba.
475. H Akın Ünver, „Politics of Digital Surveillance, National Security and Privacy", 23, žiūrėta 2020 m. rugpjūčio 30 d., https://edam.org.tr/wp-content/uploads/2018/04/Chrest_Surveillance2.pdf.
476. Mark Jaycox, „A Primer on Executive Order 12333: The Mass Surveillance Starlet", *Electronic Frontier Foundation*, June 2, 2014, žiūrėta 2020 m. rugsėjo 1 d., https://www.eff.org/deeplinks/2014/06/primer-executive-order-12333-mass-surveillance-starlet.
477. „The Global Surveillance Industry", Privacy International, žiūrėta 2020 m. rugpjūčio 30 d., https://www.privacyinternational.org/sites/default/files/2017-12/global_surveillance_0.pdf.
478. Catherine Stupp, „EU agency asks Commission to 'avoid fragmentation' in new cyber security plans", *Euractive*, žiūrėta 2020 m. rugsėjo 1 d., http://www.euractiv.com/section/cybersecurity/news/eu-agency-asks-commission-to-avoid-fragmentation-in-new-cybersecurity-plans/
479. „European Privacy Framework", *Privacy Europe*, žiūrėta 2020 m. rugsėjo 1 d., https://www.privacy-europe.com/european-privacy-framework.html.
480. „Roger Clarke's 'Privacy Introduction and Definitions'", *Roger Clarke*, žiūrėta 2020 m. rugsėjo 1 d., http://www.rogerclarke.com/DV/Intro.html#Priv.
481. „9/11 Saw Much of Our Privacy Swept aside. Coronavirus Could End It Altogether", *CNN*, žiūrėta 2020 m. rugpjūčio 30 d., https://edition.cnn.com/2020/05/16/tech/surveillance-privacy-coronavirus-npw-intl/index.html.
482. „Body Scanners", *American Civil Liberties Union*, žiūrėta 2020 m. rugsėjo 1 d., https://www.aclu.org/other/body-scanners.
483. „Impact Assessment on the use of security scanners at UK airports", *Department for Transport*, žiūrėta 2020 m. rugsėjo 1 d., http://webarchive.nationalarchives.gov.uk/+/http://www.dft.gov.uk/consultations/open/2010-23/ .
484. Cade Metz, „With $1 Billion From Microsoft, an A.I. Lab Wants to Mimic the Brain – The New York Times", žiūrėta 2020 m. rugsėjo 1 d., https://www.nytimes.com/2019/07/22/technology/open-ai-microsoft.html.
485. Alex Knapp, „Elon Musk Sees His Neuralink Merging Your Brain With A.I.", žiūrėta 2020 m. rugsėjo 1 d., https://www.forbes.com/sites/

alexknapp/2019/07/17/elon-musk-sees-his-neuralink-merging-your-brain-with-ai/#4dcca3b14b07.
486. Antonio Regalado,„EXCLUSIVE: Chinese Scientists Are Creating CRISPR Babies“, *MIT Technology Review*, žiūrėta 2020 m. rugsėjo 1 d., https://www.technologyreview.com/2018/11/25/138962/exclusive-chinese-scientists-are-creating-crispr-babies/.
487. „BBC – Ethics – Abortion: When Is the Foetus ‘Alive’?“, žiūrėta 2020 m. rugsėjo 1 d., http://www.bbc.co.uk/ethics/abortion/child/alive_1.shtml.
488. Antonio Regalado, „China’s CRISPR Babies: Read Exclusive Excerpts from the Unseen Original Research“, *MIT Technology Review*, accessed August 10, 2020, https://www.technologyreview.com/2019/12/03/131752/chinas-crispr-babies-read-exclusive-excerpts-he-jiankui-paper/.
489. Preetika Rana, „How a Chinese Scientist Broke the Rules to Create the First Gene-Edited Babies“, *Wall Street Journal*, 2019, https://www.wsj.com/articles/how-a-chinese-scientist-broke-the-rules-to-create-the-first-gene-edited-babies-11557506697.
490. Donna Harrison, „Mokslo įrodymai neigia abortų šalininkų argumentus apie gyvybės pradžią“, *Laisvos Visuomenės Institutas*, žiūrėta 2020 m. rugsėjo 1 d., https://laisvavisuomene.lt/mokslo-irodymai-neigia-abortu-salininku-argumentus-apie-gyvybes-pradzia/.
491. Projekto „Privacy and emerging fields of science and technology: Towards a common framework for privacy and ethical assessment“ rezultatas. Prieiga internete: https://www.prescient-project.eu/prescient/inhalte/download/PRESCIENT_D2.pdf .
492. „New Data Shows That Mobile Internet Is Used More but Phone Call Remains Most Popular Communication“, *European Commission*, (2016), žiūrėta 2020 m. rugsėjo 1 d., https://ec.europa.eu/digital-single-market/en/news/new-data-shows-mobile-internet-used-more-phone-call-remains-most-popular-communication.
493. Evan Andrews, „Who Invented the Internet?“, *HISTORY*, žiūrėta 2020 m. rugsėjo 1 d., https://www.history.com/news/who-invented-the-internet.
494. Christoph Engelmann ir Josina Johannsen, „ECJ Clarifies Scope of Telecoms Regulation for OTT Services“, *Technology’s Legal Edge*, July 23, 2019, https://www.technologyslegaledge.com/2019/07/ecj-clarifies-scope-of-telecoms-regulation-for-ott-services/.
495. Franklink D. Kramer, „Cyberpower and National Security: Policy Recommendations for a Strategic Framework“, National defence University Press, žiūrėta 2020 m. rugsėjo 4 d., https://ndupress.ndu.edu/Portals/68/Documents/Books/CTBSP-Exports/Cyberpower/Cyberpower-I-Chap-01.pdf?ver=2017-06-16-115055-617 .
496. Marco Mayer ir Luigi Martino, „International Politics in the Digital Age“, 8, žiūrėta 2020 m. rugsėjo 4 d., https://www.academia.edu/14336129/International_Politics_in_the_Digital_Age.

497. „Content Communication, Relational Communication“, *Hanging the Mirror*, žiūrėta 2020 m. rugsėjo 1 d., https://hangingthemirror.com/2018/02/13/content-communication-relational-communication-1-of-2/.
498. Danah Boyd, „Privacy and Publicity in the Context of Big Data“, žiūrėta 2020 m. rugsėjo 1 d., https://www.danah.org/papers/talks/2010/WWW2010.html.
499. „Doomed to Repeat History? Lessons from the Crypto Wars of the 1990s“, *New America*, žiūrėta 2020 m. rugsėjo 1 d., http://newamerica.org/cybersecurity-initiative/policy-papers/doomed-to-repeat-history-lessons-from-the-crypto-wars-of-the-1990s/.
500. „On Lawful Criminal Investigation That Respects 21st Century Data Protection – Europol and ENISA Joint Statement“, *Europol*, žiūrėta 2020 m. rugpjūčio 22 d., https://www.europol.europa.eu/publications-documents/lawful-criminal-investigation-respects-21st-century-data-protection-europol-and-enisa-joint-statement-0.
501. Harold Abelson ir kt., „Keys Under Doormats: Mandating Insecurity by Requiring Government Access to All Data and Communications“, 2015, žiūrėta 2020 m. rugsėjo 1 d., https://dspace.mit.edu/handle/1721.1/97690.
502. „The Government Wants Tech Companies to Give Them a Backdoor to Your Electronic Life“, *The Guardian*, žiūrėta 2020 m. rugsėjo 1 d., https://www.theguardian.com/commentisfree/2014/oct/17/government-internet-backdoor-surveillance-fbi.
503. „Surveillance Revelations“, *The Guardian*, 2013, žiūrėta 2020 m. rugsėjo 1 d., https://www.theguardian.com/world/2013/jun/09/edward-snowden-nsa-whistleblower-surveillance.
504. „Not Everything Is About You – Including Your Metadata“, *Digby von Muenster*, 2017, žiūrėta 2020 m. rugpjūčio 23 d., https://www.dvmlaw.com/not-everything-including-metadata/.
505. „What Is End-to-End Encryption? Another Bull's-Eye on Big Tech“, *The New York Times*, žiūrėta 2020 m. rugpjūčio 23 d., https://www.nytimes.com/2019/11/19/technology/end-to-end-encryption.html.
506. Jonathan Mayer, „Content Moderation for End-to-End Encrypted Messaging“, 9, žiūrėta 2020 m. rugsėjo 4 d., https://www.cs.princeton.edu/~jrmayer/papers/Content_Moderation_for_End-to-End_Encrypted_Messaging.pdf
507. Damie Tarabay, „Australian Government Passes Contentious Encryption Law“, *The New York Times*, December 6, 2018, sec. World, žiūrėta 2020 m. rugsėjo 4 d., https://www.nytimes.com/2018/12/06/world/australia/encryption-bill-nauru.html.
508. „Most Powerful Countries | US News Best Countries“, žiūrėta 2020 m. rugsėjo 4 d., https://www.usnews.com/news/best-countries/power-rankings .
509. „The Global Influence of the United States“, *Study.Com*, žiūrėta 2020 m. rugsėjo 4 d., https://study.com/academy/lesson/the-global-influence-of-the-united-states.html

510. „NSA Slides Explain the PRISM Data-Collection Program“, *The Washington Post*, žiūrėta 2020 m. rugsėjo 4 d., https://www.washingtonpost.com/wp-srv/special/politics/prism-collection-documents/ .
511. Peter Swire ir DeBrae Kennedy-Mayo, „How Both the EU and the U.S. Are 'Stricter' Than Each Other for the Privacy of Government Requests for Information“ *Emory University School of Law*, žiūrėta 2020 m. rugsėjo 4 d., http://law.emory.edu/elj/content/volume-66/issue-3/articles/both-eu-us-stricter-privacy-requests-information.html .
512. Francesca Bignami, „The US Legal System on Data Protection in the Field of Law Enforcement. Safeguards, Rights and Remedies for EU Citizens“, žiūrėta 2020 m. rugsėjo 4 d., https://www.europarl.europa.eu/thinktank/en/document.html?reference=IPOL_STU(2015)519215 .
513. Daniel J. Solove, „The Growing Problems with the Sectoral Approach to Privacy Law“, *TeachPrivacy*, 2015, žiūrėta 2020 m. rugsėjo 4 d., https://teachprivacy.com/problems-sectoral-approach-privacy-law/ .
514. „Data Protection Law – HG.Org“, accessed August 12, 2020, https://www.hg.org/data-protection.html.
515. Stephen P Mulligan, Wilson C Freeman ir Chris D Linebaugh, „Data Protection Law: An Overview“, 79, žiūrėta 2020 m. rugsėjo 4 d., https://fas.org/sgp/crs/misc/R45631.pdf
516. Jake Frankenfield, „How Personally Identifiable Information (PII) Works“, *Investopedia*, žiūrėta 2020 m. rugsėjo 4 d., https://www.investopedia.com/terms/p/personally-identifiable-information-pii.asp .
517. Alexander Trowbridge, „NSA Spying: Ally Anger Justified?“, žiūrėta 2020 m. rugsėjo 8 d., https://www.cbsnews.com/news/nsa-spying-ally-anger-justified/.
518. „U.S. Senate: Constitution Day“, *US Senate*, žiūrėta 2020 m. rugsėjo 4 d., https://www.senate.gov/artandhistory/history/common/generic/ConstitutionDay.htm.
519. „The Third-Party Doctrine in the Wake of a "Seismic Shift"“, *American Bar*, žiūrėta 2020 m. rugsėjo 10 d., https://www.americanbar.org/groups/litigation/committees/privacy-data-security/practice/2019/third-party-doctrine-wake-of-seismic-shift/.
520. Simon Kuper, „Edward Snowden and the Millennial Conscience“, 2019, žiūrėta 2020 m. rugsėjo 4 d., https://www.ft.com/content/0d0114fe-1ea3-11e9-b126-46fc3ad87c65.
521. „The Electronic Communications Privacy Act ECPA Regulates How Information Stored“, *American Military University*, žiūrėta 2020 m. rugsėjo 4 d., https://www.coursehero.com/file/p24shsm4/The-Electronic-Communications-Privacy-Act-ECPA-regulates-how-information-stored/.
522. „Wiretap Report 2015“, *United States Courts*, žiūrėta 2020 m. rugsėjo 4 d., http://www.uscourts.gov/statistics-reports/wiretap-report-2015.
523. „Types of Surveillance Used, Arrests, and Convictions for Intercepts Installed January 1 Through December 31, 2015“, *United States Courts,* žiūrėta 2020 m.

rugsėjo 4 d., https://www.uscourts.gov/sites/default/files/data_tables/wiretap_6_1231.2015.pdf.
524. „Major Offenses for Which Court-Authorized Intercepts Were Granted Pursuant to 18 U.S.C. § 2519 January 1 Through December 31, 2015“, *United States Courts,* žiūrėta 2020 m. rugsėjo 4 d., http://www.uscourts.gov/sites/default/files/data_tables/wiretap_3_1231.2015.pdf.
525. „Wiretap Report 2017“, *United States Courts*, žiūrėta 2020 m. rugsėjo 4 d., http://www.uscourts.gov/statistics-reports/wiretap-report-2017.
526. Sophia Cope, „House Advances Email Privacy Act, Setting the Stage for Vital Privacy Reform“, *Electronic Frontier Foundation*, 2016, žiūrėta 2020 m. rugsėjo 4 d., https://www.eff.org/deeplinks/2016/04/house-advances-email-privacy-act-setting-stage-vital-privacy-reform.
527. „Coalition Letter in Support of Email Privacy Act (April 26)“, *Center for Democracy and Technology*, žiūrėta 2020 m. rugsėjo 4 d., https://cdt.org/insights/coalition-letter-in-support-of-email-privacy-act-april-26/.
528. „U.S. DOJ Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations“, *Public Intelligence*, žiūrėta 2020 m. rugsėjo 4 d., https://publicintelligence.net/u-s-doj-searching-and-seizing-computers-and-obtaining-electronic-evidence-in-criminal-investigations/.
529. Tim Cushing Fri, „Appeals Court: Stored Communications Act Privacy Protections Cover Opened And Read Emails“, *Techdirt.*, žiūrėta 2020 m. rugsėjo 4 d., https://www.techdirt.com/articles/20190311/20480141775/appeals-court-stored-communications-act-privacy-protections-cover-opened-read-emails.shtml.
530. Zack Whittaker, „How One Judge Single-Handedly Killed Trust in the US Technology Industry“, *ZDNet*, žiūrėta 2020 m. rugsėjo 4 d., https://www.zdnet.com/article/how-one-judge-single-handedly-killed-trust-in-the-us-technology-industry/.
531. Greg Stohr, „Justice Department Asks Court to Drop Microsoft Email Case“, *Bloomberg.Com*, 2018, žiūrėta 2020 m. rugsėjo 4 d., https://www.bloomberg.com/news/articles/2018-03-31/justice-department-asks-high-court-to-drop-microsoft-email-case.
532. Mary Jo Foley, „Microsoft Bullish on Congress' Inclusion of CLOUD Act in Funding Bill“, *ZDNet*, žiūrėta 2020 m. rugsėjo 4 d., https://www.zdnet.com/article/microsoft-bullish-on-congress-inclusion-of-cloud-act-in-funding-bill/.
533. „Privacy: An Overview of Federal Statutes Governing Wiretapping and Electronic Eavesdropping“, žiūrėta 2020 m. rugsėjo 4 d., https://www.everycrsreport.com/reports/98-326.html.
534. Mu-Chia Kao, „9th Circuit: ECPA Protects Domestic Communications of Non-US Citizens“, ILI Student Blog, žiūrėta 2020 m. rugsėjo 4 d., https://blogs.law.nyu.edu/privacyresearchgroup/2012/03/9th-circuit-ecpa-protects-domestic-communications-of-non-us-citizens/.

535. „Going Dark: Encryption, Technology, and the Balances Between Public Safety and Privacy“, *Federal Bureau of Investigation*, žiūrėta 2020 m. rugsėjo 4 d., https://www.fbi.gov/news/testimony/going-dark-encryption-technology-and-the-balances-between-public-safety-and-privacy.
536. Sabrina I. Pacifici, „House Homeland Security Report – Going Dark, Going Forward: A Primer on the Encryption Debate“, BeSpacific, žiūrėta 2020 m. rugsėjo 4 d., https://www.bespacific.com/house-homeland-security-report-going-dark-going-forward-a-primer-on-the-encryption-debate/.
537. Roger Dingledine, Nick Mathewson ir Paul Syverson, „Tor: The Second-Generation Onion Router“, žiūrėta 2020 m. rugsėjo 4 d., https://www.researchgate.net/publication/2910678_Tor_The_Second-Generation_Onion_Router.
538. „Government Hacking“, *Privacy International*, žiūrėta 2020 m. rugsėjo 4 d., https://privacyinternational.org/learn/government-hacking.
539. Rhys Dipshan, „A Federal Policy Loophole Is Supporting the Hacking-for-Hire Market. Can It Be Closed?“, *Slate Magazine*, 2018, žiūrėta 2020 m. rugsėjo 5 d., https://slate.com/technology/2018/06/the-federal-policy-loophole-supporting-the-hacking-for-hire-market.html.
540. Dan Goodin, „How ‘Omnipotent’ Hackers Tied to NSA Hid for 14 Years—and Were Found at Last“, *Ars Technica*, 2015, žiūrėta 2020 m. rugsėjo 5 d., https://arstechnica.com/information-technology/2015/02/how-omnipotent-hackers-tied-to-the-nsa-hid-for-14-years-and-were-found-at-last/.
541. GReAT, „Equation: The Death Star of Malware Galaxy“, žiūrėta 2020 m. rugsėjo 5 d., https://securelist.com/equation-the-death-star-of-malware-galaxy/68750/.
542. Ellen Nakashima, „Powerful NSA Hacking Tools Have Been Revealed Online“, *Washington Post*, 2016, žiūrėta 2020 m. rugsėjo 5 d., https://www.washingtonpost.com/world/national-security/powerful-nsa-hacking-tools-have-been-revealed-online/2016/08/16/bce4f974-63c7-11e6-96c0-37533479f3f5_story.html.
543. Thomas Brewster, „Equation = NSA? Researchers Uncloak Huge ‘American Cyber Arsenal’“, žiūrėta 2020 m. rugsėjo 5 d., https://www.forbes.com/sites/thomasbrewster/2015/02/16/nsa-equation-cyber-tool-treasure-chest/#5b3df5c9417f.
544. Pierluigi Paganini, „The Alleged NSA’s Unit The Equation Group Has Been Hacked. Exploits and Tools Leaked Online“, *Security Affairs*, 2016, žiūrėta 2020 m. rugsėjo 5 d., https://securityaffairs.co/wordpress/50334/cyber-warfare-2/equation-group-hacked.html.
545. Swati Khandelwal, „The NSA Hack — What, When, Where, How, Who & Why?“, *The Hacker News*, žiūrėta 2020 m. rugsėjo 5 d., https://thehackernews.com/2016/08/nsa-hack-russia-leak.html.
546. Pierluigi Paganini, „The Alleged NSA’s Unit The Equation Group Has Been Hacked!“, *Security Affairs*, žiūrėta 2020 m. rugsėjo 5 d., http://securityaffairs.co/wordpress/50334/cyber-warfare-2/equation-group-hacked.html.

547. Rob Price, „Edward Snowden: Russia Might Have Leaked Alleged NSA Cyberweapons as a 'Warning'", *Business Insider*, žiūrėta 2020 m. rugsėjo 5 d., https://www.businessinsider.com/edward-snowden-shadow-brokers-russia-leaked-nsa-equation-group-files-warning-dnc-hacking-2016-8.
548. Matt Suiche, „Shadow Brokers: The Insider Theory", *Medium*, 2017, žiūrėta 2020 m. rugsėjo 5 d., https://blog.comae.io/shadowbrokers-the-insider-theory-ded733b39a55.
549. „Who Are The Shadow Brokers?", *Cyber Security Intelligence*, žiūrėta 2020 m. rugsėjo 5 d., https://www.cybersecurityintelligence.com/blog/who-are-the-shadow-brokers-2684.html.
550. „In Re Warrant to Search Target Computer at Premises Unknown", *CaseText*, žiūrėta 2020 m. rugsėjo 5 d., https://casetext.com/case/in-re-search.
551. Andrew Crocker, „With Remote Hacking, the Government's Particularity Problem Isn't Going Away", *Just Security*, 2016, žiūrėta 2020 m. rugsėjo 5 d., https://www.justsecurity.org/31365/remote-hacking-governments-particularity-problem-isnt/.
552. „Case 76: Silk Road (Part 1)", *Casefile: True Crime Podcast*, 2018, žiūrėta 2020 m. rugsėjo 5 d., https://casefilepodcast.com/case-76-silk-road-part-1/.
553. Joshuah Bearman, „The Untold Story of Silk Road, Part 2: The Fall", *Wired*, 2015, žiūrėta 2020 m. rugsėjo 5 d., https://www.wired.com/2015/05/silk-road-2/.
554. Nicole Lee, „Anonymity Is Dead and Other Lessons from the Silk Road Trial | Engadget", žiūrėta 2020 m. rugsėjo 5 d., https://www.engadget.com/2015-02-08-silk-road-trial-lessons.html.
555. Jerzy Kosiński, „Deepweb And Darknet – Police View, 2015, žiūrėta 2020 m. rugsėjo 5 d., https://www.researchgate.net/publication/282333966
556. Orin S. Kerr ir Sean D. Murphy, „Government Hacking to Light the Dark Web", *Stanford Law Review*, 2017, žiūrėta 2020 m. rugsėjo 5 d., https://www.stanfordlawreview.org/online/government-hacking-to-light-the-dark-web/.
557. "Hacking the World, a Discussion of Changes to Rule 41", *Fourth Amendment Advisory Committee*, žiūrėta 2020 m. rugsėjo 5 d., https://www.fourthadvisory.org/news/2016/9/29/rule41-briefing.
558. Pierluigi Paganini, „US Supreme Court Allows FBI Hacking Computers Located Worldwide", *Security Affairs*, 2016, žiūrėta 2020 m. rugsėjo 5 d., https://securityaffairs.co/wordpress/46808/laws-and-regulations/46808.html.
559. Swati Khandelwal, „U.S. Supreme Court Allows the FBI to Hack Any Computer in the World", *The Hacker News*, žiūrėta 2020 m. rugsėjo 5 d., https://thehackernews.com/2016/04/fbi-hacking-power.html.
560. „What Is A Botnet?", žiūrėta 2020 m. rugsėjo 5 d., https://us.norton.com/internetsecurity-malware-what-is-a-botnet.html.
561. Dan Goodin, „Feds Deliver Fatal Blow to Botnet That Menaced World for 7 Years", *Ars Technica*, žiūrėta 2020 m. rugsėjo 5 d., https://arstechnica.com/tech-policy/2017/04/feds-deliver-fatal-blow-to-botnet-that-menaced-world-for-7-years/.

562. Aliya Sternstein, „FBI Allays Some Critics with First Use of New Mass-Hacking Warrant“, *Ars Technica*, 2020 m. rugsėjo 5 d., https://arstechnica.com/tech-policy/2017/04/fbi-allays-some-critics-with-first-use-of-new-mass-hacking-warrant/.
563. „NSA Slides Explain the PRISM Data-Collection Program“, *The Washington Post*, žiūrėta 2020 m. rugsėjo 5 d., http://www.washingtonpost.com/wp-srv/special/politics/prism-collection-documents/.
564. Dustin Volz, „Microsoft Says No Increase in U.S. Foreign Intelligence Surveillance Requests“, *Reuters*, 2017, žiūrėta 2020 m. rugsėjo 5 d., https://www.reuters.com/article/us-microsoft-surveillance-idUSKBN17F2G7.
565. „Share CSV Files Online – ShareCSV“, žiūrėta 2020 m. rugsėjo 5 d., http://www.sharecsv.com/s/9bc26c690cafb8774138caf8f0d8ea33/sanitized_ips.csv%20https://twitter.com/Snowden/status/851121195147767808.
566. „Report to Accompany S. 1566, the Foreign Intelligence Surveillance Act of 1978 (March 14, 1978)“, *US Senate*, žiūrėta 2020 m. rugsėjo 5 d., https://www.intelligence.senate.gov/sites/default/files/publications/95701.pdf.
567. „Justice Dept Appeal to the U.S. Foreign Intelligence Surveillance Court of Review“, žiūrėta 2020 m. rugsėjo 11 d., 2020, https://fas.org/irp/agency/doj/fisa/082102appeal.html.
568. „Report of the Director of the Administrative Office of the U.S. Courts
569. on activities of the Foreign Intelligence Surveillance Courts for 2015“, žiūrėta 2020 m. rugsėjo 6 d., http://www.uscourts.gov/sites/default/files/fisc_annual_report_2015.pdf.
570. Elizabeth Goitein, „The NSA's Backdoor Search Loophole“, *Boston Review*, 2013, žiūrėta 2020 m. rugsėjo 5 d., https://bostonreview.net/blog/elizabeth-goitein-nsa-backdoor-search-loophole-freedom-act.
571. „WikiLeaks – Intelligence“, žiūrėta 2020 m. rugsėjo 6 d., https://wikileaks.org/+-Intelligence-+.html.
572. Eric Lichtblau, „Deal Reached in Congress to Rewrite Rules on Wiretapping – The New York Times“, žiūrėta 2020 m. rugsėjo 6 d., https://www.nytimes.com/2008/06/20/washington/20fisacnd.html.
573. Office of the Inspector General, „A Review of the FBI's Use of Pen Register and Trap and Trace Devices Under the Foreign Intelligence Surveillance Act in 2007 through 2009 – Executive Summary“, 7, žiūrėta 2020 m. rugsėjo 6 d., https://oig.justice.gov/reports/2015/o1506.pdf.
574. „EPIC – EPIC v. DOJ – Pen Register Reports“, *Electronic Privacy Information Center*, žiūrėta 2020 m. rugsėjo 6 d., https://epic.org/foia/doj/pen-reg-trap-trace/.
575. „Transparency Report: THE USA FREEDOM Act Business Records FISA Implementation“, žiūrėta 2020 m. rugsėjo 6 d., https://fas.org/irp/nsa/ufa-2016.pdf.
576. Administration White Paper, „Bulk Collection of Telephony Metadata Under Section 215 of the USA PATRIOT Act“, žiūrėta 2020 m. rugsėjo 6 d., https://fas.org/irp/nsa/bulk-215.pdf.

577. Jonathan Mayer, „In NSA Appeals, DOJ Misleads About Medical and Financial Records“, *Web Policy*, žiūrėta 2020 m. rugsėjo 6 d., http://webpolicy.org/2014/12/11/nsa-appeals-medical-financial-records/.
578. Margaret Hartmann, „The CIA Collects Data in Bulk, Just Like the NSA“, *Intelligencer*, žiūrėta 2020 m. rugsėjo 6 d., https://nymag.com/intelligencer/2013/11/cia-collects-data-in-bulk-just-like-the-nsa.html.
579. Ashley Gorski, „This Secret Court Opinion Reveals Mystery Tech Firm Challenged NSA Surveillance Order“, *American Civil Liberties Union*, žiūrėta 2020 m. rugsėjo 6 d., https://www.aclu.org/blog/national-security/privacy-and-surveillance/secret-court-opinion-reveals-mystery-tech-firm.
580. „Standing, Surveillance, and Technology Companies“, žiūrėta 2020 m. rugsėjo 6 d., https://harvardlawreview.org/2018/04/standing-surveillance-and-technology-companies/.
581. „ACLU Sues Over Unconstitutional Dragnet Wiretapping Law“, *American Civil Liberties Union*, žiūrėta 2020 m. rugsėjo 6 d., https://www.aclu.org/press-releases/aclu-sues-over-unconstitutional-dragnet-wiretapping-law.
582. „Amnesty International and etc. Complaint for Declaratory and Injunctive Relief“, žiūrėta 2020 m. rugsėjo 6 d., https://www.aclu.org/sites/default/files/pdfs/safefree/faa_complaint_20080710.pdf.
583. „Amnesty v. Clapper – Challenge to FISA Amendments Act“, *American Civil Liberties Union*, žiūrėta 2020 m. rugsėjo 6 d., https://www.aclu.org/cases/amnesty-v-clapper-challenge-fisa-amendments-act.
584. Tim Phillips, „Supreme Court Dismisses Lawsuit Challenging Warrantless Eavesdropping Law“, *Activist Defense*, 2013, žiūrėta 2020 m. rugsėjo 6 d., https://activistdefense.wordpress.com/2013/02/27/supreme-court-dismisses-lawsuit-challenging-warrantless-eavesdropping-law/.
585. Tim Ferriss, „What Every American Needs to Know (and Do) About FISA Today“, *YouTube*, žiūrėta 2020 m. rugsėjo 6 d., https://www.youtube.com/watch?v=hIaWdH6XaBM.
586. „NSA Prism Program Taps in to User Data of Apple, Google and Others“, *The Guardian*, 2013, žiūrėta 2020 m. rugsėjo 6 d., http://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data.
587. Laura Smith-Spark, „Merkel: Relations with U.S. 'severely Shaken' over Spying Claims“, *CNN*, žiūrėta 2020 m. rugsėjo 6 d., https://www.cnn.com/2013/10/24/world/europe/europe-summit-nsa-surveillance/index.html.
588. „NSA Slides Explain the PRISM Data-Collection Program“, *The Washington Post*, žiūrėta 2020 m. rugsėjo 4 d., https://www.washingtonpost.com/wp-srv/special/politics/prism-collection-documents/ .
589. „Facts on the Collection of Intelligence Pursuant to Section 702 of the Foreign Intelligence Surveillance Act“, žiūrėta 2020 m. rugsėjo 6 d., https://web.archive.org/web/20130611065954/http://www.dni.gov/index.php/newsroom/press-releases/191-press-releases-2013/871-facts-on-the-collection-of-intelligence-pursuant-to-section-702-of-the-foreign-intelligence-surveillance-act.

590. „NSA Prism Program Taps in to User Data of Apple, Google and Others“, *The Guardian*, 2013, žiūrėta 2020 m. rugsėjo 6 d., http://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data.
591. „Europol in Brief 2018“, *Europol*, žiūrėta 2020 m. rugsėjo 6 d., https://www.europol.europa.eu/activities-services/main-reports/europol-in-brief-2018.
592. Scott Shane, Matthew Rosenberg ir Andrew W. Lehren, „WikiLeaks Releases Trove of Alleged C.I.A. Hacking Documents“, *The New York Times*, 2017, žiūrėta 2020 m. rugsėjo 6 d., https://www.nytimes.com/2017/03/07/world/europe/wikileaks-cia-hacking.html.
593. „Trump's Trade War With China Is Officially Underway“, *The New York Times*, žiūrėta 2020 m. rugsėjo 6 d., https://www.nytimes.com/2018/07/05/business/china-us-trade-war-trump-tariffs.html.
594. „Red moon rising“, *The Economist*, žiūrėta 2020 m. rugsėjo 6 d., https://www.economist.com/leaders/2019/01/12/how-china-could-dominate-science.
595. „The China Issue“, *Massachusetts Institite of Technology (MIT) Technology Review,* žiūrėta 2020 m. rugsėjo 6 d., https://www.technologyreview.com/magazines/the-china-issue/.
596. „NSA Spied on Indian Embassy and UN Mission, Edward Snowden Files Reveal“, *The Guardian*, 2013, žiūrėta 2020 m. rugsėjo 6 d., http://www.theguardian.com/world/2013/sep/25/nsa-surveillance-indian-embassy-un-mission.
597. Dustin Volz ir Steve Holland, „White House Supports Renewal of Spy Law without Reforms: Official“, *Reuters*, 2017, žiūrėta 2020 m. rugsėjo 6 d., https://www.reuters.com/article/us-usa-trump-fisa-idUSKBN16855P.
598. „House Extends Surveillance Law, Rejecting New Privacy Safeguards“, *The New York Times*, žiūrėta 2020 m. rugsėjo 6 d., https://www.nytimes.com/2018/01/11/us/politics/fisa-surveillance-congress-trump.html.
599. „The State of Privacy in America“, *Pew Research Center*, žiūrėta 2020 m. rugsėjo 6 d., https://www.pewresearch.org/fact-tank/2016/09/21/the-state-of-privacy-in-america/.
600. „NSA Prism Program Taps in to User Data of Apple, Google and Others“, *The Guardian*, 2013, žiūrėta 2020 m. rugsėjo 6 d., http://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data.
601. Reinhard Kreissl, *Terrorism, mass surveillance and civil rights*, *CEPOL*, žiūrėta 2020 m. rugpjūčio 14 d., https://www.cepol.europa.eu/sites/default/files/26-reinhard-kreissl.pdf.
602. Ellen Nakashima, „NSA Phone Record Collection Does Little to Prevent Terrorist Attacks, Group Says“, *Washington Post*, 2014, žiūrėta 2020 m. rugsėjo 6 d., https://www.washingtonpost.com/world/national-security/nsa-phone-record-collection-does-little-to-prevent-terrorist-attacks-group-says/2014/01/12/8aa860aa-77dd-11e3-8963-b4b654bcc9b2_story.html.
603. Peter Bergen ir kt., „Do NSA's Bulk Surveillance Programs Stop Terrorists“, žiūrėta 2020 m. rugpjūčio 14 d. https://d1y8sb8igg2f8e.cloudfront.net/documents/Do-NSAs-Bulk-Surveillance-Programs-Stop-Terrorists.pdf.

604. „EPIC – Executive Order 12333“, *Electronic Privacy Information Center*, žiūrėta 2020 m. rugsėjo 6 d., https://epic.org/privacy/surveillance/12333/.
605. „Presidential Documents“, žiūrėta 2020 m. rugpjūčio 14 d., https://www.govinfo.gov/content/pkg/FR-2003-01-28/pdf/03-2069.pdf.
606. „Executive Order: Strengthened Management of the Intelligence Community“, žiūrėta 2020 m. rugsėjo 6 d., https://georgewbush-whitehouse.archives.gov/news/releases/2004/08/20040827-6.html.
607. „Executive Order 13470“, žiūrėta 2020 m. rugsėjo 6 d., https://fas.org/irp/offdocs/eo/eo-13470.htm.
608. „Executive Order 12333“, žiūrėta 2020 m. rugsėjo 7 d., https://www.dni.gov/index.php/ic-legal-reference-book/executive-order-12333.
609. „United States Signals Intelligence Directive“, žiūrėta 2020 m. rugpjūčio 14 d. https://www.dni.gov/files/documents/1118/CLEANEDFinal%20USSID%20SP0018.pdf.
610. John Napier Tye, „Meet Executive Order 12333: The Reagan Rule That Lets the NSA Spy on Americans“, *Washington Post*, 2014, žiūrėta 2020 m. rugsėjo 7 d., https://www.washingtonpost.com/opinions/meet-executive-order-12333-the-reagan-rule-that-lets-the-nsa-spy-on-americans/2014/07/18/93d2ac22-0b93-11e4-b8e5-d0de80767fc2_story.html.
611. „Youngstown Sheet & Tube Co. v. Sawyer, (Jackson., J. concurring)“, žiūrėta 2020 m. rugsėjo 7 d., https://www.law.cornell.edu/supremecourt/text/343/579.
612. „Youngstown Sheet & Tube Co. v. Sawyer, (Jackson., J. concurring)“, žiūrėta 2020 m. rugsėjo 7 d., https://www.law.cornell.edu/supremecourt/text/343/579.
613. „Justice Jackson's Test for the Exercise of Presidential Power (*Youngstown* 1952)“, žiūrėta 2020 m. rugpjūčio 14 d., http://law2.umkc.edu/faculty/projects/ftrials/conlaw/jacksontest.html.
614. Jonathan Mayer, „Executive Order 12333 on American Soil, and Other Tales from the FISA Frontier“, *Web Policy*, žiūrėta 2020 m. rugsėjo 7 d., http://webpolicy.org/2014/12/03/eo-12333-on-american-soil/.
615. „Youngstown Sheet & Tube Co. v. Sawyer, (Jackson., J. concurring)“, žiūrėta 2020 m. rugsėjo 7 d., https://www.law.cornell.edu/supremecourt/text/343/579.
616. Jonathan Mayer, „Executive Order 12333 (The President's Inherent Article II Power to Conduct Foreign Intelligence)“, *YouTube*, 2014, žiūrėta 2020 m. rugsėjo 7 d., https://www.youtube.com/watch?v=Hr36zslqQMU.
617. Adrienne LaFrance, „How Drug War Surveillance Turned Into Terrorism Surveillance“, *The Atlantic*, 2015, žiūrėta 2020 m. rugsėjo 7 d., https://www.theatlantic.com/technology/archive/2015/04/same-surveillance-state-different-war/389988/.
618. Patrick Toomey, „The NSA Continues to Violate Americans' Internet Privacy Rights“, *American Civil Liberties Union*, žiūrėta 2020 m. rugsėjo 7 d., https://www.aclu.org/blog/national-security/privacy-and-surveillance/nsa-continues-violate-americans-internet-privacy.

619. „National security agency, memorandum: the national security agency: missions, authorities, oversight and partnerships at 2–3 (2013)“, žiūrėta 2017 m. liepos 13 d., www.nsa.gov/public_info/_files/speeches_testimonies/2013_08_09_the_nsa_story.pdf .
620. Timothy Edgar, „Surveillance Reform: Privacy Board Turns to E.O. 12,333“, *Lawfare*, 2015, žiūrėta 2020 m. rugsėjo 7 d., https://www.lawfareblog.com/surveillance-reform-privacy-board-turns-eo-12333.
621. Louis Nelson, „Trump Calls Unauthorized NSA Collection of Data ‘a Disgrace’“, *Politico*, žiūrėta 2020 m. rugsėjo 7 d., https://politi.co/2z3ykoU.
622. „Data Protection, Privacy and New Technologies“, *European Union Agency for Fundamental Rights*, žiūrėta 2020 m. rugsėjo 7 d., https://fra.europa.eu/en/themes/data-protection-privacy-and-new-technologies.
623. „Surveillance by Intelligence Services: Fundamental Rights Safeguards and Remedies in the EU – Volume II: Field Perspectives and Legal Update, *European Union Agency for Fundamental Rights*, 2017, žiūrėta 2020 m. rugpjūčio 23 d., https://fra.europa.eu/sites/default/files/fra_uploads/fra-2017-surveillance-intelligence-services-vol-2_en.pdf.
624. „Roger Clarke’s ‘Privacy Introduction and Definitions’“, žiūrėta 2020 m. rugsėjo 7 d., http://www.rogerclarke.com/DV/Intro.html.
625. Ava Kofman, „Digital Jail: How Electronic Monitoring Drives Defendants Into Debt“, *The New York Times*, 2019, žiūrėta 2020 m. rugsėjo 7 d., https://www.nytimes.com/2019/07/03/magazine/digital-jail-surveillance.html.
626. „Who We Are“, *The Council of Europe in Brief*, žiūrėta 2020 m. rugsėjo 7 d., https://www.coe.int/en/web/about-us/who-we-are.
627. „Handbook on European Data Protection Law – 2018 Edition“, *European Union Agency for Fundamental Rights*, 2018, 14, žiūrėta 2020 m. rugsėjo 7 d., https://fra.europa.eu/en/publication/2018/handbook-european-data-protection-law-2018-edition.
628. „Personal Data Protection,Fact Sheets on the European Union“, *European Parliament*, žiūrėta 2020 m. rugsėjo 10 d., https://www.europarl.europa.eu/factsheets/en/sheet/157/personal-data-protection.
629. „Accession by States which are not member States of the Council of Europe“, *Council of Europe*, žiūrėta 2015 m. lapkričio 18 d., https://rm.coe.int/16809028a4.
630. „Full List“, *Treaty Office*, žiūrėta 2015 m. lapkričio 18 d., https://www.coe.int/en/web/conventions/full-list.
631. „Details of Treaty No.108“, *Council of Europe*, žiūrėta 2020 m. rugsėjo 7 d., http://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108
632. „Accession by States which are not member States of the Council of Europe“, *Council of Europe*, žiūrėta 2015 m. lapkričio 18 d., https://rm.coe.int/16809028a4.
633. „Council of Europe Data Protection Website“, *Data Protection*, žiūrėta 2015 m. lapkričio 18 d., https://www.coe.int/en/web/data-protection/home.

634. „Convention 108 Bureau of the consultative committee of the convention for the protection of individuals with regard to automatic processing of personal data“, *Council of Europe*, žiūrėta 2020 m. rugpjūčio 14 d., https://rm.coe.int/the-consultative-committee-of-the-convention-for-the-protection-of-ind/168073e153.
635. „Speaking Points for the Deputy Secretary General Opening of the 21st t-PD Bureau Meeting“, *Council of Europe*, žiūrėta 2020 m. rugpjūčio 14 d., https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016806869a9
636. „Convention 108+ : The Modernised Version of a Landmark Instrument“, *Council of Europe*, žiūrėta 2020 m. rugsėjo 7 d., https://www.coe.int/en/web/data-protection/newsroom/-/asset_publisher/7oll6Oj8pbV8/content/modernisation-of-convention-108
637. „Dutch government rejects idea of no-spy agreements between European countries“, *Policy Observatory*, žiūrėta 2020 m. rugsėjo 7 d., https://observatory.mappingtheinternet.eu/tags/intelligence%20codex.
638. „The Hague Programme Ten priorities for the next five years“, *European Commission*, žiūrėta 2020 m. rugsėjo 7 d., https://ec.europa.eu/commission/presscorner/detail/en/MEMO_05_153.
639. „Europol Review 2013“, 89, *European Police Office*, žiūrėta 2020 m. rugpjūčio 14 d., https://www.europol.europa.eu/activities-services/main-reports/europol-review-2013 .
640. „Data protection at Eurojust, *Eurojust*, žiūrėta 2020 m. rugsėjo 10 d., http://www.eurojust.europa.eu/Practitioners/Data-Protection/Pages/Data-protection-at-Eurojust.aspx.
641. „Commission proposes a comprehensive reform of data protection rules to increase users‘ control of their data and to cut costs for businesses“, *European Commission*, žiūrėta 2020 m. rugpjūčio 15 d., http://europa.eu/rapid/press-release_IP-12-46_en.htm?locale=en.
642. d., https://ico.org.uk/media/about-the-ico/documents/1042349/review-of-eu-dp-directive.pdf.
643. „Agreement on Commission's EU Data Protection Reform Will Boost Digital Single Market“, *European Commission,* žiūrėta 2020 m. rugpjūčio 15 d., https://ec.europa.eu/commission/presscorner/detail/en/IP_15_6321.
644. „Six Commission priorities for 2019-2023“, *European Commission*, žiūrėta 2020 m. rugpjūčio 15 d., http://ec.europa.eu/priorities/digital-single-market/.
645. „Agreement on Commission‘s EU data protection reform will boost Digital Single Market“, *European Commission*, žiūrėta 2020 m. rugpjūčio 15 d., http://europa.eu/rapid/press-release_IP-15-6321_en.htm.
646. „Big data“, *European Commission*, žiūrėta 2020 m. rugpjūčio 15 d., https://ec.europa.eu/digital-single-market/en/big-data.
647. „Big Data Has an 'I Don't Know' Problem“, *AgWeb*, žiūrėta 2020 m. rugpjūčio 15 d., https://www.agweb.com/article/big-data-has-an-i-dont-know-problem-NAA-ben-potter.

648. Natasha, Singer, „With a Few Bits of Data, Researchers Identify 'Anonymous' People", *The New York Times*, žiūrėta 2020 m. rugpjūčio 15 d., https://bits.blogs.nytimes.com/2015/01/29/with-a-few-bits-of-data-researchers-identify-anonymous-people/.
649. Scott Berinato, „There's No Such Thing as Anonymous Data", *Harvard Business Review*, 2015, žiūrėta 2020 m. rugsėjo 7 d., https://hbr.org/2015/02/theres-no-such-thing-as-anonymous-data.
650. Patrick Tucker, „Has Big Data Made Anonymity Impossible?", *MIT Technology Review*, žiūrėta 2020 m. rugsėjo 7 d., https://www.technologyreview.com/2013/05/07/178542/has-big-data-made-anonymity-impossible/.
651. „Attitudes on Data Protection and Electronic Identity in the European Union", *Special Eurobarometer 359*, žiūrėta 2020 m. rugsėjo 10 d., https://ec.europa.eu/commfrontoffice/publicopinion/archives/ebs/ebs_359_en.pdf.
652. „Reforma. Renginiai", *Valstybinė asmens duomenų inspekcija*, žiūrėta 2020 m. rugpjūčio 15 d., https://www.ada.lt/go.php/Renginiai975.
653. Charles Hymas, „A Decade of Smartphones: We Now Spend an Entire Day Every Week Online", *The Telegraph*, 2018, žiūrėta 2020 m. rugsėjo 7 d., https://www.telegraph.co.uk/news/2018/08/01/decade-smartphones-now-spend-entire-day-every-week-online/.
654. „How Much Time Do People Spend Online Each Day?", *UKOM*, 2018, žiūrėta 2020 m. rugsėjo 7 d., https://ukom.uk.net/insights/87-how-much-time-do-people-spend-online-each-day.php.
655. „UK Surveillance Powers Explained", *BBC News*, 2015, žiūrėta 2020 m. rugsėjo 7 d., https://www.bbc.com/news/uk-34713435.
656. Graham Smith, „Content versus Metadata", *Internet Newsletter for Lawyers*, 2017, žiūrėta 2020 m. rugsėjo 7 d., https://www.infolaw.co.uk/newsletter/2017/01/content-versus-metadata/.
657. „Briefing Note: Why Communications Data (Metadata) Matter", *Big Brother Watch*, žiūrėta 2020 m. rugpjūčio 15 d., https://www.bigbrotherwatch.org.uk/wp-content/uploads/2014/07/Communications-Data-Briefing.pdf .
658. Campbell Simpson, „Your Metadata Isn't Private Personal Information, Federal Court Decides", *Gizmodo Australia*, 2017, žiūrėta 2020 m. rugsėjo 7 d., https://www.gizmodo.com.au/2017/01/your-metadata-isnt-private-personal-information-federal-court-decides/.
659. C. Christine Porter, „De-Identified Data and Third Party Data Mining: The Risk of Re-Identification of Personal Information", *University of Washington Shidler Journal of Law, Commerce & Technology*, 2008, žiūrėta 2020 m. rugjūčio 15 d., https://digitalcommons.law.uw.edu/cgi/viewcontent.cgi?article=1075&context=wjlta.
660. „Big Data Analysis and Anonymisation Techniques under the EU General Data Protection Regulation", *Financier Worldwide*, žiūrėta 2020 m. rugsėjo 7 d., https://www.financierworldwide.com/big-data-analysis-and-anonymisation-techniques-under-the-eu-general-data-protection-regulation.

661. Will Knight, „This AI Lets You Deepfake Your Voice to Speak like Barack Obama“, *MIT Technology Review*, žiūrėta 2020 m. rugsėjo 7 d., https://www.technologyreview.com/2019/02/27/66005/this-ai-lets-you-deepfake-your-voice-to-speak-like-barack-obama/.
662. Zachary W. Rosenberg, „Returning to Plato‘s Cave: Metadata‘s Shadows in the Courtroom“, *Arizona State Law Journal*, 2016, žiūrėta 2020 m. rugpjūčio 16 d., http://arizonastatelawjournal.org/wp-content/uploads/2016/07/Rosenberg_Final.pdf.
663. Charles Arthur, „Internet Regulation: Is It Time to Rein in the Tech Giants?“, *The Observer*, 2017, žiūrėta 2020 m. rugsėjo 7 d., https://www.theguardian.com/technology/2017/jul/02/is-it-time-to-rein-in-the-power-of-the-internet-regulation.
664. Olivia Solon, „Net Neutrality: ‘father of Internet’ Joins Tech Leaders in Condemning Repeal Plan“, *The Guardian*, 2017, žiūrėta 2020 m. rugsėjo 7 d., https://www.theguardian.com/technology/2017/dec/11/net-neutrality-vint-cerf-tim-berners-lee-fcc-letter.
665. Julia Fioretti, „Europe Seeks Power to Seize Overseas Data in Challenge to Tech Giants“, *Reuters*, 2018, žiūrėta 2020 m. rugsėjo 7 d., https://www.reuters.com/article/us-eu-data-order-idUSKCN1GA0LP.
666. Jane Wakefield Cellan-Jones Rory, „Russia ‘successfully Tests’ Its Unplugged Internet“, *BBC News*, 2019, žiūrėta 2020 m. rugsėjo 7 d., https://www.bbc.com/news/technology-50902496.
667. „China and Huawei Propose Reinvention of the Internet“, žiūrėta 2020 m. rugsėjo 7 d., https://amp.ft.com/content/c78be2cf-a1a1-40b1-8ab7-904d7095e0f2?fbclid=IwAR3Ne3_yWeoJTCKtoDU2-n0uN9DkXZ038LYi-b4ORBaiXr35hmtk3_MtI8lw.
668. „How Does the Internet Work?“, *Stanford University*, žiūrėta 2020 m. rugsėjo 7 d., https://web.stanford.edu/class/msande91si/www-spr04/readings/week1/InternetWhitepaper.htm.
669. Pierre Bellanger, „De la souveraineté en général et de la souveraineté numérique en particulier“, lesechos.fr, 2011, žiūrėta 2020 m. rugpjūčio 16 d., http://archives.lesechos.fr/archives/cercle/2011/08/30/cercle_37239.htm.
670. Farid Gueham, „Digital sovereignty – steps towards a new system of internet governance“, žiūrėta 2020 m. rugpjūčio 16 d., https://euagenda.eu/upload/publications/untitled-77045-ea.pdf.
671. Dina Bass, „Microsoft Says AI Advances Will Require New Laws, Regulations“, *Bloomberg.Com*, 2018, žiūrėta 2020 m. rugsėjo 7 d., https://www.bloomberg.com/news/articles/2018-01-18/microsoft-says-ai-advances-will-require-new-laws-regulations.
672. „Global Commission on Internet Governance Paper Series“, *Centre for International Governance Innovation*, žiūrėta 2020 m. rugsėjo 7 d., https://www.cigionline.org/series/global-commission-internet-governance-paper-series.

673. Robert Tchenguiz, „A New Breed of Commercial Intelligence Company“, *Financial Times*, 2015, žiūrėta 2020 m. rugsėjo 7 d., https://www.ft.com/content/e0133cf6-cd66-11e4-9144-00144feab7de.
674. Michael Smith, „Private Intelligence Companies How the Spooks Moved in on Big Business“, žiūrėta 2020 m. rugpjūčio 17 d., https://web.archive.org/web/20090205143528/http://michaelsmithwriter.com/pdf/intelligence_companies.pdf.
675. „Search and Surveillance Act 2012 No 24 (as at 12 April 2019), Public Act Contents – New Zealand Legislation“, žiūrėta 2020 m. rugsėjo 7 d., http://www.legislation.govt.nz/act/public/2012/0024/193.0/DLM2136536.html.
676. „Human Rights Commission: Intelligence and Security Bill Good Effort, but Scrutiny Needed“, žiūrėta 2020 m. rugsėjo 7 d., https://www.hrc.co.nz/news/intelligence-and-security-bill-good-effort-scrutiny-needed/.
677. Natasha Lomas, „Mass Surveillance for National Security Does Conflict with EU Privacy Rights, Court Advisor Suggests“, *TechCrunch*, žiūrėta 2020 m. rugsėjo 7 d., https://social.techcrunch.com/2020/01/15/mass-surveillance-for-national-security-does-conflict-with-eu-privacy-rights-court-advisor-suggests/.
678. „Current Practices in Electronic Surveillance in the Investigation of Serious and Organized Crime“, *United Nations*, 2009, žiūrėta 2020 m. rugpjūčio 17 d., https://www.unodc.org/documents/organized-crime/Law-Enforcement/Electronic_surveillance.pdf.
679. Anastasiya Kazakova, „The EU's e-Evidence & the U.S. CLOUD Act: Race Only to Start“, *Kaspersky*, žiūrėta 2020 m. rugsėjo 7 d., https://www.kaspersky.com/about/policy-blog/privacy/e-evidence-and-cloud-act.
680. „Frequently Asked Questions: New EU rules to obtain electronic evidence“, *European Commission*, 2018, žiūrėta 2020 m. rugpjūčio 25 d., https://ec.europa.eu/commission/presscorner/detail/en/MEMO_18_3345.
681. „Recommendation for a Council Decision authorising the opening of negotiations in view of an agreement between the European Union and the United States of America on cross-border access to electronic evidence for judicial cooperation in criminal matters“, *European Commission*, žiūrėta 2020 m. rugpjūčio 25 d., https://ec.europa.eu/info/sites/info/files/recommendation_council_decision_eu_us_e-evidence.pdf.
682. „Facebook plans third data center in Luleå, Sweden“, *Data Center Dynamics,* žiūrėta 2020 m. rugpjūčio 29 d., https://www.datacenterdynamics.com/en/news/facebook-plans-third-data-center-in-lule%C3%A5-sweden/
683. Glenn Fleishman ir kt., „How to Find out Where Apple Stores Your ICloud Data (Spoiler: You Can't Exactly)“, *Macworld*, 2018, žiūrėta 2020 m. rugpjūčio 25 d., https://www.macworld.com/article/3274584/where-does-apple-stores-your-icloud-data.html.
684. „Azure facilities, premises, and physical security“, *Microsoft,* žiūrėta 2020 m. rugpjūčio 26 d., https://docs.microsoft.com/en-us/azure/security/fundamentals/physical-security.

685. „Microsoft“, *DataCenters*, žiūrėta 2020 m. rugpjūčio 26 d., https://www.datacenters.com/providers/microsoft.
686. „Microsoft Privacy. Where is your data located?“, *Microsoft*, žiūrėta 2020 m. rugpjūčio 26 d., https://www.microsoft.com/en-us/trust-center/privacy/data-location.
687. Mehreen Khan, „EU governments approve draft rules on sharing 'e-evidence'“, *Financial Times*, 2018, žiūrėta 2020 m. rugpjūčio 25 d., https://www.ft.com/content/63a6105a-fa24-11e8-af46-2022a0b02a6c.
688. „Draft Report. European Production and Preservation Orders for electronic evidence in criminal matters Proposal for a decision (COM(2018)0225 – C8-0155/2018 – 2018/0108(COD))“, *European Parlament*, žiūrėta 2020 m. rugpjūčio 25 d., https://www.europarl.europa.eu/doceo/document/LIBE-AM-644870_EN.pdf
689. Anastasiya Kazakova, „The EU's e-Evidence & the U.S. CLOUD Act: Race Only to Start“, *Kaspersky*, žiūrėta 2020 m. rugsėjo 8 d., https://www.kaspersky.com/about/policy-blog/privacy/e-evidence-and-cloud-act.
690. Chris Jones ir Ben Hayes, „The EU Data Retention Directive: a case study in the legitimacy and effectiveness of EU counter-terrorism policy, Securing Europe through Counter- Terrorism: Impact, Legitimacy and Effectiveness“, *Statewatch*, 2013, 4, žiūrėta 2020 m. rugpjūčio 17 d., https://www.statewatch.org/media/documents/news/2013/dec/secile-data-retention-directive-in-europe-a-case-study.pdf
691. Jamie Condliffe, „Security Experts Agree: The NSA Was Hacked“, *MIT Technology Review*, žiūrėta 2020 m. rugsėjo 8 d., https://www.technologyreview.com/2016/08/18/70386/security-experts-agree-the-nsa-was-hacked/.
692. Rob Price, „'Shadow Brokers' Claims to Hack 'Equation Group,' Group Linked to NSA“, *Business Insider*, žiūrėta 2020 m. rugsėjo 8 d., https://www.businessinsider.com/shadow-brokers-claims-to-hack-equation-group-group-linked-to-nsa-2016-8?international=true&r=US&IR=T.
693. James Carafano, „PRISM Is Essential to U.S. Security in War Against Terrorism“, *The Heritage Foundation*, žiūrėta 2020 m. rugpjūčio 17 d., https://www.heritage.org/defense/commentary/prism-essential-us-security-war-against-terrorism.
694. „Mass Surveillace“, *Council of Europe*, žiūrėta 2020 m. rugpjūčio 17 d. http://assembly.coe.int/nw/xml/XRef/Xref-XML2HTML-en.asp?fileid=21692.
695. „Online Mass-Surveillance: 'Protect Right to Privacy Even When Countering Terrorism“, *United Nations*, žiūrėta 2020 m. rugpjūčio 17 d., https://www.ohchr.org/SP/NewsEvents/Pages/DisplayNews.aspx?NewsID=15200&LangID=E.
696. „Informacinės visuomenės paslaugų samprata“, *Informacinės visuomenės plėtros komitetas*, žiūrėta 2020 m. rugsėjo 8 d., http://ivpk.lrv.lt/lt/veiklos-sritys-1/informacines-visuomenes-paslaugos-1/informacines-visuomenes-paslaugu-samprata.
697. „ECJ Clarifies Scope of Telecoms Regulation for OTT Services“, *Technology's Legal Edge*, 2019, žiūrėta 2020 m. rugsėjo 8 d., https://www.technologyslegaledge.com/2019/07/ecj-clarifies-scope-of-telecoms-regulation-for-ott-services/.

698. „Russian Agents Plunge to New Ocean Depths in Ireland to Crack Transatlantic Cables“, *The Sunday Times,* žiūrėta 2020 m. rugsėjo 8 d., https://www.thetimes.co.uk/article/russian-agents-plunge-to-new-ocean-depths-in-ireland-to-crack-transatlantic-cables-fnqsmgncz.
699. „Current Practices in Electronic Surveillance in the Investigation of Serious and Organized Crime“, United Nations, 2009, 13, žiūrėta 2020 m. rugpjūčio 17 d., https://www.unodc.org/documents/organized-crime/Law-Enforcement/Electronic_surveillance.pdf.
700. „Kanados baudžiamojo proceso kodekso 184(2) str., „Consolidated Federal Laws of Canada, Criminal Code“, *Legislative Services Branch*, 2020, žiūrėta 2020 m. rugpjūčio 17., https://laws-lois.justice.gc.ca/eng/acts/C-46/page-41.html#h-6.
701. *Review of the Search and Surveillance Act 2012 =: Ko Te Arotake i Te Search and Surveillance Act 2012*, Unredacted version, Report 141 (Wellington, New Zealand: Law Commission, Te Aka Matua o te Ture : Ministry of Justice, Tāhū o te Ture, 2017), 58, žiūrėta 2020 m. rugpjūčio 17 d., https://www.lawcom.govt.nz/sites/default/files/projectAvailableFormats/NZLC-R141-Review-of-the-Search-and-Surveillance-Act-2012-final_0.pdf.
702. „Consolidated Federal Laws of Canada, Criminal Code“, *Legislative Services Branch*, 2020, žiūrėta 2020 m. rugpjūčio 17., https://laws-lois.justice.gc.ca/eng/acts/C-46/page-41.html#h-6.
703. „U.S. DOJ Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations“.
704. „How Much Data Is There In the World?“, *Bernard Marr*, žiūrėta 2020 m. rugsėjo 9 d., https://www.bernardmarr.com/default.asp?contentID=1846.
705. „Tech Firms Can't Keep Our Data Forever: We Need a Digital Expiry Date“, *The Guardian*, 2018, žiūrėta 2020 m. rugsėjo 9 d., http://www.theguardian.com/commentisfree/2018/may/19/online-privacy-digital-expiry-date.
706. Rob Crossley, „Where in the World Is My Data and How Secure Is It?“, *BBC News*, 2016, žiūrėta 2020 m. rugsėjo 9 d., https://www.bbc.com/news/business-36854292.
707. Patrick Stump, „Are Text Messages Encrypted?“, *Rokacom*, 2018, žiūrėta 2020 m. rugpjūčio 17 d., https://www.rokacom.com/are-text-messages-encrypted/.
708. Robert Triggs, „What is SMS and How Does it Work?“, *Android Authority*, 2013, žiūrėta 2020 m. rugpjūčio 17 d., https://www.androidauthority.com/what-is-sms-280988/.
709. Suzanne Choney, „How Long Do Wireless Carriers Keep Your Data?“, *NBC News*, žiūrėta 2020 m. rugpjūčio 17 d., http://www.nbcnews.com/technolog/how-long-do-wireless-carriers-keep-your-data-120367.
710. „Smash It, Shred It, Wipe It: The Tom Brady Guide to Destroying Text Messages“, *The Guardian*, 2015., http://www.theguardian.com/technology/2015/jul/29/tom-brady-deflategate-destroy-text-messages-cellphone.
711. „Privatumas“, *Telia*, žiūrėta 2020 m. rugsėjo 9 d., https://www.telia.lt/privatumo-politika.

712. „Klientų duomenų tvarkymo bei privatumo politika“, *Tele2*, žiūrėta 2020 m. rugsėjo 9 d., https://tele2.lt/privatiems/apie-tele2/privatumo-politika. „Privatumo ir slapukų politika“, *Bitė Lietuva*, žiūrėta 2020 m. rugsėjo 9 d., https://www.bite.lt/privatumo-ir-slapuku-politika.
713. „Privacy – Government Information Requests – Apple (LT)“, *Apple Legal*, žiūrėta 2020 m. rugpjūčio 22 d., https://www.apple.com/legal/transparency/lt.html.
714. „Apple Emergency Government / Law Enforcement Information Request“, *Apple Inc.*, žiūrėta 2020 m. rugpjūčio 22 d., https://www.apple.com/legal/privacy/le-emergencyrequest.pdf .
715. „Requests For User Data“, *Facebook Inc.,* žiūrėta 2020 m. rugpjūčio 22 d., https://transparency.facebook.com/government-data-requests/country/LT.
716. „Naudotojų Informacijos Užklausos – „Google“ Skaidrumo Ataskaita“, *Google Inc.*, žiūrėta 2020 m. rugpjūčio 22 d., https://transparencyreport.google.com/user-data/overview?legal_process_breakdown=expanded:1,2&lu=legal_process_breakdown.
717. „Law Enforcement Requests Report – Microsoft CSR“, *Microsoft Inc.*, žiūrėta 2020 m. rugpjūčio 22 d., https://www.microsoft.com/en-us/corporate-responsibility/lerr.
718. Jonathan Strickland, „How IP Convergence Works“, *HowStuffWorks*, žiūrėta 2020 m. rugpjūčio 22 d., https://computer.howstuffworks.com/ip-convergence.htm.
719. Sara Morrison, „The Police Want Your Phone Data. Here's What They Can Get — and What They Can't“, *Vox*, 2020, žiūrėta 2020 m. rugpjūčio 23 d., https://www.vox.com/recode/2020/2/24/21133600/police-fbi-phone-search-protests-password-rights.
720. David L. Carter, „Law Enforcement Intelligence Operations. Concept, issues, terms“, Michigan State University, 1990, 23, žiūrėta 2020 m. rugpjūčio 22 d., https://www.ncjrs.gov/pdffiles1/Photocopy/134434NCJRS.pdf.
721. „Stabdomos itin plačias teises kriminalinei žvalgybai suteikiančios įstatymo pataisos“, *Lietuvos rytas*, žiūrėta 2020 m. rugpjūčio 22 d., https://lietuvos-diena.lrytas.lt/aktualijos/2017/06/21/news/stabdomos-itin-placias-teises-kriminalinei-zvalgybai-suteikiancios-istatymo-pataisos-1740598/.
722. Victor Immanuel Oloo, „Here's What Your Phone Knows about You“, *Dignited*, 2019, žiūrėta 2020 m. rugpjūčio 22 d., https://www.dignited.com/49959/heres-what-your-phone-knows-about-you/.
723. Pierluigi Paganini, „Ennetcom – Dutch Police confirmed to have decrypted BlackBerry PGP messages in a criminal case“, *Security Affairs*, žiūrėta 2020 m. rugpjūčio 22 d., https://securityaffairs.co/wordpress/57036/cyber-crime/blackberry-pgp-messages.html .
724. Pierluigi Paganini, „Hacking a network, using an 'invisibility cloak' – Is it that simple?“, *Security Affairs*, žiūrėta 2020 m. rugpjūčio 22 d., https://securityaffairs.co/wordpress/99465/hacking/hacking-a-network-invisibility-cloak.html.

725. „On Lawful Criminal Investigation That Respects 21st Century Data Protection – Europol and ENISA Joint Statement“, *Europol*, žiūrėta 2020 m. rugpjūčio 22 d., https://www.europol.europa.eu/publications-documents/lawful-criminal-investigation-respects-21st-century-data-protection-europol-and-enisa-joint-statement-0 .
726. Gideon Lichfield, „Inside the Race to Build the Best Quantum Computer on Earth“, *MIT Technology Review*, žiūrėta 2020 m. rugpjūčio 22 d., https://www.technologyreview.com/2020/02/26/916744/quantum-computer-race-ibm-google/.
727. „Man Behind Silk Road Website Is Convicted on All Counts“, *The New York Times*, žiūrėta 2020 m. rugsėjo 9 d., https://www.nytimes.com/2015/02/05/nyregion/man-behind-silk-road-website-is-convicted-on-all-counts.html. Alice Salles, „Silk Road Case Sets Dangerous Precedents“, 2016, žiūrėta 2020 m. rugpjūčio 22 d., https://fee.org/articles/silk-road-case-sets-dangerous-precedents/.
728. „On Lawful Criminal Investigation That Respects 21st Century Data Protection – Europol and ENISA Joint Statement“, *Europol*, žiūrėta 2020 m. rugpjūčio 22 d., https://www.europol.europa.eu/publications-documents/lawful-criminal-investigation-respects-21st-century-data-protection-europol-and-enisa-joint-statement-0 .
729. „Kenkėjiškos programinės įrangos tipai“, *Esaugumas*, žiūrėta 2020 m. rugpjūčio 22 d., https://www.esaugumas.lt/lt/kompiuteriu-virusai/kenkejiskos-programines-irangos-tipai/92
730. Kim Zetter, „Hackers Can Control Your Phone Using a Tool That's Already Built Into It“, *WIRED*, žiūrėta 2020 m. rugpjūčio 22 d., https://www.wired.com/2014/07/hackers-can-control-your-phone-using-a-tool-thats-already-built-into-it/.
731. „Tarptautinės policijos operacijos“, *Lietuvos policija*, žiūrėta 2020 m. rugpjūčio 22 d., https://policija.lrv.lt/lt/veiklos-sritys/nusikalstamu-veiklu-atskleidimas-ir-tyrimas/tarptautines-policijos-operacijos.
732. „Individuals Designated as Eligible to Serve as an Amicus Curiae Pursuant to 50 U.S.C. § 1803(i)(1)“, *US Courts*, žiūrėta 2020 m. rugpjūčio 22 d., https://www.fisc.uscourts.gov/amici-curiae.
733. Pierluigi Paganini, „Ennetcom – Dutch Police confirmed to have decrypted BlackBerry PGP messages in a criminal case“, *Security Affairs*, žiūrėta 2020 m. rugpjūčio 22 d., https://securityaffairs.co/wordpress/57036/cyber-crime/blackberry-pgp-messages.html.
734. „Pay No Attention to That Man Behind the Curtain – Exposing and Challenging Government Hacking for Surveillance, žiūrėta 2020 m. rugsėjo 9 d., https://privacyinternational.org/sites/default/files/2018-06/Pay%20No%20Attention%20to%20That%20Man%20Behind%20the%20Curtain%20-%20Exposing%20and%20Challenging%20Government%20Hacking%20for%20Surveillance.pdf .
735. Colin Neagle, „Smart Refrigerator Hack Exposes Gmail Account Credentials“, *Network World*, , 2015, žiūrėta 2020 m. rugpjūčio 22 d., https://www.

networkworld.com/article/2976270/smart-refrigerator-hack-exposes-gmail-login-credentials.html.
736. „‚Bulk hacking' by UK spy agencies is illegal, high court told", *The Guardian*, žiūrėta 2020 m. rugpjūčio 22 d., https://www.theguardian.com/technology/2019/jun/17/liberty-mounts-latest-court-challenge-to-snoopers-charter-mi5-gchq.
737. Natasha Lomas, „UK faces Human Rights challenge to state's bulk hacking abroad", *TechRunch*, žiūrėta 2020 m. rugpjūčio 22 d., https://techcrunch.com/2016/08/08/uk-faces-human-rights-challenge-to-states-bulk-hacking-abroad/
738. „MI5's use of personal data was ‚unlawful', says watchdog", *BBC News*, žiūrėta 2020 m. rugpjūčio 22 d., https://www.bbc.com/news/uk-48597111.
739. „Ethical Hacking: How To Hack A Web Server", *Infosec Resources*, žiūrėta 2020 m. rugpjūčio 22 d., https://resources.infosecinstitute.com/category/certifications-training/ethical-hacking/attacking-web-servers-and-applications/#gref.
740. „Internet and Jurisdiction Policy Network", žiūrėta 2020 m. rugpjūčio 22 d. https://www.internetjurisdiction.net/.
741. „Lietuvos kariuomenės Specialiųjų operacijų pajėgos", Lietuvos Respublikos krašto apsaugos ministerija, žiūrėta 2020 m. rugpjūčio 24 d., https://kariuomene.kam.lt/lt/kariuomenes_struktura/specialiuju_operaciju_pajegos/sop_struktura.html.
742. „Antrasis operatyvinių tarnybų departamentas", *Lietuvos Respublikos krašto apsaugos ministerija*, žiūrėta 2020 m. rugpjūčio 22 d., https://kam.lt/lt/struktura_ir_kontaktai_563/kas_institucijos_567/aotd.html.
743. „Kriminalinė žvalgyba", *Lietuvos Respublikos prokuratūra*, žiūrėta 2020 m. rugpjūčio 22 d., https://www.prokuraturos.lt/lt/veiklos-sritys/baudziamasis-persekiojimas/kriminaline-zvalgyba/186.
744. „How the US Spy Scandal Unravelled", *BBC News*, 2014, žiūrėta 2020 m. rugsėjo 9 d., https://www.bbc.com/news/world-us-canada-23123964.
745. Graham Smith, „Illuminating the Investigatory Powers Act", *Cyberleagle*, žiūrėta 2020 m. rugpjūčio 22 d., http://www.cyberleagle.com/2018/02/illuminating-investigatory-powers-act.html?utm_source=feedburner&utm_medium=email&utm_campaign=Feed%3A+Cyberleagle+%28Cyberleagle%29.
746. „Electronic Surveillance – an Overview", *ScienceDirect*, žiūrėta 2020 m. rugsėjo 9 d., https://www.sciencedirect.com/topics/computer-science/electronic-surveillance.
747. „Open-Source Intelligence", *Wikipedia*, žiūrėta 2020 m. rugpjūčio 22 d., https://en.wikipedia.org/w/index.php?title=Open-source_intelligence&oldid=970364598.
748. „Human Intelligence (Intelligence Gathering)", *Wikipedia*, žiūrėta 2020 m. rugpjūčio 22 d., https://en.wikipedia.org/w/index.php?title=Human_intelligence_(intelligence_gathering)&oldid=965753709.
749. "Mokymai „Atvirųjų šaltinių žvalgyba", *NRD Cyber Security*, žiūrėta 2020 m. rugpjūčio 22 d., https://www.nrdcs.lt/lt/Renginiai/-mokymai-atviruju-saltiniu-zvalgyba-/61.

750. „Swiss Approve New Surveillance Law“, *BBC News*, 2016, žiūrėta 2020 m. rugpjūčio 23 d., https://www.bbc.com/news/world-europe-37465853.
751. „National Security versus Global Security“, *United Nations*, žiūrėta 2020 m. rugpjūčio 23 d., https://www.un.org/en/chronicle/article/national-security-versus-global-security.
752. David C. Rapoport, „The Four Waves of Rebel Terror and September 11“, *Anthropoetics*, 8, Nr. 1 (2002), žiūrėta 2020 m. rugpjūčio 23 d., http://anthropoetics.ucla.edu/ap0801/terror/.
753. „Terrorism and Assassination“, *Oxford Reference*, žiūrėta 2020 m. rugsėjo 9 d., https://www.oxfordreference.com/view/10.1093/acref/9780191737190.timeline.0001.
754. Tim Greene, „NSA Asks Silicon Valley to Help Fight Cybercrime, Terrorism“, *Network World*, 2016, žiūrėta 2020 m. rugpjūčio 23 d., http://www.networkworld.com/article/3040175/security/nsa-asks-silicon-valley-to-help-fight-cybercrime-terrorism.html.
755. „U.S. Says It Has Unlocked IPhone Without Apple“, *The New York Times*, žiūrėta 2020 m. rugsėjo 9 d., https://www.nytimes.com/2016/03/29/technology/apple-iphone-fbi-justice-department-case.html.
756. Sari Horwitz, Shyamantha Asokan ir Julie Tate, „Trade in Surveillance Technology Raises Worries“, *Washington Post*, 2011, žiūrėta 2020 m. rugpjūčio 23 d., https://www.washingtonpost.com/world/national-security/trade-in-surveillance-technology-raises-worries/2011/11/22/gIQAFFZOGO_story.html?utm_term=.f1d6995119ae.
757. Garrett Hinck, „Wassenaar Export Controls on Surveillance Tools: New Exemptions for Vulnerability Research“, *LawFare*, žiūrėta 2020 m. rugpjūčio 23 d., https://www.lawfareblog.com/wassenaar-export-controls-surveillance-tools-new-exemptions-vulnerability-research.
758. „List of Weapons of Mass Destruction Treaties“, i*Wikipedia*, žiūrėta 2020 m. rugsėjo 9 d., https://en.wikipedia.org/w/index.php?title=List_of_weapons_of_mass_destruction_treaties&oldid=946037660.
759. „Huawei Security Scandal: Everything You Need to Know“, *Forbes*, žiūrėta 2020 m. rugsėjo 9 d., https://www.forbes.com/sites/kateoflahertyuk/2019/02/26/huawei-security-scandal-everything-you-need-to-know/#7e440b1673a5.
760. Patricia Moloney Figliola, „Digital Surveillance: The Communications Assistance for Law Enforcement Act“, 17, žiūrėta 2020 m. rugpjūčio 23 d. https://fas.org/sgp/crs/intel/RL30677.pdf.
761. „FAQ on the CALEA Expansion by the FCC“, *Electronic Frontier Foundation*, 2007, žiūrėta 2020 m. rugpjūčio 23 d., https://www.eff.org/pages/calea-faq.
762. „FCC Adopts CALEA Technical Standards“, *Federal Communications Commission*, žiūrėta 2020 m. rugpjūčio 23 d., https://transition.fcc.gov/Bureaus/Engineering_Technology/News_Releases/1999/nret9003.html
763. „Communications Assistance for Law Enforcement Act (CALEA)“, *TiaOnline*, žiūrėta 2020 m. rugpjūčio 23 d., http://standards.tiaonline.org/standards/technology/calea/index.cfm.

764. „CALEA Flexible Deployment Assistance Guide“, *TiaOnline*, žiūrėta 2020 m. rugpjūčio 23 d., http://standards.tiaonline.org/standards/technology/calea/documents/flexgide2.pdf .
765. Patricia Moloney Figliola, „Digital Surveillance: The Communications Assistance for Law Enforcement Act“, 6, žiūrėta 2020 m. rugpjūčio 23 d. https://fas.org/sgp/crs/intel/RL30677.pdf.
766. „Communications Assistance for Law Enforcement Act“, *Wikipedia*, žiūrėta 2020 m. rugsėjo 9 d., https://en.wikipedia.org/w/index.php?title=Communications_Assistance_for_Law_Enforcement_Act&oldid=949624418.
767. „FAQ on the CALEA Expansion by the FCC“, *Electronic Frontier Foundation*, žiūrėta 2020 m. rugpjūčio 23 d., https://www.eff.org/pages/calea-faq.
768. „CIA Front Companies“, žiūrėta 2020 m. rugpjūčio 23 d., http://www.jar2.com/2/Intel/CIA/CIA%20Fronts.htm Rodney Stich, *Explosive Secrets of Covert CIA Companies* (Silverpeak Enterprises, 2006).
769. Catherine Stupp, „EU agency asks Commission to 'avoid fragmentation' in new cyber security plans“, *Euractiv*, žiūrėta 2020 m. rugpjūčio 23 d., http://www.euractiv.com/section/cybersecurity/news/eu-agency-asks-commission-to-avoid-fragmentation-in-new-cybersecurity-plans/
770. „Privacy International launches the Surveillance Industry Index & New Accompanying Report“, *Privacy International*, žiūrėta 2020 m. rugpjūčio 23 d., https://privacyinternational.org/sites/default/files/global_surveillance.pdf.
771. „Privacy International's Briefing On The Data Protection Bill For The Committee Stage In The House of Lords“, *Privacy International*, žiūrėta 2020 m. rugpjūčio 23 d., http://www.privacyinternational.org/advocacy/656/privacy-internationals-briefing-data-protection-bill-committee-stage-house-lords.
772. „Africa Intelligence: Exclusive News on Africa“, žiūrėta 2020 m. rugpjūčio 23 d., https://www.africaintelligence.com/.
773. „Undermining Global Security: The European Union's Global Arms Exports“, *Amnesty International*, 2004, žiūrėta 2020 m. rugpjūčio 23 d., http://www.amnesty.eu/static/documents/Text_ACT300032004.pdf .
774. „Our Reseach“, *Defense Advanced Research Projects Agency*, žiūrėta 2020 m. rugpjūčio 23 d., https://www.darpa.mil/our-research.
775. „Defense Advanced Research Projects Agency“, žiūrėta 2020 m. rugpjūčio 23 d., https://www.darpa.mil/.
776. Evan Andrews, „Who Invented the Internet?“, Corbis, žiūrėta 2020 m. rugpjūčio 23 d., https://www.history.com/news/who-invented-the-internet.
777. „Total Information Awareness (TIA) System“, *Defense Advanced Research Projects Agency,* žiūrėta 2020 m. rugpjūčio 23 d., https://web.archive.org/web/20021003053651/http://www.darpa.mil/iao/tiasystems.htm.
778. „More about Department of Defense/NSA Spying“, *ACLU*, žiūrėta 2020 m. rugpjūčio 23 d., https://www.aclu.org/other/more-about-department-defensen-sa-spying

779. „Overview of the Information Awareness Office“, *Defense Advanced Research Projects Agency*, žiūrėta 2020 m. rugpjūčio 23 d., https://fas.org/irp/agency/dod/poindexter.html.
780. „Report to Congress Regarding the Terrorism Information Awareness Program: In response to Consolidated Appropriations Resolution“, 2003, žiūrėta 2020 m. rugpjūčio 23 d., https://epic.org/privacy/profiling/tia/may03_report.pdf.
781. Shane Harris, „TIA Lives On“, *National Journal*, 2016, žiūrėta 2020 m. rugpjūčio 23 d., http://shaneharris.com/magazinestories/tia-lives-on/.
782. Mayle, Adam ir Knott, Alex, „Outsourcing Big Brother: Office of Total Information Awareness relies on private sector to track Americans“, *The Center for Public Integrity*, žiūrėta 2020 m. rugpjūčio 23 d., https://publicintegrity.org/2002/12/17/3164/outsourcing-big-brother.
783. Amos Y. Johnson ir kt., „Human Identification at a Distance“, *Georgia Institute of Technology College of Computing*, žiūrėta 2020 m. rugpjūčio 23 d., https://www.cc.gatech.edu/cpl/projects/hid/.
784. Chris Jones, „The visible hand: the European Union's Security Industrial Policy“, *Statewatch*, 2016, 12, žiūrėta 2020 m. rugpjūčio 23 d., http://www.statewatch.org/analyses/no-297-security-industrial-policy.pdf .
785. „European Network of Law Enforcement Technology Services“, žiūrėta 2020 m. rugpjūčio 23 d., http://www.enlets.eu/.
786. „Intelligent Information System Supporting Observation, Searching and Detection for Security of Citizens in Urban Environment“, *CORDIS*, žiūrėta 2020 m. rugpjūčio 23 d., https://cordis.europa.eu/project/id/218086.
787. Ian Johnston, "EU Funding 'Orwellian' Artificial Intelligence Plan to Monitor Public for 'Abnormal Behaviour'", 2009, žiūrėta 2020 m. rugpjūčio 23 d., https://www.telegraph.co.uk/news/uknews/6210255/EU-funding-Orwellian-artificial-intelligence-plan-to-monitor-public-for-abnormal-behaviour.html.
788. „EU funding ‚Orwellian' artificial intelligence plan to monitor public for „abnormal behaviour“, PrivacyFirst, žiūrėta 2020 m. rugpjūčio 23 d., https://www.privacyfirst.eu/images/stories/PDFs/Telegraph20090919_EU-funding-Orwel.pdf .
789. Alexander Alvaro ir kt., „Written Declaration pursuant to Rule 123 of the Rules of Procedure on INDECT (intelligent information system supporting observation, searching and detection for security of citizens in urban environment)“, *European Parlament*, žiūrėta 2020 m. rugpjūčio 23 d. http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+WDECL+P7-DCL-2010-0082+0+DOC+PDF+V0//EN&language=EN . „Parliamentary questions“, *European Parlament*, žiūrėta 2020 m. rugpjūčio 23 d., https://www.europarl.europa.eu/sides/getAllAnswers.do?reference=E-2010-7521&language=EN.
790. „Parliamentary questions“, *European Parlament*, žiūrėta 2020 m. rugpjūčio 23 d., http://www.europarl.europa.eu/sides/getAllAnswers.do?reference=E-2010-6912&language=EN
791. „Valstybės užsakymai“, Lietuvos mokslo taryba, žiūrėta 2020 m. rugpjūčio 23 d., https://www.lmt.lt/lt/mokslo-finansavimas/vykdytos-mokslo-finansavimo-priemones/valstybes-uzsakymai/2295.

792. „Mokslinių tyrimų ir eksperimentinės plėtros paslaugų pirkimų vykdymo tvarkos aprašas, patvirtintas Lietuvos Respublikos Vyriausybės 2020 m. sausio 15 d. nutarimu Nr. 22“, *eSeimas,* žiūrėta 2020 m. rugpjūčio 23 d., https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/48ae1cf0391811eabd71c05e81f09716?jfwid=mmceokxwi.
793. Chris Jones, „The visible hand: the European Union's Security Industrial Policy“, *Statewatch*, 2016, 13, žiūrėta 2020 m. rugpjūčio 23 d., http://www.statewatch.org/analyses/no-297-security-industrial-policy.pdf .
794. „The SBIR and STTR Programs“, *America's Seed Fund*, žiūrėta 2020 m. rugpjūčio 23 d., https://www.sbir.gov/about/about-sbir .
795. „Three-Phase Program“, *America's Seed Fund*, žiūrėta 2020 m. rugpjūčio 23 d., https://sbir.nih.gov/about/three-phase-program
796. „The leading nonprofit defending digital privacy, free speech, and innovation for 30 years and counting!“, *Electronic Frontier Foundation*, žiūrėta 2020 m. rugpjūčio 23 d., https://w2.eff.org/Privacy/TIA/TIA-report.pdf .
797. „The SBIR and STTR Programs“, *America's Seed Fund*, žiūrėta 2020 m. rugpjūčio 23 d., https://www.sbir.gov/about/about-sbir .
798. „Silicon Valley Innovation Program“, *U. S. Department of Homeland Security,* žiūrėta 2020 m. rugpjūčio 23 d., https://www.dhs.gov/science-and-technology/hsip.
799. Ikiprekybinis pirkimas „Nacionalinė informacinio poveikio atpažinimo ir analizės ekosistema (NAAS)“, plačiau žr. http://www.lka.lt/lt/moksline-veikla/mokslo-projektine-veikla/naas.html.
800. „V. Putino patarėjas: Rusija pasirengusi atsijungti nuo tarptautinio interneto“, *DELFI,* žiūrėta 2020 m. rugpjūčio 23 d., https://www.delfi.lt/mokslas/technologijos/v-putino-patarejas-rusija-pasirengusi-atsijungti-nuo-tarptautinio-interneto.d?id=77336711.
801. „Russia may end cooperation with European Court of Human Rights: RIA“, *Reuters*, 2018, žiūrėta 2020 m. rugpjūčio 23 d., https://www.reuters.com/article/us-russia-court-echr-withdrawal/russia-may-end-cooperation-with-european-court-of-human-rights-ria-idUSKCN1GD47U
802. „The "State of Play" of Human Rights Due Diligence Anticipating the next five years“, *Institute for Human Rights and Business,* žiūrėta 2020 m. rugpjūčio 23 d., https://www.ihrb.org/pdf/The_State_of_Play_of_Human_Rights_Due_Diligence.pdf.
803. Simon Kuper, „Edward Snowden and the Millennial Conscience“, *The Financial Times*, 2019, žiūrėta 2020 m. rugsėjo 7 d., https://medium.com/financial-times/edward-snowden-and-the-millennial-conscience-e399803e8323.
804. Michel Regnier, „The 'Moment of Truth' for the Data Retention Directive: EDPS Demands Clear Evidence of Necessity“, *European Data Protection Supervisor,* 2017, žiūrėta 2020 m. rugpjūčio 17 d., https://edps.europa.eu/press-publications/press-news/press-releases/2010/moment-truth-data-retention-directive-edps-demands_en.
805. Michael J. McCarthy, „Electronic Form of 'Invisible Ink' Inside Files May Reveal Secrets“, *Wall Street Journal*, 2000, žiūrėta 2020 m. rugpjūčio 17 d., https://www.wsj.com/articles/SB972002214791170991.

MYKOLO ROMERIO UNIVERSITETAS

Sigutė Stankevičiūtė

ASMENS DUOMENŲ RINKIMO ELEKTRONINĖJE ERDVĖJE TEISĖSAUGOS IR ŽVALGYBOS TIKSLAIS REGLAMENTAVIMAS

Daktaro disertacijos santrauka
Socialiniai mokslai, teisė (S 001)

Vilnius, 2020

Daktaro disertacija rengta 2013–2019 metais Mykolo Romerio universitete, ginama Mykolo Romerio universitete pagal Mykolo Romerio universitetui su Vytauto Didžiojo universitetu Lietuvos Respublikos švietimo, mokslo ir sporto ministro 2019 m. vasario 22 d. įsakymu Nr. V-160 „Dėl doktorantūros teisės suteikimo“ suteiktą doktorantūros teisę.

Mokslinis vadovas:
Prof. dr. Vidmantas Egidijus Kurapka (Mykolo Romerio universitetas, socialiniai mokslai, teisė, S 001).

Daktaro disertacija ginama Mykolo Romerio universiteto ir Vytauto Didžiojo universiteto teisės mokslo krypties taryboje:

Pirmininkė:
prof. dr. Regina Valutytė (Mykolo Romerio universitetas, socialiniai mokslai, teisė, S 001).

Nariai:
prof. dr. Paolo Balboni (Mastrichto universitetas, Nyderlandų Karalystė, socialiniai mokslai, teisė, S 001);
prof. dr. Aurelijus Gutauskas (Vilniaus universitetas, socialiniai mokslai, teisė, S 001);
prof. dr. Raimundas Jurka (Mykolo Romerio universitetas, socialiniai mokslai, teisė, S 001);
prof. dr. Darius Štitilis (Mykolo Romerio universitetas, socialiniai mokslai, teisė, S 001).

Daktaro disertacija bus ginama viešame teisės mokslo krypties tarybos posėdyje 2020 m. gruodžio 21 d. 10 val. Mykolo Romerio universitete, I-414 aud.
Adresas: Ateities g. 20, Vilnius.

Daktaro disertacijos santrauka išsiųsta 2020 m. lapkričio 20 d.

Daktaro disertaciją galima peržiūrėti Lietuvos nacionalinėje Martyno Mažvydo bibliotekoje (Gedimino pr. 51, Vilnius) bei Mykolo Romerio universiteto bibliotekoje (Ateities g. 20, Vilnius) ir Vytauto Didžiojo universiteto bibliotekoje (K. Donelaičio g. 52, Kaunas).

Sigutė Stankevičiūtė

ASMENS DUOMENŲ RINKIMO ELEKTRONINĖJE ERDVĖJE TEISĖSAUGOS IR ŽVALGYBOS TIKSLAIS REGLAMENTAVIMAS

SANTRAUKA

Temos aktualumas. Elektroninė erdvė buvo sukurta siekiant dalintis duomenimis[1], ne juos saugoti[2]. Kas tada turėtų asmens duomenis saugoti? Asmens duomenų šaltinis – žmogus – neturi galimybių apsaugoti savo duomenų, kadangi jų valdytojais yra paslaugas el. erdvėje teikiantys juridiniai asmenys, o naudotojais – ne tik pats paslaugų teikėjas, bet ir kiti juridiniai asmenys, teisėsaugos ir žvalgybos institucijos. Teiginys, kad asmens duomenys yra XXI a. nafta[3] yra vartojamas dažnai. Tačiau, jeigu paklaustumėme visuomenės kaip mūsų asmens duomenys generuoja paslaugas elektroninėje erdvėje teikiančioms įmonėms pelną, didesnį už valstybių nacionalinius biudžetus[4], paaiškinimo iš statistinio, išsilavinimo šioje srityje neturinčio ir joje nedirbančio, asmens negautumėme. Nors dėka Europos Sąjungos (toliau – ES) asmens duomenų apsaugos reformos, dalis asmenų žino, kad jie turi teisę į asmens duomenų apsaugą. Tačiau priešprieša šiam žinojimui yra teiginys „aš neturiu ko slėpti“. Todėl visuomenei susidaro įspūdis, kad iš el. erdvės tapimo kiekvieno iš mūsų gyvenimo neatsiejama dalimi, nauda ir tenka tik mums patiems, nes gauname paslaugas, o įsigaliojus Bendrajam asmens duomenų reglamentui dar ir galime kontroliuoti savo asmens duomenų judėjimą[5]. Iš tikrųjų dėl mūsų naudojimosi el. erdve nauda tenka tiek mums paslaugas teikiančioms įvairių sričių įmonėms (elektroninių ryšių tiekėjai, socialinių tinklų teikėjai, mobiliųjų įrenginių kūrėjai, reklamos paslaugų teikėjai ir kt.) ir valstybinėms institucijoms. JAV kurdama internetą neplanavo, jog civilis jo panaudojimas sugražins prie jo kūrimo ištakų – el. erdvės naudojimo nacionalinio saugumo užtikrinimo tikslais. Pastarųjų metų asmens duomenų nutekinimo skandalai JAV[6], noras vykdyti masinį asmenų stebėjimą

[1] Elektroninė erdvė yra JAV užsakymu vykdytų mokslinių tyrimų kariniais tikslais rezultatas šiandien visuomenės plačiai naudojamas dėl to, kad JAV mokslinių tyrimų rezultatus išslaptino, o verslo subjektai rado būdą kaip iš el. erdvės gauti pelną ją pritaikant visuomenės poreikiams. Plačiau apie tai žr. https://www.history.com/news/who-invented-the-internet.

[2] John R. Vacca, *Computer and Information Security Handbook* (Morgan Kaufmann, 2009), 4.

[3] „The World's Most Valuable Resource Is No Longer Oil, but Data“, *The Economist*, žiūrėta 2020 m. rugpjūčio 30 d., https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data.

[4] Milan Babic, Jan Fichtner ir Eelke M. Heemskerk, „States versus Corporations: Rethinking the Power of Business in International Politics“, *The International Spectator* 52, no. 4 (2017): 20–43, doi:10.1080/03932729.2017.1389151. Darius Mikutavičius, „„Microsoft“ vertė pirmą kartą pasiekė trilijono dolerių ribą“, *lrt.lt*, žiūrėta 2020 m. rugpjūčio 30 d., https://www.lrt.lt/naujienos/mokslas-ir-it/11/1052527/microsoft-verte-pirma-karta-pasieke-trilijono-doleriu-riba.

[5] „What Are the Advantages of the Internet?“, *Computer Hope*, žiūrėta 2020 m. rugpjūčio 30 d., https://www.computerhope.com/issues/ch001808.htm.

[6] „NSA Collecting Phone Records of Millions of Verizon Customers Daily“, *The Guardian*, žiūrėta 2020 m. rugpjūčio 30 d., https://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order.

kovos su COVID-19 tikslais[7] rodo, kad nauda valstybėms iš masinio asmenų naudojimosi el. erdve pasireiškia per masinį asmens duomenų naudojimą ne tik verslo, bet ir valstybės poreikių tenkinimui, dažniausiai teisėsaugos ir žvalgybos tikslais. Taigi, kas turėtų saugoti mūsų asmens duomenis, jei pati el. erdvė to nedaro? Vienas iš apsaugos mechanizmų turėtų būti teisinis reglamentavimas.

Teisės į asmens duomenų apsaugą galiojimu teisėsaugos ir žvalgybos institucijoms asmens duomenis renkant elektroninėje erdvėje klausimu pradėjau domėtis daugiau nei metams likus E. Snowden informacijos apie masinį asmens duomenų rinkimą nutekinimo. Praėjo septyni metai, tačiau ši tema iki šiol išliko aktuali, kadangi ji liečia du lygiaverčius visuomenės interesus – žmogaus teisės į asmens duomenų apsaugą užtikrinimą elektroninėje erdvėje ir tos teisės atsisakymo, iš pirmo žvilgsnio, vardan apsaugos nuo dar didesnės grėsmės – terorizmo, nusikalstamumo ir pavojaus nacionaliniam saugumui. Tačiau riba tarp teisių suvaržymo vardan didesnių vertybių apsaugos nepažeidžiant pačios didžiausios vertybės – demokratijos – yra labai trapi. Tokius mokslininkų nuogąstavimus galime pamatyti pvz. profesorės, JAV elektroninės žvalgybos teismo patariamojo organo Amici Curia narės L. K. Donohue knygoje, kurioje autorė iškelia hipotezę, kad JAV vykdomas masinis asmens duomenų rinkimas elektroninėje erdvėje yra analogiškas XIII a. galiojusiai antikonstitucine pripažintai teisei Karūnos įgaliotiems asmenims bent kada įsibrauti į bent kurio iš Didžiosios Britanijos valdose esančio asmens namus[8]. Nepaisant mokslininkų ir visuomeninių judėjimų nuo 2013 m. akcentuojamos grėsmės teisės asmens duomenų apsaugą užtikrinime šiuos duomenis teisėsaugos ir žvalgybos institucijoms renkant el. erdvėje, esminių pokyčių teisės aktuose kol kas neįvyko.

Šiuo metu egzistuoja du demokratijos užtikrinimo teisėsaugos ir žvalgybos institucijoms renkant asmens duomenis el. erdvėje užtikrinimo mechanizmai, pasireiškiantys teisės į asmens duomenų apsaugą suteikimu arba išsamiu asmens duomenų rinkimo elektroninėje erdvėje teisėsaugos ir žvalgybos tikslais reglamentavimu. Pirmasis modelis yra taikomas Europoje, antrasis – JAV. Pirmasis – Europos modelis – pasižymi tuo, kad asmeniui įtvirtinama teisė į asmens duomenų apsaugą, tačiau asmens duomenų rinkimas teisėsaugos ir žvalgybos tikslais teisės aktuose yra reglamentuojamas padrikai. Antrasis – JAV modelis – pasižymi tuo, kad teisė į asmens duomenų apsaugą, kaip tokia, nėra tiesiogiai suteikiama, tačiau asmens duomenų rinkimas elektroninėje erdvėje teisėsaugos ir žvalgybos tikslais yra detaliai reglamentuojamas specialiais įstatymais, bei yra įsteigti specialūs teismai teisėsaugos ir žvalgybos asmens duomenų rinkimo elektroninėje erdvėje prašymų sankcionavimui ir su tuo susijusių bylų nagrinėjimui. Kadangi JAV ir Europos supranacionalinis asmens duomenų rinkimo el. erdvėje teisėsaugos ir žvalgybos tikslais reglamentavimas įtakoja viso likusio

[7] „9/11 Saw Much of Our Privacy Swept aside. Coronavirus Could End It Altogether", *CNN*, žiūrėta 2020 m. rugpjūčio 30 d., https://edition.cnn.com/2020/05/16/tech/surveillance-privacy-coronavirus-npw-intl/index.html.
„The Price Of Covid-19 Freedom May Be Eternal Spying", Bloomberg, žiūrėta 2020 m. rugpjūčio 30 d., https://www.bloombergquint.com/view/coronavirus-contact-tracing-apps-mean-spying-end-to-data-privacy.

[8] Laura K. Donohue, *The Future of Foreign Intelligence: Privacy and Surveillance in a Digital Age*, 1 edition (New York: Oxford University Press, 2016), 76.

pasaulio valstybių teisinius reglamentavimus, įskaitant Lietuvą, todėl JAV ir Europos supranacionalinės teisės teisinio reglamentavimo analizė yra disertacijos uždaviniais.

Ištirtumas. Asmens duomenų rinkimas el. erdvėje teisėsaugos ir žvalgybos tikslais mokslinių tyrimų objektu tapo dėl teisės į privatumą, vėliau peraugusios į teisę į asmens duomenų apsaugą, apimties išplėtimo iš fizinės aplinkos į el. erdvę. Klausimas kaip užtikrinti pusiausvyrą tarp teisėsaugos ir žvalgybos institucijų poreikio rinkti asmens duomenis el. erdvėje ir asmens teisės į asmens duomenų apsaugą įgyvendinimo yra dažnai keliamas[9], bet iki šiol neatsakytas. Kadangi informacija apie asmens duomenų rinkimą el. erdvėje teisėsaugos ir žvalgybos tikslais nėra viešai prieinama, todėl šios srities mokslinius tyrimus įtakoja keli faktoriai: mokslininko geografinė lokacija ir su asmens duomenų apsauga susiję viešai žinomi reikšmingi įvykiai. Europos mokslininkų susidomėjimui asmens duomenų apsauga žvalgybos ir teisėsaugos srityje įtaką darė į viešumą nutekinama informacija apie asmens duomenų rinkimo mastus ir vykdomas programas. Tai skatino ir įstatymų leidybos procesus. Pirmoji didesnio susidomėjimo banga buvo 2013 m. po buvusio JAV Nacionalinės žvalgybos agentūros (NSA) kontraktoriaus E. Snowden paviešintos informacijos apie PRISM programą[10]. Siekiant surasti asmens duomenų apsaugos būdus ir nustatyti *privacy by design* principo panaudojimo galimybes teisėsaugos veikloje buvo pradėti vykdyti keli EK finansuojami tarptautiniai Septintosios bendrosios programos mokslinių tyrimų projektai[11], atsirado mokslinių publikacijų, visų pirma Oksfordo ir Harvardo universitetų profesorių[12], apie teisinės asmens duomenų apsaugos reikšmę ir ypatybes, EK užsakymu jungtinė ES mokslininkų grupė parengė apžvalginę studiją apie privatumo apsaugą JAV[13]. Antroji didesnio susidomėjimo banga buvo Europos Sąjungos Teisingumo Teismui (toliau – ESTT) „Saugaus uosto" principą pripažinus neužtikrinančiu teisinės asmens duomenų apsaugos dėl JAV žvalgybos institucijų galimybės naudoti šiuos asmens duomenis[14]. Tuo metu dauguma mokslininkų analizavo teismo sprendimą ir tolimesnius

---

9 Jing Ran, „Striking the Balance between Privacy and Governance in the Age of Technology", 11 (2016): 20.

10 „NSA Collecting Phone Records of Millions of Verizon Customers Daily", *The Guardian*, žiūrėta 2020 m. rugpjūčio 30 d., https://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order.

11 „Supporting fundamental rights, PrIvacy and Ethics in surveillaNce Technologies", *Cordis*, žiūrėta 2020 m. rugpjūčio 30 d., https://cordis.europa.eu/project/id/261698.

12 Pvz., H Akın Ünver, „Politics of Digital Surveillance, National Security and Privacy", 23, žiūrėta 2020 m. rugpjūčio 30 d., https://edam.org.tr/wp-content/uploads/2018/04/Chrest_Surveillance2.pdf. Clive Norris ir kt., *The Unaccountable State of Surveillance: Exercising Access Rights in Europe*, Issues in Privacy and Data Protection (Springer International Publishing, 2017), doi:10.1007/978-3-319-47573-8. Aaron Nance, „Taking the Fear Out of Electronic Surveillance in the New Age of Terror Note", *UMKC Law Review* 70, Nr. 3 (2002 2001): 751–80. "Electronic Surveillance Recent Legislation", *Harvard Law Review* 122, no. 4 (2009 2008): 1271–78. David S. Kris, „The Rise and Fall of the FISA Wall Symposium – Spies, Secrets, and Security: The New Law of Intelligence: The Foreign Intelligence Surveillance Act", *Stanford Law & Policy Review* 17, no. 2 (2006): 487–530. Laura K. Donohue, „FISA Reform", *I/S: A Journal of Law and Policy for the Information Society* 10, no. 2 (2015 2014): 599–640. Stephen I. Vladeck, „The FISA Court and Article III Cybersurveillance in the Post-Snowden Age", *Washington and Lee Law Review* 72, no. 3 (2015): 1161–80. William C. Banks, „The Death of FISA Symposium – 9/11 Five Years On: A Look at the Global Response to Terrorism", *Minnesota Law Review* 91, no. 5 (2007 2006): 1209–1301.

13 Francesca Bignami, „The US legal system on data protection in the field of law enforcement. Safeguards, rights and remedies for EU citizens", *European Parlament*, žiūrėta 2020 m. rugsėjo 10 d., https://www.europarl.europa.eu/thinktank/en/document.html?reference=IPOL_STU(2015)519215.

14 Pvz. Dan Jerker B. Svantesson, „Cross-Border Data Transfers after the CJEU's Safe Harbour Decision: A Tale of Gordian Knots", *Alternative Law Journal* 41, no. 1 (2016): 39–42.

ES veiksmus. Nors, kaip matysime toliau disertacijoje, JAV žvalgybos institucijos teisiškai gali rinkti asmens duomenis net nesančius JAV, todėl „Saugaus uosto“ principo panaikinimas neišsprendžia tikrosios problemos. Tai rodo mokslinių tyrimų siaurumą ir platesnio pobūdžio tyrimų reikalingumą. Na ir trečioji mokslininkų domėjimosi asmens duomenų apsauga banga yra susijusi su 2018 m. ES asmens duomenų apsaugos reforma[15]. Tačiau dauguma trečiosios bangos mokslinių tyrimų yra susiję su komercine teisės į asmens duomenų apsauga puse, kurios įgyvendinimo nuostatos yra įtvirtintos Bendrajame asmens duomenų apsaugos reglamente[16]. Nepriklausomai nuo to, kuriai mokslinių tyrimų bangai priklauso, mokslininkai savo publikacijose analizuoja tik pavienius asmens teisės į asmens duomenų apsaugą žvalgybos ir teisėsaugos veikloje aspektus. Tačiau ši teisė ir jos apribojimo bei galiojimo mechanizmai yra kompleksiniai, todėl ir kompleksiniai tyrimai yra reikalingi.

Didžiausią dalį mokslinių publikacijų apie asmens duomenų rinkimą el. erdvėje teisėsaugos ir žvalgybos tikslais sudaro JAV teisės normų ir teismų precedentų analizė. Mokslinių publikacijų apie reglamentavimą JAV gausa gali būti paaiškinama tuo, kad JAV yra pirmoji pasaulio valstybė asmens duomenų rinkimą el. erdvėje pradėjusi reglamentuoti dar 1968 m., kuomet el. erdvė apėmė tik telefoninius pokalbius ir IV JAV Konstitucijos pataisa įtvirtintą teisę į privatumą iš fizinės aplinkos išplėtusi į el. erdvę. Tuo tarpu Europoje tai buvo padaryta tik 1981 m. ET priėmus Konvenciją dėl asmenų apsaugos ryšium su asmens duomenų automatizuotu tvarkymu, o ET Rekomendacijos dėl asmens duomenų tvarkymo policijos tikslais buvo paskelbtos 1987 m, t. y. 19 metų vėliau nei pirmasis tai reglamentuojantis teisės aktas JAV[17]. JAV tuo metu jau buvo sukurta visa asmens duomenų rinkimo el. erdvėje teisėsaugos ir žvalgybos tikslais teisinė bazė ir ji nuolat tobulinama iki šiol. Nuo pat atsiradimo 1968 m. JAV asmens duomenų rinkimą teisėsaugos ir žvalgybos tikslais reglamentuojantys teisės aktai dažnai buvo teisminių ginčų ir mokslinių diskusijų objektu. Todėl ir mokslinių tyrimų dėl JAV asmens duomenų rinkimo el. erdvėje teisėsaugos ir žvalgybos tikslais, paprastai, susijusiais su teismų sprendimais bylose, yra pakankamai daug. Tačiau JAV mokslininkų tyrimo objektu yra tai, kas svarbu JAV ir liečia JAV asmenų privatumo, ne Europos gyventojų apsaugą, todėl mokslininkai daugiausiai analizuoja Elektroninės komunikacijos privatumo akto (angl. *The Electronic Communications Privacy Act (ECPA)*) nuostatų taikymą[18].

---

[15] Pvz. Yi-Hsuan Chen, „EU Data Protection Law Reform: Challenges for Service Trade Liberalization and Possible Approaches for Harmonizing Privacy Standards into the Context of GATS, The“, *Spanish Yearbook of International Law* 19 (2015): 211–20. Marija Boban, „Digital Single Market and EU Data Protection Reform with Regard to the Processing of Personal Data as the Challenge of the Modern World The Legal Challenges of Modern World“, *Economic and Social Development, 16th International Scientific Conference on Economic and Social Development: The Legal Challenges of Modern World* 16 (2016): 191–201. Marina Skrinjar Vidovic, „EU Data Protection Reform: Challenges for Cloud Computing Notes“, *Croatian Yearbook of European Law and Policy* 12 (2016): 171–206.

[16] Julius Zaleskis, *Europos Sąjungos bendrasis duomenų apsaugos reglamentas ir asmens duomenų apsaugos teisė: monografija*, Teisinė literatūra (Vilnius: Registrų centras, 2019).

[17] „Council of Europe Committee of Ministers Recommendation No. R(87) 15 to the Member States on regulating the use of personal data in the police sector“, *Osce Polis*, žiūrėta 2020 m. rugsėjo 1 d., https://polis.osce.org/council-europe-committee-ministers-recommendation-no-r87-15-member-states-regulating-use-personal.

[18] Deirdre K. Mulligan, „Reasonable Expectations in Electronic Communications: A Critical Perspective on the Electronic Communications Privacy Act The Future of Internet Surveillance Law: A Symposium to Discuss Internet Surveil-

Užsienio žvalgybos elektroninėje erdvėje akto (angl. *Foreign Intelligence Surveillance Act (FISA)*) nuostatos yra analizuojamos, tačiau paprastai tik tiek, kiek tai liečia netiesioginį JAV asmenų asmens duomenų rinkimą el. erdvėje, renkant duomenis apie ne JAV asmenis[19]. Informacijos apie Vykdomosios valdžios nurodymą 12 333 (angl. *Executive Order 12 333*) yra itin mažai, mokslinių tyrimų šia tema – taip pat, nors, manoma, kad dabar Vykdomosios valdžios nurodymas (angl. *Executive Order 12 333*) gali būti pagrindinė teisinė masinio asmens duomenų rinkimo el. erdvėje priemonė[20]. Stanfordo universitetas 2013-2014 m. organizavo nuotolinius mokymus apie asmens duomenų rinkimą el. erdvėje teisėsaugos ir žvalgybos tikslais teisinį reglamentavimą JAV, kuriuose dalyvavo ir disertacijos autorė. 2015 m. Thomson Reuters leidykla išleido 2 dalių 2000 puslapių apimties knygą „*The Law of Electronic Surveillance*“[21]. Tai yra pirmoji JAV ir apskritai pasaulyje tokio pobūdžio knyga, kurioje unifikuotai apžvelgiamas teisinis JAV federalinio lygio asmens duomenų rinkimo el. erdvėje reglamentavimas. Tačiau kadangi šios knygos yra skirtos JAV rinkai, todėl ir mokslinis tyrimas yra atliekamas per JAV asmenų teisių apsaugos prizmę. Užsienio žvalgybos elektroninėje erdvėje teisės akto (angl. *Foreign Intelligence Surveillance Act*) nuostatos taikomos ne JAV asmenų atžvilgiu, knygoje apžvelgiamos labai siaurai, Vykdomosios valdžios nurodymas (angl. *Executive Order 12 333*) bei jo taikymo praktika arba asmens duomenų rinkimas vadovaujantis Baudžiamojo proceso kodekso 41 straipsniu, suteikiančiu teisę įsilaužti į bent kurioje pasaulio vietoje esančio bent kokios pilietybės asmens kompiuterį ar kitą įrenginį, iš viso nėra įtraukti į šios knygos turinį ir joje neminimi.

Asmens duomenų rinkimas el. erdvėje vyksta kitaip nei įprastinėje fizinėje aplinkoje. Renkant duomenis el. erdvėje yra neišvengiamas teisėsaugos ir žvalgybos institucijų bendradarbiavimas su verslo ir mokslo subjektais, nes duomenys, dažniausiai, yra renkami ne pačių teisėsaugos ir žvalgybos institucijų, o, jų nurodymu, el. ryšių paslaugų,

---

lance, Privacy & (and) the USA Patriot Act: Surveillance, Records & (and) Computers“, *George Washington Law Review* 72, no. 6 (2004 2003): 1557–98. Laura L. Clukey, „The Electronic Communications Privacy Act of 1986: The Impact on Software Communication Technologies Comment“, *Software Law Journal* 2, no. 2 (1988 1987): 243–64. Ariana R. Levinson, „Toward a Cohesive Interpretation of the Electronic Communications Privacy Act for the Electronic Monitoring of Employees“, *West Virginia Law Review* 114, no. 2 (2012 2011): 461–530. Robert A. Fiatal, „The Electronic Communications Privacy Act: Addressing Today's Technology (Part 1) Legal Digest“, *FBI Law Enforcement Bulletin* 57, no. 2 (1988): 25–30. Ariana R. Levinson, „Toward a Cohesive Interpretation of the Electronic Communications Privacy Act for the Electronic Monitoring of Employees“, *West Virginia Law Review* 114, no. 2 (2012 2011): 461–530.

[19] William C. Banks, „The Death of FISA Symposium – 9/11 Five Years On: A Look at the Global Response to Terrorism“, *Minnesota Law Review* 91, no. 5 (2007 2006): 1209–1301. David S. Kris, "The Rise and Fall of the FISA Wall Symposium – Spies, Secrets, and Security: The New Law of Intelligence: The Foreign Intelligence Surveillance Act“, *Stanford Law & Policy Review* 17, no. 2 (2006): 487–530.

[20] Mark Jaycox, „A Primer on Executive Order 12333: The Mass Surveillance Starlet“, *Electronic Frontier Foundation*, June 2, 2014, žiūrėta 2020 m. rugsėjo 1 d., https://www.eff.org/deeplinks/2014/06/primer-executive-order-12333-mass-surveillance-starlet. „Reagan-Era Order on Surveillance Violates Rights, Says Departing Aide“, *The New York Times*, žiūrėta 2020 m. rugsėjo 1 d., https://www.nytimes.com/2014/08/14/us/politics/reagan-era-order-on-surveillance-violates-rights-says-departing-aide.html. Barton Gellman ir Ashkan Soltani, „NSA Surveillance Program Reaches 'into the Past' to Retrieve, Replay Phone Calls“, *Washington Post*, March 18, 2014, sec. National Security, https://www.washingtonpost.com/world/national-security/nsa-surveillance-program-reaches-into-the-past-to-retrieve-replay-phone-calls/2014/03/18/226d2646-ade9-11e3-a49e-76adc9210f19_story.html.

[21] James Carr ir Patricia Bellia, *The Law of Electronic Surveillance, 2017-2 Ed.*, 1 dalis, (Clark Boardman Callaghan, 2017).

paslaugų el. erdvėje teikėjų, duomenų brokerių (angl. *data broker*) ar el. žvalgybos paslaugų teikėjų. Duomenų ir literatūros apie teisėsaugos ir žvalgybos institucijų bendradarbiavimą su privačiomis įmonėmis (verslo subjektais), jo formas ir pobūdį yra labai mažai. 2018 m. išleistoje knygoje „Habeas Data: Privacy vs. the Rise of Surveillance Tech" C. Farivar rašo apie tai, kaip įmonių kuriamos technologijos įtakoja žvalgybos pajėgumus[22]. Privacy international yra parengusi studiją apie augančią elektroninės žvalgybos paslaugų rinką[23]. Tačiau nė viename darbe nėra vertinamos teisėsaugos, žvalgybos ir verslo subjektų bendradarbiavimo formos ir asmens duomenų apsaugos galimybės bei teisinio reglamentavimo spragos. Atsakymui į šiuos klausimus nusprendžiau skirti paskutinį disertacijos skyrių, kadangi tokio bendradarbiavimo apimtys, pasak ENISA[24], didėja, o reglamentavimo ar bent koordinavimo šioje srityje kol kas nėra.

Lietuvoje mokslinės diskusijos apie asmens duomenų rinkimą el. erdvėje teisėsaugos ir žvalgybos tikslais taip pat yra keliamos. Paminėtini šie Lietuvos mokslininkai analizuojantys susijusias Lietuvos Respublikos kriminalinės žvalgybos įstatymo ir Baudžiamojo proceso kodekso (toliau – BPK) nuostatas: D. Štitilis[25], M. Laurinaitis[26], R. A. Petrauskas[27], R. Ažubalytė[28], G. Goda[29], A. Gutauskas[30], R. Jurka[31], L. Belevičiaus[32],

---

[22] Cyrus Farivar, *Habeas Data: Privacy vs. the Rise of Surveillance Tech* (Brooklyn: Melville House, 2018).

[23] „The Global Surveillance Industry", Privacy International, žiūrėta 2020 m. rugpjūčio 30 d., https://www.privacyinternational.org/sites/default/files/2017-12/global_surveillance_0.pdf.

[24] Catherine Stupp, „EU agency asks Commission to 'avoid fragmentation' in new cyber security plans", *Euractive*, žiūrėta 2020 m. rugsėjo 1 d., http://www.euractiv.com/section/cybersecurity/news/eu-agency-asks-commission-to-avoid-fragmentation-in-new-cybersecurity-plans/

[25] Darius Štitilis, „Elektroninių ryšių kontrolės nusikaltimų tyrimo tikslias teisiniai aspektai", *Informacijos mokslai : mokslo darbai* 34 (2005): 103–110. Rimantas Alfonsas Petrauskas ir Darius Štitilis, „Monitoring Electronic Communications: Privacy Issues", *Monitoring, Supervision and Information Technology : Proceedings of the First International Seminar of the Legal Framework for the Information Society (LEFIS) on Monitoring, Supervision and Information Technology, 15 June 2006, Rotterdam*, 2006, 5–20. Darius Štitilis ir Marius Laurinaitis, „IP telefonija – iššūkis elektroninių ryšių kontrolės, siekiant ištirti nusikaltimus, teisiniam reguliavimui", *Socialinių mokslų studijos*, no. 1 (2009): 205–221.

[26] Darius Štitilis ir Marius Laurinaitis, „IP telefonija – iššūkis elektroninių ryšių kontrolės, siekiant ištirti nusikaltimus, teisiniam reguliavimui", *Socialinių mokslų studijos*, no. 1 (2009): 205–221.

[27] Rimantas Alfonsas Petrauskas ir Darius Štitilis, „Monitoring Electronic Communications: Privacy Issues", *Monitoring, Supervision and Information Technology : Proceedings of the First International Seminar of the Legal Framework for the Information Society (LEFIS) on Monitoring, Supervision and Information Technology, 15 June 2006, Rotterdam*, 2006, 5–20.

[28] Rima Ažubalytė, „Privataus asmens gyvenimo ribojimas slaptomis priemonėmis: (ne)kokybiško įstatymo problema", *Jurisprudencija* 26, no. 2 (2019): 260–291, doi:10.13165/JUR-19-26-2-02. Rima Ažubalytė, „Baudžiamojo proceso principai: teisės spragų šalinimas", *Lietuvos Respublikos baudžiamojo proceso kodeksui – 10 metų : recenzuotų mokslinių straipsnių, skirtų Lietuvos ir užsienio šalių baudžiamojo proceso, baudžiamosios teisės ir kriminalistikos aktualijoms ir problematikai, rinkinys*, 2012, 13–34

[29] Gintaras Goda, „Procesinių prievartos priemonių Lietuvos Respublikos baudžiamojo proceso kodekso projekte samprata, klasifikacija ir turinys", *Teisė*, (2000): 17–27. Gintaras Goda, *Vertybiniai prioritetai baudžiamajame procese: monografija*, (Vilnius: Registrų centras, 2014).

[30] Aurelijus Gutauskas, „Kriminalinė žvalgyba ir privatus žmogaus gyvenimas", *Teisė* 113 (2019): 8–26, doi:10.15388/Teise.2019.113.1.

[31] Raimondas Jurka, „Įrodymų perdavimo Europos Sąjungos valstybių narių baudžiamojoje justicijoje iššūkiai ir atradimai", *Jurisprudencija,* (2019, 26(2)), 322.

[32] Linas Belevičius, „Techninių priemonių panaudojimo tiriant nusikaltimus teisinis reglamentavimas", *Jurisprudencija : mokslo darbai* 29 (2002): 72–85.

P. Pakutinskas[33], A. Panomariovas ir R. Ramanauskas[34], P. Tarasevičius[35], R. Marcinauskaitė[36], M. Civilka ir L. Šlapimaitė[37], J. Dešriūtė[38]. Lietuvos mokslininkai mokslinuose straipsniuose analizuoja privataus gyvenimo ribojimo elektroniniuose ryšiuose ir IP telefonijose siekiant ištirti nusikaltimus teisinio reglamentavimo ypatumus Lietuvoje. Autorės disertacijoje asmens duomenų rinkimo el. erdvėje teisėsaugos ir žvalgybos tikslais reglamentavimo Lietuvoje analizė yra paremta palyginimu su JAV teisiniu reglamentavimu ir teismų praktika. Disertacijoje taip pat yra apžvelgiamos teisinės prisijungimų prie elektroninės erdvės prielaidos (angl. *Government Hacking*) Lietuvos Respublikos kriminalinės žvalgybos įstatyme ir BPK. R. Ažubalytė moksliniame straipsnyje analizuoja kaip Lietuvos teismai privalo spręsti BPK ir Kriminalinės žvalgybos įstatymo spragas dėl asmens duomenų rinkimo el. erdvėje. Disertacijoje atlikta JAV teisės aktų ir teismų precedentų istorinė analizė parodė, kad analogiška situacija buvo ir yra JAV (2.2. disertacijos poskyris). Pirmasis pasaulyje asmens duomenų rinkimą el. erdvėje reglamentuojantis teisės aktas 1968 m. atsirado kaip 1967 m. JAV Aukščiausiojo Teismo sprendimo byloje *Berger v. New York* rezultatas. Disertacijoje atlikta istorinė JAV teismų sprendimų ir teisės aktų genezės analizė gali būti reikšminga Lietuvos Respublikos teismams, kadangi jiems šiuo metu tenka spręsti labai panašias problemas, kurias sprendė ir JAV teismai. A. Gutauskas moksliniame straipsnyje analizuoja kiek kriminalinės žvalgybos naudojamos priemonės gali teisėtai skverbtis į privatų žmogaus gyvenimą[39]. P. Pakutinsko daktaro disertacija „Elektroninių komunikacijų teisinio reguliavimo modeliai“[40] yra artimiausia autorės disertacijai. P. Pakutinskas disertacijoje analizavo elektroninių komunikacijų teisinio reguliavimo modelius, tačiau jo disertacija neapima asmens duomenų teisinės apsaugos klausimų[41], kurie yra šios disertacijos objektu.

Mokslinis naujumas ir reikšmė. Disertacijoje yra pirmasis mokslinis darbas, kuriame istoriniu ir lyginamuoju metodu yra analizuojamos bendrosios (JAV) ir kontinentinės teisės (Lietuvos) tradicijų šalių bei supranacionalinio lygmens (ET ir ES) asmens duomenų rinkimo el. erdvėje teisėsaugos ir žvalgybos tikslais teisinio

---

[33] Paulius Pakutinskas, „Elektroninių komunikacijų teisinio reguliavimo modeliai“, (daktaro disertacija, Mykolo Romerio universitetas, 2009).

[34] Artūras Panomariovas ir Ramūnas Ramanauskas, „Slaptumas – tiesos baudžiamajame procese nustatymo priemonė“, *Jurisprudencija : mokslo darbai*, no. 75 (2005): 50–57.

[35] Petras Tarasevičius, „Techninių priemonių naudojimo kriminalinėje žvalgyboje teisėtumo problemos“, *Teisė*, 2017, 84–99, doi:10.15388/Teise.2017.105.11114.

[36] Renata Marcinauskaitė, „Nusikalstamos veikos elektroninėje erdvėje“, (daktaro disertacija, Mykolo Romerio universitetas).

[37] Mindaugas Civilka ir Lina Šlapimaitė, „Asmens duomenų samprata elektroninėje erdvėje“, *Teisė*, 96 (2015): 126–148.

[38] Justina Dešriūtė, „Esminiai asmens duomenų apsaugos baudžiamajame procese reformos Europos Sąjungoje aspektai ir jų įtaka nacionaliniam teisiniam reguliavimui“, *Teisės problemos*, 1 (91), (2016): 25-51.

[39] Aurelijus Gutauskas, „Kriminalinė žvalgyba ir privatus žmogaus gyvenimas“, *Teisė* 113 (2019): 8–26, doi:10.15388/Teise.2019.113.1.

[40] Petras Tarasevičius, „Techninių priemonių naudojimo kriminalinėje žvalgyboje teisėtumo problemos“, *Teisė*, 2017, 84–99, doi:10.15388/Teise.2017.105.11114.

[41] Paulius Pakutinskas, „Elektroninių komunikacijų teisinio reguliavimo modeliai“, (daktaro disertacija, Mykolo Romerio universitetas, 2009), 7.

reglamentavimo ypatumai dėl teisės į asmens duomenų apsaugą užtikrinimo. Nors JAV reglamentavimas taip turi trūkumų (pvz. vienas iš jų – JAV teisės aktais siekiama užtikrinti tik JAV piliečių ar nuolatinių gyventojų teisę į asmens duomenų apsaugą, kiti asmenys ar jų asmens duomenys JAV jurisdikcijoje neturi, todėl JAV vykdomos ne JAV asmenų masinio asmens duomenų rinkimo programos yra teisėtos JAV teisės aktų atžvilgiu), tačiau dar 1968 m. buvo priimtas pirmasis teisės aktas, skirtas šios srities reglamentavimui, ir nuo to laikotarpio vis priimami nauji arba pataisomi galiojantys teisės aktai, o teismų vaidmuo teisėkūroje yra aktyvus. Tyrimo rezultatai rodo, kad ES ir ET teisės įtaka asmens duomenų apsaugai kuomet jie yra renkami el. erdvėje teisėsaugos ir žvalgybos tikslais yra minimali ir daugiausiai pasireiškia tik per šios teisės suteikimą asmenims ir teismų interpretavimą dėl apribojimų teisėtumo ir pagrįstumo, todėl seniausias teisinio reglamentavimo ištakas turinčių JAV teisės normų ir teismų praktikos istorinė analizė bei palyginimas su teisiniu reglamentavimu Lietuvoje ir gerosios teisinio reglamentavimo patirties perėmimas butų naudingas Lietuvos teisės aktų tobulinimui.

Tyrimo objektas. Asmens duomenų rinkimo elektroninėje erdvėje teisėsaugos ir žvalgybos tikslais teisinis reglamentavimas.

Disertacijos **mokslinė problema** formuluojama keliant tokius klausimus:

1. Kaip reglamentuoti asmens duomenų rinkimą elektroninėje erdvėje teisėsaugos ir žvalgybos tikslais Lietuvos teisės aktuose, kad būtų užtikrinama teisė į asmens duomenų apsaugą?
2. Kokie asmens duomenų rinkimo elektroninėje erdvėje teisėsaugos ir žvalgybos tikslais reglamentavimo JAV ir kitų šalių gerosios praktikos elementai galėtų būti perkelti į Lietuvos teisės aktus?
3. Kaip ES ir ET teisinis reglamentavimas įtakoja teisinę asmens duomenų rinkimo elektroninėje erdvėje teisėsaugos ir žvalgybos tikslais praktiką Lietuvoje?
4. Kodėl asmens duomenų rinkimo elektroninėje erdvėje teisėsaugos ir žvalgybos tikslais reglamentavimas JAV apriboja Lietuvos gyventojų teisės į asmens duomenų apsaugą ir privatumą įgyvendinimą?
5. Kaip teisėsaugos ir žvalgybos institucijų bendradarbiavimas su privačiais juridiniais asmenimis dėl asmens duomenų rinkimo elektroninėje erdvėje įtakoja teisės į asmens duomenų apsaugą įgyvendinimą?

Tikslas. Ištirti teisinio asmens duomenų rinkimo elektroninėje erdvėje teisėsaugos ir žvalgybos tikslais teisinio reglamentavimo ypatumus bei išskirti gerosios praktikos pavyzdžius pagal kuriuos būtų galima tobulinti Lietuvos teisės aktus.

Uždaviniai:

1. Įvertinti asmens duomenų rinkimo elektroninėje erdvėje teisėsaugos ir žvalgybos tikslais reglamentavimą bendrosios teisės tradicijos valstybėje (JAV atvejis) ir išskirti gerąją praktiką, naudotiną teisiniame reglamentavime Lietuvoje;
2. Įvertinti asmens duomenų rinkimo elektroninėje erdvėje teisėsaugos ir žvalgybos tikslais reglamentavimą supranacionaliniu lygmeniu (Europos atvejis);

3. Nustatyti ir įvertinti asmens duomenų rinkimo el. erdvėje teisėsaugos ir žvalgybos tikslais teisinio reglamentavimo santykį su teise į asmens duomenų apsaugą kontinentinės teisės tradicijos valstybėje (Lietuvos atvejis);
4. Identifikuoti dispozityvaus teisėsaugos, žvalgybos ir verslo bei mokslo bendradarbiavimo formas ir įvertinti probleminius teisės į asmens duomenų apsaugą aspektus;
5. Atsižvelgiant į nustatytus gerosios praktikos pavyzdžius parengti asmens duomenų rinkimo elektroninėje erdvėje teisėsaugos ir žvalgybos tikslais reglamentavimo Lietuvoje tobulinimo pasiūlymus.

Ginamieji teiginiai:

1. Asmens duomenų rinkimo el. erdvėje teisėsaugos ir žvalgybos tikslais reglamentavimas Lietuvos Respublikos teisės aktuose įtvirtinant specialiąsias normas tik dėl komunikacijos turinio rinkimo realiuoju laiku, istorinio pobūdžio asmens duomenų rinkimą ir teisėtą prisijungimą prie elektroninių ryšių įrenginių reglamentuojant kitų procesinių veiksmų atlikimui skirtomis normomis, neužtikrina teisės į asmens duomenų apsaugą teisėtam apribojimui keliamų reikalavimų.
2. Lietuvos teisės aktuose adaptavus JAV praktiką dėl istorinio pobūdžio asmens duomenų rinkimo el. erdvėje teisėsaugos ir žvalgybos tikslais bei JAV, Vokietijos, Didžiosios Britanijos, Lenkijos, Italijos, Nyderlandų ir Prancūzijos gerąją praktiką dėl teisėto prisijungimo prie elektroninės erdvės įrenginių reglamentavimo BPK ir Kriminalinės žvalgybos įstatymo nuostatos taptų aiškios ir tiksliau apibrėžtos, atitiktų EŽTK, Europos Sąjungos pagrindinių teisių chartijoje ir Lietuvos Respublikos Konstitucijoje įtvirtintiems teisėtiems teisės į asmens duomenų apsaugą apribojimų pagrindams.
3. ES ir ET lygiu asmens duomenų rinkimo teisėsaugos ir žvalgybos tikslais reglamentavimas šiuo metu pasireiškia tik bendrojo pobūdžio teisės į asmens duomenų apsaugą suteikimu, kuri EŽTT ir ESTT praktika yra išplečiama į el. erdvę. EŽTT ir ESTT praktika Lietuvos teismai vadovaujasi vertindami teisės į asmens duomenų apsaugos suvaržymo būtinumą, tačiau Lietuvos teisės aktai tik dalinai atitinka EŽTT praktiką dėl teisės į asmens duomenų apsaugą apribojančio įstatymo aiškumo, apribojimo proporcingumo ir sankcionavimo būtinumo.
4. JAV teisės aktuose įtvirtintas asmens duomenų rinkimo teisėsaugos ir žvalgybos tikslais reglamentavimas asmens duomenų apsaugą garantuoja tik JAV asmenims, todėl JAV žvalgybos tikslais Lietuvos gyventojų asmens duomenys gali būti teisėtai renkami vadovaujantis FISA ir EO 12 333 teisės aktų nuostatomis nepriklausomai nuo pačio asmens fizinės buvimo vietos Lietuvos Respublikoje.
5. Teisėsaugos ir žvalgybos institucijoms asmens duomenis elektroninėje erdvėje renkant dispozityvios, viešai neskelbiamos bendradarbiavimo su privačiais juridiniais asmenimis sutarties pagrindu, teisės į asmens duomenų apsaugą įgyvendinimas priklauso nuo šalių pasirenkamos sutarčiai taikytinos teisės ir asmens duomenų apsaugos nuostatų buvimo ar nebuvimo. Toks asmens duomenų rinkimo pagrindas sudaro sąlygas piktnaudžiauti teisės į asmens duomenų apsaugą suvaržymu.

Metodologija. Disertacijos tikslui pasiekti ir uždaviniams įgyvendinti naudojami skirtingi mokslinių tyrimų metodai. Duomenys disertacijai renkami vadovaujantis *teisinių dokumentų analizės, mokslinės literatūros analizės, nestruktūruoto ir struktūruoto ekspertų interviu, stebėjimo metodais.* Surinkti duomenys apdorojami taikant šiuos teorinius metodus: *sisteminės analizės, istorinį ir lyginamąjį*.

Teisinių dokumentų analizės metodu tiriama JAV, ES, ET, Lietuvos teisės aktai. Šio metodo taikymo tikslas – ištirti buvusį ir esamą asmens duomenų rinkimo teisėsaugos ir žvalgybos tikslais teisinį reglamentavimą JAV, ES, ET ir Lietuvoje. Bendrosios teisės tradicijų šalyse teismo precedentai yra labai svarbūs, todėl kokybinis JAV teismų precedentų tyrimas svarbus vertinant ir aiškinant teisės normas, jų pakeitimus, praktinį taikymą užtikrinant IV JAV Konstitucijos pataisa įtvirtintą teisę į privatumą bei kartu asmens duomenų apsaugą. JAV teismų sprendimai disertacijos tyrimui yra svarbūs ir lyginamuoju požiūriu, kadangi kai kurios dabar galiojančios Lietuvos teisės aktų nuostatos yra panašios į seniau galiojusias JAV, bet pakeistas teismų sprendimų pagrindu. EŽTT ir ESTT sprendimai dėl teisės į asmens duomenų apsaugą disertacijos tyrimui buvo reikšmingi dėl EŽTK ir Europos žmogaus teisių chartijoje įtvirtintos teisės į asmens duomenų apsaugą galiojimo ir apribojimų apimties aiškinimo. Lietuvos teismų sprendimai – dėl Kriminalinės žvalgybos įstatymo ir BPK nuostatų praktinio taikymo klausimų išaiškinimo.

Mokslinės literatūros analizės metodas naudojamas siekiant atskleisti JAV ir Europos mokslininkų požiūrį ir jų atliktų mokslinių tyrimų rezultatus dėl teisės į asmens duomenų apsaugą įgyvendinimo asmens duomenis el. erdvėje renkant teisėsaugos ir žvalgybos tikslais, šią sritį reglamentuojančių teisės aktų pakeitimus ir bei jų poveikį. Mokslinės literatūros analizė taip pat padėjo surasti paaiškinimą, kodėl žvalgybos institucijos teisiškai gali rinkti duomenis apie užsieniečius, įskaitant duomenų rinkimą el. erdvėje. Pastebėta tendencija, kad nors teisės į asmens duomenų apsaugą užtikrinimas šiuos duomenis renkant teisėsaugos ir žvalgybos tikslais yra globali problema, dauguma mokslinės literatūros yra nukreipti į šios teisės užtikrinimą nacionaliniu lygiu.

Kadangi elektroninė erdvė pasižymi greita technologine raida, atitinkamai todėl ir teisinis reglamentavimas šioje srityje yra dinamiškas ir įtakojamas politinių bei didelę galią turinčių technologinių įmonių (Facebook, Google, Apple ir kt.) sprendimų. Disertacijoje analizuojamos pasaulinės tendencijos, todėl *stebėsenos metodas* taikomas siekiant disertacijos tematikoje turėti aktualią informaciją ir gebėti prognozuoti būsimus pokyčius arba tų pokyčių poreikį. Stebėsenos objektas – pasauliniai dienraščiai *„Financial Times“, „The Economist“, „The Guardian“, „Reuters“, „politico.eu“, Massachussets Technology Review (MIT)* žurnalas.

Nestruktūrizuoto interviu metodas taikomas probleminių reglamentavimo Lietuvoje aspektus nustatymui. Nestruktūrizuotas interviu vykdomas su penkiais ekspertais, turinčiais skirtingos patirties tyrimo objekto atžvilgiu. Dėl disertacijos temos jautrumo ekspertams sudaryta galimybė išlikti anoniminiais, interviu turinio neviešinti. Todėl keturių ekspertų tapatybė negali būti atskleista, likę du yra Vytauto Didžiojo universiteto profesorius, Lietuvos atstovas NATO STO darbo grupėje dr. Tomas Krilavičius ir Alius Navickas (Finansinių nusikaltimų tyrimo tarnyba). Interviu metu visiems

ekspertams buvo pateikiami nevienodi klausimai, jie buvo formuojami atsižvelgiant į kiekvieno eksperto pateiktą informaciją ir veiklos sritį. Autorė disertacijos tema taip pat diskutavo su užsienio mokslininkais: ESSCA School of Management prof. dr. Ana Dimitrova, kurios viena iš mokslinių tyrimų sričių yra asmens duomenų rinkimo el. erdvėje reglamentavimas JAV, Europolo asmens duomenų apsaugos ekspertu dr. Jan Ellermann, privataus investicinio rizikos kapitalo fondo vadovu Ashisie Dhruve, esančiu vienu iš pirmųjų investuotojų į Microsoft, Facebook, WhatsApp bei kitas su tyrimo objektu susijusias įmones (konfidenciali informacija), IBM Q ambasadoriumi dr. Piotr Biskupski, Mysterium Network įkūrėju Robertu Višinskiu. Disertacijoje remiamasi tik nekonfidencialia informacija.

Struktūruoto interviu metodo tikslas įvertinti BPK 154 str. taikymo praktikos tendencijas ir probleminius aspektus. Struktūruoto interviu metu būdu buvo apklausti 22 pačių ikiteisminio tyrimo institucijų deleguoti tyrėjai. Prašymai atlikti tyrimą buvo išsiųsti visoms ikiteisminio tyrimo institucijoms oficialiai nurodytais el. paštais, tačiau tyrime dalyvauti sutiko tik septynios ikiteisminio tyrimo institucijos. Tyrime dalyvavusios institucijos: Specialiųjų tyrimų tarnyba, Finansinių nusikaltimų tyrimų tarnyba, Muitinės kriminalinė tarnyba, Vilniaus apskrities vyriausiasis policijos komisariatas, Vilniaus apskrities vyriausiojo policijos komisariato Kriminalinės policijos organizuoto nusikalstamumo tyrimo valdyba, Kauno apskrities vyriausiasis policijos komisariatas ir Utenos apskrities vyriausiasis policijos komisariatas. Visiems respondentams buvo pateikti vienodi klausimai. Tyrimo rezultatai naudojami disertacijos 4.1.1. poskyryje.

Tyrimo objekto pobūdis, teisinį reglamentavimą elektroninių asmens duomenų rinkime teisėsaugos ir žvalgybos tikslais įtakojantys skirtingi veiksniai (skirtingas nacionalinis teisinis reglamentavimas, teismų sprendimai, politiniai veiksniai, technologinių įmonių vaidmuo) reiškia, kad yra reikalingas sisteminis požiūris į tyrimo objekto problematiką, todėl tyrimo rezultatų analizei buvo tikslinga naudoti *sisteminės analizės metodą*. *Istorinio tyrimo* metodas padėjo nustatyti asmens duomenų rinkimo el. erdvėje reglamentavimo doktrininį pagrindą, teisinio reglamentavimo evoliuciją bei ją įtakojančius veiksnius. Disertacijos skyriai taip pat yra išdėstyti istoriniu chronologiniu požiūriu nuo seniausiai sukurto teisinio reglamentavimo iki naujausio (JAV, ET, ES ir Lietuva). *Lyginamasis* metodas naudojamas viso tyrimo metu. Juo taip pat remtasi rengiant pasiūlymu jis buvo naudojamas kaip tobulinti asmens duomenų rinkimo el. erdvėje teisėsaugos ir žvalgybos tikslais reglamentavimą Lietuvoje. Kadangi teisinis elektroninių asmens duomenų rinkimo teisėsaugos ir žvalgybos tikslais reglamentavimas atsirado JAV ir yra labiausiai išplėtotas ir kadangi didžioji dauguma ES gyventojų asmens duomenų keliauja atviru internetu per JAV arba yra saugomi JAV esančiuose ar JAV įmonėms priklausančiuose ne JAV teritorijoje esančiuose serveriuose, o reglamentavimą Lietuvoje įtakoja ET ir ES teisinis reglamentavimas, todėl lyginamojo metodo pagalba buvo lyginama JAV, ET, ES ir Lietuvos teisės aktų nuostatos ir teismų praktika.

IŠVADOS

1. Asmens duomenims elektroninėje erdvėje galiojančią teisę apsprendžia ne fizinio asmens buvimo vietos teisė, o asmens duomenų maršrutas el. erdvėje, serverių, kuriuose saugomi asmens duomenys lokacija ir teisėsaugos bei žvalgybos institucijų imperatyviu ar dispozityviu pagrindu paslaugas joms teikiančių įmonių galimybė asmens duomenis saugoti, perimti ir pateikti bei tokio pobūdžio asmens duomenų tvarkymui galiojančios teisės normos ar sutarties nuostatos. Teisės į asmens duomenų apsaugą galiojimas pagal dabartinius teisinio reglamentavimo modelius priklauso nuo kitų parametrų– fizinio asmens buvimo vietos teisės ir valstybėse galiojančių supranacionalinių ir nacionalinių teisės aktų nuostatų. Taigi problema dėl teisės į asmens duomenų apsaugą užtikrinimo atsiranda dėl to, kad asmeniui ir jo elektroniniams asmens duomenims gali galioti skirtingi teisiniai režimai, kurie keičiasi asmens duomenims keliaujant elektronine erdve.
2. Šiuo metu egzistuoja trys teisės į asmens duomenų apsaugą suvaržymo modeliai: 1) supranacionalinis, 2) bendrosios teisės tradicijų ir 3) kontinentinės teisės modeliai. Šie modeliai egzistuoja skirtinguose lygmenyse: macro lygmenyje yra ES ir ET supranacionalinis reglamentavimas, micro – JAV (kaip bendrosios teisės tradicijų valstybės) ir Lietuvos (kaip kontinentinės teisės tradicijų valstybės) reglamentavimas. Tik atsiradus meta lygmens (pasauliniam) reglamentavimui (tarptautinės sutarties ar susitarimo forma), yra įmanoma užtikrinti teisę į asmens duomenų apsaugą, kadangi elektroninė erdvė yra globali (meta lygmens).
3. Bendrosios teisės tradicijų, kurio pavyzdžiu yra reglamentavimas JAV, modeliui būdinga detali reglamentacija ir diferenciacija:
   3.1. asmenys yra skirstomi į JAV ir ne JAV, o IV JAV Konstitucijos pataisa garantuojama teisė į privatumą ir kartu asmens duomenų apsaugą galioja tik JAV asmenų, esančių JAV teritorijoje atžvilgiu. Vadinasi, visi likę pasaulio gyventojai JAV teisinėje sistemoje neturi teisės į asmens duomenų apsaugą, nepriklausomai nuo to, kad ją turi pagal nacionalinius ar virš nacionalinius teisės aktus;
   3.2. asmens duomenų rinkimas el. erdvėje teisėsaugos tikslais yra reglamentuojamas ECPA, kurioje numatytos skirtingos asmens duomenų rinkimo el. erdvėje procedūros ir apsaugos lygiai priklausomai nuo to ar yra renkama turinio ar neturininio pobūdžio duomenys (metaduomenys) bei nuo to ar jie yra renkami realiuoju laiku, ar yra istorinio pobūdžio;
   3.3. teisminis asmens duomenų rinkimo sankcionavimas yra privalomas, tačiau reikalavimai teisminio sankcionavimo pagrįstumui skiriasi priklausomai nuo asmens duomenų tipo ir pobūdžio;
   3.4. asmens duomenų rinkimas el. erdvėje žvalgybos tikslais reglamentavimas priklauso nuo asmens ir jo asmens duomenų buvimo vietos. FISA yra taikomas tuo atveju, jeigu bent vienas užsienio subjektas yra JAV arba keliauja pro JAV teritoriją – asmuo (užsienio valstybės pilietis) arba jo duomenys. EO 12 333 taikomas tuo atveju, jeigu nei vienas užsienio subjektas nėra JAV.

Taigi, nors bendrosios teisės šalyse teisminės praktikos vaidmuo yra labai svarbus, tačiau aktyvus teismo galimybės užtikrinti teisės į asmens duomenų apsaugą juos renkant teisėsaugos ir žvalgybos tikslais elektroninėje erdvėje yra ribojamos diferencijuotu teisiniu reglamentavimu.

4. Europos kontinentiniam asmens duomenų rinkimo elektroninėje erdvėje teisėsaugos ir žvalgybos tikslais modeliui turėtų būti būdinga integracija, tačiau:
   4.1. nors EŽTK ir Europos Sąjungos teisių Chartija ir galioja visų asmenų ne tik valstybių narių piliečių atžvilgiu, integracija vyksta ne per supranacionalinį teisinį reglamentavimą, o EŽTT ir ESTT plėtojamą jurisprudenciją;
   4.2. nors ET rodo iniciatyvą, kad teisė į asmens duomenų apsaugą būtų užtikrinta asmens duomenis renkant el. erdvėje teisėsaugos ir žvalgybos tikslais ir šiuo metu rengia Elektroninės žvalgybos kodeksą, tačiau faktinio, o ne deklaratyvaus, mechanizmo ji nėra pajėgi parengti ir užtikrinti, jeigu planuojamas Elektroninės žvalgybos kodeksas neturės tarptautinės sutarties statuso ir jam nepritars didžiosios valstybės, kurios žvalgybą elektroninėje erdvėje vykdo plačiausiu mastu;
   4.3. ES lygmeniu asmens duomenų rinkimas el. erdvėje teisėsaugos ir žvalgybos tikslais specialiaisiais aktais nėra reglamentuojamas. ES teisė yra netaikoma žvalgybai, taigi valstybės narės pačios sprendžia kaip reglamentuoti asmens duomenų rinkimą el. erdvėje žvalgybos tikslais. Asmens duomenų rinkimas el. erdvėje teisėsaugos tikslais disertacijos rašymo metu taip pat nėra reglamentuojamas, nors yra pradėtas rengti elektroninių įrodymų direktyvos projektas. 2018 m. įsigaliojusios Asmens duomenų tvarkymo teisėsaugos tikslais direktyvoje specialiųjų nuostatų dėl asmens duomenų rinkimo el. erdvėje nėra.
5. Asmens duomenų rinkimo elektroninėje erdvėje teisėsaugos ir žvalgybos tikslais reglamentavimas Lietuvoje yra nestruktūruotas. Specialiomis normomis reglamentuojamas tik asmens duomenų rinkimas realiuoju laiku iš elektroninių ryšių paslaugų teikėjų, kurie iki 2018 m. paskelbto Elektroninių ryšių kodekso, vadovaujantis ESTT išaiškinimu, neapėmė kitų nei telekomunikacijų paslaugų teikėjų. Istorinio pobūdžio asmens duomenų rinkimas yra vykdomas vadovaujantis BPK ir Kriminalinės žvalgybos įstatymo nuostatomis, skirtoms rinkti bendro pobūdžio duomenis (t. y. ne asmens duomenis) ne elektroninėje aplinkoje. Toks reglamentavimas tik iš dalies atitinka EŽTT jurisprudenciją dėl teisėtų EŽTK 8 str. įtvirtintos teisės į asmens duomenų apsaugą apribojimo pagrindų ir nepakankamai užtikrina teisę į asmens duomenų apsaugą. Asmens duomenų rinkimo elektroninėje erdvėje reglamentavimas Lietuvoje papildytas gerosios reglamentavimo JAV praktikos pavyzdžiais, visiškai atitiktų teisėto teisės į asmens duomenų apsaugą suvaržymui keliamus reikalavimus.
6. Vadovaujantis Konstitucijos 22 str. ir EŽTT jurisprudencija, sankcionavimas yra pirmuoju teisėto teisės į asmens duomenų apsaugą suvaržymo reikalavimu. Ne visi asmens duomenų rinkimo elektroninėje erdvėje ikiteisminio tyrimo veiksmai yra sankcionuojami teismo. Teisminis sankcionavimas nėra numatytas BPK 97 str., vadovaujantis BPK 155 str. asmens duomenys yra renkami ikiteisminio

tyrimo teisėjo pritarimu, kuris neatitinka motyvuotam teismo sprendimui keliamų reikalavimų.

7. Ikiteisminio tyrimo metu istorinio pobūdžio asmens duomenys gali būti renkami vadovaujantis BPK 97, 145, 147, 155 str., kurie nėra skirti asmens duomenų rinkimo reglamentavimui, todėl neatitinka teisėtam ir proporcingam teisės į asmens duomenų apsaugą suvaržymui keliamų reikalavimų.
8. Asmens duomenų rinkimas realiuoju laiku yra apribotas BPK 154 str. 1 d. įtvirtintomis nusikalstamomis veikomis. Istorinio pobūdžio asmens duomenų rinkimas elektroninėje erdvėje, vadovaujantis BPK 97, 145, 147, 155 str., yra galimas dėl visų BK nusikalstamų veikų. Tai neatitinka EŽTT jurisprudencijos dėl proporcingo EŽTK 8 str. įtvirtintos teisės apribojimo. Išplėtus BPK 154 str. reglamentaciją apimant istorinio pobūdžio asmens duomenų rinkimą tokiam duomenų rinkimui galiotų tokios pačios nuostatos kaip ir realiuoju laiku renkamiems asmens duomenims.
9. BPK 154 str. 6 d. įtvirtinta galimybė nesankcionuotai rinkti asmens duomenis esant bent kurio proceso dalyvio sutikimui, jeigu nesinaudojama el. ryšių teikėjų paslaugomis ir įrenginiais, nereglamentuojant sutikimo gavimo procedūrų, asmens duomenų rinkimo apimties bei nenumačius vėlesnio teismo sankcionavimo tampa lygiaverčiu teismo sprendimui. Tai reiškia, kad vieno asmens sutikimo pagrindu yra renkama ne tik sutikimą davusio asmens, bet ir visų kitų asmenų (įskaitant ne proceso dalyvių), kurie tokio sutikimo nedavė, tačiau el. erdvėje komunikuoja su sutikimą davusiu asmeniu, asmens duomenys. Toks nesankcionuotas asmens duomenų rinkimas pažeidžia Lietuvos Respublikos Konstitucijos 22 str. Ši BPK nuostata turėtų būti panaikinta.
10. Adaptuojant gerąją JAV praktiką siūlytina istorinio pobūdžio asmens duomenų rinkimą reglamentuoti ne bendromis, o specialiomis BPK nuostatomis išplečiant BPK 154 str. taikymo apimtis ir istorinio pobūdžio asmens duomenų rinkimui.
11. Siekiant įvesti teisinio aiškumo ir sureglamentuoti BPK 158 str. ir Kriminalinės žvalgybos įstatymo 10 str. 1 d. tiesiogiai nereglamentuojamą prisijungimo prie elektroninės erdvės specifiką, prisijungimas prie elektroninės erdvės BPK turėtų būti įtvirtintas kaip atskira procesinė prievartos priemonė, o Kriminalinės žvalgybos įstatyme atskiras kriminalinės žvalgybos informacijos rinkimo būdas.
12. Kriminalinės žvalgybos įstatyme įtvirtintos dvi galimybės teismo nesankcionuotai rinkti asmens duomenis: 1) iš juridinių asmenų ir 2) esant asmens sutikimui, kai nesinaudojama el. ryšių paslaugų teikėjų įrenginiais ar paslaugomis. Toks nesankcionuotas asmens duomenų rinkimas neatitinka Konstitucijos 22 str. nuostatų.
13. Lietuvoje žvalgybos institucijos asmens duomenis elektroninėje erdvėje gali rinkti žvalgybos ir kontržvalgybos tikslais. Šie tikslai reiškia, kad žvalgybos institucijos veikia arba Lietuvoje arba už Lietuvos teritorijos. Lietuvos Respublikos Konstitucija garantuojama teisė į privatumą, teismų jurisdikcija galioja tik Lietuvoje arba tik Lietuvos piliečiams, tačiau asmens duomenų rinkimas žvalgybos ir kontržvalgybos tikslais Žvalgybos įstatyme yra reglamentuojamas vienodai.

14. Žvalgybos įstatymas teisminio sankcionavimo poreikį skirsto ne pagal veiklos tikslą – žvalgybą ar kontržvalgyba – o pagal tai ar yra renkama meta duomenys ar turininio pobūdžio informacija. Tai neatitinka EŽTK 8 str. ir Konstitucijos 22 str. dėl to, kad meta duomenys taip pat yra asmens duomenys, o asmenų, kuriems galioja Lietuvos Respublikos Konstitucija atžvilgiu jie yra renkami teismui nesankcionavus. Todėl asmens duomenų rinkimas kontržvalgybos tikslais turėtų būti sankcionuojamas teismo, žvalgybos tikslais – Valstybės gynimo tarybos.
15. Teisėsaugos ir žvalgybos institucijų bendradarbiavimo su privačiais juridiniais asmenimis dėl asmens duomenų rinkimo įtaka teisės į asmens duomenų apsaugą įgyvendinimui priklauso nuo šių subjektų bendradarbiavimo formos ir tikslo: 1) sutartinio bendradarbiavimo atveju teisės į asmens duomenų apsaugą užtikrinimas tampa susitarimo ir susitarimui taikytinos teisės objektu, todėl asmens duomenų apsaugos garantijos tampa minimalios arba tokių iš viso nelieka; 2) savanoriško bendradarbiavimo atveju teisėsaugos pagal nacionalinės teisės nuostatas pateikti prašymai yra pakartotinai vertinami privataus juridinio asmens ir nevisais atvejais yra tenkinami.

Autorės mokslinių publikacijų sąrašas

1. Kurapka, Vidmantas Egidijus, Matulienė, Snieguolė, Stankevičiūtė, Sigutė. *The role of data protection reguliation for a proper implementation of vision for European forensic science 2020* // Political sciences, law, finance, economics and tourism : conference proceedings, 26 August – 1 September, 2015 Albena, Bulgaria. Vol. I : Political sciences, law.- (International multidisciplinary scientific conference on social sciences and arts. SGEM 2015, ISSN 2367- 5659). Sofia: STEF92 Technology Ltd, 2015. ISBN 9786197105469. p. 805-812. [Conference Proceedings Citation Index - Science (Web of Science)] [M.kr.: S 001].
2. Stankevičiūtė, Sigutė. *JAV naudojamų kriminalistinių nusikalstamų veikų tyrimo ir užkardymo bei žvalgybos metodų santykis su Europos žmogaus teisių konvencijos ir Europos Sąjungos pagrindinių teisių chartijos garantuojama teise į asmens duomenų apsaugą.* Kriminalistika ir teismo ekspertologija : mokslas, studijos, praktika = Criminalistics and forensic examination : science, studies, practice = Криминалистика и судебная экспертология: наука, обучение, практика. [T.] XIII. Vilnius: Lietuvos teismo ekspertizės centras, 2017.
3. Stankevičiūtė, Sigutė. *Application of the Directive on personal processed for law enforcement purposes to the collection of personal data in cyber space.* Kriminalistika ir teismo ekspertologija: mokslas, studijos, praktika = Criminalistics and forensic examination : science, studies, practice = Криминалистика и судебная экспертология : наука, обучение, практика. [T.] XIII. Vilnius : Lietuvos teismo ekspertizės centras, 2018.

Autorės skaityti pranešimai konferencijose, mokslo renginiuose

1. Stankevičiūtė, Sigutė. *The role of data protection reguliation for a proper implementation of vision for European forensic science 2020*, International multidisciplinary scientific conference on social sciences and arts. SGEM 2015, Sofia, Bulgarija.
2. Vilniaus kolegijos 2016 m. vasario 3 d. organizuotame renginyje Europos asmens duomenų apsaugos dienai paminėti, skaityta paskaita „*Teisiniai asmens duomenų apsaugos aspektai*“.
2. Teisėjų padėjėjų asociacijos kartu su Nacionaline teismų administracija 2016 m. gegužės 6 d. organizuotame seminare „Europos Žmogaus Teisių Teismo jurisprudencija. Baudžiamoji teisė ir procesas“ skaitytas pranešimas „*Asmens duomenų apsauga ir teisėsauga*“.

SIGUTĖS STANKEVIČIŪTĖS GYVENIMO APRAŠYMAS

Išsilavinimas

2013–2020	Doktorantūros studijos, Mykolo Romerio universitetas, Disertacija „Asmens duomenų rinkimo elektroninėje erdvėje teisėsaugos ir žvalgybos tikslais reglamentavimas“.
2010–2012	Teisės magistro laipsnis (Baudžiamoji teisė ir kriminologija), Mykolo Romerio universitetas, Baigiamasis darbas „Terorizmo baudžiamasis teisinis reglamentavimas“.
2006–2010	Teisės bakalauro laipsnis, Mykolo Romerio universitetas.

Sertifikatai, kvalifikacijos tobulinimas

2017 m.	Asmens duomenų apsaugos pareigūno sertifikatas, Mastrichto universitetas.
2017 m.	Electronic surveillance Law, Stanfordo universitetas.

Kalbos

Gimtoji	Lietuvių.
C1	Anglų (kalbos lygis nustatytas 2019 m. Soros International House).
B1	Rusų.

Praktinės veiklos patirtis

2020-11-03–dabar	Generolo Jono Žemaičio Lietuvos karo akademijos Gynybos inovacijų centras www.lka.lt – Patarėja.
2020-07-01–dabar	Fintech startuolis UAB „Analitika ir co“ http://dicheck.eu/en – Ekspertė teisės klausimais.
2012-07-01–2020-07-01	Mokslo, inovacijų ir technologijų agentūra (MITA) www.mita.lrv.lt *Pareigos:* Ekspertė (teisė ir inovacijos), projekto vadovė, asmens duomenų apsaugos pareigūnė. *Darbo pobūdis:* Nacionalinių strategijų kūrimas, MTEP projektų ir tarptautinių bendradarbiavimo programų valdymas.

Teisinės veiklos praktika:

- Nacionalinės politikos inovacijų pirkimų srityje kūrimas;
- Teisės aktų, programų ir projektų rengimas;
- Strateginių nacionalinių viešojo sektoriaus MTEP projektų koordinavimas (fintech, sveikatos apsaugos, IT, gynybos ir saugumo sritys);
- Nacionalinė ekspertė ikiprekybinių pirkimų ir inovatyviųjų viešųjų pirkimų srityje;
- Asmens duomenų apsauga, intelektinė nuosavybė, klasterizacija.

Tarptautinių MTEP projektų valdymas

- „innovation by developing a European Procurer Networking for security research services (iprocureNet)“ – **H2020** projekto vadovė ir nacionalinė atstovė (2018–2020);
- „Collaborative Innovation Procurement Action to Improve the Efficiency, Quality and Sustainability of Healthcare“ – **COSME** projekto vadovė ir vyr. ekspertė (2019–2020).

Nacionalinių projektų valdymas

- „Promotion of innovation procurement and pre-commercial procurement“ – Projekto vadovė (2016–2020).

Tarptautiniai santykiai

- Bendradarbiavimo programos su NASA rengėja ir atstovė Lietuvoje;
- Bendradarbiavimo programos su Kinija MTEP srityje koordinatorė.

Strateginių nacionalinių viešojo sektoriaus MTEP projektų koordinavimas (2016–2020):

- Lietuvos bankas „LB Chain platformos paslaugos sukūrimas“;
- Krašto apsaugos ministerija „Žvalgo stebėjimo sistema diena-naktis“;
- Registrų centras „Erdvinių trimačių (3D) duomenų, būtinų ūkio plėtros projektų efektyviam įgyvendinimui, parengimo, saugojimo ir valdymo technologijos bandomosios versijos sukūrimas“;
- Generolo Jono Žemaičio Lietuvos Karo akademija „Nacionalinės informacinio poveikio atpažinimo ir analizės ekosistemos (NAAS) sukūrimas“;
- VšĮ Vilniaus universiteto ligoninė Santaros klinikos „Inovatyvių įtvarų gamybos technologijos sukūrimas“;
- VšĮ Vilniaus universiteto ligoninė Santaros klinikos „Operacinio lauko išmaniosios padidintos spalvų skyros apšvietimo sistemos sukūrimas“;

– Lietuvos automobilių kelių direkcija „Nanomedžiagomis modifikuoto asfalto mišinio, didinančio automobilių kelių dangų tvarumą, sukūrimas“;
– AB „Energijos skirstymo operatorius“ „Elektros skaitiklių gedimo / pažeidimo priežasčių nustatymo metodikos ir išvadų pateikimo paslaugos sukūrimas“;
– AB „Energijos skirstymo operatorius“
– Lietuvos jūrų muziejus „Moksliniais tyrimais pagrįstos gyvūnų terapijos metodikos sukūrimas ir integravimas į holistinės medicinos sveikatos koncepciją“
– Kauno miesto savivaldybės administracija „Transporto srautų matavimas realiu laiku, taikant inovatyvias technologijas, siekiant suvaldyti „kamščių“ situaciją mieste“;
– Kauno miesto savivaldybės administracija „Intelektinės transporto valdymo sistemos, kurios pagalba įkraunamos hibridinės pavaros transporto priemonių galios mechanizmas būtų valdomas debesų sistemos pagrindu sukūrimas ir testavimas“;

Paskaitų vedimas
– Ikiprekybiniai pirkimai ir inovatyvieji viešieji pirkimai (2017–2020).

2011-02-11–2011-07-01 Advokatų kontora SORAINEN
– Teisininko padėjėja įmonių teisės srityje.

2010-08-09–2011-01-31 Ugniaus Pėdnyčios advokatų kontora
– Teisininko padėjėja.

2009-09-28–2010-06-11 Valiūnas ELLEX (Lawin) advokatų kontora
– Teisininko padėjėja finansų teisės ir ginčų praktikos grupėse.

Mokslinės veiklos patirtis

2014–2016 **Mykolo Romerio universitetas**
www.mruni.eu
Projektas „Europos Kriminalistikos 2020 vizijos įgyvendinimo Lietuvoje mokslinė koncepcija“. Projektas finansuotas Lietuvos mokslo tarybos Mokslininkų grupių programos lėšomis.
– Jaunesnioji mokslo darbuotoja. Mokslinio tyrimo sritys: Europos Kriminalistikos vizija 2020, terorizmas, el. nusikaltimai, organizuotas nusikalstamumas, elektroninė žvalgyba.

1. Bilevičiūtė, Eglė; Juodkaitė-Granskienė, Gabrielė; Kurapka, Vidmantas Egidijus; Malevski, Hendryk; Matulienė, Snieguolė; Navickienė, Žaneta; Stankevičiūtė, Sigutė. *Europos kriminalistikos bendros erdvės 2020 vizijos įgyvendinimo Lietuvoje mokslinė koncepcija : mokslo studija* / atsak. red.: Vidmantas Egidijus Kurapka, Hendryk Malevski, Snieguolė Matulienė. Vilnius : Mykolo Romerio universitetas, 2016. 372 p. ISBN 9789955198451. [M.kr.: S 001] 1.

STRAIPSNIAI IR TEZĖS KONFERENCIJOS MEDŽIAGOJE WEB OF SCIENCE IR/AR SCOPUS DB

2. Kurapka, Vidmantas Egidijus; Matulienė, Snieguolė; Stankevičiūtė, Sigutė. *The role of data protection reguliation for a proper implementation of vision for European forensic science 2020* // Political sciences, law, finance, economics and tourism : conference proceedings, 26 August – 1 September, 2015 Albena, Bulgaria. Vol. I : Political sciences, law.- (International multidisciplinary scientific conference on social sciences and arts. SGEM 2015, ISSN 2367- 5659). Sofia : STEF92 Technology Ltd, 2015. ISBN 9786197105469. p. 805-812. [Conference Proceedings Citation Index – Science (Web of Science)] [M.kr.: S 001].

STRAIPSNIAI CLARIVATE ANALYTICS DB LEIDINIUOSE (MASTER JOURNAL LIST)

3. Kurapka, Vidmantas Egidijus; Matulienė, Snieguolė; Bilevičiūtė, Eglė; Stankevičiūtė, Sigutė; Drakšas, Romualdas. *The current reforms on forensic science: international experience and first steps in Lithuania // International journal of academic research*. Baku: [Progress IPS LLC]. ISSN 2075-4124. 2014, vol. 6, no 6, p. 472-476. DOI: 10.7813/2075-4124.2014/6-6/B.69. [Zoological Record; Academic Search Complete] [M.kr.: S 001]

STRAIPSNIAI IR KONFERENCIJŲ PRANEŠIMAI LEIDINIUOSE, ĮTRAUKTUOSE Į TARPTAUTINES DUOMENŲ BAZES

4. Bilevičiūtė, Eglė; Kurapka, Vidmantas Egidijus; Matulienė, Snieguolė; Stankevičiūtė, Sigutė. *The conception of implementation of vision for European forensic science 2020 in Lithuania* // International journal of social, management, economics and business engineering / World Academy of Science, Engineering and Technology. Canakkale : World Academy of Science, Engineering and Technology. ISSN 2010-376X. 2014, Vol. 8, no. 6, p. 1790-1798. [CSA Technology Research Database; Science in Context] [M.kr.: S 001].

STRAIPSNIAI RECENZUOJAMOJE UŽSIENIO KONFERENCIJŲ MEDŽIAGOJE

5. Kurapka, Vidmantas Egidijus; Bilevičiūtė, Eglė; Matulienė, Snieguolė; Stankevičiūtė, Sigutė. *Creating a conception of the vision for european forensic science 2020 implementation in Lithuania* // 10 gadi Eiropas Savienībā – sasniegumi, problēmas un nākotnes ieceres: XV starptautiskā zinātniskā konference: Biznesa augstskolas Turība konferenču rakstu krājums = 10 Years in the European Union – achievements, problems and expectations: XV international scientific conference: proceedings of the conference of Turiba University: Rīga 2014. gada 29. maijs. Rīga: Biznesa augstskolas Turība. ISSN 1691-6069. 2014, P. 309-319. [M.kr.: S 001].

TEZĖS RECENZUOJAMOJE KONFERENCIJŲ MEDŽIAGOJE

6. Kurapka, Vidmantas-Egidijus; Bilevičiūtė, Eglė; Matulienė, Snieguolė; Stankevičiūtė, Sigutė. *Europos kriminalistikos 2020 vizijos įgyvendinimo Lietuvoje mokslinė koncepcija: problemų medis = The conception of implementation of vision for European forensic science 2020 in Lithuania: the tree of problems* // Kriminalistika ir teismo ekspertologija: mokslas, studijos, praktika = Criminalistics and forensic examination: science, studies, practice = Криминалистика и судебная экспертология: наука, обучение, практика. [T.] XI. Vilnius: Lietuvos teismo ekspertizės centras, 2015. ISBN 9789986555421. P. 453-456. [M.kr.: S 001]
7. Bilevičiūtė, Eglė; Kurapka, Vidmantas Egidijus; Matulienė, Snieguolė; Stankevičiūtė, Sigutė. *The current reforms on forensic science : international experience and first steps in Lithuania* // SOCIN 2014 : international interdisciplinary conference on social innovations „Social Innovations : theoretical and practical insights 2014“: conference abstracts : October 23-24, 2014 [Elektroninis išteklius] / Mykolas Romeris University. Vilnius : Mykolas Romeris University, 2014. ISBN 9789955196839. P. 56-57. [M.kr.: S 001]
8. Stankevičiūtė, Sigutė. *JAV naudojamų kriminalistinių nusikalstamų veikų tyrimo ir užkardymo bei žvalgybos metodų santykis su Europos žmogaus teisių konvencijos ir Europos Sąjungos pagrindinių teisių chartijos garantuojama teise į asmens duomenų apsaugą.* Kriminalistika ir teismo ekspertologija : mokslas, studijos, praktika = Criminalistics and forensic examination : science, studies, practice = Криминалистика и судебная экспертология: наука, обучение, практика. [T.] XIII. Vilnius: Lietuvos teismo ekspertizės centras, 2017.

9. Stankevičiūtė, Sigutė. *Application of the Directive on personal processed for law enforcement purposes to the collection of personal data in cyber space.* Kriminalistika ir teismo ekspertologija: mokslas, studijos, praktika = Criminalistics and forensic examination : science, studies, practice = Криминалистика и судебная экспертология : наука, обучение, практика. [T.] XIII. Vilnius : Lietuvos teismo ekspertizės centras, 2018.

MYKOLAS ROMERIS UNIVERSITY

Sigutė Stankevičiūtė

LEGAL REGULATION OF ELECTRONIC SURVEILLANCE

Summary of Doctoral Thesis
Social Sciences, Law (S 001)

Vilnius, 2020

The doctoral thesis was written during the period of 2013–2019, defended at Mykolas Romeris University according to the right to carry out doctoral studies provided to Mykolas Romeris University and Vytautas Magnus University under the order of the Minister of Education, Science and Sport of the Republic of Lithuania No. V-160 „On granting the right of doctoral studies“ dated on February 22, 2019.

Scientific supervisor:
Prof. Dr. Vidmantas Egidijus Kurapka (Mykolas Romeris University, Social Sciences, Law, S 001).

The doctoral thesis will be defended at the Law Research Council of Mykolas Romeris University and Vytautas Magnus University:

Chairperson:
Prof. Dr. Regina Valutytė (Mykolas Romeris University, Social Sciences, Law, S 001).

Members:
Prof. Dr. Paolo Balboni (Maastricht University, the Netherlands, Social Sciences, Law, S 001);
Prof. Dr. Aurelijus Gutauskas (Vilnius University, Social Sciences, Law, S 001);
Prof. Dr. Raimundas Jurka (Mykolas Romeris University, Social Sciences, Law, S 001);
Prof. Dr. Darius Štitilis (Mykolas Romeris University, Social Sciences, Law, S 001).

The public defence of the doctoral thesis will takeplace at the public meeting of the Law Research Council at Mykolas Romeris University on the 21st of December, 2020, 10 AM in the Conference Hall of Mykolas Romeris University (Room I-414).
Address: Ateities str. 20, Vilnius, Lithuania.

The doctoral thesis was sent out the 20th of November, 2020.

The doctoral thesis is available at Martynas Mažvydas National Library of Lithuania (Gedimino ave. 51, Vilnius) and the libraries of Mykolas Romeris University (Ateities str. 20, Vilnius) and Vytautas Magnus University (K. Donelaičio str. 52, Kaunas).

Sigutė Stankevičiūtė

LEGAL REGULATION OF ELECTRONIC SURVEILLANCE

SUMMARY

Relevance of the topic. Cyberspace was created to share the data[1] not to protect[2]. Who should protect the personal data then? The source of the personal data – a human being – has limited possibilities to protect their data, as the controllers of the information are legal persons providing services on the cyberspace. While among the personal data users are not solely the providers of the services but also other legal persons, law enforcement authorities and intelligence services. The statement that personal data has become the oil of XXI century[3] is often used. Nevertheless, if the general public was asked to explain how our personal data generates enormous profit for the entities providing services on cyberspace[4], an average person with no educational background or work experience in this field, would not be able to provide an answer. By virtue of the European Union (hereinafter – the EU) data protection reform, some people are now aware of their right to personal data protection; however, this knowledge is often confronted with the claim 'I have nothing to hide'. Therefore, the general public is left with the impression that as we are the recipients of the services, as well as since the enforcement of the General Personal Data Protection Regulation we can control circulation of the personal data[5], we directly benefit from cyberspace being an indispensable part of our lives. In reality, the ones who benefit from our use of cyberspace are various entities providing us with diverse services (providers of electronic communication, providers of social networks, developers of mobile devices, advertising agencies, etc.), as well as State institutions. While developing the Internet, the USA could not foresee that its civilian use will bring it back to the original aim – the use of cyberspace to ensure national security. Nevertheless, currently the Internet is not merely used as a means communication between military units with the aim to ensure national security, but as an instrument for civilian surveillance on a global scale, as well as a mechanism

[1] The first workable prototype of the Internet came in the late 1960s with the creation of ARPANET, or the Advanced Research Projects Agency Network.For more information, please visit https://www.history.com/news/who-invented-the-internet .

[2] John R. Vacca, *Computer and Information Security Handbook* (Morgan Kaufmann, 2009), 4.

[3] „The World's Most Valuable Resource Is No Longer Oil, but Data", *The Economist*, žiūrėta 2020 m. rugpjūčio 30 d., https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data.

[4] Milan Babic, Jan Fichtner ir Eelke M. Heemskerk, „States versus Corporations: Rethinking the Power of Business in International Politics", *The International Spectator* 52, no. 4 (2017): 20–43, doi:10.1080/03932729.2017.1389151. Darius Mikutavičius, „„Microsoft" vertė pirmą kartą pasiekė trilijono dolerių ribą", *lrt.lt*, žiūrėta 2020 m. rugpjūčio 30 d., https://www.lrt.lt/naujienos/mokslas-ir-it/11/1052527/microsoft-verte-pirma-karta-pasieke-trilijono-doleriu-riba.

[5] „What Are the Advantages of the Internet?", *Computer Hope*, žiūrėta 2020 m. rugpjūčio 30 d., https://www.computerhope.com/issues/ch001808.htm.

for forecasting actions by masses, institutions or other countries. Recent scandals related to personal date leakage in the USA[6], the desire to conduct mass electronic surveillance in order to control COVID-19[7] shows that not only business but also states, in particular law enforcement authorities and intelligence services, can benefit from the profound amount of personal data collected as a result of massive use of cyberspace. So, who should protect our personal data? As personal data protection was not the aim of cyberspace creators, one of the basic measures to ensure the right to personal data protection is legal framework.

I started to be interested in the problematic aspects of personal data protection under electronic surveillance more than a year prior to E. Snowden leak on massive personal data collection. Seven years have passed since then; however, the question is still relevant as it concerns two equally important public interests: ensuring human right to personal data protection on cyberspace and waving of this right, at the first sight, to protect from even greater threats – terrorism, criminality and national security.

Nevertheless, the line between restriction of this right for the sake of protection of superior values and non-violation of the most important value – democracy – is very thin. The concerns about it are raised in many research papers. But I would like exclude a book written by well-known professor L. K. Donohue and a member of Amici Curia of USA FISA court where the author puts forward a hypothesis that massive electronic surveillance by the USA is analogous to the XIII century law allowing appointed by the Crown persons to break into any private British household at any time, which was eventually recognised as anti-constitutional law[8]. Regardless the threats to ensure the right to personal data protection, which were pointed out by scientist and public participation movements, substantial changes in legal acts have not taken place yet.

Two essential traditional mechanisms, which ensure democracy when the law enforcing authorities and intelligent services are collecting personal information, can be singled out. These mechanisms are materialized as either granting the right to personal data protection or comprehensive regulation on electronic surveillance for law enforcement and intelligence purposes. The former model is applicable in Europe, the latter – in the USA. In the European model, the right to personal data protection is bestowed upon an individual; however, personal data collection for law enforcement and intelligence purposes is regulated in a fragmented way.

In the USA model, the right to personal data protection as such is not directly granted; however, electronic surveillance for law enforcement and intelligence purposes is meticulously regulated by special laws and special courts are established.

---

[6] „NSA Collecting Phone Records of Millions of Verizon Customers Daily“, *The Guardian*, žiūrėta 2020 m. rugpjūčio 30 d., https://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order.

[7] „9/11 Saw Much of Our Privacy Swept aside. Coronavirus Could End It Altogether“, *CNN*, žiūrėta 2020 m. rugpjūčio 30 d., https://edition.cnn.com/2020/05/16/tech/surveillance-privacy-coronavirus-npw-intl/index.html.
„The Price Of Covid-19 Freedom May Be Eternal Spying“, Bloomberg, žiūrėta 2020 m. rugpjūčio 30 d., https://www.bloombergquint.com/view/coronavirus-contact-tracing-apps-mean-spying-end-to-data-privacy.

[8] Laura K. Donohue, *The Future of Foreign Intelligence: Privacy and Surveillance in a Digital Age*, 1 edition (New York: Oxford University Press, 2016), 76.

The aim of such courts is to authorise requests by the law enforcing authorities and intelligence services regarding personal data collection on cyberspace, as well as handling related to this field trials.

Since the USA and European supranational models for personal data collection on cyberspace for law enforcement and intelligence purposes influence legal framework of the remaining states around the world, including Lithuania, analysis of the USA and European supranational legal framework is the objective of this doctoral thesis.

Overview of research in this field. Electronic surveillance for law enforcement and intelligence purposes became an object of scientific research as the right for privacy had extended from physical environment to cyberspace. The question how to ensure the balance between the need of law enforcement authorities and intelligence services to collect personal data on cyberspace and personal data protection, is often raised[9], but has not been answered yet.

As the information about electronic surveillance for law enforcement and intelligence purposes is not publically available, scientific research in this field is affected by the following factors: researcher's geographical location and all the important events related to personal data protection that are available to the public. The interest of European researchers in personal data protection in electronic surveillance was sparked also by leaked information related to the volumes of personal data collection and ongoing electronic surveillance programmes. It also triggered legislation processes. The first bigger wave of researchers interest was in 2013, when the former subcontractor of USA National Security Agency (NSA) E. Snowden, revealed information about PRISM programme[10]. In order to find measures for personal data protection and determine possibilities for usage of *privacy by design* principle in law enforcement activities, several international projects were funded by the European Commission under the Seventh Framework Programme[11]; scientific research papers on legal importance and specifics of personal data protection under electronic surveillance were published[12];

---

[9] Jing Ran, „Striking the Balance between Privacy and Governance in the Age of Technology", 11 (2016): 20.

[10] „NSA Collecting Phone Records of Millions of Verizon Customers Daily", *The Guardian*, žiūrėta 2020 m. rugpjūčio 30 d., https://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order.

[11] „Supporting fundamental rights, PrIvacy and Ethics in surveillaNce Technologies", *Cordis*, žiūrėta 2020 m. rugpjūčio 30 d., https://cordis.europa.eu/project/id/261698.

[12] Pvz., H Akın Ünver, „Politics of Digital Surveillance, National Security and Privacy", 23, žiūrėta 2020 m. rugpjūčio 30 d., https://edam.org.tr/wp-content/uploads/2018/04/Chrest_Surveillance2.pdf. Clive Norris ir kt., *The Unaccountable State of Surveillance: Exercising Access Rights in Europe*, Issues in Privacy and Data Protection (Springer International Publishing, 2017), doi:10.1007/978-3-319-47573-8. Aaron Nance, „Taking the Fear Out of Electronic Surveillance in the New Age of Terror Note", *UMKC Law Review* 70, Nr. 3 (2002 2001): 751–80. "Electronic Surveillance Recent Legislation", *Harvard Law Review* 122, no. 4 (2009 2008): 1271–78. David S. Kris, „The Rise and Fall of the FISA Wall Symposium – Spies, Secrets, and Security: The New Law of Intelligence: The Foreign Intelligence Surveillance Act", *Stanford Law & Policy Review* 17, no. 2 (2006): 487–530. Laura K. Donohue, „FISA Reform", *I/S: A Journal of Law and Policy for the Information Society* 10, no. 2 (2015 2014): 599–640. Stephen I. Vladeck, „The FISA Court and Article III Cybersurveillance in the Post-Snowden Age", *Washington and Lee Law Review* 72, no. 3 (2015): 1161–80. William C. Banks, „The Death of FISA Symposium – 9/11 Five Years On: A Look at the Global Response to Terrorism", *Minnesota Law Review* 91, no. 5 (2007 2006): 1209–1301.

the EU research group was commissioned by the European Commission to draft an overview study on USA privacy protection[13].

The second bigger wave of interest happened when the Court of Justice of the European Union (CJEU), invalidated 'safe habour' principle as the one not ensuring legal personal data protection due to possibilities to use this personal information by USA intelligence agencies[14]. Back then, the majority of researches analysed the decision of the court and the further actions by the EU. Nevertheless, as it is revealed in this doctoral thesis, USA intelligent services have legal rights to collect personal data beyond the USA, thus invalidation of the 'safe harbour' principle does not solve the real problem. This shows a limited scope of the scientific research and the need for a more extensive approach. The third wave of interest is linked to the EU personal data protection reform of 2018[15]. However, the majority of the scientific research under the third wave of interest is linked to commercial side of right to personal data protection, implementation provisions thereof are enshrined in the General Personal Data Protection Regulation[16]. Regardless of a research wave a researcher belongs to, in scientific publications, only separate aspects of individual's right to personal data protection in activities of law enforcing and intelligence agencies are analysed. However, the electronic surveillance law and its restrictions on personal data protection as well as its enforcement mechanisms are complex, and therefore complex research is needed.

The USA law and court precedents are analysed in most of scientific publications on electronic surveillance. The abundance of scientific publications on the regulation of the the USA can be explained by the fact that the the USA is the first country in the world started to regulate electronic surveillance as early as 1968, when cyber space included only telephone conversations and the IV Amendment of the USA Constitution extended the right to privacy from the physical environment to cyber space. In Europe, meanwhile, this was only done in 1981. Following the adoption by the Council of Europe of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, the Recommendations on the Processing of Personal Data for Police Purposes were published in 1987, i.e. 19 years later than

---

[13] Francesca Bignami, „The US legal system on data protection in the field of law enforcement. Safeguards, rights and remedies for EU citizens", *European Parlament*, žiūrėta 2020 m. rugsėjo 10 d., https://www.europarl.europa.eu/thinktank/en/document.html?reference=IPOL_STU(2015)519215

[14] Pvz. Dan Jerker B. Svantesson, „Cross-Border Data Transfers after the CJEU's Safe Harbour Decision: A Tale of Gordian Knots", *Alternative Law Journal* 41, no. 1 (2016): 39–42.

[15] Pvz. Yi-Hsuan Chen, „EU Data Protection Law Reform: Challenges for Service Trade Liberalization and Possible Approaches for Harmonizing Privacy Standards into the Context of GATS, The", *Spanish Yearbook of International Law* 19 (2015): 211–20. Marija Boban, „Digital Single Market and EU Data Protection Reform with Regard to the Processing of Personal Data as the Challenge of the Modern World The Legal Challenges of Modern World", *Economic and Social Development, 16th International Scientific Conference on Economic and Social Development: The Legal Challenges of Modern World* 16 (2016): 191–201. Marina Skrinjar Vidovic, „EU Data Protection Reform: Challenges for Cloud Computing Notes", *Croatian Yearbook of European Law and Policy* 12 (2016): 171–206.

[16] Julius Zaleskis, *Europos Sąjungos bendrasis duomenų apsaugos reglamentas ir asmens duomenų apsaugos teisė: monografija*, Teisinė literatūra (Vilnius: Registrų centras, 2019).

the first legislation in the USA[17]. In the USA, the entire legal framework for electronic surveilance was already in place and is constantly being improved to date. Since its inception in 1968. USA legislation on electronic surveillance has often been the subject of litigation and scientific debate. Therefore, there is ample research on the collection of U.S. personal data in cyberspace for law enforcement and intelligence purposes, usually related to the famous court precedents. However, the focus of U.S. researchers is on what matters in the U.S. and concerns the protection of the privacy of the USA people, not the European population, so researchers focus on the application of the provisions of the Electronic Communications Privacy Act (ECPA)[18]. The provisions of the Foreign Intelligence Surveillance Act (FISA) are analyzed, but mostly only to the extent that they relate to the indirect collection of personal data of U.S. individuals in cyberspace through the collection of data about non-U.S. Individuals[19]. There is very little publicly availible information on Executive Order 12 333, and there is very little research on the subject, although it is now thought that Executive Order 12 333 may be the main legal basis for a mass surveillance[20]. Stanford University 2013-2014 organized online learning on electronic surveillance law in the USA, in which the author of the dissertation also participated. 2015 Thomson Reuters publishes 2-part book "The Law of Electronic Surveillance"[21]. It is the first book of its kind in the USA and in the world in general to provide a unified overview of the legal regulation on electronic surveillance in USA. However, because these books are intended for the USA market, so too

[17] „Council of Europe Committee of Ministers Recommendation No. R(87) 15 to the Member States on regulating the use of personal data in the police sector", *Osce Polis*, žiūrėta 2020 m. rugsėjo 1 d., https://polis.osce.org/council-europe-committee-ministers-recommendation-no-r87-15-member-states-regulating-use-personal.

[18] Deirdre K. Mulligan, „Reasonable Expectations in Electronic Communications: A Critical Perspective on the Electronic Communications Privacy Act The Future of Internet Surveillance Law: A Symposium to Discuss Internet Surveillance, Privacy & (and) the USA Patriot Act: Surveillance, Records & (and) Computers", *George Washington Law Review* 72, Deirdre K. Mulligan, „Reasonable Expectations in Electronic Communications: A Critical Perspective on the Electronic Communications Privacy Act The Future of Internet Surveillance Law: A Symposium to Discuss Internet Surveillance, Privacy & (and) the USA Patriot Act: Surveillance, Records & (and) Computers", *George Washington Law Review* 72, no. 6 (2004 2003): 1557–98. Laura L. Clukey, „The Electronic Communications Privacy Act of 1986: The Impact on Software Communication Technologies Comment", *Software Law Journal* 2, no. 2 (1988 1987): 243–64. Ariana R. Levinson, „Toward a Cohesive Interpretation of the Electronic Communications Privacy Act for the Electronic Monitoring of Employees", *West Virginia Law Review* 114, no. 2 (2012 2011): 461–530. Robert A. Fiatal, „The Electronic Communications Privacy Act: Addressing Today's Technology (Part 1) Legal Digest", *FBI Law Enforcement Bulletin* 57, no. 2 (1988): 25–30. Ariana R. Levinson, „Toward a Cohesive Interpretation of the Electronic Communications Privacy Act for the Electronic Monitoring of Employees", *West Virginia Law Review* 114, no. 2 (2012 2011): 461–530.

[19] William C. Banks, „The Death of FISA Symposium – 9/11 Five Years On: A Look at the Global Response to Terrorism", *Minnesota Law Review* 91, no. 5 (2007 2006): 1209–1301. David S. Kris, "The Rise and Fall of the FISA Wall Symposium - Spies, Secrets, and Security: The New Law of Intelligence: The Foreign Intelligence Surveillance Act", *Stanford Law & Policy Review* 17, no. 2 (2006): 487–530.

[20] Mark Jaycox, „A Primer on Executive Order 12333: The Mass Surveillance Starlet", *Electronic Frontier Foundation*, June 2, 2014, žiūrėta 2020 m. rugsėjo 1 d., https://www.eff.org/deeplinks/2014/06/primer-executive-order-12333-mass-surveillance-starlet. „Reagan-Era Order on Surveillance Violates Rights, Says Departing Aide", *The New York Times*, žiūrėta 2020 m. rugsėjo 1 d., https://www.nytimes.com/2014/08/14/us/politics/reagan-era-order-on-surveillance-violates-rights-says-departing-aide.html. Barton Gellman ir Ashkan Soltani, „NSA Surveillance Program Reaches 'into the Past' to Retrieve, Replay Phone Calls", *Washington Post*, March 18, 2014, sec. National Security, https://www.washingtonpost.com/world/national-security/nsa-surveillance-program-reaches-into-the-past-to-retrieve-replay-phone-calls/2014/03/18/226d2646-ade9-11e3-a49e-76adc9210f19_story.html.

[21] James Carr ir Patricia Bellia, *The Law of Electronic Surveillance, 2017-2 Ed.*, 1 dalis, (Clark Boardman Callaghan, 2017).

is research conducted through the prism of protecting USA individual rights. The provisions of the Foreign Intelligence Surveillance Act apply to non-US individuals, the book provides a very narrow overview, the Executive Order 12 333 and its application practices, or the collection of personal data under the Code of Criminal Procedure 41 Article, which gives the right to hack into a computer or other device of a person of any nationality located anywhere in the world, is not included in the content of this book at all and is not mentioned in it.

The collection of personal data in cyberspace takes place differently than in a physical environment. Therefore, the cooperation of law enforcement and intelligence institutions with business is inevitable, as the data are usually collected not by the law enforcement and intelligence institutions themselves, but by their communication services, cyber service providers, data brokers or electronic surveillance service providers. There is very little data and literature on law enforcement and intelligence cooperation with private companies (business entities), its forms and nature. 2018 in the book "Habeas Data: Privacy vs. the Rise of Surveillance Tech" C. Farivar writes about how technology developed by companies affects intelligence and electronic surveillance capabilities[22]. Privacy international has prepared a study on the growing market for electronic intelligence services[23]. However, none of the works assesses the forms of cooperation between law enforcement, intelligence and business entities and the possibilities of personal data protection and regulatory gaps. I decided the last chapter of the dissertation to answer these questions because the number of cases of co-operation between law enforcement or surveillance institutions with companies increases according to the ENISA[24], while there is no legal regulation or at least coordination proposed yet.

In Lithuania, scientific discussions on electronic surveillance law are also being raised. The following Lithuanian scientists analyzing the relevant provisions of the Law on Criminal Intelligence of the Republic of Lithuania and the Code of Criminal Procedure (hereinafter – CPC) and should be mentioned: D. Štitilis[25], M. Laurinaitis[26], R. A. Petrauskas[27],

---

[22] Cyrus Farivar, *Habeas Data: Privacy vs. the Rise of Surveillance Tech* (Brooklyn: Melville House, 2018).

[23] „The Global Surveillance Industry", Privacy International, žiūrėta 2020 m. rugpjūčio 30 d., https://www.privacyinternational.org/sites/default/files/2017-12/global_surveillance_0.pdf.

[24] Catherine Stupp, „EU agency asks Commission to 'avoid fragmentation' in new cyber security plans", *Euractive*, žiūrėta 2020 m. rugsėjo 1 d., http://www.euractiv.com/section/cybersecurity/news/eu-agency-asks-commission-to-avoid-fragmentation-in-new-cybersecurity-plans/.

[25] Darius Štitilis, „Elektroninių ryšių kontrolės nusikaltimų tyrimo tikslias teisiniai aspektai", *Informacijos mokslai : mokslo darbai* 34 (2005): 103–110. Rimantas Alfonsas Petrauskas ir Darius Štitilis, „Monitoring Electronic Communications: Privacy Issues", *Monitoring, Supervision and Information Technology : Proceedings of the First International Seminar of the Legal Framework for the Information Society (LEFIS) on Monitoring, Supervision and Information Technology, 15 June 2006, Rotterdam*, 2006, 5–20. Darius Štitilis ir Marius Laurinaitis, „IP telefonija – iššūkis elektroninių ryšių kontrolės, siekiant ištirti nusikaltimus, teisiniam reguliavimui", *Socialinių mokslų studijos*, no. 1 (2009): 205–221.

[26] Darius Štitilis ir Marius Laurinaitis, „IP telefonija – iššūkis elektroninių ryšių kontrolės, siekiant ištirti nusikaltimus, teisiniam reguliavimui", *Socialinių mokslų studijos*, no. 1 (2009): 205–221.

[27] Rimantas Alfonsas Petrauskas ir Darius Štitilis, „Monitoring Electronic Communications: Privacy Issues", *Monitoring, Supervision and Information Technology : Proceedings of the First International Seminar of the Legal Framework for the Information Society (LEFIS) on Monitoring, Supervision and Information Technology, 15 June 2006, Rotterdam*, 2006, 5–20.

R. Ažubalytė[28], G. Goda[29], A. Gutauskas[30], R. Jurka[31], L. Belevičiaus[32], P. Pakutinskas[33], A. Panomariovas ir R. Ramanauskas[34], P. Tarasevičius[35], R. Marcinauskaitė[36], M. Civilka ir L. Šlapimaitė[37], J. Dešriūtė[38]. Lithuanian researchers analyze the restriction of private life in electronic communications and IP telephony in criminal investigation in Lithuania. In the author's dissertation, the analysis of regulation in Lithuania for law enforcement and intelligence purposes is based on a comparison with US legal regulation and case law. The dissertation also reviews the legal preconditions of Government Hacking in the Law on Criminal Intelligence of the Republic of Lithuania and the CPC. In her scientific article, R. Ažubalytė analyzes how Lithuanian courts must address the gaps in the CPC and the Law on Criminal Intelligence regarding the electronic surveillance. The historical analysis of US legislation and court precedents performed in the dissertation showed that a similar situation was and is in the USA (Section 2.2. of the dissertation). The world's first law governing electronic surveillance in 1968 appeared as a result of U.S. Supreme Court judgment in *Berger v. New York* in 1967. The historical analysis of the genesis of USA court decisions and legal acts performed in the dissertation may be significant for the courts of the Republic of Lithuania, as they currently have to deal with very similar problems that have been resolved by USA courts.

Another Lithuanian scientist A. Gutauskas discusses about the boundaries of criminal intelligence in accordance with the right to privacy[39]. P. Pakutinskas' doctoral

---

[28] Rima Ažubalytė, „Privataus asmens gyvenimo ribojimas slaptomis priemonėmis: (ne)kokybiško įstatymo problema", *Jurisprudencija* 26, no. 2 (2019): 260–291, doi:10.13165/JUR-19-26-2-02. Rima Ažubalytė, „Baudžiamojo proceso principai: teisės spragų šalinimas", *Lietuvos Respublikos baudžiamojo proceso kodeksui – 10 metų : recenzuotų mokslinių straipsnių, skirtų Lietuvos ir užsienio šalių baudžiamojo proceso, baudžiamosios teisės ir kriminalistikos aktualijoms ir problematikai, rinkinys*, 2012, 13–34

[29] Gintaras Goda, „Procesinių prievartos priemonių Lietuvos Respublikos baudžiamojo proceso kodekso projekte samprata, klasifikacija ir turinys", *Teisė,* (2000): 17–27. Gintaras Goda, *Vertybiniai prioritetai baudžiamajame procese: monografija*, (Vilnius: Registrų centras, 2014).

[30] Aurelijus Gutauskas, „Kriminalinė žvalgyba ir privatus žmogaus gyvenimas", *Teisė* 113 (2019): 8–26, doi:10.15388/Teise. 2019.113.1.

[31] Raimondas Jurka, „Įrodymų perdavimo Europos Sąjungos valstybių narių baudžiamojoje justicijoje iššūkiai ir atradimai", *Jurisprudencija,* (2019, 26(2)), 322.

[32] Linas Belevičius, „Techninių priemonių panaudojimo tiriant nusikaltimus teisinis reglamentavimas", *Jurisprudencija : mokslo darbai* 29 (2002): 72–85.

[33] Paulius Pakutinskas, „Elektroninių komunikacijų teisinio reguliavimo modeliai", (daktaro disertacija, Mykolo Romerio universitetas, 2009).

[34] Artūras Panomariovas ir Ramūnas Ramanauskas, „Slaptumas – tiesos baudžiamajame procese nustatymo priemonė", *Jurisprudencija : mokslo darbai*, no. 75 (2005): 50–57.

[35] Petras Tarasevičius, „Techninių priemonių naudojimo kriminalinėje žvalgyboje teisėtumo problemos", *Teisė*, 2017, 84–99, doi:10.15388/Teise.2017.105.11114.

[36] Renata Marcinauskaitė, „Nusikalstamos veikos elektroninėje erdvėje", (daktaro disertacija, Mykolo Romerio universitetas).

[37] Mindaugas Civilka ir Lina Šlapimaitė, „Asmens duomenų samprata elektroninėje erdvėje", *Teisė*, 96 (2015): 126–148.

[38] Justina Dešriūtė, „Esminiai asmens duomenų apsaugos baudžiamajame procese reformos Europos Sąjungoje aspektai ir jų įtaka nacionaliniam teisiniam reguliavimui", *Teisės problemos*, 1 (91), (2016): 25–51.

[39] Aurelijus Gutauskas, „Kriminalinė žvalgyba ir privatus žmogaus gyvenimas", *Teisė* 113 (2019): 8–26, doi:10.15388/Teise.2019.113.1.

dissertation "Models of Legal Regulation of Electronic Communications"[40] is the closest to the author's dissertation. In his dissertation, P. Pakutinskas analyzed the models of legal regulation of electronic communications[41], but his dissertation does not cover the issues of legal protection of personal data, which are the object of this dissertation.

Novelty and significance of the research. This dissertation is the first scientific study where the laws on electronic surveillance of countries of common (USA) and continental (Lithuanian) law traditions and supranational regulation level (CoE and EU) are analyzed. As it is reviled in a dissertation, although there are shortcomings in USA regulation (for example, the right to personal data protection applies only to USA people, so other individuals or their personal data do not fall are not protected. Consequently, leading to mass collection of non-USA personal data to be legally justified), however, since 1968 not only the laws on electronic surveillance are constantly amended but also the court rulings has impact on the legislation in this field.

The research results also show that the impact of EU and CoE regulation on personal data protection in electronic surveillance is minimal. The main advantage this regulation is enactment of the right to privacy and data protection at supranational level and judicial interpretation of the legality and reasonableness of restrictions this right. Regulation of electronic surveillance in Lithuania is episodic and not clear. Therefore, the historical analysis of regulation on electronic surveillance in USA, the jurisprudential doctrine of USA and supranational court was essential for comparison with regulation and helped to find the gaps in Lithuanian laws as well as propose the improvement.

The object of the research is the legal regulation of electronic surveillance for law enforcement and intelligence purposes.

Research problem consists of fallowing questions:

1. How to regulate electronic surveillance for law enforcement and intelligence purposes and guarantee the right to personal data protection to individuals?
2. Which elements of regulation of electronic surveillance in USA and other countries could be adopted in Lithuanian laws?
3. How the regulation of CoE and EU on electronic surveillance influence legal practice in Lithuania?
4. Why and how the USA regulation on electronic surveillance restricts the right to personal data protection of Lithuanian citizens?
4. How the cooperation between law enforcement and intelligence institutions with private legal entities on electronic surveillance influence the implementation of right to personal data protection?

The objective of research was to analyze the peculiarities of the legal regulation on electronic surveillance for the purposes of law enforcement and intelligence and to identify good practice examples that could improve Lithuanian laws.

---

[40] Petras Tarasevičius, „Techninių priemonių naudojimo kriminalinėje žvalgyboje teisėtumo problemos", *Teisė*, 2017, 84–99, doi:10.15388/Teise.2017.105.11114.

[41] Paulius Pakutinskas, „Elektroninių komunikacijų teisinio reguliavimo modeliai", (daktaro disertacija, Mykolo Romerio universitetas, 2009), 7.

Tasks:

1. To evaluate the regulation on electronic for law enforcement and intelligence purposes in common law country (case of the USA) and to identify the good practice of this regulation that could be adopted in Lithuanian regulation;
2. To evaluate the regulation of the collection of personal data in cyberspace for law enforcement and intelligence purposes at the supranational level (European case);
3. To evaluate the regulation on electronic for law enforcement and intelligence purposes in continental law country and identify the relation with the right to the protection of personal data (the case of Lithuania);
4. To identify the forms of dispositive cooperation of law enforcement and intelligence institutions with private legal entities and evaluate problematic aspects of ensuring the right to personal data protection.
5. Taking into account the analyzed examples of good practice, to prepare proposals for the improvement of the regulation on electronic surveillance for law enforcement and intelligence purposes in Lithuania.

Statements to defense:

1. Current legal regulation on electronic surveillance for law enforcement and intelligence purposes in Lithuania does not ensure the restriction on the right to personal data protection to be in accordance with the requirements ensuring this right not to be obeyed because of the lack of proper regulation for collection of meta data, historical personal data and law enforcement hacking as well as existing gaps allowing to overcome judicial oversight.
2. Adoption of good practice from regulation of electronic surveillance in USA and regulation of government hacking in Germany, UK, Poland, Italy, the Netherlands and France to Lithuanian laws would make the provisions of CPC and the Law of Criminal Intelligence of the Republic of Lithuania more precisely defined, transparent, clear and in accordance with the requirements of ECHR, the Charter of Fundamental Rights of the European Union and the Constitution of the Republic of Lithuania where the legitimate grounds for restricting the right to the protection of personal data are stipulated.
3. At EU and CoE level, the regulation of electronic surveillance is currently limited to granting of a right to the protection of personal data, which was extended by ECtHR and the CJEU to the cyber space. Lithuanian courts follow the case law of the ECtHR and the CJEU in assessing the necessity of restricting the right to protection of personal data. However, Lithuanian legislation is only partially in line with ECtHR and the CJEU case law on the clarity of the law restricting the right to personal data protection, the proportionality and necessity of this restriction.
4. The regulation of electronic surveillance for law enforcement and intelligence purposes in the US legislation guarantees the right to personal data protection only for USA persons. Therefore the personal data of Lithuanian residents can be legally collected for US intelligence purposes in accordance with FISA and EO 12 333 legal acts regardless of the person's physical location in Lithuania.

5. When law enforcement and intelligence authorities collect personal data in the cyber space on the basis of a dispositive, non-public cooperation agreement with private legal entities, the exercise of the right to personal data protection depends on the choice of contract law and personal data protection provisions. This makes an opportunity to abuse the restriction of the right to protection of personal data.

Methodology. Different research methods were used while conducting research and writing a dissertation. The relevant data for the dissertation were collected in accordance with the methods of *analysis of legal documents, analysis of scientific literature, unstructured and structured interviews of experts, monitoring*. The collected data were processed using the following theoretical methods: *systematic, historical and comparative analyses*.

The method of analysis of legal documents was used to analyze the laws of the USA, EU, CoE and Lithuania. The purpose of this method was to investigate the past and present legal regulation of the electronic surveillance in the USA, the EU, the CoE and Lithuania. Since in countries with common law traditions the court precedents are very important, therefore a qualitative study of USA court precedents was significant in assessing and interpreting laws, their amendments, practical application ensuring the right to privacy enshrined in the 4th Amendment of USA Constitution. The decisions of the USA courts are also important for the dissertation from a comparative point of view, as some provisions of the current Lithuanian laws are similar to the previous ones in the USA which were amended on the basis of court decisions. The decisions of the ECtHR and the CJEU on the right to personal data protection were significant for the interpretation of the validity and limitations of the right to the protection of personal data enshrined in the ECHR and the European Charter of Human Rights. Lithuanian court rulings helped to point out and clarify the issues related to practical application of the Law on Criminal Intelligence and the provisions of the CPC on electronic surveillance.

The method of analysis of scientific literature was used to reveal the views of USA and European researchers and the results of their research on the implementation of the right to personal data protection in electronic surveillance, amendments to legislation in this area and their impact to ensuring the right to personal data protection. An analysis of the scientific literature also helped to explain why intelligence agencies can legally collect data on aliens, including the collection of personal data cyber space. Author of dissertation noticed a tendency that while ensuring the right to the protection in electronic surveillance is a global problem, most of the scientific literature is focused on ensuring this right at the national level.

Due to the rapid technological development of the cyberspace, the legal regulation in this field is dynamic and influenced by the decisions of politicians and powerful technological companies (Facebook, Google, Apple, etc.). Since the dissertation analyzes global trends, therefore the *monitoring method* was applied in order to have relevant information on a topic and to be able to predict future changes or the need for those changes. The subject of monitoring was the global newspapers and portals *Fi-*

nancial Times, The Economist, The Guardian, Reuters, politico.eu, Massachussets Technology Review (MIT) magazine.

The method of unstructured interviews was applied to identify problematic aspects of regulation in Lithuania. An unstructured interview was conducted with six experts with different experiences on a research object. Due to the sensitivity of the dissertation topic, experts had the opportunity to remain anonymous and the content of the interview not to be disclosed. Therefore, the identities of the four experts cannot be revealed, the remaining two are professor of Vytautas Magnus University, Lithuania's representative in the NATO STO working group prof. dr. Tomas Krilavičius and Alius Navickas from Financial Crime Investigation Service. During the interviews, all experts were asked different questions in accordance with their expertise. The author also discussed with fallowing foreign researchers on her research topic: ESSCA School of Management prof. dr. Ana Dimitrova, senior data protection specialist at Europol dr. Jan Ellermann, IBM Q Ambassador dr. Piotr Biskupski, founder of the Mysterium Network Robert Višinskis. The dissertation is based only on non-confidential information.

The purpose of *the structured interview method* was to evaluate the trends and problematic aspects of application of Art 154 of CPC in practice. During the structured interview, 22 investigators seconded by the pre-trial investigation institutions themselves were interviewed. Inquire to participate at the structured interview were sent to all pre-trial investigation authorities of Lithuania by e-mail. However, only seven of which agreed to participate in the research: Special Investigation Service, Financial Crime Investigation Service, Customs Criminal Service, Vilnius County Chief Police Commissariat, Vilnius County Chief Police Commissariat Criminal Police Organized Crime Investigation Board, Kaunas County Chief Police Commissariat and Utena County Chief Police Commissariat. All respondents were asked the same questions. The research results are used in the 4.1.1. subsection of the dissertation.

The nature of the research object, different factors influencing the legal regulation of electronic surveillance (different national legal regulations, court decisions, political factors, the role of technological companies and other) presupposed that a systematic approach to the research object was needed.

The method of *systematic analysis* was applied. The *method of historical research* helped to determine the doctrinal basis of electronic surveillance, the evolution of legal regulation and the factors influencing it. The chapters of the dissertation are also arranged in historical chronological order from the oldest developed legal regulation to the most recent (USA, CoE, EU and Lithuania). The *comparative method* was used throughout all the study. It was also used in the preparation of the proposals on legal regulation of electronic surveillance in Lithuania.

As the legal regulation of electronic surveillance originated in the USA and is the most developed, and as the vast majority of EU citizens' data travel through the USA, are stored in USA servers, or belongs to the USA companies, while Coe and EU influence the trends of legal regulation in Lithuania, the comparative approach was used to compare the provisions of legal regulation in USA, CoE, EU with Lithuanian legislation and case law.

CONCLUSIONS

1. The law applicable to personal data in cyberspace is determined not by the law of the location of the natural person, but by the route of personal data in it, the location of servers where personal data is stored and the ability of private companies to store, take over and provide the information required by law enforcement and intelligence institutions as well as the applicable laws or contractual provisions.
2. Meanwhile, the validity of the right to personal data protection under the current regulatory model depends on completely different things: the law of the place of residence of the natural person and the provisions of supranational and national legislation in force in the countries. Thus, the problem of ensuring the right to personal data protection arises from the fact that a person and his electronic personal data are generally subject to different legal regimes.
3. Currently there are three models of regulation of electronic surveillance: 1) supranational, 2) common law, and 3) continental law traditions models. These models exist at different levels: at the *macro* level there is supranational regulation of the EU and CoE, *micro* – USA (as a state of common law traditions) and Lithuania (as a state of continental law traditions) regulation. Only with the advent of *meta* level (global) regulation (in the form of an international treaty or agreement) is it possible to guarantee the right to the protection of personal data, as the cyberspace itself is global (*meta* level).
4. The model of common law traditions, exemplified by US regulation, is characterized by detailed regulation and differentiation:
   4.1. individuals are divided into USA and non-USA persons. IV Amendment of the USA Constitution guarantees the right to privacy and, at the same time, the protection of personal data only to USA persons within USA territory. Consequently, all the rest of the world's population in the USA legal system is not entitled to the protection of personal data, regardless of whether they have it under national or supranational laws;
   4.2. the electronic surveillance for law enforcement purposes is regulated by the ECPA, which sets out different procedures and levels of protection of personal data depending on whether content or non-content data (metadata) is collected and whether the data is real-time or historical nature;
   4.3. judicial oversight of electronic surveillance is compulsory but the requirements to apply for grant court orders differs for different type of personal data;
   4.4. the collection of personal data in cyberspace for intelligence purposes is governed by FISA and EO 12 333. FISA applies when at least one item is in the USA or travels through US territory – a non-USA person or his or her personal data. EO 12 333 applies when neither the person, nor his or her data is in USA.

Thus, although the role courts is very important in common law countries, the courts have limited powers because of differentiated legal regulation.

5. The continental European model for electronic surveillance should be characterized by integration, but:
   5.1. integration does not take place through supranational legal regulation, but through the jurisprudence developed by the ECtHR and the CJEU;
   5.2. although the CoE is taking the initiative to ensure the right to the personal data protection in electronic surveillance and is currently developing an Electronic Intelligence Code, however, CoE is not in a position to develop and ensure a *de facto* rather than declarative mechanism as long as the code will not have the status of an international treaty and will not be accepted by the major states, which conduct intelligence in the cyber space on a large scale;
   5.3. at EU level, the electronic surveillance is not regulated by special laws. Intelligence is exemption from EU law, so the regulation on electronic surveillance depends on the decisions on each Member States. Electronic surveillance for law enforcement purposes at the time of writing is also not regulated, although the draft E-evidence directive is prepared. The specific provisions on electronic surveillance is not subject to Directive on the processing of personal data for law enforcement purposes space.
6. The regulation of electronic surveillance in Lithuania is currently unstructured. Special norms for electronic surveillance regulate only the real-time collection of personal data from electronic communications service providers, which until The Electronic Communications Code of 2018, as interpreted by the CJEU, did not cover non-telecommunications service providers. The collection of historical personal data is carried out in accordance with the common provisions of the CPC and the Law on Criminal Intelligence which are not designated to regulate electronic surveillance. Such regulation is only partially in line with the case law of the ECtHR on the lawful restrictions of the right to privacy and personal data protection and does not provide sufficient guarantees for preventing the abuse. On the other hand, if Lithuanian laws on electronic surveillance would be amended fallowing the examples of good regulatory practice in the USA, it would comply with the requirements for the justified restriction of the right to personal data protection.
7. The lawfulness of restriction of the right to personal data protection depends on judicial oversight. Judicial oversight is compulsory in accordance to Article 22 of the Constitution of the Republic of Lithuania and ECtHR jurisprudence. However, judicial oversight of electronic surveillance is not always required according to Lithuanian laws. Judicial oversight does not apply for electronic surveillance under Article 97 of CPC. Also, the Article 155 of CPC requires only formal judicial approval while Article 22 of the Constitution of the Republic of Lithuania sets out the requirement to motivate the court order.
8. The is no specific provisions for electronic surveillance of stored personal data in CPC. Therefore, law enforcement institutions collect stored personal data on the basis of Articles 97, 145, 147 and 155 of CPC. Mentioned articles of CPC is not designated to collect personal data. Therefore, the requirements for

lawful restriction of the right to privacy and personal data protection are not reinforced. This regulatory gap makes collection of stored personal data for law enforcement purposes not in accordance with Article 22 of the Constitution of the Republic of Lithuania, Article 8 of ECHR and Article 7 of the Charter of Fundamental Rights of the European Union

9. Real time electronic surveillance under the Article 154 of CPC is possible for investigation of limited number of crimes. Contrary, electronic surveillance of stored personal data under the Articles 97, 145, 155 is not limited by precise crime list. This does not meet the ECtHR jurisprudence on proportionality of restriction of right to privacy enshrined in Article 8 of ECHR. Thus, the Article 154 of CPC should be amended to regulate both real time and stored data electronic surveillance. Consequently, the same rules would apply for electronic surveillance leaving no grounds for abusing the power of law enforcement institutions.
10. Article 154(6) of CPC and Article 9(7) of the Law on Criminal Intelligence sets the possibility to collect personal data upon the consent a person with no judicial authorization required if the services and equipment of electronic communications providers are not used. The procedures and a scope of personal data collection upon any person's consent is not regulated by Article 154(6) of CPC and Article 9(7) of the Law on Criminal Intelligence. Such judicially unauthorized collection of personal data violates Article 22 of the Constitution of the Republic of Lithuania. This provision of the CPC and the Law on Criminal Intelligence should be repealed.
11. Despite that the government hacking restricts the right to privacy and personal data protection the most of all the methods of electronic surveillance, there is no special provisions in CPC and the Law on Criminal Intelligence to regulate it. Consequently, government hacking should be enacted as a special a measure of procedural coercion in CPC and a special measure of gathering information for criminal intelligence in the Law on Criminal Intelligence.
12. The is no judicial authorization required for electronic surveillance under in the Law on Criminal Intelligence if the data is collected from 1) legal persons and 2) upon a consent of a person. Such unauthorized collection of personal data violates Article 22 of the Constitution of the Republic of Lithuania.
13. Lithuanian intelligence institutions may conduct electronic surveillance for the intelligence and counter-intelligence purposes. These goals mean that intelligence institutions operate either in Lithuania or outside the territory of Lithuania. The Constitution of the Republic of Lithuania guarantees the right to privacy as well as the jurisdiction of Lithuanian courts applies only in the territory of Lithuania or only for Lithuanian citizens. Despite this, regulation of electronic surveillance for intelligence and counter-intelligence purposes is the same.
14. The Law on Intelligence does not classify the need for judicial authorization of electronic surveillance according to the purpose of the activity – intelligence or counter-intelligence – but according to whether metadata or content data is being collected. This is not in a line with Article 8 of the ECHR and Article 22 of

the Constitution of the Republic of Lithuania because metadata is also personal data. Hence, the collection of personal data for counter-intelligence purposes should be authorized by court, for intelligence purposes – by the State Defense Council.

15. Ensuring the right to personal data protection depends on the forms and purposes of law enforcement and surveillance institutions with private legal persons: 1) in the case of cooperation based on a contract, the choice of the applicable law is the subject of an agreement. Therefore, there might be only minimal guarantees for the personal data protection in a contract or no guarantees at all; 2) in the case of voluntary cooperation, requests from law enforcement are reassessed by a private legal entities and the personal data is not always provided.

PUBLICATIONS

1. Kurapka, Vidmantas Egidijus, Matulienė, Snieguolė, Stankevičiūtė, Sigutė. *The role of data protection reguliation for a proper implementation of vision for European forensic science 2020* // Political sciences, law, finance, economics and tourism : conference proceedings, 26 August – 1 September, 2015 Albena, Bulgaria. Vol. I : Political sciences, law.- (International multidisciplinary scientific conference on social sciences and arts. SGEM 2015, ISSN 2367- 5659). Sofia: STEF92 Technology Ltd, 2015. ISBN 9786197105469. p. 805-812. [Conference Proceedings Citation Index - Science (Web of Science)] [M.kr.: S 001].
2. Stankevičiūtė, Sigutė. *JAV naudojamų kriminalistinių nusikalstamų veikų tyrimo ir užkardymo bei žvalgybos metodų santykis su Europos žmogaus teisių konvencijos ir Europos Sąjungos pagrindinių teisių chartijos garantuojama teise į asmens duomenų apsaugą.* Kriminalistika ir teismo ekspertologija : mokslas, studijos, praktika = Criminalistics and forensic examination : science, studies, practice = Криминалистика и судебная экспертология: наука, обучение, практика. [T.] XIII. Vilnius: Lietuvos teismo ekspertizės centras, 2017.
3. Stankevičiūtė, Sigutė. *Application of the Directive on personal processed for law enforcement purposes to the collection of personal data in cyber space.* Kriminalistika ir teismo ekspertologija: mokslas, studijos, praktika = Criminalistics and forensic examination : science, studies, practice = Криминалистика и судебная экспертология : наука, обучение, практика. [T.] XIII. Vilnius : Lietuvos teismo ekspertizės centras, 2018.

CURICULUM VITAE OF SIGUTĖ STANKEVIČIŪTĖ

Education

2013–2020	PhD degree in Law, Mykolas Romeris University, Thesis "Legal Regulation of Electronic Surveillance".
2010–2012	Master degree in Law (Criminal Law and Criminology), Mykolas Romeris University. Master thesis is about criminalization of terrorism in Criminal Code of the Republic of Lithuania.
2006–2010	Bachelor degree in Law, Mykolas Romeris University.

Sertification

2017 m.	Data protection officer certification, Maastricht University
2015 m.	Electronic surveillance Law, Stanford University

Languages

Mother Tong	Lithuanian.
C1	English.
B1	Russian

Work experience

02-11-2020–current Defense Innovation Center of General Jonas Žemaitis Military Academy of Lithuania
www.lka.lt
– Advisor.

01-07-2020–current Fintech startup UAB "Analitika ir co"
http://dicheck.eu/en
– Legal expert.

01-07-2012-01–07-2020 Agency for Science, Innovation and Technology (MITA)
www.mita.lrv.lt

Job titles:
legal expert on innovation, project manager, data protection officer

Roles:
Creation of national strategies, management of R&D projects and international cooperation programs

Legal expertise:
- Drafting national policies, laws, programs and projects;
- Supervision of national strategic R&D projects in public sector (including defence and national security sectors);
- National expert on pre-commercial procurement and innovation procurement;

– Legal expert on data protection, intellectual property protection, clusterization;
– Data protection officer.

International project management

– "innovation by developing a European Procurer Networking for security research services (iprocureNet) – **H2020** Project manager and national representative (2018–2020);
– "Collaborative Innovation Procurement Action to Improve the Efficiency, Quality and Sustainability of Healthcare" – **COSME** project manager and senior expert (2019–2020).

National project management

– "Promotion of innovation procurement and pre-commercial procurement" – Project manager (2016–2020).

International relations

– National contact point for cooperation with NASA;
– National contact point for cooperation with China on R&D.

Coordinator of strategic national R&D projects (2016–2020):

– Bank of Lithuania "LB Chain sandbox";
– Ministry of Defense "Day-night surveillance device";
– Centre of Registers "Creation technology for development, storage and management of spatial 3D (3D) data necessary for the effective implementation of economic development projects";
– Military academy "Establishment of a National Ecosystem for Information Impact Recognition and Analysis (NAAS)";
– Kaunas City Municipality "Measurement of transport flows in real time using innovative technologies in order to manage the situation of traffic jams in the city";
– Kaunas City Municipality "Development and testing of intelligent transport management systems (rechargeable hybrid drives for controlling vehicle power mechanisms)";
– Lithuanian Sea Museum "Development and integration of research-based animal therapy in the concept of holistic medical health";
– Lithuanian Road Administration "Creation of nanomaterial modified asphalt mix to enhance road surface sustainability";
– Vilnius City Municipality "Humanization of the public environment by rationalizing traffic in the central part of the city";
– Vilnius University Hospital Santaros Klinikos "Development of intelligent high-resolution lighting system for the surgery";
– Vilnius University Hospital Santaros Klinikos "Development of technology for creation of braces in innovative way" and etc.

Lecturing

– Pre-commercial procurement and innovation procurement (2017–2020).

11-02-2011–01-07-2011 Law Firm SORAINEN
– Legal assistant in company law.

09-08-2010–31-01-2011 Ugniaus Pėdnyčios Law Firm
– Legal assistant.

28-09-2009–11-06-2010 Law Firm Valiūnas Ellex (Lawin)
– Legal assistant in Fintech law and litigation.

Research experience

2014–2016 Mykolas Romeris University
www.mruni.eu
Project "Scientific approach on implementation of European Forensic Science Vision in Lithuania", funded by Lithuanian Research Council
– Junior researcher on implementation of European Forensic Science vision 2020, focused on fight against terrorism, cybercrime, organized crime, electronic surveillance.

2014–current
1. Bilevičiūtė, Eglė; Juodkaitė-Granskienė, Gabrielė; Kurapka, Vidmantas Egidijus; Malevski, Hendryk; Matulienė, Snieguolė; Navickienė, Žaneta; Stankevičiūtė, Sigutė. *Europos kriminalistikos bendros erdvės 2020 vizijos įgyvendinimo Lietuvoje mokslinė koncepcija : mokslo studija* / atsak. red.: Vidmantas Egidijus Kurapka, Hendryk Malevski, Snieguolė Matulienė. Vilnius : Mykolo Romerio universitetas, 2016. 372 p. ISBN 9789955198451. [M.kr.: S 001] 1.
2. Kurapka, Vidmantas Egidijus; Matulienė, Snieguolė; Stankevičiūtė, Sigutė. *The role of data protection reguliation for a proper implementation of vision for European forensic science 2020* // Political sciences, law, finance, economics and tourism : conference proceedings, 26 August – 1 September, 2015 Albena, Bulgaria. Vol. I : Political sciences, law.- (International multidisciplinary scientific conference on social sciences and arts. SGEM 2015, ISSN 2367- 5659). Sofia : STEF92 Technology Ltd, 2015. ISBN 9786197105469. p. 805-812. [Conference Proceedings Citation Index – Science (Web of Science)] [M.kr.: S 001].
3. Kurapka, Vidmantas Egidijus; Matulienė, Snieguolė; Bilevičiūtė, Eglė; Stankevičiūtė, Sigutė; Drakšas, Romualdas. *The current reforms on forensic science: international experience and first steps in Lithuania // International journal of academic research*. Baku: [Progress IPS LLC]. ISSN 2075-4124. 2014, vol. 6, no 6, p. 472-476. DOI: 10.7813/2075-4124.2014/6-6/B.69. [Zoological Record; Academic Search Complete] [M.kr.: S 001]

4. Bilevičiūtė, Eglė; Kurapka, Vidmantas Egidijus; Matulienė, Snieguolė; Stankevičiūtė, Sigutė. *The conception of implementation of vision for European forensic science 2020 in Lithuania* // International journal of social, management, economics and business engineering / World Academy of Science, Engineering and Technology. Canakkale : World Academy of Science, Engineering and Technology. ISSN 2010-376X. 2014, Vol. 8, no. 6, p. 1790-1798. [CSA Technology Research Database; Science in Context] [M.kr.: S 001].
5. Kurapka, Vidmantas Egidijus; Bilevičiūtė, Eglė; Matulienė, Snieguolė; Stankevičiūtė, Sigutė. *Creating a conception of the vision for european forensic science 2020 implementation in Lithuania* // 10 gadi Eiropas Savienībā – sasniegumi, problēmas un nākotnes ieceres: XV starptautiskā zinātniskā konference: Biznesa augstskolas Turība konferenču rakstu krājums = 10 Years in the European Union – achievements, problems and expectations: XV international scientific conference: proceedings of the conference of Turiba University: Rīga 2014. gada 29. maijs. Rīga: Biznesa augstskolas Turība. ISSN 1691-6069. 2014, P. 309-319. [M.kr.: S 001].
6. Kurapka, Vidmantas-Egidijus; Bilevičiūtė, Eglė; Matulienė, Snieguolė; Stankevičiūtė, Sigutė. *Europos kriminalistikos 2020 vizijos įgyvendinimo Lietuvoje mokslinė koncepcija: problemų medis = The conception of implementation of vision for European forensic science 2020 in Lithuania: the tree of problem*s // Kriminalistika ir teismo ekspertologija: mokslas, studijos, praktika = Criminalistics and forensic examination: science, studies, practice = Криминалистика и судебная экспертология: наука, обучение, практика. [T.] XI. Vilnius: Lietuvos teismo ekspertizės centras, 2015. ISBN 9789986555421. P. 453-456. [M.kr.: S 001]
7. Bilevičiūtė, Eglė; Kurapka, Vidmantas Egidijus; Matulienė, Snieguolė; Stankevičiūtė, Sigutė. *The current reforms on forensic science : international experience and first steps in Lithuania* // SOCIN 2014 : international interdisciplinary conference on social innovations „Social Innovations : theoretical and practical insights 2014“: conference abstracts : October 23-24, 2014 [Elektroninis išteklius] / Mykolas Romeris University. Vilnius : Mykolas Romeris University, 2014. ISBN 9789955196839. P. 56-57. [M.kr.: S 001]

8. Stankevičiūtė, Sigutė. *JAV naudojamų kriminalistinių nusikalstamų veikų tyrimo ir užkardymo bei žvalgybos metodų santykis su Europos žmogaus teisių konvencijos ir Europos Sąjungos pagrindinių teisių chartijos garantuojama teise į asmens duomenų apsaugą.* Kriminalistika ir teismo ekspertologija : mokslas, studijos, praktika = Criminalistics and forensic examination : science, studies, practice = Криминалистика и судебная экспертология: наука, обучение, практика. [T.] XIII. Vilnius: Lietuvos teismo ekspertizės centras, 2017.
9. Stankevičiūtė, Sigutė. *Application of the Directive on personal processed for law enforcement purposes to the collection of personal data in cyber space.* Kriminalistika ir teismo ekspertologija: mokslas, studijos, praktika = Criminalistics and forensic examination : science, studies, practice = Криминалистика и судебная экспертология : наука, обучение, практика. [T.] XIII. Vilnius : Lietuvos teismo ekspertizės centras, 2018.

Stankevičiūtė, Sigutė

ASMENS DUOMENŲ RINKIMO ELEKTRONINĖJE ERDVĖJE TEISĖSAUGOS IR ŽVALGYBOS TIKSLAIS REGLAMENTAVIMAS: daktaro disertacija. – Vilnius: Mykolo Romerio universitetas, 2020. P. 376.

Bibliogr. 265–324 p.

Disertacijos rašymo metu atlikto tyrimo tikslas – ištirti teisinio asmens duomenų rinkimo elektroninėje erdvėje teisėsaugos ir žvalgybos tikslais teisinio reglamentavimo ypatumus bei išskirti gerosios praktikos pavyzdžius pagal kuriuos būtų galima tobulinti Lietuvos teisės aktus. Chronologine tvarka disertacijoje yra analizuojama bendrosios teisės tradicijų (Jungtinių Amerikos Valstijų), supranacionalinio lygmens (Europos Tarybos ir Europos Sąjungos) ir kontinentinės teisės tradicinių (Lietuvos) asmens duomenų rinkimo elektroninėje erdvėje teisėsaugos ir žvalgybos tikslais reglamentavimas. Pagrindinė mokslinio tyrimo išvada – asmens duomenų rinkimo elektroninėje erdvėje teisėsaugos ir žvalgybos tikslais reglamentavimas Lietuvos teisės aktuose neatitinka teisėtam teisės į asmens duomenų apsaugą suvaržymui keliamų reikalavimų.

The objective of research was to analyze the peculiarities of the legal regulation on electronic surveillance for the purposes of law enforcement and intelligence and to identify good practice examples that could improve Lithuanian laws. The regulation of electronic surveillance in common law (the case of United States), at a supranational level (the case of Council of Europe and European Union) and continental law (the case of Lithuania) is analyzed in dissertation in chronological sequence. The main conclusion of a research is that the regulation of electronic surveillance in Lithuanian laws does not comply with the requirements for lawful restriction of the right to personal data protection.

Sigutė Stankevičiūtė

ASMENS DUOMENŲ RINKIMO ELEKTRONINĖJE ERDVĖJE TEISĖSAUGOS IR ŽVALGYBOS TIKSLAIS REGLAMENTAVIMAS

Daktaro disertacija
Socialiniai mokslai, teisė (S 001)

Mykolo Romerio universitetas
Ateities g. 20, Vilnius
Puslapis internete www.mruni.eu
El. paštas roffice@mruni.eu
Tiražas 20 egz.

Parengė spaudai leidykla „Žara“

Spausdino BĮ UAB „Baltijos kopija“
Kareivių g. 13B, 09109 Vilnius
spauda@kopija.lt
http://kopija.lt