EUROOPA
KOMISJON

Brüssel, 9.10.2024
COM(2024) 451 final

KOMISJONI ARUANNE EUROOPA PARLAMENDILE JA NÕUKOGULE

ELi-USA andmekaitseraamistikku käsitleva kaitse piisavuse otsuse toimimise esimese perioodilise läbivaatamise kohta

1. ESIMENE PERIOODILINE LÄBIVAATAMINE – TAUST, ETTEVALMISTUS JA PROTSESS

Komisjon leidis oma 10. juuli 2023. aasta otsuses (edaspidi „kaitse piisavuse otsus“), et ELi-USA andmekaitseraamistik (edaspidi „andmekaitseraamistik“) tagab Euroopa Liidust Ameerika Ühendriikides asuvatele organisatsioonidele edastatavatele isikuandmetele piisava kaitsetaseme[1]. Kaitse piisavuse otsuse kohaselt peab komisjon tegema perioodilisi läbivaatamisi, millest esimene peaks toimuma siis, kui liikmesriikidele kaitse piisavuse otsusest teatamise kuupäevast on möödunud üks aasta. Käesolevas aruandes võetakse kokku esimese läbivaatamise tulemused.

Nagu on nõutud kaitse piisavuse otsuse põhjenduses 211, kontrolliti pärast uue raamistiku esimest kohaldamisaastat toimunud esimesel läbivaatamisel seda, kas kõik raamistikus ette nähtud elemendid on rakendatud ja kas need toimivad tõhusalt. Läbivaatamine hõlmas raamistiku toimimise kõiki aspekte, sealhulgas pärast kaitse piisavuse otsuse vastuvõtmist toimunud õiguslikke muudatusi.

Läbivaatamise ettevalmistamise käigus kogus komisjon teavet asjaomastelt sidusrühmadelt, eelkõige valitsusvälistelt organisatsioonidelt, kellel on eksperditeadmised digitaalõiguste ja eraelu puutumatuse valdkonnas,[2] andmekaitseraamistiku kohaselt kinnitatud organisatsioonidelt nende kutseorganisatsioonide[3] kaudu ning raamistiku rakendamises osalevatelt USA ametiasutustelt. Lisaks on komisjon kogunud tagasisidet üldsuselt konkreetse tagasisidekorje kaudu portaalis „Avaldage arvamust!“[4].

Läbivaatamiskoosolek toimus 18.–19. juulil 2024 Washingtonis. Selle avasid ELi õigus- ja tarbijaküsimuste volinik Didier Reynders ja USA kaubandusminister Gina Raimondo[5].

ELi puhul viisid läbivaatamise ellu Euroopa Komisjoni õigus- ja tarbijaküsimuste peadirektoraadi esindajad koos Euroopa Andmekaitsenõukogu määratud viie esindajaga, kes

[1] Komisjoni 10. juuli 2023. aasta rakendusotsus (EL) 2023/1795, mis põhineb Euroopa Parlamendi ja nõukogu määrusel (EL) 2016/679 ning käsitleb isikuandmete kaitse taseme piisavust ELi-USA andmekaitseraamistiku alusel.

[2] Komisjon saatis küsimustiku üheksale valitsusvälisele organisatsioonile (Human Rights Watch, American Civil Liberties Union, Consumer Federation of America, Centre for Digital Democracy, New America Open Technology Institute, Access Now, Electronic Frontier Foundation, Electronic Privacy Information Center, Centre for Democracy and Technology), keskendudes USA õigusraamistiku, järelevalve- ja täitmise tagamise mehhanismide asjaomastele muudatustele ning õiguskaitsemehhanismide toimimisele. 9. juulil 2024 toimus ka komisjoni talituste ja Euroopa Andmekaitsenõukogu esindajate ning nende valitsusväliste organisatsioonide veebikohtumine.

[3] Komisjon saatis küsimustiku üheksale kutseorganisatsioonile (Software & Information Industry Association, U.S. Chamber of Commerce, Information Technology Industry Council, the Software Alliance, Centre for Information Policy Leadership, Interactive Advertising Bureau, United States Council for International Business, Computer and Communications Industry Association, Engine), keskendudes andmekaitseraamistiku kohaselt kinnitatud ettevõtjate kogemustele, eelkõige kinnitamise protsessile, andmekaitseraamistiku põhimõtete järgimiseks astutud sammudele, üksikisikute taotluste ja kaebuste menetlemise mehhanismidele jne.

[4] Saadud tagasiside on kättesaadav järgmise lingi kaudu: https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/14379-EU-US-Data-Privacy-Framework-report-of-the-Commission-on-how-the-framework-is-functioning_et.

[5] Läbivaatamiskoosolek korraldati teemade kaupa ning iga päevakorrapunkti tutvustas lühiettekandega asjaomane USA ametiasutus, ELi esindaja või organisatsioon. Lühitutvustusele järgnes üksikasjalik küsimuste ja vastuste voor. Raamistiku kaubandusaspekte (st andmekaitseraamistiku kohaselt kinnitatud ettevõtjate suhtes kehtivate nõuete kohaldamine ja täitmise tagamine) käsitleti esimesel päeval, teisel päeval aga arutati küsimusi, mis on seotud valitsuse juurdepääsuga isikuandmetele.

esindasid erinevaid riiklikke andmekaitseasutusi ja Euroopa Andmekaitseinspektorit[6]. USA poolel osalesid kaubandusministeeriumi (Department of Commerce), välisministeeriumi (Department of State), föderaalse kaubanduskomisjoni (Federal Trade Commission), transpordiministeeriumi (Department of Transportation), riikliku luurejuhi büroo (Office of the Director of National Intelligence), justiitsministeeriumi (Department of Justice), luureühenduse peainspektori (Inspector General for the Intelligence Community) ning eraelu puutumatuse ja kodanikuvabaduste järelevalve komisjoni (Privacy and Civil Liberties Oversight Board) liikmed. Lisaks andsid asjakohastel läbivaatamisistungitel teavet vaidluste lahendamise teenuseid pakkuvate sõltumatute organisatsioonide ja Ameerika vahekohtute assotsiatsiooni (American Arbitration Association) esindajad. Läbivaatamisel kasutati ka andmekaitseraamistiku kohaselt kinnitatud organisatsioonide ettekandeid selle kohta, kuidas ettevõtjad täidavad raamistiku nõudeid.

Komisjon tugines järelduste tegemisel lisaks teabele, mis on pärit avalikkusele kättesaadavatest materjalidest, nagu kohtuotsused, asjaomaste USA ametiasutuste rakenduseeskirjad ja menetlused, valitsusväliste organisatsioonide aruanded ja uuringud, andmekaitseraamistiku kohaselt kinnitatud ettevõtjate läbipaistvusaruanded, sõltumatute järelevalveasutuste aastaaruanded ning ajakirjanduses ilmunud artiklid.

2. TÄHELEPANEKUD

2.1. Kaubandusaspektid

2.1.1. Kinnitamise protsess

Selleks et USA ettevõtja saaks andmekaitseraamistiku alusel EList edastatud isikuandmeid vastu võtta, peab ta kaubandusministeeriumile kinnitama ja seejärel igal aastal uuesti kinnitama, et ta järgib teatavaid andmekaitsenõudeid (edaspidi „andmekaitseraamistiku põhimõtted“). Kinnitamine eeldab, et ettevõtja suhtes kohaldatakse föderaalse kaubanduskomisjoni või transpordiministeeriumi volitusi uurimise läbiviimiseks ja nõuete täitmise tagamiseks ning et ta kinnitab avalikult oma kohustust järgida andmekaitseraamistiku põhimõtteid ning avalikustab oma privaatsustingimused ja rakendab neid täielikult[7]. Enne kinnitamise lõpuleviimist kontrollib kaubandusministeerium, kas ettevõtja vastab kõigile kinnitamise nõuetele[8].

Läbivaatamiskoosolekul selgitas kaubandusministeerium, et andmekaitseraamistiku esimesel aastal on keskendutud kinnitamisprotsessi kehtestamisele, sealhulgas spetsiaalsete IT-vahendite väljatöötamisele, menetluste ajakohastamisele, ettevõtjatega suhtlemisele ning muule teavitus- või teadlikkuse suurendamise tegevusele. Läbivaatamiskoosoleku kuupäeva seisuga on andmekaitseraamistiku kohase kinnituse saanud enam kui 2 800 ettevõtjat. See tähendab, et andmekaitseraamistiku esimesel kohaldamisaastal on kinnituse saanud rohkem ettevõtjaid kui eelmise raamistiku Privacy Shield raames[9]. Kaubandusministeeriumi esitatud teabe kohaselt on 70 % osalejatest VKEd ning suur osa andmekaitseraamistiku põhimõtete järgimist kinnitanud ettevõtjatest (47 %) tegutsevad info- ja kommunikatsioonitehnoloogia

[6] Komisjoni ja Euroopa Andmekaitsenõukogu esindajad kohtusid 12. juunil ja 10. juulil 2024, et valmistuda läbivaatamiseks, arutada saadud teavet ja teha kindlaks, milliste aspektide kohta tuleb koguda veel teavet ja milliseid tuleb täiendavalt selgitada.

[7] Kaitse piisavuse otsuse I lisa I jao punkt 2.

[8] Kaitse piisavuse otsuse III lisa.

[9] Samal ajavahemikul oli raamistiku Privacy Shield alusel saanud kinnituse 2 400 ettevõtjat.

(IKT) sektoris. Lisaks on 60 % ettevõtjatest saanud kinnituse üksnes muude kui personaliandmete jaoks, 2,5 % ettevõtjatest on saanud kinnituse üksnes personaliandmete jaoks ning 37,5 % nii personaliandmete kui ka muude andmete jaoks.

Kaubandusministeerium on võtnud vastu ettevõtjate taotluste menetlemiseks vajaliku korra. Ettevõtjad peavad esitama oma taotlused kinnituse saamiseks kaubandusministeeriumi andmekaitseraamistiku veebisaidil (https://www.dataprivacyframework.gov/). See sisaldab teavet selle kohta, kuidas andmekaitseraamistikuga ühineda[10] ja millised on ettevõtja kohustused raamistiku alusel[11]. Kaubandusministeeriumi erimeeskond, mis tegutseb andmekaitseraamistiku direktori vastutusalas, vastutab kõigi andmekaitseraamistiku juhtimise ja haldamisega seotud aspektide eest, sealhulgas kinnitamise protsessi ja nõuetele vastavuse järelevalve eest. Iga taotlus määratakse konkreetsele töötajale, kes tegeleb asjaomase ettevõtjaga kogu kinnitamise protsessi jooksul.

Ettevõtjad esitavad raamistiku alusel kinnituse saamiseks oma taotluse, sealhulgas privaatsustingimuste kavandi. Kaubandusministeerium kontrollib, kas see vastab andmekaitseraamistiku asjakohastele nõuetele. Kui organisatsioonid soovivad saada kinnituse ettevõtjate kontserni eri üksustele (nt tütarettevõtjatele), palub kaubandusministeerium kas ühte terviklikku privaatsustingimusi sisaldavat dokumenti, milles on selgelt märgitud kõik hõlmatud üksused, või iga üksuse jaoks eraldi dokumenti. Kaubandusministeerium kontrollib taotluses märgitud sõltumatu kaebuste menetlemise mehhanismi[12] kaudu ka seda, kas organisatsioon on selles tegelikult registreerunud. Ettevõtjate puhul, kes valivad andmekaitseasutuste kolleegiumi (nt kuna nad töötlevad personaliandmeid), kontrollib kaubandusministeerium, kas ettevõtja on tasunud kolleegiumi teenuste kasutamiseks nõutavad tasud. Vajaduse korral kontrollib kaubandusministeerium ka seda, kas taotleja kuulub föderaalse kaubanduskomisjoni või transpordiministeeriumi jurisdiktsiooni alla (ja tal on seepärast õigus andmekaitseraamistikuga ühineda).

Kui kõik tingimused on täidetud, teatab kaubandusministeerium organisatsioonile, et ta võib oma veebisaidil avaldada privaatsustingimused, milles viidatakse andmekaitseraamistikule. Kui privaatsustingimused on avaldatud, annab kaubandusministeerium põhimõtete järgimisele oma kinnituse ja lisab ettevõtja oma veebisaidil olevasse andmekaitseraamistikuga ühinenute nimekirja. Andmekaitseraamistikule saab EList isikuandmete saamiseks tugineda alates kuupäevast, mil kaubandusministeerium kandis organisatsiooni sellesse nimekirja[13].

Nagu läbivaatamiskoosolekul selgitati, on kaubandusministeeriumi seni tehtud kontrollide tulemusel tagasi lükatud 33 taotlust, sest need ei vastanud andmekaitseraamistiku nõuetele. Üldiselt teeb kaubandusministeerium ettevõtjaga koostööd, et võimalikud puudused kõrvaldada. Kui kaubandusministeerium leiab puudusi, teatab ta ettevõtjale, et need tuleb kõrvaldada, ning kui ettevõtja ei vasta teatava aja jooksul või ei järgi kinnituse esitamisel muul moel kaubandusministeeriumi menetlusi, loetakse ta taotlusest loobunuks. Kui algse kinnitamise protsessi ei ole 12 kuu jooksul lõpule viidud või taotlust muudetud, leiab kaubandusministeerium, et sellest on loobutud.

[10] https://www.dataprivacyframework.gov/program-articles/How-to-Join-the-Data-Privacy-Framework-(DPF)-Program-(part%E2%80%931).

[11] https://www.dataprivacyframework.gov/key-requirements.

[12] Erasektori vaidluste lahendamise mehhanismid, mille abil uuritakse üksikisikute kaebusi ja vaidlusi ning lahendatakse need kiiresti ja üksikisikule tasuta.

[13] Kaitse piisavuse otsuse I lisa I jao punkt 3.

Iga-aastase korduskinnituse tähtaeg on iga ettevõtja puhul kindlaks määratud andmekaitseraamistiku nimekirjas. Selleks et tuletada ettevõtjatele meelde vajadust taotleda korduskinnitust, on kaubandusministeerium loonud süsteemi, mis saadab meeldetuletusi kinnituse aegumise kohta. Organisatsioonid saavad meeldetuletuse üks kuu enne tähtaega, seejärel kaks nädalat enne ja seejärel üks päev enne tähtaega. Ettevõtjad, kes lasevad oma kinnitusel aeguda, kustutatakse andmekaitseraamistiku nimekirjast. Nagu on kirjeldatud kaitse piisavuse otsuse III lisas, on kaubandusministeeriumi veebisaidil eraldi jaotis, milles on loetletud USA organisatsioonid, mis ei ole enam aktiivsed osalejad, ning toodud välja põhjused (nt aegumine või loobumine), miks asjaomased ettevõtjad on nimekirjast kustutatud (edaspidi „endiste osalejate nimekiri“). Kui organisatsioonid eemaldatakse andmekaitseraamistiku nimekirjast selle tõttu, et nad on lasknud oma kinnitusel aeguda, võtab kaubandusministeerium nendega ühendust, et teha kindlaks, kas nad soovivad loobuda või kavatsevad taotleda korduskinnitust, ning kui organisatsioon seda soovib, siis kontrollida, kas nad on aegumise ajal kohaldanud andmekaitseraamistiku alusel saadud isikuandmete suhtes andmekaitseraamistiku põhimõtteid, ning selgitada, milliseid samme nad astuvad, et lahendada probleemid, mille tõttu on nende korduskinnitus edasi lükkunud. Kui ettevõtjad teatavad kaubandusministeeriumile, et nad soovivad andmekaitseraamistikus osalemisest loobuda, küsib kaubandusministeerium, kinnitust selle kohta, kas nad tagastavad või kustutavad andmekaitseraamistiku alusel saadud andmed; säilitavad need ja jätkavad andmekaitseraamistiku põhimõtete kohaldamist selliste andmete suhtes (mida tuleb igal aastal kinnitada) või säilitavad need ja kehtestavad muud kaitsemeetmed (näiteks lepingu tüüptingimused, mille on vastu võtnud Euroopa Komisjon).

Kutseorganisatsioonidelt ja ettevõtjatelt saadud tagasiside näitab, et andmekaitseraamistiku kohaselt kinnitatud ettevõtjad on astunud mitmeid samme, et tagada andmekaitseraamistiku põhimõtete järgimine. Näiteks on organisatsioonid kaebuste menetlemise, nõuete täitmise tagamise ja vastutuse põhimõtte järgimiseks teinud sisekontrolle kas enesehindamise või välise vastavuskontrolli teel. Kahe läbivaatamiskoosolekul osalenud erasektori sõltumatu kaebuste menetlemise mehhanismi kohaselt kasutavad nad ka välist vastavuskontrolli, mille raames vaadatakse läbi eraelu puutumatuse põhimõtted, ning ühe erasektori sõltumatu kaebuste menetlemise mehhanismi kohaselt pakub ta ka auditeid ja pistelisi kontrolle, keskendudes näiteks juurdepääsu, valikuvõimaluse ja edasisaatmise põhimõtetele. Lisaks on kinnituse saanud ettevõtjad välja töötanud asutusesisesed vastavusprogrammid ja järelevalvemehhanismid, koolitanud töötajaid, rakendanud mehhanisme, mis võimaldavad üksikisikutel kasutada oma õigusi, koostanud eraelu puutumatuse mõjuhinnanguid ja vaadanud läbi kehtivad lepingud.

2.1.2. Nõuetele vastavuse järelevalve, osalemise kohta esitatud valeväited ja täitmise tagamine

Andmekaitseraamistiku kohaselt vastutab kaubandusministeerium andmekaitseraamistiku põhimõtetele vastavuse järelevalve eest, milleks ta kasutab mitmesuguseid vahendeid, sealhulgas *ex officio* kontrolle (omal algatusel), *ad hoc* pistelisi kontrolle ja nõuetele vastavuse küsimustikke. See hõlmab raamistikus osalemise kohta esitatud valeväidete kindlakstegemist näiteks internetiotsingute kaudu[14] ja nende suhtes meetmete võtmist.

[14] Vt kaitse piisavuse otsuse III lisa. Valeväited võivad tekkida näiteks siis, kui ettevõtja väidab, et osaleb andmekaitseraamistikus, aga ta kas ei ole kinnitamise protsessi alustanud või on seda alustanud, kuid ei ole lõpetanud või on lasknud oma kinnitusel aeguda.

Selleks et jälgida, kas andmekaitseraamistiku põhimõtete järgimist kinnitanud ettevõtjad järgivad põhimõtteid, on kaubandusministeerium viimase aasta jooksul tuginenud peamiselt *ad hoc* veebiotsingutele ja (sotsiaal)meedia kontrollidele. Kaubandusministeerium teatas, et ta ei ole sel esimesel aastal leidnud andmekaitseraamistiku põhimõtete järgimisel probleeme ega ole andnud ühegi ettevõtjaga seotud juhtumit üle föderaalsele kaubanduskomisjonile või transpordiministeeriumile võimalike täitemeetmete võtmiseks. Samuti on ta loonud spetsiaalse kontaktpunkti, et hõlbustada koostööd andmekaitseasutustega ning võtta üksikisikutelt vastu kaebusi ja teistelt asutustelt (nt andmekaitseasutused või föderaalne kaubanduskomisjon) esildisi. Viimase aasta jooksul ei ole siiski esitatud ühtegi esildist ega kaebust. Kuigi andmekaitseraamistiku esimesel tegevusaastal keskenduti raamistiku loomisele ja kinnitamise protsessile, selgitas kaubandusministeerium läbivaatamiskoosolekul, et ta kavatseb teha vastavuskontrolle automatiseeritud vahenditega, mis võimaldavad teha neid süstemaatilisemalt, ning töötab praegu välja selleks vajalikke IT-vahendeid.

Komisjon tunnistab, et kaubandusministeerium pidi esimesel aastal keskenduma raamistiku loomisele ja kinnitamise protsessile. Edaspidi on oluline, et kaubandusministeerium suurendaks jõupingutusi põhimõtete järgimise järelevalve ja kontrollimise alal, sest see on vajalik raamistiku jätkuva ulatusliku järgimise tagamiseks ja selliste juhtumite avastamiseks (sealhulgas ettevõtjate võimalikud valeväited osalemise kohta), mille jaoks on vaja täiendavaid täitemeetmeid. Sellega seoses tunneb komisjon heameelt, et kaubandusministeerium kinnitas oma kavatsust töötada välja ja kasutada (automatiseeritud) vahendeid, et teha tõhusamalt ja süstemaatilisemalt kindlaks nõuetele vastavusega seotud probleemid ja valeväited, ning on seisukohal, et see peaks olema osa laiemast jõupingutusest kasutada rohkem mitmesuguseid tema käsutuses olevaid vahendeid (nt pistelised kontrollid, vastavuskontrolli küsimustikud, teabenõuded jne), sealhulgas selleks, et kontrollida vastavust andmekaitseraamistiku erinõuetele[15].

Andmekaitseraamistikku kohaldavad organisatsioonid kuuluvad föderaalse kaubanduskomisjoni ja transpordiministeeriumi jurisdiktsiooni alla. Läbivaatamiskoosolekul kinnitas transpordiministeerium, et asjakohaste täitemeetmete võtmiseks on olemas kõik menetlused. Samuti selgitas ta, et andmekaitseraamistikuga on ühinenud väga vähesed tema jurisdiktsiooni alla kuuluvad ettevõtjad (st mõned piletimüügiagendid, kuid mitte ükski lennuettevõtja). Föderaalne kaubanduskomisjon kinnitas, et ta kontrollib kõigis oma eraelu puutumatuse uurimistes süstemaatiliselt andmekaitseraamistiku rikkumisi. Seni ei ole föderaalne kaubanduskomisjon saanud teistelt asutustelt ühtegi esildist. Komisjon on saanud mõned kaebused, kus mainitakse andmekaitseraamistikku, kuid kaks neist käsitlesid endiste osaliste nimekirjas olevaid ettevõtjaid, kaks olid seotud ettevõtjatega, kes ei osalenud raamistikus, ja üks ei puudutanud EList edastatud isikuandmeid. Käesoleva aruande koostamise ajal ei olnud föderaalne kaubanduskomisjon teinud otsuseid andmekaitseraamistiku järgimise tagamiseks, kuid ta kinnitas, et praegu on uurimise all mitu andmekaitseraamistiku kohaselt kinnitatud ettevõtjat.

Komisjon väljendab heameelt selle üle, et föderaalne kaubanduskomisjon kontrollib süstemaatiliselt andmekaitseraamistiku rikkumisi kõigis tema toimetatavates eraelu puutumatuse uurimistes. Kuna andmekaitseraamistiku jätkuv tulemuslikkus sõltub selle usaldusväärsest täitmisest, eeldatakse, et föderaalne kaubanduskomisjon kasutab oma

[15] Näiteks seoses andmete edasisaatmisega, milleks kasutatakse andmekaitseraamistiku 3. põhimõtte punktis b sätestatud võimalust taotleda andmete edasisaatmist käsitleva lepingu asjakohaste eraelu puutumatuse sätete kokkuvõtet või tüüpkoopiat.

raamistikukohaseid uurimisvolitusi, sealhulgas võtab ennetavalt kontrollimeetmeid, mis keskenduvad andmekaitseraamistiku konkreetsete nõuete järgimisele ja/või teatavatele sektoritele.

2.1.3. Kaebuste menetlemine

Andmekaitseraamistik pakub ELi üksikisikutele mitmeid võimalusi midagi ette võtta, kui andmekaitseraamistiku kohaselt kinnitatud organisatsioonid neid põhimõtteid ei järgi[16]. Selle hulka kuulub vaidluste lahendamine otsekontaktide kaudu andmekaitseraamistiku organisatsiooniga, kes peab vastama asjaomasele isikule 45 päeva jooksul. Üksikisikud võivad esitada kaebuse ka sõltumatule kaebuste menetlemise mehhanismile, mille organisatsioon on määranud kaebusi uurima ja lahendama. Olenevalt asjaoludest võib see olla kas alternatiivne vaidluste lahendamise organ või andmekaitseasutus[17]. Kui ükski muu õiguskaitsevahend ei ole andmesubjekti kaebust rahuldavalt lahendanud, võivad üksikisikud viimase abinõuna algatada ELi-USA andmekaitseraamistiku kolleegiumis siduva vahekohtumenetluse.

2.1.3.1. Kaebuste käsitlemine ettevõtjate poolt

Kutseorganisatsioonide ja ettevõtjate vastused komisjoni saadetud küsimustikele näitavad, et andmekaitseraamistiku kohaselt kinnitatud ettevõtjad on saanud andmekaitseraamistiku põhimõtete mittejärgimise asjus üksikisikutelt väga vähe kaebusi või ei ole neid üldse saadud. Samal ajal on ettevõtjad kehtestanud mitmesugused mehhanismid ja vahendid, mis võimaldavad üksikisikutel kasutada oma õigusi ja esitada kaebusi, sealhulgas veebipõhiste vormide, e-posti ja telefoni teel.

2.1.3.2. *Sõltumatud kaebuste menetlemise mehhanismid*

Läbivaatamiskoosolekul saadud tagasiside ja kutseorganisatsioonidelt laekunud teave näitavad, et sõltumatutele kaebuste menetlemise mehhanismidele on esitatud väga vähe kaebusi. Ettevõtjate valitud sõltumatute kaebuste menetlemise mehhanismide hulka kuuluvad BBB riiklikud programmid, JAMS, TRUSTe ja VeraSafe. Andmekaitseraamistiku kohaselt tuleb sõltumatutel kaebuste menetlemise mehhanismidel avaldada aastaaruanne koondstatistikaga nende vaidluste lahendamise teenuste kasutamise kohta. Käesoleva aruande vastuvõtmise ajal olid kõik asjaomased sõltumatud kaebuste menetlemise mehhanismid oma aastaaruande avaldanud[18].

---

[16] Vt kaitse piisavuse otsuse punkt 2.4.

[17] Andmekaitseraamistiku põhimõtete järgimist kinnitanud organisatsioonidel on kohustus andmekaitseasutuse läbiviidaval uurimisel ja kaebuse lahendamisel koostööd teha, kui kaebus on seotud töösuhte raames kogutud personaliandmete töötlemisega või kui nad on vabatahtlikult nõustunud järelevalveasutuste järelevalvele alluma.

[18] ANA – https://www.ana.net/content/show/id/accountability-dpf-consumers;
BBB National Programs – https://assets.bbbprograms.org/docs/default-source/eu-privacy-shield/dpf_periodicalreport_072024.pdf; ICDR – AAA – https://go.adr.org/rs/294-SFS-516/images/Data%20Privacy%20Framework%20IRM%20Program%20Report%202023-2024%20FINAL.pdf?version=0;
Insights Association – https://www.insightsassociation.org/Portals/INSIGHTS/Insights%20Association%20DPF%20Services%20Program%202024%20Annual%20Report_Final_1.pdf;
JAMS – https://www.jamsadr.com/files/Uploads/Documents/2024-Annual-Report-DPF-Cases.pdf;
Privacy Trust DPF Services – https://privacytrust.com/fserve/PrivacyTrust_Dispute_Resolution_Report_2023_2024.pdf;
TRUSTe Dispute Resolution – https://trustarc.com/wp-content/uploads/2024/07/2024-Independent-Recourse-Mechanism-Annual-Report.pdf;

Lisaks tutvustasid BBB ja VeraSafe läbivaatamiskoosolekul üksikasjalikult oma eelmise aasta tegevust. Nad teatasid, et nende teenuseid valinud ettevõtjate arv on võrreldes varasemate raamistikega suurenenud ning märkisid, et nad on saanud mõned kaebused, millest enamik ei olnud siiski vastuvõetavad. Näiteks sai BBB ELi üksikisikutelt 87 kaebust, millest ainult kaks vastasid vaidluste lahendamise mehhanismi tingimustele. Kuigi BBB selgitas, et kaebusi menetletakse keskmiselt viie tööpäeva jooksul, lõpetati need kaks kaebust, sest üksikisikud jätsid vastamata. VeraSafe sai 26 kaebust, millest kuus vastasid vaidluste lahendamise mehhanismi tingimustele. Neist kaks, mis käsitlesid juurdepääsu- ja kustutamistaotlusi, lahendati, kaks on endiselt pooleli ning kahest kas loobuti või menetlus lõpetati üksikisiku vastuse puudumise tõttu. Mõlema sõltumatu kaebuste menetlemise mehhanismi kohaselt püüdsid nad vastata kaebustele keeles, milles isik nende poole pöördus.

Andmekaitseraamistiku põhimõtete järgimist kinnitanud ettevõtjad, kes töötlevad EList edastatud personaliandmeid, peavad nende andmete puhul valima oma sõltumatuks kaebuste menetlemise mehhanismiks ELi andmekaitseasutused, seevastu andmekaitseraamistikule tuginedes muud liiki isikuandmete edastamisel võib andmekaitseraamistiku põhimõtete järgimist kinnitanud ettevõtja valida ELi andmekaitseasutused oma sõltumatuks kaebuste menetlemise mehhanismiks vabatahtlikult. Tegelikult valis üle poole andmekaitseraamistiku kohaselt kinnitatud ettevõtjatest läbivaatamise ajal selle lahenduse[19] ja see on tervitatav. Pärast kaitse piisavuse otsuse vastuvõtmist on Euroopa Andmekaitsenõukogu võtnud vastu ELi andmekaitseasutuste mitteametliku kolleegiumi kodukorra. Kolleegium on pädev andma USA organisatsioonidele siduvat nõu, kui üksikisiku kaebus EList edastatud isikuandmete töötlemise kohta andmekaitseraamistiku alusel on jäänud lahendamata. Kolleegiumi moodustavad kodukorra kohaselt üks andmekaitseasutus, kes tegutseb juhtiva andmekaitseasutusena, ja koos teiste andmekaitseasutustega, mis on määratud kaasläbivaatajateks[20]. Ta annab siduvat nõu 60 päeva jooksul alates andmekaitseraamistiku alusel esitatud kaebuse saamisest. Euroopa Andmekaitsenõukogu on avaldanud ka kaebuse vormi,[21] mida kasutada andmekaitseasutustele kaebuste esitamiseks, ning „Euroopa üksikisikute korduma kippuvad küsimused“[22] ja „Ettevõtjate korduma kippuvad küsimused“[23] andmekaitseraamistiku kohta. Kolleegium ei olnud läbivaatamise ajal kaebusi saanud.

2.1.3.3. Siduv vahekohtumenetlus

Kaubandusministeerium valis siduva vahekohtumenetluse haldamiseks välja vaidluste lahendamise rahvusvahelise keskuse (International Centre for Dispute Resolution), mis on USA vahekohtute assotsiatsiooni (American Arbitration Association) rahvusvaheline osakond. Pärast kaitse piisavuse otsuse vastuvõtmist valis kaubandusministeerium koos komisjoniga

---

Verasafe – https://verasafe.com/wp-content/uploads/2020/06/VeraSafe-DPF-Dispute-Resolution-Program-Annual-Report-2024.pdf.

[19] Veidi pärast läbivaatamiskoosolekut märgiti andmekaitseraamistiku veebisaidil, et 2 892 osalejast 1 511 on oma kaebuste menetlemise mehhanismiks valinud mõne ELi andmekaitseasutuse.

[20] Euroopa Andmekaitsenõukogu võttis 17. aprillil 2024 vastu ELi-USA andmekaitseraamistiku kohase ELi andmekaitseasutuste mitteametliku kolleegiumi töökorra. See on kättesaadav siin: https://www.edpb.europa.eu/system/files/2024-04/dpf_rules-of-procedure_informal-panel-dpas_en.pdf.

[21] https://www.edpb.europa.eu/our-work-tools/our-documents/other-guidance/eu-us-data-privacy-framework-template-complaint-form_en.

[22] https://www.edpb.europa.eu/our-work-tools/our-documents/other-guidance/eu-us-data-privacy-framework-faq-european-individuals_en.

[23] https://www.edpb.europa.eu/our-work-tools/our-documents/other-guidance/eu-us-data-privacy-framework-faq-european-businesses_en.

välja 11 vahekohtunikku, kellel on kogemusi eraelu puutumatuse valdkonnas ja erinev taust (sealhulgas vahekohtusüsteem, kohtusüsteem, akadeemilised ringkonnad ja kodanikuühiskond)[24]. Lisaks on vastu võetud andmekaitseraamistiku kolleegiumi vahekohtu reeglid[25] ja vahekohtunike käitumisjuhend,[26] mis on kõik kättesaadavad vaidluste lahendamise rahvusvahelise keskuse veebisaidil. Läbivaatamise ajaks ei olnud ükski ELi isik vahekohtumenetlust veel kasutanud.

2.1.4. Juhendid, koostöö ja teadlikkuse suurendamine

Alates andmekaitseraamistiku jõustumisest on kaubandusministeerium korraldanud mitmesuguseid teadlikkuse suurendamise üritusi, nagu teabetuure, veebiseminare ja konverentse, loonud kontaktid kutseorganisatsioonidega ja suhelnud otse enam kui 3 000 ettevõtjaga, et anda teavet andmekaitseraamistiku kohta. Samuti on ta avaldanud suunised, sealhulgas korduma kippuvate küsimuste vormis, mis on suunatud üksikisikutele, samuti ELi ja USA ettevõtjatele[27]. Euroopa Andmekaitsenõukogu on omakorda välja töötanud üksikisikutele ja ettevõtjatele suunatud kaebuste vormid ja korduma kippuvad küsimused. Kui komisjon võttis vastu kaitse piisavuse otsuse, avaldas ta samal põhimõttel andmekaitseraamistiku kohta küsimuste ja vastuste dokumendi ning teabelehe[28].

Samal ajal selgus läbivaatamiskoosolekul, et üksikisikute teadlikkuse suurendamiseks ja ettevõtjatele suuniste andmiseks on vaja teha rohkem tööd. Ettevõtjatelt ja sõltumatutelt kaebuste menetlemise mehhanismidelt saadud tagasiside ning väga väike kaebuste arv viitavad sellele, et üksikisikud ei pruugi alati olla teadlikud oma õigustest ja/või nende kasutamise mehhanismist. Läbivaatamiskoosolekul väljendas kaubandusministeerium huvi teha koostööd ELi andmekaitseasutustega, et parandada ELi üksikisikute teadlikkust raamistikust. Komisjon toetab selliseid algatusi ja astub ka samme üksikisikute paremaks teavitamiseks, sealhulgas esitab oma veebisaidil andmekaitseraamistiku kohta lisateavet, näiteks lisab linke ja viiteid asjakohastele juhenddokumentidele, mille on vastu võtnud Euroopa Andmekaitsenõukogu, kaubandusministeerium ja teised USA ametiasutused.

Andmekaitseraamistiku põhimõtteid käsitlevate suuniste küsimuses leppisid Euroopa Andmekaitsenõukogu esindajad läbivaatamiskoosolekul kokku, et teevad lähikuudel koostööd, et anda täiendavaid selgitusi andmekaitseraamistiku kohase personaliandmete mõiste ja selliste andmete töötlemise suhtes kohaldatavate erikohustuste kohta. Uuriti sellistesse suunistesse lisatavaid elemente. Näiteks võiks nendes suunistes kirjeldada teatavaid praktilisi stsenaariume, kus töötajate andmeid töödeldakse andmekaitseraamistiku alusel (nt pilveteenuse pakkuja poolt), ning selgitada selliste stsenaariumide puhul, millised andmekaitseraamistikuga seotud kohustused oleksid asjakohased. Lisaks võiks ta soovitada ettevõtjatel, kes saavad ELi üksikisikutest töötajate andmeid (kuid ei pruugi neid andmeid töösuhte kontekstis kasutada), valida oma sõltumatuks kaebuste menetlemise mehhanismiks andmekaitseasutuste kolleegiumi. See tagaks, et need isikud saavad pöörduda nii-öelda kodulähedase asutuse poole, mis on vajaduse korral paremini tuttav personaliandmete suhtes kohaldatava riigisisese õigusega.

---

[24] https://go.adr.org/DPF_Arbitrator_Bios.html.
[25] https://go.adr.org/rs/294-SFS-516/images/IC.DR-AAA_EU-US_DPF_AnnexI_Arbitration_Rules.pdf.
[26] https://go.adr.org/rs/294-SFS-516/images/Code_of_Conduct_for_Arbitrators_Appointed_to_EU-US_DPF_AnnexI_Arbitrations.pdf.
[27] Vt nt https://www.dataprivacyframework.gov/US-Businesses.
[28] https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/eu-us-data-transfers_en.

Andmekaitseraamistiku nõuded andmete edasisaatmise kohta on samuti üks konkreetne aspekt, mille puhul tundub, et kasu oleks põhjalikumatest suunistest (mis põhinevad ka kutseorganisatsioonidelt saadud teabel). Lisaks märkis kaubandusministeerium, et tasub uurida, kas mõned sektorid võiksid saada kasu täiendavatest suunistest selle kohta, kuidas oma tegevuses andmekaitseraamistiku põhimõtteid kohaldada, nt tervishoiualaste teadusuuringute ja finantsteenuste valdkonnas.

Komisjon tervitab mõlema poole valmisolekut töötada välja suunised ja loodab, et töö eespool nimetatud teemadega algab varsti.

Üldisemalt on USA ametiasutuste ja andmekaitseasutuste vahelise teabevahetuse ja koostöö tagamiseks loodud mitu mehhanismi, sealhulgas on föderaalses kaubanduskomisjonis ja kaubandusministeeriumis määratud spetsiaalsed kontaktpunktid, et tegeleda andmekaitseasutuste päringute ja esildistega.

2.1.5. Asjaomased muudatused USA õigussüsteemis

Pärast kaitse piisavuse otsuse vastuvõtmist on USA eraelu puutumatuse valdkonna õigusraamistikus toimunud mitmeid muudatusi. Sealhulgas seadusandlikke ja regulatiivseid muudatusi ning kohtupraktika valdkonnas toimunud muudatusi. Üldiselt näitavad need, et ELi ja USA lähenemisviisid teatavatele eraelu puutumatusega seotud probleemidele on muutunud sarnasemaks, sealhulgas sarnaste õigusmõistete kasutamise kaudu. Mõned neist muudatustest ei ole veel lõpule viidud ja neid tuleb täiendavalt jälgida.

Föderaalsel tasandil andis president välja mitu täidesaatvat korraldust, mis on isikuandmete kasutamise seisukohast olulised. Eelkõige keelatakse või piiratakse 28. veebruari 2024. aasta täidesaatva korraldusega 14117[29] teatavat liiki tundlike isikuandmetega (nt terviseandmed, biomeetrilised tunnused, genoomiandmed) seotud tehingud üksustega mõnes „probleemriigis“[30]. Vastuvõetud täidesaatva korraldusega antakse peaprokurörile ülesanne esitada ettepanekud korralduse rakendamist täpsustavate määruste kohta, kuid neid ei ole käesoleva aruande vastuvõtmise ajal veel välja antud. Lisaks keskendutakse 30. oktoobri 2023. aasta täidesaatvas korralduses 14110 tehisintellekti kohta[31] ohutu, turvalise ja usaldusväärse tehisintellekti arendamisele. Selles nõutakse, et mitu föderaalasutust töötaksid välja tehisintellektiga seotud ohutusstandardid ja suunised, sealhulgas eraelu puutumatusele avalduvate konkreetsete tehisintellektiga seotud riskide kohta ja privaatsuse säilitamise meetodite kohta.

Viimastel aastatel on kongressis esitatud mitu eraelu puutumatuse föderaalse seaduse eelnõu, 20 USA osariiki on aga alates 2024. aasta juulist vastu võtnud põhjalikud eraelu puutumatuse seadused, millest kaheksat juba kohaldatakse: California, Colorado, Oregoni, Virginia, Connecticut, Utah, Texas ja Florida. Lisaks on 17 USA osariiki võtnud vastu õigusaktid, milles

---

[29] https://www.federalregister.gov/documents/2024/03/01/2024-04573/preventing-access-to-americans-bulk-sensitive-personal-data-and-united-states-government-related.

[30] Nagu peaprokurör 3. mail 2024 välja antud eelteatises eeskirjade koostamise ettepaneku kohta välja pakkus, kuuluvad nende hulka Hiina, Kuuba, Hongkong ja Macau, Iraan, Põhja-Korea ja Venezuela. Vt https://www.federalregister.gov/documents/2024/03/05/2024-04594/national-security-division-provisions-regarding-access-to-americans-bulk-sensitive-personal-data-and.

[31] https://www.federalregister.gov/documents/2023/11/01/2023-24283/safe-secure-and-trustworthy-development-and-use-of-artificial-intelligence.

käsitletakse automaatset töötlemist (või vähemalt mõnda selle vormi) ja lubatakse üldiselt loobuda teatavat liiki otsustamisest, mis põhineb profiilianalüüsil[32].

Kohtupraktika arenguga seoses on mitu kodanikuühiskonna esindajat osutanud Ülemkohtu hiljutisele otsusele kohtuasjas Loper Bright Enterprises *vs.* Raimondo (28. juuni 2024). Selle kohtuotsusega tühistatakse Chevroni doktriini kohaldav varasem kohtupraktika, mis nõuab, et kohtud kohaldaksid põhimõtet, mille kohaselt peab reguleeriv asutus juhul, kui selle ameti poolt kohaldatavas seaduses esineb mitmetimõistetavust, tõlgendama õigust mõistlikul viisil. Eelkõige on mõned valitsusvälised organisatsioonid väljendanud muret selle üle, millist mõju avaldab kõnealune Ülemkohtu otsus föderaalse kaubanduskomisjoni pädevusele koostada eeskirju eraelu puutumatuse valdkonnas, tunnistades samas, et tema nõuete täitmise tagamise volitustele ei pruugi olla mingit mõju või see võib olla piiratud. Läbivaatamiskoosolekul teatas föderaalne kaubanduskomisjon, et kõnealuse kohtuotsuse täpsed tagajärjed ei ole veel teada. Samal ajal selgitas ta, et föderaalne kaubanduskomisjon koostab eeskirju föderaalse kaubanduskomisjoni seaduses sätestatud volituse alusel, mis erinevad teiste haldusasutuste omadest ja mille puhul Chevroni doktriin ei ole nii asjakohane. Hiljutisel kohtuotsusel võib seega olla selles valdkonnas piiratud mõju.

Lisaks teavitas föderaalne kaubanduskomisjon hiljutistest muudatustest oma lähenemisviisis automaatsele töötlemisele ja tehisintellektile. Selle hulka kuulub koos teiste täitevasutustega vastu võetud ühisavaldus diskrimineerimise ja kallutatuse vastu automatiseeritud süsteemides[33] ning mitu täitemeedet, milles föderaalne kaubanduskomisjon keskendub muu hulgas läbipaistvusele, automaatse töötlemise õiglusele ja üksikisikute võimalustele tulemusi vaidlustada. Sellega seoses on kõige märkimisväärsem föderaalse kaubanduskomisjoni 2024. aasta märtsi otsus ettevõtja Rite Aid kohta, millega kehtestati ettevõtjale viieaastane keeld kasutada turvaeesmärkidel näotuvastustehnoloogiat[34]. Eelkõige leidis föderaalne kaubanduskomisjon, et Rite Aid ei võtnud mõistlikke meetmeid, et vältida ekslikke tulemusi ja tarbijaid kasutatavast tehnoloogiast teavitada. Üldisemalt käsitles föderaalne kaubanduskomisjon läbivaatamiskoosolekul oma praegusi prioriteete ja eelkõige valdkondi, kus tema arvates tuleb edaspidi täitmise tagamisel üles näidata rohkem initsiatiivi. See hõlmab

[32] Kuigi profiilianalüüsi mõiste erineb riigiti, määratletakse profiilianalüüsi üldiselt kui isikuandmete automaatset töötlemist, mille eesmärk on hinnata, analüüsida või prognoosida tuvastatud või tuvastatava füüsilise isiku majandusliku olukorra, tervise, isiklike eelistuste, huvide, usaldusväärsuse, käitumise, asukoha või liikumisega seotud isiklikke aspekte. Tavaliselt võivad tarbijad profiilianalüüsist loobuda. Profiilianalüüsi käsitlevad õigusaktid on välja töötatud järgmised osariigid: Colorado (Colo. Rev. Stat. Ann. § 6-1-1306), Connecticut (Conn. Gen. Stat. Ann. § 42–518), Delaware (Del. Code Ann. tit. 6, § 12D–104), Florida (Fla. Stat. Ann. § 501.705), Indiana (Ind. Code Ann. § 24-15-3-1), Kentucky (Ky. Rev. Stat. Ann. § 367.3615), Maryland (Maryland Online Data Privacy Act of 2024, jõustunud 9. mail 2024), Minnesota (Minn. Stat. Ann. § 325O.07), Montana (Mont. Code Ann. § 30-14-2808), Nebraska (Neb. Rev. Stat. Ann. § 87–1107), New Hampshire (N.H. Rev. Stat. Ann. § 507-H:4), New Jersey (N.J. Stat. Ann. § 56:8–166.8), Oregon (Or. Rev. Stat. Ann. § 646A.574), Rhode Island (Rhode Island Data Transparency and Privacy Protection Act, jõustunud 29. juunil 2024), Tennessee (Tenn. Code Ann. § 47-18-3304), Texas (Tex. Bus. & Com. Code Ann. § 541.051) ja Virginia (Va. Code Ann. § 59.1–577).

[33] https://files.consumerfinance.gov/f/documents/cfpb_joint-statement-enforcement-against-discrimination-bias-automated-systems_2023-04.pdf.

[34] https://www.ftc.gov/legal-library/browse/cases-proceedings/2023190-rite-aid-corporation-ftc-v.

tundlike andmete (nt terviseandmed, biomeetrilised andmed, asukohatuvastus) kaitset,[35] laste ja alaealiste kaitset internetis[36] ning andmeturvet[37].

Komisjon jälgib ka edaspidi tähelepanelikult neid ja muid USAs toimuvaid muudatusi, eelkõige mis tahes edasisi samme tervikliku föderaalse eraelu puutumatuse seaduse suunas ning ülemkohtu hiljutise kohtupraktika võimalikku mõju föderaalse kaubanduskomisjoni rollile eraelu puutumatuse valdkonnas.

Komisjon avaldab heameelt teabe üle, mis föderaalne kaubanduskomisjon esitas oma hiljutiste täitemeetmete ja praeguste prioriteetide kohta, mis suures osas vastavad andmekaitsenõuete täitmise tagamise suundumustele ja prioriteetidele Euroopas. Föderaalne kaubanduskomisjon osaleb ka aktiivselt võrgustikus, mille komisjon lõi 2024. aasta märtsis ja mis ühendab riike, kes saavad kasu ELi kaitse piisavuse otsusest[38]. Ulatuslikum ühtlustamine peaks soodustama ja hõlbustama tihedamat koostööd eraelu puutumatuse nõuete täitmise tagamise eest vastutavate asutuste vahel mõlemal pool Atlandi ookeani, eelkõige andmekaitseraamistiku toimimisega seotud küsimustes.

2.2. Aspektid, mis on seotud ELi-USA andmekaitseraamistiku alusel edastatud isikuandmetele juurdepääsu ja nende kasutamisega USA avaliku sektori asutuste poolt

Kaitse piisavuse otsus sisaldab üksikasjalikku hinnangut normidele, millega reguleeritakse andmekaitseraamistiku kohaselt kinnitatud ettevõtjatele EList edastatavate isikuandmete kogumist ja kasutamist USA avaliku sektori asutuste poolt, eelkõige kriminaalõiguskaitse ja riikliku julgeoleku eesmärgil. Pärast kaitse piisavuse otsuse vastuvõtmist ei ole – nagu USA ametiasutused läbivaatamiskoosolekul kinnitasid – andmekaitseraamistiku esimesel aastal andmetele õiguskaitse või regulatiivsetel eesmärkidel juurdepääsu suhtes kohaldatavas õigusraamistikus tehtud olulisi muudatusi. Seetõttu puudutavad allpool esitatud järeldused üksnes riikliku julgeoleku valdkonnas toimunut.

Kaitse piisavuse otsuses tehtud järeldused luureasutuste juurdepääsu kohta andmetele tuginevad nende tingimuste ja piirangute analüüsile, mida kohaldatakse mitme asjaomase õigusasutuse osalusel korraldatava signaaliluureoperatsiooni suhtes, eelkõige välisluure jälitustegevuse seaduse (FISA) paragrahvi 702 ja täidesaatva korralduse 12333[39] alusel, mida

[35] Vt nt hiljutine föderaalse kaubanduskomisjoni korraldus ettevõtja X-Mode vastu tundliku asukohateabe müümise ja jagamise tõttu (https://www.ftc.gov/system/files/ftc_gov/pdf/X-ModeSocialDecisionandOrder.pdf) ja ettevõtja Monument vastu seoses tundlike terviseandmete avalikustamisega kolmandatele isikutele turunduslikel eesmärkidel (https://www.ftc.gov/system/files/ftc_gov/pdf/MonumentOrderFiled.pdf).

[36] Näiteks algatas föderaalne kaubanduskomisjon hiljuti uurimise, mille tulemuseks oli kohtuasi TikToki ja selle emaettevõtja Bytedance vastu laste eraelu puutumatuse seaduse väidetava rikkumise tõttu. Väidetavalt ei täitnud kumbki ettevõtja nõuet teavitada vanemaid ja saada nende nõusolek enne, kui hakatakse koguma ja kasutama alla 13aastaste laste isikuandmeid (https://www.ftc.gov/news-events/news/press-releases/2024/08/ftc-investigation-leads-lawsuit-against-tiktok-bytedance-flagrantly-violating-childrens-privacy-law).

[37] Vt ülevaade hiljutistest täitemeetmetest föderaalses kaubanduskomisjonis (FTC 2023 Privacy and Data Security Update): https://ec.europa.eu/commission/presscorner/detail/en/mex_24_1307.

[38] Vt https://ec.europa.eu/commission/presscorner/detail/en/mex_24_1307. 2024. aasta märtsi koosoleku tulemusena otsustati korraldada mitu temaatilist istungit. Esimene neist toimus 2024. aasta juulis ja sellel keskenduti selliste vahendite väljatöötamisele, mis võivad toetada väikeseid ja keskmise suurusega ettevõtjaid eraelu puutumatust käsitlevate õigusaktide järgimisel.

[39] Muud meetmed, mida saab seoses EList edastatavate andmetega välisluure jälitustegevuse seaduse alusel võtta, on individuaalne elektrooniline jälgimine (FISA paragrahv 105), füüsilised otsingud (FISA paragrahv 302), pealtkuulamisseadmete kasutamine (FISA paragrahv 402) ning äridokumentide kogumine teatavatelt ettevõtjatelt (ühistranspordiettevõtjad, ühiskondlikud majutusasutused, sõidukite rendileandjad või füüsilised laoruumid, FISA

on täiendatud ja karmistatud Ameerika Ühendriikide presidendi poolt 7. oktoobril 2022 vastu võetud täidesaatva korraldusega 14086 Ameerika Ühendriikide signaaliluure kaitsemeetmete tõhustamise kohta (korraldus 14086). Korralduses 14086 sätestatud kaitsemeetmeid kohaldatakse kogu USA signaaliluuretegevuse suhtes, olenemata sellest, millisel õiguslikul alusel tegevus põhineb ja kus see toimub, ning nendega kaitstakse USA-väliste isikute (sealhulgas eurooplaste) andmeid[40]. Korraldusega 14086 loodi ka uus õiguskaitsemehhanism, mille kaudu üksikisikud ELis saavad neid siduvaid kaitsemeetmeid kasutada ja hageda.

Järgmistes punktides kirjeldatakse samme, mida USA ametiasutused on võtnud pärast kaitse piisavuse otsuse vastuvõtmist korralduse 14086 täitmiseks ning eespool nimetatud õigusraamistiku asjaomaseid muudatusi.

2.2.1. Asjaomased muudatused USA õigusraamistikus

2.2.1.1. Korralduse 14086 rakendamine luureasutuste poolt

Korraldusega 14086 kehtestatud piirangud ja kaitsemeetmed täiendavad FISA paragrahviga 702 ja korraldusega 12333 sätestatud piiranguid ja kaitsemeetmeid. Need on kõigile luureasutustele siduvad ning nende kasutuselevõttu on edendatud iga asutuse vastu võetud põhimõtete ja menetluste kaudu.

Esimese läbivaatamise käigus kinnitasid USA ametiasutused, et korralduses 14086 ei ole pärast selle vastuvõtmist muudatusi tehtud. Lisaks selgitati, et USA president ei ole kasutanud korralduse 14086 paragrahvi 2 punkti b alapunkti i alapunktis B ja paragrahvi 2 punkti b alapunkti ii alapunktis C ette nähtud volitusi, et ajakohastada selliste õiguspäraste eesmärkide loetelu, mille jaoks võib kasutada signaaliluuret, ega nende eesmärkide loetelu, mille jaoks võib kasutada masskogutud andmeid[41]. Selleks et määrata kindlaks konkreetsemad luureprioriteedid, mille jaoks signaaliluureandmeid võib tegelikult koguda, kehtestati korraldusega 14086 erimenetlus. Eelkõige tuleb konsulteerida riikliku luurejuhi büroo kodanikuvabaduste kaitse ametnikuga, et hinnata iga prioriteedi puhul, kas 1) see edendab üht või mitut korralduses loetletud õiguspärast eesmärki; 2) see ei olnud kavandatud signaaliluureandmete kogumiseks korralduses loetletud keelatud eesmärgil ega eeldanud seda ning 3) see kehtestati pärast kõigi isikute eraelu puutumatuse ja kodanikuvabaduste asjakohast kaalumist[42]. Riikliku luurejuhi büroo kodanikuvabaduste kaitse ametnik kinnitas läbivaatamiskoosolekul, et ta vaatas läbi riikliku luurejuhi poolt 2023. aasta riiklikus luureprioriteetide raamistikus esitatud prioriteedid, jõudis järeldusele, et need vastavad eespool nimetatud nõuetele, ning jagas oma järeldust riikliku luurejuhiga, kes omakorda esitas prioriteedid kinnitamiseks presidendile. Riikliku luurejuhi büroo kodanikuvabaduste kaitse ametnik pakkus korralduse 14086 nõuete alast koolitust ka luureühenduse osalejatele, kes on kaasatud luureprioriteetide väljatöötamisesse.

USA ametiasutused on viimase aasta jooksul astunud ka täiendavaid praktilisi samme, et rakendada korraldust 14086 oma igapäevases tegevuses. Eelkõige on luureasutused

paragrahv 501). Neid erinevaid õiguslikke aluseid analüüsitakse üksikasjalikult kaitse piisavuse otsuses (põhjendused 142–152).

[40] Lisateabe saamiseks vt kaitse piisavuse otsuse punkt 3.2.1.2.

[41] Nende õiguspäraste eesmärkide hulka kuulub näiteks kaitse spionaaži, sabotaaži, mõrva või muu luuretegevuse eest, mida viib läbi välisriigi valitsus, organisatsioon või isik või mida viiakse läbi välisriigi valitsuse, organisatsiooni või isiku poolt või nimel või tema abiga; kaitse välisriigi valitsuse, organisatsiooni või isiku poolt või nende nimel korraldatava terrorismi, pantvangide võtmise ning isikute vangistuses hoidmise eest.

[42] Korralduse 14086 paragrahvi 2 punkti b alapunkt ii.

kehtestanud täiendavad sise-eeskirjad ja suunised korralduse kohaldamiseks, näiteks sisemenetlused (siselubade andmise nõuete, dokumenteeritud juurdepääsukontrolli kaudu, nii et teabele on juurdepääs ainult isikutel, kes on saanud nõuetekohase väljaõppe ja kellel on vajalikud missiooninõuded jne), et tagada teabe vajalikkuse ja proportsionaalsuse nõuete täitmine nii sihitud kui ka masskogumise korral[43]. Lisaks on korraldatud eri luureasutuste (nt NSA, CIA, FBI) töötajatele korralduse 14086 kohta koolitusi, sealhulgas riikliku luurejuhi büroo kodanikuvabaduste kaitse ametniku korraldatud iga-aastaseid ja sihtotstarbelisi koolitusi ning kohustuslikke koolitusi kõigile riikliku luurejuhi büroo uutele töötajatele.

Komisjon tervitab mitmesuguseid meetmeid, mis on võetud korralduse 14086 rakendamiseks ja järgimise tagamiseks. Kuna korralduse kaitsemeetmete praktilisel kohaldamisel tuleb kogemusi juurde, sooviks komisjon tulevaste läbivaatamiste käigus võimaluse korral arutada konkreetseid näiteid selle kohta, kuidas korraldust praktikas kohaldatakse (võttes samal ajal arvesse kohaldatavaid konfidentsiaalsuskaalutlusi).

2.2.1.2. Välisluure jälitustegevuse seaduse paragrahvi 702 kohaldamise uuesti lubamine

FISA paragrahv 702 lubab võtta välisluureinfo kogumise sihtmärgiks USA-väliseid isikuid, kelle puhul on piisavalt alust arvata, et nad asuvad väljaspool Ameerika Ühendriike. Teabe kogumine toimub välisluure jälitustegevuse kohtule esitatud ja tema heakskiidetud iga-aastaste sertifikaatide alusel. Nendes sertifikaatides määratakse kindlaks kogutava välisluureteabe konkreetsed kategooriad. 21. juulil 2023 teatas riikliku luurejuhi büroo, et FISA paragrahvi 702 alusel on kolm heakskiidetud sertifikaati, mis hõlmavad järgmisi välisluureteabe kategooriaid: 1) välisriikide valitsused ja nendega seotud üksused, 2) terrorismivastane võitlus ja 3) massihävitusrelvade leviku vastane võitlus[44]. Sertifikaadid peavad sisaldama ka sihtimis- ja minimeerimismenetlusi, mille välisluure jälitustegevuse kohus on heaks kiitnud[45]. Eelkõige nõutakse sihtimiseks, et USA ettevõtjad, kes vastavad FISA määratlusele „elektroonilise side teenuse osutaja“, avalikustaksid elektroonilise side andmed, mis on saadetud või saadud kasutades identimistunnust, mis tuvastab spetsiifilise sidevahendi, nt telefoninumbri või e-posti aadressi. USA valitsus on avaldanud FISA paragrahvi 702 kohta mitu dokumenti, et teavitada üldsust jälgimisprogrammide toimimisest, kohaldatavatest nõuetest ja eraelu puutumatuse kaitsest ning välisluure jälitustegevuse kohtu rollist[46].

Kui kongress ei olnud FISA paragrahvi 702 kohaldamist uuesti lubanud, pidi see aegumisklausli tõttu aeguma 2023. aasta lõpus. Pärast ajutist uuesti lubamist ilma muudatusteta võttis kongress 19. aprillil 2024 vastu luuretegevuse reformimise ja Ameerika turvalisuse seaduse (Reforming Intelligence and Securing America Act, RISAA), millega anti kaheks aastaks uus luba FISA paragrahvi 702 kohaldamiseks ja tehti selles mitu muudatust. Need meetmed võib üldjoontes jagada kahte kategooriasse: 1) muudeti FISA paragrahvi 702 alusel lubatud jälgimistoimingute ulatust ning 2) tehti institutsioonilisi ja menetluslikke muudatusi.

---

[43] Vt https://www.intel.gov/ic-on-the-record-database/results/oversight/1278-odni-releases-ic-procedures-implementing-new-safeguardsin-executive-order-14086, avaldatud 3. juulil 2023.

[44] https://www.intelligence.gov/ic-on-the-record-database/results/1307-release-of-documents-related-to-the-2023-fisa-section-702-certifications.

[45] Sellised menetlused piiravad andmete kogumist konkreetsel välisluure eesmärgil, juurdepääsu andmebaasidele, kus säilitatakse FISA paragrahvi 702 alusel saadud teavet (sealhulgas juurdepääsukontrolli kaudu), ning piiravad sellise teabe kasutamist, säilitamist ja levitamist.

[46] https://www.intel.gov/foreign-intelligence-surveillance-act.

Muudatused FISA paragrahvi 702 alusel lubatud jälgimistoimingute ulatuses

RISAAga on tehtud FISA paragrahvi 702 alusel teostatavate jälgimistoimingute ulatuses kolm peamist muudatust.

Esiteks on nn temaatiline kogumine lõplikult keelatud[47]. See osutab teabe kogumisele, mille puhul paragrahvi 702 kohane identimistunnus (näiteks e-posti aadress) ei ole sõnumite „saaja“ või „saatja“, vaid sisaldab pigem viidet identimistunnusele sõnumi sees (nt e-posti sõnumid, mida ei saadeta asjaomasele e-posti aadressile või asjaomaselt e-posti aadressilt, kuid mis sisaldavad seda e-posti aadressi e-kirja tekstis või sõnumi kehas). Kuigi selline kogumine oli juba välistatud pärast FISA muutmist 2018. aastal, nähti FISAga siiski ette võimalus tulevikus nn temaatilist kogumist uuesti alustada pärast konkreetset loamenetlust, millesse on kaasatud välisluure jälitustegevuse kohus ja kongress. RISAA viimase muudatusega on see võimalus välja jäetud.

Teiseks on välisluureteabe määratlust laiendatud nii, et see hõlmaks ka uimastivastase võitluse teavet[48]. Läbivaatamiskoosolekul selgitasid USA ametiasutused, et muudatus tehti praeguse fentanüülikriisi ning rahvusvaheliste uimastikaubitsejate ja -tootjate põhjustatud suureneva ohu tõttu riiklikule julgeolekule. Seda arvesse võttes kinnitati, et see mõiste kuulub mitme korralduses 14086 loetletud õiguspärase eesmärgi alla, st eesmärk mõista või hinnata välismaiste organisatsioonide võimeid, kavatsusi või tegevust, mis kujutavad endast kohest või võimalikku ohtu Ameerika Ühendriikide või tema liitlaste riiklikule julgeolekule; eesmärk mõista või hinnata üleilmset julgeolekut mõjutavaid rahvusvahelisi ohte, sealhulgas rahvaterviseohte, ning eesmärk kaitsta rahvusvaheliste kuritegelike ohtude eest[49].

Kolmandaks laiendati RISAAga „elektroonilise side teenuse osutaja“ määratlust ja suurendati seeläbi nende ettevõtjate ringi, keda võidakse kohustada esitama teavet FISA paragrahvi 702 kohaselt[50]. Määratlus hõlmab nüüd ka teisi teenuseosutajaid, kellel on „juurdepääs seadmetele, mida kasutatakse või võidakse kasutada traat- või elektroonilise side edastamiseks või salvestamiseks“, jättes sõnaselgelt välja avalikud majutusasutused, eluruumid, üldkasutatavad ehitised ja toitlustusasutused. Kongressile saadetud kirjas viitas justiitsministeerium sellele muudatusele kui tehnilisele muudatusele, mille eesmärk on hõlmata „äärmiselt väikest“ hulka tehnoloogiaettevõtjaid, keda välisluure jälitustegevuse kohtu ja välisluure jälitustegevuse apellatsioonikohtu hiljutiste otsuste kohaselt ei hõlmanud elektroonilise side teenuse osutaja eelmine määratlus[51]. Samas kirjas kohustus justiitsministeerium kohaldamisala kitsendama ja kohaldama seda liiki teenuseosutaja määratlust üksnes kohtuvaidluses, mille tulemusel tehakse välisluure jälitustegevuse kohtu otsus. Sellest tulenevalt on asjaomased ettevõtjad nimetatud kongressi jaoks mõeldud salastatud lisas. Mitmed valitsusvälised organisatsioonid, sealhulgas need, kes andsid läbivaatamise käigus tagasisidet, väljendasid muret selle määratluse laiendamise pärast ja väitsid, et see võib hõlmata paljusid USA ettevõtjaid (kuna paljud neist osutavad mingit liiki teenuseid ja omavad juurdepääsu sideseadmetele). Seda muret arvestades on luureühenduse toetusel esitatud veel üks muudatusettepanek 2025. eelarveaasta luurelubade

[47] RISAA paragrahv 22.
[48] RISAA paragrahv 23.
[49] Korralduse 14086 paragrahvi 2 punkti b alapunkti ii alapunkti A alapunktid 2, 3 ja 10.
[50] RISAA paragrahv 25.
[51] https://www.justice.gov/opa/media/1348621/dl?inline. Vt välisluure jälitustegevuse kohtu 2022. aasta otsus (https://www.intel.gov/assets/documents/702%20Documents/declassified/2022-FISC-ECSP-OPINION.pdf) ja välisluure jälitustegevuse apellatsioonikohtu otsus, millega seda otsust kinnitati (https://www.intel.gov/assets/documents/702%20Documents/declassified/2023_FISC-R_ECSP_Opinion.pdf).

seaduse eelnõus, mis on praegu kongressis arutamisel. Kui kongress peaks muudatuse heaks kiitma, tagaks see, et elektroonilise side teenuse osutaja määratlusele vastavate ettevõtjate hulka lisanduksid ainult ettevõtjad, keda on nimetatud eelmainitud välisluure jälitustegevuse kohtu otsustes. Samuti nähakse eelnõus ette, et iga sellisele ettevõtjale adresseeritud suunis tuleb edastada välisluure jälitustegevuse kohtule, et ta saaks kontrollida, kas ettevõtja kuulub tõepoolest selle kohaldamisalasse. Oma kirjas kongressile kohustus justiitsministeerium esitama kongressile iga kuue kuu järel aruande ajakohastatud määratluse kohaldamise kohta, et võimaldada kongressil teostada määratluse kitsa kohaldamise üle asjakohast järelevalvet.

Oluline on see, et USA ametiasutused ning eraelu puutumatuse ja kodanikuvabaduste järelevalve komisjon kinnitasid läbivaatamiskoosolekul, et FISA paragrahvi 702 kohaselt andmete kogumise ja kasutamise suhtes kohaldatakse jätkuvalt täielikult kõiki korralduse 14086 kaitsemeetmeid. Seega kuigi RISAAga laiendatakse mõnevõrra nende ettevõtjate ringi, kes võivad saada korralduse esitada teavet, ei piira see õiguste kasutamist. Siiski on oluline jälgida edasist (seadusandlikku ja aruandlusega seotud) arengut ning saada teavet nende uute eeskirjade kohaldamise kohta praktikas. See hõlmab näiteks välisluure ja elektroonilise side teenuse osutajate määratluste laiendamise mõju FISA paragrahvi 702 sihtmärkide arvule (millest riikliku luurejuhi büroo igal aastal teatab, vt läbipaistvuse kohta allpool). FISA paragrahvi 702 kohta hiljuti eraelu puutumatuse ja kodanikuvabaduste järelevalve komisjoni koostatud aruande (vt allpool) tulevane järelaruanne peaks sisaldama selle kohta eriti põhjalikku teavet.

Institutsionaalsed ja menetluslikud muudatused

Institutsionaalsete ja menetluslike sätete suhtes kodifitseeriti RISAAs mitu menetlust, mida juba praktikas järgiti, ja kehtestati uued kaitsemeetmed. Kuigi mõned muudatused puudutavad ainult USA isikuid, suurendavad mitmed neist nii selliste USA kui ka USA-väliste isikute kaitset, kelle andmeid võib FISA paragrahvi 702[52] alusel koguda, ja mis on seetõttu andmekaitseraamistiku toimimise seisukohast olulised.

Esiteks kehtestati mitu täiendavat vastutus-, järelevalve- ja aruandlusnõuet. Konkreetselt peavad föderaalse juurdlusbüroo töötajad nüüd igal aastal läbima koolituse eeskirjade kohta, mida kohaldatakse FISA paragrahvi 702 alusel saadud teabepäringute suhtes[53]. Samuti peab FBI andma kongressile aru oma päringutega seotud tegevusest (nt päringud, mille puhul kasutatakse pakktehnoloogiat, st ühe päringu osana tehakse mitut päringut) ja kehtestatud aruandlusmeetmetest, millega tagatakse vastavus päringute tegemise õiguslikele nõuetele (RISAA paragrahvid 11–12). Lisaks on justiitsministeeriumi peainspektorile tehtud ülesandeks koostada aruanne päringute tegemise nõuete täitmise kohta FBI poolt (RISAA paragrahv 9). Üldisemas plaanis on välisluure jälitustegevuse kohtu, riikliku luurejuhi büroo ja peaprokuröri menetluste läbipaistvuse suurendamiseks nüüd vaja viia 180 päeva jooksul lõpule välisluure jälitustegevuse kohtu otsuste salastatusest vabastamise läbivaatamine (RISAA paragrahv 7). Lisaks tuleb säilitada kõigi välisluure jälitustegevuse kohtu ja välisluure jälitustegevuse

[52] Lisaks tehti RISAAga mõned muudatused FISA paragrahvi 105 kohases traditsioonilises individualiseeritud elektroonilises jälgimises (välisluure jälitustegevuse kohtu määruse alusel, mis väljastatakse, kui on olemas küllaldane alus). Luureasutuse poolt peaprokurörile esitatud individualiseeritud elektroonilise jälgimise korralduse taotlemiseks on nüüd vaja vande all antud ütlust, mis põhjendab seisukohta, et FISA paragrahvi 105 tingimused on täidetud (RISAA paragrahvi 6 punkt a). Võõrvõimude või nende agentide elektroonilise jälgimise võimalikku kestust on pikendatud 120 päevalt ühele aastale (RISAA paragrahvi 6 punkt g).

[53] RISAA paragrahvi 2 punkt d.

apellatsioonikohtu (kui välisluure jälitustegevuse kohtu otsuse saab edasi kaevata) kohtuistungite protokollid ja edastada need kongressile (RISAA paragrahv 8).

Teiseks kehtestati RISAAga täiendavad piirangud FISA paragrahvi 702 alusel kogutud andmete kasutamisele FBI poolt. RISAA paragrahvi 2 punktis d on sätestatud, et pakktehnoloogiat tohib päringu tegemiseks kasutada üksnes pärast FBI advokaadilt heakskiidu saamist, välja arvatud juhul, kui esinevad kiireloomulised asjaolud. Lisaks ei tohi FBI nüüd automaatselt kontrollida FISA paragrahvi 702 alusel saadud minimeerimata teavet ning peab selle asemel tagama, et analüütikud peavad sellise teabe otsimiseks tegema kinnitava valiku. Samuti on RISAA keelanud FBI-l teha päringuid, mille ainus eesmärk on leida ja otsida tõendeid kuritegeliku tegevuse kohta (välja arvatud juhul, kui on põhjendatud veendumus, et need võivad aidata leevendada või kõrvaldada ohtu elule või raskeid kehavigastusi või täita vajaduse korral kohtumenetluses avalikustamiskohustusi)[54]. Lisaks on FBI-l keelatud kaasata analüütilistesse andmehoidlatesse minimeerimata andmeid, välja arvatud juhul, kui sihtisik on oluline käimasoleva riikliku julgeolekualase uurimise seisukohast[55].

Kolmandaks on muudetud teatavaid sätteid, mis käsitlevad *amici curiae* staatust ja rolli välisluure jälitustegevuse kohtus[56]. *Amici curiae* on määratud eksperdid, kes abistavad kohut (ja apellatsioonikohut) eraelu puutumatuse ja kodanikuvabadustega seotud küsimustes või aitavad selgitada tehnoloogilisi probleeme, kui tegeletakse konkreetse valitsuse taotlusega. Kuigi varem oli FISAs nõutud, et *amicus curiae* omaks eksperditeadmisi eraelu puutumatuse ja kodanikuvabaduste, luureandmete kogumise, kommunikatsioonitehnoloogia või muude asjakohaste valdkondade kohta, nõutakse selles nüüd põhimõtteliselt eksperditeadmisi eraelu puutumatuse ja kodanikuvabaduste ning luureandmete kogumise valdkonnas. Kohtul oli varemgi võimalus määrata *amicus curiae* alati, kui ta pidas seda asjakohaseks, ja ta pidi seda tegema seaduse uudse või olulise tõlgenduse korral. Pärast loa uuendamist peab välisluure jälitustegevuse kohus määrama *amicus curiae* ka iga kord, kui tal palutakse heaks kiita FISA paragrahvi 702 kohased sertifikaadid ja nendega kaasnevad menetlused (nt sihtimismenetlused), välja arvatud juhul, kui ta leiab, et see ei oleks asjakohane või põhjustaks tõenäoliselt põhjendamatu viivituse[57]. Lisaks võib kohus ühe *amicus curiae* asemel nüüd otsustada nimetada neid mitu. Samuti selgitatakse, et *amicus curiae* esitatav teave peab „piirduma nende konkreetsete küsimustega, millele kohus on viidanud“, kuigi valdkonnad, mille kohta *amicus curiae* võib märkusi esitada, on jäänud laiaks (st õiguslikud argumendid ja teave, mis on seotud USA isikute eraelu puutumatuse ja kodanikuvabaduste kaitsega, luureandmete kogumise ja kommunikatsioonitehnoloogiaga või mis tahes muu asjakohase valdkonnaga).

RISAA paragrahviga 18 luuakse täiendavate FISA reformide kohta soovituste esitamiseks FISA reformikomisjon, mis koosneb muu hulgas kongressi liikmetest, eraelu puutumatuse ja kodanikuvabaduste järelevalve komisjoni esimehest, riikliku luurejuhi esimesest asetäitjast ja peaprokuröri asetäitjast ning kongressi poolt ametisse nimetatavatest lisaliikmetest[58].

---

[54] RISAA paragrahvi 3 punkt a.

[55] RISAA paragrahvi 3 punkt b. Kui see on kiireloomuliste asjaolude tõttu vajalik, võib FBI direktor otsustada teha sellest sättest erandi, millest tuleb kongressile teatada.

[56] Selguse huvides tuleb märkida, et need muudatused ei mõjuta eriadvokaatide staatust ega rolli andmekaitseasju läbivaatavas kohtus, nagu USA läbivaatamiskoosolekul kinnitas.

[57] RISAA paragrahvi 5 punkt b.

[58] Paragrahvis 18 nõutakse konkreetselt, et esindaja ei oleks kongressi liige.

Komisjon jälgib tähelepanelikult edasist arengut FISA paragrahvi 702 osas, sealhulgas eraelu puutumatuse ja kodanikuvabaduste järelevalve komisjoni järelevalvetegevuse kontekstis (vt allpool), reformikomisjoni tööd ja FISA eelseisvat läbivaatamist kahe aasta pärast.

2.2.1.3. Jälitustegevus praktikas: arvnäitajad ja suundumused

Riikliku luurejuhi büroo iga-aastane statistiline läbipaistvusaruanne riiklike julgeoleku järelevalveasutuste kasutamise kohta luureühenduse poolt 2023. aastal (avaldatud 2024. aasta aprillis)[59] näitab, et FISA paragrahvi 702 kohaste eesmärkide arv suurenes 245 073-lt 2022. kalendriaastal 268 590-le 2023. kalendriaastal. Aruandes selgitatakse, et eesmärkide arvu kõikumisel võib olla mitmeid põhjusi, sealhulgas muutused tegevusprioriteetides, ülemaailmsed sündmused, tehniline suutlikkus, sihtrühmade käitumine ja muutused telekommunikatsioonisektoris. Aruandes märgitakse ka, et FISA paragrahvi 402 (pealtkuulamisseadmed) aluste sihtmärkide seas ei olnud ühtki USA-välist isikut (üks isik 2021. aastal ja mitte ühegi isikut 2022. aastal), FISA paragrahvi 501 (juurdepääs ühistranspordiettevõtjate, sõidukite rendileandjate või füüsiliste laoruumide äridokumentidele) alusel anti välja kuus korraldust (11 korraldust nii 2021. kui ka 2022. aastal) kuue sihtmärgi kohta (2021. aastal 13 ja 2022. aastal 11) ja need hõlmasid 5 412 kordumatut tunnust (2021. aastal 23 157 ja 2022. aastal 55 431), mida kasutati selliste korralduste alusel kogutud teabe edastamiseks.

Justiitsministeeriumi iga-aastases välisluure jälitustegevuse seaduse aruandes kongressile märgitakse, et 2023. aastal esitati välisluure jälitustegevuse kohtule 327 taotlust elektrooniliseks jälgimiseks vastavalt FISA paragrahvile 105 ja/või füüsiliste otsingute tegemiseks välisluure eesmärkidel vastavalt FISA paragrahvile 302[60]. Sihtrühma kuuluvate isikute koguarv jäi vahemikku 500–999. Riikliku julgeoleku teabenõuete kohta seisab aruandes, et teabe saamiseks USA-väliste isikute kohta esitati 10 115 taotlust (see arv ei sisalda üksnes abonendiandmete küsimist), milles paluti teavet 3 033 erineva USA-välise isiku kohta[61].

Mitu andmekaitseraamistiku kohaselt kinnitatud ettevõtjat (nt Google, Meta) kasutavad USA õiguses sätestatud võimalust avaldada läbipaistvusaruandeid, milles antakse teavet konkreetsel aruandeperioodil saadud FISA kohaste taotluste ja riikliku julgeoleku teabenõuete arvu kohta. Käesoleva aruande koostamise ajal ei olnud statistika FISA taotluste kohta pärast 2023. aasta juulit veel kättesaadav. Näiteks teatas Google, et on 2023. aasta juulist detsembrini saanud 500–999 riikliku julgeoleku teabenõuet, mis puudutasid 2 000–2 499 kontot[62]. Meta teatas, et ta sai samal aruandeperioodil 0–499 riikliku julgeoleku teabenõuet, mis puudutasid 500–999 kontot[63]. Näitajad on viimastel aastatel püsinud üsna stabiilsed. Läbipaistvuse suurendamiseks

[59] https://www.dni.gov/files/CLPT/documents/2024_ASTR_for_CY2023.pdf.
[60] https://www.justice.gov/nsd/media/1350236/dl?inline.
[61] Võrreldes eelmise aruandeaastaga (2022) on need arvnäitajad jäänud suures osas stabiilseks. Võrdluseks olgu märgitud, et 2022. aastal esitati välisluure jälitustegevuse kohtule 317 lõplikku elektroonilise jälgimise ja/või füüsilise otsingu taotlust välisluure eesmärkidel. Nende isikute koguarv, kelle kohta esitati elektroonilise jälgimise korraldus, jäi vahemikku 0–499. FBI esitas 2022. aastal 9 103 riikliku julgeoleku teabenõuet teabe saamiseks USA-väliste isikute kohta (see arv ei sisalda üksnes abonendiandmete küsimist). Allikas: https://irp.fas.org/agency/doj/fisa/2022rept.pdf.
[62] https://transparencyreport.google.com/user-data/us-national-security.
[63] https://transparency.meta.com/reports/government-data-requests/country/US/.

avaldavad mõned ettevõtjad (nt Google) saadud riikliku julgeoleku teabenõuded ennetavalt pärast seda, kui nende konfidentsiaalsuspiirang on kaotatud[64].

2.2.1.4. Muud suundumused

Läbivaatamise ettevalmistamise käigus on mitmed valitsusvälised organisatsioonid tõstatanud küsimusi USA luureasutuste poolse andmete kogumise uute viiside kohta, nagu andmete ostmine äriettevõtjatelt, eelkõige teabemaakleritelt. Nad selgitasid, et kuigi nii kogutud andmeid tuleb sellegipoolest töödelda kooskõlas muude nõuetega, sealhulgas korraldusega 12333,[65] toimub selline kogumine väljaspool FISA ja korralduse 14086 raamistikku.

Sellega seoses tuleks meelde tuletada, et mis tahes liiki vabatahtliku andmete jagamise suhtes kolmandate isikutega kohaldatakse andmekaitseraamistiku alusel mitut üksikasjalikku tingimust. Esiteks ei tohi kinnituse saanud organisatsioon jagada andmeid kolmanda isikuga (kes ei ole agent / volitatud töötleja) ilma asjaomasele üksikisikule teadet esitamata ja valikuvõimalust pakkumata[66]. Teiseks võib kolmandale isikule andmete edasisaatmise eest vastutuse põhimõtte kohaselt edasisaatmine toimuda ainult 1) piiratud ja kindlaksmääratud eesmärkidel, 2) ELi-USA andmekaitseraamistiku organisatsiooni ja kolmanda isiku vahelise lepingu alusel ning 3) ainult juhul, kui selle lepinguga nõutakse, et kolmas isik pakuks põhimõtetega tagatud kaitsetasemega võrdset kaitset[67].

Nagu ka läbivaatamiskoosolekul arutatud, on föderaalne kaubanduskomisjon võtnud täitemeetmeid tundlikke tarbijaandmeid müüvate teabemaaklerite suhtes. Näiteks X-Mode'i ja selle õigusjärglase Outlogici vastu algatatud kohtuasjas võttis föderaalne kaubanduskomisjon 9. jaanuaril 2024 vastu määruse, millega keelati ettevõtjal müüa asukohatuvastusandmeid kolmandatele isikutele ning kustutada andmed, mida ta oli ebaseaduslikult kasutanud ja jaganud. Föderaalne kaubanduskomisjon leidis uurimise käigus muu hulgas, et ettevõtja ei teavitanud üksikisikuid täielikult nende asukohatuvastusandmete kasutamisest ja müügist, ei kehtestanud meetmeid, mis võimaldaksid üksikisikutel jälgimisest loobuda, lubas kasutada andmeid potentsiaalselt diskrimineerivatel eesmärkidel ega seadnud piiranguid sellise teabe kasutamisele kolmandate isikute poolt[68]. Komisjon eeldab, et föderaalne kaubanduskomisjon kasutab sama lähenemisviisi siis, kui andmekaitseraamistiku kohaselt kinnitatud ettevõtjad rikuvad andmeid jagades eespool nimetatud sätteid.

Lõpetuseks väärib märkimist, et 2024. aasta mais avaldas riikliku luurejuhi büroo luureühenduse poliitikaraamistiku müügiteabe kohta[69]. Kõnealuses raamistikus on sätestatud mitmed põhimõtted ja nõuded, mida luureasutused peaksid äritehingu raames teabe hankimisel ja kasutamisel järgima, sealhulgas selleks, et minimeerida riske, mis mõjutavad eraelu puutumatust ja kodanikuvabadusi.

2.2.2. Sõltumatu järelevalve

[64] https://transparencyreport.google.com/user-data/us-national-security.
[65] Vt näiteks korralduse 12333 punkt 2.4 kogumismeetodite kohta.
[66] Vt kaitse piisavuse otsuse põhjendus 40.
[67] Vt kaitse piisavuse otsuse põhjendus 38.
[68] https://www.ftc.gov/news-events/news/press-releases/2024/01/ftc-order-prohibits-data-broker-x-mode-social-outlogic-selling-sensitive-location-data.
[69] https://www.dni.gov/files/ODNI/documents/CAI/Commercially-Available-Information-Framework-May2024.pdf. Luureasutustelt on raamistiku järgimist nõutud alates 2024. aasta augustist.

USA luureasutuste tegevuse üle teostavad järelevalvet mitmed organid, sealhulgas eraelu puutumatuse ja kodanikuvabaduste ametnikud, peainspektorid, kongress ning eraelu puutumatuse ja kodanikuvabaduste järelevalve komisjon._Eelkõige nõutakse korraldusega 14086, et igal luureasutusel oleksid kõrged õigus-, järelevalve- ja vastavusametnikud, et tagada kohaldatava USA õiguse järgimine. Seda järelevalvefunktsiooni täidavad ametnikud, kellel on määratud nõuetele vastavuse kontrolli ülesanne, samuti eraelu puutumatuse ja kodanikuvabaduste ametnikud ning peainspektorid[70]. Nad peavad tegema perioodilist järelevalvet signaaliluuretegevuse üle ja tagama, et kõik mittevastavused parandatakse. Luureasutused peavad võimaldama sellistele ametnikele järelevalveülesannete täitmiseks juurdepääsu kogu asjakohasele teabele ega tohi võtta meetmeid nende järelevalvetegevuse takistamiseks või ebakohaseks mõjutamiseks.

Läbivaatamiskoosolekul osales riikliku luurejuhi büroo luureühenduse peainspektori büroo peanõunik, kellel on ulatuslik pädevus kogu luureühenduses ja kellel on õigus uurida kaebusi või teavet väidetava ebaseadusliku tegevuse või võimu kuritarvitamise kohta. Ta kinnitas, et luureühenduse peainspektor kontrollib järelevalvetegevuse raames süstemaatiliselt korralduse 14086 järgimist. Ta viitas ka luureühenduse teiste peainspektorite hiljutisele järelevalvetegevusele, mida on üksikasjalikult kirjeldatud korrapärastes aruannetes. Näiteks teavitas riikliku julgeolekuasutuse peainspektor kongressi poolaastaaruandes, mis hõlmas ajavahemikku 2023. aasta aprillist kuni septembrini,[71] riikliku julgeolekuasutuse sihtimisotsuste ja -taotluste sisekontrolliraamistiku hindamisest. Selles jõuti järeldusele, et raamistik toimib nõuetekohaselt ning sellega tagatakse kodanikuvabadusi ja eraelu puutumatust kaitsvate seaduste, suuniste ja poliitika järgimine. Samas aruandes mainitakse ka uurimist, mille käigus selgus, et üks riikliku julgeolekuasutuse töötaja kuritarvitas signaaliluurevahendit loata eesmärkidel.

Korralduse 14086 kohaselt on eraelu puutumatuse ja kodanikuvabaduste järelevalve komisjonile[72] antud konkreetsed järelevalveülesanded[73]. Eraelu puutumatuse ja kodanikuvabaduste järelevalve komisjoni esimees ja selle kolm liiget osalesid läbivaatamiskoosolekul ning teatasid, et kõnealune komisjon andis 2023. aasta aprillis luureasutustele nõu korralduse 14086 rakendamise põhimõtete ja menetluste eelnõude kohta ning temaga konsulteeriti andmekaitseasju läbivaatava kohtu kohtunike ja eriadvokaatide

[70] Igal luureasutusel on peainspektor, kes on seaduse kohaselt sõltumatu ja vastutab asutuse riikliku julgeoleku eesmärgil teostatava tegevusega seotud auditite ja uurimiste läbiviimise eest. Neil on juurdepääs kõigile asjakohastele (sealhulgas salastatud) materjalidele, vajaduse korral kohtukorralduse alusel, ning nad võivad võtta tunnistajatelt ütlusi. Peainspektorid edastavad kuriteokahtlusega juhtumid prokuratuurile ja annavad asutuste juhtidele soovitusi parandusmeetmete võtmiseks. Kuigi nende soovitused ei ole siduvad, tehakse nende aruanded, sealhulgas järelmeetmete (või nende puudumise) kohta, üldiselt avalikuks ja saadetakse kongressile. Vt selle kohta kaitse piisavuse otsuse joonealune märkus 136 peainspektori rolli kohta.

[71] https://oig.nsa.gov/reports/Article/3609957/semiannual-report-to-congress-1-april-2023-to-30-september-2023/.

[72] Eraelu puutumatuse ja kodanikuvabaduste järelevalve komisjon on sõltumatu asutus, kellele on usaldatud ülesanded terrorismivastase võitluse poliitika ja selle rakendamise valdkonnas, et kaitsta eraelu puutumatust ja kodanikuvabadusi. Ta pääseb juurde kogu asjakohasele (sealhulgas salastatud) teabele, viib läbi vestlusi ja võtab ütlusi. Ta võib anda õiguskaitse- ja luureasutustele soovitusi ning annab korrapäraselt aru kongressile ja presidendile. Tema aruanded tehakse üldsusele võimalikult suures ulatuses kättesaadavaks.

[73] https://documents.pclob.gov/prod/Documents/EventsAndPress/834a1977-f420-4b2a-ae93-8a522b2c7c74/Trans-Atlantic%20Data%20Privacy%20Framework%20EO%20press%20release%20(FINAL)%20-%20Completed%20508%20-%2010202022.pdf.

ametisse nimetamise küsimuses. Eraelu puutumatuse ja kodanikuvabaduste järelevalve komisjon käivitas ka järelevalveprojekti, mille eesmärk on 1) vaadata läbi luureasutuste vastu võetud ajakohastatud põhimõtete ja menetluste rakendamine, et tagada nende kooskõla korraldusega, ning 2) vaadata igal aastal läbi uue õiguskaitsemehhanismi toimimine (vt allpool)[74]. Eraelu puutumatuse ja kodanikuvabaduste järelevalve komisjoni liikmed kinnitasid, et komisjon kavatseb mõlemad läbivaatamised läbi viia lähitulevikus. Seoses õiguskaitsega selgitasid nad, et kaebuste puudumise tõttu keskendub eraelu puutumatuse ja kodanikuvabaduste järelevalve komisjoni läbivaatus mehhanismi loomiseks kehtestatud põhimõtetele ja menetlustele.

Seoses muude järelevalvetegevustega avaldas eraelu puutumatuse ja kodanikuvabaduste järelevalve komisjon 28. septembril 2023 aruande FISA paragrahvi 702 kohta[75]. See aruanne on 2014. aasta varasema aruande järelmeede ning sisaldab ajakohastatud faktilist ja õiguslikku teavet FISA paragrahvi 702 kohaste jälgimisprogrammide toimimise kohta. Aruanne sisaldab ka kohaldatavate nõuete järgimise soovitusi luureasutustele ning ettepanekuid kongressile FISA paragrahvi 702 mitme aspekti edasiseks tugevdamiseks seoses selle kohaldamise uuesti lubamisega (sealhulgas kodifitseerides korralduses 14086 loetletud jälgimistegevuse õiguspärased eesmärgid)[76]. Läbivaatamiskoosolekul teatas eraelu puutumatuse ja kodanikuvabaduste järelevalve komisjon, et ootab luureasutustelt peatselt soovituste rakendamise kohta vastuseid, mida võetakse arvesse tulevases järelmeetmete aruandes. Muud käimasolevad järelevalveprojektid hõlmavad siseterrorismi vastast võitlust ja selle mõju eraelu puutumatusele ja kodanikuvabadustele ning avatud lähtekoodiga või kaubanduslikult kättesaadavate andmete kogumist FBI poolt[77].

Valitsusvälised organisatsioonid, kellega läbivaatamise käigus konsulteeriti, väljendasid ka muret selle pärast, et mitme eraelu puutumatuse ja kodanikuvabaduste järelevalve komisjoni liikme ametiaeg lõpeb lähitulevikus, mistõttu võib komisjonil puududa kvoorum. Eelkõige on lõppenud esimehe ametiaeg ja üleminekuperiood, mille jooksul ta saab ametis olla, lõpeb 2025. aasta jaanuaris, samal ajal on täitmata veel üks koht ning järgmise aasta jaanuaris vabaneb kolmas. Läbivaatamiskoosolekul selgitasid liikmed, et neile oleks ootamatu, kui eraelu puutumatuse ja kodanikuvabaduste järelevalve komisjon ei saavutaks kvoorumit, sest praegu vabale kohale on juba esitatud kandidaat (ja ootab senati kinnitust)[78]. Samuti rõhutasid nad, et isegi kui andmekaitsenõukogu kaotab kvoorumi, ei mõjuta see tema suutlikkust jätkata järelevalveprojektide elluviimist. Võttes siiski arvesse eraelu puutumatuse ja kodanikuvabaduste järelevalve komisjoni olulist rolli korralduse 14086 rakendamise läbivaatamisel, jälgib komisjon tähelepanelikult tulevaste vabade töökohtade ning kandidaatide määramise ja ametisse nimetamise seisu.

2.2.3. Õiguskaitse

[74] https://www.pclob.gov/OversightProjects/Details/1115.
[75] https://documents.pclob.gov/prod/Documents/OversightReport/8ca320e5-01d3-4d6a-8106-3384aad6ff31/2023%20PCLOB%20702%20Report%20-%20Nov%2017%202023%20-%201446.pdf.
[76] Komisjon märgib, et mõned neist soovitustest on lisatud RISAAsse, sealhulgas soovitus nn temaatilise kogumise kohta ja soovitus välisluure jälitustegevuse kohtu ekspertide (*amici curiae*) rolli tugevdamise kohta.
[77] https://www.pclob.gov/OversightProjects.
[78] https://documents.pclob.gov/prod/Documents/EventsAndPress/deb9cd13-12af-4250-998e-a520a2419a6b/PCLOB%20nominee%20press%20release%206-13-24.pdf.

Korraldusega 14086, mida täiendab peaprokuröri määrus, loodi uus õiguskaitsemehhanism, et menetleda ja lahendada üksikisikute esitatud vastuvõetavaid kaebusi USA signaaliluuretegevuse kohta[79]. Igal ELi üksikisikul on õigus esitada USAsse edastatud isikuandmete suhtes õiguskaitsemehhanismile kaebus signaaliluuretegevust reguleeriva USA õiguse (nt korraldus 14086, FISA paragrahv 702, korraldus 12333) väidetava rikkumise kohta, mis kahjustab tema eraelu puutumatust ja kodanikuvabadusi. Üksikisikud võivad esitada kaebuse ELi liikmesriigi andmekaitseasutusele, kes suunab kaebuse Euroopa Andmekaitsenõukogu sekretariaadi kaudu õiguskaitsemehhanismile. Mehhanism koosneb kahest tasandist, riikliku luurejuhi büroo kodanikuvabaduste kaitse ametnik viib läbi kaebuste esialgse uurimise ja annab üksikisikutele võimaluse kaevata kodanikuvabaduste kaitse ametniku otsus edasi sõltumatusse andmekaitseasju läbivaatavasse kohtusse. Kui riikliku luurejuhi büroo kodanikuvabaduste kaitse ametnik või andmekaitseasju läbivaatav kohus on läbivaatamise lõpule viinud, teatab riigi ametiasutus isikule, et „läbivaatamise käigus ei tuvastatud ühtegi kaebuses hõlmatud rikkumist“ või et „riikliku luurejuhi büroo kodanikuvabaduste kaitse ametnik või andmekaitseasju läbivaatav kohus tegi otsuse, millega nõutakse asjakohaste õiguskaitsemeetmete võtmist“. Riikliku luurejuhi büroo kodanikuvabaduste kaitse ametniku ja andmekaitseasju läbivaatava kohtu otsused on luureasutustele siduvad.

Pärast kaitse piisavuse otsuse vastuvõtmist on astutud täiendavaid samme, et muuta õiguskaitsemehhanism täielikult toimivaks.

14. novembril 2023 nimetati andmekaitseasju läbivaatavasse kohtusse ametisse kaheksa kohtunikku (st kaks kohtunikku rohkem, kui on nõutud korralduses 14086, mida on täiendatud peaprokuröri määrustega USA föderaalsete õigusnormide kogumi 28. jaotise § 201.3 punktis a)[80]. Nad nimetati ametisse korralduses 14086 sätestatud kriteeriumide alusel ja kooskõlas selles kehtestatud korraga, sealhulgas pärast konsulteerimist eraelu puutumatuse ja kodanikuvabaduste järelevalve komisjoniga[81]. Nende hulka kuuluvad endised föderaalse ringkonnakohtu ja apellatsioonikohtu kohtunikud, endine USA peaprokurör ning eraelu puutumatuse ja kodanikuvabaduste järelevalve komisjoni endine liige. Nagu korralduses nõutakse, on vähemalt pooltel kohtunikest eelnev töökogemus kohtunikuna. Lisaks määrati 2024. aasta aprillis andmekaitseasju läbivaatavasse kohtusse üksikisikute huve esindama kaks eriadvokaadi – juristi, kellel on eksperditeadmised nii eraelu puutumatuse kui ka riikliku julgeoleku valdkonnas. Läbivaatamiskoosolekul kinnitati, et kõik kohtunikud ja eriadvokaadid on läbinud rangeima julgeolekukontrolli ning seetõttu on neil andmekaitseasju läbivaatava kohtu ülesannete täitmisel juurdepääs salastatud materjalidele. Andmekaitseasju läbivaatav kohus oli avaldanud ka korduma kippuvad küsimused, mis annavad rohkem teavet tema rolli, sõltumatuse ja toimimise kohta[82].

Kaebuste menetlemise kohta võttis riikliku luurejuhi büroo 6. detsembril 2022 vastu luureühenduse suunise 126, millega reguleeritakse üksikasjalikult kaebuste uurimise ja lahendamise protsessi eri aspekte (tähtaegade kehtestamine, turvaliste elektrooniliste teabehoidlate ja sidekanalite loomine, nõue, et kodanikuvabaduste kaitse ametnik ja luureühenduse üksused teeksid õiguskaitsemehhanismi iga-aastase läbivaatamise raames

[79] Vt kaitse piisavuse otsuse põhjendused 176–194.

[80] https://www.justice.gov/opa/pr/attorney-general-merrick-b-garland-announces-judges-data-protection-review-court.

[81] Korralduse 14086 paragrahvi 3 punkti d alapunkt A.

[82] https://www.justice.gov/opcl/dprc-resources.

eraelu puutumatuse ja kodanikuvabaduste järelevalve komisjoniga koostööd jne)[83]. Seda suunist kohaldatakse kogu USA luureühenduses ja seda on täiendatud sisemenetlustega, mille on vastu võtnud luureasutused oma koostöö kohta riikliku luurejuhi büroo kodanikuvabaduste kaitse ametnikuga kaebuse menetlemisel (nt turvalise andmehoidla väljatöötamine kaebuste ja neile vastavate dokumentide jagamiseks ning turvaline teabevahetus asjaomaste asutuste vahel). Andmekaitseasju läbivaatav kohus annab lähikuudel välja ka üksikasjalikumad eeskirjad kaebuste menetlemise ja muude menetluslike aspektide kohta.

Euroopa Liidus ja Ameerika Ühendriikides on võetud mitmeid lisameetmeid, et teavitada üldsust ning hõlbustada kaebuste esitamist ja menetlemist. Nende hulka kuuluvad Euroopa Andmekaitsenõukogu vastu võetud teatis uue õiguskaitsemehhanismi kohta,[84] kaebuse näidisvorm (mille kõik andmekaitseasutused tõlgivad oma riigikeelde ja avaldavad)[85] ning töökord, millega reguleeritakse riiklike järelevalveasutuste ja Euroopa Andmekaitsenõukogu sekretariaadi koostööd[86]. Riikliku luurejuhi büroo avaldas ka korduma kippuvad küsimused ja teabelehe uue õiguskaitsemehhanismi kohta ning tegeles üldsuse teadlikkuse suurendamisega[87].

Lisaks on Euroopa Andmekaitsenõukogu ja asjaomased USA ametiasutused viimase aasta jooksul teinud tihedat koostööd mitmes tegevusvaldkonnas. Nagu läbivaatamiskoosolekul kinnitati, võtsid nad kasutusele krüpteeritud sidekanali, et edastada kaebusi ELi liikmesriikide ametiasutustelt Euroopa Andmekaitsenõukogu sekretariaadile, Euroopa Andmekaitsenõukogu sekretariaadilt riikliku luurejuhi büroo kodanikuvabaduste kaitse ametnikule ning justiitsministeeriumi eraelu puutumatuse ja kodanikuvabaduste ametile, aga ka riikliku luurejuhi büroo kodanikuvabaduste kaitse ametniku ja teiste USA ametiasutuste (nt andmekaitseasju läbivaatav kohus) vahel. Lisaks selgitas riikliku luurejuhi büroo kodanikuvabaduste kaitse ametnik, et kaebuste menetlemisel on kehtestatud täiendavad sisemenetlused, mis puudutavad luureasutuste koostööd riikliku luurejuhi büroo kodanikuvabaduste kaitse ametnikuga.

Eraelu puutumatuse ja kodanikuvabaduste amet, kes pakub andmekaitseasju läbivaatavale kohtule haldustuge, teatas ka, et kohtul on oma sihtotstarbeline eelarverida ja tal on oma ülesannete täitmiseks vajalikud ruumid ühes turvaliste arvutite, sülearvutite, telefonide ja muu sellisega. Nagu on nõutud korraldusega 14086, on kaubandusministeerium võtnud vajalikud meetmed, sealhulgas loonud krüpteeritud sidekanali suhtluseks riikliku luurejuhi büroo kodanikuvabaduste kaitse ametnikuga, et registreerida andmed kõigi saadud vastuvõetavate kaebuste kohta. Kaubandusministeerium võtab korrapäraselt ühendust riikliku luurejuhi büroo kodanikuvabaduste kaitse ametnikuga, et selgitada välja, kas konkreetse kaebusega seotud teabe salastatus on kustutatud. Kui see on kustutatud, teavitab kaubandusministeerium sellest asjaomast isikut, et tal oleks võimalik sellisele teabele juurde pääseda.

---

[83] https://www.dni.gov/files/documents/ICD/ICD_126-Implementation-Procedures-for-SIGINT-Redress-Mechanism.pdf.

[84] https://www.edpb.europa.eu/our-work-tools/our-documents/other-guidance/information-note-data-protection-framework-redress_en.

[85] https://www.edpb.europa.eu/our-work-tools/our-documents/other-guidance/template-complaint-form-us-office-director-national_en.

[86] https://www.edpb.europa.eu/our-work-tools/our-documents/other-guidance/rules-procedure-data-protection-framework-redress_en.

[87] https://www.dni.gov/files/CLPT/documents/Fact_Sheets/The_Role_of_the_ODNI_CLPO_FAQs.pdf ja https://www.dni.gov/files/CLPT/documents/Fact_Sheets/Data_Privacy_Framework.pdf.

Läbivaatamiskoosoleku ajal ei olnud ELi järelevalveasutused saanud ühtegi kaebust ja seetõttu ei olnud uut õiguskaitsemehhanismi veel kasutatud.

3. KOKKUVÕTE

Esimese läbivaatamise käigus kogutud teabe põhjal järeldab komisjon, et USA ametiasutused on kehtestanud vajalikud struktuurid ja menetlused, et tagada andmekaitseraamistiku tulemuslik toimimine. Komisjon hindab kõrgelt USA ametiasutustega tehtud väga head koostööd läbivaatamise elluviimisel.

Esimese läbivaatamise käigus kontrolliti praegu loomulikult eelkõige, kas kõik raamistiku toimimise elemendid on paigas, kuid nii kinnituse saanud ettevõtjate poolse andmetöötluse suhtes kui ka avaliku sektori asutuste juurdepääsul andmetele kohaldatavate kaitsemeetmete praktilise kohaldamise kogemused on paratamatult piiratud, sest möödunud on vaid üks tegevusaasta. Seepärast jälgib komisjon lähikuudel ja -aastatel tähelepanelikult asjaomaseid suundumusi, pöörates erilist tähelepanu 1) eraelu puutumatuse ja kodanikuvabaduste järelevalve komisjoni eelseisvatele aruannetele korralduse 14086 rakendamise ja signaaliluuretegevuse õiguskaitsemehhanismi, eelkõige andmekaitseasju läbivaatava kohtu toimimise kohta; 2) FISA paragrahvi 702 võimalikele edasistele muudatustele ning 3) eraelu puutumatuse ja kodanikuvabaduste järelevalve komisjoni liikmete määramisele ja ametisse nimetamisele, et täita tulevasi vabu ametikohti.

Lisaks peab komisjon jätkuva ja tulemusliku toimimise tagamiseks oluliseks järgmist:

- nagu läbivaatamiskoosolekul teatati, kasutab kaubandusministeerium täielikult ära andmekaitseraamistikuga ette nähtud vahendeid, et jälgida põhimõtete järgimist ettevõtjate poolt ja avastada valeväiteid osalemise kohta;
- föderaalne kaubanduskomisjon arendab edasi ennetavat lähenemisviisi uurimisele ja selle tagamisele, et andmekaitseraamistiku kohaselt kinnitatud ettevõtjad andmekaitseraamistiku põhimõtteid täidaksid, ning
- kaubandusministeerium, föderaalne kaubanduskomisjon ja ELi andmekaitseasutused töötavad välja ühised suunised andmekaitseraamistiku põhimõtete põhinõuete kohta, nt personaliandmete ja andmete edasisaatmise kohta.

Võttes arvesse läbivaatamise tulemusi ja nagu on ette nähtud kaitse piisavuse otsuse põhjenduses 211, peab komisjon asjakohaseks teha järgmine perioodiline läbivaatamine kolme aasta pärast. Selleks ajaks peaks olema andmekaitseraamistiku praktilisel kohaldamisel kogunenud rohkem kogemusi ja peaks olema võimalik võtta arvesse eespool nimetatud tulevasi muudatusi. Kaitse piisavuse otsuse artikli 3 lõike 4 kohaselt konsulteerib komisjon seepärast tulevaste läbivaatamiste perioodilisuse küsimuses Euroopa Andmekaitsenõukogu ja isikuandmete kaitse üldmääruse artikli 93 lõike 1 alusel loodud komiteega.