EUROOPAN
KOMISSIO

Bryssel 9.10.2024
COM(2024) 451 final

KOMISSION KERTOMUS EUROOPAN PARLAMENTILLE JA NEUVOSTOLLE

EU:n ja Yhdysvaltojen tietosuojakehyksestä annetun tietosuojan riittävyyttä koskevan päätöksen toiminnan ensimmäisestä määräaikaistarkastelusta

1. ENSIMMÄINEN MÄÄRÄAIKAISTARKASTELU – TAUSTA, VALMISTELU JA PROSESSI

Komissio totesi 10. heinäkuuta 2023 antamassaan päätöksessä[1] (tietosuojan riittävyyttä koskeva päätös), että EU:n ja Yhdysvaltojen tietosuojakehys tarjoaa tietosuojan riittävän tason henkilötiedoille, jotka siirretään EU:sta Yhdysvalloissa sijaitseville organisaatioille. Tietosuojan riittävyyttä koskevassa päätöksessä edellytetään, että komissio suorittaa määräaikaistarkasteluja ja että ensimmäinen tarkastelu suoritetaan vuoden kuluessa päivästä, jona tietosuojan riittävyyttä koskeva päätös on annettu tiedoksi jäsenvaltioille. Tämä kertomus saattaa päätökseen tämän ensimmäisen tarkastelun.

Tämä ensimmäinen tarkastelu on tehty uuden kehyksen ensimmäisen toimintavuoden jälkeen. Kuten tietosuojan riittävyyttä koskevan päätöksen johdanto-osan 211 kappaleessa edellytetään, siinä keskityttiin tarkistamaan, onko kaikki kehyksessä määrätyt osatekijät pantu täytäntöön ja toimivatko ne tehokkaasti. Tarkastelu kattoi kaikki kehyksen toimintaan liittyvät näkökohdat, ja siinä otettiin huomioon myös tietosuojan riittävyyttä koskevan päätöksen hyväksymisen jälkeen tapahtunut oikeudellinen kehitys.

Komissio valmistautui tarkasteluun keräämällä tietoa asiaan liittyviltä sidosryhmiltä, varsinkin kansalaisjärjestöiltä[2], joilla on asiantuntemusta digitaalisista oikeuksista ja tietosuojasta, tietosuojakehyksen mukaisesti varmennetuilta organisaatioilta niiden toimialajärjestöjen[3] kautta sekä kehyksen täytäntöönpanoon osallistuvilta Yhdysvaltojen viranomaisilta. Lisäksi komissio on kerännyt palautetta suurelta yleisöltä Kerro mielipiteesi -portaalissa esitetyn kannanottopyynnön[4] avulla.

Washingtonissa järjestettiin 18. ja 19. heinäkuuta 2024 tarkastelukokous, jonka avasivat oikeus- ja kuluttaja-asioista vastaava komission jäsen Didier Reynders ja Yhdysvaltojen kauppaministeri Gina Raimondo.[5]

---

[1] Komission täytäntöönpanopäätös (EU) 2023/1795, annettu 10 päivänä heinäkuuta 2023, Euroopan parlamentin ja neuvoston asetuksen (EU) 2016/679 nojalla EU:n ja Yhdysvaltojen tietosuojakehyksen tarjoaman tietosuojan tason riittävyydestä.

[2] Komissio lähetti kyselylomakkeen yhdeksälle kansalaisjärjestölle (Human Rights Watch, Yhdysvaltain kansalaisvapausliitto, Consumer Federation of America, Center for Digital Democracy, New America Open Technology Institute, Access Now, Electronic Frontier Foundation, Electronic Privacy Information Center ja Center for Democracy and Technology). Kyselyssä keskityttiin Yhdysvaltojen oikeudellisen kehyksen asiaan liittyvään kehitykseen, valvonta- ja täytäntöönpanomekanismeihin sekä oikeussuojamekanismien toimintaan. Komission yksiköt ja Euroopan tietosuojaneuvoston edustajat tapasivat näitä kansalaisjärjestöjä myös verkossa 9. heinäkuuta 2024.

[3] Komissio lähetti kyselylomakkeen yhdeksälle toimialajärjestölle (Software & Information Industry Association, Yhdysvaltojen kauppakamari, Information Technology Industry Council, Software Alliance, Centre for Information Policy Leadership, Interactive Advertising Bureau, United States Council for International Business, Computer and Communications Industry Association ja Engine). Kyselyssä keskityttiin muun muassa tietosuojakehyksen mukaisesti varmennettujen yritysten kokemuksiin, erityisesti varmennusprosessiin, tietosuojakehyksen periaatteiden noudattamiseksi toteutettuihin toimiin ja yksityishenkilöiden pyyntöjen ja valitusten käsittelymekanismeihin.

[4] Saatuun palautteeseen voi tutustua seuraavan linkin kautta: 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_fi.

[5] Tarkastelukokous eteni aihepiireittäin. Kunkin esityslistan kohdan esitteli ensin lyhyesti asiasta vastaava Yhdysvaltojen viranomainen, EU:n edustaja tai organisaatio, minkä jälkeen käsiteltiin yksityiskohtaisesti kysymyksiä ja vastauksia. Ensimmäisenä päivänä käsiteltiin kehyksen kaupallisia näkökohtia (eli

EU:n puolelta tarkastelun suorittivat Euroopan komission oikeus- ja kuluttaja-asioiden pääosaston edustajat, viisi Euroopan tietosuojaneuvoston nimeämää edustajaa, jotka olivat peräisin eri kansallisista tietosuojaviranomaisista, ja Euroopan tietosuojavaltuutettu.[6] Yhdysvaltain puolelta tarkasteluun osallistui kauppaministeriön, ulkoasiainministeriön, liittovaltion kauppakomission, liikenneministeriön, kansallisen tiedustelujohtajan toimiston (ODNI), oikeusministeriön ja tiedusteluyhteisön valvontaviranomaisen edustajia sekä yksityisyyden suojan ja kansalaisvapauksien valvonnasta vastaavan lautakunnan (PCLOB) jäseniä. Lisäksi riippumattomia riitojenratkaisupalveluja tarjoavien organisaatioiden ja American Arbitration Association -yhdistyksen edustajat antoivat tietoa niiden kannalta merkityksellisten tarkastelutilaisuuksien aikana. Tarkasteluun saatiin tietoa myös muutamilta tietosuojakehyksen mukaisesti varmennetuilta organisaatioilta, jotka kertoivat siitä, miten yritykset noudattavat kehyksessä asetettuja vaatimuksia.

Komissio on hyödyntänyt kertomuksen laatimisessa myös julkisesti saatavilla olevaa aineistoa, kuten tuomioistuimien päätöksiä, Yhdysvaltojen asiaankuuluvien viranomaisten täytäntöönpanosääntöjä ja -menettelyjä, kansalaisjärjestöjen raportteja ja tutkimuksia, tietosuojakehyksen mukaisesti varmennettujen yritysten avoimuusraportteja, riippumattomien valvontaelinten vuosikertomuksia ja tiedotusvälineiden raportteja.

2. HAVAINNOT

2.1. Kaupalliset näkökohdat

2.1.1. Varmennusprosessi

Jotta yhdysvaltalainen yritys voi vastaanottaa EU:sta tietosuojakehyksen nojalla siirrettyjä henkilötietoja, sen on varmennettava – ja sen jälkeen vuosittain varmennettava uudelleen – Yhdysvaltojen kauppaministeriölle sitoutuvansa tiettyihin tietosuojavaatimuksiin (tietosuojakehyksen periaatteisiin). Varmennus edellyttää, että yritys on liittovaltion kauppakomission tai liikenneministeriön tutkinta- ja täytäntöönpanovallan alainen, sitoutuu julkisesti noudattamaan tietosuojakehyksen periaatteita ja julkistaa tietosuojaperiaatteensa sekä panee nämä vaatimukset kaikilta osin täytäntöön.[7] Ennen kuin kauppaministeriö vahvistaa varmennuksen, se varmistaa, että yritys on täyttänyt kaikki varmennusta koskevat vaatimukset.[8]

Kauppaministeriö selitti tarkastelukokouksessa, että tietosuojakehyksen ensimmäisen toimintavuoden aikana on keskitytty varmennusprosessin käyttöön ottoon. Tähän on liittynyt esimerkiksi asiaan liittyvien tietoteknisten välineiden kehittäminen, menettelyjen päivittäminen, yhteydenpito yrityksiin ja muut tiedotustoimet. Tarkastelukokoukseen mennessä yli 2 800 yritystä oli varmennettu tietosuojakehyksen mukaisesti. Tämä tarkoittaa, että tietosuojakehyksen ensimmäisen toimintavuoden aikana siihen oli antanut varmennuksen useampi yritys kuin aiemmassa Privacy Shield -järjestelyssä[9]. Kauppaministeriön toimittamien

tietosuojakehyksen mukaisesti varmennettuihin yrityksiin sovellettavien vaatimusten soveltamista ja täytäntöönpanoa) ja toisena päivänä kysymyksiä, jotka liittyivät viranomaisten pääsyyn henkilötietoihin.

[6] Komissio ja Euroopan tietosuojaneuvoston edustajat tapasivat 12. kesäkuuta ja 10. heinäkuuta 2024 valmistellakseen tarkastelua, keskustellakseen saaduista tiedoista ja selvittääkseen, mistä asioista oli kerättävä lisätietoja ja mitä asioita oli selvennettävä.

[7] Tietosuojan riittävyyttä koskevan päätöksen liitteessä I oleva I.2 kohta.

[8] Tietosuojan riittävyyttä koskevan päätöksen liite III.

[9] Vastaavana ajanjaksona Privacy Shield -järjestelyyn varmennettuja yrityksiä oli 2 400.

tietojen mukaan 70 prosenttia osallistujista on pk-yrityksiä ja suuri määrä tietosuojakehyksen mukaisesti varmennetuista yrityksistä (47 %) toimii tieto- ja viestintätekniikan alalla. Lisäksi 60 prosenttia yrityksistä on antanut varmennuksen pelkästään muiden kuin henkilöstötietojen osalta, 2,5 prosenttia yrityksistä on antanut varmennuksen pelkästään henkilöstötietojen osalta ja 37,5 prosenttia sekä henkilöstötietojen että muiden kuin henkilöstötietojen osalta.

Kauppaministeriö on ottanut käyttöön tarvittavat menettelyt yritysten hakemusten käsittelemiseksi. Yritysten on toimitettava varmennushakemuksensa tietosuojakehystä koskevalla kauppaministeriön verkkosivustolla (https://www.dataprivacyframework.gov/). Sivustolla on tietoa siitä, miten tietosuojakehykseen liitytään[10] ja mitä velvoitteita yrityksellä on kehyksen nojalla[11]. Kauppaministeriössä toimivan tietosuojakehyksestä vastaavan johtajan vastuulla oleva erityisryhmä vastaa kaikista tietosuojakehyksen johtoon ja hallintoon liittyvistä asioista, varmennusprosessi ja vaatimusten noudattamisen seuranta mukaan luettuina. Kukin hakemus osoitetaan tietylle henkilöstön jäsenelle, joka vastaa kyseisestä yrityksestä koko varmennusprosessin ajan.

Jotta yritykset voivat antaa tietosuojakehyksen mukaisen varmennuksen, ne toimittavat hakemuksen, joka sisältää tietosuojaperiaatteiden luonnoksen. Kauppaministeriö tarkistaa, että se on tietosuojakehyksen asiaan liittyvien vaatimusten mukainen. Kun organisaatiot haluavat varmennuksen saman konsernin eri yksiköille (kuten eri tytäryhtiöille), kauppaministeriö pyytää ja tarkastaa joko kattavat tietosuojaperiaatteet, joissa selkeästi ilmoitetaan kaikki niiden piiriin kuuluvat yksiköt, tai kullekin yksikölle laaditut erilliset tietosuojaperiaatteet. Kauppaministeriö varmistaa myös, että organisaatio on tosiasiassa rekisteröity hakemuksessa ilmoitettuun riippumattomaan muutoksenhakumekanismiin[12]. Kun yritykset ovat valinneet mekanismiksi tietosuojaviranomaisten paneelin (esimerkiksi koska ne käsittelevät henkilöstötietoja), kauppaministeriö tarkistaa, että yritys on suorittanut vaaditut maksut paneelin käyttämiseksi. Tarvittaessa kauppaministeriö tarkistaa myös, että hakija kuuluu liittovaltion kauppakomission tai liikenneministeriön toimivaltaan (ja voi siten liittyä tietosuojakehykseen).

Jos kaikki ehdot täyttyvät, kauppaministeriö ilmoittaa organisaatiolle, että se voi julkaista verkkosivustollaan tietosuojaperiaatteensa, joissa viitataan tietosuojakehykseen. Kun tietosuojaperiaatteet on julkaistu, kauppaministeriö vahvistaa varmennuksen ja lisää yrityksen verkkosivustollaan olevaan tietosuojakehykseen osallistuvien organisaatioiden luetteloon (tietosuojakehyksen osallistujaluettelo). Yritys voi hyödyntää tietosuojakehystä henkilötietojen vastaanottamiseksi EU:sta siitä päivästä lähtien, jona kauppaministeriö merkitsee organisaation kyseiseen luetteloon.[13]

Kuten tarkastelukokouksessa selitettiin, kauppaministeriön tähän mennessä tekemissä tarkastuksissa on hylätty 33 hakemusta, koska ne eivät täyttäneet tietosuojakehyksen vaatimuksia. Yleisesti ottaen kauppaministeriö tekee yhteistyötä yrityksen kanssa mahdollisten puutteiden korjaamiseksi. Jos kauppaministeriö havaitsee puutteita, se ilmoittaa yritykselle, että yrityksen on korjattava puutteet ja että jos yritys ei toimi asetettujen määräaikojen sisällä tai ei muuten anna kauppaministeriön menettelytapojen mukaista omaa varmennusta, yrityksen

[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] Yksityisen sektorin riitojenratkaisumekanismeja, joissa jokaisen henkilön valitukset ja häntä koskevat riidat tutkitaan ja ratkaistaan ripeästi ilman, että henkilölle aiheutuu kuluja.

[13] Tietosuojan riittävyyttä koskevan päätöksen liitteessä I olevan I jakson 3 kohta.

katsotaan luopuneen hakemuksesta. Jos ensimmäistä varmennusta ei ole saatettu päätökseen tai muutettu 12 kuukauden kuluessa, kauppaministeriö katsoo, että varmennuksesta on luovuttu.

Kunkin yrityksen vuotuisen uudelleenvarmennuksen määräaika ilmoitetaan tietosuojakehyksen osallistujaluettelossa. Kauppaministeriö muistuttaa yrityksiä uudelleenvarmennuksen hakemisesta järjestelmällä, jossa yrityksille lähetetään muistutuksia siitä, että niiden varmennus raukeaa pian. Organisaatioille toimitetaan muistutus kuukausi ennen määräaikaa, kaksi viikkoa ennen määräaikaa ja vielä päivä ennen määräaikaa. Organisaatiot, jotka ovat antaneet varmennuksensa raueta, poistetaan tietosuojakehyksen osallistujaluettelosta. Kuten tietosuojan riittävyyttä koskevan päätöksen liitteessä III kuvataan, kauppaministeriön verkkosivustolla olevassa osiossa on luettelo niistä yhdysvaltalaisista organisaatioista, jotka eivät enää osallistu aktiivisesti tietosuojakehykseen, ja ilmoitetaan syyt, joiden vuoksi kyseiset yritykset on poistettu luettelosta (esimerkiksi varmennuksen raukeaminen tai kehyksestä vetäytyminen). Kun organisaatiot poistetaan tietosuojakehyksen osallistujaluettelosta sen vuoksi, että ne ovat antaneet varmennuksensa raueta, kauppaministeriö ottaa niihin yhteyttä vahvistaakseen, haluavatko ne vetäytyä vai aikovatko ne sen sijaan tehdä uudelleenvarmennuksen. Jälkimmäisessä tapauksessa kauppaministeriö varmistaa, että organisaatio on soveltanut tietosuojakehyksen periaatteita kehyksen puitteissa saatuihin henkilötietoihin sinä aikana, kun sen varmennus oli rauenneena, ja selventää, mitä toimia organisaatio aikoo toteuttaa ratkaistakseen ongelmat, jotka ovat viivyttäneet uudelleenvarmennuksen tekemistä. Kun yritykset ilmoittavat kauppaministeriölle, että ne haluavat vetäytyä tietosuojakehyksestä, niiden on vahvistettava, aikovatko ne palauttaa tai poistaa tietosuojakehyksen perusteella saadut tiedot, säilyttää ne ja jatkaa tietosuojakehyksen periaatteiden soveltamista tällaisiin tietoihin (joka on vahvistettava vuosittain) tai säilyttää ne ja ottaa käyttöön muita suojatoimia (kuten Euroopan komission hyväksymiä vakiosopimuslausekkeita).

Toimialajärjestöiltä ja yrityksiltä saadun palautteen mukaan tietosuojakehyksen mukaisesti varmennetut yritykset ovat toteuttaneet useita toimia varmistaakseen tietosuojakehyksen periaatteiden noudattamisen. Organisaatiot ovat esimerkiksi suorittaneet *muutoksenhaku-, täytäntöönpano- ja vastuuperiaatteen* noudattamiseksi sisäisiä tarkastuksia joko oman varmennuksen tai ulkopuolisen tahon suorittamien arviointien avulla. Tarkastelukokoukseen osallistuneet kahden yksityisellä sektorilla toimivan riippumattoman muutoksenhakumekanismin edustajat selittivät, että mekanismit tarjoavat myös ulkopuolisen tahon suorittamia arviointeja tarkastamalla tietosuojaperiaatteita. Yhden yksityisellä sektorilla toimivan riippumattoman muutoksenhakumekanismin edustaja selitti, että mekanismi tarjoaa myös tarkastuksia ja pistokokeita, jotka voivat koskea esimerkiksi *tiedonsaantiperiaatetta*, *valintaperiaatetta* ja *tietojen edelleen siirtämistä* koskevaa periaatetta. Lisäksi varmennetut yritykset ovat laatineet periaatteiden noudattamista koskevia sisäisiä ohjelmia ja valvontamekanismeja, kouluttaneet työntekijöitä, ottaneet käyttöön mekanismeja, joiden avulla yksilöt voivat käyttää oikeuksiaan, suorittaneet tietosuojaa koskevia vaikutustenarviointeja ja tarkastelleet voimassa olevia sopimuksia uudelleen.

2.1.2. Vaatimusten noudattamisen seuranta, osallistumista koskevat totuudenvastaiset väitteet ja täytäntöönpano

Tietosuojakehyksen nojalla kauppaministeriö vastaa tietosuojakehyksen periaatteiden noudattamisen valvonnasta käyttämällä erilaisia välineitä, kuten viran puolesta (oma-aloitteisesti) tehtäviä tarkastuksia, tapauskohtaisesti tarkastuksia paikan päällä ja noudattamista

koskevia kyselyjä. Tähän sisältyy se, että pyritään havaitsemaan tietosuojakehykseen osallistumista koskevat totuudenvastaiset väitteet ja puuttumaan niihin, muun muassa tekemällä verkkohakuja.[14]

Kauppaministeriö on valvonut tietosuojakehykseen osallistuvien yritysten periaatteiden noudattamista viime vuoden aikana pääasiassa tekemällä tapauskohtaisesti verkkohakuja ja (sosiaalisen) median tarkastuksia. Kauppaministeriö ilmoitti, että se ei ole havainnut tietosuojakehyksen periaatteiden noudattamiseen liittyviä ongelmia tämän ensimmäisen vuoden aikana eikä se ole siirtänyt yhtään yritystä koskevaa tapausta liittovaltion kauppakomission tai liikenneministeriön käsiteltäväksi mahdollisia lainvalvontatoimia varten. Se on myös perustanut erityisen yhteyspisteen helpottamaan yhteistyötä tietosuojaviranomaisten kanssa ja ottamaan vastaan yksityishenkilöiden tekemiä valituksia ja muilta viranomaisilta (esimerkiksi tietosuojaviranomaisilta tai liittovaltion kauppakomissiolta) siirrettyjä tapauksia. Yhteyspisteelle ei ole kuitenkaan kuluneen vuoden aikana siirretty tapauksia eikä tehty valituksia. Tietosuojakehyksen ensimmäisen toimintavuoden aikana keskityttiin kehyksen ja varmennusprosessin käyttöönottoon. Kauppaministeriö selitti kuitenkin tarkastelukokouksessa, että se aikoo suorittaa vaatimusten noudattamista koskevia tarkastuksia automatisoidusti, jotta ne voidaan suorittaa järjestelmällisemmin, ja kehittää parhaillaan tähän tarvittavia tietoteknisiä välineitä.

Komissio on samaa mieltä siitä, että kauppaministeriön oli keskitettävä tänä ensimmäisenä vuonna toimensa tietosuojakehyksen ja varmennusprosessin käyttöönottoon. Jatkossa on tärkeää, että kauppaministeriö tehostaa tietosuojakehyksen periaatteiden noudattamisen valvontaa ja tarkastamista. Tämä on tarpeen, jotta voidaan varmistaa, että tietosuojakehyksen noudattaminen pysyy korkealla tasolla, ja havaita lisätoimenpiteitä edellyttävät tapaukset, mukaan lukien mahdolliset totuudenvastaiset väitteet yritysten osallistumisesta tietosuojakehykseen. Tältä osin komissio suhtautuu myönteisesti siihen, että kauppaministeriö vahvisti aikovansa kehittää ja käyttää (automaattisia) välineitä, jotta vaatimusten noudattamiseen liittyvät ongelmat ja totuudenvastaiset väitteet voidaan havaita tehokkaammin ja järjestelmällisemmin. Komissio katsoo myös, että tämän olisi oltava osa kauppaministeriön laajempia toimia, joilla parannetaan sen käytettävissä olevien erilaisten välineiden (kuten paikan päällä tehtävien tarkastusten, periaatteiden noudattamisen tarkastelua koskevien kyselylomakkeiden ja tietopyyntöjen) hyödyntämistä, myös tietosuojakehyksen erityisvaatimusten noudattamisen todentamisessa[15].

Tietosuojakehykseen osallistuvat organisaatiot kuuluvat liittovaltion kauppakomission ja liikenneministeriön toimivaltaan. Tarkastelukokouksessa liikenneministeriö vahvisti, että sillä on käytössä kaikki prosessit asianmukaisten lainvalvontatoimien toteuttamiseksi. Se selitti myös, että tietosuojakehykseen on liittynyt vain muutamia sen toimivaltaan kuuluvia yrityksiä (eli muutamia lipunvälittäjiä, mutta ei lentoyhtiöitä). Liittovaltion kauppakomissio vahvisti, että se tarkastaa kaikissa tietosuojaa koskevissa tutkimuksissaan järjestelmällisesti, onko tietosuojakehystä rikottu. Toistaiseksi liittovaltion kauppakomissiolle ei ole siirretty tapauksia muilta viranomaisilta. Se on saanut muutamia valituksia, joissa mainitaan tietosuojakehys.

[14] Ks. tietosuojan riittävyyttä koskevan päätöksen liite III. Totuudenvastaisista väitteistä on kyse esimerkiksi silloin, kun yritys väittää osallistuvansa tietosuojakehykseen ja joko ei ole koskaan aloittanut varmennusprosessia tai on aloittanut prosessin mutta ei ole saattanut sitä päätökseen tai on antanut varmennuksensa raueta.

[15] Esimerkiksi tietojen edelleen siirtämisen osalta käyttämällä tietosuojakehyksen periaatteen 3 b mukaista mahdollisuutta pyytää yhteenvetoa tai olennaiset osat sisältävää jäljennöstä tietojen edelleen siirtämistä koskevien sopimusten yksityisyyden suojaa koskevista määräyksistä.

Kaksi niistä koski kuitenkin yrityksiä, jotka ovat tietosuojakehyksen osallistujaluettelosta poistettujen yritysten luettelossa, kaksi liittyi yrityksiin, jotka eivät osallistuneet kehykseen, ja yksi ei koskenut EU:sta siirrettyjä henkilötietoja. Tämän kertomuksen laatimisajankohtana liittovaltion kauppakomissio ei ollut antanut päätöksiä, joissa määrätään tietosuojakehykseen liittyviä täytäntöönpanotoimia. Se kuitenkin vahvisti, että useita tietosuojakehyksen mukaisesti varmennettuja yrityksiä tutkitaan parhaillaan.

Komissio on tyytyväinen siihen, että liittovaltion kauppakomissio tarkastaa tietosuojaa koskevissa tutkimuksissaan järjestelmällisesti, onko tietosuojakehystä rikottu. Tietosuojakehyksen jatkuva tehokkuus riippuu sen vankasta täytäntöönpanosta. Näin ollen odotetaan, että liittovaltion kauppakomissio käyttää edelleen kehyksen mukaisia tutkintavaltuuksiaan, muun muassa toteuttamalla proaktiivisesti tehotarkastuksia, joissa keskitytään tiettyjen tietosuojakehyksen vaatimusten noudattamiseen ja/tai tiettyihin toimialoihin.

2.1.3. Valitusten käsittely

Tietosuojakehys tarjoaa EU:n alueella asuville henkilöille erilaisia mahdollisuuksia muutoksenhakuun tapauksissa, joissa varmennetut organisaatiot eivät noudata tietosuojakehyksen periaatteita.[16] Henkilöt voivat esimerkiksi pyrkiä riitojenratkaisuun ottamalla suoraan yhteyttä tietosuojakehykseen osallistuvaan organisaatioon, jonka on toimitettava vastaus asianomaiselle henkilölle 45 päivän kuluessa. Henkilöt voivat myös esittää valituksen riippumattomalle muutoksenhakumekanismille, jonka organisaatio on nimittänyt tutkimaan ja ratkaisemaan valitukset. Tapauksen mukaan tämä mekanismi voi olla joko vaihtoehtoinen riitojenratkaisuelin tai tietosuojaviranomainen[17]. Viimesijaisena keinona rekisteröidyt voivat turvautua EU:n ja Yhdysvaltojen tietosuojakehyksen paneelin sitovaan välimiesmenettelyyn, jos heidän valitustaan ei ole ratkaistu tyydyttävällä tavalla minkään muun saatavilla olevan oikeussuojamekanismin avulla.

2.1.3.1. Valitusten käsittely yrityksissä

Toimialajärjestöiltä ja yrityksiltä komission lähettämiin kyselylomakkeisiin saatujen vastausten mukaan tietosuojakehyksen mukaisesti varmennetut yritykset ovat saaneet hyvin vähän – jos lainkaan – valituksia yksityishenkilöiltä tietosuojakehyksen periaatteiden noudattamatta jättämisestä. Yritykset ovat kuitenkin ottaneet käyttöön erilaisia mekanismeja ja välineitä, joiden avulla henkilöt voivat käyttää oikeuksiaan ja tehdä valituksia, muun muassa verkkopohjaisten lomakkeiden välityksellä, sähköpostitse ja puhelimitse.

2.1.3.2. *Riippumattomat muutoksenhakumekanismit*

Tarkastelukokouksen aikana saadun palautteen ja toimialajärjestöjen toimittamien tietojen mukaan riippumattomiin muutoksenhakumekanismeihin on tehty hyvin vähän valituksia. Yritykset ovat valinneet riippumattomiksi muutoksenhakumekanismeiksi muun muassa seuraavia toimijoita: BBB National Programs, JAMS, TRUSTe ja VeraSafe. Tietosuojakehyksessä edellytetään, että riippumattomat muutoksenhakumekanismit julkaisevat vuosittain kertomuksen, jossa esitetään niiden riitojenratkaisupalvelujen käyttöä

[16] Ks. tietosuojan riittävyyttä koskevan päätöksen 2.4 jakso.

[17] Tietosuojakehykseen osallistuvat organisaatiot ovat velvollisia tekemään yhteistyötä tietosuojaviranomaisten kanssa näiden tutkiessa ja ratkaistessa valituksia, jotka koskevat työsuhteen yhteydessä kerättyjen henkilöstötietojen käsittelyä tai kun asianomainen organisaatio on vapaaehtoisesti suostunut tietosuojaviranomaisten valvontaan.

koskevat kootut tilastot. Tämän kertomuksen antamisajankohtana kaikki asianomaiset riippumattomat muutoksenhakumekanismit olivat julkaisseet vuosittaisen kertomuksensa[18].

Lisäksi BBB ja VeraSafe esittelivät tarkastelukokouksessa yksityiskohtaisesti viime vuoden toimintaansa. Ne ilmoittivat, että niiden palvelut valinneiden yritysten määrä oli lisääntynyt aiempiin kehyksiin verrattuna, ja mainitsivat saaneensa jonkin verran valituksia, joista valtaosaa ei tosin voitu ottaa käsiteltäväksi. Esimerkiksi BBB vastaanotti 87 valitusta EU:n kansalaisilta, joista vain kaksi voitiin ottaa käsiteltäväksi. BBB selitti, että valitukset käsitellään keskimäärin viiden työpäivän kuluessa, mutta näiden kahden valituksen käsittely lopulta lopetettiin, koska henkilöt eivät vastanneet yhteydenottoihin. VeraSafe vastaanotti 26 valitusta, joista kuusi voitiin ottaa käsiteltäväksi. Kaksi tietoihin pääsyä ja tietojen poistamista koskevaa valitusta ratkaistiin. Kahden valituksen käsittely on edelleen kesken, ja kahden käsittely joko raukesi tai lopetettiin, koska henkilö ei vastannut yhteydenottoihin. Molemmat riippumattomat muutoksenhakumekanismit selittivät, että ne pyrkivät vastaamaan valituksiin valituksen esittäneen henkilön kielellä.

Tietosuojakehykseen osallistuvien yritysten, jotka käsittelevät EU:sta siirrettyjä henkilöstötietoja, on valittava kyseisten tietojen osalta riippumattomaksi muutoksenhakumekanismiksi EU:n tietosuojaviranomaiset. Tietosuojakehykseen osallistuva yritys voi kuitenkin vapaaehtoisesti valita EU:n tietosuojaviranomaiset riippumattomaksi muutoksenhakumekanismiksi myös muuntyyppisten tietosuojakehyksen perusteella siirrettävien henkilötietojen osalta. Tarkastelun toteuttamisajankohtana yli puolet tietosuojakehyksen mukaisesti varmennetuista yrityksistä oli valinnut tämän vaihtoehdon[19], mikä on tervetullutta. Euroopan tietosuojaneuvosto on tietosuojan riittävyyttä koskevan päätöksen antamisen jälkeen hyväksynyt EU:n tietosuojaviranomaisten epävirallisen paneelin työjärjestyksen. Paneeli on toimivaltainen antamaan yhdysvaltalaisille organisaatioille sitovia ohjeita yksityishenkilöiden tekemistä, ratkaistavina olevista tietosuojakehykseen liittyvistä valituksista, jotka koskevat EU:sta tietosuojakehyksen puitteissa siirrettyjen tietojen käsittelyä. Paneelin työjärjestyksen[20] mukaan paneeli koostuu tietosuojaviranomaisista, joista yksi toimii johtavana tietosuojaviranomaisena muut toimivat arvioijina. Paneeli antaa sitovia ohjeita 60 päivän kuluessa tietosuojakehykseen liittyvän valituksen vastaanottamisesta. Euroopan

[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;
PrivacyTrustin tietosuojakehykseen liittyvät palvelut – 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;
Verasafe – https://verasafe.com/wp-content/uploads/2020/06/VeraSafe-DPF-Dispute-Resolution-Program-Annual-Report-2024.pdf.

[19] Pian tarkastelukokouksen jälkeen tietosuojakehyksen verkkosivustolla ilmoitettiin, että 2 892 osallistujasta 1 511 oli valinnut EU:n tietosuojaviranomaisen muutoksenhakumekanismikseen.

[20] Euroopan tietosuojaneuvosto hyväksyi 17. huhtikuuta 2024 EU:n tietosuojaviranomaisten epävirallisen paneelin työjärjestyksen EU:n ja Yhdysvaltojen tietosuojakehyksen mukaisesti. Se on saatavilla osoitteessa https://www.edpb.europa.eu/system/files/2024-04/dpf_rules-of-procedure_informal-panel-dpas_en.pdf.

tietosuojaneuvosto on myös julkaissut mallilomakkeen valitusten tietosuojaviranomaisille toimittamista varten[21] sekä tietosuojakehystä koskevia usein kysyttyjä kysymyksiä EU:ssa oleville henkilöille[22] ja yrityksille[23]. Paneeli ei ollut saanut valituksia tarkastelun toteuttamisajankohtaan mennessä.

2.1.3.3. Sitova välimiesmenettely

Kauppaministeriö valitsi sitovan välimiesmenettelyn hallinnoijaksi International Centre for Dispute Resolution -keskuksen (ICDR), joka on American Arbitration Association -yhdistyksen kansainvälinen osasto. Tietosuojan riittävyyttä koskevan päätöksen hyväksymisen jälkeen kauppaministeriö valitsi yhdessä komission kanssa 11 välimiestä[24], joilla on kokemusta tietosuoja-asioista ja jotka tulevat eri taustoista, mukaan lukien välimiesmenettely, oikeuslaitos, tiedeyhteisö ja kansalaisyhteiskunta. Lisäksi on hyväksytty välimiesmenettelysäännöt[25] tietosuojakehyksen paneelia varten ja välimiehiä koskevat käytännesäännöt[26], jotka ovat saatavilla ICDR:n verkkosivustolla. Tarkastelun toteuttamisajankohtana yksikään EU:ssa oleva henkilö ei ollut käynnistänyt välimiesmenettelyä.

2.1.4. Ohjeet, yhteistyö ja tunnettuuden parantaminen

Tietosuojakehyksen voimaantulon jälkeen kauppaministeriö on järjestänyt tietosuojakehyksestä tiedotuskiertueita, -webinaareja ja -seminaareja sekä ollut yhteydessä toimialajärjestöihin ja suoraan yli 3 000 yritykseen. Se on myös julkaissut ohjeita muun muassa yksityishenkilöille sekä EU:n ja Yhdysvaltojen yrityksille[27] suunnattujen usein kysyttyjen kysymysten muodossa. Euroopan tietosuojaneuvosto on puolestaan laatinut valituslomakkeita ja usein kysyttyjä kysymyksiä yksityishenkilöille ja yrityksille. Myös komissio julkaisi tietosuojakehystä koskevia kysymyksiä ja vastauksia koskevan tietosivun tietosuojan riittävyyttä koskevan päätöksen antamisen yhteydessä.[28]

Tarkastelukokouksessa kävi kuitenkin ilmi, että kansalaisille tiedottamiseksi ja yritysten ohjeistamiseksi on tehtävä vieläkin enemmän. Yritysten ja riippumattomien muutoksenhakumekanismien antama palaute ja valitusten hyvin pieni määrä viittaavat siihen, että ihmiset eivät välttämättä aina ole tietoisia oikeuksistaan ja/tai mekanismista, jonka avulla he voivat käyttää oikeuksiaan. Tarkastelukokouksessa kauppaministeriö ilmaisi kiinnostuksensa tehdä yhteistyötä EU:n tietosuojaviranomaisten kanssa, jotta voidaan lisätä EU:ssa olevien henkilöiden tietoisuutta tietosuojakehyksestä. Komissio kannustaa toteuttamaan tällaisia aloitteita ja aikoo myös itse kehittää yksityishenkilöille tiedottamista muun muassa antamalla verkkosivustollaan lisätietoja tietosuojakehyksestä. Se aikoo esimerkiksi lisätä verkkosivustolle linkkejä ja viittauksia Euroopan tietosuojaneuvoston sekä

[21] https://www.edpb.europa.eu/our-work-tools/our-documents/other-guidance/eu-us-data-privacy-framework-template-complaint-form_fi.
[22] https://www.edpb.europa.eu/our-work-tools/our-documents/other-guidance/eu-us-data-privacy-framework-faq-european-individuals_fi.
[23] https://www.edpb.europa.eu/our-work-tools/our-documents/other-guidance/eu-us-data-privacy-framework-faq-european-businesses_fi.
[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] Ks. esimerkiksi 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.

kauppaministeriön ja muiden Yhdysvaltojen viranomaisten antamiin asiaan liittyviin ohjeasiakirjoihin.

Tietosuojakehyksen periaatteita koskevien ohjeiden osalta Euroopan tietosuojaneuvoston edustajat sopivat tarkastelukokouksessa tekevänsä tulevina kuukausina yhteistyötä, jotta voidaan selventää tietosuojakehyksen mukaista henkilöstötietojen käsitettä ja tällaisten tietojen käsittelyyn sovellettavia velvoitteita. Kokouksessa tarkasteltiin eri osatekijöitä, joita näihin ohjeisiin voitaisiin sisällyttää. Ohjeissa voitaisiin esimerkiksi käsitellä tiettyjä käytännön skenaarioita, joissa henkilöstötietoja käsitellään tietosuojakehyksen mukaisesti (esim. pilvipalvelun tarjoajan toimesta), ja selittää, mitä tietosuojakehyksen velvoitteita tällaisissa skenaarioissa sovellettaisiin. Lisäksi ohjeissa voitaisiin ehdottaa, että yritykset, jotka saavat EU:n kansalaisten henkilöstötietoja (mutta eivät välttämättä käytä näitä tietoja työsuhteen yhteydessä), valitsisivat tietosuojaviranomaisten paneelin riippumattomaksi muutoksenhakumekanismikseen. Näin varmistettaisiin, että kyseiset henkilöt voivat ottaa yhteyttä lähellään olevaan viranomaiseen, joka tarvittaessa tuntee paremmin henkilöstötietoihin sovellettavat kansalliset lait.

Lisäksi (myös toimialajärjestöiltä saadun palautteen perusteella) vaikuttaisi hyödylliseltä antaa enemmän ohjeita tietosuojakehyksen vaatimuksista, joita sovelletaan tietojen jatkosiirtämiseen. Kauppaministeriön mukaan olisi myös syytä selvittää, olisiko hyödyllistä antaa tietyille toimialoille lisäohjeita tietosuojakehyksen periaatteiden soveltamisesta niiden toimintaan esimerkiksi terveysalan tutkimuksen ja rahoituspalvelujen alalla.

Komissio pitää myönteisenä, että molemmat osapuolet ovat valmiita laatimaan ohjeita, ja odottaa, että edellä mainittuja aiheita koskeva työ aloitetaan pian.

Yhdysvaltojen viranomaisten ja tietosuojaviranomaisten välisen tietojenvaihdon ja yhteistyön varmistamiseksi on yleisemmin otettu käyttöön useita mekanismeja. Liittovaltion kauppakomissioon ja kauppaministeriöön on esimerkiksi nimetty erityisiä yhteyspisteitä, jotka käsittelevät tietosuojaviranomaisten tiedusteluja ja siirtämiä tapauksia.

2.1.5. Yhdysvaltojen oikeusjärjestelmän asiaan liittyvä kehitys

Yhdysvaltojen oikeudellisessa kehyksessä on tapahtunut tietosuojan riittävyyttä koskevan päätöksen hyväksymisen jälkeen jonkin verran tietosuojaan liittyvää kehitystä lainsäädännön, sääntelyn ja oikeuskäytännön suhteen. Muutokset ovat yleisesti ottaen lähentäneet EU:n ja Yhdysvaltojen lähestymistapoja tiettyihin tietosuojaan liittyviin haasteisiin, muun muassa samankaltaisten oikeudellisten käsitteiden käytön myötä. Tämä kehitys jatkuu osittain edelleen, ja sitä on seurattava jatkossa.

Liittovaltion tasolla presidentti antoi useita toimeenpanoasetuksia, jotka ovat merkityksellisiä henkilötietojen käytön kannalta. Erityisesti voidaan mainita 28. helmikuuta 2024 annettu toimeenpanoasetus 14117[29], jolla kielletään liiketoimet, joihin liittyy tiettyjä arkaluonteisten henkilötietojen ryhmiä (esimerkiksi terveystiedot, biometriset tunnisteet tai genomitieto), tietyissä huolta aiheuttavissa maissa[30] olevien yksikköjen kanssa tai rajoitetaan tällaisia toimia.

[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] Tällaisia maita ovat oikeusministeriön 3. toukokuuta 2024 antamassa etukäteisilmoituksessa (Advance Notice of Proposed Rulemaking) esitetyn ehdotuksen mukaisesti Kiina, Kuuba, Hongkong ja Macao, Iran, Pohjois-Korea ja Venezuela. Ks. https://www.federalregister.gov/documents/2024/03/05/2024-04594/national-security-division-provisions-regarding-access-to-americans-bulk-sensitive-personal-data-and.

Kyseisessä toimeenpanoasetuksessa kehotetaan oikeusministeriä ehdottamaan asetuksia – joita ei ole vielä annettu tämän kertomuksen antamisajankohtana – sen täytäntöönpanon tarkentamiseksi. Lisäksi 30. lokakuuta 2023 annettiin tekoälyä koskeva toimeenpanoasetuksessa 14110[31], jossa pääpainona on turvallisen ja luotettavan tekoälyn kehittäminen. Toimeenpanoasetuksessa edellytetään, että useat liittovaltion virastot laativat tekoälyyn liittyviä turvallisuusnormeja ja ohjeita, myös tekoälyn riskeistä, jotka liittyvät nimenomaisesti tietosuojaan, ja yksityisyyttä suojaavista tekniikoista.

Lainsäädäntötyön osalta voidaan todeta, että kongressissa viime vuosina esitettyjen tietosuojaa koskevien liittovaltion lakien lisäksi 20 Yhdysvaltojen osavaltiota on saattanut heinäkuuhun 2024 mennessä voimaan laaja-alaisia tietosuojalakeja. Ne ovat tulleet voimaan kahdeksassa osavaltiossa: Kalifornia, Colorado, Oregon, Virginia, Connecticut, Utah, Texas ja Florida. Lisäksi 17 Yhdysvaltojen osavaltiota on antanut lainsäädäntöä, joka koskee automaattista käsittelyä (tai ainakin joitakin sen muotoja) ja joka yleisesti ottaen mahdollistaa tietyntyyppisen profiloinnin[32] perustuvan päätöksenteon kieltämisen.

Oikeuskäytännön kehityksen osalta voidaan todeta, että useat kansalaisyhteiskunnan edustajat ovat tuoneet esiin hiljattain (28. kesäkuuta 2024) asiassa *Loper Bright Enterprises v. Raimondo* annetun korkeimman oikeuden tuomion. Tuomio kumoaa aiemman oikeuskäytännön, joka perustuu asiassa *Chevron* esitettyyn puolustukseen ja jonka mukaisesti tuomioistuimet soveltavat periaatetta, jossa ne ottavat huomioon sääntelyviraston kohtuullisen tulkinnan laista tapauksissa, joissa kyseisen viraston täytäntöön panema laki on monitulkintainen. Kansalaisjärjestöt ovat ilmaisseet huolensa tämän korkeimman oikeuden tuomion vaikutuksesta liittovaltion kauppakomission sääntelyvaltaan tietosuoja-asioissa todeten kuitenkin, että tuomion vaikutus liittovaltion kauppakomission täytäntöönpanovaltuuksiin voi olla pieni tai merkityksetön. Liittovaltion kauppakomissio ilmoitti tarkastelukokouksessa, että on vielä liian aikaista sanoa, mitä vaikutuksia tuomiolla tarkalleen ottaen on. Se kuitenkin selitti, että liittovaltion kauppakomission hallinnollisten määräysten antaminen perustuu liittovaltion kauppakomissiota koskevaan lakiin, joka on eri kuin muita hallinnollisia virastoja koskevat lait ja jonka osalta *Chevron*-oikeuskäytäntö oli vähemmän merkityksellinen. Hiljattain annetun tuomion vaikutus voi siis jäädä sen osalta vähäiseksi.

Lisäksi liittovaltion kauppakomissio tiedotti automaattista käsittelyä ja tekoälyä koskevassa lähestymistavassaan viime aikoina tapahtuneesta kehityksestä. Liittovaltion kauppakomissio

---

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

[32] Eri osavaltioissa on eroja siinä, mitä ’profiloinnilla’ tarkoitetaan. Yleisesti ottaen profiloinnilla kuitenkin tarkoitetaan mitä tahansa henkilötietojen automaattista käsittelyä, jossa arvioidaan, analysoidaan tai ennakoidaan tunnistetun tai tunnistettavissa olevan luonnollisen henkilön henkilökohtaisia ominaisuuksia, jotka liittyvät taloudelliseen tilanteeseen, terveyteen, henkilökohtaisiin mieltymyksiin, kiinnostuksen kohteisiin, luotettavuuteen, käyttäytymiseen, sijaintiin tai liikkeisiin. Yleensä kuluttajat voivat kieltäytyä profiloinnista. Seuraavat osavaltiot ovat laatineet profilointia koskevaa lainsäädäntöä: 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, saatettu voimaan 9.5.2024), 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, saatettu voimaan 29.6.2024), Tennessee (Tenn. Code Ann. 47-18-3304 §), Texas (Tex. Bus. & Com. Code Ann. 541.051 §) ja Virginia (Va. Code Ann. 59.1-577 §).

on esimerkiksi antanut muiden täytäntöönpanoviranomaisten kanssa yhteisen lausuman[33] automaattisissa järjestelmissä esiintyvästä syrjinnästä ja vääristymistä sekä toteuttanut useita lainvalvontatoimia, jotka kohdistuvat muun muassa avoimuuteen, automaattisen käsittelyn oikeudenmukaisuuteen ja henkilöiden mahdollisuuksiin riitauttaa tulokset. Tältä osin merkille pantavin tapaus oli liittovaltion kauppakomission maaliskuussa 2024 antama *Rite Aid* -yritystä koskeva päätös[34], jolla kyseistä yritystä kiellettiin käyttämästä kasvojentunnistusteknologiaa turvallisuustarkoituksiin viideksi vuodeksi. Liittovaltion kauppakomissio totesi erityisesti, että *Rite Aid* ei toteuttanut kohtuullisia toimenpiteitä estääkseen virheelliset tulokset ja tiedottaakseen kuluttajille teknologian käytöstä. Yleisemmin liittovaltion kauppakomissio toi tarkastelukokouksessa esiin tämänhetkisiä painopisteitään ja erityisesti osa-alueita, joilla sen mielestä täytäntöönpanotoimien olisi jatkossa oltava proaktiivisempia. Tällaisia osa-alueita ovat muun muassa arkaluonteisten tietojen (esimerkiksi terveystietojen, biometristen tietojen ja geopaikannuksen)[35] suojaaminen, lasten[36] ja alaikäisten suojelu verkossa ja tietoturva[37].

Komissio seuraa edelleen tiiviisti edellä käsiteltyä ja muuta Yhdysvalloissa tapahtuvaa kehitystä, erityisesti mahdollisia toimia kattavan liittovaltion tietosuojalain aikaansaamiseksi ja korkeimman oikeuden viimeaikaisen oikeuskäytännön mahdollista vaikutusta liittovaltion kauppakomission rooliin tietosuoja-asioissa.

Komissio suhtautuu myönteisesti liittovaltion kauppakomission toimittamiin tietoihin sen hiljattain toteuttamista lainvalvontatoimista ja tämänhetkisistä painopisteistä, jotka vastaavat suurelta osin tietosuojan täytäntöönpanon kehityssuuntauksia ja painopisteitä Euroopassa. Liittovaltion kauppakomissio osallistuu myös aktiivisesti komission maaliskuussa 2024[38] käynnistämään verkostoon, joka kokoaa yhteen maita, joista on annettu tietosuojan riittävyyttä koskeva EU:n päätös. Tämän lähentymisen pitäisi edistää tiiviimpää yhteistyötä tietosuojan toteutumisen valvonnasta EU:ssa ja Yhdysvalloissa vastaavien tahojen välillä, erityisesti tietosuojakehyksen toiminnan kannalta olennaisissa asioissa.

2.2. Yhdysvaltojen viranomaisten pääsy EU:n ja Yhdysvaltojen tietosuojakehyksen puitteissa siirrettyihin henkilötietoihin ja näiden tietojen käyttö

Tietosuojan riittävyyttä koskeva päätös sisältää yksityiskohtaisen arvioinnin säännöistä, joita Yhdysvaltojen viranomaisten on noudatettava, kun ne keräävät ja käyttävät EU:sta

[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.

[35] Ks. esimerkiksi liittovaltion kauppakomission X-Modelle hiljattain antama määräys arkaluonteisten sijaintitietojen myynnistä ja jakamisesta (https://www.ftc.gov/system/files/ftc_gov/pdf/X-ModeSocialDecisionandOrder.pdf) ja Monumentille antama määräys arkaluonteisten terveystietojen luovuttamisesta kolmansille osapuolille markkinointia varten (https://www.ftc.gov/system/files/ftc_gov/pdf/MonumentOrderFiled.pdf).

[36] Liittovaltion kauppakomissio on esimerkiksi hiljattain ilmoittanut, että sen tutkinnan seurauksena TikTokia ja sen emoyhtiötä Bytedancea vastaan käynnistetään oikeudenkäynti väitetystä lasten yksityisyyden suojaa koskevan lain rikkomisesta. Väitteiden mukaan kumpikaan yrityksistä ei noudattanut vaatimusta, jonka mukaan vanhemmille on ilmoitettava ja heidän suostumuksensa on saatava ennen alle 13-vuotiaiden lasten henkilötietojen keräämistä ja käyttämistä (https://www.ftc.gov/news-events/news/press-releases/2024/08/ftc-investigation-leads-lawsuit-against-tiktok-bytedance-flagrantly-violating-childrens-privacy-law).

[37] Ks. yhteenveto hiljattaisista lainvalvontatoimista liittovaltion kauppakomission vuoden 2023 tietosuojaa ja tietoturvaa koskevassa päivityksessä: https://ec.europa.eu/commission/presscorner/detail/fi/mex_24_1307.

[38] Ks. https://ec.europa.eu/commission/presscorner/detail/fi/IP_23_2413. Maaliskuun 2024 kokouksen tuloksena päätettiin järjestää useita teemakohtaisia tilaisuuksia. Ensimmäinen järjestettiin heinäkuussa 2024, ja siinä käsiteltiin sellaisten välineiden kehittämistä, jotka voivat tukea pk-yrityksiä tietosuojalakien noudattamisessa.

tietosuojakehyksen mukaisesti varmennettuihin yrityksiin siirrettyjä henkilötietoja, erityisesti lainvalvontatarkoituksia ja kansalliseen turvallisuuteen liittyviä tarkoituksia varten. Yhdysvaltojen viranomaiset vahvistivat tarkastelukokouksessa, että tietoihin pääsyyn lainvalvontatarkoituksia tai sääntelyn tarkoituksia varten sovellettavassa oikeudellisessa kehyksessä ei ole tapahtunut muutoksia tietosuojan riittävyyttä koskevan päätöksen antamisen jälkeen tietosuojakehyksen ensimmäisen toimintavuoden aikana. Tästä syystä jäljempänä esitetyt havainnot koskevat vain kansalliseen turvallisuuteen liittyvissä asioissa tapahtunutta kehitystä.

Tietosuojan riittävyyttä koskevassa päätöksessä esitetyt johtopäätökset tiedusteluelinten pääsystä tietoihin perustuvat analyysiin ehdoista ja rajoituksista, joita sovelletaan signaalitiedustelutoimintaan useiden asiaan liittyvien oikeusperustojen nojalla, erityisesti ulkomaantiedustelun valvontaa koskevan lain (Foreign Intelligence Surveillance Act, FISA-laki) 702 §:n ja toimeenpanoasetuksen 12333[39] nojalla sellaisena kuin niitä on täydennetty ja vahvistettu Yhdysvaltojen signaalitiedustelutoiminnan suojatoimien tehostamisesta 7. lokakuuta 2022 annetulla Yhdysvaltojen presidentin toimeenpanoasetuksella 14086 (Enhancing Safeguards for United States Signals Intelligence). Toimeenpanoasetuksessa 14086 vahvistettuja suojatoimia sovelletaan kaikkeen Yhdysvaltojen signaalitiedustelutoimintaan riippumatta siitä, mihin toimivaltaan tiedustelutoiminta perustuu ja missä sitä toteutetaan, ja ne suojaavat ei-yhdysvaltalaisten (myös eurooppalaisten) henkilöiden tietoja.[40] Toimeenpanoasetuksella 14086 perustettiin myös uusi oikeussuojamekanismi, jonka avulla EU:ssa olevat yksityishenkilöt voivat vedota näihin sitoviin suojatoimiin ja vaatia niiden täytäntöönpanoa.

Seuraavissa kohdissa kuvaillaan toimenpiteitä, joita Yhdysvaltojen viranomaiset ovat toteuttaneet tietosuojan riittävyyttä koskevan päätöksen antamisen jälkeen toimeenpanoasetuksen 14086 noudattamiseksi, ja edellä mainitussa oikeudellisessa kehyksessä tapahtunutta asiaan liittyvää kehitystä.

2.2.1. Yhdysvaltojen oikeudellisen kehyksen asiaan liittyvä kehitys

2.2.1.1. Toimeenpanoasetuksen 14086 täytäntöönpano tiedusteluelimissä

Toimeenpanoasetuksella 14086 käyttöön otetut rajoitukset ja suojatoimet täydentävät FISA-lain 702 §:ssä ja toimeenpanoasetuksessa 12333 säädettyjä rajoituksia ja suojatoimia. Ne sitovat kaikkia tiedusteluelimiä, ja kukin elin on ottanut käyttöön käytänteitä ja menettelyjä niiden toteuttamiseksi käytännössä.

Osana ensimmäistä tarkastelua Yhdysvaltojen viranomaiset vahvistivat, että toimeenpanoasetukseen 14086 ei ole tehty muutoksia sen hyväksymisen jälkeen. Lisäksi viranomaiset selvensivät, että Yhdysvaltain presidentti ei ole käyttänyt toimeenpanoasetuksen 14086 2 §:n b momentin i kohdan B alakohdassa ja 2 §:n b momentin ii kohdan C alakohdassa tarkoitettuja valtuuksia päivittääkseen luetteloa legitiimeistä tavoitteista, joihin signaalitiedustelutiedoilla voidaan pyrkiä, tai luetteloa tarkoituksista, joihin valikoimattomasti

[39] Muita toimenpiteitä, joita FISA-lain nojalla voidaan toteuttaa EU:sta siirrettävien tietojen osalta, ovat yksilöllinen sähköinen valvonta (FISA 105 §), fyysinen etsintä (FISA 302 §), lähtevän ja saapuvan teleliikenteen tietojen tallennusjärjestelmien (pen registers, trap and trace devices) käyttö (FISA 402 §) ja liiketoimintatietojen kerääminen tietyistä yrityksistä (yleisistä kuljetusliikkeistä, julkisista majoituspalveluista, ajoneuvojen vuokrauspalveluista tai fyysisistä varastotiloista, FISA 501 §). Näitä eri oikeusperustoja analysoidaan yksityiskohtaisesti tietosuojan riittävyyttä koskevassa päätöksessä (johdanto-osan 142–152 kappaleessa).

[40] Lisätietoja on tietosuojan riittävyyttä koskevan päätöksen 3.2.1.2 jaksossa.

kerättyjä tietoja voidaan käyttää[41]. Jotta voitiin määrittää tarkemmin tiedustelun painopisteet, joita varten signaalitiedustelutietoja voidaan tosiasiassa kerätä, toimeenpanoasetuksessa 14086 otettiin käyttöön erityinen menettely. Sen mukaan on erityisesti kuultava kansallisen tiedustelujohtajan toimiston alaisuudessa toimivaa kansalaisvapauksien suojelusta vastaavaa virkamiestä (ODNI CLPO) arvioitaessa kunkin painopisteen osalta, 1) edistääkö painopiste yhtä tai useampaa toimeenpanoasetuksessa lueteltua legitiimiä tavoitetta, 2) onko painopiste sellainen, että sitä ei ole suunniteltu eikä sen odoteta johtavan signaalitiedustelutietojen keräämiseen toimeenpanoasetuksessa kiellettyä tavoitetta varten ja 3) onko painopiste vahvistettu sen jälkeen, kun on otettu asianmukaisesti huomioon kaikkien henkilöiden yksityisyyden suoja ja kansalaisvapaudet heidän kansalaisuudestaan tai asuinpaikastaan riippumatta.[42] ODNI CLPO vahvisti tarkastelukokouksessa, että hän oli arvioinut kansallisen tiedusteluviraston johtajan vuoden 2023 kansallisia tiedustelun painopisteitä koskevassa kehyksessä ehdottamat painopisteet, todennut, että ne täyttivät edellä mainitut vaatimukset, ja toimittanut päätelmänsä kansallisen tiedusteluviraston johtajalle, joka puolestaan toimitti painopisteet presidentin vahvistettaviksi. ODNI CLPO järjesti myös koulutusta toimeenpanoasetuksen 14086 vaatimuksista tiedustelun painopisteiden laatimiseen osallistuvalle tiedusteluyhteisölle.

Lisäksi Yhdysvaltojen viranomaiset ovat viime vuonna toteuttaneet käytännön toimia toimeenpanoasetuksen 14086 panemiseksi täytäntöön päivittäisessä toiminnassaan. Tiedusteluelimet ovat erityisesti ottaneet käyttöön muita toimeenpanoasetuksen soveltamista koskevia sisäisiä toimintakäytäntöjä ja ohjeita, esimerkiksi sisäisiä prosesseja (kuten sisäisiä lupavaatimuksia tai dokumentoitu pääsynvalvonta, jotta tietoihin saavat pääsyn vain asianmukaisesti koulutetut henkilöt, joiden tehtävä edellyttää sitä), joilla varmistetaan, että tarpeellisuutta ja oikeasuhteisuutta koskevia toimeenpanoasetuksen vaatimuksia noudatetaan sekä kohdennetun että valikoimattoman tietojenkeruun yhteydessä.[43] Lisäksi eri tiedusteluelinten (kuten kansallisen turvallisuusviraston, CIA:n ja FBI:n) henkilöstölle on tarjottu toimeenpanoasetusta 14086 koskevaa koulutusta, mukaan lukien ODNI CLPO:n järjestämät vuosittaiset ja tapauskohtaiset koulutustilaisuudet sekä pakolliset koulutukset kaikille ODNIssa aloittaville uusille työntekijöille.

Komissio suhtautuu myönteisesti eri toimenpiteisiin, jotka on otettu käyttöön toimeenpanoasetuksen 14086 panemiseksi täytäntöön ja sen noudattamisen varmistamiseksi. Kun toimeenpanoasetuksen suojatoimien käytännön soveltamisesta on saatu enemmän kokemusta, komissio arvostaisi mahdollisuutta keskustella tulevissa tarkasteluissa konkreettisista esimerkeistä siitä, miten toimeenpanoasetusta sovelletaan käytännössä (asiaan liittyvät luottamuksellisuusnäkökohdat huomioon ottaen).

2.2.1.2. FISA-lain 702 §:n uusiminen

FISA-lain 702 §:n mukaan ulkomaantiedustelutietojen hankinnan kohteena voi olla ei-yhdysvaltalaisia henkilöjä, joiden voidaan kohtuudella uskoa olevan Yhdysvaltojen ulkopuolella. Tietojen hankkiminen toteutetaan ulkomaantiedustelun valvonnasta vastaavalle

[41] Tällaisia legitiimejä tavoitteita tai tarkoituksia ovat muun muassa suojautuminen vakoilulta, sabotaasilta, salamurhilta tai muulta ulkomaisen hallituksen, järjestön tai henkilön toimesta tai puolesta toteutetulta tiedustelutoiminnalta, terrorismin torjunta, panttivankitilanteet ja henkilöiden pitäminen vankina ulkomaisen hallituksen, järjestön tai henkilön toimesta tai puolesta.

[42] Toimeenpanoasetuksen 14086 2 §:n b momentin iii kohta.

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

tuomioistuimelle (FISC-tuomioistuin) toimitettujen ja sen hyväksymien vuotuisten sertifiointien perusteella. Sertifioinneissa yksilöidään kerättävien ulkomaisten tiedustelutietojen luokat. ODNI ilmoitti 21. heinäkuuta 2023, että FISA-lain 702 §:n nojalla on hyväksytty kolme sertifiointia, jotka kattavat seuraavat ulkomaisten tiedustelutietojen luokat: 1) ulkomaiset hallitukset ja niihin liittyvät yksiköt, 2) terrorismin torjunta ja 3) joukkotuhoaseiden leviämisen estäminen.[44] Sertifiointien on myös sisällettävä FISC-tuomioistuimen hyväksymät kohdentamis- ja minimointimenettelyt[45]. Kohdentaminen toteutetaan pyytämällä, että FISA-laissa vahvistetun sähköisten viestintäpalvelujen tarjoajan määritelmän mukaiset yhdysvaltalaiset yritykset luovuttavat sähköisen viestinnän tiedot tiettyjen valintakriteerien perusteella yksilöityihin viestintävälineisiin (kuten puhelinnumeroon tai sähköpostiosoitteeseen) lähetetyn tai niistä lähetettävän viestinnän osalta. Yhdysvaltojen hallitus on julkaissut useita FISA-lain 702 §:ää koskevia aineistoja tiedottaakseen yleisölle valvontaohjelmien toiminnasta, sovellettavista vaatimuksista ja yksityisyyden suojasta sekä FISC-tuomioistuimen roolista.[46]

Raukeamislausekkeen vuoksi FISA-lain 702 §:n oli määrä raueta vuoden 2023 lopussa, jollei kongressi uusi sitä. Kongressi uusi 702 §:n ensin tilapäisesti tekemättä siihen mitään muutoksia. Sen jälkeen kongressi hyväksyi 19. huhtikuuta 2024 tiedustelun uudistamista ja Yhdysvaltojen suojaamista koskevan lain (Reforming Intelligence and Securing America Act, RISAA-laki), jolla FISA-lain 702 § uusittiin kahdeksi vuodeksi ja jolla siihen tehtiin useita muutoksia. Ne voidaan laajasti ottaen jakaa kahteen ryhmään: 1) muutokset FISA-lain 702 §:n nojalla sallitun tiedustelutoiminnan soveltamisalaan ja 2) institutionaaliset ja menettelylliset muutokset.

Muutokset FISA-lain 702 §:n nojalla sallitun tiedustelutoiminnan soveltamisalaan

RISAA-laissa on otettu käyttöön kolme pääasiallista muutosta tiedustelutoimintaan, jota FISA-lain 702 §:n nojalla voidaan toteuttaa.

Ensinnäkin RISAA-laissa kielletään sellaisten tietojen kerääminen, joissa viitataan kohteeseen.[47] Tällä tarkoitetaan sellaisen viestinnän keräämistä, jonka osalta 702 §:n valintakriteeri (kuten sähköpostiosoite) ei ole viestinnän lähettäjä tai vastaanottaja, vaan viestintä sisältää viittauksen tällaiseen valintakriteeriin (tämä tarkoittaa esimerkiksi sähköpostiviestejä, jotka ei ole lähetetty valittuun sähköpostiosoitteeseen tai valitusta sähköpostiosoitteesta, vaan joiden tekstissä tai sisällössä on valittu sähköpostiosoite). Tällaisten tietojen kerääminen suljettiin pois jo FISA-lakiin vuonna 2018 tehdyllä muutoksella. FISA-laki mahdollisti kuitenkin edelleen sen, että kohteeseen viittaavien tietojen kerääminen olisi voitu aloittaa tulevaisuudessa uudelleen erityisellä lupamenettelyllä, johon osallistuvat FISC-tuomioistuin ja kongressi. Tämä mahdollisuus on poistettu RISAA-lailla käyttöönotetulla uusimmalla muutoksella.

Toiseksi ulkomaantiedustelutietojen määritelmää on laajennettu sisältämään huumausaineiden torjuntaan liittyvät tiedot[48]. Tarkastelukokouksessa Yhdysvaltojen viranomaiset selittivät, että

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

[45] Tällaisilla menettelyillä rajoitetaan tietojen kerääminen tiettyyn ulkomaantiedustelutarkoitukseen, rajoitetaan pääsyä tietokantoihin, joihin FISA-lain 702 §:n nojalla hankitut tiedot tallennetaan (muun muassa pääsyn valvonnan avulla), ja asetetaan rajoituksia tällaisten tietojen käytölle, säilyttämiselle ja levittämiselle.

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

[47] RISAA-lain 22 §.

[48] RISAA-lain 23 §.

muutos tehtiin nykyisen fentanyylikriisin ja kansainvälisten huumausainekauppiaiden ja huumausaineiden valmistajien aiheuttaman kasvavan kansallisen turvallisuusuhan vuoksi. Tätä taustaa vasten vahvistettiin, että tämä käsite kuuluu useiden toimeenpanoasetuksessa 14086 lueteltujen legitiimien tavoitteiden piiriin. Niitä ovat pyrkimys ymmärtää tai arvioida Yhdysvaltojen kansallista turvallisuutta tai sen liittolaisia uhkaavien tai mahdollisesti uhkaavien ulkomaisten organisaatioiden valmiuksia, pyrkimyksiä tai toimintaa, pyrkimys ymmärtää tai arvioida maailmanlaajuiseen turvallisuuteen vaikuttavia kansainvälisiä uhkia, kansanterveysriskit mukaan luettuina, ja pyrkimys suojautua kansainvälisiltä rikosuhkilta.[49]

Kolmanneksi RISAA-lailla laajennettiin ’sähköisten viestintäpalvelujen tarjoajan’ määritelmää. Soveltamisalan laajentamisen myötä yhä useampia yrityksiä voidaan vaatia toimittamaan tietoja FISA-lain 702 §:n nojalla.[50] Määritelmä kattaa nyt myös muut palveluntarjoajat, joilla on ”pääsy laitteisiin, joita käytetään tai voidaan käyttää langallisen tai sähköisen viestinnän välittämiseen tai tallentamiseen”. Siinä suljetaan kuitenkin nimenomaisesti pois julkiset majoituspalvelut, asuntopalvelut, julkiset palvelut ja ravitsemisliikkeet. Oikeusministeriö viittasi kongressille osoitetussa kirjeessä tähän muutokseen teknisenä muutoksena, jonka tarkoituksena oli kattaa ”erittäin pieni” määrä teknologiayrityksiä, jotka eivät FISC-tuomioistuimen ja ulkomaantiedustelun valvonnan muutoksenhakutuomioistuimen (FISCR-tuomioistuin) viimeaikaisten päätösten mukaan sisältyneet sähköisten viestintäpalvelujen tarjoajan aiempaan määritelmään.[51] Oikeusministeriö sitoutui samassa kirjeessä rajaamaan soveltamisalaa siten, että tätä määritelmää sovelletaan yksinomaan sentyyppiseen palveluntarjoajaan, jota FISC-tuomioistuimen päätökseen johtaneessa riita-asiassa tarkoitetaan. Tämän tuloksena asianomaiset yritykset nimetään kongressille tarkoitetussa turvallisuusluokitellussa liitteessä. Useat – myös tarkastelun yhteydessä palautetta antaneet – kansalaisjärjestöt ilmaisivat huolensa määritelmän soveltamisalan laajentamisesta ja väittivät, että sen piiriin voisi kuulua paljon yhdysvaltalaisia yrityksiä (koska monet niistä tarjoavat jonkinlaista palvelua ja niillä on pääsy viestintälaitteisiin). Näiden huolenaiheiden vuoksi tiedusteluyhteisön tuella on ehdotettu uutta muutosta ehdotuksessa tiedustelutoiminnan talousarviota koskevaksi vuoden 2025 laiksi (Intelligence Authorization Act for Fiscal Year 2025), joka on parhaillaan kongressin käsiteltävänä. Jos kongressi hyväksyy tämän muutoksen, sillä varmistettaisiin, että sähköisten viestintäpalvelujen tarjoajan määritelmän piiriin kuuluvat muut yritykset rajoittuisivat pelkästään edellä mainituissa FISC-tuomioistuimen tuomioissa mainittuihin yrityksiin. Lakiehdotuksessa suunnitellaan myös, että jokainen tällaiselle yritykselle osoitettu määräys olisi ilmoitettava FISC-tuomioistuimelle, jotta se voi arvioida, kuuluuko yritys todella määritelmän piiriin. Oikeusministeriö sitoutui kongressille osoitetussa kirjeessä raportoimaan kongressille kuuden kuukauden välein päivitetyn määritelmän soveltamisesta, jotta kongressi voi valvoa asianmukaisesti määritelmän suppeaa soveltamista.

On tärkeää huomata, että Yhdysvaltojen viranomaiset ja PCLOB vahvistivat tarkastelukokouksessa, että myös näiden muutosten jälkeen toimeenpanoasetuksen 14086 suojatoimia sovelletaan edelleen kaikilta osin kaikkeen FISA-lain 702 §:n nojalla

[49] Toimeenpanoasetuksen 14086 2 §:n b momentin ii kohdan A alakohdan 2, 3 ja 10 alakohta.
[50] RISAA-lain 25 §.
[51] https://www.justice.gov/opa/media/1348621/dl?inline. Ks. FISC-tuomioistuimen päätös vuodelta 2022 (https://www.intel.gov/assets/documents/702%20Documents/declassified/2022-FISC-ECSP-OPINION.pdf) ja FISCR-tuomioistuimen tuomio, jolla kyseinen päätös pidetään voimassa (https://www.intel.gov/assets/documents/702%20Documents/declassified/2023_FISC-R_ECSP_Opinion.pdf).

toteutettavaan tietojen keräämiseen ja käyttöön. Vaikka RISAA-lain myötä määräyksiä voidaan antaa suuremmalle joukolle yrityksiä, sillä ei rajoiteta oikeuksien käyttöä. On kuitenkin tärkeää seurata edelleen (lainsäädännön ja raportoinnin) kehitystä ja saada tietoa siitä, miten uusia sääntöjä sovelletaan käytännössä. Tähän kuuluu esimerkiksi se, millainen vaikutus ulkomaantiedustelutietojen ja sähköisten viestintäpalvelujen tarjoajan määritelmien laajentamisella on FISA-lain 702 §:n mukaisten kohteiden määrään (jotka ODNI ilmoittaa vuosittain, ks. jäljempänä oleva avoimuutta käsittelevä osio). Tästä saadaan todennäköisesti tietoa erityisesti FISA-lain 702 §:ää käsittelevän hiljattain annetun PCLOB:n raportin (ks. jäljempänä) tulevassa seurantaraportissa.

Institutionaaliset ja menettelylliset muutokset

Institutionaalisten ja menettelyllisten muutosten osalta RISAA-lailla kodifioitiin useita jo käytössä olleita menettelyjä ja otettiin käyttöön uusia suojatoimia. Osa näistä koskee vain yhdysvaltalaisia henkilöitä. Useilla muutoksilla kuitenkin lisätään sellaisten yhdysvaltalaisten ja ei-yhdysvaltalaisten henkilöiden suojaa, joiden tietoja voidaan kerätä FISA-lain 702 §:n nojalla[52], minkä vuoksi ne ovat merkityksellisiä tietosuojakehyksen toiminnan kannalta.

RISAA-laissa otettiin ensinnäkin käyttöön useita vastuuvelvollisuutta, valvontaa ja raportointia koskevia lisävaatimuksia. FBI:n henkilöstölle on nyt annettava vuosittain koulutusta säännöistä, joita sovelletaan FISA-lain 702 §:n nojalla saatuihin tietoihin tehtäviin kyselyihin.[53] FBI:n on myös raportoitava kongressille kyselytoiminnastaan (esimerkiksi sellaisten kyselyjen lukumäärästä, joissa käytetään eräkäsittelyyn perustuvia tekniikoita eli joissa yhdessä kyselyssä käytetään useita avainsanoja) ja vastuuvelvollisuuteen liittyvistä toimenpiteistä, jotka on otettu käyttöön kyselyihin sovellettavien lakisääteisten vaatimusten noudattamisen varmistamiseksi (RISAA-lain 11–12 §). Lisäksi oikeusministeriön valvontaviranomaista kehotetaan laatimaan raportti siitä, miten FBI noudattaa kyselyihin liittyviä vaatimuksia (RISAA-lain 9 §). Yleisemmin FISC-tuomioistuimen menettelyjen avoimuuden lisäämiseksi ODNIn ja oikeusministerin on nyt 180 päivän kuluessa saatettava päätökseen FISC-tuomioistuinten päätösten turvallisuusluokituksen poistamista koskeva tarkastelu (RISAA-lain 7 §). Lisäksi selostukset kaikista FISC-tuomioistuimen ja FISCR-tuomioistuimen (jossa FISC-tuomioistuimen päätöksiin voidaan hakea muutosta) käsittelyistä on säilytettävä ja välitettävä kongressille (RISAA-lain 8 §).

Toiseksi RISAA-laissa asetettiin lisärajoituksia sille, miten FBI voi käyttää FISA-lain 702 §:n nojalla kerättyjä tietoja. RISAA-lain 2 §:n d momentissa määrätään, että eräkäsittelyyn perustuva kysely voidaan tehdä vasta, kun sille on saatu hyväksyntä FBI:ssä työskentelevältä asianajajalta, jos asiaan ei liity pakottavia olosuhteita. Lisäksi FBI ei enää saa tarkistaa automaattisesti FISA-lain 702 §:n nojalla hankittuja tietoja, joita ei ole minimoitu, vaan sen on varmistettava, että tällaisiin tietoihin tehdään hakuja vain, kun analyytikot valitsevat ne nimenomaisesti haun kohteeksi. RISAA-laissa on myös kielletty FBI:tä tekemästä kyselyjä,

[52] Lisäksi RISAA-lailla otettiin käyttöön joitakin muutoksia, jotka koskevat FISA-lain 105 §:n nojalla toteutettavaa perinteistä yksilöllistä sähköistä valvontaa (FISC-tuomioistuimen antaman määräyksen perusteella, jos perusteltua syytä koskeva vaatimus täyttyy). Kun tiedusteluelin hakee oikeusministeriltä määräystä yksilöllisen sähköisen valvonnan toteuttamista varten, sen on annettava valaehtoinen vakuutus, jossa perustellaan näkemys siitä, että FISA-lain 105 §:n edellytykset täyttyvät (RISAA-lain 6 §:n a momentti). Vieraaseen valtaan tai vieraan vallan asiamiehiin kohdistuvan sähköisen valvonnan mahdollista kestoa on pidennetty 120 päivästä yhteen vuoteen (RISAA-lain 6 §:n g momentti).

[53] RISAA-lain 2 §:n d momentti.

joiden tarkoituksena on ainoastaan löytää ja hankkia todisteita rikollisesta toiminnasta (paitsi jos on perusteltu syy uskoa, että tiedot voisivat auttaa lieventämään henkeen tai vakavaan ruumiinvammaan kohdistuvaa uhkaa tai poistamaan sen, tai jos se on tarpeen tiedonantovelvollisuuden noudattamiseksi riita-asiassa).[54] FBI ei myöskään saa sisällyttää analytiikkaa koskeviin arkistoihin tietoja, joita ei ole minimoitu, ellei kohdehenkilö ole merkityksellinen käynnissä olevan kansallista turvallisuutta koskevan tutkimuksen kannalta.[55]

Kolmanneksi eräitä määräyksiä, jotka koskevat *amici curiaen* asemaa ja roolia FISC-tuomioistuimessa, on muutettu.[56] Nimityksellä *amicus* (monikossa *amici*) tarkoitetaan FISC-tuomioistuimen (ja FISCR-tuomioistuimen) avuksi nimettyjä asiantuntijoita, jotka avustavat yksityisyyteen ja kansalaisvapauksiin liittyvissä asioissa tai auttavat selventämään tiettyyn hallituksen tekemään hakemukseen liittyviä teknisiä kysymyksiä. FISA-laissa edellytettiin aiemmin, että *amicus* oli asiantunteva yksityisyyttä ja kansalaisvapauksia, tiedustelutietojen keräämistä, viestintäteknologiaa tai muita asiaankuuluvia aloja koskevissa asioissa. Nyt laissa edellytetään periaatteessa, että hänellä on yksityisyyteen tai kansalaisvapauksiin ja tiedustelutietojen keräämiseen liittyvää asiantuntemusta. FISC-tuomioistuimella oli jo mahdollisuus nimittää *amicus* missä tahansa asianmukaiseksi katsomassaan tapauksessa, ja sillä oli velvollisuus nimittää *amicus* käsitellessään lain uutta tai merkittävää tulkintaa. FISA-lain 702 §:n uusimisen jälkeen FISC-tuomioistuimen on myös nimitettävä *amicus* aina, kun sitä pyydetään hyväksymään FISA-lain 702 §:n mukaisia sertifiointeja ja niihin liittyviä menettelyjä (esimerkiksi kohdentamismenettelyjä), ellei se katso, että tämä ei olisi asianmukaista tai aiheuttaisi kohtuuttoman viivästyksen.[57] Lisäksi FISC-tuomioistuin voi nyt päättää nimittää yhden tai useamman *amicin*. Muutoksen myötä selvennettiin myös, että *amicus* voi toimittaa vain tietoja, jotka auttavat puuttumaan tuomioistuimen yksilöimiin tiettyihin ongelmiin. Tosin aihepiirit, joita *amicus* voi kommentoida, ovat edelleen laaja-alaisia (oikeudelliset argumentit ja tiedot, jotka liittyvät yhdysvaltalaisten henkilöiden yksityisyyden ja kansalaisvapauksien suojaan, tiedustelutietojen keräämiseen ja viestintäteknologiaan tai muihin asiaankuuluviin aloihin).

Lisäksi RISAA-lain 18 §:ssä perustetaan FISA-lain uudistuskomissio (FISA Reform Commission), jossa koostuu muun muassa kongressin jäsenistä, PCLOB:n puheenjohtajasta, kansallisen tiedustelupalvelun varapääjohtajasta ja varaoikeusministeristä sekä kongressin nimittämistä lisäjäsenistä[58] ja joka suosittelee uusia FISA-uudistuksia.

Komissio seuraa tiiviisti muuta FISA-lain 702 §:ään liittyvää kehitystä muun muassa PCLOB:n valvontatoimien (ks. jäljempänä), uudistuskomission työn ja kahden vuoden jälkeen toteutettavan FISA-lain tulevan uudelleentarkastelun osalta.

2.2.1.3. Valvontatoimet käytännössä: lukuja ja kehityssuuntauksia

Huhtikuussa 2024 julkaistusta ODNIn vuoden 2023 avoimuusraportista ”Annual Statistical Transparency Report Regarding the Intelligence Community’s Use of National Security Surveillance Authorities for Calendar Year”[59] käy ilmi, että FISA-lain 702 §:n mukaisten

[54] RISAA-lain 3 §:n a momentti.
[55] RISAA-lain 3 §:n b momentti. Kun se on välttämätöntä pakottavien olosuhteiden vuoksi, FBI:n johtaja voi päättää tehdä tähän määräykseen poikkeuksen, josta on ilmoitettava kongressille.
[56] Selvennykseksi todettakoon, että nämä muutokset eivät vaikuta erityisasiamiesten asemaan ja rooliin tietosuojaa käsittelevässä muutoksenhakutuomioistuimessa, kuten Yhdysvallat vahvisti tarkastelukokouksessa.
[57] RISAA-lain 5 §:n b momentti.
[58] RISAA-lain 18 §:ssä nimenomaisesti edellytetään kongressin ulkopuolista edustusta.
[59] https://www.dni.gov/files/CLPT/documents/2024_ASTR_for_CY2023.pdf.

kohteiden määrä on kasvanut: kalenterivuonna 2022 kohteita oli 245 073 ja kalenterivuonna 2023 yhteensä 268 590. Raportissa selitetään, että kohteiden lukumäärän vaihtelut voivat liittyä useisiin syihin, kuten operatiivisten painopisteiden muutoksiin, maailman tapahtumiin, teknisiin valmiuksiin, kohteiden käyttäytymiseen ja televiestintäalan muutoksiin. Raportissa todetaan myös, että FISA-lain 402 §:n (lähtevän ja saapuvan teleliikenteen tietojen tallennusjärjestelmät (pen registers, trap and trace authority)) nojalla toteutettavien toimien kohteena ei ollut ei-yhdysvaltalaisia henkilöitä (vuonna 2021 ei-yhdysvaltalaisia oli kohteena yksi ja vuonna 2022 ei yhtään). FISA-lain 501 §:n (pääsy yleisten kuljetusliikkeiden, ajoneuvojen vuokrauspalvelujen tai fyysisten varastotilojen liiketoimintatietoihin) nojalla puolestaan annettiin kuusi määräystä (verrattuna 11:een vuosina 2021 ja 2022), jotka koskivat kuutta kohdetta (verrattuna 13:een vuonna 2021 ja 11:een vuonna 2022) ja kattoivat 5 412 yksilöllistä tunnistetta (verrattuna 23 157:ään vuonna 2021 ja 55 431:een vuonna 2022), joita käytettiin tällaisten määräysten nojalla kerättyjen tietojen toimittamiseen.

Oikeusministeriön vuotuisessa FISA-laista annetussa raportissa kongressille ilmoitetaan, että kalenterivuoden 2023 aikana FISC-tuomioistuimeen tehtiin 327 hakemusta sähköisen valvonnan ja/tai fyysisten etsintöjen tekemisestä ulkomaantiedustelutarkoituksissa FISA-lain 105 §:n ja 302 §:n nojalla.[60] Kohteena olleiden henkilöiden kokonaismäärä oli 500–999. Kansallista turvallisuutta koskevien kirjeiden (NSL) osalta raportissa todetaan, että ei-yhdysvaltalaisia henkilöitä koskevista tiedoista tehtiin 10 115 pyyntöä (pois lukien pyynnöt, jotka koskevat vain tilaajatietoja), joiden avulla pyrittiin hankkimaan tietoja 3 330:sta eri ei-yhdysvaltalaisesta henkilöstä.[61]

Useat tietosuojakehyksen mukaisesti varmennetut yritykset (kuten Google ja Meta) käyttävät Yhdysvaltojen lainsäädännön tarjoamaa mahdollisuutta julkaista avoimuusraportteja, joissa tiedotetaan yritysten tietyn raportointikauden aikana saamien FISA- ja NSL-pyyntöjen määristä. Tämän kertomuksen laatimisajankohtana ei ollut vielä saatavilla tilastoja heinäkuun 2023 jälkeen tehdyistä FISA-pyynnöistä. Esimerkiksi Google ilmoitti saaneensa heinäkuun ja joulukuun 2023 välisenä aikana 500–999 NSL-pyyntöä, jotka vaikuttivat 2 000–2 499 tiliin.[62] Meta ilmoitti saaneensa samana aikana 0–499 NSL-pyyntöä, jotka vaikuttivat 500–999 tiliin.[63] Määrät ovat pysyneet suhteellisen samalla tasolla viime vuosina. Avoimuuden lisäämiseksi jotkin yritykset (esimerkiksi Google) julkaisevat proaktiivisesti saamansa kansallista turvallisuutta koskevat kirjeet salassapitomääräysten päätyttyä.[64]

2.2.1.4. Muut toimet

Tarkasteluun valmistautumisen yhteydessä useat kansalaisjärjestöt ovat tuoneet esiin kysymyksiä Yhdysvaltojen tiedusteluelinten uusista tiedonhankintatavoista, joissa tietoja ostetaan kaupallisilta toimijoilta, erityisesti datan välittäjiltä. Kansalaisjärjestöt selittivät, että vaikka tällä tavoin kerättyjä tietoja on silti käsiteltävä muiden vaatimusten, kuten

[60] https://www.justice.gov/nsd/media/1350236/dl?inline.

[61] Luvut ovat pysyneet suhteellisen samoina edelliseen raportointivuoteen (2022) verrattuna. Vertailun vuoksi vuonna 2022 FISC-tuomioistuimeen tehtiin 317 lopullista hakemusta sähköisen valvonnan ja/tai fyysisten etsintöjen tekemisestä ulkomaantiedustelutarkoituksissa. Sähköistä valvontaa koskevien määräysten kohteena olevien henkilöiden kokonaismäärä oli 0–499. FBI esitti 9 103 NSL-pyyntöä ei-yhdysvaltalaisia henkilöitä koskevista tiedoista vuonna 2022 (pois lukien pyynnöt, jotka koskivat vain tilaajatietoja). Lähde: 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/.

[64] https://transparencyreport.google.com/user-data/us-national-security.

toimeenpanoasetuksen 12333[65], mukaisesti, tällainen tiedonhankinta tapahtuu FISA-lain ja toimeenpanoasetuksen 14086 ulkopuolella.

Tältä osin on syytä muistaa, että kaikenlaiseen vapaaehtoiseen tietojen jakamiseen kolmansien osapuolten kanssa sovelletaan tietosuojakehyksen nojalla useita yksityiskohtaisia edellytyksiä. Ensinnäkin varmennettu organisaatio ei saa jakaa tietoja kolmannen osapuolen (joka ei toimi edustajana tai käsittelijänä) kanssa ilmoittamatta siitä asianomaisille ja tarjoamatta heille valintaoikeutta.[66] Toiseksi *tietojen edelleen siirtämiseen liittyvää vastuuvelvollisuutta koskevan periaatteen* mukaisesti tietoja voidaan siirtää edelleen vain 1) rajoitettuihin ja täsmennettyihin tarkoituksiin, 2) tietosuojakehykseen osallistuvan organisaation ja kolmannen osapuolen välisen sopimuksen perusteella ja 3) ainoastaan, jos sopimuksessa edellytetään, että kolmannen osapuolen on tarjottava suojan taso, joka vastaa järjestelyn periaatteiden takaamaa suojan tasoa.[67]

Lisäksi, kuten myös tarkastelukokouksessa keskusteltiin, liittovaltion kauppakomissio on toteuttanut lainvalvontatoimia arkaluonteisia kuluttajatietoja myyviä datan välittäjiä vastaan. Esimerkiksi asiassa *X-Modea* ja sen seuraajaa *Outlogicia* vastaan liittovaltion kauppakomissio antoi 9. tammikuuta 2024 määräyksen, jolla kielletään yritystä myymästä geopaikannustietoja kolmansille osapuolille ja määrätään se poistamaan tiedot, joita se oli käyttänyt ja jakanut lainvastaisesti. Liittovaltion kauppakomission tutkimuksessa todettiin muun muassa, että kyseinen yritys ei tiedottanut kattavasti henkilöille heidän geopaikannustietojensa käytöstä ja myynnistä, se ei ollut ottanut käyttöön toimenpiteitä, joiden avulla henkilöt voisivat kieltää seurannan, eikä se rajoittanut kolmansien osapuolten mahdollisuuksia käyttää tällaisia tietoja ja että yritys oli sallinut tietojen käytön mahdollisesti syrjiviin tarkoituksiin.[68] Komissio odottaa, että liittovaltion kauppakomissio noudattaa samaa toimintatapaa, jos tietosuojakehyksen mukaisesti varmennetut yritykset jakavat tietoja edellä mainittujen määräysten vastaisesti.

Lisäksi ODNI julkaisi toukokuussa 2024 kaupallisesti saatavilla olevia tietoja koskevan tiedusteluyhteisön toimintakehyksen (Intelligence Community Policy Framework for Commercially Available Information)[69]. Toimintakehyksessä vahvistetaan useita periaatteita ja vaatimuksia, joita tiedusteluelinten olisi noudatettava hankkiessaan ja käyttäessään tietoja kaupankäynnin yhteydessä, yksityisyyteen ja kansalaisvapauksiin kohdistuvien riskien minimointi mukaan luettuna.

2.2.2. Riippumaton valvonta

Yhdysvaltojen tiedusteluelinten toimintaa valvovat eri elimet, kuten yksityisyyden suojasta ja kansalaisvapauksista vastaavat virkamiehet, valvontaviranomaiset, kongressi ja PCLOB. Erityisesti toimeenpanoasetuksessa 14086 edellytetään, että kullakin tiedusteluelimellä on oikeusalasta, valvonnasta ja vaatimustenmukaisuudesta vastaavia korkean tason virkamiehiä

[65] Ks. esimerkiksi toimeenpanoasetuksen 12333 2.4 § keräystekniikoista
[66] Ks. tietosuojan riittävyyttä koskevan päätöksen johdanto-osan 40 kappale.
[67] Ks. tietosuojan riittävyyttä koskevan päätöksen johdanto-osan 38 kappale.
[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 Toimintakehystä on sovellettu tiedusteluelimiin elokuussa 2024 alkaen.

sovellettavan Yhdysvaltojen lainsäädännön noudattamisen varmistamiseksi. Valvontatehtävää hoitavat virkamiehet, jotka on nimetty sääntöjenmukaisuuden valvomisen tehtävään, sekä yksityisyyden suojasta ja kansalaisvapauksista vastaavat virkamiehet ja valvontaviranomaiset.[70] Näiden on valvottava säännöllisesti signaalitiedustelutoimintaa ja varmistettava, että vaatimustenvastaisuudet korjataan. Tiedusteluelinten on annettava kyseisille virkamiehille pääsy kaikkiin merkityksellisiin tietoihin, joita he tarvitsevat valvontatehtäviensä suorittamiseksi, eivätkä elimet saa ryhtyä toimiin estääkseen valvontatoimia tai vaikuttaakseen niihin epäasianmukaisesti.

Tarkastelukokoukseen osallistui ODNIn yhteydessä toimivan tiedusteluyhteisön ylitarkastajan (Intelligence Community Inspector General (ICIG)) toimiston pääneuvonantaja. ICIG:llä on kattava toimivalta koko tiedusteluyhteisön suhteen ja valtuudet tutkia valituksia tai tietoja väitetystä lainvastaisesta menettelystä tai toimivallan väärinkäytöstä. Hän vahvisti, että ICIG tarkastaa järjestelmällisesti toimeenpanoasetuksen 14086 noudattamisen osana valvontatoimiaan. Hän viittasi myös tiedusteluyhteisön muiden valvontaviranomaisten viimeaikaisiin valvontatoimiin, joita käsitellään säännöllisissä raporteissa. Huhtikuun ja syyskuun 2023 välistä ajanjaksoa käsittelevässä puolivuotisraportissaan[71] kansallisen turvallisuusviraston valvontaviranomainen esimerkiksi antoi kongressille tietoja arvioinnista, jonka se oli tehnyt kansallisen turvallisuusviraston sisäisestä kohdentamispäätösten ja -pyyntöjen valvontakehyksestä. Raportissa todettiin, että kyseinen kehys toimi asianmukaisesti ja sillä voidaan varmistaa, että kansalaisvapauksia ja yksityisyyttä suojaavia lakeja, määräyksiä ja politiikkoja noudatetaan. Raportissa mainitaan myös tutkimus, jossa selvisi, että kansallisen turvallisuusviraston työntekijä oli käyttänyt signaalitiedusteluun tarkoitettua välinettä väärin luvattomiin tarkoituksiin.

Toimeenpanoasetuksen 14086 nojalla PCLOB:llä[72] on myös erityisiä valvontatehtäviä[73]. PCLOB:n puheenjohtaja ja kolme jäsentä osallistuivat tarkastelukokoukseen ja ilmoittivat, että PCLOB antoi huhtikuussa 2023 tiedusteluelimille neuvoja liittyen tiedusteluelinten ehdotuksiin käytännöiksi ja menettelyiksi, joilla ne panevat toimeenpanoasetuksen 14086 täytäntöön. Sitä myös kuultiin tietosuojaa käsittelevän muutoksenhakutuomioistuimen (DPCR-tuomioistuin) tuomareiden ja erityisasiamiesten nimittämisestä. PCLOB käynnisti

[70] Kullakin tiedusteluelimellä on valvontaviranomainen, joka on siitä lakisääteisesti riippumaton ja vastuussa tarkastuksista ja tutkimuksista, jotka koskevat tiedusteluelimen kansalliseen turvallisuuteen liittyviä toimia. Valvontaviranomaisilla on pääsy kaikkiin asiaan liittyviin (myös turvallisuusluokiteltuihin) tietoihin, tarvittaessa haasteteitse, ja ne voivat ottaa todistajanlausuntoja. Valvontaviranomaiset saattavat epäiltyjä rikoksia koskevat asiat tuomioistuinten käsiteltäviksi ja antavat elinten johtajille suosituksia korjaavista toimista. Niiden antamat suositukset eivät ole sitovia, mutta niiden tarkastuskertomukset, myös seurantakertomukset, (tai niiden puuttuminen) yleensä julkistetaan ja lähetetään kongressille. Katso tältä osin tietosuojan riittävyyttä koskevan päätöksen alaviite 136 valvontaviranomaisen roolista.

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

[72] PCLOB on riippumaton elin, jonka vastuualaan kuuluu terrorismin vastainen politiikka ja sen täytäntöönpano yksityisyyden suojan ja kansalaisvapauksien suojelemiseksi. Se voi saada käyttöönsä kaikki asiaankuuluvat (myös turvallisuusluokitellut) tiedot, suorittaa haastatteluja ja kuulla todistajia. Se voi antaa suosituksia lainvalvonta- ja tiedusteluviranomaisille, ja se raportoi säännöllisesti kongressille ja presidentille. Sen raportit julkistetaan mahdollisimman laajalti.

[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.

myös valvontahankkeen, jonka tarkoituksena on 1) arvioida tiedusteluelinten hyväksymien päivitettyjen käytäntöjen ja menettelyjen täytäntöönpanoa sen varmistamiseksi, että ne ovat yhdenmukaisia toimeenpanoasetuksen kanssa, ja 2) tehdä vuotuinen arviointi uuden oikeussuojamekanismin (ks. jäljempänä) toiminnasta.[74] PCLOB:n jäsenet vahvistivat, että PCLOB aikoo toteuttaa molemmat arvioinnit lähitulevaisuudessa. Jäsenet selittivät, että koska valituksia ei ole tehty, PCLOB keskittyy oikeussuojamekanismin arvioinnissa mekanismin käyttöön ottamiseksi laadittuihin käytäntöihin ja menettelyihin.

Muiden valvontatoimien osalta PCLOB julkaisi 28. syyskuuta 2023 raportin[75] FISA-lain 702 §:stä. Raportti on jatkoa aiempaan, vuonna 2014 julkaistuun raporttiin, ja se sisältää päivitettyjä asiatietoja ja oikeudellisia tietoja FISA-lain 702 §:n mukaisten tarkkailuohjelmien toiminnasta. Raportissa annetaan myös suosituksia siitä, miten tiedusteluelimet noudattavat sovellettavia vaatimuksia, ja ehdotuksia kongressille siitä, miten FISA-lain 702 §:n useita näkökohtia voidaan edelleen vahvistaa sen uusimisen yhteydessä (muun muassa kodifioimalla toimeenpanoasetuksessa 14086 luetellut valvontatoimien legitiimit tavoitteet).[76] Tarkastelukokouksessa PCLOB ilmoitti, että se odottaa saavansa pian vastauksia tiedusteluelimiltä suositustensa täytäntöönpanosta, ja näitä vastauksia hyödynnetään tulevassa seurantaraportissa. Muista käynnissä olevista valvontahankkeista yksi liittyy kotimaisen terrorismin torjuntaan ja sen vaikutukseen yksityisyyteen ja kansalaisvapauksiin ja yksi siihen, miten FBI kerää julkisiin lähteisiin perustuvia tai kaupallisesti saatavilla olevia tietoja.[77]

Tarkastelun yhteydessä kuullut kansalaisjärjestöt ilmaisivat huolensa siitä, että useiden PCLOB:n jäsenten toimikauden on määrä päättyä lähitulevaisuudessa, minkä seurauksena PCLOB saattaa menettää päätösvaltaisuutensa. Kansalaisjärjestöt totesivat erityisesti, että puheenjohtajan toimikausi on päättynyt ja ajanjakso, jonka hän voi hoitaa toimea tilapäisesti, päättyy tammikuussa 2025, ja että toinen jäsenen paikka on täyttämättä ja kolmas vapautuu myös ensi vuoden tammikuussa. PCLOB:n jäsenet selittivät tarkastelukokouksessa, että he eivät pitäneet todennäköisenä, että PCLOB menettää päätösvaltaisuutensa, koska tällä hetkellä täyttämättä olevaan toimeen on jo tehty nimitys[78] (joka odottaa senaatin vahvistusta). Jäsenet korostivat myös, että vaikka PCLOB menettäisi päätösvaltaisuutensa, se ei vaikuttaisi PCLOB:n kykyyn jatkaa valvontahankkeiden toteuttamista. Komissio seuraa kuitenkin tiiviisti tulevien avoimien toimien ja nimitysten/nimeämisten tilannetta, koska PCLOB:llä on tärkeä rooli toimeenpanoasetuksen 14086 täytäntöönpanon arvioimisessa.

2.2.3. Oikeussuojakeinot

Toimeenpanoasetuksella 14086, jota on täydennetty oikeusministerin asetuksella, perustettiin uusi oikeussuojamekanismi, jotta voidaan käsitellä ja ratkaista yksityishenkilöiden tekemät vaatimukset täyttävät valitukset, jotka koskevat Yhdysvaltojen signaalitiedustelutoimintaa.[79] Jokaisella EU:ssa olevalla henkilöllä on oikeus tehdä oikeussuojamekanismin kautta valitus

[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] Komissio toteaa, että osa näistä suosituksista on sisällytetty osaksi RISAA-lakia, mukaan lukien suositus kohteeseen viittaavien tietojen keräämisestä ja suositus FISC-tuomioistuimen asiantuntijoiden (*amici*) roolin vahvistamisesta.
[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.
[79] Tietosuojan riittävyyttä koskevan päätöksen johdanto-osan 176–194 kappale.

signaalitiedustelutoimintaa koskevan Yhdysvaltojen lainsäädännön (esimerkiksi toimeenpanoasetuksen 14086, FISA-lain 702 §:n tai toimeenpanoasetuksen 12333) väitetystä rikkomisesta, joka liittyy Yhdysvaltoihin siirrettyjä henkilötietoja ja joka vaikuttaa kielteisesti henkilön yksityisyyteen ja kansalaisvapauksiin liittyviin etuihin. Henkilöt voivat toimittaa valituksen EU:n jäsenvaltion tietosuojaviranomaiselle, joka ohjaa valituksen Euroopan tietosuojaneuvoston sihteeristön kautta oikeussuojamekanismiin. Mekanismi koostuu kahdesta tasosta: ODNI CLPO:n suorittamasta valitusten alustavasta tutkinnasta ja henkilöiden mahdollisuudesta hakea CLPO:n päätökseen muutosta riippumattomassa DPRC-tuomioistuimessa. Kun ODNI CLPO tai DPRC-tuomioistuin on saattanut tarkastelun päätökseen, valituksen tekijälle ilmoitetaan kansallisen viranomaisen välityksellä, että ”tarkastelussa ei havaittu soveltamisalaan kuuluvia rikkomisia” tai että ”ODNI CLPO tai DPRC-tuomioistuin on antanut päätöksen, jossa vaaditaan asianmukaista korjausta”. ODNI CLPO:n ja DPRC-tuomioistuimen päätökset sitovat tiedusteluelimiä.

Tietosuojan riittävyyttä koskevan päätöksen hyväksymisen jälkeen on toteutettu lisätoimia oikeussuojamekanismin saattamiseksi kokonaisuudessaan toimintakykyiseksi.

DPRC-tuomioistuimen perustamisessa edettiin, kun tuomioistuimeen nimitettiin 14. marraskuuta 2023 kahdeksan tuomaria (eli kaksi enemmän kuin mitä edellytettiin toimeenpanoasetuksessa 14086 täydennettynä oikeusministerin asetuksilla; 28 CFR 201.3 §:n a momentti).[80] Tuomarit nimitettiin toimeenpanoasetuksessa 14086[81] vahvistettujen kriteerien perusteella ja samassa asetuksessa vahvistetun menettelyn mukaisesti, mukaan lukien muun muassa PCLOB:n kuulemisen jälkeen. Tuomareissa on liittovaltion piirituomioistuimen ja muutoksenhakutuomioistuinten entisiä tuomareita, entinen Yhdysvaltojen oikeusministeri ja PCLOB:n entinen jäsen. Kuten toimeenpanoasetuksessa edellytetään, vähintään puolella tuomareista on aiempaa tuomioistuinkokemusta. Lisäksi huhtikuussa 2024 on nimitetty kaksi erityisasiamiestä (oikeusalan ammattilaista, joilla on kokemusta yksityisyyttä ja kansallista turvallisuutta koskevista asioista), jotka edustavat henkilöiden etuja DPRC-tuomioistuimessa. Tarkastelukokouksessa vahvistettiin, että kaikista tuomareista ja erityisasiamiehistä on tehty korkein turvallisuusselvitys ja että he saavat näin ollen käyttöönsä turvallisuusluokiteltuja aineistoja suorittaessaan DPRC-tuomioistuimen tehtäviä. DPRC-tuomioistuin oli myös julkaissut usein kysyttyjä kysymyksiä[82], joiden vastauksissa annettiin lisätietoa tuomioistuimen roolista, riippumattomuudesta ja toiminnasta.

Valitusten käsittelyn osalta ODNI hyväksyi 6. joulukuuta 2022 tiedusteluyhteisöä koskevan määräyksen nro 126 (Intelligence Community Directive 126)[83]. Sillä säännellään yksityiskohtaisesti valitusten tutkinta- ja tuomioistuinmenettelyn eri näkökohtia (muun muassa asettamalla määräaikoja, perustamalla turvallinen sähköinen rekisteri ja viestintäkanavat ja edellyttämällä, että CLPO ja tiedusteluyhteisön toimijat tekevät yhteistyötä PCLOB:n kanssa oikeussuojamekanismin vuotuisen arvioinnin yhteydessä). Määräystä sovelletaan koko Yhdysvaltojen tiedusteluyhteisöön, ja sitä on täydennetty edelleen yksittäisten tiedusteluelinten käyttöön ottamilla sisäisillä menettelyillä, jotka koskevat niiden yhteistyötä ODNI CLPO:n kanssa valitusten käsittelyn yhteydessä (esimerkiksi turvallisen rekisterin

[80] https://www.justice.gov/opa/pr/attorney-general-merrick-b-garland-announces-judges-data-protection-review-court.
[81] Toimeenpanoasetuksen 14086 3 §:n d momentin A kohta.
[82] https://www.justice.gov/opcl/dprc-resources.
[83] https://www.dni.gov/files/documents/ICD/ICD_126-Implementation-Procedures-for-SIGINT-Redress-Mechanism.pdf

kehittäminen valitusten ja vastauksena toimitettavien asiakirjojen jakamista varten ja turvallinen viestintä asianomaisten elinten välillä). DPRC-tuomioistuin antaa tulevina kuukausina myös yksityiskohtaisempia sääntöjä valitusten käsittelystä ja muista menettelyllisistä näkökohdista.

Euroopan unionissa ja Yhdysvalloissa toteutettiin joitakin lisätoimenpiteitä, joilla tästä aihepiiristä tiedotetaan suurelle yleisölle ja helpotetaan valitusten toimittamista ja käsittelyä. Euroopan tietosuojaneuvosto on esimerkiksi julkaissut uutta oikeussuojamekanismia koskevan tiedotteen[84], valituslomakkeen mallin[85] (joka kaikkien tietosuojaviranomaisten olisi käännettävä ja julkaistava kansallisilla kielillä) ja työjärjestyksen[86], joka koskee kansallisten valvontaviranomaisten ja Euroopan tietosuojaneuvoston sihteeristön välistä yhteistyötä. ODNI on puolestaan julkaissut usein kysyttyjä kysymyksiä ja tietokoosteen uudesta oikeussuojamekanismista ja toteuttanut tiedotustoimia.[87]

Lisäksi Euroopan tietosuojaneuvosto ja asianomaiset Yhdysvaltojen viranomaiset ovat viime vuoden aikana tehneet tiivistä yhteistyötä useiden operatiivisten näkökohtien osalta. Kuten tarkastelukokouksessa vahvistettiin, ne ovat erityisesti ottaneet käyttöön salatun viestintäkanavan valitusten välittämiseksi EU:n kansallisilta viranomaisilta Euroopan tietosuojaneuvoston sihteeristölle, Euroopan tietosuojaneuvoston sihteeristöltä ODNI CLPO:lle ja oikeusministeriön yksityisyyden ja kansalaisvapauksien suojasta vastaavalle toimistolle sekä valitusten välittämiseksi OCNI CLPO:n ja Yhdysvaltojen muiden viranomaisten (esimerkiksi DPRC-tuomioistuimen) välillä. Lisäksi ODNI CLPO selitti, että yksittäisten tiedusteluviranomaisten ja ODNI CLPO:n välistä yhteistyötä varten on otettu käyttöön uusia sisäisiä menettelyjä valitusten käsittelyn osalta.

Yksityisyyden ja kansalaisvapauksien suojasta vastaava toimisto, joka antaa hallinnollista tukea DPRC-tuomioistuimelle, ilmoitti myös, että DPRC-tuomioistuimen toimintaa rahoitetaan tuomioistuimen omasta erillisestä budjettikohdasta ja että sille annetaan sen tehtävien suorittamiseksi tarvittavat välineet, kuten suojatut tietokoneet, kannettavat tietokoneet ja puhelimet. Kuten toimeenpanoasetuksessa 14086 edellytetään, kauppaministeriö on myös toteuttanut tarvittavat toimenpiteet pitääkseen kirjaa kaikista saaduista vaatimukset täyttävistä valituksista. Tähän sisältyy salatun viestintäkanavan käyttöönotto ODNI CLPO:n kanssa. Kauppaministeriö ottaa säännöllisesti yhteyttä ODNI CLPO:hon selvittääkseen, onko yksittäiseen valitukseen liittyvien tietojen turvallisuusluokitus poistettu. Jos turvallisuusluokitus on poistettu, kauppaministeriö ilmoittaa asiasta asianomaiselle henkilölle, jotta hän voi tutustua kyseisiin tietoihin.

EU:n valvontaviranomaiset eivät olleet saaneet yhtään valitusta tarkastelukokoukseen mennessä, minkä vuoksi uutta oikeussuojamekanismia ei ollut vielä käytetty.

[84] https://www.edpb.europa.eu/our-work-tools/our-documents/other-guidance/information-note-data-protection-framework-redress_fi.
[85] https://www.edpb.europa.eu/our-work-tools/our-documents/other-guidance/template-complaint-form-us-office-director-national_fi.
[86] https://www.edpb.europa.eu/our-work-tools/our-documents/other-guidance/rules-procedure-data-protection-framework-redress_fi.
[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.

3. PÄÄTELMÄT

Komissio katsoo tässä ensimmäisessä tarkastelussa kerättyjen tietojen perusteella, että Yhdysvaltojen viranomaiset ovat ottaneet käyttöön tarvittavat rakenteet ja menettelyt sen varmistamiseksi, että tietosuojakehys toimii tehokkaasti. Komissio arvostaa tarkastelun suorittamisessa tehtyä erittäin hyvää yhteistyötä Yhdysvaltain viranomaisten kanssa.

Tässä ensimmäisessä tarkastelussa keskityttiin luonnollisesti selvittämään, onko kaikki tietosuojakehyksen perustavanlaatuiset osatekijät otettu käyttöön. Koska tietosuojakehys on ollut toiminnassa vasta yhden vuoden ajan, on väistämätöntä, että suojatoimien käytännön soveltamisesta varmennettujen yritysten suorittamaan tietojen käsittelyyn ja viranomaisten tietoihin pääsyyn on saatu vain vähän kokemusta. Komissio seuraa näin ollen tiiviisti asiaan liittyvää kehitystä tulevina kuukausina ja vuosina ja kiinnittää erityistä huomiota 1) PCLOB:n tuleviin raportteihin toimeenpanoasetuksen 14086 täytäntöönpanosta ja signaalitiedustelun oikeussuojamekanismin, erityisesti DPRC-tuomioistuimen, toiminnasta, 2) FISA-lain 702 §:ään mahdollisesti tehtäviin tuleviin muutoksiin ja 3) uusien jäsenten nimittämiseen PCLOB:ssa avautuviin työpaikkoihin.

Komissio pitää tietosuojakehyksen jatkuvan ja tehokkaan toiminnan varmistamiseksi tärkeänä, että

- kuten tarkastelukokouksessa ilmoitettiin, kauppaministeriö hyödyntää kattavammin tietosuojakehyksessä vahvistettuja erilaisia välineitä valvoakseen, että yritykset noudattavat tietosuojakehyksen periaatteita, ja havaitakseen tietosuojakehykseen osallistumista koskevat totuudenvastaiset väitteet
- liittovaltion kauppakomissio kehittää proaktiivista lähestymistapaansa siihen, miten se tutkii ja valvoo sitä, että varmennetut yritykset noudattavat tietosuojakehyksen periaatteita
- kauppaministeriö, liittovaltion kauppakomissio ja EU:n tietosuojaviranomaiset laativat tietosuojakehyksen periaatteiden keskeisistä vaatimuksista yhteisiä ohjeita, esimerkiksi liittyen henkilöstötietoihin ja tietojen siirtämiseen edelleen.

Tarkastelun tulosten perusteella ja tietosuojan riittävyyttä koskevan päätöksen johdanto-osan 211 kappaleen mukaisesti komissio pitää asianmukaisena, että seuraava määräaikaistarkastelu suoritetaan kolmen vuoden kuluttua. Silloin tietosuojakehyksen käytännön soveltamisesta pitäisi olla enemmän kokemusta ja edellä mainittu tuleva kehitys voidaan ottaa huomioon. Komissio aikoo näin ollen tietosuojan riittävyyttä koskevan päätöksen 3 artiklan 4 kohdan mukaisesti kuulla Euroopan tietosuojaneuvostoa ja yleisen tietosuoja-asetuksen 93 artiklan 1 kohdalla perustettua komiteaa tulevien tarkastelujen ajankohdista.