

TARTU ÜLIKOOL
ÕIGUSTEADUSKOND
Eraõiguse osakond

Markus Laja

**USA UUE ANDMEKAITSERAAMISTIKU ALUSEL TEOSTATAVA
SIGNAALLUURE VASTAVUS EUROOPA LIIDU POOLT NÕUTAVALE
ANDMEKAITSE TASEMELE ATLANDI-ÜLESE ISIKUANDMETE
EDASTAMISE KONTEKSTIS**

Magistritöö

Juhendajad
PhD Aleksei Kelli
MA Margot Arnus

Tallinn
2023

SISUKORD

SISSEJUHATUS.....	4
1. Atlandi-ülene isikuandmete edastamine	10
1.1. Õiguslik alus isikuandmete edastamiseks EL-ist kolmandatesse riikidesse	10
1.1.1. GDPR-i artikkel 45 – edastamine adekvaatsusotsuse alusel	11
1.1.2. GDPR-i artikkel 46 – edastamine asjakohaste kaitsemeetmete kohaldamisel ..	13
1.1.3. GDPR-i artikkel 49 – erandid konkreetsetes olukordades	14
1.2. EL-i ja USA erinevad lähenemised andmekaitsele	15
1.2.1. Andmekaitse kui põhiõigus EL-i kontekstis	15
1.2.2. USA privaatsusõigus	16
1.3. Ülevaade USA privaatsusõiguse ja signaalluuretegevuse vahekorra-	19
1.3.1. Edward Snowdeni paljastused USA luuretegevuse kohta	19
1.3.2. Signaalluure teostamist võimaldavad õigusaktid.....	20
1.3.2.1. FISA paragrahv 702	20
1.3.2.2. Korraldus EO 12333	23
1.3.3. Signaalluure teostamist piiravad õigusaktid	24
1.3.3.1. Poliitikasuunis PPD-28	24
1.3.3.2. Korraldus EO 14086	26
1.4. USA poolt varasemad loodud andmekaitseraamistikud andmevahetuseks EL-iga ja seonduvad Euroopa Kohtu lahendid.....	30
1.4.1. Safe Harbor ja Euroopa Kohtu lahend <i>Schrems</i>	30
1.4.2. Privacy Shield ja Euroopa Kohtu lahend <i>Schrems II</i>	33
2. USA uue andmekaitseraamistiku vastavus Euroopa Andmekaitsevennukogu tagatistele ..	39
2.1. Euroopa olulised tagatised	39
2.2. Tagatis A – kas töötlemine põhineb selgetel, täpsetel ja ligipäätavatel eeskirjadel?	40
2.2.1. EL-i õiguse nõuded	40
2.2.2. USA andmekaitse tase	41
2.2.3. Vahejärelalus.....	43

2.3. Tagatis B – kas signaalluurega taotletavad seaduslikud eesmärgid on vajalikud ja proportsionaalsed?.....	43
2.3.1. EL-i õiguse nõuded	43
2.3.2. USA andmekaitse tase	45
2.3.3. Vahejärelalus.....	51
2.4. Tagatis C – kas USA andmekaitseraamistik tagab sõltumatu järelevalvemehhanismi?	52
2.4.1. EL-i õiguse nõuded	52
2.4.2. USA andmekaitse tase	53
2.4.3. Vahejärelalus.....	59
2.5. Tagatis D – kas eurooplastele on nende õiguste rikkumise korral tagatud tõhusad õiguskaitsevahendid?.....	59
2.5.1. EL-i õiguse nõuded	59
2.5.2. USA andmekaitse tase	60
2.5.3. Vahejärelalus.....	67
2.6. Järeldus USA andmekaitse taseme kohta.....	68
KOKKUVÕTE	71
Abstract	75
LÜHENDID	82
KASUTATUD MATERJALIDE LOETELU	85

SISSEJUHATUS

USA on Euroopa Liidu (edaspidi ka „EL“) suurim kaubanduspartner: 2021. aastal eksportis USA Euroopasse 283 miljardi dollari eest digitaalteenuseid.¹ USA ja EL-i vahelistele suhetele viidatakse mõnikord ka terminiga „Atlandi-ülene“, mis tähistab midagi USA ja EL-i vahelist.² Tänapäeval on USA suuretevõtete poolt Atlandi-ülese andmeedastuse kaudu pakutavad elektroonise side ja sotsiaalmeedia teenused nagu nt Gmail, Facebook, Instagram jt saanud suureks osaks meie igapäevaelust. Ligi aasta aega tagasi ähvardas aga ootamatult USA tehnoloogiaettevõtte Meta lõpetada EL-is Facebooki ja Instagrami teenuse pakkumise.³ Põhjus seisneb suuresti EL-i karmides nõuetes, mis on seatud isikuandmete töötlemisele ning nende kolmandatesse riikidesse, sh USA-sse edastamisele.

EL-i mure isikuandmete USA-sse edastamisega sai alguse 2013. aastal, kui sai teatavaks USA luureagentuuride poolt teostatav ulatuslik inimeste jälgimine.⁴ Seejuures tuli välja, et USA valitsus kasutab inimeste jälgimiseks⁵ ka suurte USA teenusepakkujate (nt Google, Meta, Microsoft ja Apple) abi.⁶ See viis arusaamani, et kuivõrd selliseid teenuseid kasutatakse suurel hulgal ka EL-is, võib USA potentsiaalselt jälgida ka EL-i kodanikke.

¹ Hamilton, D.S, Quinlan, J-P. The Transatlantic Economy 2023: Annual Survey of Jobs, Trade and Investment between the United States and Europe. Washington, DC: Foreign Policy Institute, Johns Hopkins University SAIS/Transatlantic Leadership Network, 2023.

Jobs, Trade and Investment between the United States and Europe. Kättesaadav: <https://transatlanticrelations.org/wp-content/uploads/2023/03/Transatlantic-Economy-Report-2023.pdf> (19.04.2023), lk 62-63.

² *Ibidem, passim*; vt ka nt Kivimaa, C. Euroopa Komisjoni rakendusotsuse (EL) 2016/1250 kehtivust mõjutavad olulised arengud USA ja Euroopa Liidu õiguses. Magistritöö – Tartu: Tartu Ülikool, 2017., lk 11.

³ Shear, S. Meta says it may shut down Facebook and Instagram in Europe over data-sharing dispute. CNBC, 07.02.2022. Kättesaadav: <https://www.cnbc.com/2022/02/07/meta-threatens-to-shut-down-facebook-and-instagram-in-europe.html> (23.04.2023).

⁴ Greenwald, G.E., MacAskill, E. NSA Prism program taps in to user data of Apple, Google and others. The Guardian. Kättesaadav: <https://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data> (19.04.2023).

⁵ Sellist jälgimist nimetatakse „signaalluureks“ (ingl k *signals intelligence*), mis tähendab tehniliste ja elektrooniliste tehnikavahenditega sidekanalite kaudu edastatava informatsiooni kogumist ja salvestamist. Vt nt The National Security Agency. Signals Intelligence (SIGINT) Overview. Kättesaadav: <https://www.nsa.gov/Signals-Intelligence/Overview/> (24.04.2023).

⁶ *Ibidem*.

Käesolevaks hetkeks on eurooplaste⁷ mure viinud selleni, et USA ja EL-i vahel on viimase 10 aasta jooksul kaks erinevat andmevahetusraamistikku, mis võimaldasid digitaalmajandusel ilma suurtemate takistusteta toimida, Euroopa Kohtu poolt kehtetuks tunnistatud. Tulekul on kolmas selline raamistik ingliskeelse nimega *European Union-U.S. Data Privacy Framework*⁸ (edaspidi „USA uus andmekaitseraamistik“), mille eesmärk on adresseerida Euroopa Kohtu kriitikat varasemate raamistike osas. Juba praegu eksisteerib ka selle uue raamistiku osas vastakaid arvamusi. Kas lõpuks on USA ja EL jõudnud kokkuleppele, mis võimaldab digitaalmajandusel efektiivselt toimida, kuid samas austab ka inimeste õigust privaatsusele ja andmekaitsele? Või on pooled piltlikult öeldes astunud kolmandat korda sama reha otsa, mis tähendaks potentsiaalselt, et Euroopa Kohus tunnistab ka selle andmevahetusraamistiku kehtetuks. Nende küsimuste uurimisele käesolev magistritöö keskendubki.

Täpsemalt on magistritöö eesmärk välja selgitada, kas USA uue andmekaitseraamistikuga kehtestatud piirangud signaalluure teostamisele tagavad selle, et USA luureagentuuride signaalluuretegevus vastab EL-i poolt nõutavale andmekaitse tasemele. Magistritöö eesmärgi saavutamiseks on autor püstitanud neli uurimisküsimust. Uurimisküsimused on tuletatud Euroopa Andmekaitsekohtu poolt formuleeritud tagatistest, mida tuleks järgida, et jälgimismeetmete kaudu eraelu puutumatus ja andmekaitse põhiõiguste riivamine isikuandmete edastamisel EL-ist USA-sse oleks demokraatlikus ühiskonnas vajalik ja proportsionaalne. Euroopa Andmekaitsekohtu tagatised, millel magistritöö uurimisküsimused põhinevad, on peamiselt tuletatud Euroopa Kohtu praktikast, mis on seotud Euroopa Liidu põhiõiguste harta⁹ (edaspidi „põhiõiguste harta“) artiklitega 7, 8, 47 ja 52.

⁷ Käesolevas töös mõeldakse termini „eurooplasted“ all EL-i kodanikke ja kõiki muid andmesubjekte, kelle suhtes kohaldub Euroopa Parlamendi ja nõukogu määrus (EL) 2016/679, 27. aprill 2016, füüsiliste isikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise ning direktiiv 95/46/EÜ kehtetuks tunnistamise kohta (isikuandmete kaitse üldmäärus) artikkel 3.

⁸ Euroopa Komisjoni pressiteade. Questions & Answers: EU-U.S. Data Privacy Framework, draft adequacy decision, 13.12.2022. Kättesaadav: https://ec.europa.eu/commission/presscorner/detail/en/qanda_22_7632 (23.04.2023).

⁹ Euroopa Liidu põhiõiguste harta. – ELT C 326/02 2012, lk 391-407.

Eeltoodust lähtuvalt on magistritöö uurimisküsimused järgnevad:

1. Kas USA uus andmekaitseraamistik sätestab selged, täpsed ja ligipääsetavad (avalikud) reeglid signaalluuretegevuse käigus isikuandmete töötlemisele?
2. Kas USA uus andmekaitseraamistik tagab, et signaalluuretegevusega kaasnevad põhiõiguste riived on vajalikud ja proportsionaalsed?
3. Kas USA uus andmekaitseraamistik tagab, et signaalluure raames teostatava isikuandmete töötlemise õiguspärasust kontrollib sõltumatu järelevalvemehhanism?
4. Kas USA uus andmekaitseraamistik tagab üksikisikutele – kes leiavad, et nende õigusi on rikutud – tõhusad õiguskaitsevahendid oma õiguste kaitsmiseks?

Magistritöö autor on püstitanud hüpoteesi, et USA uus andmekaitseraamistik tagab selle, et USA luureagentuuride signaalluuretegevus vastab EL-i poolt nõutavale andmekaitse tasemele. Hüpoteesi püstitamist põhjendab siinkirjutaja sellega, et peamine Euroopa Kohtu varasem kriitika USA poolt tagatava andmekaitse taseme kohta kohtuasjas *Schrems II* seisnes selles, et 1) USA luureagentuuride teostatav signaalluure ei vastanud vajalikkuse ja proportsionaalsuse põhimõtetele ning 2) USA-s puudus sõltumatu järelevalveasutus, mis saaks tagada eurooplastele tõhusad õiguskaitsevahendid, kui nad leiavad, et nende õigusi on signaalluure teostamisega rikutud¹⁰. USA on proportsionaalsuse ja vajalikkuse põhimõtted nüüd enda siseriiklikus õiguses sätestanud. Need põhimõtted on kirja pandud president Joe Bideni poolt 7. oktoobril allkirjastatud korralduses nr 14086¹¹ (ingl k *Executive Order 14086* – edaspidi „korraldus EO 14086“). Samuti luuakse koostoimes korralduse EO 14086 ja USA justiitsministri määrusega nr 5517-2022¹² (ingl k *Attorney General Order No. 5517-2022* – edaspidi „justiitsministri määrus“) uus andmekaitse kontrollkohus (ingl k *Data Protection Review Court* – edaspidi „DPRC“), mille ülesandeks saab olema eurooplaste

¹⁰ EKo C-311/18, *Data Protection Commissioner vs Facebook Ireland Limited and Maximilian Schrems*, ECLI:EU:C:2020:559, p 184 ja p 194-197.

¹¹ Executive Order 14086. Enhancing Safeguards for United States Signals Intelligence Activities. Kättesaadav: <https://www.presidency.ucsb.edu/documents/executive-order-14086-enhancing-safeguards-for-united-states-signals-intelligence> (20.04.2023).

¹² Attorney General Order No. 5517-2022, 10.14.2022. Kättesaadav: <https://www.federalregister.gov/documents/2022/10/14/2022-22234/data-protection-review-court> (20.04.2023).

kaebuste menetlemine, mis USA hinnangul tagab eurooplastele tõhusad õiguskaitsevahendid.¹³ Hüpoteesi kontrollimiseks tuleb siinkirjutajal välja selgitada, kas USA rakendab signaalluure teostamisel eelnimetatud põhimõtteid ka sisuliselt samaväärselt nagu näeb ette Euroopa Kohtu praktika ning kas DPRC järelevalvemehhanismina vastab põhiõiguste harta artiklist 47 tulenevatele nõuetele, eelkõige sõltumatuse kriteeriumile.

Peamiselt keskendub siinkirjutaja analüüsi käigus USA uue andmekaitseraamistikuga seonduvatele nüanssidele, millele varasemalt juhtis Euroopa Kohus tähelepanu *Schrems I*¹⁴ ja *Schrems II* lahendites. Nendeks on korralduse nr 12333¹⁵ (ingl k *Executive Order 12333* – edaspidi „korraldus EO 12333“) ja USA välisluure ja jälitustegevuse seaduse¹⁶ (ingl k *Foreign Intelligence Surveillance Act* – edaspidi „FISA“) paragrahvi 702 alusel teostatav signaalluure. Euroopa Komisjon on küll USA andmekaitse taseme kohta koostatud rakendusotsuse eelnõus¹⁷ (edaspidi „adekvaatsusotsuse eelnõu“) hinnanud ka USA uue andmekaitseraamistiku üldpõhimõtteid ning samuti USA õiguskaitseorganite – nagu nt politsei – ligipääsu isikuandmetele ja selle kooskõla EL-i õigusega. Kuivõrd Euroopa Kohtu jaoks oli EL-i õiguse kontekstis eelnimetatud kohtulahendites probleemne just USA luureagentuuride ligipääs isikuandmetele, mis toimub põhiliselt korralduse EO 12333 ja FISA paragrahvi 702 alusel, siis magistritöö piiratud mahu tõttu keskendubki autor just nendele õigusaktidele.

Eestikeelseid sarnases valdkonnas uurimis-, magistri-, või doktoritöid on siinkirjutajale teadaolevalt vähe kirjutatud. Carel Kivimaa kirjutas 2017. aastal magistritöö¹⁸, kus käsitles

¹³ The White House. FACT SHEET: President Biden Signs Executive Order to Implement the European Union-U.S. Data Privacy Framework. Kättesaadav: <https://www.whitehouse.gov/briefing-room/statements-releases/2022/10/07/fact-sheet-president-biden-signs-executive-order-to-implement-the-european-union-u-s-data-privacy-framework/> (23.04.2023).

¹⁴ EKo C-362/14, *Maximilian Schrems vs Data Protection Commissioner*, ECLI:EU:C:2015:650.

¹⁵ Executive Order 12333. United States Intelligence Activities. Kättesaadav: <https://www.archives.gov/federal-register/codification/executive-order/12333.html> (20.04.2023).

¹⁶ FISA Amendments Act of 2008. Kättesaadav: <https://www.congress.gov/bill/110th-congress/house-bill/6304/text> (19.04.2023).

¹⁷ Euroopa Komisjon. Draft Commission Implementing Decision pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate level of protection of personal data under the EU-US Data Privacy Framework, 13.12.2022. Kättesaadav: https://commission.europa.eu/document/e5a39b3c-6e7c-4c89-9dc7-016d719e3d12_en (20.04.2023).

¹⁸ Kivimaa, C.

Euroopa Komisjoni poolt USA-le antud eelmise rakendusotsusega (EL) 2016/1250¹⁹ (edaspidi „adekvaatusotsus 2016/1250“) seonduvaid õiguslikke küsimusi. Peamiselt keskendus ta sellele, kas USA andmekaitseraamistiku *Privacy Shield* poolt tagatav andmekaitse tase vastas EL-i poolt nõutavale andmekaitse tasemele. Kivimaa magistritöö erinevus käesoleva magistritööga seisneb esiteks selles, et praeguseks hetkeks on *Privacy Shield* ning selle suhtes antud Euroopa Komisjoni adekvaatusotsus 2016/1250 kehtetuks tunnistatud ning on avaldatud USA uus andmekaitseraamistik ja Euroopa Komisjoni poolt ka adekvaatsuotsuse eelnõu selle raamistiku suhtes. Samuti võrdles Kivimaa peamiselt *Privacy Shieldi* ning Euroopa Parlamendi ja nõukogu määruse (EL) 2016/679²⁰ (ingl k *General Data Protection Regulation* – edaspidi „GDPR“) isikuandmete töötlemise põhimõtteid, kuid käesolevas töös siinkirjutaja eeltoodud põhimõtteid põhjalikult ei käsitle ning keskendub vaid USA luureagentuuride poolt teostatavale signaalluurele ning selle vastavusele EL-i õigusega. Luuretegevusega kaasnevaid riiveid isikute põhiõigustele käsitlesid magistritöödes ka 2016. aastal Piret Schasmin²¹ ning 2017. aastal Kätlin Helena Sehver²². Nendes töodes aga analüüsiti Eesti elektroonilise side andmete säilitamise regulatsiooni vastavust EL-i õigusele. Peale eelnimetatud magistritööde kirjutamist on Euroopa Kohus teinud mitu olulist lahendit, kus on luure-ja jälgimistegevust käsitletud, millest peamised on *Schrems II*, *La Quadrature Du Net*²³, *Privacy International*²⁴ ning samuti nt Euroopa Inimõiguste Kohtu (edaspidi „EIK“) lahend *Big Brother Watch*²⁵. Hiljutisemalt on 2021. aastal kirjutatud magistritöös²⁶ Airiin Antson analüüsinud Euroopa Kohtu praktikat seoses sideandmete säilitamisega, aga sarnaselt Sehveri ja Schasminiga

¹⁹ Euroopa Komisjoni rakendusotsus (EL) 2016/1250, 12. juuli 2016, isikuandmete kaitse piisavuse kohta ELi-USA andmekaitseraamistikus *Privacy Shield* vastavalt Euroopa Parlamendi ja nõukogu direktiivile 95/46/EÜ, ELT L 207, 01.08.2016, lk 1-112.

²⁰ 27. aprilli 2016. aasta Euroopa Parlamendi ja nõukogu määrus (EL) 2016/679 füüsiliste isikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise ning direktiivi 95/46/EÜ kehtetuks tunnistamise kohta (isikuandmete kaitse üldmäärus). – ELT L 119/1, 04.05.2016, lk 1-88.

²¹ Schasmin, P. Privaatsusõiguse piiramise õiguslik raamistik Euroopa Inimõiguste Kohtu ning Euroopa Kohtu lahendite alusel. Magistritöö. – Tallinn: Tartu Ülikool, 2016.

²² Sehver, K.H. Privaatsusõiguse riive proportsionaalsuse hindamise kriteeriumid Euroopa Liidu õiguses elektroonilise side andmete kaitse valdkonna näitel. Magistritöö. – Tallinn: Tartu Ülikool, 2017.

²³ EKo liidetud kohtuasjad C-511/18, C-512/18 ja C-520/18, *La Quadrature du Net and Others vs Premier ministre and Others*, ECLI:EU:C:2020:791.

²⁴ EKo C-623/17, *Privacy International vs Secretary of State for Foreign and Commonwealth Affairs and Others*, ECLI:EU:C:2020:790.

²⁵ EIKo 58170/13, 62322/14, 24960/15, *Big Brother Watch and Others vs the United Kingdom*.

²⁶ Antson, A. Elektroonilise side andmete säilitamise ja põhiõiguste tagamise vahekord kriminaalmenetluses. Magistritöö – Tallinn: Tartu Ülikool, 2021.

keskendus ta selles töös Eesti kriminaalmenetluse vastavusele Euroopa Kohtu praktikast tulenevatele nõuetele. Kokkuvõtvalt ei ole siinkirjutajale teadaolevalt eestikeelses kirjanduses USA uue andmekaitseraamistiku vastavust EL-i õigusest tulenevatele nõuetele veel jõutud põhjalikult uurida, eriti arvestades ka seda, et uus raamistik avaldati alles pool aastat tagasi. Seetõttu on käesoleva magistritöö teema uudne ja aktuaalne.

Magistritöö koosneb kahest peatükist. Esimeses peatükis analüüsib autor, millistel õiguslikel alustel on isikuandmeid võimalik EL-ist välja edastada. Seejärel käsitleb autor USA ja EL-i fundamentaalselt erinevaid lähenemisi andmekaitsele ja privaatsusele, seda kuidas suhestuvad USA-s omavahel privaatsus ning signaalluure ning viimaks annab ülevaate varasemalt Euroopa Kohtu poolt kehtetuks tunnistatud USA ja EL-i vahelistest andmekaitseraamistikest. Magistritöö teises peatükis keskendub siinkirjutaja esimeses peatükis kindlaks tehtud õigusaktide ja raamistiku põhjal uurimisküsimustele vastamisele, püstitatud hüpoteesi kontrollimisele ning seeläbi ka magistritöö eesmärgi saavutamisele.

Magistritöö on olemuselt kvalitatiivne, mistõttu autor on töö kirjutamisel kasutanud traditsioonilisi õigusteaduslikke uurimismeetodeid: peamiselt analüütilist ja võrdlevat meetodit. Magistritöö kirjutamisel võrdles autor USA ja EL-i õigusakte, nende õigusaktide alusel tagatavat andmekaitse taset, erinevate õigusteadlaste seisukohti ning analüüsis kohtupraktikat. Magistritöö peamised allikad on andmekaitset ja luuretegevust käsitlev õiguskirjandus, EL-i ja USA õigusaktid, Euroopa Kohtu ja Euroopa Inimõiguste Kohtu praktika, vähemal määral ka USA kohtupraktika. Lisaks kasutas siinkirjutaja erinevate EL-i asutuste (nt Euroopa Komisjon, Euroopa Parlament ja Euroopa Andmekaitse nõukogu) otsuseid, suuniseid ning arvamusi.

Autor tänab enda juhendajaid Aleksei Kellit ning Margot Arnust, kelle toetus ja nõuanded võimaldasid sellel tööl valmida.

Magistritööd iseloomustavad järgnevad märksõnad: 1) andmekaitse; 2) privaatsus; 3) andmeedastus; 4) luure.

1. Atlandi-ülene isikuandmete edastamine

1.1. Õiguslik alus isikuandmete edastamiseks EL-ist kolmandatesse riikidesse

EL-is reguleerib isikuandmete kolmandatesse riikidesse edastamist kaks õigusakti: juba ülalnimetatud GDPR ning Euroopa Parlamendi ja nõukogu direktiiv (EL) 2016/680²⁷ (ingl k *Law Enforcement Directive* – edaspidi „LED“). Kõnealuse magistritöö kontekstis ei ole LED asjakohane, sest magistritöö käsitleb olukordi, kus isikuandmete piiriülene edastamine toimub põhiliselt erasektori tegevuse raames ning USA luureasutused saavad isikuandmete ligipääsu hiljem, mitte esialgse andmeedastuse käigus. Teisisõnu öeldes, LED kohaldub olukordades, kus ei kohaldu GDPR, aga magistritöö keskendub põhiliselt GDPR-i kohaldamisalas olevatele küsimustele. Magistritöö autor toob siinkohal näiteks, et GDPR-i reguleerimisalas on olukord, kus eurooplane saadab e-kirja Gmaili vahendusel ning seejärel nõuab USA luureagentuur tehnoloogiaettevõttelt Google (Gmaili teenusepakkuja) välja e-kirja sisu ning saab seega ligipääsu e-kirja saatnud eurooplase isikuandmetele.

Lisaks GDPR-ile on andmete edastamise seisukohalt eurooplaste jaoks olulise tähtsusega põhiõiguste harta. Põhiõiguste harta artikkel 8 näeb ette, et õigus isikuandmete kaitsele on igaühe põhiõigus. Põhiõiguste harta muutus 2009. aasta 1. detsembril Lissaboni lepingu²⁸ jõustumisega EL-i jaoks õiguslikult siduvaks. Lissaboni lepingu artikkel 6 punktiga 1 anti põhiõiguste hartale samaväärne õigusjõud EL-i aluslepingutega. Seetõttu tuleb GDPR-i tõlgendamisel arvestada ka põhiõiguste hartas sätestatud, mida on samuti toonitanud Euroopa Kohus *Schrems II* lahendis.²⁹

GDPR-is reguleerib isikuandmete edastamist kolmandatesse riikidesse V peatükk. GDPR-i artiklis 44 sätestatud üldpõhimõtete kohaselt tohib isikuandmeid EL-ist kolmandatesse

²⁷ 27. aprilli 2016. aasta Euroopa Parlamendi ja nõukogu direktiiv (EL) 2016/680, mis käsitleb füüsiliste isikute kaitset seoses pädevates asutustes isikuandmete töötlemisega süütegude tõkestamise, uurimise, avastamise ja nende eest vastutusele võtmise või kriminaalkaristuste täitmisele pööramise eesmärgil ning selliste andmete vaba liikumist ning millega tunnistatakse kehtetuks nõukogu raamotsus 2008/977/JSK. – L 119/89, 04.05.2016, lk 1-43.

²⁸ Lissaboni leping, millega muudetakse Euroopa Liidu lepingut ja Euroopa Ühenduse asutamislepingut. – ELT C 306, 17.12.2007, lk 1–271.

²⁹ EKo C-311/18, *Schrems II*, p 99.

riikidesse edastada ainult juhul, kui on täidetud GDPR-iga nõutavad tingimused andmete edastamisele. GDPR-i V peatükk võimaldab andmeedastust kolmandatesse riikidesse peamiselt kolmel erineval juhul:

1. edastamine toimub Euroopa Komisjoni poolt vastu võetud otsuse alusel, millega Euroopa Komisjon kinnitab, et kõnealuses kolmandas riigis on tagatud piisav andmekaitse tase (GDPR artikkel 45);
2. edastamine toimub asjakohaste kaitsemeetme kohaldamisel (GDPR artikkel 46);
3. erandlik edastamine konkreetsetes olukordades (GDPR artikkel 49).

1.1.1. GDPR-i artikkel 45 – edastamine adekvaatsusotsuse alusel

GDPR-i artikkel 45 lõike 1 kohaselt võib kolmandale riigile või rahvusvahelisele organisatsioonile isikuandmeid edastada, kui Euroopa Komisjon on teinud otsuse, et asjaomane kolmas riik, asjaomase kolmanda riigi territoorium, kõnealuse kolmanda riigi üks või mitu kindlaksmääratud sektorit või rahvusvaheline organisatsioon tagab isikuandmete kaitse piisava taseme (edaspidi „adekvaatsusotsus“). Sama artikli lõike 2 alusel (punktid a-c) võtab Euroopa Komisjon eelkõige arvesse näiteks, kas kõnealuses riigis või territooriumil austatakse inimõiguseid ja põhivabadusi; kuidas on seal reguleeritud ligipääs isikuandmetele riigiasutuste poolt; kas seal riigis eksisteerib sõltumatu järelevalveasutus, mis teeb tõhusat järelevalvet selle üle, et selles riigis või territooriumil täidetakse kohalduvaid andmekaitse norme; missugused rahvusvahelised või muud kohustused on kõnealune kolmas riik või territoorium endale isikuandmete kaitse tagamisega seoses võtnud.

Andmekaitse taseme piisavuse üle otsustamise kohta on EL-i andmekaitseasutuste töörühm (edaspidi: „WP29“), kes on praegu funktsioneeriva Euroopa Andmekaitse nõukogu õiguseellane, avaldanud töödokumendi, millega antakse suuniseid ja selgitusi selle osas, mis on kõige olulisemad kriteeriumid hindamaks, kas kolmas riik vastab EL-i andmekaitse nõuetele, st kas kolmas riik tagab piisava andmekaitse taseme.³⁰ Töödokumenti on mitu korda uuendatud ja ajakohastatud andmekaitseõiguse pideva muutumise ja GDPR-i

³⁰ Artikkel 29 töörühm. Töödokument WP 114, 25. 11. 2005. Kättesaadav: <https://ec.europa.eu/newsroom/article29/items/614108> (19.04.2023), lk 7.

kohaldamisel juurde saadud praktiliste kogemuste tõttu.³¹ Viimati muudeti dokumenti 6. veebruaril 2018. GDPR-i jõustumisega WP29 küll asendati Euroopa Andmekaitsekoostöögruppi, kuid Euroopa Andmekaitsekoostöu on selle töödokumendi ka üle kinnitanud³² ning seega on see jätkuvalt asjakohane. Kokkuvõtvalt võib WP29 töödokumendi põhjal öelda, et kaks põhilist aspekti kolmanda riigi andmekaitsetaseme hindamisel on: 1) kolmanda riigi poolt kohaldavate normide sisu ja 2) vahendid, millega kolmas riik või territoorium tagab, et norme kohaldatakse tulemuslikult. Euroopa Komisjon peab selle pinnalt kontrollima, kas nende kahe põhielemendi rakendamine praktikas ka õnnestub.³³

Teine oluline dokument kolmanda riigi andmekaitse taseme hindamisel on Euroopa Andmekaitsekoostöu poolt välja antud soovitused, mille esialgse kavandi koostas Euroopa Andmekaitsekoostöu õiguseellane WP29 peale *Schrems I* lahendit, millega tunnistati kehtetuks³⁴ andmekaitseraamistik *Safe Harbor*.³⁵ Selle dokumendi eesmärk oli välja selgitada tingimused, mis peavad olema täidetud selleks, et jälgimismeetmete kaudu privaatsuse ja andmekaitse põhiõiguste riivamine ei rikuks vajalikkuse ja proportsionaalsuse põhimõtteid.³⁶ Sarnaselt eelmises lõigus mainitud töödokumendiga, on Euroopa Andmekaitsekoostöu selle üle kinnitanud³⁷ ning uuema kohtupraktika valguses ka ajakohastanud.³⁸

Kuigi Euroopa olulised tagatised on Euroopa Andmekaitsekoostöu poolt koostatud soovitused, millel ei ole õiguslikult siduvat mõju, saab neid efektiivselt kasutada, et anda hinnang kolmanda riigi poolt tagatava andmekaitse taseme kohta, sest need põhinevad

³¹ *Ibidem*, lk 2.

³² Vt Euroopa Andmekaitsekoostöu. Endorsement of GDPR WP29 guidelines by the EDPB, 25.05.2018. Kättesaadav: https://edpb.europa.eu/news/news/2018/endorsement-gdpr-wp29-guidelines-edpb_en (20.04.2023).

³³ Artikkel 29 töörühm, 2005, lk 2.

³⁴ Vt lähemalt *infra*, ptk 1.4.1.

³⁵ Euroopa Andmekaitsekoostöu. Soovitused 02/2020 Euroopa oluliste tagatiste kohta jälgimismeetmete kontekstis, 10.11.2020. Kättesaadav: https://edpb.europa.eu/sites/default/files/files/file1/edpb_recommendations_202002_europeanessentialguaranteessurveillance_et.pdf (20.04.2023), lk 4.

³⁶ *Ibidem*.

³⁷ Euroopa Andmekaitsekoostöu. Endorsement of GDPR WP 29 Guidelines by the EDPB.

³⁸ Euroopa Andmekaitsekoostöu soovitused (2020), lk 4.

signaalluurega seondual Euroopa ja Euroopa Inimõiguste Kohtu praktikal. Kuivõrd käesolev töö keskendub sellele, kuidas mõjutab USA luureagentuuride poolt teostatav signaalluure USA õigusaktide alusel tagatavat andmekaitse taset eurooplaste isikuandmetele, siis sel põhjusel autor analüüsibki magistritöö raames USA andmekaitse taseme vastavust Euroopa Andmekaitse nõukogu poolt koostatud Euroopa olulistele tagatistele.

Euroopa Komisjon on selle magistritöö kirjutamise seisuga välja andnud 13 adekvaatsusotsust järgnevatele riikidele ja territooriumitele: Andorra, Argentiina, Kanada, Fääri Saared, Guernsey, Iisrael, Man (ingl k *Isle of Man*), Jaapan, Jersey, Uus-Meremaa, Korea Vabariik ja Šveits.³⁹ Kõnealuse magistritöö kirjutamise hetkel eksisteerib maailmas 195 riiki.⁴⁰ Sellest võiks järeldada, et andmekaitsestandardid – milleni adekvaatsusotsust taotleb riik peab küündima – on kõrged, arvestades kui vähe adekvaatsusotsuseid on Euroopa Komisjon teinud. Ometigi on USA suhtes varasemalt juba välja antud kaks adekvaatsusotsust ning Euroopa Kohtu hinnangul⁴¹ ei vastanud neist kumbki EL-i andmekaitsestandarditele. Selle pinnalt võib tõstatada küsimuse, miks annab Euroopa Komisjon annab USA suhtes välja adekvaatsusotsuseid, mis tegelikult ei vasta EL-i andmekaitse tasemele. Vastus sellele küsimusele ei ole ilmselt puhtalt õiguslik, vaid pigem majanduslik või (õigus)poliitiline, seega autor pikemalt sel teemal ei peatu, kuid siinkirjutaja arvates on tõenäoline, et põhjus võib seisneda selles, et Euroopa Komisjon ei soovi takistada EL-i ja USA-vahelise digitaalkaubanduse toimimist. Nagu sissejuhatuses mainitud – USA on EL-i suurim kaubanduspartner.

1.1.2. GDPR-i artikkel 46 – edastamine asjakohaste kaitsemeetmete kohaldamisel

Adekvaatsusotsuse puudumise korral teine alus võimaldamaks isikuandmete edastamist EL-i piiridest väljapoole on GDPR-i artikkel 46. Selle artikli lõike 1 kohaselt võib isikuandmeid kolmandale riigile edastada ainult juhul, kui on sätestatud asjakohased kaitsemeetmed ning

³⁹ Euroopa Komisjoni koduleht. Adequacy decisions. Kättesaadav: https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en (19.04.2023).

⁴⁰ World of Meter koduleht. How many countries are there in the world? Kättesaadav: <https://www.worldometers.info/geography/how-many-countries-are-there-in-the-world/> (19.04.2023).

⁴¹ Vt põhjalikumalt *infra*, ptk 1.4.

tingimusel, et andmesubjektide kohtulikult kaitstavad õigused ja tõhusad õiguskaitsevahendid on neile kättesaadavad.

Peamine kaitsemeede, mille alusel artikkel 46 võimaldab isikuandmete edastamist EL-ist välja, on artikkel 46 lõige 2 punkti c kohaselt Euroopa Komisjoni poolt vastu võetud standardsed andmekaitseklauslid. Andmeedastuse puhul USA-sse tuginevad andmeid edastavad ettevõtted lausa 85% juhtudest just nendele meetmetele.⁴² Ka nt sissejuhatuses mainitud Meta tugineb Facebooki teenuse osutamise raames toimuva andmeedastuse korral just standardsetele andmekaitseklauslitele. Max Schrems – kelle kaebuste tulemusena tunnistati kehtetuks eelmised kaks USA-ELi vahelist andmekaitseraamistiku – tugineski oma kaebuses sellele, et Facebooki poolt nende klauslite kasutamine ei ole piisav, et kaitsta tema isikuandmeid selle eest, et USA luureagentuurid neile ligi ei pääseks.⁴³ Jätkuvad probleemid standardsete andmekaitseklauslitega on samuti üks peamistest põhjustest, miks Meta on ähvardanud Facebooki teenuse pakkumise EL-is lõpetada.⁴⁴ Kuigi USA luureagentuuridega esinevad probleemid on mõlemas kontekstis asjakohased, siis piiratud mahu tõttu keskendub käesolev magistritöö neile just USA uue andmekaitseraamistiku analüüsi võtmes.

1.1.3. GDPR-i artikkel 49 – erandid konkreetsetes olukordades

GDPR-i artikkel 49 lõike 1 kohaselt, juhul kui puuduvad nii adekvaatsusotsus kui ka asjakohased kaitsemeetmed, võib isikuandmete edastamine kolmandasse riiki lubatud olla ainult konkreetsetel erandlikel tingimustel. Sama lõike all on need tingimused ka loetletud: sinna hulka kuuluvad näiteks andmesubjekti selgesõnaline nõusolek, vajadus täita andmesubjektiga sõlmitud lepingut, avalikust huvist tingitud kaalukad põhjused.

Euroopa Andmekaitsekoostöö on enda andmeedastust käsitlevates suunistes selgitanud, et artikkel 49 alusel edastamine peab tõesti olema erandlik. Selle artikli alusel andmete

⁴² Digital Europe koduleht. Schrems 2 data transfers survey: 85% of companies in Europe use standard contractual clauses. <https://www.digitaleurope.org/news/schrems-2-data-transfers-survey-85-of-companies-in-europe-use-standard-contractual-clauses/> (19.04.2023).

⁴³ Vt *infra*, ptk 1.4.2.

⁴⁴ Vt Sheard, S.

edastamist tuleb tõlgendada kitsendavalt, et erand ei muutuks reegliks. Sellist tõlgendust toetab ka asjaolu, et kui andmeedastus toimub artikkel 49 alusel, siis ei ole andmesubjektidele tagatud täiendavaid kaitsemeetmeid, mis omakorda suurendab riski, et andmesubjekti põhiõigusi- ja vabadusi võidakse rikkuda.⁴⁵ Seetõttu oleks käesolevas magistritöös detailselt analüüsitav USA uus andmekaitseraamistik andmesubjekti vaatest paremat kaitset pakkuv lahendus.

Järgmises alapeatükis analüüsib autor seda, kuidas üldiselt käsitletakse EL-is ja USA-s andmekaitset ja privaatsust ning milles seisnevad nende erinevad lähenemised

1.2. EL-i ja USA erinevad lähenemised andmekaitsele

1.2.1. Andmekaitse kui põhiõigus EL-i kontekstis

Õigusteadlased Douwe Korff ja Ian Brown on põhjendatult juhtinud tähelepanu, et EL-is nähakse andmekaitset kui fundamentaalset ning universaalset inim- ja põhiõigust. EL-i õiguskorras on see sätestatud *sui generis* õigusena, tuleneb ELi aluslepingutest ja põhiõiguste harta artiklist 8,⁴⁶ nagu ka magistritöö peatükis 1.1 sai mainitud. Sellest järeldub, et iga liikmesriigi eraelu puutumatust või andmekaitset puudutavad seadused peaksid kohalduma igasugusele isikuandmete töötlemisele, olenemata isiku kodakondsusest, staatusest või asukohast (st isegi kui nad ei ole liikmesriigi kodanikud või elanikud või asuvad füüsiliselt väljaspool liikmesriigi territooriumi) – seda tuntakse kui universaalsuse printsiipi.⁴⁷ See tähendab, et olukorras, kus isikuandmeid edastatakse EL-i

⁴⁵ Euroopa Andmekaitsekoostöögrupi. Suunised 2/2018 määruse 2016/679 artiklis 49 sätestatud erandite kohta, 25. mai 2018. Kättesaadav: https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_2_2018_derogations_et.pdf (19.04.2023), lk 4.

⁴⁶ Brown, I., Korff, D. Exchanges of Personal Data After the Schrems II Judgment. Study for the European Parliament's Committee on Civil Liberties. Kättesaadav: [https://www.europarl.europa.eu/RegData/etudes/STUD/2021/694678/IPOL_STU\(2021\)694678_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/STUD/2021/694678/IPOL_STU(2021)694678_EN.pdf) (19.04.2023), lk 18.

⁴⁷ *Ibidem*.

piiridest välja (nt USA-sse), ei tohiks see mõjutada isikuandmetele tagatavat andmekaitse taset.⁴⁸

Samuti iseloomustab EL-i universaalset lähenemist Euroopa inimõiguste ja põhivabaduste kaitse konventsiooni⁴⁹ (edaspidi „EIÕK“) artikli 8 lõikes 1 sätestatu, mille kohaselt on igaühel õigus sellele, et austataks tema era- ja perekonnaelu ja kodu ning sõnumite saladust. EIÕK artikli 6 lõike 3 kohaselt on EIÕK-ga tagatud põhiõigused osa EL-i õiguse üldpõhimõtetest. Sarnaselt EIÕK artikkel 8 lõikes 1 sätestatuga on ka põhiõiguste harta artiklis 7 sisuliselt samasuguse sõnastusega põhiõigus. See võib tekitada küsimuse, kas põhiõiguste harta artiklist 8 tulenevat õigust andmekaitsele peaks käsitlema erinevalt põhiõiguste harta artiklist 7 ja EIÕK artiklist 8 tulenevat õigust eraelu puutumatuselle (teisiseõnu õigust privaatsusele) ning mis on nende sisuline vahe. Selle magistritöö kontekstis ei ole selline analüüs siiski vajalik, sest nii Euroopa Kohus kui ka EIK käsitlevaid neid ühise hübriidõigusena, mille kohta võib täpsemalt lugeda Kätlin Helena Sehveri 2017. aastal kirjutatud magistritööst.⁵⁰ Seega pikemalt siinkirjutaja nende õiguste eristamisel ei peatu ja käsitleb neid käesoleva töö kontekstis samuti ühise hübriidõigusena.

1.2.2. USA privaatsusõigus

Võrreldes Euroopa Liiduga – kus nähakse õigust privaatsusele ja andmekaitsele igaüheõigusena ning samuti kus eksisteerib üks õigusakt (GDPR), mis reguleerib andmekaitset terve liidu tasandil – on USA privaatsusõigus rohkem killustatud. USA Kongress on vastu võtnud mitmeid üksikuid seadusi, mille eesmärk on tagada üksikisikute isikuandmete kaitse.⁵¹ Need seadused erinevad oluliselt oma eesmärgi ja ulatuse poolest. Enamik neist kehtestab andmekaitsekohustused konkreetsetes sektoris tegutsevate teenusepakkujate suhtes, nt finantsasutuste, tervishoiuasutuste ja sideteenuse pakkujate suhtes või teatud eriliigiliste andmete kaitsmiseks, nagu nt laste isikuandmed. Näiteks

⁴⁸ *Ibidem*, lk 25.

⁴⁹ Euroopa inimõiguste ja põhivabaduste kaitse konventsioon. Euroopa Nõukogu, 4.11.1950. – RT II 2010, 14, 54.

⁵⁰ Vt nt Sehver, K.H., lk 21.

⁵¹ Zachary S., Heck, A. *A Litigator's Primer on European Union and American Privacy Laws and Regulations*, 44 LITIG, 2018, lk 59. (viidatud: Korff, D., Brown, I., lk 69, joonealune viide nr 123).

sideandmete jäädvustamise seadus⁵² (ingl k *Stored Communications Act* – SCA) keelab teatud interneti teenusepakkujate salvestatud elektroonilisele sidele juurdepääsu. Samuti keelavad mõned seadused laiaulatuslikke tegevusi, mis ei ole küll seotud ainult andmekaitsega, kuid siiski piiravad seda, kuidas ettevõtted tohivad isikuandmeid töödelda.⁵³

Privaatsusõigust reguleeritakse USA-s erinevalt ka osariikide tasandil. Magistritöö kirjutamise seisuga on laiapõhjaliselt privaatsusõigust reguleerivad õigusaktid – mis käsitlevad isikuandmete töötlemist – vastu võetud California, Colorado, Connecticut, Iowa, Virginia ja Utah osariikides.⁵⁴ Arvestades, et USA-s eksisteerib kokku 50 osariiki⁵⁵, võib magistritöö autori hinnangul järeldada, et osariikide tasandil reguleeritakse privaatsusõigust hetkel siiski vähe. Viidatud osariikidest kõige arenenum on privaatsusõiguse kaitse Californias, kus võeti 2018. aastal vastu California tarbija privaatsuse seadus⁵⁶ (ingl k *California Consumer Privacy Act* – edaspidi „CCPA“), mis jõustus 1. jaanuaril 2020. CCPA andis California tarbijatele õiguse teada saada, millist teavet ettevõtted nende kohta koguvad, õiguse nõuda enda isikuandmete kustutamist, õiguse takistada ettevõtetel tarbijate isikuandmete müümist ning samuti tekitas CCPA ettevõtetele, kes ei võtnud kasutusele mõistlikke samme tarbijate isikliku informatsiooni kaitseks, aluse nende vastutusele võtmiseks. Aastal 2020 3. novembril võeti privaatsuse kaitse täiendavaks tugevdamiseks vastu California privaatsusõiguste seadus⁵⁷ (ingl k *California Privacy Rights Act* – edaspidi „CPRA“), mis jõustus käesoleva aasta 1. jaanuaril.⁵⁸

CPRA kohaldub mis tahes äritegevuse puhul, mille raames kogutakse, säilitatakse, jagatakse, müüakse, avaldatakse ja/või kasutatakse tarbija isikuandmeid. CPRA-s

⁵² Stored Communications Act (SCA, codified at 18 U.S.C. Chapter 121 §§ 2701–2712). Kättesaadav: <https://www.law.cornell.edu/uscode/text/18/part-I/chapter-121> (20.04.2023).

⁵³ Kerr, O.S., A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending it. 72 George Washington Law Review 1208 (2004), lk 1212. Kättesaadav: <https://ssrn.com/abstract=421860> (23.04.2023).

⁵⁴ The International Association of Privacy Professionals. US State Privacy Legislation Tracker. Kättesaadav: <https://iapp.org/resources/article/us-state-privacy-legislation-tracker/> (19.04.2023).

⁵⁵ USA saatkonna koduleht. States of the Union. Kättesaadav: <https://uk.usembassy.gov/states-of-the-union-states-of-the-u-s/> (19.04.2023).

⁵⁶ California Consumer Privacy Act of 2018 (CCPA). Kättesaadav: <https://oag.ca.gov/privacy/ccpa> (20.04.2023).

⁵⁷ California Privacy Rights Act of 2020 (CPRA). Kättesaadav: <https://www.caprivacy.org/cpra-text/> (20.04.2023).

⁵⁸ Brown, I., Korff, D., lk 81.

sisalduvad siiski mõned piirangud, mille tõttu on selle kohaldamisala pigem piiratud. Esiteks, see kohaldub ainult ettevõtetele, mille äritegevus toimub California osariigis ning samuti peab ettevõtte aastane käive ületama 25 miljonit dollarit; ettevõtte peab äritegevuse raames ostma, müüma või jagama 100 000 või enama tarbija või leibkonna isikuandmeid või peab ettevõtte aastakäibest vähemalt 50 protsenti tulenema tarbijate isikuandmete müümisest või jagamisest. Piirates seaduse reguleerimisala „ettevõtetega“, ei kata CPRA isikuandmete töötlemist mittetulundusühingute poolt, nagu nt heategevusorganisatsioonid, kodanikuühendused, kirikud, erakonnad, paljud haridusasutused jne, mis aga seevastu on EL-i andmekaitseõigusega hõlmatud.⁵⁹ Veelgi enam, isegi ettevõtetele kohaldamise kontekstis on künnis kõrge. CPRA künnised tähendavad, et CPRA ei kohaldu enamikele California väikestele või keskmise suurusega ettevõtetele. Samuti ei kohaldu see seadus enamikele väikestele ja suurtele ettevõtetele – kes Californias ei baseeru – isegi olukorras, kus nende äritegevus leiab aset Californias ning samuti kui nad koguvad tarbijate isikuandmeid Californias. Kokkuvõtvalt võib öelda, et reeglina CPRA ei kohaldu üksikisikute suhtes, kes elavad väljaspool Californiat, sh EL-is. California seadusandja, nagu ka USA Kongress föderaalset tasandil, ei rakenda põhimõtet, mille kohaselt andmekaitseõigused ja privaatsusõigused on universaalsed – erinevalt EL-ist.⁶⁰

USA erinevat lähenemist privaatsusele illustreerib hästi ka järgnev: USA põhiseaduse neljas parandus⁶¹ näeb ette, et „inimeste õigust turvalisusele oma isiku, maja, dokumentide ja mõju suhtes ebamõistlike läbiotsimiste ja haarangute vastu ei tohi rikkuda ning läbiotsimismääruseid ei väljastata, välja arvatud tõenäolise põhjuse korral, mis tugineb vandeale või kinnitusele ning milles kirjeldatakse konkreetselt läbiotsitavat asukohta ja läbiotsitavaid isikuid või esemeid“. ⁶² Teisiti öeldes – USA põhiseaduse neljas parandus keelab isikute põhjendamatu läbiotsimise, nende asjade konfiskeerimise ning seab tingimuseks, et läbiotsimismäärust ei väljastataks kergekäeliselt, vaid eksisteeriks põhjendatud kahtlus, et isik, kelle suhtes läbiotsimist teostatakse, on pannud toime kuriteo. EL-i ja USA vaheline loodud *ad hoc* töörühm, kelle ülesandeks oli uurida Snowdeni 2013.

⁵⁹ *Ibidem*.

⁶⁰ *Ibidem*.

⁶¹ The Fourth Amendment (Amendment IV) to the United States Constitution. Kättesaadav: <https://constitution.congress.gov/constitution/amendment-4/> (21.04.2023).

⁶² Rakendusotsus 2016/1250, joonealune viide 179.

aastal tehtud avaldusi⁶³ luuretegevusega seoses, on aga märkinud, et USA ülemkohtu praktika⁶⁴ kohaselt laieneb põhiseaduse neljas parandus ainult USA kodanikele ja USA-s alaliselt elavatele teiste riikide kodanikele – välismaalased (sh eurooplased, kes USA-s ei resideeru) ei saa neljandast parandusest tulenevat õigust kasutada.⁶⁵

1.3. Ülevaade USA privaatsusõiguse ja signaalluuretegevuse vahekorra

1.3.1. Edward Snowdeni paljastused USA luuretegevuse kohta

2013. aasta 7. juunil avaldasid briti ajalehe The Guardian ajakirjanikud Glenn Edward Greenwald ja Edward MacAskill artikli, kus nad kirjutasid, et USA Riiklik Julgeolekuagentuur (ingl k *National Surveillance Agency* – edaspidi „NSA“) on saanud otsese ligipääsu USA teenusepakkujate – nagu näiteks Google, Facebook ja Apple – süsteemidele.⁶⁶ Artikli autorid selgitasid, et nende valdusesse on sattunud ülisalajane dokument, mille kohaselt NSA pääseb suhtlusvõrgustike süsteemidele ligi programmi nimega *PRISM* raames.⁶⁷ See võimaldab luureametnikel koguda materjale, mille hulka kuuluvad otsinguajalugu, e-kirjade sisu, edastatud failid ning reaajas peetavad vestlused.⁶⁸ Artikli kohaselt olid juba alates 2007. aastast mõned maailma suurimad internetibrändid programmis osalenud ja NSA-le informatsiooni edastanud.⁶⁹ Esimene liituja oli Microsoft; 2008. aastal liitus Yahoo; 2009. aastal Google ja Facebook; 2011. aastal ka Eesti päritoluga Skype ning 2012. aastal liitus Apple.⁷⁰

Mõned päevad hiljem avaldasid eelnimetatud ajakirjanikud koos Laura Poitrasega uue artikli, kus nad avaldasid isiku identiteeti, kes neile NSA luuretegevusest teada andis ja

⁶³ Snowdeni paljastuste kohta vt lähemalt järgmine alaptk.

⁶⁴ *United States vs Verdugo-Urquidez*, 494 U.S. 259 (1990). Kättesaadav: <https://caselaw.findlaw.com/court/us-supreme-court/494/259.html> (21.04.2023).

⁶⁵ The *ad hoc* EU-US Working Group on Data Protection. Report on the findings by the EU Co-chairs of the *ad hoc* EU-US Working Group on Data Protection, 27.11.2013. Kättesaadav: <https://data.consilium.europa.eu/doc/document/ST-16987-2013-INIT/en/pdf> (21.04.2023).

⁶⁶ Greenwald, G.E., MacAskill, E. NSA Prism program taps in to user data of Apple, Google and others.

⁶⁷ *Ibidem*.

⁶⁸ *Ibidem*.

⁶⁹ *Ibidem*.

⁷⁰ *Ibidem*.

sellega seonduvaid materjale saatis.⁷¹ Vilepuhujaks oli endine NSA töötaja Edward Snowden.⁷² Snowden põhjendas informatsiooniga avalikuks tulemist sellega, et ta südametunnistus ei luba pealt vaadata, kuidas USA valitsus hävitab selle ülisuure salaja ehitatud jälgimisvõrgustikuga inimeste privaatsuse, internetivabaduse ja põhiõigused.⁷³

Eelnimetatud paljastuste olulisus selle magistritöö kontekstis seisneb selles, et sealt sai alguse EL-i poolne kahtlus seoses sellega, kas USA poolt teostatav jälgimistegevus võib ka mõjutada EL-i kodanikke. See esialgne kahtlus on nüüdseks kulmineerunud sellega, et Euroopa Kohus on tunnistanud kehtetuks juba kaks järjestikust andmevahetusraamistikku EL-i ja USA vahel. Seonduvat kohtupraktikat ja selle põhjendusi käsitleb siinkirjutaja lähemalt peatükis 1.4. Enne seda aga selgitab magistritöö autor järgmises peatükis, missuguste õigusaktide alusel võivad USA luureagentuurid Euroopa kodanikke suhtes signaalluuret teostada, kui ulatuslik selline luuretegevus praktikas on ning kuidas USA on püüdnud sellise jälgimistegevusega kaasnevaid riiveid isikute põhiõigustele vähendada.

1.3.2. Signaalluure teostamist võimaldavad õigusaktid

1.3.2.1. FISA paragrahv 702

USA välisluure ja jälitustegevuse seadus⁷⁴ (*Foreign Intelligence Surveillance Act* – edaspidi „FISA“) on USA parlamendi ehk Kongressi poolt vastu võetud õigusakt. Kõnealuse magistritöö kontekstis on fookuses FISA paragrahv 702, mis võimaldab USA luurel koguda, kasutada ja edastada elektroonilise side sisu USA teenusepakkujate käest, kelle hulka kuuluvad näiteks Google ja Facebook.

⁷¹ Greenwald, G.E jt. Edward Snowden: the whistleblower behind the NSA surveillance revelations. The Guardian, 11.06.2013. Kättesaadav: <https://www.theguardian.com/world/2013/jun/09/edward-snowden-nsa-whistleblower-surveillance> (23.04.2023).

⁷² *Ibidem*.

⁷³ *Ibidem*.

⁷⁴ FISA Amendments Act of 2008. Kättesaadav: <https://www.congress.gov/bill/110th-congress/house-bill/6304/text> (19.04.2023).

FISA paragrahv 702 võeti USA Kongressi poolt vastu 2008. aastal eesmärgiga võidelda terrorismi vastu 2001. aasta 11. septembril toimunud terrorirünnakute tõttu.⁷⁵ FISA paragrahv 702 kodifitseeris osa terrorismi järelvalve programmist (ingl k *Terrorist Surveillance Program*), mille USA president George W. Bush oli väljaspool FISA raamistikku salaja asutanud.⁷⁶ FISA paragrahvi 702 alusel saab USA valitsus jälgida isikute suhtlust (ingl k *communications*), kes arvatakse olevat USA territooriumist väljaspool, eesmärgiga koguda välisluureteavet.⁷⁷ Sellise teabe kogumiseks kasutavad luureametnikud „valijaid“ (ingl k *selectors*), nagu nt telefoninumbrid või e-posti aadressid.⁷⁸ Selleks, et selline luuretegevus oleks õiguspärane, ei tohi jälgitavad isikud olla „USA isikud“ (ingl k *United States Persons*), kes paragrahv 1801 punkti (i) kohaselt on USA kodanikud ja alalised elanikud.

Nagu eelmises lõigus mainitud, võivad USA luureametnikud FISA paragrahvi 702 alusel isikute suhtlust jälgida eesmärgiga koguda välisluureteavet.⁷⁹ Paragrahvi 702 kohaselt kuuluvad välisluureteabe alla rünnakud USA vastu, spionaaž, sabotaaž, rahvusvaheline terrorism, massihävitusrelvade levitamine ja viimaks, väga laia tõlgendamisruumiga kategooria: teave võõrvõimu või välisterritooriumi kohta, mis seondub USA välispoliitika teostamisega.⁸⁰ Õigusteadlased Peter Margulies ja Ira Rubinstein selgitavad, miks on problemaatiline, et viimasena nimetatud välisluureteabe kategooria on niivõrd laialt tõlgendatav. Nad toovad näiteks olukorra, kus USA välisluure jälgib välisriigi kodaniku kommunikatsioone, keda kahtlustatakse rahvusvahelise terrorirünnaku planeerimises. Interneti ülesehituse ja praeguste tehnoloogiliste piirangute tõttu eeldab sihtmärgi terrorismi puudutavatele e-kirjadele ligipääsu saamine ka sihtmärgi teistele e-kirjadele ligipääsu saamist. Analoogia toovad nad välja situatsiooni, kus isik vaatab e-kirja lehekülge, kus kuvatakse hiljuti saadetud sõnumeid. Sellel leheküljel on nähtavad mitmed erinevad e-

⁷⁵ Rubinstein, I., Margulies, P. Risk and Rights in Transatlantic Data Transfers: EU Privacy Law, U.S. Surveillance, and the Search for Common Ground. – Connecticut Law Review 2022/54(2), lk 401.

⁷⁶ Margulies, P. Searching for Accountability Under FISA: Internal Separation of Powers and Surveillance Law. – Marquette Law Review 2021/104. Kättesaadav: <https://scholarship.law.marquette.edu/mulr/vol104/iss4/6/> (12.02.2023), lk 1201.

⁷⁷ *Ibidem*.

⁷⁸ *United States vs Hasbajrami*, 945 F.3d 641 (2d Cir. 2019), p 653. Kättesaadav: <https://casetext.com/case/united-states-v-hasbajrami-2>.

⁷⁹ *Supra*, viide 22.

⁸⁰ Rubinstein, I., Margulies, P., lk 401.

kirjad: mõned, mis on tööga seotud, kui ka võib olla mõned isikliku iseloomuga e-kirjad. Praeguste tehnoloogiliste piirangute tõttu, kui USA välisluureametnik kogub FISA paragrahvi 702 alusel isiku e-kirju, siis lisaks terrorismitegevusega seonduvatele e-kirjadele kogutakse automaatselt ka samal leheküljel asuvad kõik teised e-kirjad, nt jälgitava isiku mõne pereliikme tervisliku seisundiga seonduvad.⁸¹ Magistritöö seisukohast on see oluline, sest selliselt mittevajaliku informatsiooni kogumine sarnaneb andmete masskogumisega, mida Euroopa Kohus on kritiseerinud ning sellise meetodi rakendamist lubanud ainult väga üksikutes olukordades.⁸² Lähemalt analüüsib autor masskogumisega seonduvaid probleeme peatükis 2.2.

Järgnevalt selgitab autor seda, kuidas käib FISA paragrahv 702 alusel signaalluure teostamiseks loa saamine. Selleks, et FISA paragrahvi 702 alusel jälgimist teostada, esitavad USA peaprokurör ja riigi luuredirektor välisluurekohtule iga-aastased kinnitused, mille kohaselt signaalluure teostamise oluline eesmärk on omandada välisluureteavet.⁸³ Kinnitustega koos tuleb esitada ka informatsioon selle kohta, missuguseid jälgimisprogramme hakatakse rakendama. Hiljemalt 30 päeva jooksul vaatab välisluurekohus kinnitused üle.⁸⁴ Kui kohus on kinnitused üle vaadanud ja heaks kiitnud, siis võivad luureanalüütikud alata FISA paragrahvi 702 alusel jälgimistegevuse.⁸⁵ Kohus kiidab jälgimise heaks juhul, kui need on seadusega kooskõlas ja ei riku USA põhiseaduse neljandast parandusest tulenevaid õiguseid.⁸⁶ Sisuliselt tähendab eeltoodu seda, et kohtu luba pole vaja konkreetsete isikute jälgimiseks ega kohus ei kontrolli ka seda, kas sihtmärgiks olevad isikud on üldse õigesti valitud, millele juhtis Euroopa Kohus ka Schrems II lahendis tähelepanu.⁸⁷ Samuti nagu varem mainitud⁸⁸, ei laiene eurooplastele ka USA põhiseaduse neljandast parandusest tulenevad õigused. Seega vaatamata sellele, et esmapilgul võiks tunduda, et jälgimise teostamise üle teostatakse põhjalikku kontrolli, siis

⁸¹ *Ibidem*, lk 403.

⁸² EKo *La Quadrature du Net*, p 139.

⁸³ Jaycox, M.M. lk 73.

⁸⁴ *Ibidem*.

⁸⁵ *Ibidem*.

⁸⁶ *Ibidem*.

⁸⁷ EKo *Schrems II*, p 179.

⁸⁸ Vt ptk 1.2.2.

eurooplaste jälgimisel esinevad õigusaktides kehtestatud kontrollimehhanismides puudujäägid.

1.3.2.2. Korraldus EO 12333

Teine EL-i vaatenurgast probleemne USA õigusakt, mis võimaldab signaalluuret teostada, on korraldus EO 12333⁸⁹ (ingl k *Executive Order 12333*).⁹⁰ Korraldus EO 12333 võeti vastu president Ronald Reagani poolt aastal 1981.⁹¹ Selle korralduse alusel toimub enamuse NSA signaalluuretegevusest, mille raames kogutakse isikuandmeid.⁹² Korraldus EO 12333 peamine fookus on luuretegevuse võimaldamine isikute suhtes, kes asuvad väljaspool USA-d ning kes ei ole „USA isikud“.⁹³ See annab volituse ka muud tüüpi jälgimiseks seni kuni konkreetne jälgimistegevus ei ole juba kaetud FISA-ga. See on oluline, sest FISA katab kogu elektroonilisest jälgimistegevusest ainult ühte väikest osa.⁹⁴

Euroopa Kohus kritiseeris lahendis *Schrems II* ka USA jälgimistegevust, mida viidi läbi Korraldus EO 12333 alusel. Korraldus EO 12333 käsitleb kõiki USA välisluure jälgimistegevusi, sh neid, mis jäävad väljapoole FISA mõjuala, nt luuretegevus, mida teostatakse välismaal ning mis on suunatud inimeste vastu, kes ei lähe „USA isikute“⁹⁵ alla. EO 12333 alusel võib NSA koguda, töödelda, analüüsida, toota ja jagada signaalluureteavet ja -andmeid, kui eeltoodud tegevuste eesmärk on toetada riiklike ja osakondlike missioone. Samuti on USA eraelu puutumatuse ja kodanikuvabaduste järelevalve komisjon (ingl k *Privacy and Civil Liberties Oversight Board* – edaspidi „PCLOB“) 2014. aastal koostatud raportis kirjeldanud, et USA valitsus teostab EO 12333 alusel välisluurega seonduvaid tegevusi ka väljaspool USA territooriumi inimeste osas, kes ei ole „USA isikud“. Mõnel juhul võib selline jälgimistegevus ka lausa koguda samasugust informatsiooni, mida USA

⁸⁹Executive Order 12333. United States Intelligence Activities. Kättesaadav: <https://www.archives.gov/federal-register/codification/executive-order/12333.html> (20.04.2023).

⁹⁰ Jaycox, M. M. No Oversight, No Limits, No Worries: Primer on Presidential Spying and Executive Order 12,333. – Harvard National Security Journal, 2021/12(1). Kättesaadav: <https://heinonline.org/HOL/P?h=hein.journals/harvardnsj12&i=59> (13.02.2023), lk 75.

⁹¹ *Ibidem*.

⁹² *Ibidem*.

⁹³ *Ibidem*.

⁹⁴ *Ibidem*.

⁹⁵ Vt definitsiooni „USA isikud“ kohta lähemalt ptk 1.3.2.1.

valitsus juba omandab FISA paragrahvi 702 alusel. Kuivõrd aga selline andmete kogumine toimub väljaspool USA territooriumi, siis ei rakendu sellele FISA paragrahvist 702 tulenevad piirangud luuretegevusele.⁹⁶ Piirangute puudumine on sisuliselt viinud lausa selleni, et NSA kogub korraldus EO 12333 alusel nii palju informatsiooni, et ei jõua seda kõike isegi analüüsida.⁹⁷

Korraldus EO 12333 sisaldab küll mõningaid kaitsemeetmeid, mida kohaldatakse välisriikide suhtes teostatava jälgimistegevuse sihtes, aga ka need privaatsuse kaitsemeetmed ei laiene välisriikide kodanikele.⁹⁸ Näiteks, välismaal läbiviidava jälgimistegevuse osas kohustab korraldus EO 12333 USA peaprokuröri kindlaks tegema, kas on tõenäoline, et jälgimistegevuse sihtmärk on välisvõimu agent, aga seda ainult juhul kui jälgimist teostatakse „USA isiku“ vastu, kelle jälgimiseks oleks korrakaitse tagamise eesmärkidel olnud vaja kirjalikku luba.⁹⁹ Lisaks sellele sätestab korraldus EO 12333 sõnaselgelt, et see ei tekita USA vastu ühtegi õiguslikult jõustatavat õigust ega hüve. Seetõttu leidis Euroopa Kohus *Schrems II* lahendis, et ELi andmesubjektidel ei olnud korraldus EO 12333 alusel jõustatavaid õigusi ning korraldus ei sisaldanud piisavaid kaitsemeetmeid, et piirata jälgimistegevust rangelt vajalikuga.¹⁰⁰

1.3.3. Signaalluure teostamist piiravad õigusaktid

1.3.3.1. Poliitikasuunis PPD-28

Magistritöö senise analüüsi põhjal on selgunud, kui laiad volitused on USA luureagentuuridele antud, et inimeste suhtes jälgimistegevust teostada. PCLOB-i poolt 2014. aasta juulis avaldatud raporti kohaselt kogus USA valitsus 2011. aasta seisuga igal aastal üle 250 miljoni interneti vahendusel toimuva suhtluse; sellele lisanduvad veel ka

⁹⁶ Linebaugh, C.D., Liu, E.C. EU Data Transfer Requirements and U.S. Intelligence Laws: Understanding *Schrems II* and Its Impact on the EU-U.S. Privacy Shield. Congressional Research Service, 17.03.2021/R46724. Kättesaadav: <https://sgp.fas.org/crs/row/R46724.pdf> (20.04.2023), lk 11.

⁹⁷ Jaycox, M.M., lk 89.

⁹⁸ Linebaugh, C.D., Liu, E.C., lk 11.

⁹⁹ *Ibidem*.

¹⁰⁰ EKo *Schrems II*, p 184 ja 192.

telefonivestlused.¹⁰¹ PCLOB märkis veel ka, et 2014. aasta seisuga on see number tõenäoliselt juba märgatavalt suurem.¹⁰² Ilmselt mõistis USA valitsus ühel hetkel ka ise, et selline sisuliselt ilma piirideta signaalluure ei tohiks olla lubatud, mistõttu võttis 2014. aasta 17. jaanuaril – umbes 7 kuud peale Edward Snowdeni paljastusi USA luuretegevuse kohta – tollane president Barack Obama vastu presidentiaalse poliitikasuunise nr 28¹⁰³ (Presidential Policy Directive 28 – edaspidi „PPD-28“). Suunis PPD-28 kui täitevvõimu poolt välja antud poliitikasuunis omab samasugust materiaalõiguslikku mõju nagu presidendi korraldus ning jääb jõusse ka täitevvõimu vahetumisel.¹⁰⁴ Magistritöö kirjutamise seisuga on PPD-28 komponent, mis käsitleb signaalluurele rakendatavaid piiranguid, asendatud korraldusega EO 14086¹⁰⁵, mille kohta annab siinkirjutaja ülevaate järgmises alapeatükis.

PPD-28 nägi ette kaitsemeetmed, mille eesmärk on kaitsta nende välisriikide kodanike privaatsust, kelle teabevahetust USA luureagentuurid juhuslikult koguvad teiste välisriikide kodanike jälgimisel, kes võivad kujutada ohtu USA riiklikule julgeolekule.¹⁰⁶ Suunise PPD-28 eesmärk oli kindlaks määrata põhimõtted kas, miks, millal ja kuidas võib USA läbi viia signaalluure välisluure ja vastuluure raames, austades samaaegselt demokraatlikke printsiipe, universaalseid inimõiguseid, ülemaailmset kaubandust, eraelu puutumatust ja kodanikuvabadusi.¹⁰⁷

PPD-28 käsitleb mitmeid probleeme: riskid USA suhetele partnerriikidega; majanduslikud mõjud, mis kaasnevad usalduse kaotusega USA ettevõtetele ja teiste riikide vähenenud tahe

¹⁰¹ Medine, D jt. Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act. Privacy and Civil Liberties Oversight Board, 02.07.2014. Kättesaadav: <https://irp.fas.org/offdocs/pclob-702.pdf> (20.04.2023), lk 116.

¹⁰² *Ibidem*.

¹⁰³ Presidential Policy Directive 28 regarding signals intelligence activities. Kättesaadav: <https://obamawhitehouse.archives.gov/the-press-office/2014/01/17/presidential-policy-directive-signals-intelligence-activities> (20.04.2023).

¹⁰⁴ USA justiitsministeeriumi õigusbüroo seisukoht. Legal Effectiveness of a Presidential Directive, as Compared to an Executive Order; 29.01.2000. Kättesaadav: <https://www.justice.gov/olc/opinion/legal-effectiveness-presidential-directive-compared-executive-order> (15.02.2023).

¹⁰⁵ Executive Order 14086. Enhancing Safeguards for United States Signals Intelligence Activities. Kättesaadav: <https://www.presidency.ucsb.edu/documents/executive-order-14086-enhancing-safeguards-for-united-states-signals-intelligence> (20.04.2023).

¹⁰⁶ Cameron, K, Raul, A.C. The Economic Case for Preserving PPD28 and Privacy Shield. Lawfare, 17.01.2017. Kättesaadav: <https://www.lawfareblog.com/economic-case-preserving-ppd-28-and-privacy-shield> (14.02.2023).

¹⁰⁷ *Ibidem*.

osaleda rahvusvahelistes andmeajamise, privaatsuse ja regulatiivsetes režiimides; usalduse kaotus USA võetud kohustuste kohta, mis seonduvad ülemaailmselt turvalise interneti tagamisega; ning luureallikate- ja meetodite kaitsmine.¹⁰⁸ PPD-28 rõhutab samuti põhimõtet, mille kohaselt kõigil isikutel, olenemata kodakondsusest, on õigustatud huvi privaatsusele oma isikuandmete töötlemisel.¹⁰⁹ President Barack Obama võttis PPD-28 vajalikkuse kokku, öeldes, et nagu me tasakaalustame julgeolekut ja privaatsust kodudes, nõuab meie ülemaailmne juhtpositsioon, et tasakaalustaksime oma julgeolekunõudeid vajadusega säilitada usaldus ja koostöö inimeste ja juhtidega ümber maailma.¹¹⁰

PPD-28 vastu võtmise järgselt tekkis palju vaidlusi küsimuses, kas nimetatud akt oli reaalne samm edasi privaatsusõiguse kaitseks või oli tegu lihtsalt sümboolse žestiga, mille eesmärk oli näidata avalikkusele, et USA tegeleb probleemiga, aga praktikas signaalluure teostamisel palju ei muutu.¹¹¹ Tagasi vaadates võib siinkirjutaja hinnangul nüüd väita, et õigus oli sellel koolkonnal, kes arvas, et tegu on pigem žestiga ja sisuliselt olukord ei muutu. Seda seisukohta jagas Euroopa poolt vaadatuna Euroopa Kohus *Schrems II* lahendis, kus kohus leidis, et vaatamata PPD-28 poolsete piirangutele signaalluure teostamisele, ei vasta USA luureagentuuride teostatav signaalluure proportsionaalsuse põhimõttest tulenevatele nõuetele.¹¹²

1.3.3.2. Korraldus EO 14086

President Biden kirjutas 7. oktoobril 2022 alla korraldusele EO 14086.¹¹³ Korralduse EO 14086 vastu võtmine oli tingitud Euroopa Komisjoni ja USA valitsuse läbirääkimistest eesmärgiga rajada uus andmekaitseraamistik, mis vastaks EL-i õigusest tulenevatele

¹⁰⁸ The White House. Press Release of the Office of the Press Secretary. Presidential Policy Directive Signals Intelligence Activities (PPD-28). Kättesaadaval: <https://obamawhitehouse.archives.gov/the-press-office/2014/01/17/presidential-policy-directive-signals-intelligence-activities> (15.02.2023).

¹⁰⁹ *Ibidem*.

¹¹⁰ The White House. Press Release of the Office of the Press Secretary. Remarks by the President on Review of Signals Intelligence. Kättesaadav: <https://obamawhitehouse.archives.gov/the-press-office/2014/01/17/remarks-president-review-signals-intelligence> (15.02.2023).

¹¹¹ Machtiger, P. G. Fixing PPD-28: Implementation Issues and Proposed Revisions for Privacy Protections in Signals Intelligence. – New York University Journal of Legislation and Public Policy 2020/23(1). Kättesaadav: <https://heinonline.org/HOL/P?h=hein.journals/nyulpp23&i=233> (14.02.2023), lk 232.

¹¹² EKo *Schrems II*, p 183.

¹¹³ Lawne, R. EO 14086 and the EU-U.S. Data Privacy Framework. Fieldfisher, 22.11.2022. Kättesaadav: <https://www.fieldfisher.com/en/insights/eo-14086-and-the-eu-us-data-privacy-framework> (24.04.2023).

nõuetele ning Euroopa Kohtu varasemale kriteeriale.¹¹⁴ See asendab ka suunise PPD-28 sätteid, mis varasemalt reguleerisid signaalluure teostamist ja sellele piirangute seadmist.¹¹⁵

Korraldus EO 14086 paragrahv 2 punkt (b)(i)(A) seab täiendavad sisulised piirangud, määratledes 12 legitiimset eesmärki, mille korral on signaalluureteabe kogumine lubatud.

Need 12 eesmärki on järgnevad:

1. välisriigi valitsuse, välisriigi sõjaväe, välisriigi rühmituse, välisriigis asuva poliitilise organisatsiooni või sellise välisriigi valitsuse või sõjaväe nimel tegutseva või nende kontrolli all tegutseva üksuse mõistmine või hindamine;
2. välismaiste organisatsioonide, sealhulgas rahvusvaheliste terroriorganisatsioonide võimete, kavatsuste tegevuste mõistmine või hindamine, mis kujutavad kohest või potentsiaalset ohtu USA või tema liitlaste või partnerite riiklikule julgeolekule;
3. globaalset julgeolekut mõjutavate rahvusvaheliste ohtude, sealhulgas kliima- ja muude ökoloogiliste muutuste, rahvatervise riskide, humanitaarohutude, poliitiliste ebastabiilsuste ja geograafiliste rivaalitsemissete mõistmine või hindamine;
4. välismaiste sõjaliste võimete ja tegevuste eest kaitsmine;
5. kaitsmine terrorismi, pantvangide võtmise ja isikute vangistuses hoidmise eest (sealhulgas pantvangide ja vangide tuvastamine, asukoha määramine ja päästmine) välisriigi valitsuse, välisorganisatsiooni või välisriigi isiku poolt või nimel;
6. kaitsmine spionaaži, sabotaaži, mõrva või muu luuretegevuse eest, mida viib läbi, aitab läbi viia välisriigi valitsus, välisorganisatsioon või välismaa isik või seda tehakse nende nimel;
7. kaitsmine massihävitussrelvade või nendega seotud tehnoloogiate arendamise, omamise või levikuga seotud ohtude eest ning välisriigi valitsuse,

¹¹⁴ *Ibidem.*

¹¹⁵ Euroopa Andmekaitseametnikute arvamus (2023), p 19.

välisorganisatsiooni või välisriigi isiku poolt, nimel või abiga toime pandud ohtude eest;

8. kaitsmine välisriigi valitsuse, välisorganisatsiooni või välisriigi isiku loodud või ära kasutatud küberjulgeolekuohtude või pahatahtliku kübertegevuse eest, mida teostab välisriigi valitsus, välisorganisatsioon, või välismaa isik või tehakse seda nende nimel;
9. USA või tema liitlaste või partnerite töötajaid ähvardavate ohtude eest kaitsmiseks;
10. kaitsmine rahvusvaheliste kuritegelike ohtude eest, sealhulgas ebaseadusliku rahastamise ja sanktsioonidest kõrvale hoidmise eest, mis on seotud ühe või mitme selle paragrahvi lõigus b(i) nimetatud eesmärgiga;
11. valimiste ja poliitiliste protsesside, valitsuse vara ja USA infrastruktuuri (nii füüsilise kui elektroonilise) terviklikkuse kaitsmine välisriigi valitsuse, välisorganisatsiooni või välisriigi isiku poolt, nimel või abiga läbi viidud tegevuse eest;
12. andmekogumise või operatiivsuutlikkuse või tegevuste edendamine, et edendada paragrahvi lõigus b(i) määratletud legitiimset eesmärki.

Samuti näeb korraldus EO 14086 paragrahv 2(B) ette, et president võib eelnevalt nimetatud eesmärkide loetelu laiendada, võttes arvesse uusi riikliku julgeoleku nõudeid, nagu uued või kõrgendatud ohud USA riiklikule julgeolekule. Kuigi korralduse EO 14086 sama säte näeb ette, et luuredirektor teeb avalikuks presidendi muudatused lubatud eesmärkidele, siis on selle avalikuks tegemise nõudele kehtestatud erand. Selle erandi kohaselt võib president keelata eesmärkide muudatuste avalikuks tegemise, kui see võib ohustada USA riikliku julgeolekut. Sellist mitteavalikku õigusaktide muutmist võib sisuliselt käsitleda salaõigusena, millega kaasnevaid õiguslikke probleeme ja selle vastavust EL-i õigusele analüüsib siinkirjutaja peatükis 2.1.

Korraldus EO 14086 paragrahv 3 kehtestab ka kolmeastmelise mehhanismi õiguskaitsevahendite kasutamiseks „kvalifitseeritud riikide“ jaoks, mille hulka kuuluvad riigid või piirkondlikud majanduslikud organisatsioonid, mille määrab USA peaprokurör, konsulteerides riigisekretäri, kaubandusministri ning riikliku luuredirektoriga, peale seda kui on kindlaks tehtud, et nendel riikidel on 1) seadused, mis nõuavad asjakohaseid

kaitsemeetmeid signalluuretegevuse läbiviimisel USA-st nende territooriumile edastatud USA isikute isikuandmete osas; 2) nad lubavad või eeldatavasti lubavad isikuandmete edastamist ärilistel eesmärkidel USA ja oma territooriumi vahel; 3) nende määramine „kvalifitseeritud riikideks“ võib edendada USA rahvuslikke huve.¹¹⁶

See „kvalifitseeritud riikide“ eeltingimus on käesoleva magistritöö seisukohast oluline, sest just selle alusel saaksidki hakata eurooplased – kes arvavad, et signaalluure teostades on rikutud nende õigusi – õiguskaitsevahendeid kasutama. Euroopa Komisjoni adekvaatsusotsuse eelnõu kohaselt kavatseb USA lisada EL-i „kvalifitseeritud riikide“ nimekirja.¹¹⁷ Samuti on eelnõus komisjon selgitanud, et adekvaatsusotsus jõustubki ainult tingimusel, et EL tervikuna sinna lisatakse.¹¹⁸

Uue mehhanismi esimene aste on kodanikuvabaduste ja eraelu puutumatuse voliniku (ingl k *Civil Liberties Protection Officer* – edaspidi „CLPO“) poolt kvalifitseeruvate kaebuste esialgne uurimine. Kvalifitseeruva riigi pädev ametiasutus võib esitada CLPO-le kaebuse, kui nende arvates on aset leidnud rikkumine, mis viitab kvalifitseeruvast riigist USA-sse edastatud andmetega seotud luuretegevusele, mis 1) mõjutab negatiivselt kaebuse esitaja eraelu puutumatust ja kodanikuvabadusega seonduvaid huve; 2) rikub korraldust EO 14086 või muid kohalduvaid USA seaduseid. Kui CLPO teeb kaebuse esitaja kasuks otsuse, siis on tal pädevus määrata sobiv viis, kuidas rikkumine tuleks heastada. Korraldus EO 14086 näeb ette, et USA luurekogukond toetaks ning abistaks CLPO-d uurimise läbiviimiseks vajalikule teable ligipääsu saamisel ning CLPO poolt kaebuse läbivaatamisel. CLPO poolt tehtud otsused on luurekogukonna jaoks siduvad.¹¹⁹

Teine etapp on DPRC poolt kaebuste läbivaatamine, mille näol on tegemist kohtuorganiga, mille otsused on samuti kõikide luurekogukonna elementide jaoks siduvad. DPRC-sse määratakse kohtunikud, kelle nimetab ametisse USA peaprokurör, konsulteerides kaubandusministri, luuredirektori ja PCLOB-iga, kes koosnevad õiguspraktikutest ning

¹¹⁶ Johnson, C., Liu, Y. What's in Biden's Executive Order on Signals Intelligence? – Lawfare, 14.10.2022. Kättesaadav: <https://www.lawfareblog.com/whats-bidens-executive-order-signals-intelligence> (20.04.2023).

¹¹⁷ Adekvaatsusotsuse eelnõu, lk 47, joonealune viide 320.

¹¹⁸ *Ibidem*, lk 54.

¹¹⁹ *Ibidem*.

kellel on asjakohane kogemus andmekaitse ja riikliku julgeoleku küsimustes, kes ei ole USA valitsuse töötajad ning kellel on eelistatult eelnev kogemus kohtunikuna. Peale CLPO poolt esimeses astmes tehtud otsust saavad nii kaebaja kui ka luurevõrgustik esitada DPRC-le läbivaatamiseks apellatsiooniavalduse. Seejärel kutsub DPRC kaasuse arutamiseks kokku kolmest kohtunikust koosneva kolleegiumi, kes on kõik läbinud eelneva julgeolekukontrolli. Kaebuse esitaja huvide eest määratakse seisma ka eriadvokaat (ingl k *special advocate*), kes saab samuti kohtukolleegiumiga suhelda ja neile juhtumiga seonduvat vajalikku informatsiooni edastada.¹²⁰

Kolmas aste on PCLOB-i poolt iga-aastane esimese kahe astme läbi vaatamine. Korralduse EO 14806 alusel kohustatakse PCLOB-i läbi viima iga-aastast kaebuste menetlemise protsessi, sh kontrollima, kas:

- (1) CLPO ja DPRC menetlesid kaebuseid nõutava aja jooksul;
- (2) CLPO ja DPRC saavad menetlemiseks vajaminevale teabele täieliku ligipääsu;
- (3) CLPO ja DPRC tegutsevad kooskõlas korralduses EO 14086 sätestatud nõuetega;
- (4) CLPO ja DPRC võtavad nõuetekohaselt arvesse korraldus EO 14086 artiklis 2 sätestatud kaitsemeetmeid;
- (5) luurekogukond on täielikult järginud CLPO ja DPRC poolt tehtud otsuseid.¹²¹

1.4. USA poolt varasemad loodud andmekaitseraamistikud andmevahetuseks EL-iga ja seonduvad Euroopa Kohtu lahendid

1.4.1. Safe Harbor ja Euroopa Kohtu lahend *Schrems*

Magistritöö autor selgitas peatükis 1.2, et EL ja USA lähenevad isikuandmete kaitsmisele fundamentaalselt erinevalt. EL-i ja USA ametnikud mõistsid, et pärast Euroopa Parlamendi ja nõukogu direktiivil 95/46/EÜ¹²² (edaspidi „andmekaitse direktiiv 95/46“) vastu võtmist

¹²⁰ *Ibidem*.

¹²¹ *Ibidem*.

¹²² Euroopa Parlamendi ja nõukogu 24.10.1995. a direktiiv 95/46/EÜ üksikisikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise kohta; ELT L 281, 23.11.1995, lk 31-50.

1995. aastal, töötasid olulised erinevused nende andmekaitseraamistike vahel häirida või takistada isikuandmete edastamist EL-i ja USA vahel. Nad muretsesid, et need erinevad lähenemised andmekaitsele võivad negatiivselt mõjutada paljusid ettevõtteid ja tööstuseid mõlemal pool Atlandi ookeani ning samuti võib see mõjutada EL-i ja USA vahelist kaubandus-ja investeerimissuhet.¹²³ Pärast USA ja EL-i vahelisi läbirääkimisi leppisid pooled kokku mehhanismis, mis võimaldaks USA ettevõtetel tagada piisav andmekaitse tase, nagu seda nõudis andmekaitse direktiiv 95/46. 2000. aastal andis USA kaubandusministeerium välja *Safe Harbori* privaatsuspõhimõtted, mida seejärel tunnustas ka Euroopa Komisjon.¹²⁴ Kokku lepiti seitsmes põhimõttes: 1) teatamise põhimõte; 2) valikuvõimaluse põhimõte; 3) kolmandatele osapooltele edastamise põhimõte; 4) turvalisuse põhimõte; 5) andmeterviklikkuse põhimõte; 6) juurdepääsu põhimõte; 7) nõuete täitmise tagamise põhimõte.¹²⁵

Safe Harbor andmekaitseraamistikus võisid osaleda kõik USA organisatsioonid, kes kuulusid USA föderalse kaubanduskomisjoni (ingl k *Federal Trade Commission* – FTC) reguleerimisalasse, kelle ülesandeks on kontrollida, et USA tarbijakaitse seadustest peetaks kinni; sh nendest, mis on seotud ebaausate ja petlike töövõtetega ning nendest, mis on seotud USA lennuettevõtete ja piletiagentuuride tegevusega, kellele kohaldub USA transpordiministeeriumi (ingl k *Department of Transportation* – DOT) regulatsioon. *Safe Harbori* nimekirjas oli umbes 4500 ettevõtet. Selleks, et oleks võimalik organisatsiooni sinna nimekirja lisada, pidi vastav organisatsioon ise kinnitama, et nad järgivad *Safe Harbori* põhimõtteid. Samuti kinnitas FTC, et on võtnud endale kohustuse läbi vaadata kõik viited rikkumistele, mis neile EL-i liikmesriikide asutuste poolt saadetakse.¹²⁶

Nii erasektori juriidilised isikud kui ka föderalsed ja osariikide ametiasutused, kelle ülesanne on kontrollida ebaausate ja petlike töövõtete kasutamist reguleerivate seadustest kinnipidamist, pidid *Safe Harbori* kokkulepet jõustama (ingl k *enforce*). Erasektori poolne

¹²³ Weiss, M.A., Archick, K. U.S.-EU Data Privacy: From Safe Harbor to Privacy Shield. Congressional Research Service, 19.05.2016/R44257. Kättesaadav: <https://sgp.fas.org/crs/misc/R44257.pdf> (19.04.2023), lk 5.

¹²⁴ *Ibidem*.

¹²⁵ *Ibidem*, lk 5-6.

¹²⁶ *Ibidem*.

kontrollimine koosnes kolmest elemendist: verifitseerimine, vaidluste lahendamine ning õiguskaitsevahendite tagamine. Pidev nende elementide rikkumine tähendas seda, et organisatsioon eemaldati *Safe Harbori* nimekirjast, mille kohta tehti ka *Safe Harbori* ametlikul veebilehel vastav muudatus.¹²⁷

6. oktoobril 2015. aastal avaldas Euroopa Kohus otsuse, millega tunnistas *Safe Harbori* kehtetuks. Euroopa Kohtu otsuse tingis Austria kodaniku Max Schrems poolt esitatud kaebus Iirimaa andmekaitsevolinikule.¹²⁸ Kaebuses tõi Schrems välja, et Facebooki poolt tema isikuandmete edastamine EL-is (Iirimaa) asuvast serverist USA-s asuvasse serverisse rikub EL-i õigust, sest USA-s ei tagata isikuandmetele piisavat kaitset, võttes arvesse 2013. aasta juunis Snowdeni poolt avalikustatud informatsiooni seoses USA luuretegevusega.¹²⁹ Iirimaa andmekaitsevolinik jättis kaebuse rahuldamata, märkides, et tal puudub pädevus kaebust menetleda, sest Facebook edastas isikuandmeid tuginedes *Safe Harbori* raamistikule. Seetõttu oli Iiri andmekaitsevolinik enda hinnangul seotud Euroopa Komisjoni 2000. aastal välja antud adekvaatsusotsusega¹³⁰, milles komisjon kinnitas, et *Safe Harbori* alusel tagatav andmekaitse tase on andmekaitse direktiiv 95/46 kontekstis piisav. Iirimaa Kõrge Kohtu (ingl k *High Court*) taotlusel vaagis Euroopa Kohus, kas Iirimaa andmekaitsevolinik võib uurida Facebooki poolt kasutatavaid andmekaitsemeetmeid eesmärgiga hinnata nende meetmete piisavust või kas Iirimaa andmekaitsevolinik pidi lähtuma Euroopa Komisjoni 2000. aastal tehtud otsusest *Safe Harbori* piisavuse kohta.¹³¹

Euroopa Kohus tegi enda 2015. aasta 6. oktoobril avaldatud otsuses mitu järeldust, millest esimene oli see, et Euroopa Komisjoni poolt eksisteeriv adekvaatsusotsus kolmanda riigi andmekaitse taseme kohta ei tähenda seda, et EL-i liikmesriikide andmekaitseasutused ei omaks pädevust hinnata selle kolmanda riigi andmekaitse taset ning seda, kas EL-i kodanike – kelle andmeid kolmandasse riiki töötlemiseks edastatakse – töödeldakse kooskõlas EL-i

¹²⁷ *Ibidem*.

¹²⁸ EKo *Schrems*, p 28.

¹²⁹ *Ibidem*, p 28.

¹³⁰ Euroopa Komisjoni otsus, 26. juuli 2000, vastavalt Euroopa Parlamendi ja nõukogu direktiivile 95/46/EÜ piisava kaitse kohta, mis on ette nähtud programmi Safe Harbor põhimõtetega ja sellega seotud korduma kippuvate küsimustega, mille on välja andnud Ameerika Ühendriikide kaubandusministeerium; 2000/520/EÜ. – ELT L

215/7, 25.08.2000, lk 119-138.

¹³¹ Weiss, M.A., Archick, K, lk 6-7.

õigusest tulenevate nõuetega, eeskätt andmekaitse direktiiviga 95/46 ja põhiõiguste hartaga.¹³² Teine järeldus oli see, et Euroopa Kohus tunnistas andmekaitseraamistiku *Safe Harbor* kehtetuks, põhjusel, et Euroopa Komisjon ei olnud sisuliselt hinnanud, kas USA tagab enda siseriikliku õiguse või endale võetud rahvusvaheliste kohustustega sisuliselt samaväärse kaitsetaseme, nagu on tagatud EL-is.¹³³ Kõnealuse magistratöö kontekstis on aga kõige olulisem järgnev järeldus, mille Euroopa Kohus selles lahendis tegi ning mille on tabavalt kokku võtnud Carel Kivimaa enda 2017. aastal kirjutatud magistratöös. Võttes kokku Euroopa Kohtu otsuse punktid 86-88 ja 89-98, märkis Kivimaa, et *Safe Harbor* võimaldas USA andmetöötlejatel riikliku julgeoleku, avaliku huvi või õiguskorra tagamise eesmärgidel *Safe Harbori* andmetöötluspõhimõtetest piiramatult kõrvale kalduda.¹³⁴ EL-i õiguse kohaselt aga peab õigusakt, millega kaasneb sekkumine põhiõigusesse (nagu nt õigus privaatsusele ja õigus andmekaitsele), sisaldama täpseid ja selgeid õigusnorme, mis reguleerivad selle meetme ulatust ja kohaldamisala ning millega on kehtestatud miinimumnõuded, nii et andmesubjektidel oleksid piisavad tagatised, mis võimaldavad nende andmeid tõhusalt kuritarvitamise ohu ning ebaseadusliku juurdepääsu ja kasutamise eest kaitsta.¹³⁵ See aga tähendas, et andmekaitseraamistiku *Safe Harbor* alusel edastatavad Euroopa kodanike isikuandmed võisid sattuda USA ametiasutuste valdusesse.¹³⁶ Seesuguseid olukordi aga *Safe Harbor* ei reguleerinud.¹³⁷ Samuti puudus sellistes olukordades vajalik järelevalve, mistõttu ei taganud *Safe Harbor* Euroopa kodanikele sisuliselt samaväärset andmekaitse taset andmekaitse direktiiv 95/46 artikkel 25 lõike 6 tähenduses.¹³⁸

1.4.2. Privacy Shield ja Euroopa Kohtu lahend *Schrems II*

USA ja EL-i vahelised arutelud seoses *Safe Harbori* raamistiku ajakohastamisega algasid juba 2013. aasta lõpus vastuseks kasvavale eurooplaste murele USA luureagentuuride jälgimisprogrammide pärast. Isegi enne Snowdeni 2013. aasta juunis tehtud paljastusi olid

¹³² Ibidem, lk 7.

¹³³ EKo *Schrems*, p 96-97.

¹³⁴ Kivimaa, C., lk 36.

¹³⁵ Ibidem.

¹³⁶ Ibidem.

¹³⁷ Ibidem.

¹³⁸ Ibidem.

mõned Euroopa privaatsusaktivistid juba pikemat aega väitnud, et *Safe Harbori* andmekaitseraamistik sisaldas endas olulisi andmekaitsetõrkeid. Nad väitsid näiteks, et mõned ettevõtted ei rakendanud *Safe Harbori* nõudeid täielikult, kuna nõuete täitmise osas ei olnud kohustuslik iga-aastane vastavuskontrolli läbiviimine ning aastate jooksul oli sadu ettevõtteid esitanud valeväiteid selle kohta, et nad kuuluvad *Safe Harbori* nimekirja.¹³⁹ Teised leidsid, et USA poolt *Safe Harbori* nõuete täitmise kontroll on puudulik, juhtides tähelepanu sellele, et FTC esitas hagi ainult kümne ettevõtte vastu esimese 13 aasta jooksul, mil *Safe Harbori* raamistik oli kehtinud.¹⁴⁰ Samuti väitsid kriitikud, et *Safe Harbori* tingimustes lepitati kokku 1990. aastate lõpus, kui internet oli alles lapsekingades, mistõttu oleks aeg seda ümber hinnata ja ajakohastada.¹⁴¹

Sellise kriitika ning samuti väidete tõttu, et mõned *Safe Harboris* osalevad ettevõtted, sh nt Microsoft ja Google, võisid olla seotud USA luuretegevusega, kutsusid mitmed Euroopa andmekaitseametnikud ja Euroopa Parlamendi liikmed üles Euroopa Komisjoni *Safe Harbori* raamistiku alusel andmeedastust peatama. Euroopa Komisjon keeldus seda tegemast põhjendusel, et see kahjustaks EL-i ärilisi huve ning Atlandi-ülest majandust. Vaatamata sellele nõustus Euroopa Komisjon, et *Safe Harboris* eksisteerib mitmeid puudujääke. 2013. aasta novembris andis Euroopa Komisjon välja 13 soovitus¹⁴², mille eesmärk oli *Safe Harborit* turvalisemaks muuta. Sinna alla kuulus ka USA ametiasutuste juurdepääsu piiramine isikuandmetele, mida *Safe Harborile* tuginedes USA-sse edastatakse.¹⁴³ Läbirääkimiste vältel – nii enne kui ka pärast Euroopa Kohtu otsust asjas *Schrems* – olidki väidetavalt võtmeküsimusteks *Safe Harbori* erandid, mis võimaldasid riikliku julgeoleku kaalutlustel andmetele ligipääsu ning samuti EL-i poolsed nõuded, mille kohaselt tuleks sellist ligipääsu piirata.¹⁴⁴ 2016. aasta veebruaris teatasid USA ja EL-i ametnikud, et on jõutud kokkuleppele raamistikus, millega *Safe Harbor* asendatakse. Uue raamistiku nimeks sai *Privacy Shield*, mis pidi võimaldama EL-i kodanike isikuandmeid

¹³⁹ Weiss, M.A., Archick, K., lk 9.

¹⁴⁰ Nielsen, N. Hundreds of US companies make false data protection claims. – EUObserver, 08.10.2013. Kättesaadav: <https://euobserver.com/rule-of-law/121695> (19.04.2023).

¹⁴¹ Weiss, M.A., Archick, K., lk 9.

¹⁴² Vt Euroopa Komisjoni pressiteade. European Commission calls on the U.S. to restore trust in EU-U.S. data flows. Kättesaadav: https://ec.europa.eu/commission/presscorner/detail/en/IP_13_1166 (20.04.2023).

¹⁴³ Weiss, M.A., Archick, K., lk 9.

¹⁴⁴ *Ibidem*.

jättkuvalt USA-sse edastada, kuid järgides Euroopa Kohtu poolt asjas *Schrems* kehtestatud nõudeid.¹⁴⁵

29. veebruaril 2016 avaldasid USA ja EL-i ametiasutused uue andmeedastusraamistiku täisteksti ja seda täiendavad dokumendid. Uus raamistik oli *Safe Harboriga* võrreldes oluliselt pikem ja detailsem. *Privacy Shield* sisaldas küll sisuliselt samu seitset põhimõtet, mis eksisteerisid juba *Safe Harboris*, aga *Privacy Shield* hõlmas endas ka täiendavaid põhimõtteid, mille eesmärk oli peamiselt eelnimetatud põhimõtteid täpsustada, toetada ja selgitada. Need täiendavad põhimõtted käsitlesid peamiselt tundlike isikuandmeid, kolmandate isikute vastutust, andmekaitseasutuste pädevust ja volitusi, personaliandmeid, ravimeid ja meditsiinitooteid ning avalikult kättesaadavaid andmeid. Erinevalt *Safe Harborist* sisaldas *Privacy Shield* ka USA riikliku julgeoleku ametnike poolt antud kinnitusi ja valitsusametnike kirju, mis puudutasid *Privacy Shieldi* poolt pakutavat kaitset EL-i kodanike isikuandmetele. *Privacy Shieldiga* lisandus täiendavalt veel ka mehhanism vaidluste lahendamiseks.¹⁴⁶

EL-i ja USA ametiasutuste sõnul adresseeris *Privacy Shield* Euroopa Kohtu poolt lahendis *Schrems* tõstatatud probleemkohti. *Privacy Shieldiga* lubati võtta täiendavad kohustused, rangemalt *Privacy Shieldi* nõuete täitmist kontrollida, sätestada selgemad kaitsemeetmed ja läbipaistvuskohustused ning efektiivselt tagada EL-i kodanike õiguste kaitsmine mitmete erinevate õiguskaitsevahenditega.¹⁴⁷ Kõnealuse magistritöö kontekstis on olulisemad viimased kaks:

1. USA justiitsministeerium ja riikliku luuredirektori büroo andsid kirjalikud kinnitused, et USA ametiasutuste ligipääs EL-i kodanike isikuandmetele allutatakse selgetele piirangutele, kaitsemeetmetele ning järelevalvemehhanismidele. Samuti väitis USA valitsus, et *Privacy Shieldi* vastuvõtmisega välistatakse ka USA luureagentuuride poolt teostatav massjälgimine isikuandmete suhtes, mida EL-ist USAsse edastatakse;

¹⁴⁵ *Ibidem*.

¹⁴⁶ *Ibidem*, lk 9-10.

¹⁴⁷ *Ibidem*, lk 10.

2. USA välisministeeriumi valitsusalasse luuakse eriombudsman, kelle ülesanne on läbi vaadata kaebused seoses USA luureagentuuride ligipääsuga EL-i kodanike isikuandmetele. Loodav kaebuste lahendamise mehhanism pidi olema luureagentuuridest sõltumatu ning tal pidi olema pädevus kaebusi läbi vaadata olukordades, tingimusel, et EL-i kodanik – kes kahtlustab, et tema õigusi on rikutud – võtab ombudsmaniga ühendust läbi enda kohaliku EL-i andmekaitseasutuse.¹⁴⁸

Peale *Privacy Shieldi* andmevahetusraamistiku avaldamist kirjutas selle suhtes arvamuse WP29 töögrupp. Kuigi töögrupp märkis, et uus andmekaitseraamistik sisaldab enda eelkäijaga võrreldes mitmeid parandusi, väljendas WP 29 töögrupp siiski suurt muret mitmete äriliste ja riikliku julgeolekuga seonduvate aspektide pärast. Kõnealuse magistritöö kontekstis olid neist kõige olulisemad: 1) mehhanismid õiguskaitsevahendite kasutamiseks on liiga keerulised; 2) USA riigiametnike antud kinnitused – mille kohaselt masskogutud isikuandmetele ligipääsu korral on ette nähtud selged piirangud, kaitsemeetmed ning järelevalvevalve – ei ole WP29 töögrupi hinnangul siiski piisavad, et vastata EL-i õigusest tulenevatele nõuetele.¹⁴⁹

Vaatamata WP29 töögrupi poolt tähelepanu juhitud probleemkohtadele võttis Euroopa Komisjon siiski 12. juulil 2016. aastal vastu adekvaatsusotsuse 2016/1250, millega kinnitas, et USA tagab piisava kaitsetaseme isikuandmetele, mida EL-ist USA-s paiknevatele organisatsioonidele *Privacy Shieldi* alusel edastatakse.¹⁵⁰ Seejärel sõnastas Max Schrems, kelle kaebusest alguse saanud menetluse tulemusena tunnistas Euroopa Kohus lahendis *Schrems* kehtetuks raamistiku *Safe Harbor*, enda esialgselt Iirimaa andmekaitsevolinikule esitatud kaebuse ümber. Max Schrems leidis ümbersõnastatud kaebuses, et standardsed andmekaitseklauslid – millele tuginedes Facebook edastab oma teenuse osutamisel isikuandmeid EL-ist USA-sse – ei paku piisavat kaitset selle vastu, et USA luureagentuurid isikuandmetele ligi ei pääseks ning samuti üleüldiselt, et andmekaitseraamistik *Privacy Shield* ei paku andmekaitse taset, mis vastaks EL-i õigusest tulenevatele nõuetele.¹⁵¹ Iirimaa

¹⁴⁸ *Ibidem*, lk 10.

¹⁴⁹ *Ibidem*.

¹⁵⁰ Vt adekvaatsusotsus 2016/1250, artikkel 1 lg 1.

¹⁵¹ EKo *Schrems II*, p 50-57.

andmekaitsevolinik pöördus seejärel Iirimaa Kõrge Kohtu poole, kes omakorda esitas Euroopa Kohtule eelotsusetaotluse. Eelotsusetaotluses küsis Iirimaa Kõrge Kohus esiteks, kas EL-ist USA-sse standardsete andmekaitseklauslite alusel¹⁵² isikuandmete edastamine rikub andmesubjektide põhiõiguste harta artiklitest 7 või 8 tulenevaid õigusi ning teiseks, kas standardsete andmekaitseklauslite poolt pakutavad kaitsemeetmed on EL-i õiguse kontekstis piisavad.¹⁵³ Selle magistritöö kontekstis on aga kõige relevantsemad Iirimaa Kõrge Kohtu küsimused selle kohta, kas USA-s pakutav andmekaitse tase on kooskõlas põhiõiguste harta artiklitest 47 ja 52 tulenevate nõuetega, mille kohaselt peab isikule olema tagatud õiguste rikkumise korral õigus tõhusale õiguskaitsevahendile kohtus ning sellise õiguse piiramine peab demokraatlikus ühiskonnas olema vajalik ja proportsionaalne.¹⁵⁴

2020. aasta 16. juulil tegigi Euroopa Kohus lahendi *Schrems II*, milles tunnistas kehtetuks rakendusotsuse 2016/1250 ning seeläbi ka andmekaitseraamistiku *Privacy Shield*. Euroopa Kohus arutas selles lahendis kahte probleemi, mis käesoleva magistritöö kontekstis on väga olulise tähtsusega. Esiteks väljendas Euroopa Kohus kahtlust selle osas, kas USA õigus tagab isikuandmete piisava kaitse taseme GDPR-i artikkel 45 alusel koosmõjus põhiõiguste harta artiklitega 7, 8 ja 47.¹⁵⁵ Euroopa Kohus leidis, et *Privacy Shieldi* alusel loodud ombudsman ei olnud USA täitevvõimust piisavalt sõltumatu, puudusid piisavad kaitsemeetmed, et teda tagandamise eest kaitsta ning samuti ei olnud ombudsmanil pädevust teha USA luureagentuuridele siduvaid otsuseid.¹⁵⁶ Seega sisuliselt nõustus Euroopa Kohus WP29 töögrupi poolt tehtud hinnanguga, mida siinkirjutaja käsitles magistritöö eelmisel leheküljel. Teiseks leidis Euroopa Kohus, et USA luureagentuuride poolt kasutatavad jälgimisprogrammid FISA paragrahv 702 ja korraldus EO 12333 koostoimes suunisega PPD-28 ei vasta vajalikkuse ja proportsionaalsuse põhimõtetele.¹⁵⁷ Põhiline probleemkoht, millele Euroopa Kohus tähelepanu juhtis, oli see, et suunis PPD-28 võimaldab andmete „laiaulatusliku kogumist“, mis tähendab „suhteliselt suure koguse signaaliluure teel

¹⁵² Eelotsuse taotluse esitamise hetkel reguleeris standardsete andmekaitseklauslite alusel isikuandmete edastamist andmekaitse direktiiv 95/46 artikkel 26 lõige 4, aga Euroopa Kohtu otsuse tegemise hetkel oli jõustunud GDPR, kus reguleerib seda küsimust artikkel 46.

¹⁵³ EKo *Schrems II*, p 68.

¹⁵⁴ *Ibidem*.

¹⁵⁵ *Ibidem*, p 168.

¹⁵⁶ *Ibidem*, p 193-197.

¹⁵⁷ *Ibidem*, p 184.

kogutava teabe või andmete omandamist tingimustel, kus luureühendusel ei ole võimalik otsingu täpsustamiseks kasutada midagi, mille abil identifitseerida konkreetseid objekte“.¹⁵⁸ Teisisõnu, tegu on andmete „masskogumisega“, mida magistritöö autor käsitleb põhjalikumalt peatükis 2.2.

Viimase kahe alapeatüki kokkuvõtteks võib siinkohal öelda, et peamine põhjus, miks Euroopa Kohus varasemad kaks andmekaitseraamistikku *Safe Harbor* ja *Privacy Shield* kehtetuks tunnistas, seisnes selles, et USA luureagentuuride EL-i kodanike suhtes teostatav jälgimistegevus ei vasta EL-i õigusest tulenevatele nõuetele. Vaatamata sellele, et Euroopa Kohus juhtis sellele juba tähelepanu aastal 2015 lahendis *Schrems*, kiitis Euroopa Komisjon heaks ka järgmise andmekaitseraamistiku, kuigi USA ei olnud jälgimistegevuse piirangute osas suuri sisulisi muudatusi teinud. Nagu autor peatükis 1.1.1. mainis, siis Euroopa Komisjon on kokku adekvaatsusotsuseid välja andnud üpriski vähe. Seega magistritöö autori jaoks on ebaselge, miks USA-le neid otsuseid kergekäelisemalt antakse. Siinkirjutaja hinnangul saab olema huvitav näha, kas Euroopa Komisjon kiidab heaks ka USA uue andmekaitseraamistiku, mille tulemusel ootaks ees juba potentsiaalselt kolmanda EL-i ja USA vahelise andmekaitseraamistiku kehtetuks tunnistamine Euroopa Kohtu poolt.

Magistritöö esimeses peatükis analüüsis autor, missugustel õiguslikel alustel saab andmeedastus USA ja EL-i vahel toimida. Samuti selgitas autor välja, missugustel õiguslikel alustel USA teostab eurooplaste suhtes signaalluuret, mis riivab nende õigust privaatsusele ja andmekaitsele. Samuti käsitles autor seda, missuguste õigusaktidega on USA üritanud selliseid riiveid leevendada ning seda, missuguse hinnangu on Euroopa Kohus USA senistele püüdlustele andnud lahendites *Schrems* ja *Schrems II*. Järgmisena liigub autor edasi selle juurde, et vastata küsimusele, kas USA uus andmekaitseraamistik tagab EL-i õiguse kontekstis piisava andmekaitse taseme, st kas uus raamistik aitab parendada varasemaid puudujääke signaalluurele piirangute seadmisel.

¹⁵⁸ *Ibidem*, p 183.

2. USA uue andmekaitseraamistiku vastavus Euroopa Andmekaitseenõukogu tagatistele

2.1. Euroopa olulised tagatised

Nagu sissejuhatuses mainitud – magistritöö uurimisküsimused on tuletatud Euroopa Andmekaitseenõukogu poolt formuleeritud Euroopa olulistest tagatistest, mille järgimine on tähtis selleks, et signaalluure teostamise käigus ei riivataks privaatsus- ja andmekaitsepõhiõiguseid rohkem kui on vajalik ja proportsionaalne EL-i õiguse tähenduses. USA uue andmekaitseraamistiku vastavust nendele tagatistele analüüsis 2022. aasta novembris ka õigusteadlane ja emeriitprofessor Douwe Korff¹⁵⁹, aga tema koostatud analüüsi hetkel ei olnud Euroopa Komisjon veel avaldanud adekvaatsusotsuse eelnõud USA uue andmekaitseraamistiku suhtes; samuti ei olnud Euroopa Andmekaitseenõukogu koostanud selleks hetkeks arvamust adekvaatsusotsuse eelnõu osas. Seetõttu leiab siinkirjutaja, et kõnealune uurimisprobleem on jätkuvalt aktuaalne ja väärib analüüsimist, eriti arvestades seda kui Korffist erinevale seisukohale on Euroopa Komisjon adekvaatsusotsuse eelnõus asunud.

Nagu Korff enda analüüsis ka viitas, põhinevad Euroopa Andmekaitseenõukogu olulised tagatised suures osas Euroopa Kohtu praktikal, sh lahenditel *Schrems I*, *Schrems II*, *La Quadrature du Net* ning *Privacy International*.¹⁶⁰ Samuti on mõned Euroopa Andmekaitseenõukogu seisukohad oluliste tagatiste osas tuletatud ka EIK-i praktikast. Magistritöö mahupiirangu tõttu ei ole autor eelnevates magistritöö eelmises peatükis kõiki neist lahenditest süvitsi käsitlenud. Kuivõrd aga käesolev uurimus keskendub USA ja EL-i vahelisele andmevahetusele, siis on siinkirjutaja siiski andnud peatükis 1.4 *Schrems* ja *Schrems II* lahenditest põhjalikuma ülevaate, sest need lahendid käsitlesidki otseselt Atlandi-ülest andmeedastust.

¹⁵⁹ Vt Korff, D. The inadequacy of the US Executive Order on Enhancing Safeguards For US Signals Intelligence Activities, 11.11.2022. Kättesaadav: <https://www.ianbrown.tech/2022/11/11/the-inadequacy-of-the-us-executive-order-on-enhancing-safeguards-for-us-signals-intelligence-activities/> (20.04.2023).

¹⁶⁰ *Ibidem*, lk 5.

Euroopa olulised tagatised, mida autor järgnevalt analüüsima hakkab, on jaotatud neljaks:

- A. isikuandmete töötlemine peaks põhinema selgetel, täpsetel ning ligipääsetavatel (avalikel) eeskirjadel;
- B. signaalluure teostamise eesmärgid peavad olema vajalikud ja proportsionaalsed;
- C. isikuandmete töötlemise õiguspärasust peab kontrollima sõltumatu järelevalvemehhanism;
- D. üksikisikutele – kes leiavad, et nende õigusi on rikutud – peavad olema kättesaadavad tõhusad õiguskaitsevahendid.¹⁶¹

2.2. Tagatis A – kas töötlemine põhineb selgetel, täpsetel ja ligipääsetavatel eeskirjadel?

2.2.1. EL-i õiguse nõuded

Euroopa Andmekaitsekoostöökoostöö poolt esimene välja toodud tagatis põhineb põhiõiguste harta artiklidel 8 ja 52; varasemal Euroopa Kohtu praktikal: otsustel *Schrems II* ja *Privacy International*; EIK-i kohtulahenditel *Liberty*, *Weber ja Saravia*, *Malone* ning *Zakharov*.¹⁶² Käesoleva analüüsi kontekstis üks olulisemaid Euroopa Andmekaitsekoostöökoostöö poolt tuletatud Euroopa Liidu õiguse nõuetest ongi see, et isikuandmete töötlemine põhineks täpsel, selgel, aga ka juurdepääsetaval õiguslikul alusel, mille Euroopa Andmekaitsekoostöökoostöö tuletas EIK-i lahendist *Malone*.¹⁶³ ¹⁶⁴ Euroopa Andmekaitsekoostöökoostöö viitab ka veel lahendile *Zakharov*, kus EIK leidis, et salajaste jälgimismeetmete kasutamisel – nt sidevahendite pealtkuulamisele – on oluline kehtestada pealtkuulamiseks selged ja üksikasjalikud eeskirjad. Kohus lisas veel ka, et kuivõrd pealtkuulamiseks kasutatav tehnoloogia muutub järk-järgult keerukamaks (mis teeb inimeste jälgimise lihtsamaks), on

¹⁶¹ Euroopa Andmekaitsekoostöökoostöö soovitus (2020), lk 8 ja 9.

¹⁶² *Ibidem*.

¹⁶³ EIKo *Malone*, p 65 ja 66.

¹⁶⁴ Euroopa Andmekaitsekoostöökoostöö soovitus (2020), lk 9.

sellises olukorras ametiasutuste poolt meelevaldsuse oht ilmne, mis suurendab selgete ja üksikasjalike eeskirjade sätestamise olulisust veelgi.¹⁶⁵ Kõnealuse magistritöö kontekstis on see EIK-i seisukoht väga asjakohane, sest ka USA luureagentuuride poolt teostatav signaalluure toimub infotehnoloogilisi vahendeid kasutades, mis on pidevalt muutumas ja arenemas. Seda, kas USA signaalluure vastab EIK-i kohtuasjades *Malone* ja *Zakharov* välja toodud standarditele¹⁶⁶, magistritöö autor järgnevalt analüüsibki.

2.2.2. USA andmekaitse tase

Esmapilgul võib tunduda, et korraldus EO 14086, millel sisuliselt USA uus andmekaitseraamistik põhineb, tagab signaalluure lubatavuse ainult selgetel ja üksikasjalikel juhtudel. Sellele järeldusele saaks jõuda tuginedes asjaolule, et korraldus EO 14086 sätestab 12 erinevat legitiimset eesmärki¹⁶⁷, mille korral tohib signaalluuret teostada. Siiski, nagu varem mainitud, on presidendil tegelikult õigus nende eesmärkide loetelu laiendada.¹⁶⁸ Selle probleemi on õigusteadlastest tõstatanud juba ka Elisabeth Goitein.¹⁶⁹ Goitein selgitab, et korraldus EO 14086 võimaldab sõnaselgelt „salaõiguse rakendamist“, sh selle kõige kahjulikumal variandil, milleks on salareeglite kogum, mis erineb avalikult kättesaadavast versioonist ja eksitab seega aktiivselt avalikkust.¹⁷⁰ Goiteini hinnangul on raske ette kujutada, et Euroopa Kohus aktsepteeriks reegleid, mis võivad – aga ei pruugi – ühtida tegelikult kehtivate piirangutega.¹⁷¹ Siinkirjutaja nõustub Goiteini seisukohaga. Seda põhjusel, et nagu eelnevas alapeatükis mainitud, on ka EIK „salaõiguse“ rakendamist tauninud lahendis *Zakharov*.¹⁷² Euroopa Kohus ise ei ole küll magistritöö autorile teadaolevalt varasemates lahendites salaõiguse õiguspärasust EL-i õiguse kontekstis analüüsinud, kuid Euroopa Kohus on enda seisukohtade kujundamisel viidanud varasemates

¹⁶⁵ EIKo *Zakharov*, p 229.

¹⁶⁶ EIKo *Malone*, p 65 ja 66; EIKo *Zakharov*, p 229.

¹⁶⁷ Vt *supra*, ptk 1.3.3.2.

¹⁶⁸ *Ibidem*.

¹⁶⁹ Goitein, E. The Biden Administration's SIGINT Executive Order, Part I: New Rules Leave Door Open to Bulk Surveillance, 31.10.2022. Kättesaadav: <https://www.justsecurity.org/83845/the-biden-administrations-sigint-executive-order-part-i-new-rules-leave-door-open-to-bulk-surveillance/> (19.04.2023).

¹⁷⁰ *Ibidem*.

¹⁷¹ *Ibidem*.

¹⁷² EIKo *Zakharov*, p 229.

lahendites ka EIK-i praktikale.¹⁷³ Seega siinkirjutaja hinnangul on tõenäoline, et kui Euroopa Kohus tulevikus analüüsiks salaõiguse problemaatikat, siis nõustuks ta EIK-i lahendis *Zakharov* välja toodud seisukohaga. Samuti on Euroopa Parlament juba 2014. aastal koostatud raportis – mille käigus uuriti NSA jälgimisprogrammide mõju ELi kodanikele – leidnud, et salajased õigusaktid rikuvad õigusriigi põhimõtet.¹⁷⁴ Õigusteadlastest on Goiteini kriitikaga seoses korralduse EO 14086 poolt võimaldatava salaõiguse rakendamisega nõustunud ka emeriitprofessor Korff.¹⁷⁵ Probleem salaõigusega ei ole küll siiski uus – Goitein juhtis juba 2016. aastal tähelepanu sellele, et USA justiitsministeeriumi õigusnõuniku büroo (ingl k *US Department of Justice's Office of Legal Counsel*) annab regulaarselt riikliku julgeoleku küsimustes välja õigustõlgendusi, mis on salastatud ning on USA täitevvõimule siduvad.¹⁷⁶ Isegi kui kohus jääb hiljem eriarvamusele, siis USA justiitsministeerium ei kavatse seda uurima hakata ega kedagi vastutusele võtma selle eest, et ta sellisele salastatud arvamusele tuginedes tegutses ja otsuseid langetas.¹⁷⁷ Selliseid salastatud õigusnõustaja arvamusi kasutati George W. Bushi administratsiooni ajal, et õigustada inimeste piinamist ja põhjendamatut jälgimist. Hiljem Bushi poolt justiitsministeeriumi õigusnõuniku büroo juhiks määratud Jack Goldsmith jälgis kõrvalt, kuidas büroo juristid toimetasid FISA-ga samamoodi nagu teiste seadustega, mis neile ei meeldinud – nad sisuliselt salaja ignoreerisid neid, tuginedes hapratele juriidilistele arvamustele, mida nad valvasid nii hoolikalt, et keegi ei saaks operatsioonide õiguslikku alust kahtluse alla seada.¹⁷⁸

¹⁷³ Vt nt EKo C-487/19, W.Ż, ECLI:EU:C:2021:798, p 129; EKo C-132/20, *BN and Others vs Getin Noble Bank S.A.* ECLI:EU:C:2022:235, p 121.

¹⁷⁴ Euroopa Parlamendi 12.03.2014 vastu võetud resolutsioon USA Riikliku Julgeolekuagentuuri jälgimisprogrammi ja ELi liikmesriikide jälgimisasutuste ning nende mõju kohta ELi kodanike põhiõigustele ja Atlandi-ülesele koostööle justiits- ja siseküsimustes (2013/2188(INI)). Kättesaadav: https://www.europarl.europa.eu/doceo/document/TA-7-2014-0230_ET.html (21.04.2023), p 13.

¹⁷⁵ Korff, D. The Inadequacy of the US Executive Order on Enhancing Safeguards For US Signals Intelligence Activities, lk 9.

¹⁷⁶ Goitein, E. The New Era of Secret Law. – Brennan Center for Justice at New York University School of Law, 18.10.2016, lk 37.

¹⁷⁷ *Ibidem*.

¹⁷⁸ *Ibidem*, lk 38.

2.2.3. Vahejärelus

Eeltoodust lähtuvalt leiab siikirjutaja, et korralduses EO 14086 sätestatud reeglid, mis võimaldavad signaalluure läbi viia, ei ole piisavalt selged ega täpsed. Asjaolu, et korraldus EO 14086 võimaldab presidendi diskretsioonil signaalluure eesmärkide loetelu laiendada viitab sellele, et signaalluure eesmärgid on sätestatud abstraktselt ning neid on võimalik liiga laialt tõlgendada.

Samuti võib president kehtestada uusi reegleid, mis tähendab, et eesmärgid ei ole ka ühiskonna liikmetele piisavalt avalikult kättesaadavad, mis suurendab luureagentuuride poolset meelevaldse jälgimistegevuse teostamise ohtu.

Kokkuvõtvalt leiab siikirjutaja, et USA uus andmekaitseraamistik ei vasta Euroopa Andmekaitsekoostöötagatisele A, mille kohaselt andmete töötlemine peaks põhinema selgetel, täpsetel ja ligipääsetavatel (avalikel) eeskirjadel. Sellega sai magistritöö raames püstitatud esimene uurimisküsimus eitava vastuse.

2.3. Tagatis B – kas signaalluurega taotletavad seaduslikud eesmärgid on vajalikud ja proportsionaalsed?

2.3.1. EL-i õiguse nõuded

Teise tagatisena on Euroopa Andmekaitsekoostöötagatise kohustuse, mille kohaselt on vaja tõendada, et taotletavad seaduslikud eesmärgid, mille tarbeks luuretegevust teostatakse, on vajalikud ja proportsionaalsed.¹⁷⁹ Selle tagatise konstrueerimisel on Euroopa Andmekaitsekoostöötagatise lähtunud põhiõiguste harta artiklist 52 ning Euroopa Kohtu lahenditest *Schrems I*, *Schrems II*, *La Quadrature du Net* ja *Privacy International*.¹⁸⁰ Proportsionaalsuse põhimõtte tuleneb põhiõiguste harta artikkel 52 lõike 1 esimesest ja teisest lausest. Esimese lause kohaselt tohib põhiõiguste hartaga tunnustatud õiguste ja vabaduste teostamist piirata ainult nimetatud õiguste ja vabaduste olemust arvestades. Teise

¹⁷⁹ Euroopa Andmekaitsekoostöötagatise soovitused (2020), lk 9 ja 10.

¹⁸⁰ *Ibidem*.

lause kohaselt tohib proportsionaalsuse põhimõtte alusel õigustele ja vabadustele piiranguid seada ainult juhul, kui need on vajalikud ning vastavad tegelikult liidu tunnustatud üldist huvi pakkuvatele eesmärkidele või kui on vajalik teiste isikute õiguste ja vabaduste kaitsmine.¹⁸¹

Proportsionaalsuse põhimõtte sisustamisel on Euroopa Kohus selgitanud, et vastata küsimusele, kas eraelu puutumatuse ja andmete kaitse õiguse piiramine on õigustatud, tuleb ühelt poolt hinnata sellise piiranguga kaasneva riive raskust ning teiselt poolt tuleb kontrollida, kas piiranguga taotletava üldisele huvile vastava eesmärgi olulisus on selle raskusastmega vastavuses.¹⁸²

Vajalikkuse põhimõtet¹⁸³ sisustades on Euroopa Andmekaitsekohtu tuginenud otsustele *Schrems I*, *Schrems II* ja *Privacy International* ning leidnud, et õigusakt, mis annab üldise loa säilitada kõigi isikute isikuandmeid, ilma et säilitamisele oleks ette nähtud piirangud ning ilma, et oleks ette nähtud objektiivne kriteerium, mis võimaldaks ametiasutuste juurdepääsu ning nende hilisemat andmete kasutamist piirata, ei vasta vajalikkuse põhimõttele.¹⁸⁴

Luuretegevuse vajalikkuse ja proportsionaalsuse kontekstis on asjakohane ka Euroopa Kohtu viimane seisukoht isikuandmete masskogumisega seoses. Nimelt leidis Euroopa Kohus lahendis *La Quadrature du Net*, et elektroonilise side vahendite kõikide kasutajate liiklus-ja asukohaandmete säilitamine (teisisõnu „masskogumine“) on lubatud ainult siis, kui riik seisab silmitsi tõelise ja vahetu või ettearvatava suure riikliku julgeolekuohuga.¹⁸⁵

¹⁸¹ EKo *Schrems II*, p 174

¹⁸² EKo *La Quadrature du Net*, p 131.

¹⁸³ Autori märkus: Euroopa Andmekaitsekohtu soovitude (2020) eestikeelses versioonis on küll kasutatud terminit „vajaduse põhimõte“, aga siinkirjutaja hinnangul oleks õigem seda nimetada „vajalikkuse põhimõtteks“, sest selliselt on põhimõtet nimetatud ka Euroopa Kohtu lahendite eestikeelsetes versioonides, vt nt EKo *Schrems II*, p 76.

¹⁸⁴ Euroopa Andmekaitsekohtu soovitud (2020), p 37.

¹⁸⁵ EKo *La Quadrature du Net*, p 137.

2.3.2. USA andmekaitse tase

Nagu eelmises alapeatükis mainitud, Euroopa Kohus on varasemalt leidnud, et luuretegevuse käigus tekitatud riived isikute põhiõigustele peavad olema vajalikud ja proportsionaalsed. Nende nõuete mittetäitmine oligi üks peamisi põhjuseid, miks Euroopa Kohus tunnistas kehtetuks *Privacy Shield* õigusraamistikku.¹⁸⁶ Korraldusega EO 14086 on terminid „vajalikkus“ ja „proportsionaalsus“ USA õigussüsteemi üle võetud. Esmapilgul võiks seega arvata, et probleem on ära lahendatud. Tegelikult aga tõusetub küsimus sellest, kas need terminid on ainult näiliselt üle võetud või on edaspidi USA luureagentuuride tegevus ka sisulises mõttes vajalik ja proportsionaalne selliselt, nagu nõuab seda EL-i õigus ja Euroopa Kohtu praktika. Selles küsimuses lähevad nii õigusteadlaste kui ka erinevate EL-i andmekaitseasutuste arvamused lahku. Max Schrems – kelle kaebuste tulemusena tunnistas Euroopa Kohus kehtetuks eelmised USA andmekaitseraamistikud – on asunud seisukohale, et USA on sisuliselt „kopeerinud“ need kaks terminit korraldusse EO 14086, aga massiline eurooplaste jälgimine siiski praktikas tegelikult jätkub.¹⁸⁷ Max Schremsi arvamust jagavad ka õigusteadlased Goitein ja Korff. Goiteini hinnangul on ebatõenäoline, et USA valitsus hakkab vajalikkuse ja proportsionaalsuse põhimõtteid rakendama sarnaselt Euroopa Kohtuga. Seda põhjusel, et justiitsministri määruses, millega asutatakse DPRC, on sätestatud, et korraldust EO 14086 ja seal sisalduvaid termineid tõlgendatakse eranditult USA õiguse ja sealse õigustraditsiooni – mitte ühegi muu õigusallika – valguses. Goitein märgib, et on üks asi nentida tõsiasja, et USA ei ole kõnealuses kontekstis seotud USA-väliste kohtutega, aga on hoopis teine asi väita, et USA tugineb rahvusvahelisest õigusest laenatud terminite tõlgendamisel ainult USA õigusele, arvestamata seejuures üleüldse rahvusvaheliste kohtute (nagu nt Euroopa Kohtu) otsuseid.¹⁸⁸ Siiski eksisteerib ka seisukohti, mille kohaselt hakkab USA valitsus tõlgendama vajalikkust ja proportsionaalsust lähtuvalt Euroopa Kohtu praktikast, mida autor käsitleb allpool.

¹⁸⁶ Vt EKo *Schrems II*.

¹⁸⁷ Schrems, M. First reaction: Executive Order on US Surveillance unlikely to satisfy EU law. NOYB – European Center for Digital Rights, 07.10.2022. Kättesaadav: <https://noyb.eu/en/new-us-executive-order-unlikely-satisfy-eu-law> (19.04.2023).

¹⁸⁸ Goitein, E (2022).

Kõigepealt käsitleb siinkirjutaja masskogumise kui ühe jälgimismeetodi vastavust vajalikkusele ja proportsionaalsusele põhimõtetele. Seejärel uurib autor konkreetselt seda, kas USA valitsuse poolt nende põhimõtete sätestamine korralduses EO 14086 annaks ka alust arvata, et USA hakkab edaspidi signaalluure teostamisel neid põhimõtteid ka sisuliselt tõlgendama lähtuvalt Euroopa Kohtu praktikast. Siinkirjutaja suunab tähelepanu sellele, et uuema Euroopa Kohtu praktika valguses võib andmete masskogumist rakendada ainult sisuliselt vahetu riigi julgeolekut ähvardava suure ohu korral.¹⁸⁹

Goiteini hinnangul eksisteerivad USA valitsuse poolt korraldusega EO 14086 signaalluure piiramise püüdlustel fundamentaalsed puudujäägid. Probleem praeguse lähenemisega seisneb selles, et on ette nähtud eesmärgid, mille saavutamise jaoks on jälgimistegevus lubatud, selle asemel, et seada piiranguid sellele, keda üldse jälgida tohib. Näiteks üks eesmärkidest võimaldab jälgimistegevust kohaldada, et kaitsta küberjulgeolekut ähvardavate välisohtude eest.¹⁹⁰ Goitein möönab, et selline eesmärk on ilmselgelt küll legitiimne, kuid küberjulgeoleku kaitse antud juhul võiks õigustada kõikide internetis toimuvate tegevuste pidevat jälgimist. Tõepoolest – EO 14086 näeb sõnaselgelt ette masskogumise – kinnitades, et vähemalt mõnel juhul ei piira konkreetsete eesmärkide sätestamine andmete kogumist üldse.¹⁹¹ Jätkates masskogumise vajalikkuse probleemiga, kirjeldab Goitein põhjendatult, kuidas korraldus EO 14086 võimaldab koguda isikuandmeid, mille kogumiseks ei ole üldse legitiimset vajadust. Andmete masskogumiseks peab luureagentuur küll teoreetiliselt kindlaks tegema, et see on vajalik, kuid see „vajalikkuse test“ kehtib igat vormi jälgimise korral: nii massjälgimise kui ka muude jälgimismeetodite puhul. Sellise nõude seadmine andmete masskogumisele aga ei piira masskogumise rakendamist täiendavalt võrreldes muude, privaatsust vähem riivavate andmekogumismeetoditega. Kõik, mida sellise „vajalikkuse testi“ seadmine teeb, on kinnitada USA poolset seisukohta, et andmete masskogumine võib vahel ka vajalik olla. Goitein möönab küll, et korraldus EO 14086 sätestab luureagentuuridele kohustuse rakendada mõistlikke meetodeid ja tehnilisi meetmeid, et piirata mitterelevantsete andmete kogumist, aga täiendavaid suuniseid – kuidas seda saavutada – ette ei anna. Olukorras, kus

¹⁸⁹ EKo *La Quadrature du Net*, p 137.

¹⁹⁰ Vt ptk 1.3.3.2.

¹⁹¹ Goitein, E (2022).

pole teada, missugused need meetmed on ja kui hästi nad töötavad, pole ka võimalik hinnata, missugune mõju nendel nõuetel ka masskogumisega kaasnevatele privaatsuse riivetele reaalselt on.¹⁹² Samuti on Euroopa Andmekaitsekoostöönõukogu avaldanud muret USA kaitsemeetmete osas, mis peaksid masskogumisega kaasnevaid riiveid privaatsusele maandama.¹⁹³

Euroopa Komisjon on adekvaatsusotsuse eelnõus masskogumist ka käsitlenud. Komisjon on leidnud, et andmete masskogumine on ainult võimalik korraldus EO 12333 alusel, mitte FISA paragrahvi 702 alusel. Lisaks on komisjon enda analüüsis leidnud, et kui on vajalik masskogumist rakendada, siis kohalduvad korralduses EO 14086 sätestatud kaitsemeetmed.¹⁹⁴ Komisjon on aga lihtsalt viidanud korralduses EO 14808 sätestatule, mille paragrahvi 2 (c)(ii)(A) kohaselt, kui tehakse kindlaks, et luurealase prioriteedi edendamiseks on vajalik andmete masskogumine, siis kohaldatakse mõistlikke meetodeid ja tehnilisi meetmeid, et piirata kogutud andmeid ainult sellega, mis on vajalik konkreetse luureprioriteedi edendamiseks.¹⁹⁵ Ülalpool viitas siinkirjutaja aga juba Goiteini poolt tehtud analüüsile, kus ta illustreeris tabavalt, et seni kuni pole selge, mis need „mõistlikud meetodid ja tehnilised meetmed“ endast reaalselt kujutavad, pole ka võimalik hinnata, kui efektiivselt need töötavad.¹⁹⁶ Täiendavalt on Goitein tegelikult tähelepanu juhtinud veel ka sellele, et president Obama poolt 2014. aastal vastu võetud suunis PPD-28 pakkus tegelikult masskogutud andmete kasutamise vastu mõnevõrra tugevamat kaitset kui uue andmekaitseraamistiku põhjal pakub president Bideni korraldus EO 14086, mis asendab nüüd suunist PPD-28.¹⁹⁷ Kui PPD-28 nägi ette, et masskogutud andmete põhjal tehtavad päringud on lubatud ainult siis, kui päringu tulemusel on suur tõenäosus saada asjakohast informatsiooni, siis korraldus EO 14086 on seda standardit lõdvendanud: nüüd on sellised andmepäringud teoorias lubatud ka siis, kui eksisteerib vähimgi võimalus, et päringu

¹⁹² Goitein, E (2022).

¹⁹³ Euroopa Andmekaitsekoostöönõukogu. Opinion 5/2023 on the European Commission Draft Implementing Decision on the adequate protection of personal data under the EU-US Data Privacy Framework. Kättesaadav: https://edpb.europa.eu/our-work-tools/our-documents/opinion-art-70/opinion-52023-european-commission-draft-implementing_en (20.04.2023), p 163.

¹⁹⁴ Adekvaatsusotsuse eelnõu, p 134.

¹⁹⁵ *Ibidem*.

¹⁹⁶ *Supra*, lk 46.

¹⁹⁷ Goitein, E (2022).

tulemusel võib kätte saada relevantset informatsiooni.¹⁹⁸ Samuti soovib siinkirjutaja kommenteerida ka Euroopa Komisjoni poolt märgitud, mille kohaselt andmete masskogumine on võimalik ainult korraldus EO 12333 alusel ning et FISA paragrahv 702 seda ei võimalda. Magistritöö autor on ülalpool¹⁹⁹ tähelepanu juhtinud sellele, et tehnoloogiliste piirangute tõttu kogutakse ka FISA paragrahv 702 alusel isikute kohta informatsiooni, kes tegelikult ei ole luuresihtmärgiks. Kuigi see ei lähe otseselt Euroopa Kohtu poolt *La Quadrature du Net* lahendis välja toodud definitsiooni²⁰⁰ alla, siis kogutakse siiski informatsiooni ka isikute kohta, kes ei ole signaalluure eesmärkide saavutamiseks kuidagi seotud. Teisisõnu kogutakse ka FISA paragrahv 702 alusel informatsiooni isikute kohta, mida ei saa pidada rangelt vajalikuks.

Masskogutud andmete teemal on Euroopa Komisjon veel juhtinud tähelepanu sellele, et suunatud kogumist (spetsiifiliste märksõnade alusel otsimine) tuleb prioriteetida masskogumise üle. Samuti on komisjon analüüsis rõhunud sellele, et masskogutud andmeid võib kasutada kuuel erineval eesmärgil. Need eesmärgid aga on sisuliselt täpselt samad²⁰¹ nagu olid sätestatud suunises PPD-28, mille kohta Euroopa Kohus on juba varem järeldanud, et seal sätestatud piirangud andmete masskogumisele ei vasta proportsionaalsuse mõttele ega taga seda, et USA teostatav signaalluure piirduks rangelt vajalikuga.²⁰² Seega jääb siinkirjutajale arusaamatuks, miks Euroopa Komisjon on enda hinnangu andmisel rõhutanud asjaolu, et masskogutud andmeid võib nüüd kasutada kuuel erineval eesmärgil, jättes sellega mulje, et USA on masskogutud andmete kasutamist rohkem piiranud võrreldes eelmise andmekaitseraamistikuga, mille Euroopa Kohus kehtetuks tunnistas. See omakorda jätab mulje, et nüüd on USA poolt tagatav andmekaitse tase kõrgem kui varasemalt. Tegelikult aga ei ole masskogutud andmete kasutamisega selles küsimuses sisulisi muudatusi tehtud.

Järgnevalt käsitleb siinkirjutaja argumenti, mille kohaselt on siiski võimalik, et USA hakkab vajalikkuse ja proportsionaalsuse põhimõtteid sisustama samaväärselt nagu on siiani seda

¹⁹⁸ *Ibidem*.

¹⁹⁹ Vt ptk 1.3.2.1.

²⁰⁰ Selle lahendi kohaselt on masskogumiseks käsitletav elektroonilise side vahendite kõikide kasutajate liiklus- ja asukohaandmete säilitamine (EKo *La Quadrature du Net*, p 137).

²⁰¹ Vt suunis PPD-28 paragrahv 2; korraldus EO 14086 paragrahv 2(c)(ii)(B)

²⁰² EKo *Schrems II*, p 183 ja 184.

teinud Euroopa Kohus. Professor Peter Margulies on sellise seisukoha põhjendamiseks viidanud USA pretsedendile²⁰³, mille kohaselt võib kohus USA õigust kohaldades teatud seadusandlikke ja täitevmeetmeid tõlgendada kitsalt.²⁰⁴ Samuti viitab ta USA ülemkohtu rohkem kui 100 aasta vanusele kohtulahendile²⁰⁵, kus kohus leidis, et rahvusvaheline õigus moodustab osa USA õigusest. EL-i andmekaitseasutustest on Saksamaal asuv Hamburgi andmekaitseasutus samuti märkinud, et eeldus – mille kohaselt USA ei tõlgenda proportsionaalsust nii nagu nõuab Euroopa Kohus – on spekulatiivne.²⁰⁶

Magistritöö autori hinnangul on vähetõenäoline, et USA hakkab signaalluure teostamisel vajalikkuse ja proportsionaalsuse põhimõtteid rakendama sisuliselt samaväärselt nagu EL-i õigus seda nõuab. Siinkirjutaja juhib tähelepanu USA varasemale signaalluure rakenduspraktikale, mille tõttu on juba kaks erinevat raamistikku Euroopa Kohtu poolt kehtetuks tunnistatud. Läbiv põhjus oli mõlemal juhul isikute massjälgimine. Eelneva analüüsi tulemusel jõudis siinkirjutaja järeldusele, et massjälgimine jätkub ka vaatamata uue andmekaitseraamistikuga kehtestatud täiendavatele luuretegevuse piirangutele. Nagu ka eelnevalt mainitud, siis Euroopa Kohtu praktikast lähtuvalt on massjälgimine õigustatud ainult sisuliselt vahetu riigi julgeolekut ähvardava suure ohu korral.²⁰⁷ Nagu Goitein selgitas, korraldus EO 14086 seevastu rakendab masskogumise vajalikkuse hindamisel samasugust standardit nagu rakendatakse ka muude jälgimisvormide korral.²⁰⁸ Näiteks on masskogumine võimalik küberjulgeoleku kaitsmiseks, mis on olemuselt väga abstraktne ja võimaldaks sisuliselt terve interneti jälgimist.²⁰⁹ Goitein on samuti viidanud USA riiklikule luureprioriteetide raamistikule²¹⁰, kus käsitletakse immigratsiooni ja organiseeritud

²⁰³ Vt *City of Cleburne vs Cleburne Independent Living Center*, 473 U.S. 432 (1985). Kättesaadav: <https://www.law.cornell.edu/supremecourt/text/473/432> (20.04.2023).

²⁰⁴ Margulies, P. *Adjudicating Algorithms: Accountability in Regulation of Surveillance, Privacy, and Discrimination*. Roger Williams University School of Law Legal Studies Paper, 01.03.2023, No. 216. Kättesaadav: <https://ssrn.com/abstract=4375080> (20.04.2023), lk 30, joonealune viide 174.

²⁰⁵ Vt *Paquete Habana vs United States*, 175 U.S. 677, 700 (1900). Kättesaadav: <https://supreme.justia.com/cases/federal/us/175/677/> (20.04.2023).

²⁰⁶ The Hamburg Commissioner for Data Protection and Freedom of Information. *Data protection in the USA – current situation*, 29.11.2022. Kättesaadav: https://datenschutz-hamburg.de/assets/pdf/2022-11-29_Information_Executive_Order.pdf (20.04.2023), p 2.

²⁰⁷ EKo *La Quadrature du Net*, p 137.

²⁰⁸ Goitein, E (2020).

²⁰⁹ *Ibidem*.

²¹⁰ Office of the Director of National Intelligence. *Annual Threat Assessment of the US Intelligence Community*, 09.04.2023. Kättesaadav: <https://www.dni.gov/files/ODNI/documents/assessments/ATA-2021-Unclassified-Report.pdf> (25.04.2023).

kuritegevust kui suuri julgeolekuohtusid.²¹¹ See viitab USA üldisele praktikale tõlgendada julgeolekuohtusid väga laialt.²¹² Siinkirjutaja tuletab meelde, et president võib korraldus EO 14086 paragrahv 2(B) alusel jälgimise eesmärkide loetelu veel ka laiendada ning seda lausa salaja teha, kui see jällegi ohustab riikliku julgeolekut (mida samuti tõlgendatakse väga abstraktselt). See omakorda annab võimaluse sisuliselt ükskõik missugusel eesmärgil masskogumist rakendada seni kuni see „ohustab riikliku julgeolekut“, jättes sellele äärmiselt laia tõlgendusruumi. Selline lähenemine on siinkirjutaja hinnangul kategooriliselt vastuolus Euroopa Kohtu seisukohaga, mille kohaselt õigustab masskogumist ainult suur julgeolekuoht, mis osutub tõeliseks ja vahetuks või ettearvatavaks.²¹³ Sellise ohu alla võiksid autori hinnangul kuuluda nt 2001. aasta 11. septembril USA-s toimunud terrorirünnakud. Seega olukorras, kus EL-i õigusest lähtuvalt saab masskogumine olla vajalik nii suure ohu, nagu nt terrorirünnaku korral, aga USA õigus võimaldab masskogumist rakendada nt immigratsioonikuritegude korral, tuleb järeldada, et selline lähenemine ei ole kooskõlas vajalikkuse ega proportsionaalsuse põhimõtetega ega Euroopa Kohtu praktikaga.

Isegi olukorras, kus eksisteerib rohkem kui 100 aastat vana USA kohtulahend (nagu juhtis tähelepanu professor Margulies), mis teoreetiliselt ei välista DPRC poolt vajalikkuse ja proportsionaalsuse põhimõtete rakendamist, siis USA viimase 10 aasta praktika (Snowdeni 2013. a paljastused, lahendid *Schrems I* ja *Schrems II*) näitab siinkirjutaja hinnangul, et sellele rohkem kui 100 aastat vanale kohtulahendile tuginemise tõenäosus kohtunike poolt on väike. Samuti on selles olukorras tegu juba sisuliselt *ex post* kontrolliga, st hakatakse tagantjärele hindama, kas jälgimine oli vajalik ja proportsionaalne, aga siinkirjutaja hinnangul on andmekaitse- ja privaatsusõiguste riivete vähendamiseks ning rikkumiste ennetamiseks olulisem *ex ante* kontroll, st et jälgimismeetme kasutamise vajalikkust ja proportsionaalsust hinnataks enne seda, kui isikute õigusi on juba rikutud ja seega potentsiaalselt kahju tekitatud. Eeltoodust lähtuvalt ei saa magistritöö autor professor Marguliesi argumendiga nõustuda.

²¹¹ Goitein, E (2022).

²¹² *Ibidem*.

²¹³ EKo *La Quadrature du Net*, p 137.

2.3.3. Vahejärelalus

Kokkuvõtvalt leiab siinkirjutaja, et USA luureagentuuride teostatav signaalluure ei saa uue andmekaitseraamistiku alusel olema vajalik ja proportsionaalne EL-i õiguse tähenduses. Euroopa Komisjoni põhjendused ei ole sisulised: komisjon on ainult kirjeldanud seda, mis korralduses EO 14086 formaalselt kirjas on. Euroopa Komisjon on sisuliselt hindamata jätnud, kas ka reaalsed meetmed, mida korraldus EO 14086 alusel kasutusele võetakse, tagaksid, et jälgimistegevusega – eelkõige andmete masskogumisega – piiratakse isikute põhiõiguseid proportsionaalselt ning üksnes nii palju, kui on vältimatult vajalik. Komisjon viitas oma argumentatsioonis ka asjaolule, et korraldus EO 14086 järgi võib masskogutud isikuandmeid kasutada üksnes kuue erineva eesmärgi saavutamiseks. Siinkirjutaja juhtis aga tähelepanu sellele, et viidatud kuus eesmärki eksisteerisid samasugusel kujul juba EO 14086 eelkäija (suunise PPD-28) tekstis. Suunis PPD-28 osas leidis Euroopa Kohus juba *Schrems II* lahendis, et selle pakutavad tagatised ei ole EL-i õiguse standarditele vastavad. Samuti arvestades, et justiitsministri määruses eksisteerib lause, mille kohaselt tuleb USA andmekaitseraamistikku ja seal sätestatud termineid tõlgendada lähtuvalt USA õigustraditsioonist ja kohtupraktikast, siis on siinkirjutaja hinnangul tõenäoline, et USA kavatsus ei ole lähtuda Euroopa Kohtu tõlgendustest. Kui see oleks vastupidi, siis oleks see ka kuskil sätestatud või oleks USA valitsusasutused Euroopa Komisjonile selle kohta kinnituse saatnud, nagu on saadetud²¹⁴ muudes küsimustes. Professor Marguliesi poolt välja pakutud vastuargument – mille kohaselt DPRC kohtunikud võivad vajalikkuse ja proportsionaalsuse põhimõtteid tõlgendada Euroopa Kohtu praktikast lähtuvalt, sest eksisteerib üks rohkem kui 100 aasta vanune kohtulahend, mis sellist tõlgendamist teoreetiliselt lubab – ei ole samuti piisavalt faktipõhine. Olukorras, kus USA õigus võimaldab masskogumist rakendada küberjulgeolekuohtude (mida tõlgendatakse abstraktselt) ja immigratsioonikuritegude ennetamise või uurimise korral, kuid EL-i õiguses on selline jälgimine õigustatud ainult vahetu suure riikliku julgeolekuohu (nagu nt terrorism) korral, ei ole võimalik järeldada, et USA uus andmekaitseraamistik piiraks jälgimistegevust määral, mis oleks vajalik ja proportsionaalse põhiõiguste harta artikkel 52 tähenduses

²¹⁴ Vt nt adekvaatsusotsuse eelnõu lisa II jj.

tõlgendatuna lähtuvalt Euroopa Kohtu praktikast. Sellega tuleb ka magistritöö teisele uurimisküsimusele vastata eitavalt.

2.4. Tagatis C – kas USA andmekaitseraamistik tagab sõltumatu järelevalvemehhanismi?

2.4.1. EL-i õiguse nõuded

Kolmanda tagatisena on Euroopa Andmekaitsekohtu välja toonud sõltumatu järelevalve mehhanismi olemasolu, mille nõue tuleneb põhiõiguste harta artikli 47 esimesest lõikest, mille kohaselt peab kohus olema sõltumatu ja erapooletu. Selle tagatise formuleerimisel Euroopa Andmekaitsekohtu peamiselt lähtunud Euroopa Kohtu lahenditest *Schrems*, *Schrems II*, *La Quadrature du Net* ja *Privacy International*. Samuti on Euroopa Andmekaitsekohtu tuginenud mitmele EIK-i lahendile, millest peamised on *Klass*, *Big Brother Watch* ning *Zakharov*.²¹⁵

EIK-i praktikast tuleneb et kui on tegu eraelu puutumatuse või andmekaitse õiguse mis tahes riivamisega, siis sellise riivamise korral tuleb kohaldada tõhusat, sõltumatut ja erapooletut järelevalvesüsteemi, mille näeb ette kas kohtunik või mõni muu sõltumatu organ.²¹⁶ Sõltumatuse kriteeriumi nõudeid analüüsis Euroopa Kohus *Schrems II* lahendis, kus kohus leidis, et üks olulisi aspekte sõltumatuse hindamise puhul on asjaolu, kas järelevalveorgan (antud kaasuses oli tegu *Privacy Shieldi* alusel loodud ombudsmaniga) on sõltumatu täitevvõimust. Viidatud lahendis leidis Euroopa Kohus, et ombudsman ei olnud piisavalt iseseisev, sest ombudsmani määras ametisse riigisekretär ja ta kuulub USA välisministeeriumi koosseisu. Samuti ei eksisteerinud erilisi kaitsemeetmeid ombudsmani tagandamise vastu ega tema ametisse nimetamise otsuse tühistamise vastu.²¹⁷

²¹⁵ Euroopa Andmekaitsekohtu soovitusel (2020), lk 11-12.

²¹⁶ EIKo 5029/71, *Klass and Others vs Germany*, p 17 ja 51.

²¹⁷ EKo *Schrems II*, p 195.

2.4.2. USA andmekaitse tase

Võrreldes esimese kahe Euroopa Andmekaitse nõukogu poolt sõnastatud tagatisega on järgneva tagatise – ning selle kohta, kas USA uus andmekaitseraamistik sellele tagatisele ka vastab – rohkem õigusteadlaste poolt avaldatud vastakaid arvamusi. Seetõttu käsitleb magistritöö autor siinkohal põhjalikumalt mõlema poole argumente.

Õigusteadlased Théodore Christakis, Kenneth Propp ja Peter Swire on arvamusel, et koostoimes korralduse EO 14086 ja USA justiitsministri määrusega loodud kohtuorgan on EL-i standardite kohaselt sõltumatu.²¹⁸ Nende hinnangul on tagatud DPRC kohtunike sõltumatus, mh läbi selle, et neid on raske ametist eemaldada.²¹⁹ Nad selgitavad, et USA õigussüsteemi kohaselt on justiitsministri poolt välja antud määrusel õiguslikult siduv mõju, mistõttu on see sobiv vahend, et määratleda protseduurid õiguskaitsevahendite kasutamise taotluste ja kaebuste läbivaatamiseks.²²⁰ Selleks, et kaitsta meelevaldsete või ootamatute muudatuste tegemise eest, tuleb määruse muutmiseks või kehtetuks tunnistamiseks järgida samasuguseid avalikke menetluslike samme, mis olid vajalikud, et seda määrust esmakordselt jõustada.²²¹ Christakis jt viitavad eeltoodud seisukoha põhjendamiseks ka USA ülemkohtu otsusele asjas *Motor Vehicles Manufacturers Association vs State Farm Mutual Automobile Insurance Co*²²², kus ülemkohus jõudis samasugusele järeldusele. Christakis jt leiavad, et käesolev lahendus tagab nii EL-ile kui ka DPRC kohtunikele kaitse justiitsministri määruse ootamatu tühistamise eest ning seeläbi tagab ka DPRC sõltumatuse seni kuni määrust avalikult ja lõplikult muudetakse. Siiski pakuvad Christakis jt omalt poolt veel välja, et Euroopa Komisjoni poolt antav adekvaatsusotsus võiks olla seotud justiitsministri määruse kehtivusega, ehk teisisõnu, kui justiitsministri määrus peaks kaotama kehtivuse, siis kaotaks kehtivuse ka adekvaatsusotsus. See motiveeriks USA

²¹⁸ Christakis, T jt. The redress mechanism in the Privacy Shield successor: On the independence and effective powers of the DPRC. – The International Association of Privacy Professionals, 11.10.2022. Kättesaadav: <https://iapp.org/news/a/the-redress-mechanism-in-the-privacy-shield-successor-on-the-independence-and-effective-powers-of-the-dprc/> (20.04.2023).

²¹⁹ *Ibidem*.

²²⁰ *Ibidem*.

²²¹ *Ibidem*.

²²² *Motor Vehicle Manufacturers Association of the United States, Inc. vs State Farm Mutual Automobile Insurance Company*, 463 U.S. 29 (1983). Kättesaadav: <https://supreme.justia.com/cases/federal/us/463/29/#tab-opinion-1955213> (21.04.2023).

valitsust määrust jõusse jätma ning seda mitte muutma ilma eelneva heakskiiduta Euroopa Komisjoni poolt.²²³

Magistritöö kirjutamise seisuga on Euroopa Komisjon adekvaatsusotsuse eelnõu juba avaldanud, kuid Euroopa Komisjon ei ole Christakise jt ettepanekuga kaasa läinud, st justiitsministri määruse kehtivus ei ole seotud adekvaatsusotsuse kehtivusega. Euroopa Komisjon on küll adekvaatsusotsuse eelnõu punktis 212 välja toonud, et nõuetekohaselt põhjendatud tungiva kiireloomulisuse korral, näiteks kui korraldust EO 14086 või justiitsministri määrust muudetakse viisil, mis kahjustab kõnealuses otsuses kirjeldatud kaitsetaset, kasutab Euroopa Komisjon võimalust otsus peatada, kehtetuks tunnistada või seda muuta. Arvestades USA presidentide mõningat varasemat praktikat tunnistada kehtetuks eelnevate valitsusjuhtide korraldusi – nt USA eelmine president Donald Trump tunnistas kehtetuks²²⁴ mitu president Barack Obama poolt välja antud korraldust – võiks see anda alust kahelda selles, kas DPRC senises formaadis tulevikus ka kehtima jääb. Presidendaalsete aktide ebastabiilsuse probleemile juhtis juba tähelepanu ka Kivimaa enda 2017. aastal kirjutatud magistritöös.²²⁵ Võimatu on küll ette ennustada, kas Euroopa Komisjon kasutaks punktis 212 sätestatud võimalust, kuid arvestades ka asjaoluga, et varasemad adekvaatsusotsused, mis anti USA andmekaitseraamistikele *Safe Harbor* ja *Privacy Shield*, pidid oma kehtivuse kaotamiseks jõudma Euroopa Kohtu ette analüüsimiseks – Euroopa Komisjon ise nende kehtivusega probleemi ei tuvastanud – arvab siinkirjutaja, et Euroopa Komisjon ei kiirustaks praeguse adekvaatsusotsuse eelnõu punktis 212 kirjeldatud õigust kasutama, st adekvaatsusotsust kas nt peatama või kehtetuks tunnistama, isegi siis, kui tõusetuks küsimusi selle osas, kas USA poolt tagatav andmekaitse tase on peale adekvaatsusotsuse vastu võtmist langenud. Arvestades siiski asjaolu, et eeltoodu põhineb mineviku faktidel ning tuleviku ette näha on võimatu, siis eeltoodu põhjal ei saa teha tõsikindlaid järeldusi selle osas, kas ja kuidas see võiks mõjutada DPRC kohtunike sõltumatust.

²²³ Christakis, T jt (oktoober 2022).

²²⁴ Executive Order 13782. Revocation of Federal Contracting Executive Orders, 27.03.2017. Kättesaadav: <https://www.govinfo.gov/content/pkg/DCPD-201700200/pdf/DCPD-201700200.pdf> (20.04.2023).

²²⁵ Kivimaa, C., lk 51.

Õigusteadlastest on samuti uue kohtuorgani sõltumatuse küsimust analüüsinud Ashley Gorski. Erinevalt Christakisest jt arvab Gorski, et USA uus andmekaitseraamistik ei taga siiski DPRC kohtunike sõltumatust piisaval määral. Gorski märgib, et vaatamata USA praeguse valitsuse püüdlustele tagada DPRC iseseisvus, on see siiski olemuslikult administratiivne ning asub täitevvõimu all: DPRC kohtunikud valitakse ametisse USA justiitsministri poolt, mitte kolmanda osapoolte poolt, kes ei ole luuretegevusega seotud; presidendil on võimalik kohtunikke ilma mingisuguste piiranguteta ametist tagandada ning samuti võib president DPRC poolt tehtud kohtuotsuseid tühistada. Seega DPRC ei funktsioneerigi täielikult autonoomselt ning pole ka vaba hierarhiilistest piirangutest.²²⁶

Gorski poolt mainitu osas, mille kohaselt USA president tohib kohtunikke ametist tagandada ja DPRC kohtuotsuseid tühistada, siinkirjutaja seisukohta ei võta, sest selle väite analüüsimiseks ei ole magistritöö kirjutamise hetkel piisavalt informatsiooni. Korralduses EO 14086 sellist õigust sätestatud ei ole, erinevalt nt presidendi õigusest²²⁷ luuretegevuse teostamise eesmärkide loetelu laiendada. Samuti on Euroopa Andmekaitsekoostööde adegvaatsusotsuse kohta koostatud arvamuses maininud, et adekvaatsusotsus sellele küsimusele otsest vastust ei anna, kuid Euroopa Andmekaitsekoostööde arusaama kohaselt presidendil sellist pädevust siiski ei eksisteeri.²²⁸

Kohtunike sõltumatuse hindamisel on samuti oluline keskenduda sellele, kuidas mõjutab nende sõltumatust ametisse nimetamise kord, ametiaja pikkus ning samuti ametist eemaldamise kord. Gorski leidis, et kohtunike sõltumatus pole tagatud seetõttu, et neid on võimalik presidendi poolt ilma mingisuguste piiranguteta ametist tagandada. Lisaks märgib Gorski, et kuivõrd kohtunikud nimetatakse ametisse neljaks aastaks – ning neid on võimalik peale esimese ametiaja lõppu tagasi nimetada – siis võib see kaudselt neid mõjutada tegema otsuseid USA valitsuse kasuks, et kindlustada uus ametiaeg.²²⁹ Gorski viitab²³⁰ ka Euroopa

²²⁶ Gorski, A. The Biden Administration's SIGINT Executive Order, Part II: Redress for Unlawful Surveillance, 04.11.2022. Kättesaadav: <https://www.justsecurity.org/83927/the-biden-administrations-sigint-executive-order-part-ii/> (19.04.2023).

²²⁷ Vt *supra*, ptk 1.3.3.2.

²²⁸ Euroopa Andmekaitsekoostööde arvamus (2023), p 225.

²²⁹ Gorski, A.

²³⁰ *Ibidem*.

Kohtu lahendile asjas *Commission vs Poland* C-619/18, kus Euroopa Kohus selgitas, et kohtute sõltumatuse ja erapooletuse tagamiseks peab kohus täitma enda ülesandeid täiesti iseseisvalt ning olema kaitstud väljastpoolt tuleva sekkumise või surve eest, mis võib kahjustada kohtunike otsustusvabadust ja mõjutada nende otsuseid.²³¹ Samuti peab olema tagatud kohtunike objektiivsus ning see, et kohtunikud ise ei tunneks mingisugust huvi konkreetse vaidluse lahenduse vastu.²³² Sõltumatust ja erapooletust tagavad normid peavad võimaldama ümber lükata õigussubjektide mis tahes põhjendatud kahtlused selle osas, kas kõnealune kohus on väljaspool väliste tegurite haardeulatust ning kas ta on – võttes arvesse vastanduvaid huve – neutraalne.²³³

Siinkirjutaja ei nõustu Gorski poolt tehtud järeldusega, mille kohaselt DPRC kohtunike sõltumatus ei ole tagatud põhjusel, et nad võivad teha valitsuse poole kallutatud otsuseid eesmärgiga saada endale ametiaja pikendus täiendavaks neljaks aastaks. Ainuüksi asjaolust, et kohtunikku on võimalik peale esimest ametiaega tagasi valida, ei saa järeldada, et kohtunik võib teha kallutatud otsuseid, eesmärgiga kindlustada endale ametisse tagasi valimine. Magistritöö autor toob siinkohal võrdluseks Euroopa Kohtu kohtunike valimise korra: EL-i toimimise lepingu²³⁴ artikli 253 kohaselt nimetatakse Euroopa Kohtu kohtunikud ametisse kuueks aastaks. Sama artikli kohaselt on ametiaja lõppemisel võimalik kohtunik uueks ametiajaks tagasi nimetada. Oluline lähtekoht on siin ka see, et kolmanda riigi andmekaitse taseme adekvaatsuse hindamisel tuleb kontrollida, kas kolmas riik tagab sisuliselt samaväärse kaitsetaseme nagu on tagatud EL-is.²³⁵ Kuivõrd nii ELi kui ka DPRC kohtunikke on võimalik peale ametiaja lõppemist tagasi nimetada, siis siinkirjutaja hinnangul selles küsimuses on kohtunike sõltumatus tagatud nii USA-s kui ka EL-is sisuliselt samaväärselt. Magistritöö autorile ei tundu ka tõenäoline, et Euroopa Kohus võiks selle põhjal – et DPRC kohtunikud on määratud ametiajaga ja võimalusega neid peale ametiaja lõppu tagasi nimetada – jõuda järeldusele, et nad ei ole piisavalt sõltumatud.

²³¹ EKo C-619/18, *European Commission vs Republic of Poland*, ECLI:EU:C:2019:531, p 108.

²³² *Ibidem*.

²³³ *Ibidem*.

²³⁴ Euroopa Liidu toimimise lepingu konsolideeritud versioonid (2016/C 202/01). – ELT C 202, 07.06.2016, lk 1-388.

²³⁵ Vt nt Euroopa Andmekaitsekoostöösoovitused (2020), p 4.

Sellisel juhul oleks tegemist sisuliselt kaksikmoraaliga, st kritiseeritaks USA lähenemist olukorras, kus EL ise on kasutamas analoogset lahendust. Ka Euroopa Andmekaitsekohtu on enda adekvaatsusotsuse eelnõu kohta koostatud arvamuses jõudnud siinkirjutajaga sarnasele järeldusele ning leidnud, et DPCR kohtunike nelja-aastane ametiaeg – võimalusega neid ametisse tagasi valida – ei anna alust kahelda nende sõltumatuses.²³⁶

Üks erinevus küll DPCR ja Euroopa Kohtu kohtunike ametiaegade osas on nende kestvus. Nagu varasemalt mainitud, kohtunikud valitakse DPCR-sse neljaks aastaks ja Euroopa Kohtusse kuueks aastaks. Täiendavaks võrdluseks võib siinkohal veel tuua ka EIK-i kohtunikud, kes valitakse EIÕK artikkel 23 lõike 1 kohaselt lausa üheksaks aastaks. Vaatamata sellele, et EIK-i kohtunike ametiaeg on rohkem kui kaks korda pikem kui DPCR kohtunike ametiaeg, ei leia autor ka siinkohal põhjust, miks see võiks DPCR kohtunike sõltumatust võrreldes Euroopa Kohtu või EIK-i kohtunikega mõjutada. Nimelt seoses kohtuniku ametiaja pikkusega on EIK 2021. aastal tehtud lahendis *Centrum för Rättvisa vs Sweden* samuti otsustanud, et nelja-aastane kohtuniku ametiaeg on sõltumatu kontrollimehhanismi tagamiseks piisav.²³⁷

Järgnevalt käsitleb siinkirjutaja Gorski poolt välja toodud argumenti, mille kohaselt ei ole DPCR täielikult autonoomne ja vaba hierarhiilistest piirangutest, kuivõrd asub täitevvõimu haldusalas ja samuti valib ametisse kohtunikud USA justiitsminister ning mitte mõni teine isik, kes ei ole luurevõrgustikuga seotud. Gorski poolt tõstatatud argument on asjakohane, sest lahendis *Schrems II* kritiseeris Euroopa Kohus eelmise andmekaitseraamistiku *Privacy Shield* alusel loodud ombudsmani funktsiooni sõltumatust täitevvõimust.²³⁸ Lahendis *HID and BA vs Refugee Applications Commission* on Euroopa Kohus selgitanud, et asjaolu, mille kohaselt kohtuorgani liikmed valib ametisse minister, ei sea iseenesest selle kohtuorgani sõltumatust kahtluse alla.²³⁹ Selline kohtunike valimise praktika on tavapärane ka mitmes

²³⁶ Euroopa Andmekaitsekohtu aramus (2023), p 226.

²³⁷ EIKo 35252/08, *Centrum för Rättvisa vs Sweden*, p 346.

²³⁸ EKo *Schrems II*, p 195.

²³⁹ EKo C-175/11, *H. I. D. and B. A. vs Refugee Applications Commissioner and Others*, ECLI:EU:C:2013:45, p 99.

EL-i liikmesriigis.²⁴⁰ Ka Gorski enda poolt eelnevalt viidatud lahendis *Commission vs Poland* jõudis Euroopa Kohus järeldusele, et asjaolu, et kohtuniku ametiaja pikendamise üle otsustab president, ei tähenda tingimata, et oleks rikutud sõltumatuse põhimõtet.²⁴¹ Eeltoodust lähtuvalt leiab siinkirjutaja, et asjaolu, mille kohaselt DPRC kohtunikud valib ametisse USA justiitsminister, ei viita sõltumatuse põhimõtte rikkumisele EL-i õiguse tähenduses. Lisaks eelnevalt mainitule ei tohi korraldus EO 14086 paragrahv 3(d)(iv) kohaselt USA justiitsminister sekkuda ka DPRC tegevusse ega ei tohi ka justiitsministri määruse paragrahv 201.7(d) kohaselt kohtunikke enne nende ametiaja lõppu tagasi kutsuda ega nende suhtes muid distsiplinaarmeetmeid rakendada, välja arvatud kui selleks on mõjuv põhjus, nt kui kohtunik on pannud toime kuriteo. Sellega on USA adresseerinud ka Euroopa Kohtu poolt lahendis *Schrems II* välja toodud kriitikat, mille kohaselt *Privacy Shieldi* alusel loodud ombudsmani ametist tagandamise vastu ei eksisteerinud erilisi kaitsemeetmeid.²⁴²

Siinkirjutaja juhib veel ka tähelepanu eelnevalt Christakise jt poolt välja toodud argumendile, mille kohaselt DPRC iseseisvuse tagamisele aitab kaasa asjaolu, et justiitsministri määruses sätestatud nõudeid ei saa kergesti muuta. Nagu magistr töö autor ka ise küll tähelepanu juhtis, siis nt president Trump tunnistas enda valitsusajal kehtetuks mitmeid president Obama poolt antud korraldusi. Lähtuvalt Christakise jt argumendist aga selleks, et DPRC-d reguleerivaid sätteid muuta saaks, tuleb magistr töö autori arusaama kohaselt vastu võtta uus korraldus, mis omakorda volitab USA justiitsministrit vastu võtma uue määruse, millega siis oleks alles võimalik esialgset määrust muuta või seda tühistada. Arvestades et seda tuleb ka teha järgides samasuguseid avalikke menetluslikke samme nagu järgiti, et neid õigusakte esmakordselt vastu võtta, välistab see omakorda ka nt salaõiguse kohaldamise, mida autor käsitles peatükis 2.2.

²⁴⁰ *Ibidem*.

²⁴¹ EKo *Commission vs Poland*, p 111.

²⁴² EKo *Schrems II*, p 195.

2.4.3. Vahejärelalus

Kokkuvõtvalt jõuab siinkirjutaja eelnevate õigusaktide ja õigusteadlaste arvamuste analüüsimise pinnalt järeldusele, et kuigi DPRC näol on formaalselt tegu administratiivse organiga, siis sellele vaatamata eksisteerivad piisavad kaitsemeetmed, et tagada DPRC sõltumatus täitevvõimust. Kuigi eksisteerib mõnetine varasem praktika, mille kohaselt on USA presidendid tunnistanud eelnevate presidentide poolt välja antud korraldusi kehtetuks, siis selle vastu pakub kaitset asjaolu, et DPRC ei ole asutatud otseselt presidendi korraldusega, vaid hoopis justiitsministri määrusega. Võrreldes varasemalt kehtetuks tunnistatud korraldustega nõuaks selle määruse kehtetuks tunnistamine täiendavaid menetluslikke samme, mis ei ole ainuüksi presidendi pädevuses. Samuti ei tohi DPRC kohtunikke enne nende ametiaja lõppu tagasi kutsuda ega nende suhtes muid distsiplinaarmeetmeid rakendada, välja arvatud kui selleks on mõjuv põhjus, nt kui kohtunik on pannud toime kuriteo. Seega eksisteerivad ka piisavad kaitsemeetmed kohtunike ametist tagandamise vastu, mida ei olnud *Privacy Shield* ombudsmani puhul.

USA on siinkirjutaja hinnangul seega ka ära lahendanud probleemid, mille tõttu Euroopa Kohus leidis lahendis *Schrems II*, et eelmise andmekaitseraamistiku alusel loodud ombudsman ei olnud piisavalt sõltumatu. Järelikult kolmandale uurimisküsimusele tuleb vastata selliselt, et USA uus andmekaitseraamistik tagab, et DPRC on järelevalvemehhanismina piisavalt sõltumatu ning vastab seega põhiõiguste harta artiklist 47 tulenevatele nõuetele.

2.5. Tagatis D – kas eurooplastele on nende õiguste rikkumise korral tagatud tõhusad õiguskaitsevahendid?

2.5.1. EL-i õiguse nõuded

Viimane Euroopa Andmekaitsekoogu poolt tuletatud tagatis tuleneb põhiõiguste harta artikli 47 esimesest lõikest, mille kohaselt „igaühel, kelle liidu õigusega tagatud õigusi või vabadusi rikutakse, on selles artiklis kehtestatud tingimuste kohaselt õigus tõhusale

õiguskaitsevahendile kohtus“.²⁴³ Samuti on järgneva analüüsi kontekstis oluline ka ausa kohtupidamise põhimõte, millele juhtis tähelepanu Gorski.²⁴⁴ See põhimõte on tuletatud põhiõiguste harta artikkel 47 teisest lausest. Selle kohaselt peab menetlusosalistel olema võimalik tutvuda kohtule esitatud tõenditega; esitada nende tõendite kohta oma hinnang, et menetlusosalistel oleks võimalik kohut veenda; ning omada menetluslikku võrdsust vastaspoolega.²⁴⁵

Autor soovib siinkohal ära märkida, et järgneva analüüsi käigus tuleb järjekordselt juttu ka sõltumatuse kriteeriumist, kuid veidi erineva rõhuasetusega. Nimelt siinkirjutaja ei analüüsi järgnevalt mitte seda, kas DPRC on enda otsuste tegemisel sõltumatu²⁴⁶, vaid pigem seda, kas CLPO, st USA uue kaebuste lahendamise mehhanismi esimene aste²⁴⁷, on esialgse kaebuse uurimisel ja faktide kogumisel piisavalt sõltumatu, et tal oleks võimalik kaebuseid tõhusalt uurida, mis lõppkokkuvõttes viiks selleni, et DPRC kaebuste lahendamise mehhanismi teise astmena saab otsuse teha piisava informatsiooni ja õigete faktide põhjal.

2.5.2. USA andmekaitse tase

Nagu peatükis 1.3.3.2 mainitud, siis USA uue andmekaitseraamistiku alusel kehtestatakse kolmeastmeline mehhanism. Esimese kahe astme (CLPO ja DPRC) funktsioon on eurooplastest andmesubjektide kaebusi menetleda. Kõigepealt saavad kaebajad läbi EL-i kohaliku andmekaitseasutuse esitada CLPO-le kaebuse, kelle otsuse peale on võimalik edasi kaevata DPRC-sse. Kolmas aste (PCLOB) hakkab teostama järelevalvet selle üle, kas esimesed kaks astet on kaebuseid nõuetekohaselt lahendanud. PCLOB ise aga eurooplaste kaebuseid menetlema ei hakka, seega siinkirjutaja keskendub järgmise analüüsi raames eelkõige CLPO ja DPRC-ga seonduvate aspektide analüüsimisele.

Christakis jt on seisukohal, et korraldus EO 14086 ja USA justiitsministri määrus sisaldavad mitmeid sätteid, mis võimaldavad uuel kohtuorganil tõhusat kaebuste uurimist. Korralduse

²⁴³ Euroopa Andmekaitsekoostöökoostöösoovitused (2020), p 43.

²⁴⁴ Gorski, A.

²⁴⁵ *Ibidem*.

²⁴⁶ DPRC sõltumatuse analüüsi kohta vt ptk 2.4.

²⁴⁷ Vt CLPO kohta lähemalt ptk 1.3.3.2.

kohaselt peavad DPRC kohtunikud läbima turvakontrolli, mis on vajalik, et saada ligipääs salastatud riiklikule julgeolekuteabele. Tõhusale uurimisfunktsioonile viitabki Christakise jt hinnangul asjaolu, et CLPO viib läbi esialgse kaebuse uurimise, st tegeleb kõigepealt faktide kogumisega enne esmase otsuse tegemisega. Seda otsust võib siis kaebaja apelleerida, mille korral vaatab selle läbi ka DPRC kui kaebuste lahendamise mehhanismi teine etapp. Korraldus EO 14086 kohaselt peavad USA luureagentuurid tagama CLPO-le juurdepääsu informatsioonile, mis on vajalik uurimise läbiviimiseks ning luureagentuurid ei tohi võtta kasutusele ühtegi meetet, mis võiks takistada või sobimatult mõjutada CLPO poolt läbiviidavat uurimist.²⁴⁸

Korraldus EO 14086 kohaselt peab luurekogukonna iga element samuti tagama juurdepääsu teabele, mida DPRC kohtupaneel nõuab, et kaebust läbi vaadata. Lisaks ei tohi ükski luurekogukonna element võtta kasutusele meetmeid, mille eesmärk on takistada või sobimatult mõjutada kohtupaneeli poolt asja läbivaatamist. Christakis jt sõnul ei ole need lihtsalt ebamäärase avaldused, millel puudub õiguslik mõju. Nad selgitavad, et korraldusest EO 14086 tulenevate kohustuste eiramine on sisuliselt USA presidendi korralduse eiramine, mis tooks korraldust eiranud täitevorgani töötajatele kaasa tõsised tagajärjed ja sanktsioonid.²⁴⁹

Teiseks peab sõltumatu uurimise tagamiseks kaebuste lahendamise organil olema võimalik vastu võtta otsuseid, mis on siduvad.²⁵⁰ Christakis jt viitavad siinkohal otsusele *Schrems II*, kus Euroopa Kohus leidis²⁵¹, et eelmise andmekaitseraamistiku alusel loodud ombudsmani mehhanism seda tingimust ei täitnud.²⁵² Christakis jt leiavad, et EO-ga 14086 on USA valitsus Euroopa Kohtu kriitikat arvesse võtnud ja probleemi ära lahendanud. Nimelt sätestab EO 14086 sisuliselt, et iga luureühenduse element ja iga luureühenduse elementi

²⁴⁸ Christakis, T jt (oktoober 2022).

²⁴⁹ *Ibidem*.

²⁵⁰ *Ibidem*.

²⁵¹ EKo *Schrems II*, p 195.

²⁵² Christakis jt (oktoober 2022).

sisaldav agentuur on kohustatud DPRC otsuseid järgima. Nende hinnangul sisaldab EO 14086 mitmeid järelevalveprotseduure, sh kontrolli PCLOB-i poolt.²⁵³

Gorski on Christakisest jt erineval seisukohal: nimelt tema arvates ei saa CLPO ja DPRC poolt läbiviidavat kaebemenetlust lugeda põhiõiguste harta artikliga 47 kooskõlas olevaks.²⁵⁴ Kui Christakis jt leidsid, et „tõhususe“ tagab – nii nagu seda nõuab harta artikkel 47 – asjaolu, et 1) kaebuste läbivaatamise organil on laiad uurimisvolitused ja 2) kaebuste läbivaatamise organi otsused on luureasutustele siduvad²⁵⁵, siis kaebaja subjektiivsete õiguste perspektiivist ei ole nad „tõhusust“ analüüsinud. Magistritöö autor leiab, et Gorski poolt välja toodud probleemkohad, mille kohaselt menetluse piirangud, salajasus ja menetluslik ebaõiglus ei vasta EL-i õiguse standardile, kaaluvad üle Christakise jt argumentid. Christakis jt seadsid tõhususe kriteeriumite täitmiseks kohtuorgani uurimisvolituste olemasolu ja siduvate otsuste vastuvõtmise pädevuse, mille nad tuletasid *Schrems II* lahendist, kuid Euroopa Kohus on leidnud lahendis *La Quadrature Du Net*, et tõhusa õiguskaitsevahendi kasutamise eelduseks põhiõiguste harta artikli 47 tähenduses on siiski ka isiku subjektiivsed õigused: nt õigus olla teavitatud, et isikut jälgitakse; õigus tutvuda isikuandmetega, mille suhtes jälgimistegevust teostati ning vajadusel nõuda nende andmete parandamist või kustutamist.²⁵⁶ Eeltoodust lähtuvalt leiab siinkirjutaja, et tõhusa õiguskaitsevahendi analüüsimisel põhiõiguste harta artikli 47 tähenduses olid T. Christakis jt lahendanud ära ainult pool võrrandist, jättes käsitlemata puudused seoses kaebaja subjektiivsete õigustega.

Gorski on tähelepanu juhtinud ka sellele, et USA uue andmekaitseraamistiku alusel on probleemiks USA välisluure jälgimise alla kuuluvate isikute teavitamata jätmine.²⁵⁷ Gorski viitab *Schrems II* lahendi kohtujuristi arvamusele, kes kritiseeris USA suutmatust teavitada isikuid asjaolust, et neid jälgitakse isegi peale seda, kui jälgimine oli lõpetatud ning jälgimisest teada andmine ei oleks enam käimasolevat uurimist ohtu seadnud.²⁵⁸ Gorski

²⁵³ Christakis, jt (oktoober 2022).

²⁵⁴ Gorski, A.

²⁵⁵ Vt *supra*, lk 57, viide 226.

²⁵⁶ EKo *La Quadrature du Net*, p 190.

²⁵⁷ Gorski, A.

²⁵⁸ EKo C-311/18, Data Protection Commissioner vs Facebook Ireland Limited and Maximilian Schrems, ECLI:EU:C:2020:559, kohtujurist H. Saugmandsgaard Øe ettepanek, p 320.

viitab²⁵⁹ ka Euroopa Kohtu otsusele *La Quadrature du Net*, kus Euroopa Kohus selgitas, et isiku teavitamine on oluline selleks, et isikul oleks võimalik oma õiguste tõhusaks kaitseks kohtusse pöörduda, nagu seda näeb ette põhiõiguste harta artikli 47 esimene lause.²⁶⁰ Gorski leiab siinkirjutaja hinnangul põhjendatult, et olukorras, kus isik ei ole isegi teadlik, et teda on jälgitud, siis ei ole tal võimalik ju ka hinnata, kas on esinenud tema õiguste rikkumine ning järelikult ei ole tal ka efektiivselt võimalik enda õiguste kaitseks kohtusse pöörduda.

Muret seoses teavitamata jätmisega on avaldanud ka Euroopa Andmekaitsekohtu enda selle aasta 28. veebruaril avaldatud arvamuses, millega andis hinnangu Euroopa Komisjoni adekvaatsusotsuse eelnõule.²⁶¹ Esmalt viitas Euroopa Andmekaitsekohtu kohtulahendile *Kadi II*²⁶², kus tuli Euroopa Kohtul käsitleda ühelt poolt riigisaladuse kaitsmise huve ning teiselt poolt õiglase kohtumenetluse ja võistleva menetluse vastandlikke huve.²⁶³ Euroopa Kohus selgitas, et ülekaalukad liikmesriigi julgeolekuga seonduvad kaalutlused võivad takistada puudutatud isikule teatud andmetest või tõenditest teatamist.²⁶⁴ Sellises olukorras aga peab liikmesriigi kohus siiski rakendama kohtuliku kontrolli raames vahendeid, mis võimaldavad tasakaalustada ühelt poolt legitiimseid julgeolekukaalutlusi ning teiselt poolt vajadust tagada õigussubjektile tema õiguste kaitse.²⁶⁵ Selleks peab liikmesriigi kohus kontrollima, kas isiku teavitamata jätmine on põhjendatud tuginedes riikliku julgeoleku kaalutlustele.²⁶⁶ Siinkirjutaja juhib tähelepanu, et EL-i riikidest kasutab nt Prantsusmaa USA-ga mõnevõrra sarnast mehhanismi, kus kaebajale ei teavitata, kas teda on jälgitud või mitte. Seda aga ainult juhul, kui kaebaja suhtes ka reaalselt ebaseaduslikku jälgimistegevust ei tuvastatud. Olukorras, kus ebaseaduslik jälgimine aga tuvastati, teavitab andmesubjekti kaebust lahendav organ sellest andmesubjekti ja nõuab jälgimistegevust teostanud asutuselt, et rikkumine heastataks. Heastamine võib seisneda nt jälgimiseks antud volituse

²⁵⁹ Gorski, A.

²⁶⁰ EKo *La Quadrature du Net*, p 190.

²⁶¹ Euroopa Andmekaitsekohtu arvamus (2023), p 239.

²⁶² EKo liidetud kohtuasjad C-584/10 P, C-593/10 P ja C-595/10 P, *European Commission and Others vs Yassin Abdullah Kadi*, ECLI:EU:C:2013:518.

²⁶³ Euroopa Andmekaitsekohtu arvamus (2023), p 240.

²⁶⁴ EKo *Kadi II*, p 125.

²⁶⁵ *Ibidem*.

²⁶⁶ *Ibidem*, p 126.

tühistamises või ebaseaduslikult töödeldud isikuandmete kustutamises.²⁶⁷ Prantsusmaa lähenemine on järelikult USA lahendusest parem selles osas, et olukorras, kus ebaseaduslik jälgimistegevus on aset leidnud, antakse isikule sellest siiski vähemalt teada, ehk aitab paremini tagada kaebaja subjektiivseid õiguseid (õigus olla teavitatud, et isikut jälgitakse; õigus tutvuda isikuandmetega, mille suhtes jälgimistegevust teostati ning vajadusel nõuda nende andmete parandamist või kustutamist). See omakorda tagab andmesubjektile tõhusa õiguskaitsevahendi kasutamise võimaluse põhiõiguste harta artikli 47 tähenduses.

Euroopa Komisjon on adekvaatsusotsuse eelnõus CLPO ja DPRC vastuste andmist ja otsuste tegemist samuti põgusalt käsitlenud. Euroopa Komisjon kirjeldab, et kui CLPO on asja ülevaatamise lõpetanud, siis ta teavitab kaebajat, et 1) kaebuse hindamise käigus ei tuvastatud ühtegi rikkumist; või 2) CLPO on teinud otsuse, millega nõuab kaebaja õiguste rikkumise heastamist.²⁶⁸ Euroopa Komisjon leiab, et selline mehhanism võimaldab kaitsta ühelt poolt riiklikku julgeolekut, tagades teostatud signaalluure konfidentsiaalsuse, aga teiselt poolt andes siiski isikutele teada, et nende kaebust on nõuetekohaselt uuritud ning see on ära lahendatud. Euroopa Komisjon rõhutab veel, et otsust saab vaidlustada ning edasi kaevata DPRC-le, kes hindab, kas CLPO on kaebuse korrektselt läbi vaadanud. Ning kui kaebus jõuab DPRC ette läbi vaatamiseks, siis määratakse kaebaja huvide eest seisma eriadvokaat (ingl k *special advocate*).²⁶⁹ Põhjalikku analüüsi Euroopa Komisjon selle mehhanismiga seoses ei tee, vaid piirdub sisuliselt lihtsalt mehhanismi kirjeldamisega. Hinnangu andmisena saaks siiski käsitleda seda, et Euroopa Komisjon väitis, et mehhanism tagab selle, et CLPO on kaebust nõuetekohaselt uurinud ja selle ära lahendanud. Adekvaatsusotsuse eelnõu punktis 192 leiab Euroopa Komisjon kokkuvõtvalt, et isikutele on tagatud õiguste efektiivne kaitse. Magistritöö kirjutaja hinnangul ei saa Komisjoni järeldusega nõustuda. Euroopa Komisjon on jätnud hindamata selle, et tegelikult on sisuliselt tegemist üldsõnalise vastusega²⁷⁰, mistõttu on sisuliselt võimatu seda põhistatult edasi kaevata. See aga tähendab, et kaebajale ei ole kokkuvõtvalt tagatud subjektiivseid

²⁶⁷ European Union Agency for Fundamental Rights. Surveillance by intelligence services: fundamental rights safeguards and remedies in the EU. Volume II: field perspectives and legal update, 2017. Kättesaadav: https://fra.europa.eu/sites/default/files/fra_uploads/fra-2017-surveillance-intelligence-services-vol-2_en.pdf (20.04.2023), lk 130. (viidatud: France, Council of State (Conseil d'Etat), M. A.B., No. 396669, 05.05.2017.)

²⁶⁸ Adekvaatsusotsuse eelnõu, p 175.

²⁶⁹ *Ibidem*.

²⁷⁰ Vt *supra*, lk 62-63.

õiguseid (nt õigust olla teavitatud ning õigust tutvuda kohtuasja materjalidega), mis on Euroopa Kohtu praktikast²⁷¹ lähtuvalt põhiõiguste harta artikli 47 tähenduses olulised, et õiguskaitsevahendit saaks tõhusana käsitleda.

Euroopa Komisjon on adekvaatsusotsuse eelnõus punktis 184 põgusalt käsitlenud kaebuste lahendamise teise astme ehk DPRC poolt kaebajale edastatavaid vastuseid. Euroopa Komisjon kirjeldab vastuste edastamise protsessi, mille kohaselt kõigepealt saadetakse DPRC paneeli poolt tehtud otsus CLPO-le. Olukordades, kus DPRC poolt kaebuse läbivaatamise tingis kaebaja poolt tehtud avaldus, teavitatakse kaebajat läbi liikmesriigi kohaliku asutuse²⁷², et DPRC on enda hinnangu kaebusele andnud, lisades juurde, et hinnangu käigus ei tuvastatud ühtegi rikkumist või juhul, kui rikkumine tuvastati, siis on DPRC teinud otsuse, millega kohustab rikkumist heastama.²⁷³ Magistritöö autori hinnangul on ka siin Euroopa Komisjon jätnud sisuliselt hindamata, kas antud mehhanism vastab põhiõiguste harta artiklis 47 sätestatud nõuetele ning selle asemel lihtsalt andnud pinnapealse ülevaate sellest, mis justiitsministri määruses kirjas on. Euroopa Komisjon ei ole otsesõnu küll öelnud, et ta leiab, et kaebuste lahendamise teine etapp vastab EL-i õigusest tulenevatele standarditele, kuid adekvaatsusotsuse eelnõu punktis 193 on Euroopa Komisjon leidnud, et USA andmekaitseraamistik tervikuna tagab sisuliselt samaväärse kaitse nagu EL-i õigus, siis saab sellest järeldada, et Euroopa Komisjon on ka seisukohal, et DPRC poolt antavate vastustega suuri probleeme ei esine. Siinkirjutaja sellega jällegi ei nõustu ja leiab seevastu, et DPRC poolt edastatavad vastused on üldsõnalised – nagu arvas ka Gorski – ei saa selliselt edastatavad vastused kuidagi tagada, et kaebajatel oleks ligipääs tõhusale õiguskaitsevahendile nii nagu nõuab põhiõiguste harta artikli 47 esimene lause.

Üks aspektidest, mis on õigusekspertide seas palju diskussiooni tekitanud, on asjaolu, et USA ei andnud kaebuste lahendamise pädevust föderalkohtutele, vaid asutas hoopis uue kaebuste lahendamise organi, mis formaalselt asub täitevvõimu haldusalas. Samuti on Euroopa Kohus *Schrems II* kohtuasjas selgitanud, et tulenevalt põhiõiguste harta artiklist 47

²⁷¹ EKo *La Quadrature du Net*, p 190.

²⁷² Autori märkus: nt Eestis oleks selleks asutuseks Andmekaitse Inspeksioon.

²⁷³ Adekvaatsusotsuse eelnõu, p 184.

peab „õigussubjektil peab olema võimalus kasutada õiguskaitsevahendeid sõltumatus ja erapooletus kohtus, et tutvuda teda puudutavate isikuandmetega või lasta neisse parandusi teha või neid kustutada.“²⁷⁴ Sellega on tõstatatud küsimus, kas USA loodud uus kaebuste lahendamise organ saab üldse printsiibis Euroopa Kohtu seatud standarditele vastata. Euroopa Andmekaitsekohtu on juhtinud tähelepanu ka sellele, et põhiõiguste harta artikli 47 tõlkes paljudes erinevates keeltes mainivad sõna otseses mõttes „kohut“, kuigi ingliskeelses versioonis on kirjas „tribunal“, mis annaks võimaluse jõuda sellisele tõlgendusele, et kaebust lahendav organ põhiõiguste harta artikli 47 mõistes ei pea ilmtingimata olema „kohus“ kõige kitsamas mõttes.²⁷⁵ Viidates Euroopa Kohtu seisukohale²⁷⁶ lahendis *Schrems II* ja EIK-i mitmes lahendis välja toodud seisukohtadele²⁷⁷ on Euroopa Andmekaitsekohtu jõudnud järeldusele, et nii Euroopa Kohus kui ka EIK ei lähtu oma hinnangu andmisel puhtformaalsetest kriteeriumitest, vaid hindavad sisuliselt, kas konkreetne kaebust lahendav organ saab garanteerida kaebajale põhiõiguste harta artiklist 47 tulenevad tagatised.²⁷⁸

Siinkirjutaja selgitab Christakise jt analüüsile²⁷⁹ tuginedes, miks õiguskaitsevahendite tagamise seisukohast on eurooplastele isegi tõhusam, et kaebusi hakkab läbi vaatama administratiivse iseloomuga kohtuorgan ning mitte föderalkohus. Nimelt Christakis jt selgitavad, et USA põhiseaduse kolmanda artikli²⁸⁰ kohaselt on föderalkohtutel pädevus menetleda ainult selliseid kaasuseid, kus kaebaja suudab ära näidata talle tekkinud faktilise kahju. 2021. aastal tegi USA ülemkohus otsuse asjas *TransUnion vs Ramirez*²⁸¹, mille tagajärjel muutus privaatsusõiguse rikkumiste tulemusel tekkinud kahju tõendamine veelgi

²⁷⁴ EKo *Schrems II*, p 194.

²⁷⁵ Euroopa Andmekaitsekohtu arvamus (2023), p 218.

²⁷⁶ Vt EKo *Schrems II*, p 197.

²⁷⁷ Vt EIKo *Klass*, p 67; EIKo *Big Brother Watch*, p 359

²⁷⁸ Euroopa Andmekaitsekohtu arvamus (2023), p 218.

²⁷⁹ Christakis jt (oktoober 2022).

²⁸⁰ Article Three of the United States Constitution. Kättesaadav: <https://constitution.congress.gov/browse/article-3/> (22.04.2023).

²⁸¹ Vt *TransUnion LLC vs Ramirez*, 41 S. Ct. 2190 (2021). Kättesaadav: https://www.supremecourt.gov/opinions/20pdf/20-297_4g25.pdf (22.04.2023).

raskemaks.²⁸² Nimelt kordas ülemkohus 2016. aastal lahendis *Spokeo*²⁸³ lahendis välja toodud seisukohta ning laiendas seda nüüd ka privaatsusõiguse rikkumisele.²⁸⁴ Sisuliselt selgitas ülemkohus, et asjaolu, et seadusega on kellelegi kaebeõigus antud, ei tähenda automaatselt seda, et isikule on tekkinud faktiline kahju ning et tal eksisteeriks kaebuse menetlemise suhtes põhjendatud huvi.²⁸⁵ Lahendis *TransUnion vs Ramirez* leidis kohus, et isegi isikutel – kelle krediidiinfo lekkimise tulemusena pidas USA valitsus neid ekslikult potentsiaalseteks terroristideks – puudus faktiline kahju, mis annaks neile kaebeõiguse.²⁸⁶ Koostoimes korralduse EO 14086 ja justiitsministri määrusega asutatud DPRC-le kaebuse esitamisel aga faktilise kahju tekkimist tõendama ei pea. Sellele juhtis tähelepanu ka Euroopa Komisjon adekvaatsusotsuse eelnõus.²⁸⁷ Eelnõu kohaselt ei pea kaebaja faktiliselt ära näitama, et USA luureagentuurid on tema isikuandmetele ligipääsu saanud. Kaebaja peab ainult ära näitama baasinformatsiooni, nt missugused isikuandmed on kaebaja arvates USA-sse edastatud; millise sidevõrgustiku kaudu; millised USA valitsusasutused on andmete töötlemisel kaebaja õigusi rikkunud (juhul kui see peaks kaebajale teada olema, aga see ei ole kohustuslik) ning missugust resolutsiooni kaebaja kaebuse esitamisega taotleb.²⁸⁸

2.5.3. Vahejärelkus

Vaatamata sellele, et DPRC on eurooplaste perspektiivist kaebuste lahendamiseks parem variant kui USA föderaalkohtud, ei saa kokkuvõtvalt siiski järeldusele jõuda, et on täidetud kõik põhiõiguste harta artiklist 47 tulenevad nõuded tõhusale õiguskaitsevahendile. Uus mehhanism eurooplastest andmesubjektide kaebuste menetlemiseks tagab küll efektiivsema uurimisfunktsiooni faktide kindlaks tegemiseks ja informatsiooni kogumiseks, kuid kaebuse esitajatele ei ole piisavalt tagatud subjektiivsed õigused, nt õigus olla teavitatud, et neid jälgitakse; õigus tutvuda isikuandmetega, mille suhtes jälgimistegevust teostati ning

²⁸² Christakis, T., jt. EU/US Adequacy Negotiations and the Redress Challenge: Whether a New U.S. Statute is Necessary to Produce an “Essentially Equivalent” Solution. – European Law Blog, 31.01.2022. Kättesaadav: https://europeanlawblog.eu/2022/01/31/eu-us-adequacy-negotiations-and-the-redress-challenge-whether-a-new-u-s-statute-is-necessary-to-produce-an-essentially-equivalent-solution/#_edn2 (22.04.2023).

²⁸³ Vt *Spokeo, Inc. vs Robins*, 578 U.S. 330 (2016). Kättesaadav: <https://supreme.justia.com/cases/federal/us/578/13-1339/> (22.04.2023).

²⁸⁴ Christakis T, jt (jaanuar 2022).

²⁸⁵ *Ibidem*.

²⁸⁶ *Ibidem*.

²⁸⁷ Adekvaatsusotsuse eelnõu, p 170.

²⁸⁸ *Ibidem*.

vajadusel õigus nõuda nende andmete parandamist või kustutamist. Arvestades, et Euroopa Kohus on neid kriteeriume oluliseks pidanud, et õiguskaitsevahend oleks põhiõiguste harta artikli 47 tähenduses tõhus²⁸⁹, siis siinkirjutaja hinnangul ei saa nõustuda õigusteadlaste arvamusega, kelle hinnangul selline USA poolt pakutav lahendus on piisav. Euroopa Komisjon jõudis adekvaatsusotsuse eelnõus samuti järeldusele, et kaebajatele on tagatud tõhus õiguskaitsevahend. Komisjon ei hinnanud aga sisuliselt seda, kas kaebajat jälgimisest teatatakse ning kuidas mõjutab kaebajale edastatavate vastuste üldsõnalisus seda, kas kaebajal on võimalik nt CLPO otsuse peale DPRC-sse apellatsioon esitada, et oma õiguseid tõhusalt artikli 47 tähenduses tõhusalt kaitsta. Aga nagu eelnevalt mainitud, siis magistritöö jõudis järeldusele, et kaebajale ei ole neid õiguseid efektiivselt tagatud, seega ei saa ka Euroopa Komisjoni järeldusega nõustuda. Järelikult vastus magistritöö neljandale uurimisküsimusele on, et eurooplastele ei ole nende õiguste rikkumise korral tagatud õigus tõhusale õiguskaitsevahendile põhiõiguste harta artikli 47 esimese lause kohaselt.

2.6. Järeldus USA andmekaitse taseme kohta

Järgnevalt võtab autor kokku eelneva analüüsi pinnalt tehtud vahejäreldused selle kohta, kas USA uus andmekaitseraamistik vastab Euroopa Andmekaitsekoogu poolt sätestatud Euroopa olulistele tagatistele, mille järgimine on tähtis selleks, et signaalluure teostamise käigus ei riivataks privaatsus- ja andmekaitsepõhiõiguseid rohkem kui on vajalik ja proportsionaalne EL-i õiguse tähenduses. Seeläbi esitab autor magistritöö uurimisküsimuste vastused.

Vastus esimesele uurimisküsimusele oli eitav: USA andmekaitseraamistik ei sätesta selged, täpsed ja ligipääsetavad (avalikud) reeglid signaalluuretegevuse käigus isikuandmete töötlemisele. USA uus andmekaitseraamistik võimaldab presidendil salaja, ilma avalikkust teavitamata, muuta korraldust EO 14086, mis sätestab signaalluure teostamise eesmärgid ning piirangud.

²⁸⁹ EKo *La Quadrature du Net*, p 190.

Vastus teisele uurimisküsimusele oli eitav: USA andmekaitseraamistik ei taga, et signaalluure teostamisega kaasnevad põhiõiguste riived oleksid vajalikud ja proportsionaalsed põhiõiguste harta artikli 52 tähenduses, tõlgendatuna lähtuvalt Euroopa Kohtu praktikast. USA uus andmekaitseraamistik võimaldab luureagentuuridel teostada signaalluuret, mille käigus toimub isikuandmete masskogumine, st kogutakse suure hulga isikute isikuandmeid, ilma eelnevalt välja selgitamata, kas konkreetsete isikute jälgimine aitab kaasa signaalluure teostamise eesmärgile.

Vastus kolmandale uurimisküsimusele oli jaatav: USA uus andmekaitseraamistik tagab, et USA signaalluure raames teostatavat isikuandmete töötlemise õiguspärasust kontrollib sõltumatu järelevalvemehhanism. Koostoimes korralduse EO 14086 ja justiitsministri määrusega loodav DPRC on täitevvõimust piisavalt sõltumatu. Sõltumatus on tagatud läbi tagatiste, mis kaitsevad DPRC kohtunikke selle eest, et neid eemaldatakse ametist ilma mõjuva põhjuseta.

Vastus neljandale uurimisküsimusele oli eitav: USA uus andmekaitseraamistik ei taga üksikisikutele – kes leiavad, et nende õigusi on rikutud – tõhusaid õiguskaitsevahendeid oma õiguste kaitsmiseks. Üksikisikutele ei ole tagatud järgnevad subjektiivsed õigused: õigus olla teavitatud, et neid jälgitakse; õigus tutvuda isikuandmetega, mille suhtes jälgimistegevust teostati ning vajadusel nõuda nende andmete parandamist või kustutamist. Seega ei saa üksikisikud kasutada tõhusaid õiguskaitsevahendeid põhiõiguste harta artikli 47 tähenduses.

Eelneva analüüsi pinnalt selgub, et USA uus andmekaitseraamistik vastab ainult ühele neljast Euroopa olulisest tagatisest. Euroopa Andmekaitsekoostöögrupp on küll märkinud, et Euroopa olulised tagatised on vaid üks osa hindamisest, mis tuleb läbida, et vastata küsimusele, kas kolmandas riigis on tagatud selline andmekaitse tase, mis on samaväärne EL-is tagatava tasemega.²⁹⁰ Võttes arvesse aga seda, et Euroopa Kohtu varasem kriitika on peamiselt olnud suunatud USA signaalluurele ja selle mittevastavusele EL-i poolt nõutavale andmekaitse, siis siinkirjutaja hinnangul võib järeldada, et kui USA uus

²⁹⁰ Euroopa Andmekaitsekoostöögrupp soovitusel (202), p 8.

andmekaitseraamistik vastab ainult ühele signaalluuret käsitlevale olulisele tagatisele neljast, siis ei saa vastata sealne andmekaitse tase sellele, mis on sisuliselt samaväärne EL-is tagatuga. Järelikult ei leidnud kinnistust ka magistritöö autori püstitatud hüpotees.

Eeltoodust lähtuvalt juhul, kui Euroopa Komisjon otsustab USA uue andmekaitseraamistiku suhtes GDPR-i artikkel 45 lõike 1 alusel anda välja adekvaatsusotsuse, siis on siinkirjutaja hinnangul tõenäoline, et ka see otsus tunnistatakse Euroopa Kohtu poolt lähiaastatel kehtetuks.

KOKKUVÕTE

Magistritöö eesmärk oli välja selgitada, kas USA uue andmekaitseraamistikuga kehtestatud piirangud signaalluurele tagavad selle, et USA luureagentuuride signaalluuretegevus vastab EL-i poolt nõutavale andmekaitse tasemele. Magistritöö eesmärgi saavutamiseks püstitas autor neli uurimisküsimust, mis on tuletatud Euroopa Andmekaitsekoostöö poolt sätestatud Euroopa olulistest tagatistest. Nende tagatistele vastavuse hindamine on oluline, et teha selgeks, kas jälgimismeetmete kaudu privaatsuse ja andmekaitse põhiõiguste riivamine rikub vajalikkuse ja proportsionaalsuse põhimõtteid.

Magistritöö esimeses peatükis andis autor kõigepealt ülevaate sellest, millistel õiguslikel alustel võib EL-ist isikuandmeid kolmandatesse riikidesse – sh USA-sse – edastada. Andmeid tohib kolmandatesse riikidesse edastada põhiliselt kolmel GDPR-is sätestatud alusel. Esimene õiguslik alus on artikkel 45 lg 1 alusel, mille kohaselt võib andmete edastamine toimuda juhul, kui Euroopa Komisjon on kolmanda riigi suhtes andnud välja adekvaatsusotsuse, millega Euroopa Komisjon on kinnitanud, et kolmandas riigis tagatav andmekaitse tase on EL-i õiguse kontekstis piisav. Adekvaatsusotsuse puudumisel on teiseks õiguslikuks aluseks artikkel 46 lg 1, mille kohaselt tohib isikuandmeid edastada siis, kui on sätestatud asjakohased kaitsemeetmed, aitavad tagada selle, et andmesubjektidele on kättesaadavad kohtulikult kaitstavad õigused ja tõhusad õiguskaitsevahendid. Põhiliselt kasutatakse sellistest kaitsemeetmetest standardseid andmekaitseklausleid. Kolmas õiguslik alus on artikkel 49, kuid sellele saab tugineda vaid väga erandlikel juhtudel.

Esimeses peatükis analüüsis autor ka USA ja EL-i fundamentealselt üksteisest erinevat lähenemist andmekaitsele. EL-is on andmekaitse põhiõigus, mille kohaselt on kõikidel õigus privaatsusele ning sellele, et nende andmed oleksid kaitstud. Selline kaitse peab laienema ka olukordadele, kus isikuandmed edastatakse EL-i piiridest välja, sh USA-sse. USA-s seevastu sellist universaalset lähenemist ei eksisteeri. Seal reguleeritakse privaatsust põhjalikumalt vaid üksikutes sektorites, nt on andmekaitsekohustused kehtestatud finantsasutuste,

tervishoiuasutuste ja sideteenuse pakkujate suhtes või teatud eriliigiliste andmete kaitsmiseks, nagu nt laste isikuandmed.

Olles teinud kindlaks õigusliku aluse andmete edastamiseks ja välja selgitanud, milles seisneb USA ja EL-i andmekaitsele lähenemise erinevus, analüüsis autor õigusakte, mis võimaldavad Atlandi-ülese andmeedastuse käigus eurooplaste isikuandmete suhtes teostada signaalluuret. See on põhiliselt võimalik kahe õigusakti alusel: FISA paragrahv 702 ja korraldus EO 12333. Lähtuvalt Edward Snowdeni 2013. aastal tehtud avaldustest, et USA teostab ülemaailmselt massilist isikute jälgimist, on USA valitsus üritanud sellist jälgimistegevust ka piirata president Obama poolt vastu võetud õigusaktiga PPD-28. Seda eelkõige põhjusel, et säiliks suurtemate takistusteta digitaalkaubandus EL-iga, kelle õiguskorraga on sellise massiline isikute jälgimine vastuolus.

Autor analüüsis ka kahte kohtulahendit *Schrems* ja *Schrems II*, millega Euroopa Kohus tunnistas pärast Snowdeni avaldusi kehtetuks kaks varasemat adekvaatsusotsust, mis võimaldasid GDPR-i artikli 45 alusel isikuandmeid Atlandi-üleselt ilma suuremate piiranguteta edastada. Peamised põhjused nende adekvaatsusotsuste kehtetuks tunnistamisel seisnesid selles, et esiteks USA teostatav signaalluure ei olnud vajalik ja proportsionaalne EL-i õiguse tähenduses ning teiseks, et USA-s puudus sõltumatu järelevalveasutus, kes saaks tagada eurooplastele tõhusad õiguskaitsevahendid, kui nad leiavad, et nende õigusi on signaalluure teostamisega rikutud.

2022. aasta oktoobris avaldas USA uus andmekaitseraamistik, mis baseerub peamiselt president Bideni allkirjastatud korraldusel EO 14086, mille ülesanne on adresseerida Euroopa Kohtu kriitikat varasemate õigusraamistike osas ning piirata signaalluuret piisaval määral, et USA uus andmekaitseraamistik saaks vastata sisuliselt samaväärsele andmekaitse tasemele nagu nõuab EL-i õigus. Olles eelnevalt kindlaks teinud peamised õigusaktid, mille alusel USA-s signaalluuret teostatakse ja ka omakorda selle teostamist piiratakse, keskendus autor teises peatükis sellele, kas nendel õigusaktidel põhinev USA uus andmekaitseraamistik tagab EL-i perspektiivist vaadatuna piisava andmekaitse taseme.

Esimesele uurimisküsimusele leidis autor vastuse peatükis 2.2. Vastus sellele uurimisküsimusele oli eitav. USA andmekaitseraamistik ei sätesta piisavalt selged, täpsed ja ligipääsetavad (avalikud) reeglid signaalluuretegevuse käigus isikuandmete töötlemisele. USA uus andmekaitseraamistik võimaldab presidendil salaja, ilma avalikkust teavitamata, muuta korraldust EO 14086, mis sätestab signaalluure teostamise eesmärgid ning piirangud.

Peatükis 2.3 sai vastuse teine uurimisküsimus ning see oli eitav. USA andmekaitseraamistik ei taga, et signaalluuretegevusega kaasnevad põhiõiguste riived oleksid vajalikud ja proportsionaalsed põhiõiguste harta artikli 52 tähenduses. USA andmekaitseraamistik võimaldab luureagentuuridel teostada signaalluuret, mille käigus toimub isikuandmete masskogumine, st kogutakse suure hulga isikute isikuandmeid, ilma eelnevalt välja selgitamata, kas konkreetsete isikute jälgimine aitab kaasa signaalluure teostamise eesmärgile.

Vastus kolmandale uurimisküsimusele selgus peatükis 2.4 ning oli jaatav. USA uus andmekaitseraamistik tagab, et USA signaalluure raames teostatavat isikuandmete töötlemise õiguspärasust kontrollib järelevalvemehhanism, mis vastab põhiõiguste harta artiklist 47 tulenevale sõltumatuse kriteeriumile. Peamine tagatis, mis aitab sõltumatust saavutada, on see, et DPRC kohtunike ametist tagandamise vastu eksisteerivad kaitsemeetmed, mis puudusid eelmise andmekaitseraamistiku alusel funktsioneerinud ombudsmanil.

Vastus neljandale uurimisküsimusel oli eitav ning selgus peatükis 2.5. USA uus andmekaitseraamistik ei taga üksikisikutele – kes leiavad, et nende õigusi on rikutud – tõhusaid õiguskaitsevahendeid oma õiguste kaitsmiseks põhiõiguste harta artikli 47 tähenduses. Üksikisikutele ei ole tagatud järgnevad subjektiivsed õigused: õigus olla teavitatud, et isikut jälgitakse; õigus tutvuda isikuandmetega, mille suhtes jälgimistegevust teostati ning õigus vajadusel nõuda nende andmete parandamist või kustutamist. Need on

Euroopa Kohtu praktikast lähtuvalt olulised, et isikutel oleks võimalik oma õiguseid efektiivselt kaitsta.

Eeltoodust lähtuvalt sai jaatava vastuse ainult kolmas uurimisküsimus. Seega on tagatud ainult üks Euroopa Andmekaitsekohtu tagatis neljast tagatisest, mis on olulised, et signaalluure teostamise käigus ei riivataks privaatsus- ja andmekaitsepõhiõiguseid rohkem kui on vajalik ja proportsionaalne EL-i õiguse tähenduses. Võttes arvesse, et Euroopa Kohus on kaks erinevat andmekaitseraamistiku just nende põhimõtete rikkumise tõttu kehtetuks tunnistanud, siis autori hinnangul tuleb järeldada, et olukorras, kus on tagatud vaid üks tagatis neljast, ei vasta USA uue andmekaitseraamistiku alusel tagatav andmekaitse tase sellele, mis on sisuliselt samaväärne EL-is tagatuga. Järelikult ei leidnud kinnitust ka magistritöö autori püstitatud hüpotees. Juhul kui Euroopa Komisjon otsustab USA uue andmekaitseraamistiku suhtes anda välja adekvaatsusotsuse, siis on siinkirjutaja hinnangul tõenäoline, et ka see otsus tunnistatakse Euroopa Kohtu poolt lähiaastatel kehtetuks.

Abstract

COMPLIANCE OF SIGNALS INTELLIGENCE ACTIVITIES CONDUCTED UNDER THE NEW DATA PROTECTION FRAMEWORK OF THE UNITED STATES WITH THE LEVEL OF DATA PROTECTION REQUIRED BY THE EUROPEAN UNION IN THE CONTEXT OF TRANSATLANTIC DATA TRANSFERS

The United States (hereinafter: the US) is the largest trading partner of the European Union (hereinafter: the EU). In 2021, the US exported \$283 billion worth of digital services to Europe. Electronic communication and social media services, such as Gmail, Facebook and Instagram – that are provided by large US technology companies – have become a large part of the daily lives of European citizens. Almost a year ago, however, the US technology company Meta suddenly threatened to stop offering its Facebook and Instagram services in the EU. The main reason for that is the strict legal framework that governs the processing of personal data and the transfer thereof to third countries, including to the US.

The EU's concern with personal data transfers to the US began in 2013 when the large-scale surveillance by US intelligence agencies became known due to the revelations of former US National Security Agency (hereinafter: NSA) employee Edward Snowden. It was revealed that the US government also uses the help of large US technology companies to monitor people all over the world. This led to the realization that since such services are offered in the EU, the US could potentially be monitoring EU citizens as well. This concern of the EU has led to the invalidation of two different EU-US data transfer frameworks by the European Court of Justice (hereinafter: the CJEU) in less than 10 years, which had enabled the smooth functioning of the digital economy between the EU and the US. In October 2022, a third such framework was announced by the US and the European Commission called the EU-US Data Privacy Framework (hereinafter also: the DPF), which aims to address the criticism of the two different previous data frameworks by the CJEU, which led to their invalidation.

The purpose of this thesis is to find out whether the new safeguards implemented with the DPF on US signals intelligence activities ensure that such activities of US intelligence

agencies meet the level of data protection required under EU law. The author of this thesis set out to achieve this purpose by analyzing whether the DPF meets the requirements of the European Data Protection Board's (hereinafter: EDPB) European Essential Guarantees (hereinafter: EEGs) for surveillance measures.

The author also formulated a hypothesis that the DPF offers an adequate level of protection as required under EU law. The reason for that is the fact that previous CJEU criticism of the level of protection provided by the US has been that 1) the US does not ensure that interferences to fundamental rights caused by signals intelligence activities are limited to what is strictly necessary and proportionate in a democratic society and 2) the US does not provide for independent oversight on the legality of processing of personal data when conducting signals intelligence activities.

At first glance, it would seem that the US has taken those criticisms of the CJEU into account when developing the DPF. The new EO 14086 states that the signals intelligence activities conducted by US intelligence agencies must be necessary to advance a validated intelligence priority and also conducted only to the extent and manner that is proportionate to such validated intelligence priority. The new EO 14086 also authorizes the creation of a new Data Protection Review Court (hereinafter: the DPRC), which at first glance seems to be more independent from the executive than the previous supervisory mechanism under the EU-US Privacy Shield (hereinafter: the Privacy Shield) – the ombudsman. The new EO 14086 states that judges are given safeguards that would protect from their removal from office. The absence of any such meaningful safeguards was the main criticism of the CJEU directed at the independence of the ombudsman mechanism and one of the reasons for the invalidation of the Privacy Shield.

The EEGs, which the author set out to analyze, are guarantees that are mostly based on the jurisprudence of the CJEU related to Articles 7, 8, 47 and 52 of the Charter of Fundamental Rights of the European Union (hereinafter: the Charter of Fundamental Rights). The EDPB has also taken into account the jurisprudence of the European Court of Human Rights (hereinafter: the ECtHR) which relates to Article 8 of the European Convention on Human Rights (hereinafter: the ECHR), as the jurisprudence of the ECtHR is binding on member states of the EU.

The EEGs were originally identified after the Schrems I judgement with which the CJEU invalidated the original data transfer agreement between the EU and US called the EU-US Safe Harbor Framework (hereinafter: the Safe Harbor). The EEGs are guarantees that need to be respected to make sure interferences caused via surveillance measures to the rights set out in Articles 7 (the right to privacy) and Article 8 (the right to the protection of personal data) – when transferring personal data – do not go beyond what is strictly necessary and proportionate under Article 52 of the Charter of Fundamental Rights.

The thesis is qualitative in nature, which is why the author has used traditional legal research methods: mostly the analytical and comparative method. The author has compared the legislation of the EU and the US and the level of data protection ensured by their respective legal systems. The author has also analyzed the case law of the CJEU and the ECtHR, compared and analyzed the opinions of various legal scholars. The main sources used in the thesis are EU and US legislation, the opinions of legal scholars, relevant case law of the CJEU and ECtHR and to a smaller extent, US case law. The author has also used legal literature related to privacy, data protection and surveillance; the decisions, guidelines and opinions of various EU institutions, such as the European Commission, the European Parliament and the EDPB.

The master's thesis consists of two main chapters. In the first chapter, the author analyzes the legal basis on which personal data can be transferred out of the EU. The main three different conditions for personal data transfers are: transfers on the basis of an adequacy decision; transfers that are subject to appropriate safeguards; and derogations for specific situations. In this thesis the author has focused on the first legal basis – Article 45 of the General Data Protection Regulation (hereinafter: the GDPR), because this would be the legal basis on which the European Commission would determine that the DPF offers an adequate level of protection to data transferred from the EU to the US.

The author then analyzes the fundamentally different approaches of the EU and the US to data protection and privacy. In the EU, data protection and privacy are seen as a universal human right whereas in the US, privacy is highly regulated mostly only in specific sectors, such as the financial and healthcare sector. In the first chapter the author also identifies the two main legal acts on which US signals intelligence activities are based that authorize the

surveillance of European citizens. Those are Executive Order 12333 (hereinafter: the EO 12333) and Section 702 of the Foreign Intelligence Surveillance Act (hereinafter: the FISA 702).

The author also identified the main two acts which are supposed to help mitigate the interferences to the rights to privacy and data protection that are caused by signals intelligence activities. Those two legal acts are Presidential Policy Directive (hereinafter: the PPD-28) and the Executive Order 14086 (hereinafter: the EO 14086).

Lastly, in the first chapter the author also analyzed the two CJEU decisions (Schrems I and Schrems II), which invalidated Safe Harbor and Privacy Shield – the two previous data transfer agreements between the EU and the US. Those two CJEU decisions are critical for the analysis that follows in the second chapter, because those decisions laid out the main requirements that the US would need to provide in order to ensure an adequate level of protection of personal data under EU law.

In the second chapter the author sets out to analyze whether the DPF meets the requirements of the EEGs. The four EEGs are as follows. Firstly, processing of personal data should be based on clear, precise and publicly accessible rules. Secondly, the legitimate objectives pursued by the surveillance activities need to be necessary and proportional to the interference caused to the rights of the data subjects. Thirdly, the interferences caused to the data subjects by surveillance activities should be subjected to an independent and impartial oversight system. Fourthly, effective and enforceable rights must be available to the data subjects – whose rights to privacy and data protection have or may have been violated through the conducting of signals intelligence. Based on the analysis the author sets out to determine whether the DPF ensures an essentially equivalent level of data protection to that which is guaranteed in the EU.

With regard to the first EEG, the author found that the rules laid down in EO 14086, which enable the conducting of signals intelligence, are not sufficiently clear and precise. EO 14086 allows the president to expand the list of priorities for which signals intelligence is permitted, for example in the name of national security. The US has a history of interpreting threats to national security in a very abstract and broad manner, which the author addresses

down below under the analysis of the second EEG. As regards amending the list of priorities for which signals intelligence can be authorized – the president can also authorize such amendments in secret in the name of national security. This is not in line with the jurisprudence of the ECtHR relating to surveillance. The ECtHR has stated that when covert surveillance measures are used, such as the interception of communications, it is important to establish clear and precise rules. The court has also added that as technology used for such surveillance becomes progressively more sophisticated (therefore making it easier to monitor people), the risk of arbitrariness by the surveillance authorities is obvious in such a situation, which further increases the importance of setting clear and precise rules.

With regard to the second EEG, the author found that the DPF does not ensure that interferences to the rights of data subjects are limited to what is strictly necessary and proportionate in a democratic society within the meaning of Article 52 of the Charter of Fundamental Rights. The EO 14086 permits collection of data without the use of discriminants, i.e. data that is not tied to a specific surveillance target (hereinafter: bulk collection) in cases where it is not clear whether such bulk collection of data is necessary to achieve the legitimate purposes for which the collection was originally authorized. CJEU case law has established that bulk collection should only be allowed in very extreme circumstances, such as a serious threat to national security, which is shown to be genuine and present or foreseeable, such as terrorist attacks. The US, however, interpretes national security in a very abstract and broad manner. For example, the US has in the past interpreted threats of organized crime and immigration as threats to national security, which would then authorize intelligence agencies to conduct bulk collection to fight against immigration or threats of organized crime under the veil of national security. This interpretation goes a lot farther than that of the jurisprudence of the CJEU.

With regard to the third EEG, the author found that the DPF ensures that interferences caused to the data subject by surveillance activities are subject to an independent and impartial oversight system as required under Article 47 of the Charter of Fundamental Rights. The Data Protection Review Court (DPRC) which is to be created under the new framework has sufficient independence from the executive power. In the case of Schrems I, the CJEU found that the oversight mechanism operating under the previous framework Privacy Shield was not sufficiently independent from the executive, mostly due to a lack of safeguards which

would protect from removal from office. Under the new framework, the safeguards granted to the DPRC judges have been improved. Under the DPF, the US Attorney General may not intervene with the day-to-day job of the judges and the Attorney General may also not remove the judges or take disciplinary action against them prior to the end of their term, except as warranted in very limited circumstances. For example when the judges have committed a crime.

With regard to the fourth and final EEG, the author found that the new framework does not provide for effective legal remedies to individuals who believe their rights have been violated via the conducting of surveillance by US intelligence agencies. Individuals are not guaranteed the subjective rights that the CJEU has deemed to be important in order for the remedy to be considered effective under Article 47 of the Charter of Fundamental Rights, such as the right to be informed. The main issue under the new US framework is that the individuals are not informed of the fact whether they have been subject to surveillance or not. If the individual is not informed, they do not have the opportunity to bring a meaningful case to the court to protect their rights under Article 47 of the Charter of Fundamental Rights.

Based on the above, the new US framework only complies with one of the EEGs: the existence of an independent and impartial oversight system as required under Article 47 of the Charter of Fundamental Rights. The EDPB has explained that in order to assess the adequacy of the level of protection of a third country, the EEGs are only part of the whole assessment process to determine whether the third country offers a level of data protection which is essentially equivalent to that guaranteed under EU law. In spite of that, in the opinion of the author, based on the previous analysis it can be concluded that the new US framework does not offer a level of protection that is essentially equivalent. The reason for that is the fact that US surveillance has been the most problematic aspect to the CJEU when evaluating the previous data transfer frameworks between the EU and the US. As long as that remains an issue under the new framework, the US cannot in the opinion of the author guarantee an adequate level of protection as required under EU law. This also means that author's hypothesis was not supported.

In the event that the European Commission decides to adopt an adequacy decision based on the new US framework, in the opinion of the author it is highly likely that such a decision

will be invalidated by the CJEU in the upcoming years, similarly to the previous two frameworks Safe Harbor and Privacy Shield in the CJEU decisions Schrems and Schrems II.

LÜHENDID

Adekvaatsusotsused	Euroopa Komisjoni rakendusotsused, millega hinnatakse kolmandate riikide õiguskorda või nende poolt võetud rahvusvahelisi kohustusi andmekaitse taseme poolest piisavaks
Adekvaatsusotsuse eelnõu	Euroopa Komisjoni rakendusotsuse eelnõu USA uue andmekaitseraamistiku kaitse taseme piisavuse kohta: Draft Commission Implementing Decision pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate level of protection of personal data under the EU-US Data Privacy Framework, 13.12.2022
Andmekaitse direktiiv 95/46	Euroopa Parlamendi ja nõukogu 24.10.1995. a direktiiv 95/46/EÜ üksikisikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise kohta
CCPA	<i>California Consumer Privacy Act of 2018</i>
CLPO	<i>Chief Liberties Protection Officer</i>
CPRA	<i>California Privacy Rights Act of 2020</i>
DOT	<i>Department of Transportation</i>
DPRC	<i>Data Protection Review Court</i>
EIK	Euroopa Inimõiguste Kohus
EIKo	Euroopa Inimõiguste Kohtu otsus

EKo	Euroopa Kohtu otsus
EL	Euroopa Liit
EO 12333	<i>Executive Order 12333</i>
EO 14086	<i>Executive Order 14086</i>
EIÕK	Euroopa inimõiguste ja põhivabaduste kaitse konventsioon
FISA	<i>Foreign Intelligence Surveillance Act</i>
FTC	<i>Federal Trade Commission</i>
GDPR	<i>General Data Protection Regulation</i> – Euroopa Parlamendi ja nõukogu määrus (EL) 2016/679, 27. aprill 2016, füüsiliste isikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise ning direktiiv 95/46/EÜ kehtetuks tunnistamise kohta (isikuandmete kaitse üldmäärus)
Justiitsministri määrus	<i>Attorney General Order No. 5517-2022</i>
LED	<i>Law Enforcement Directive</i> – 27. aprilli 2016. aasta Euroopa Parlamendi ja nõukogu direktiiv (EL) 2016/680, mis käsitleb füüsiliste isikute kaitset seoses pädevates asutustes isikuandmete töötlemisega süütegude tõkestamise, uurimise, avastamise ja nende eest vastutusele võtmise või kriminaalkaristuste täitmisele pööramise eesmärgil ning selliste andmete vaba liikumist ning millega tunnistatakse kehtetuks nõukogu raamotsus 2008/977/JSK

NSA	<i>National Surveillance Agency</i>
PCLOB	<i>Privacy and Civil Liberties Oversight Board</i>
PPD-28	<i>Presidential Policy Directive 28</i>
Põhiõiguste harta	Euroopa Liidu põhiõiguste harta
USA uus andmekaitseraamistik	<i>European Union-U.S. Data Privacy Framework</i>
WP29	EL-i andmekaitseasutuste tööühm

KASUTATUD MATERJALIDE LOETELU

Kirjandus

1. Antson, A. Elektroonilise side andmete säilitamise ja põhiõiguste tagamise vahekord kriminaalmenetluses. Magistritöö – Tallinn: Tartu Ülikool, 2021.
2. Brown, I., Korff, D. Exchanges of Personal Data After the Schrems II Judgment. Study for the European Parliament's Committee on Civil Liberties. Kättesaadav: [https://www.europarl.europa.eu/RegData/etudes/STUD/2021/694678/IPOL_STU\(2021\)694678_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/STUD/2021/694678/IPOL_STU(2021)694678_EN.pdf) (19.04.2023).
3. Cameron, K, Raul, A.C. The Economic Case for Preserving PPD28 and Privacy Shield. – Lawfare, 17.01.2017. Kättesaadav: <https://www.lawfareblog.com/economic-case-preserving-ppd-28-and-privacy-shield> (14.02.2023).
4. Christakis T, jt. EU/US Adequacy Negotiations and the Redress Challenge: Whether a New U.S. Statute is Necessary to Produce an “Essentially Equivalent” Solution. – European Law Blog, 31.01.2022. Kättesaadav: https://europeanlawblog.eu/2022/01/31/eu-us-adequacy-negotiations-and-the-redress-challenge-whether-a-new-u-s-statute-is-necessary-to-produce-an-essentially-equivalent-solution/#_edn2 (22.04.2023).
5. Christakis, T jt. The redress mechanism in the Privacy Shield successor: On the independence and effective powers of the DPRC. – The International Association of Privacy Professionals, 11.10.2022. Kättesaadav: <https://iapp.org/news/a/the-redress-mechanism-in-the-privacy-shield-successor-on-the-independence-and-effective-powers-of-the-dprc/> (20.04.2023).
6. Goitein, E. The Biden Administration’s SIGINT Executive Order, Part I: New Rules Leave Door Open to Bulk Surveillance, 31.10.2022. Kättesaadav: <https://www.justsecurity.org/83845/the-biden-administrations-sigint-executive-order-part-i-new-rules-leave-door-open-to-bulk-surveillance/> (19.04.2023).
7. Goitein, E. The New Era of Secret Law. – Brennan Center for Justice at New York University School of Law, 18.10.2016.

8. Gorski, A. The Biden Administration's SIGINT Executive Order, Part II: Redress for Unlawful Surveillance, 04.11.2022. Kättesaadav: <https://www.justsecurity.org/83927/the-biden-administrations-sigint-executive-order-part-ii/> (19.04.2023).
9. Hamilton, D.S., Quinlan, J-P. The Transatlantic Economy 2023: Annual Survey of Jobs, Trade and Investment between the United States and Europe. Washington, DC: Foreign Policy Institute, Johns Hopkins University SAIS/Transatlantic Leadership Network, 2023. Jobs, Trade and Investment between the United States and Europe. Kättesaadav: <https://transatlanticrelations.org/wp-content/uploads/2023/03/Transatlantic-Economy-Report-2023.pdf> (19.04.2023).
10. Jaycox, M. M. No Oversight, No Limits, No Worries: Primer on Presidential Spying and Executive Order 12,333. – Harvard National Security Journal, 2021/12(1). Kättesaadav: <https://heinonline.org/HOL/P?h=hein.journals/harvardnsj12&i=59> (13.02.2023).
11. Johnson, C., Liu, Y. What's in Biden's Executive Order on Signals Intelligence? – Lawfare, 14.10.2022. Kättesaadav: <https://www.lawfareblog.com/whats-bidens-executive-order-signals-intelligence> (20.04.2023).
12. Kerr, O.S., A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending it. 72 George Washington Law Review 1208 (2004). Kättesaadav: <https://ssrn.com/abstract=421860> (23.04.2023).
13. Kivimaa, C. Euroopa Komisjoni rakendusotsuse (EL) 2016/1250 kehtivust mõjutavad olulised arengud USA ja Euroopa Liidu õiguses. Magistritöö – Tartu: Tartu Ülikool, 2017.
14. Korff, D. The inadequacy of the US Executive Order on Enhancing Safeguards For US Signals Intelligence Activities, november 2022. Kättesaadav: <https://www.ianbrown.tech/2022/11/11/the-inadequacy-of-the-us-executive-order-on-enhancing-safeguards-for-us-signals-intelligence-activities/> (20.04.2023).
15. Lawne, R. EO 14086 and the EU-U.S. Data Privacy Framework. Fieldfisher, 22.11.2022. Kättesaadav: <https://www.fieldfisher.com/en/insights/eo-14086-and-the-eu-us-data-privacy-framework> (24.04.2023).
16. Linebaugh, C.D., Liu, E.C. EU Data Transfer Requirements and U.S. Intelligence Laws: Understanding Schrems II and Its Impact on the EU-U.S. Privacy Shield. Congressional

- Research Service, 17.03.2021/R46724. Kättesaadav: <https://sgp.fas.org/crs/row/R46724.pdf> (20.04.2023).
17. Machtiger, P. G. Fixing PPD-28: Implementation Issues and Proposed Revisions for Privacy Protections in Signals Intelligence. – New York University Journal of Legislation and Public Policy 2020/23(1). Kättesaadav: <https://heinonline.org/HOL/P?h=hein.journals/nyulpp23&i=233> (14.02.2023).
18. Margulies, P. Adjudicating Algorithms: Accountability in Regulation of Surveillance, Privacy, and Discrimination. Roger Williams University School of Law Legal Studies Paper, 01.2023. No. 216. Kättesaadav: <https://ssrn.com/abstract=4375080> (20.04.2023).
19. Margulies, P. Searching for Accountability Under FISA: Internal Separation of Powers and Surveillance Law. – Marquette Law Review 2021/104. Kättesaadav: <https://scholarship.law.marquette.edu/mulr/vol104/iss4/6/> (12.02.2023).
20. Medine, D jt. Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act. Privacy and Civil Liberties Oversight Board, 02.07.2014. Kättesaadav: <https://irp.fas.org/offdocs/pclob-702.pdf> (20.04.2023).
21. Nielsen, N. Hundreds of US companies make false data protection claims. – EUObserver, 08.10.2013. Kättesaadav: <https://euobserver.com/rule-of-law/121695> (19.04.2023).
22. Rubinstein, I., Margulies, P. Risk and Rights in Transatlantic Data Transfers: EU Privacy Law, U.S. Surveillance, and the Search for Common Ground. – Connecticut Law Review 2022/54(2).
23. Schasmin, P. Privaatsusõiguse piiramise õiguslik raamistik Euroopa Inimõiguste Kohtu ning Euroopa Kohtu lahendite alusel. Magistritöö. – Tallinn: Tartu Ülikool, 2016.
24. Sehver, K.H. Privaatsusõiguse riive proportsionaalsuse hindamise kriteeriumid Euroopa Liidu õiguses elektroonilise side andmete kaitse valdkonna näitel. Magistritöö. – Tallinn: Tartu Ülikool, 2017.
25. Zachary S., Heck, A. A Litigator's Primer on European Union and American Privacy Laws and Regulations, 44 LITIG, 2018. (viidatud: Brown, I., Korff, D. Exchanges of Personal Data After the Schrems II Judgment. Study for the European Parliament's Committee on Civil Liberties).

26. Weiss, M.A., Archick, K. U.S.-EU Data Privacy: From Safe Harbor to Privacy Shield. Congressional Research Service, 19.05.2016/R44257. Kättesaadav: <https://sgp.fas.org/crs/misc/R44257.pdf> (19.04.2023).

Kasutatud õigusaktid

Kasutatud Euroopa Liidu õigusaktid

27. Euroopa Komisjoni otsus, 26. juuli 2000, vastavalt Euroopa Parlamendi ja nõukogu direktiivile 95/46/EÜ piisava kaitse kohta, mis on ette nähtud programmi Safe Harbor põhimõtetega ja sellega seotud korduma kippuvate küsimustega, mille on välja andnud Ameerika Ühendriikide kaubandusministeerium; 2000/520/EÜ. – ELT L 215/7, 25.08.2000, lk 119-138.
28. Euroopa Komisjoni rakendusotsus (EL) 2016/1250, 12. juuli 2016, isikuandmete kaitse piisavuse kohta ELi-USA andmekaitseraamistikus Privacy Shield vastavalt Euroopa Parlamendi ja nõukogu direktiivile 95/46/EÜ – ELT L 207, 01.08.2016, lk 1-112.
29. Euroopa Liidu toimimise lepingu konsolideeritud versioonid (2016/C 202/01). – ELT C 202, 07.06.2016, lk 1-388.
30. Euroopa Liidu põhiõiguste harta – ELT C 326. 26. oktoober 2012, lk 391-407.
31. Euroopa Parlamendi ja nõukogu 24.10.1995. a direktiiv 95/46/EÜ üksikisikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise kohta – ELT L 281, 23.11.1995, lk 31-50.
32. Euroopa Parlamendi ja nõukogu 24.10.1995. a direktiiv 95/46/EÜ üksikisikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise kohta; ELT L 281, 23.11.1995, lk 31-50.
33. Euroopa Parlamendi ja nõukogu direktiiv (EL) 2016/680, 27. aprill 2016, mis käsitleb füüsiliste isikute kaitset seoses pädevates asutustes isikuandmete töötlemisega süütegude tõkestamise, uurimise, avastamise ja nende eest vastutusele võtmise või kriminaalkaristuste täitmisele pööramise eesmärgil ning selliste andmete vaba liikumist ning millega tunnistatakse kehtetuks nõukogu raamotsus 2008/977/JSK. – L 119/89, 04.05.2016, lk 1-43.

34. Euroopa Parlamendi ja nõukogu määrus (EL) 2016/679, 27. aprill 2016, füüsiliste isikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise ning direktiiv 95/46/EÜ kehtetuks tunnistamise kohta – ELT L 119/1, 04.05.2016, lk 1-88.
35. Lissaboni leping, millega muudetakse Euroopa Liidu lepingut ja Euroopa Ühenduseasutamislepingut – ELT C 306, 17.12.2007, lk 1-271.

Muud õigusaktid

36. Euroopa inimõiguste ja põhivabaduste kaitse konventsioon. Euroopa Nõukogu, 4.11.1950. – RT II 2010, 14, 54.

USA õigusaktid

37. Article Three of the United States Constitution. Kättesaadav: <https://constitution.congress.gov/browse/article-3/> (22.04.2023).
38. Attorney General Order No. 5517-2022, 10.14.2022. Kättesaadav: <https://www.federalregister.gov/documents/2022/10/14/2022-22234/data-protection-review-court> (20.04.2023).
39. California Consumer Privacy Act of 2018 (CCPA). Kättesaadav: <https://oag.ca.gov/privacy/ccpa> (20.04.2023).
40. California Privacy Rights Act of 2020 (CPRA). Kättesaadav: <https://www.caprivacy.org/cpra-text/> (20.04.2023).
41. Executive Order 12333. United States Intelligence Activities. Kättesaadav: <https://www.archives.gov/federal-register/codification/executive-order/12333.html> (20.04.2023).
42. Executive Order 13782. Revocation of Federal Contracting Executive Orders, 27.03.2017. Kättesaadav: <https://www.govinfo.gov/content/pkg/DCPD-201700200/pdf/DCPD-201700200.pdf> (20.04.2023).
43. Executive Order 14086. Enhancing Safeguards for United States Signals Intelligence Activities. Kättesaadav: <https://www.presidency.ucsb.edu/documents/executive-order-14086-enhancing-safeguards-for-united-states-signals-intelligence> (20.04.2023).
44. FISA Amendments Act of 2008. Kättesaadav: <https://www.congress.gov/bill/110th-congress/house-bill/6304/text> (19.04.2023).

45. Presidential Policy Directive 28 regarding signals intelligence activities. Kättesaadav: <https://obamawhitehouse.archives.gov/the-press-office/2014/01/17/presidential-policy-directive-signals-intelligence-activities> (20.04.2023).
46. Stored Communications Act (SCA, codified at 18 U.S.C. Chapter 121 §§ 2701–2712). Kättesaadav: <https://www.law.cornell.edu/uscode/text/18/part-I/chapter-121> (20.04.2023).
47. The Fourth Amendment (Amendment IV) to the United States Constitution. Kättesaadav: <https://constitution.congress.gov/constitution/amendment-4/> (21.04.2023).

Kohtupraktika

Euroopa Inimõiguste Kohtu lahendid

48. EIKo 5029/71, *Klass and Others vs Germany*.
49. EIKo 8691/79, *Malone vs the United Kingdom*.
50. EIKo 35252/08, *Centrum för Rättvisa vs Sweden*.
51. EIKo 47143/06, *Roman Zakharov vs Russia*.
52. EIKo 54934/00, *Weber and Saravia vs Germany*.
53. EIKo 58170/13, 62322/14, 24960/15, *Big Brother Watch and Others vs the United Kingdom*.
54. EIKo 58243/00, *Liberty and Others vs the United Kingdom*.

Euroopa Kohtu lahendid

55. EKo C-132/20, *BN and Others vs Getin Noble Bank S.A.* ECLI:EU:C:2022:235.
56. EKo C-175/11, *H. I. D. and B. A. vs Refugee Applications Commissioner and Others*, ECLI:EU:C:2013:45.
57. EKo C-311/18, *Data Protection Commissioner vs Facebook Ireland Limited and Maximillian Schrems*, ECLI:EU:C:2020:559.
58. EKo C-362/14, *Maximillian Schrems vs Data Protection Commissioner*, ECLI:EU:C:2015:650.
59. EKo C-487/19, *W.Ż.*, ECLI:EU:C:2021:798.

60. EKo liidetud kohtuasjad C-511/18, C-512/18 ja C-520/18, *La Quadrature du Net and Others vs Premier ministre and Others*, ECLI:EU:C:2020:791.
61. EKo liidetud kohtuasjad C-584/10 P, C-593/10 P ja C-595/10 P, *European Commission and Others vs Yassin Abdullah Kadi*, ECLI:EU:C:2013:518.
62. EKo C-619/18, *European Commission vs Republic of Poland*, ECLI:EU:C:2019:531.
63. EKo C-623/17, *Privacy International vs Secretary of State for Foreign and Commonwealth Affairs and Others*, ECLI:EU:C:2020:790.
64. EKo C-682/15, *Berlioz Investment Fund SA vs Directeur de l'administration des contributions directes*, ECLI:EU:C:2017:373.

USA kohtute lahendid

65. *City of Cleburne vs Cleburne Independent Living Center*, 473 U.S. 432 (1985). Kättesaadav: <https://www.law.cornell.edu/supremecourt/text/473/432> (20.04.2023).
66. *Motor Vehicle Manufacturers Association of the United States, Inc. vs State Farm Mutual Automobile Insurance Company*, 463 U.S. 29 (1983). Kättesaadav: <https://supreme.justia.com/cases/federal/us/463/29/#tab-opinion-1955213> (21.04.2023).
67. *Paquete Habana vs United States*, 175 U.S. 677, 700 (1900). Kättesaadav: <https://supreme.justia.com/cases/federal/us/175/677/> (20.04.2023).
68. *Spokeo, Inc. vs Robins*, 578 U.S. 330 (2016). Kättesaadav: <https://supreme.justia.com/cases/federal/us/578/13-1339/> (22.04.2023).
69. *TransUnion LLC vs Ramirez*, 41 S. Ct. 2190 (2021). Kättesaadav: https://www.supremecourt.gov/opinions/20pdf/20-297_4g25.pdf (22.04.2023).
70. *United States vs Hasbajrami*, 945 F.3d 641 (2d Cir. 2019). Kättesaadav: <https://casetext.com/case/united-states-v-hasbajrami-2> (19.04.2023).
71. *United States vs Verdugo-Urquidez*, 494 U.S. 259 (1990). Kättesaadav: <https://caselaw.findlaw.com/court/us-supreme-court/494/259.html> (21.04.2023).

Muud kasutatud materjalid

72. Artikkel 29 töörihm. Töödokument WP 114, 25.11.2005. Kättesaadav: <https://ec.europa.eu/newsroom/article29/items/614108> (19.04.2023).

73. Digital Europe koduleht. Schrems 2 data transfers survey: 85% of companies in Europe use standard contractual clauses. <https://www.digitaleurope.org/news/schrems-2-data-transfers-survey-85-of-companies-in-europe-use-standard-contractual-clauses/> (19.04.2023).
74. Euroopa Andmekaitse nõukogu. Opinion 5/2023 on the European Commission Draft Implementing Decision on the adequate protection of personal data under the EU-US Data Privacy Framework. Kättesaadav: https://edpb.europa.eu/our-work-tools/our-documents/opinion-art-70/opinion-52023-european-commission-draft-implementing_en (20.04.2023).
75. Euroopa Andmekaitse nõukogu. Soovitused 02/2020 Euroopa oluliste tagatiste kohta jälgimismeetmete kontekstis, 10.11.2020. Kättesaadav: https://edpb.europa.eu/sites/default/files/files/file1/edpb_recommendations_202002_european_essential_guarantees_surveillance_et.pdf (20.04.2023).
76. Euroopa Andmekaitse nõukogu. Endorsement of GDPR WP29 guidelines by the EDPB, 25.05.2018. Kättesaadav: https://edpb.europa.eu/news/news/2018/endorsement-gdpr-wp29-guidelines-edpb_en (20.04.2023).
77. Euroopa Andmekaitse nõukogu. Suunised 2/2018 määruse 2016/679 artiklis 49 sätestatud erandite kohta, 25. 05. 2018. Kättesaadav: https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_2_2018_derogations_et.pdf (19.04.2023).
78. European Union Agency for Fundamental Rights. Surveillance by intelligence services: fundamental rights safeguards and remedies in the EU. Volume II: field perspectives and legal update, 2017. Kättesaadav: https://fra.europa.eu/sites/default/files/fra_uploads/fra-2017-surveillance-intelligence-services-vol-2_en.pdf (20.04.2023).
79. Euroopa Komisjon. Draft Commission Implementing Decision pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate level of protection of personal data under the EU-US Data Privacy Framework, 13.12.2022. Kättesaadav: https://commission.europa.eu/document/e5a39b3c-6e7c-4c89-9dc7-016d719e3d12_en (20.04.2023).
80. Euroopa Komisjoni koduleht. Adequacy decisions. Kättesaadav: https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en (19.04.2023).

81. EKo C-311/18, Data Protection Commissioner vs Facebook Ireland Limited and Maximillian Schrems, ECLI:EU:C:2020:559, kohtujurist H. Saugmandsgaard Øe ettepanek.
82. Euroopa Komisjoni pressiteade. European Commission calls on the U.S. to restore trust in EU-U.S. data flows. Kättesaadav: https://ec.europa.eu/commission/presscorner/detail/en/IP_13_1166 (20.04.2023).
83. Euroopa Komisjoni pressiteade. Questions & Answers: EU-U.S. Data Privacy Framework, draft adequacy decision, 13.12.2022. Kättesaadav: https://ec.europa.eu/commission/presscorner/detail/en/qanda_22_7632 (23.04.2023).
84. Euroopa Parlamendi 12.03.2014 vastu võetud resolutsioon USA Riikliku Julgeolekuagentuuri jälgimisprogrammi ja ELi liikmesriikide jälgimisasutuste ning nende mõju kohta ELi kodanike põhiõigustele ja Atlandi-ülesele koostööle justiits- ja siseküsimustes (2013/2188(INI)). Kättesaadav: https://www.europarl.europa.eu/doceo/document/TA-7-2014-0230_ET.html (21.04.2023).
85. France, Council of State (Conseil d'Etat), M. A.B., No. 396669, 05.05.2017. (viidatud: European Union Agency for Fundamental Rights. Surveillance by intelligence services: fundamental rights safeguards and remedies in the EU. Volume II: field perspectives and legal update, 2017.
86. Greenwald, G.E jt. Edward Snowden: the whistleblower behind the NSA surveillance revelations. The Guardian, 11.06.2013. Kättesaadav: <https://www.theguardian.com/world/2013/jun/09/edward-snowden-nsa-whistleblower-surveillance> (23.04.2023).
87. Greenwald, G.E., MacAskill, E. NSA Prism program taps in to user data of Apple, Google and others. The Guardian, 07.06.2013. Kättesaadav: <https://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data> (19.04.2023).
88. Office of the Director of National Intelligence. Annual Threat Assessment of the US Intelligence Community, 09.04.2023. Kättesaadav: <https://www.dni.gov/files/ODNI/documents/assessments/ATA-2021-Unclassified-Report.pdf> (25.04.2023).

89. Schrems, M. First reaction: Executive Order on US Surveillance unlikely to satisfy EU law. NOYB – European Center for Digital Rights, 07.10.2022. Kättesaadav: <https://noyb.eu/en/new-us-executive-order-unlikely-satisfy-eu-law> (19.04.2023).
90. Shear, S. Meta says it may shut down Facebook and Instagram in Europe over data-sharing dispute. CNBC, 07.02.2022. Kättesaadav: <https://www.cnn.com/2022/02/07/meta-threatens-to-shut-down-facebook-and-instagram-in-europe.html> (23.04.2023).
91. The *ad hoc* EU-US Working Group on Data Protection. Report on the findings by the EU Co-chairs of the *ad hoc* EU-US Working Group on Data Protection, 27.11.2013. Kättesaadav: <https://data.consilium.europa.eu/doc/document/ST-16987-2013-INIT/en/pdf> (21.04.2023).
92. The Hamburg Commissioner for Data Protection and Freedom of Information. Data protection in the USA – current situation, 29.11.2022. Kättesaadav: https://datenschutz-hamburg.de/assets/pdf/2022-11-29_Information_Executive_Order.pdf (20.04.2023).
93. The International Association of Privacy Professionals. US State Privacy Legislation Tracker. Kättesaadav: <https://iapp.org/resources/article/us-state-privacy-legislation-tracker/> (19.04.2023)
94. The National Security Agency. Signals Intelligence (SIGINT) Overview. Kättesaadav: <https://www.nsa.gov/Signals-Intelligence/Overview/> (24.04.2023).
95. The White House. FACT SHEET: President Biden Signs Executive Order to Implement the European Union-U.S. Data Privacy Framework. Kättesaadav: <https://www.whitehouse.gov/briefing-room/statements-releases/2022/10/07/fact-sheet-president-biden-signs-executive-order-to-implement-the-european-union-u-s-data-privacy-framework/> (23.04.2023).
96. The White House. Press Release of the Office of the Press Secretary. Presidential Policy Directive Signals Intelligence Activities (PPD-28). Kättesaadav: <https://obamawhitehouse.archives.gov/the-press-office/2014/01/17/presidential-policy-directive-signals-intelligence-activities> (15.02.2023).
97. The White House. Press Release of the Office of the Press Secretary. Remarks by the President on Review of Signals Intelligence. Kättesaadav: <https://obamawhitehouse.archives.gov/the-press-office/2014/01/17/remarks-president-review-signals-intelligence> (15.02.2023).

98. USA justiitsministeeriumi õigusbüroo seisukoht. Legal Effectiveness of a Presidential Directive, as Compared to an Executive Order; 29.01.2000. Kättesaadav: <https://www.justice.gov/olc/opinion/legal-effectiveness-presidential-directive-compared-executive-order> (15.02.2023).
99. USA saatkonna koduleht. States of the Union. Kättesaadav: <https://uk.usembassy.gov/states-of-the-union-states-of-the-u-s/> (19.04.2023).
100. World of Meter koduleht. How many countries are there in the world? Kättesaadav: <https://www.worldometers.info/geography/how-many-countries-are-there-in-the-world/> (19.04.2023).