EUROPOS
KOMISIJA

Briuselis, 2024 10 09
COM(2024) 451 final

KOMISIJOS ATASKAITA EUROPOS PARLAMENTUI IR TARYBAI

dėl sprendimo, priimto dėl ES ir JAV duomenų privatumo sistemos teikiamo asmens duomenų apsaugos lygio tinkamumo, veikimo pirmosios periodinės peržiūros

1. PIRMOJI PERIODINĖ PERŽIŪRA: APLINKYBĖS, PASIRENGIMAS IR PROCESAS

Komisija 2023 m. liepos 10 d. sprendime (toliau – sprendimas dėl tinkamumo) nustatė, kad ES ir JAV duomenų privatumo sistemos (toliau – DPS) teikiamas Jungtinių Amerikos Valstijų organizacijoms iš Europos Sąjungos perduodamų asmens duomenų apsaugos lygis yra tinkamas[1]. Sprendime dėl tinkamumo nustatyta, kad Komisija turi atlikti periodines peržiūras, o pirmoji iš jų turėtų būti atlikta praėjus vieniems metams nuo tos dienos, kai valstybėms narėms pranešta apie sprendimą dėl tinkamumo. Šia ataskaita užbaigiama ši pirmoji peržiūra.

Kaip reikalaujama sprendimo dėl tinkamumo 211 konstatuojamojoje dalyje, per šią pirmą peržiūrą, atliekamą po pirmųjų naujosios sistemos veikimo metų, pagrindinis dėmesys skirtas patikrinimui, ar visi numatyti sistemos elementai yra įdiegti ir veiksmingai funkcionuoja. Peržiūra apėmė visus sistemos veikimo aspektus, atsižvelgiant ir į teisinius pokyčius, įvykusius nuo tada, kai priimtas sprendimas dėl tinkamumo.

Rengdamasi peržiūrai Komisija rinko informaciją iš susijusių suinteresuotųjų subjektų, visų pirma, iš skaitmeninių teisių ir privatumo srityje kompetentingų nevyriausybinių organizacijų (NVO)[2], DPS sertifikuotų organizacijų (per jų prekybos asociacijas)[3], taip pat JAV institucijų, dalyvaujančių įgyvendinant šią sistemą. Be to, Komisija, portale „Išsakykite savo nuomonę“ paskelbusi specialų kvietimą teikti informaciją, surinko plačiosios visuomenės atsiliepimų[4].

2024 m. liepos 18 ir 19 d. Vašingtone vyko peržiūros susitikimas. Jį pradėjo už teisingumą ir vartotojų reikalus atsakingas Europos Komisijos narys Didier Reyndersas ir JAV prekybos sekretorė Gina Raimondo[5].

Peržiūrą iš ES pusės atliko Europos Komisijos Teisingumo ir vartotojų reikalų generalinio direktorato atstovai kartu su penkiais Europos duomenų apsaugos valdybos (toliau – EDAV) paskirtais atstovais iš įvairių nacionalinių duomenų apsaugos institucijų (toliau – DAI) ir

[1] 2023 m. liepos 10 d. Komisijos įgyvendinimo sprendimas (ES) 2023/1795, priimtas pagal Europos Parlamento ir Tarybos reglamentą (ES) 2016/679, dėl tinkamo asmens duomenų apsaugos lygio pagal ES ir JAV duomenų privatumo sistemą.

[2] Komisija devynioms NVO („Human Rights Watch“, „American Civil Liberties Union“, „Consumer Federation of America“, „Center for Digital Democracy“, „New America Open Technology Institute“, „Access Now“, „Electronic Frontier Foundation“, „Electronic Privacy Information Center“, „Center for Democracy and Technology“) nusiuntė klausimyną, kuriame daugiausia dėmesio skirta aktualiems JAV teisinės sistemos pokyčiams, priežiūros ir vykdymo užtikrinimo mechanizmams ir teisių gynimo mechanizmų veikimui. Be to, 2024 m. liepos 9 d. įvyko Komisijos tarnybų ir EDAV atstovų virtualus susitikimas su šiomis NVO.

[3] Komisija devynioms prekybos asociacijoms („Software & Information Industry Association“, „U.S. Chamber of Commerce“, „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“, „Engine“) nusiuntė klausimyną, kuriame daugiausia dėmesio skirta DPS sertifikuotų bendrovių patirčiai, visų pirma sertifikavimo procesui, veiksmams, kurių imtasi siekiant laikytis DPS principų, asmenų prašymų ir skundų nagrinėjimo mechanizmams ir kt.

[4] Gautus atsiliepimus galima rasti internete adresu https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/14379-ES-ir-JAV-duomenu-privatumo-sistema-Komisijos-ataskaita-del-sistemos-veikimo_lt.

[5] Peržiūros susitikimas organizuotas pagal temas, kiekvienas teminis darbotvarkės punktas pristatytas trumpu atitinkamos JAV institucijos, ES atstovo ar organizacijos pranešimu ir tada nuodugniai atsakyta į visus užduotus klausimus. Pirmąją susitikimo dieną aptarti sistemos komerciniai aspektai (t. y. reikalavimų, taikomų DPS sertifikuotoms bendrovėms, taikymas ir vykdymo užtikrinimas), o antrąją dieną svarstyti su valdžios sektoriaus prieiga prie asmens duomenų susiję klausimai.

Europos duomenų apsaugos priežiūros pareigūno tarnybos[6]. Atliekant peržiūrą, iš JAV pusės dalyvavo Prekybos departamento (DoC), Valstybės departamento, Federalinės prekybos komisijos (FTC), Transporto departamento (DoT), Nacionalinės žvalgybos direktoriaus biuro (ODNI), Teisingumo departamento (DoJ), žvalgybos bendruomenės generalinio inspektoriaus atstovai, taip pat Privatumo ir piliečių laisvių priežiūros valdybos (PCLOB) nariai. Be to, per atitinkamus peržiūros posėdžius informacijos suteikė organizacijų, teikiančių nepriklausomo ginčų sprendimo paslaugas, ir Amerikos arbitražo asociacijos atstovai. Atliekant peržiūrą taip pat remtasi iš DPS sertifikuotų organizacijų pranešimų apie tai, kaip bendrovės laikosi šios sistemos reikalavimų, gauta informacija.

Komisijos nustatyti faktai taip pat pagrįsti tokia viešai prieinama medžiaga kaip teismų sprendimai, atitinkamų JAV institucijų taikomos įgyvendinimo taisyklės ir procedūros, nevyriausybinių organizacijų ataskaitos ir tyrimai, DPS sertifikuotų bendrovių parengtos skaidrumo ataskaitos, nepriklausomų priežiūros įstaigų metinės ataskaitos ir žiniasklaidos pranešimai.

2. NUSTATYTI FAKTAI

2.1. Komerciniai aspektai

2.1.1. Sertifikavimo procesas

Kad galėtų gauti asmens duomenis, perduodamus iš ES pagal DPS, JAV bendrovė turi būti Prekybos departamento sertifikuota ir vėliau kasmet pakartotinai sertifikuojama kaip besilaikanti konkrečių duomenų apsaugos reikalavimų (toliau – DPS principai). Sertifikavimo reikalavimai yra tokie, kad bendrovės atžvilgiu būtų naudojamasi Federalinės prekybos komisijos ar Transporto departamento tyrimo ir vykdymo užtikrinimo įgaliojimais ir ji viešai deklaruotų savo įsipareigojimą laikytis DPS principų, viešai atskleistų savo privatumo politiką ir visapusiškai įgyvendintų tuos reikalavimus[7]. Prieš užbaigdamas sertifikavimo procedūrą Prekybos departamentas patikrina, ar bendrovė įvykdė visus sertifikavimo reikalavimus[8].

Peržiūros susitikime Prekybos departamentas paaiškino, kad šiais pirmaisiais DPS taikymo metais dėmesys sutelktas į sertifikavimo proceso diegimą, įskaitant tam skirtų IT priemonių kūrimą, procedūrų atnaujinimą, ryšių su bendrovėmis užmezgimą ir kitos įtraukimo ar informuotumo didinimo veiklos vykdymą. Peržiūros susitikimo dieną jau buvo daugiau kaip 2 800 DPS sertifikuotų bendrovių. Tai reiškia, kad DPS sertifikuotų bendrovių yra daugiau negu ankstesnėje – privatumo skydo – sistemoje pirmaisiais jos veikimo metais sertifikuotų bendrovių[9]. Iš Prekybos departamento pateiktos informacijos matyti, kad 70 proc. dalyvių yra MVĮ ir daug DPS dalyvaujančių bendrovių (47 proc.) veikia informacijos, ryšių ir technologijų (IRT) sektoriuje. Be to, 60 proc. bendrovių yra sertifikuotos tik dėl nesusijusių su žmogiškaisiais ištekliais duomenų, 2,5 proc. bendrovių yra sertifikuotos tik dėl žmogiškųjų išteklių duomenų, o 37,5 proc. – ir dėl žmogiškųjų išteklių duomenų, ir dėl nesusijusių su žmogiškaisiais ištekliais duomenų.

[6] Komisijos ir EDAV atstovai susitikimuose, įvykusiuose 2024 m. birželio 12 d. ir liepos 10 d., pasirengė peržiūrai, aptarė gautą informaciją ir nustatė, dėl kurių aspektų reikia papildomai surinkti informacijos ir pateikti išaiškinimą.

[7] Sprendimo dėl tinkamumo I priedo I.2 skirsnis.

[8] Sprendimo dėl tinkamumo III priedas.

[9] Per analogišką laikotarpį pagal privatumo skydo sistemą buvo sertifikuota 2 400 bendrovių.

Prekybos departamentas patvirtino reikiamas bendrovių paraiškų tvarkymo procedūras. Sertifikavimo paraiškas bendrovės turi teikti Prekybos departamento DPS svetainėje (https://www.dataprivacyframework.gov/). Joje pateikta informacijos apie tai, kaip prisijungti prie DPS[10], ir apie bendrovės pareigas šioje sistemoje[11]. Už visus su DPS valdymu ir administravimu susijusius aspektus, įskaitant sertifikavimo procesą ir atitikties stebėseną, atsako speciali Prekybos departamento darbo grupė, pavaldi paskirtam Duomenų privatumo sistemos direktoriui. Kiekviena paraiška paskiriama tvarkyti konkrečiam darbuotojui ir šis per visą sertifikavimo procesą yra atsakingas už atitinkamą bendrovę.

Kad būtų sertifikuota pagal sistemą, bendrovė pateikia paraišką, įskaitant privatumo politikos projektą. Prekybos departamentas patikrina, ar ji atitinka aktualius DPS reikalavimus. Kai organizacijos nori sertifikuoti atskirus bendrovių grupės subjektus (pvz., atskiras patronuojamąsias bendroves), Prekybos departamentas prašo pateikti ir peržiūri vieną visapusiškos privatumo politikos dokumentą, kuriame aiškiai nurodyti visi subjektai, kuriems jis taikomas, arba atskirus politikos dokumentus dėl kiekvieno subjekto. Be to, Prekybos departamentas dėl paraiškoje nurodyto nepriklausomo teisių gynimo mechanizmo (angl. *independent recourse mechanism*, IRM)[12] patikrina, ar organizacija iš tiesų yra užsiregistravusi juo naudotis. Dėl bendrovių, kurios yra pasirinkusios duomenų apsaugos institucijos kolegiją (pvz., dėl to, kad tvarko žmogiškųjų išteklių duomenis), Prekybos departamentas patikrina, ar bendrovė yra sumokėjusi reikiamus mokesčius, kad galėtų naudotis tokios kolegijos paslaugomis. Prireikus Prekybos departamentas taip pat patikrina, ar pareiškėjas priklauso Federalinės prekybos komisijos arba Transporto departamento jurisdikcijai (taigi ar jis atitinka prisijungimo prie DPS sąlygas).

Jeigu yra įvykdytos visos sąlygos, Prekybos departamentas informuoja organizaciją, kad ji gali savo interneto svetainėje paskelbti savo privatumo politiką su nuoroda į DPS. Kai privatumo politika jau yra viešai paskelbta, Prekybos departamentas patvirtina sertifikavimą ir įtraukia bendrovę į savo svetainėje skelbiamą DPS sąrašą. Asmens duomenis iš ES galima pagal DPS gauti nuo tos dienos, kai Prekybos departamentas įtraukia organizaciją į tą sąrašą[13].

Kaip paaiškinta peržiūros susitikime, Prekybos departamentui atlikus patikras iki šiol 33 paraiškos atmestos dėl to, kad neatitiko DPS reikalavimų. Paprastai Prekybos departamentas bendradarbiauja su bendrove siekdamas, kad bet kokie trūkumai būtų pašalinti. Kai Prekybos departamentas nustato trūkumų, jis informuoja bendrovę, kad ji turi juos pašalinti ir kad jei ji per nustatytą laikotarpį nepateiks atsakymo ar dėl kitų priežasčių nebaigs savo sertifikavimo pagal Prekybos departamento procedūras, bus laikoma, kad ji atsisakė paraiškos. Jei pirminis sertifikavimas nebaigiamas arba reikiami pakeitimai neatliekami per 12 mėnesių, Prekybos departamentas laiko, kad atsisakyta dalyvauti šiame procese.

Kasmetinio pakartotinio sertifikavimo terminas, taikomas kiekvienai bendrovei, yra nurodytas DPS sąraše. Siekdamas priminti bendrovėms, kad reikia prašyti pakartotinio sertifikavimo, Prekybos departamentas sukūrė sistemą, kurioje siunčiami priminimai, kad sertifikavimo galiojimas netrukus baigsis. Organizacijos gauna priminimą likus mėnesiui, tada likus dviem savaitėms ir, galiausiai, likus vienai dienai iki termino. Tos, kurie leidžia pasibaigti jų

[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] Privačiojo sektoriaus ginčų sprendimo mechanizmai, pagal kuriuos kiekvieno asmens skundai ir ginčai nagrinėjami ir greitai išsprendžiami, tam asmeniui nepatiriant jokių išlaidų.

[13] Sprendimo dėl tinkamumo I priedo I skirsnio 3 dalis.

sertifikavimo galiojimui, išbraukiamos iš DPS sąrašo. Kaip aprašyta sprendimo dėl tinkamumo III priede, Prekybos departamento svetainės atskirame skyrelyje pateiktame sąraše (angl. *inactive list*, toliau – nebedalyvaujančių organizacijų sąrašas) nurodytos JAV organizacijos, kurios nebėra aktyvios sistemos dalyvės, ir nurodytos atitinkamos priežastys, dėl kurių tos bendrovės išbrauktos iš dalyvių sąrašo (pvz., leido pasibaigti sertifikavimo galiojimui arba pasitraukė iš sistemos). Kai organizacijos išbraukiamos iš DPS sąrašo dėl to, kad leido pasibaigti sertifikavimo galiojimui, Prekybos departamentas su jomis susisiekia siekdamas sužinoti, ar jos nori pasitraukti iš sistemos, ar ketina atlikti pakartotinį sertifikavimą; pastaruoju atveju, kai jos ketina atlikti pakartotinį sertifikavimą, Prekybos departamentas siekia įsitikinti, kad tuo laikotarpiu, kai sertifikavimas yra nustojęs galioti, jos taiko DPS principus asmens duomenims, gautiems pagal DPS, ir išsiaiškinti, kokių veiksmų jos imsis likusioms problemoms, dėl kurių pakartotinis sertifikavimas atidėtas, išspręsti. Kai bendrovės praneša Prekybos departamentui, kad nori pasitraukti iš DPS, Prekybos departamentas reikalauja, kad jos nurodytų, ar grąžins arba ištrins pagal DPS gautus duomenis, ar juos toliau saugos ir tokiems duomenims toliau taikys DPS principus (tai turi būti patvirtinama kiekvienais metais), ar toliau saugos duomenis ir imsis kitų apsaugos priemonių (tokių kaip Europos Komisijos patvirtintos standartinės sutarčių sąlygos).

Iš prekybos asociacijų ir bendrovių gauti atsiliepimai rodo, kad DPS sertifikuotos bendrovės ėmėsi tam tikrų veiksmų DPS principų laikymuisi užtikrinti. Pavyzdžiui, siekdamos laikytis *teisių gynimo, vykdymo užtikrinimo ir atsakomybės principo* organizacijos atliko vidaus patikras, kurių forma buvo įsivertinimas arba išorinė reikalavimų laikymosi peržiūra. Du peržiūros susitikime dalyvavę privačiojo sektoriaus nepriklausomų teisių gynimo mechanizmų (IRM) teikėjai paaiškino, kad jie taip pat atlieka išorinę reikalavimų laikymosi peržiūrą, per kurią peržiūrima privatumo politika, o vienas iš privačiojo sektoriaus nepriklausomų teisių gynimo mechanizmų teikėjų paaiškino, kad jis taip pat atlieka auditus ir atsitiktines patikras, skirdamas dėmesį, pavyzdžiui, *prieigos*, *pasirinkimo* ir *tolesnio duomenų perdavimo* principams. Be to, sertifikuotos bendrovės yra parengusios vidaus reikalavimų laikymosi programas ir priežiūros mechanizmus, išmokiusios darbuotojus, įdiegusios mechanizmus, skirtus tam, kad asmenys galėtų naudotis savo teisėmis, atlikusios poveikio privatumui vertinimus ir peržiūrėjusios esamas sutartis.

2.1.2. Atitikties stebėsena, neteisingi teiginiai apie dalyvavimą ir vykdymo užtikrinimas

Pagal DPS Prekybos departamentas yra atsakingas už atitikties DPS principams stebėseną, vykdomą naudojant įvairias priemones, įskaitant *ex officio* patikras (atliekamas savo iniciatyva), *ad hoc* patikras vietoje ir atitikties klausimynus. Tai apima neteisingų teiginių apie dalyvavimą sistemoje paiešką ir jų šalinimą, pavyzdžiui, atliekant paiešką internete[14].

Prekybos departamentas, stebėdamas, kaip DPS dalyvaujančios bendrovės laikosi sistemos principų, praėjusiais metais daugiausia rėmėsi *ad hoc* paieškomis internete ir (socialinės) žiniasklaidos patikromis. Prekybos departamentas pranešė, kad tais pirmaisiais metais neaptiko DPS principų nesilaikymo problemų ir nei Federalinei prekybos komisijai, nei Transporto departamentui nenurodė jokių bendrovių, dėl kurių galėtų būti imamasi vykdymo užtikrinimo veiksmų. Jis taip pat įkūrė specialų kontaktinį centrą, kad būtų palengvintas bendradarbiavimas

[14] Žr. sprendimo dėl tinkamumo III priedą. Neteisingų teiginių gali atsirasti, pavyzdžiui, kai bendrovė teigia dalyvaujanti DPS, tačiau ji niekada nėra pradėjusi sertifikavimo proceso arba yra jį pradėjusi, bet neužbaigusi, arba yra leidusi pasibaigti sertifikavimo galiojimui.

su DAI, gaunami asmenų skundai ir priimami kitų institucijų (pvz., DAI ar Federalinės prekybos komisijos) perduodami nagrinėti klausimai. Vis dėlto praėjusiais metais jokių nagrinėtinų klausimų Prekybos departamentui neperduota, taip pat jis negavo jokių skundų. Pirmaisiais DPS veikimo metais pagrindinis dėmesys skirtas sistemos kūrimui ir sertifikavimo procesui, o peržiūros susitikime Prekybos departamentas paaiškino planuojantis atitikties patikras atlikti automatizuotai, kad jos būtų atliekamos sistemingiau, ir šiuo metu kuriantis tam reikalingas IT priemones.

Komisija pripažįsta, kad Prekybos departamentui per šiuos pirmuosius metus daugiausia pastangų reikėjo skirti sistemos kūrimui ir sertifikavimo procesui. Ateityje svarbu, kad Prekybos departamentas sustiprintų pastangas stebėti ir tikrinti sistemos principų laikymąsi, nes tai būtina siekiant užtikrinti, kad sistemos reikalavimų laikymosi lygis nuolat būtų aukštas, ir nustatyti atvejus (įskaitant galimus neteisingus bendrovių teiginius apie dalyvavimą), kai reikia imtis tolesnių vykdymo užtikrinimo veiksmų. Šiuo atžvilgiu Komisija palankiai vertina tai, kad Prekybos departamentas patvirtino ketinantis kurti ir naudoti (automatizuotas) priemones tam, kad veiksmingiau ir sistemingiau nustatytų atitikties problemas ir neteisingus teiginius, ir mano, kad tai turėtų būti priskirta prie bendrų pastangų daugiau naudotis įvairiomis turimomis priemonėmis (pvz., patikromis vietoje, reikalavimų laikymosi peržiūros klausimynais, prašymais suteikti informaciją ir kt.), be kita ko, tikrinant atitiktį konkretiems DPS reikalavimams[15].

DPS dalyvaujančios organizacijos priklauso Federalinės prekybos komisijos ir Transporto departamento jurisdikcijai. Transporto departamentas peržiūros susitikime patvirtino esąs įdiegęs visus procesus, reikalingus, kad būtų imamasi tinkamų vykdymo užtikrinimo veiksmų. Jis taip pat paaiškino, kad prie DPS prisijungė labai nedaug bendrovių, priklausančių jo jurisdikcijai (t. y. prisijungė keli bilietų pardavėjai, tačiau neprisijungė jokių oro transporto bendrovių). Federalinė prekybos komisija patvirtino, kad atlikdama kiekvieną savo tyrimą dėl privatumo ji nuosekliai tikrina, ar nėra DPS pažeidimų. Federalinei prekybos komisijai kitos institucijos iki šiol neperdavė jokių nagrinėtinų klausimų. Ji gavo kelis skundus, kuriuose minima DPS, nors du iš jų susiję su bendrovėmis, įtrauktomis į nebedalyvaujančių organizacijų sąrašą, kiti du – su bendrovėmis, nedalyvaujančiomis šioje sistemoje, o vienas skundas nesusijęs su asmens duomenimis, perduotais iš ES. Tuo metu, kai atlikta ši peržiūra, Federalinė prekybos komisija dar nebuvo priėmusi jokių sprendimų užtikrinti DPS reikalavimų vykdymą, nors ji patvirtino, kad šiuo metu atliekamas tyrimas dėl kelių DPS sertifikuotų bendrovių.

Komisija palankiai vertina tai, kad Federalinė prekybos komisija per visus savo tyrimus dėl privatumo nuosekliai tikrina, ar nėra DPS pažeidimų. Kadangi tolesnis DPS veiksmingumas priklauso nuo griežto jos reikalavimų vykdymo užtikrinimo, tikimasi, kad Federalinė prekybos komisija toliau naudosis savo tyrimo įgaliojimais šioje sistemoje, be kita ko, iniciatyviai imdamasi koordinuotų veiksmų, sutelktų į konkrečių DPS reikalavimų laikymąsi ir (arba) reikalavimų laikymąsi tam tikruose sektoriuose.

2.1.3. Skundų nagrinėjimas

ES asmenims DPS suteikta įvairių galimybių ginti savo teises tais atvejais, kai sertifikuotos organizacijos nesilaiko DPS principų[16]. Tai apima problemos sprendimą tiesiogiai susisiekiant

[15] Pavyzdžiui, kai tai susiję su tolesniu duomenų perdavimu, naudojantis galimybe pagal DPS 3 principo b punktą reikalauti pateikti atitinkamų privatumo nuostatų, įtrauktų į tolesnio duomenų perdavimo sutartis, santrauką ar reprezentatyvią jų kopiją.

[16] Žr. sprendimo dėl tinkamumo 2.4 skirsnį.

su DPS dalyvaujančia organizacija, o ši privalo pateikti nukentėjusiam asmeniui atsakymą per 45 dienas. Asmenys taip pat gali pateikti skundą nagrinėti pagal nepriklausomą teisių gynimo mechanizmą (IRM), kurį organizacija yra paskyrusi skundams nagrinėti ir spręsti. Priklausomai nuo aplinkybių, tai gali būti alternatyvaus ginčų sprendimo įstaiga arba DAI[17]. Galiausiai, jei duomenų subjekto skundas nėra patenkinamai išsprendžiamas jokiais kitais prieinamais teisių gynimo būdais, asmenys gali, kaip kraštutinę priemonę, inicijuoti privalomą arbitražą ES ir JAV DPS kolegijoje.

2.1.3.1. Skundų nagrinėjimas bendrovėse

Iš prekybos asociacijų ir bendrovių atsakymų į Komisijos nusiųstus klausimynus matyti, kad DPS sertifikuotos bendrovės yra gavusios labai nedaug (arba visai negavusios) asmenų skundų dėl DPS principų nesilaikymo. Be to, bendrovės yra įdiegusios įvairius mechanizmus ir priemones, kad asmenys galėtų naudotis savo teisėmis ir teikti skundus, be kita ko, užpildydami formas internetu, kreipdamiesi e. paštu ir telefonu.

2.1.3.2. *Nepriklausomi teisių gynimo mechanizmai (IRM)*

Iš peržiūros susitikime gautų atsiliepimų ir iš prekybos asociacijų suteiktos informacijos matyti, kad skundų, pateiktų nagrinėti pagal nepriklausomus ginčų sprendimo mechanizmus, būta labai nedaug. Tarp bendrovių pasirinktų nepriklausomų teisių gynimo mechanizmų yra „BBB National Programs“, JAMS, TRUSTe ir „VeraSafe“. Pagal DPS reikalavimus nepriklausomų teisių gynimo mechanizmų teikėjai privalo skelbti metines ataskaitas su suvestiniais statistiniais duomenimis apie naudojimąsi jų ginčų sprendimo paslaugomis. Tuo metu, kai priimta ši ataskaita, jau buvo paskelbtos visų atitinkamų nepriklausomų teisių gynimo mechanizmų metinės ataskaitos[18].

Be to, per peržiūros susitikimą BBB ir „VeraSafe“ išsamiuose pranešimuose apžvelgė savo praėjusių metų veiklą. Šie nepriklausomų teisių gynimo mechanizmų teikėjai pranešė, kad, palyginti su padėtimi pagal ankstesnes sistemas, verslo dalyvių, kurie renkasi jų paslaugas, skaičius padidėjo, ir nurodė gavę skundų, nors didžioji dauguma jų nebuvo tinkami nagrinėti. Pavyzdžiui, BBB gavo 87 skundus iš ES asmenų, tačiau tik du iš jų buvo tinkami nagrinėti. BBB paaiškino, kad skundai išnagrinėjami vidutiniškai per 5 darbo dienas, tačiau tų dviejų skundų nagrinėjimas galiausiai sustabdytas dėl to, kad negauta atsakymo iš atitinkamų asmenų.

[17] DPS dalyvaujančios organizacijos privalo bendradarbiauti per DAI atliekamą tyrimą ir skundo sprendimą, kai tai susiję su žmogiškųjų išteklių duomenų, surinktų darbo santykių aplinkybėmis, tvarkymu arba kai atitinkama organizacija yra savanoriškai sutikusi būti DAI prižiūrima.

[18] ANA: https://www.ana.net/content/show/id/accountability-dpf-consumers;
„BBB National Programs“: https://assets.bbbprograms.org/docs/default-source/eu-privacy-shield/dpf_periodicalreport_072024.pdf; ICDR – AAA: https://go.adr.org/rs/294-SFS-516/images/Data%20Privacy%20Framework%20IRM%20Program%20Report%202023-2024%20FINAL.pdf?version=0;
„Insights Association“: https://www.insightsassociation.org/Portals/INSIGHTS/Insights%20Association%20DPF%20Services%20Program%202024%20Annual%20Report_Final_1.pdf;
JAMS: https://www.jamsadr.com/files/Uploads/Documents/2024-Annual-Report-DPF-Cases.pdf;
„Privacy Trust DPF Services“: https://privacytrust.com/fserve/PrivacyTrust_Dispute_Resolution_Report_2023_2024.pdf;
„TRUSTe Dispute Resolution“: https://trustarc.com/wp-content/uploads/2024/07/2024-Independent-Recourse-Mechanism-Annual-Report.pdf;
„Verasafe“: https://verasafe.com/wp-content/uploads/2020/06/VeraSafe-DPF-Dispute-Resolution-Program-Annual-Report-2024.pdf.

„VeraSafe“ gavo 26 skundus, šeši iš jų buvo tinkami nagrinėti. Du iš pastarųjų skundų buvo susiję su prašymais leisti susipažinti su duomenimis ir ištrinti duomenis ir buvo išspręsti, du skundai tebėra neišnagrinėti, o likę du buvo atsiimti arba jų nagrinėjimas sustabdytas dėl to, kad negauta atitinkamo asmens atsakymo. Abu nepriklausomų teisių gynimo mechanizmų teikėjai paaiškino, kad stengiasi į skundą atsakyti jį pateikusio asmens kalba.

DPS dalyvaujančios bendrovės, kurios tvarko iš ES perduotus žmogiškųjų išteklių duomenis, turi pasirinkti ES duomenų apsaugos institucijas (DAI) kaip savo nepriklausomą teisių gynimo mechanizmą dėl tų duomenų, o dėl kitų rūšių asmens duomenų, perduodamų remiantis DPS, DPS dalyvaujanti bendrovė gali savanoriškai rinktis ES DAI kaip savo nepriklausomą teisių gynimo mechanizmą. Tuo metu, kai buvo atliekama peržiūra, iš tiesų daugiau kaip pusė DPS sertifikuotų bendrovių buvo pasirinkusios šį sprendimą[19], o tai yra vertinama palankiai. Priėmus sprendimą dėl tinkamumo, EDAV vėliau patvirtino neformalios ES DAI kolegijos darbo tvarkos taisykles. Kai yra neišspręstų pagal DPS pateiktų skundų, kuriuos asmenys pateikė dėl asmens duomenų, perduotų iš ES pagal DPS, tvarkymo, ši kolegija turi kompetenciją pateikti JAV organizacijoms rekomendacijų, į kurias atsižvelgti privaloma. Kolegiją pagal jos darbo tvarkos taisykles sudaro viena DAI, veikianti kaip vadovaujanti DAI, ir kitos paskirtosios DAI, kartu atliekančios peržiūrą[20]. Ji per 60 dienų nuo skundo pagal DPS gavimo pateikia rekomendacijas, į kurias atsižvelgti privaloma. EDAV taip pat yra paskelbusi pavyzdinę skundo formą, skirtą skundams DAI teikti[21], ir dažnai užduodamų klausimų rinkinius (DUK) Europos asmenims[22] ir įmonėms[23] apie DPS. Tuo metu, kai atlikta peržiūra, ši kolegija dar nebuvo gavusi jokių skundų.

2.1.3.3. Privalomas arbitražo mechanizmas

Privalomo arbitražo mechanizmo administratoriumi Prekybos departamentas išrinko Tarptautinį ginčų sprendimo centrą (angl. *International Centre for Dispute Resolution*, ICDR), kuris yra Amerikos arbitražo asociacijos tarptautinis padalinys. Priėmus sprendimą dėl tinkamumo, Prekybos departamentas kartu su Komisija išrinko 11 arbitrų, turinčių patirties privatumo srityje ir kompetentingų įvairiose srityse, įskaitant arbitražą, teismų sistemą, akademinę bendruomenę ir pilietinę visuomenę[24]. Be to, patvirtintos DPS kolegijos arbitražo taisyklės[25] ir arbitrų elgesio kodeksas[26]; visi šie dokumentai yra prieinami ICDR interneto svetainėje. Tuo metu, kai buvo atliekama peržiūra, dar nebuvo ES asmenų, pasinaudojusių arbitražo mechanizmu.

2.1.4. Gairės, bendradarbiavimas ir informuotumo didinimas

[19] Netrukus po tos dienos, kurią įvyko peržiūros susitikimas, DPS interneto svetainėje nurodyta, kad 1 511 iš 2 892 sistemos dalyvių kaip teisių gynimo mechanizmą yra pasirinkę ES duomenų apsaugos instituciją.
[20] 2024 m. balandžio 17 d. EDAV patvirtino neformalios ES DAI kolegijos, veikiančios pagal ES ir JAV duomenų privatumo sistemą, darbo tvarkos taisykles. Su jomis galima susipažinti internete adresu https://www.edpb.europa.eu/system/files/2024-04/dpf_rules-of-procedure_informal-panel-dpas_en.pdf.
[21] https://www.edpb.europa.eu/our-work-tools/our-documents/other-guidance/eu-us-data-privacy-framework-template-complaint-form_lt.
[22] https://www.edpb.europa.eu/our-work-tools/our-documents/other-guidance/eu-us-data-privacy-framework-faq-european-individuals_lt.
[23] https://www.edpb.europa.eu/our-work-tools/our-documents/other-guidance/eu-us-data-privacy-framework-faq-european-businesses_lt.
[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.

Nuo DPS įsigaliojimo Prekybos departamentas vykdo įvairią informuotumo didinimo veiklą organizuodamas informacines keliones, internetinius seminarus ir konferencijas, susisiekdamas su prekybos asociacijomis ir tiesiogiai palaikydamas ryšius su daugiau kaip 3 000 bendrovių, kad būtų suteikta informacijos apie DPS. Jis taip pat yra paskelbęs gairių, be kita ko, dažnai užduodamų klausimų (DUK) forma, asmenims, taip pat ES ir JAV įmonėms[27]. EDAV savo ruožtu parengė skundų formas ir DUK asmenims ir įmonėms. Be to, priimdama sprendimą dėl tinkamumo Komisija paskelbė klausimų ir atsakymų rinkinį ir informacijos suvestinę apie DPS[28].

Be to, peržiūros susitikime išaiškėjo, kad reikia įdėti daugiau darbo siekiant didinti asmenų informuotumą ir suteikti gairių bendrovėms. Iš bendrovių ir nepriklausomų teisių gynimo mechanizmų teikėjų pateiktos informacijos ir iš to, kad yra labai nedaug skundų, atrodo, kad asmenys gali ne visada žinoti apie savo teises ir (arba) naudojimosi jomis mechanizmą. Peržiūros susitikime Prekybos departamentas išreiškė norą bendradarbiauti su ES DAI didinant ES asmenų informuotumą apie DPS. Komisija skatina tokias iniciatyvas ir taip pat imasi veiksmų, kad asmenys būtų geriau informuoti, be kita ko, savo interneto svetainėje pateikia papildomos informacijos apie DPS, pavyzdžiui, įtraukdama hipersaitus ir nuorodas į atitinkamus EDAV, Prekybos departamento ir kitų JAV institucijų priimtus rekomendacinius dokumentus.

Kalbant apie gaires dėl DPS principų, peržiūros susitikime EDAV atstovai susitarė ateinančiais mėnesiais bendradarbiauti, kad būtų išsamiau paaiškinta žmogiškųjų išteklių duomenų samprata pagal DPS ir konkrečios pareigos, taikomos tvarkant tokius duomenis. Nagrinėti įvairūs elementai, kuriuos reikėtų įtraukti į tokias gaires. Pavyzdžiui, šiose gairėse būtų galima aptarti tam tikrus praktinius scenarijus, kai darbuotojų duomenys būtų tvarkomi (pvz., debesijos paslaugų teikėjo) pagal DPS, ir paaiškinti, kurios pareigos pagal DPS būtų aktualios. Be to, šiose gairėse būtų galima pasiūlyti bendrovėms, kurios gauna ES asmenų – darbuotojų – duomenis (bet nebūtinai naudoja tokius duomenis darbo santykių aplinkybėmis), kaip savo nepriklausomą teisių gynimo mechanizmą pasirinkti DAI kolegiją. Taip būtų užtikrinta, kad tie asmenys galėtų kreiptis į instituciją, kuri būtų „arčiau namų“ ir prireikus turėtų daugiau žinių apie taikytinus nacionalinės teisės aktus, kurie taikomi žmogiškųjų išteklių duomenims.

Be to, konkretus aspektas, dėl kurio, atrodo, būtų naudinga (remiantis ir iš prekybos asociacijų gauta informacija) pateikti daugiau gairių, yra DPS reikalavimai dėl tolesnio duomenų perdavimo. Prekybos departamentas taip pat nurodė, kad vertėtų ištirti, ar kai kuriems sektoriams gali būti naudinga gauti papildomų gairių dėl DPS principų taikymo jų veiklai, pavyzdžiui, sveikatos mokslinių tyrimų ir finansinių paslaugų srityse.

Komisija palankiai vertina abipusį pasirengimą rengti gaires ir tikisi, kad darbas minėtomis temomis bus pradėtas netrukus.

Apskritai yra sukurti keli mechanizmai siekiant užtikrinti mainus ir bendradarbiavimą tarp JAV institucijų ir DAI, be kita ko, paskirti specialūs kontaktiniai centrai Federalinėje prekybos komisijoje ir Prekybos departamente DAI užklausoms ir perduotiems klausimams nagrinėti.

2.1.5. Aktualūs JAV teisinės sistemos pokyčiai

[27] Žr., pvz., https://www.dataprivacyframework.gov/US-Businesses.
[28] https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/eu-us-data-transfers_lt.

Nuo tada, kai priimtas sprendimas dėl tinkamumo, JAV teisinėje sistemoje įvyko tam tikrų pokyčių privatumo srityje. Tai, be kita ko, buvo teisėkūros, reguliavimo ir teismų praktikos pokyčiai. Šie pokyčiai iš esmės rodo, kad ES ir JAV požiūriai į tam tikrus su privatumu susijusius iššūkius vis labiau sutampa, be kita ko, vartojamos panašios teisinės sąvokos. Kai kurie iš šių pokyčių tebevyksta ir reikės juos toliau stebėti.

Federaliniu lygmeniu Prezidentas priėmė kelis asmens duomenų naudojimui aktualius vykdomuosius potvarkius (angl. *Executive Orders*, EO). Visų pirma, 2024 m. vasario 28 d. Vykdomuoju potvarkiu Nr. 14117[29] uždrausti arba apriboti sandoriai, apimantys tam tikrų kategorijų neskelbtinus asmens duomenis (pvz., sveikatos duomenis, biometrinius identifikatorius, žmogaus genominius duomenis), su kai kurių susirūpinimą keliančių šalių[30] subjektais. Priimtu potvarkiu generaliniam prokurorui nurodyta siūlyti reglamentavimo aktus, kuriais šio potvarkio įgyvendinimas būtų labiau konkretizuotas (tuo metu, kai priimta ši ataskaita, tokių aktų dar nebuvo priimta). Be to, 2023 m. spalio 30 d. Vykdomajame potvarkyje Nr. 14110 dėl dirbtinio intelekto[31] orientuojamasi į saugaus, apsaugoto ir patikimo dirbtinio intelekto kūrimą. Jame reikalaujama, kad kelios federalinės agentūros parengtų su DI susijusius saugos standartus ir gaires, be kita ko, dėl konkrečios su DI susijusios rizikos privatumui ir dėl privatumo išsaugojimo būdų.

Teisėkūros darbe per kelerius pastaruosius metus Kongrese pateikti federalinių privatumo įstatymų projektai, o iki 2024 m. liepos mėn. 20 JAV valstijų priėmė visapusiškus privatumo įstatymus; aštuoniose iš jų – Kalifornijoje, Kolorade, Oregone, Virdžinijoje, Konektikute, Jutoje, Teksase ir Floridoje – tie įstatymai jau pradėti taikyti. Be to, 17 JAV valstijų priėmė teisės aktus, kuriais reglamentuojamas automatizuotas duomenų tvarkymas (ar bent kai kurios jo formos) ir iš esmės suteikiama galimybė atsisakyti asmens duomenų tvarkymo per tam tikro pobūdžio sprendimų priėmimo, grindžiamo profiliavimu, procesus[32].

Kalbant apie teismų praktikos pokyčius, keli pilietinės visuomenės atstovai atkreipė dėmesį į neseniai priimtą Aukščiausiojo Teismo sprendimą byloje *Loper Bright Enterprises v. Raimondo*

---

[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] Tarp šių šalių (angl. *countries of concern*), kaip 2024 m. gegužės 3 d. paskelbtame išankstiniame pranešime apie siūlomą taisyklių nustatymą (angl. *Advance Notice of Proposed Rulemaking*) pasiūlė generalinis prokuroras, yra Honkongas ir Makao, Iranas, Kinija, Kuba, Šiaurės Korėja ir Venesuela. Žr. https://www.federalregister.gov/documents/2024/03/05/2024-04594/national-security-division-provisions-regarding-access-to-americans-bulk-sensitive-personal-data-and.

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

[32] Nors profiliavimo samprata įvairiose valstijose šiek tiek skiriasi, profiliavimas bendrai apibrėžiamas kaip bet kokios formos automatizuotas asmens duomenų tvarkymas, atliekamas siekiant įvertinti, analizuoti ar prognozuoti individualius su fizinio asmens, kurio tapatybė yra žinoma arba gali būti nustatyta, ekonomine padėtimi, sveikata, asmeniniais prioritetais, interesais, patikimumu, elgesiu, buvimo vieta ar judėjimu susijusius aspektus. Paprastai galimybę atsisakyti asmens duomenų tvarkymo, atliekamo profiliavimo tikslais, turi vartotojai. Teisės aktus dėl profiliavimo yra parengusios šios valstijos: Koloradas (*Colo. Rev. Stat. Ann. § 6-1-1306*), Konektikutas (*Conn. Gen. Stat. Ann. § 42-518*), Delaveras (*Del. Code Ann. tit. 6, § 12D-104*), Florida (*Fla. Stat. Ann. § 501.705*), Indiana (*Ind. Code Ann. § 24-15-3-1*), Kentukis (*Ky. Rev. Stat. Ann. § 367.3615*), Merilendas (*Maryland Online Data Privacy Act of 2024*, priimta 2024 m. gegužės 9 d.), Minesota (*Minn. Stat. Ann. § 325O.07*), Montana (*Mont. Code Ann. § 30-14-2808*), Nebraska (*Neb. Rev. Stat. Ann. § 87-1107*), Naujasis Hampšyras (*N.H. Rev. Stat. Ann. § 507-H:4*), Naujasis Džersis (*N.J. Stat. Ann. § 56:8-166.8*), Oregonas (*Or. Rev. Stat. Ann. § 646A.574*), Rod Ailandas (*Rhode Island Data Transparency and Privacy Protection Act*, priimta 2024 m. birželio 29 d.), Tenesis (*Tenn. Code Ann. § 47-18-3304*), Teksasas (*Tex. Bus. & Com. Code Ann. § 541.051*) ir Virdžinija (*Va. Code Ann. § 59.1-577*).

(2024 m. birželio 28 d.). Šiuo sprendimu paneigta ankstesnė teismų praktika dėl *Chevron* doktrinos, pagal kurią teismai vadovaujasi principu, kad tuo atveju, kai reguliavimo agentūros vykdomo įstatymo nuostatose esama dviprasmiškumo, viršenybė teiktina tos agentūros pateiktam pagrįstam teisės aiškinimui. Visų pirma, kai kurios NVO išreiškė susirūpinimą dėl šio Aukščiausiojo Teismo sprendimo poveikio Federalinės prekybos komisijos įgaliojimams nustatyti taisykles privatumo srityje, kartu pripažindamos, kad tai gali neturėti jokio poveikio jos turimiems vykdymo užtikrinimo įgaliojimams arba toks poveikis gali būti ribotas. Peržiūros susitikime Federalinė prekybos komisija informavo, kad dar per anksti tiksliai žinoti, koks bus šio teismo sprendimo poveikis. Kartu ji paaiškino, kad Federalinės prekybos komisijos taisyklės nustatomos pagal Federalinės prekybos komisijos įstatymu (angl. *Federal Trade Commission Act*) suteiktus įgaliojimus, kurie skiriasi nuo kitų administracinių agentūrų įgaliojimų ir kuriems *Chevron* doktrina mažiau aktuali. Taigi neseniai priimto teismo sprendimo poveikis šioje srityje gali būti ribotas.

Be to, Federalinė prekybos komisija informavo apie tai, kaip pastaruoju metu keitėsi jos požiūris į automatizuotą duomenų tvarkymą ir dirbtinį intelektą. Be kita ko, priimtas bendras pareiškimas kartu su kitomis vykdymo užtikrinimo institucijomis dėl kovos su diskriminavimu ir šališkumu automatizuotose sistemose[33], taip pat imtasi kelių vykdymo užtikrinimo veiksmų, kuriuos vykdydama Federalinė prekybos komisija dėmesį kreipia, be kita ko, į skaidrumą, automatizuoto duomenų tvarkymo sąžiningumą ir asmenų gebėjimą užginčyti rezultatus. Reikšmingiausias šiuo atžvilgiu atvejis yra 2024 m. kovo mėn. Federalinės prekybos komisijos sprendimas, nepalankus bendrovei „Rite Aid“, kuriuo nustatytas draudimas tai bendrovei 5 metus naudoti veido atpažinimo technologiją saugumo tikslais[34]. Visų pirma Federalinė prekybos komisija nustatė, kad bendrovė „Rite Aid“ nesiėmė pagrįstų priemonių, kuriomis būtų išvengiama klaidingų rezultatų ir vartotojai būtų informuojami apie naudojamą technologiją. Peržiūros susitikime Federalinė prekybos komisija bendrai aptarė savo dabartinius prioritetus ir išskyrė sritis, kuriose, jos nuomone, ateityje vertėtų pereiti prie iniciatyvesnio požiūrio į vykdymo užtikrinimą. Tai apima neskelbtinų duomenų (pvz., sveikatos duomenų, biometrinių duomenų, geografinės buvimo vietos duomenų)[35] apsaugą, vaikų[36] ir nepilnamečių apsaugą internete ir duomenų saugumą[37].

Komisija toliau atidžiai stebės šiuos ir kitus pokyčius JAV, visų pirma bet kokius tolesnius veiksmus, kurių imamasi siekiant priimti visapusišką federalinį privatumo įstatymą, ir galimą

[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] Pvz., žr. naujausią Federalinės prekybos komisijos nutarimą prieš bendrovę „X-Mode“ dėl neskelbtinos buvimo vietos informacijos pardavimo ir dalijimosi ja (https://www.ftc.gov/system/files/ftc_gov/pdf/X-ModeSocialDecisionandOrder.pdf) ir nutarimą prieš bendrovę „Monument“ dėl neskelbtinų sveikatos duomenų atskleidimo trečiosioms šalims rinkodaros tikslais (https://www.ftc.gov/system/files/ftc_gov/pdf/MonumentOrderFiled.pdf).

[36] Pavyzdžiui, Federalinė prekybos komisija neseniai pranešė apie tyrimą, po kurio pareikštas ieškinys bendrovei „TikTok“ ir jos patronuojančiajai bendrovei „Bytedance“ dėl įtariamo vaikų privatumo teisės nuostatų pažeidimo. Abi bendrovės įtariamos nesilaikiusios reikalavimo, kad prieš renkant ir naudojant vaikų iki 13 metų asmens duomenis būtų apie tai pranešta tėvams ir būtų gautas tėvų sutikimas (https://www.ftc.gov/news-events/news/press-releases/2024/08/ftc-investigation-leads-lawsuit-against-tiktok-bytedance-flagrantly-violating-childrens-privacy-law).

[37] Žr. pastarojo meto vykdymo užtikrinimo veiklos apžvalgą: The FTC 2023 Privacy and Data Security Update. https://ec.europa.eu/commission/presscorner/detail/en/mex_24_1307.

naujausios Aukščiausiojo Teismo praktikos poveikį Federalinės prekybos komisijos vaidmeniui privatumo srityje.

Komisija palankiai vertina Federalinės prekybos komisijos suteiktą informaciją apie jos pastarojo meto vykdymo užtikrinimo veiklą ir dabartinius prioritetus, kurie daugeliu atžvilgių atitinka duomenų apsaugos užtikrinimo Europoje tendencijas ir prioritetus. Federalinė prekybos komisija taip pat aktyviai dalyvauja tinklo, vienijančio valstybes, kurioms yra palankus 2024 m. kovo mėn. Komisijos priimtas ES sprendimas dėl tinkamumo, veikloje[38]. Ši didesnė konvergencija turėtų paskatinti ir palengvinti glaudesnį privatumo apsaugą užtikrinančių institucijų abiejose Atlanto pusėse bendradarbiavimą, visų pirma su DPS veikimu susijusiais klausimais.

2.2. Aspektai, kurie yra aktualūs, kai JAV viešojo sektoriaus institucijos turi prieigą prie asmens duomenų, perduodamų pagal ES ir JAV duomenų privatumo sistemą, ir naudoja tuos duomenis

Sprendime dėl tinkamumo išsamiai įvertintos taisyklės, kuriomis reglamentuojama, kaip JAV viešojo sektoriaus institucijos renka ir naudoja (visų pirma baudžiamosios teisėsaugos ir nacionalinio saugumo tikslais) asmens duomenis, iš ES perduodamus DPS sertifikuotoms bendrovėms. Nuo tada, kai priimtas sprendimas dėl tinkamumo, per pirmuosius DPS taikymo metus nebuvo reikšmingų pokyčių, susijusių su teisine sistema dėl prieigos prie duomenų teisėsaugos ar reguliavimo tikslais (JAV institucijos tai patvirtino peržiūros susitikime). Taigi, nustatyti faktai, kurie išdėstyti toliau, yra susiję tik su pokyčiais nacionalinio saugumo srityje.

Sprendime dėl tinkamumo padarytos išvados dėl žvalgybos agentūrų prieigos prie duomenų yra pagrįstos analize dėl sąlygų ir apribojimų, taikomų signalų žvalgybos operacijoms pagal kelis aktualius teisinius pagrindus, visų pirma Užsienio žvalgybos stebėjimo įstatymo (angl. *Foreign Intelligence Surveillance Act*, toliau – FISA) 702 straipsnį ir Vykdomąjį potvarkį Nr. 12333[39], papildytą ir sugriežtintą 2022 m. spalio 7 d. JAV prezidento priimtu Vykdomuoju potvarkiu Nr. 14086 dėl Jungtinių Valstijų vykdomoje signalų žvalgyboje taikomų apsaugos priemonių griežtinimo (EO 14086). Vykdomajame potvarkyje Nr. 14086 nustatytos apsaugos priemonės taikomos visoje JAV signalų žvalgybos veikloje nepriklausomai nuo tokios veiklos teisinio pagrindo ir vykdymo vietos ir jomis apsaugomi ne JAV asmenų (įskaitant europiečius) duomenys[40]. Vykdomuoju potvarkiu Nr. 14086 taip pat nustatytas naujas teisių gynimo mechanizmas, pagal kurį asmenys Europos Sąjungoje gali pasinaudoti šiomis privalomomis apsaugos priemonėmis ir užtikrinti jų taikymą.

Tolesniuose skirsniuose apibūdinami veiksmai, kurių nuo tada, kai priimtas sprendimas dėl tinkamumo, JAV institucijos ėmėsi laikydamosi Vykdomojo potvarkio Nr. 14086, taip pat aktualūs su pirmiau nurodyta teisine sistema susiję pokyčiai.

---

[38] Žr. https://ec.europa.eu/commission/presscorner/detail/en/mex_24_1307. Po 2024 m. kovo mėn. įvykusio susitikimo nuspręsta surengti teminių posėdžių ciklą. Pirmasis iš jų įvyko 2024 m. liepos mėn.: jame dėmesys skirtas priemonių, kuriomis galima padėti mažosioms ir vidutinėms įmonėms laikytis privatumo teisės aktų, kūrimui.

[39] Kitos priemonės, kurių pagal FISA gali būti imamasi dėl duomenų, perduodamų iš ES, yra individualizuotas elektroninis stebėjimas (FISA 105 straipsnis), fizinė krata (FISA 302 straipsnis), renkamų telefono numerių registrų arba gaunamų skambučių sekiklių naudojimas (FISA 402 straipsnis) ir tam tikrų bendrovių (viešojo transporto vežėjų, viešųjų apgyvendinimo įstaigų, transporto priemonių nuomos įstaigų ar saugyklų) verslo įrašų rinkimas (FISA 501 straipsnis). Šie įvairūs teisiniai pagrindai išsamiai išnagrinėti sprendime dėl tinkamumo (142–152 konstatuojamosiose dalyse).

[40] Daugiau informacijos apie tai pateikta sprendimo dėl tinkamumo 3.2.1.2 skirsnyje.

2.2.1. Aktualūs su JAV teisine sistema susiję pokyčiai

2.2.1.1. Vykdomojo potvarkio Nr. 14086 įgyvendinimas žvalgybos agentūrose

Vykdomuoju potvarkiu Nr. 14086 nustatytais apribojimais ir apsaugos priemonėmis papildyti FISA 702 straipsnyje ir Vykdomajame potvarkyje Nr. 12333 nustatyti apribojimai ir apsaugos priemonės. Jie yra privalomi visoms žvalgybos agentūroms ir toliau įgyvendinami pagal kiekvienos agentūros patvirtintą politiką ir procedūras.

Per pirmąją peržiūrą JAV institucijos patvirtino, kad Vykdomojo potvarkio Nr. 14086 priėmimo jo pakeitimų nepadaryta. Taip pat paaiškinta, kad JAV prezidentas nesinaudojo Vykdomojo potvarkio Nr. 14086 2 straipsnio b punkto i papunkčio B dalyje ir 2 straipsnio b punkto ii papunkčio C dalyje numatytais įgaliojimais atnaujinti signalų žvalgybos teisėtų tikslų sąrašą arba tikslų, kuriems gali būti naudojami masiškai renkami duomenys, sąrašą[41]. Vykdomuoju potvarkiu Nr. 14086 nustatyta konkreti procedūra, pagal kurią nustatomi konkretesni žvalgybos prioritetai, kuriems iš tiesų gali būti renkami signalų žvalgybos duomenys. Visų pirma turi būti pasikonsultuota su Nacionalinės žvalgybos direktoriaus biuro (ODNI) piliečių laisvių apsaugos pareigūnu siekiant dėl kiekvieno prioriteto įvertinti, ar 1) pagal jį daroma pažanga siekiant vieno arba daugiau tame vykdomajame potvarkyje nurodytų teisėtų tikslų, 2) jis nėra nustatytas tam, kad signalų žvalgybos duomenys būtų renkami draudžiamu tikslu, nurodytu tame vykdomajame potvarkyje, ir nenumatoma, kad jis turėtų tokį poveikį, ir 3) jis yra nustatytas tinkamai atsižvelgiant į visų asmenų privatumą ir pilietines laisves[42]. Peržiūros susitikime ODNI piliečių laisvių apsaugos pareigūnė (ODNI CLPO) patvirtino, kad ji peržiūrėjo nacionalinės žvalgybos direktorės 2023 m. nacionalinėje žvalgybos prioritetų programoje pasiūlytus prioritetus, padarė išvadą, kad jie atitinka minėtus reikalavimus, ir perdavė savo išvadą nacionalinės žvalgybos direktorei, o ši pateikė tuos prioritetus Prezidentui patvirtinti. ODNI CLPO taip pat teikė su Vykdomojo potvarkio Nr. 14086 reikalavimais susijusį mokymą tiems žvalgybos bendruomenės nariams, kurie dalyvauja nustatant žvalgybos prioritetus.

Be to, JAV institucijos praėjusiais metais ėmėsi tolesnių praktinių veiksmų įgyvendindamos Vykdomąjį potvarkį Nr. 14086 savo kasdienėje veikloje. Visų pirma, žvalgybos agentūros nustatė tolesnę to vykdomojo potvarkio taikymo vidaus politiką ir gaires, pavyzdžiui, vidaus procesus (taikant vidaus leidimo reikalavimus, dokumentais pagrįstą prieigos kontrolę, kad prieigą prie informacijos gautų tik tinkamai išmokyti asmenys, kuriems taikomi būtini misijos reikalavimai, ir kt.), skirtus užtikrinti, kad ir tikslinis, ir masinis duomenų rinkimas atitiktų šiame vykdomajame potvarkyje nustatytus būtinumo ir proporcingumo reikalavimus[43]. Be to, įvairių žvalgybos agentūrų (pvz., Nacionalinės saugumo agentūros, Centrinės žvalgybos valdybos, Federalinio tyrimų biuro) darbuotojams suteiktas mokymas apie Vykdomąjį potvarkį Nr. 14086, apimantis ODNI CLPO kasmet ir prireikus organizuojamus mokymo kursus ir privalomą visų naujų ODNI darbuotojų mokymą.

Komisija palankiai vertina įvairias priemones, kurių imtasi Vykdomajam potvarkiui Nr. 14086 įgyvendinti ir jo laikymuisi užtikrinti. Kadangi įgyjama daugiau patirties praktikoje taikant šiuo vykdomuoju potvarkiu nustatytas apsaugos priemones, Komisija būtų dėkinga, jei būtų galima

[41] Šie teisėti tikslai ar teisėta paskirtis apima, pavyzdžiui, apsaugą nuo šnipinėjimo, sabotažo, nužudymo ar kitokios žvalgybos veiklos, kurią vykdo užsienio valdžia, organizacija ar asmuo arba kuri vykdoma jų vardu arba jiems padedant, taip pat apsaugą nuo terorizmo, įkaitų paėmimo ir asmenų laikymo nelaisvėje, kurį vykdo užsienio valdžia, organizacija ar asmuo arba kuris vykdomas jų vardu.

[42] Vykdomojo potvarkio Nr. 14086 2 straipsnio b punkto iii papunktis.

[43] Žr. https://www.intel.gov/ic-on-the-record-database/results/oversight/1278-odni-releases-ic-procedures-implementing-new-safeguardsin-executive-order-14086 (paskelbta 2023 m. liepos 3 d.).

per būsimas peržiūras aptarti konkrečius pavyzdžius, kaip šis vykdomasis potvarkis taikomas praktikoje (laikantis taikytinų konfidencialumo nuostatų).

2.2.1.2. Pakartotinis leidimas taikyti Užsienio žvalgybos stebėjimo įstatymo (FISA) 702 straipsnį

Pagal FISA 702 straipsnį leidžiama, siekiant įgyti užsienio žvalgybos informacijos, stebėti ne JAV asmenis, kurie pagrįstai laikomi esančiais už JAV teritorijos ribų. Ši informacija įgyjama pagal metinius sertifikatus, pateiktus Užsienio žvalgybos stebėjimo teismui (angl. *Foreign Intelligence Surveillance Court*, toliau – FISC) ir jo patvirtintus. Šiuose sertifikatuose nurodomos konkrečios užsienio žvalgybos informacijos, kuri bus renkama, kategorijos. ODNI 2023 m. liepos 21 d. pranešė, kad yra trys patvirtinti sertifikatai pagal FISA 702 straipsnį, apimantys šias užsienio žvalgybos kategorijas: 1) užsienio valstybių valdžią ir su ja susijusius subjektus, 2) kovą su terorizmu ir 3) kovą su ginklų platinimu[44]. Šis sertifikavimas turi apimti ir tikslinio duomenų rinkimo bei renkamų duomenų kiekio mažinimo procedūras, kurias patvirtina FISC[45]. Visų pirma, tikslinio duomenų rinkimo tvarka yra tokia: FISA elektroninių ryšių paslaugų teikėjo apibrėžtį atitinkančių JAV bendrovių prašoma atskleisti elektroninių ryšių duomenis, susijusius su pranešimais, gaunamais arba siunčiamais pasirinkto stebėjimo objekto (angl. *selector*), kuris yra konkreti ryšio paskyra, pavyzdžiui, telefono numeris ar e. pašto adresas. JAV vyriausybė yra paskelbusi informacinės medžiagos apie FISA 702 straipsnį, kuria siekiama informuoti visuomenę apie stebėjimo programų veikimą, taikomus reikalavimus ir privatumo apsaugos priemones, taip pat FISC vaidmenį[46].

Dėl laikino galiojimo sąlygos FISA 702 straipsnis turėjo nustoti galioti 2023 m. pabaigoje, nebent Kongresas būtų pakartotinai leidęs jį taikyti. Pakartotinai leidęs laikinai toliau jį taikyti be jokių pakeitimų, Kongresas 2024 m. balandžio 19 d. priėmė Žvalgybos reformos ir Amerikos apsaugos įstatymą (angl. *Reforming Intelligence and Securing America Act*, toliau – RISAA), kuriuo pakartotinai leista dvejų metų laikotarpiu taikyti FISA 702 straipsnį ir padaryti keli pakeitimai. Pastaruosius galima skirstyti į dvi bendras kategorijas: 1) pagal FISA 702 straipsnį leidžiamos sekimo veiklos apimties pakeitimus ir 2) institucinius ir procedūrinius pakeitimus.

Stebėjimo veiklos, leidžiamos pagal FISA 702 straipsnį, apimties pakeitimai

RISAA padaryti trys pagrindiniai stebėjimo veiklos, kuri gali būti vykdoma pagal FISA 702 straipsnį, apimties pakeitimai.

Pirma, galutinai uždrausta rinkti netiesioginius duomenis (angl. *abouts*) apie stebėjimo objektą[47], t. y. perimti siunčiamus pranešimus, kai pagal 702 straipsnį pasirinktas stebėjimo objektas (pvz., e. pašto adresas) nėra tų pranešimų adresatas ar siuntėjas, o yra tik nurodytas siunčiamame pranešime (pvz., kai e. laiškai nėra siunčiami pasirinktu stebėti e. pašto adresu ar iš jo, tačiau pasirinktas stebėti e. pašto adresas minimas e. laiško tekste ar pagrindinėje dalyje). Nors po FISA pakeitimo, atlikto 2018 m., FISA nebeapėmė tokio duomenų rinkimo, FISA tebebuvo numatyta galimybė ateityje vėl pradėti rinkti netiesioginius duomenis apie stebėjimo

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

[45] Tokiomis procedūromis duomenų rinkimas apribojamas pagal konkretų užsienio žvalgybos tikslą, ribojama prieiga (be kita ko, prieigos kontrolės priemonėmis) prie duomenų bazių, kuriose saugoma pagal FISA 702 straipsnį gauta informacija, ir nustatomi tokios informacijos naudojimo, saugojimo ir sklaidos apribojimai.

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

[47] RISAA 22 straipsnis.

objektą pagal specialią leidimo suteikimo procedūrą, kurioje dalyvautų FISC ir Kongresas. Naujausiu RISAA padarytu pakeitimu ši galimybė panaikinta.

Antra, užsienio žvalgybos informacijos apibrėžtis išplėsta įtraukiant kovai su narkotikais svarbią informaciją[48]. Peržiūros susitikime JAV institucijos paaiškino, kad tai nustatyta atsižvelgiant į dabartinę fentanilio krizę ir į didėjančią tarptautinių narkotikų prekeivių ir gamintojų keliamą grėsmę nacionaliniam saugumui. Atsižvelgiant į šias aplinkybes, patvirtinta, kad tokia samprata atitinka kelis iš Vykdomajame potvarkyje Nr. 14086 nurodytų teisėtų tikslų, t. y. suprasti arba įvertinti užsienio organizacijų, keliančių realią ar potencialią grėsmę JAV ar jos sąjungininkų nacionaliniam saugumui, pajėgumus, ketinimus ar veiklą; suprasti arba įvertinti tarptautines grėsmes, darančias poveikį pasauliniam saugumui, įskaitant riziką visuomenės sveikatai, ir apsisaugoti nuo tarpvalstybinio nusikalstamumo grėsmių[49].

Trečia, RISAA išplėsta elektroninių ryšių paslaugų teikėjo (angl. *electronic communication service provider*, ECSP) apibrėžtis, taigi taikymo sritis apima daugiau bendrovių, kurios gali būti priverstos teikti informaciją pagal FISA 702 straipsnį[50]. Dabar elektroninių ryšių paslaugų teikėjo apibrėžtis apima ir kitus paslaugų teikėjus, turinčius „prieigą prie įrangos, kuri yra arba gali būti naudojama pranešimams laidinio ar elektroninio ryšio priemonėmis perduoti ar saugoti“, nors aiškiai nustatyta, kad ji neapima viešųjų apgyvendinimo įstaigų, gyvenamųjų būstų, bendruomeninių įstaigų ir maitinimo paslaugų įstaigų. Teisingumo departamentas Kongresui adresuotame rašte šį pakeitimą nurodė kaip techninio pobūdžio pakeitimą, skirtą taikyti „labai nedaug“ technologijų bendrovių, kurių, pagal FISC ir Užsienio žvalgybos stebėjimo apeliacinio teismo (FISCR) pastarojo meto sprendimus, neapėmė ankstesnė elektroninių ryšių paslaugų teikėjo apibrėžtis[51]. Tame rašte Teisingumo departamentas įsipareigojo siaurinti taikymo sritį taikydamas šią apibrėžtį taip, kad ji apimtų vien to tipo paslaugų teikėjus, dėl kurių po bylinėjimosi priimtas FISC sprendimas. Taigi susijusios bendrovės yra nurodytos įslaptintame Kongresui skirtame priede. Kelios NVO, įskaitant tas, kurios pateikė atsiliepimų per peržiūrą, išreiškė susirūpinimą dėl šio apibrėžties išplėtimo, teigdamos, kad taip ji galėtų apimti daug JAV įmonių (nes daugelis jų teikia tam tikro pobūdžio paslaugas ir turi prieigą prie ryšio įrangos). Atsižvelgiant į tokį išreikštą susirūpinimą, žvalgybos bendruomenei pritariant, pasiūlytas dar vienas pakeitimas 2025 finansinių metų Žvalgybos leidimų įstatymo projekte, kuris šiuo metu svarstomas Kongrese. Jei Kongresas patvirtintų šį pakeitimą, juo būtų užtikrinta, kad papildomos bendrovės, įtraukiamos į elektroninių ryšių paslaugų teikėjo apibrėžtį, būtų tik tos, kurios nurodytos minėtuose FISC sprendimuose. Šiame įstatymo projekte taip pat numatyta, kad apie kiekvieną tokiai bendrovei skirtą nurodymą turėtų būti pranešama FISC, kad šis galėtų patikrinti, ar ta bendrovė iš tiesų patenka į taikymo sritį. Savo rašte Kongresui Teisingumo departamentas įsipareigojo kas šešis mėnesius pranešti Kongresui apie bet kokį atnaujintos elektroninių ryšių paslaugų teikėjo apibrėžties taikymą, kad Kongresas galėtų tinkamai prižiūrėti siaurą šios apibrėžties taikymą.

[48] RISAA 23 straipsnis.
[49] Vykdomojo potvarkio Nr. 14086 (EO 14086) 2 straipsnio b punkto ii papunkčio A dalies 2, 3 ir 10 punktai.
[50] RISAA 25 straipsnis.
[51] https://www.justice.gov/opa/media/1348621/dl?inline. Žr. FISC 2022 m. sprendimą (https://www.intel.gov/assets/documents/702%20Documents/declassified/2022-FISC-ECSP-OPINION.pdf) ir Užsienio žvalgybos stebėjimo apeliacinio teismo (FISCR) sprendimą, kuriuo tas FISC sprendimas paliktas galioti (https://www.intel.gov/assets/documents/702%20Documents/declassified/2023_FISC-R_ECSP_Opinion.pdf).

Svarbu tai, kad peržiūros susitikime JAV institucijos ir Privatumo ir piliečių laisvių priežiūros valdyba (angl. *Privacy and Civil Liberties Oversight Board*, toliau – PCLOB) patvirtino, kad visos Vykdomajame potvarkyje Nr. 14086 numatytos apsaugos priemonės toliau visapusiškai taikomos visų duomenų rinkimui ir naudojimui pagal FISA 702 straipsnį ir po šių pakeitimų. Taigi, nors RISAA šiek tiek išplėsta bendrovių, kurios gali gauti nurodymą perduoti duomenis, aprėptis, juo neapribotas naudojimasis teisėmis. Vis dėlto bus svarbu stebėti tolesnius (teisėkūros ir ataskaitų teikimo) pokyčius ir gauti informacijos apie šių naujų taisyklių taikymą praktikoje. Tai apima, pavyzdžiui, užsienio žvalgybos ir elektroninių ryšių paslaugų teikėjų apibrėžčių išplėtimo poveikį stebėjimo objektų pagal FISA 702 straipsnį skaičiui (kurį kasmet praneša ODNI; dėl skaidrumo žr. toliau). Itin informatyvi šiuo atžvilgiu turėtų būti tolesnė ataskaita, kuri ateityje bus parengta po neseniai pateiktos PCLOB ataskaitos dėl FISA 702 straipsnio (žr. toliau).

Instituciniai ir procedūriniai pakeitimai

Dėl institucinių ir procedūrinių pakeitimų pažymima, kad RISAA įformintos kelios procedūros, kurių iki tol jau laikytasi praktikoje, ir nustatyta naujų apsaugos priemonių. Nors kai kurios iš jų aktualios tik JAV asmenims, keliais pakeitimais padidinama ir JAV, ir ne JAV asmenų, kurių duomenys gali būti renkami pagal FISA 702 straipsnį, apsauga[52], taigi jie yra aktualūs DPS veikimui.

Pirma, nustatyta papildomų atskaitomybės, priežiūros ir ataskaitų teikimo reikalavimų. Visų pirma, Federalinio tyrimų biuro darbuotojai dabar turi būti kasmet mokomi apie taisykles, taikomas užklausoms dėl informacijos, kuri gaunama pagal FISA 702 straipsnį[53]. Federalinis tyrimų biuras taip pat turi teikti Kongresui ataskaitas dėl savo užklausų teikimo veiklos (pvz., kiek užklausų teikiama naudojant grupinio darbo technologijas (angl. *batch job technologies*), t. y. į vieną užklausą įtraukiant kelis užklausos žodžius ar frazes) ir atskaitomybės priemonių, skirtų užtikrinti, kad būtų laikomasi teisinių reikalavimų dėl užklausų (RISAA 11–12 straipsniai). Be to, Teisingumo departamento generaliniam inspektoriui nurodoma parengti ataskaitą, kaip Federaliniame tyrimų biure laikomasi reikalavimų dėl užklausų (RISAA 9 straipsnis). Apskritai, siekiant padidinti FISC procedūrų skaidrumą, ODNI ir generalinis prokuroras dabar privalo užbaigti FISC sprendimų išslaptinimo peržiūrą per 180 dienų (RISAA 7 straipsnis). Be to, visų FISC ir Užsienio žvalgybos stebėjimo apeliacinio teismo (FISCR, kuriame galima apskųsti FISC sprendimus) posėdžių stenogramos turi būti saugomos ir perduodamos Kongresui (RISAA 8 straipsnis).

Antra, RISAA nustatyti papildomi Federalinio tyrimų biuro naudojimosi duomenimis, surinktais pagal FISA 702 straipsnį, apribojimai. RISAA 2 straipsnio d punkte nustatyta, kad užklausa naudojant grupavimo technologiją (angl. *batch technology*) gali būti pateikta tik gavus Federalinio tyrimų biuro teisininko sutikimą, nebent būtų skubos aplinkybių, kuriomis tai netaikytina. Be to, Federaliniam tyrimų biurui dabar draudžiama automatiškai tikrinti

[52] Be to, RISAA padaryta pakeitimų, susijusių su įprastiniu individualizuotu elektroniniu stebėjimu pagal FISA 105 straipsnį (remiantis FISC orderiu, išduodamu, jei laikomasi standarto įrodyti pakankamą pagrindą, angl. *standard of probable cause*). Dabar, kai žvalgybos agentūra pateikia generaliniam prokurorui prašymą duoti nurodymą vykdyti individualizuotą elektroninį stebėjimą, reikia priesaika patvirtinto pareiškimo, kuriuo būtų pagrįstai nurodyta, kad FISA 105 straipsnio sąlygos yra įvykdytos (RISAA 6 straipsnio a punktas). Galima užsienio valdžios ar užsienio valdžios agentų elektroninio stebėjimo trukmė pratęsta nuo 120 dienų iki vienų metų (RISAA 6 straipsnio g punktas).

[53] RISAA 2 straipsnio d punktas.

informaciją, gautą pagal FISA 702 straipsnį, kurios kiekis nėra sumažintas iki minimumo, ir jis turi užtikrinti, kad analitikai privalėtų patvirtinti pasirinkimą atlikti paiešką remiantis tokia informacija. RISAA taip pat Federaliniam tyrimų biurui uždrausta teikti užklausas, kurių vienintelė paskirtis būtų rasti ir gauti nusikalstamos veiklos įrodymų (nebent būtų pagrįstai manoma, kad tai galėtų padėti sumažinti ar pašalinti grėsmę gyvybei ar sunkaus sužalojimo pavojų, arba tai reikalinga siekiant įvykdyti prievoles atskleisti informaciją bylinėjantis)[54]. Be to, Federaliniam tyrimų biurui draudžiama į analitines duomenų saugyklas įtraukti asmens duomenis, kurių kiekis nėra sumažintas iki minimumo, nebent tikslinis asmuo būtų aktualus vykdomam nacionalinio saugumo tyrimui[55].

Trečia, pakeistos tam tikros nuostatos, susijusios su *amici curiae* statusu ir vaidmeniu FISC[56]. *Amici curiae* skiriami ekspertais, kad padėtų šiam teismui (ir FISCR) spręsti su privatumu ir piliečių laisvėmis susijusius klausimus arba išaiškinti technologinius klausimus nagrinėjant konkretų valdžios pateiktą prašymą. Nors anksčiau FISA buvo nustatytas reikalavimas, kad *amici curiae* turėtų kompetenciją privatumo ir piliečių laisvių, žvalgybos duomenų rinkimo, ryšių technologijų ar kitose aktualiose srityse, dabar pagal šį įstatymą iš esmės privaloma turėti kompetenciją privatumo ir (arba) piliečių laisvių, ir žvalgybos duomenų rinkimo srityse. FISC jau turėjo galimybę paskirti *amicus curiae* bet kuriuo atveju, kai, jo nuomone, tai buvo tikslinga, ir privalėjo paskirti *amicus curiae* spręsdamas dėl naujo arba reikšmingo teisės aiškinimo. Po pakartotinio leidimo suteikimo FISC dabar taip pat privalo paskirti *amicus curiae* kiekvieną kartą, kai jo prašoma patvirtinti sertifikatus pagal FISA 702 straipsnį ir susijusias procedūras (pvz., tikslinio duomenų rinkimo procedūras), nebent jis nustatytų, kad tai būtų netikslinga arba, tikėtina, dėl to būtų nepagrįstai vėluojama[57]. Be to, dabar šis teismas, užuot paskyręs tik vieną *amicus curiae*, gali nuspręsti paskirti vieną arba daugiau *amici curiae*. Taip pat išaiškinta, kad informacija, kurią teikia *amici curiae*, turi „apsiriboti tuo, kas reikalinga konkretiems teismo nurodytiems klausimams spręsti“, nors sritys, dėl kurių *amici curiae* gali teikti pastabų, tebėra plačios (t. y. teisiniai argumentai ir informacija, susiję su Jungtinių Valstijų asmenų privatumo ir pilietinių laisvių apsauga, žvalgybos duomenų rinkimu ir ryšių technologijomis ar bet kuria kita aktualia sritimi).

Galiausiai, RISAA 18 straipsniu įsteigta FISA reformų komisija, kurią, be kita ko, sudaro Kongreso nariai, PCLOB pirmininkas, nacionalinės žvalgybos direktoriaus vyriausiasis pavaduotojas ir generalinio prokuroro pavaduotojas, taip pat papildomi Kongreso skiriami nariai[58]; jos paskirtis – rekomenduoti papildomas FISA reformas.

Komisija atidžiai stebės tolesnius su FISA 702 straipsniu susijusius pokyčius, be kita ko, dėl PCLOB vykdomos priežiūros veiklos (žr. toliau), Reformų komisijos darbo ir būsimos FISA peržiūros, kuri bus atlikta po dvejų metų.

2.2.1.3. Stebėjimo veikla praktikoje: skaičiai ir tendencijos

ODNI metinės statistikos skaidrumo ataskaitos dėl žvalgybos bendruomenės naudojimosi nacionalinio saugumo tikslais vykdomo stebėjimo įgaliojimais 2023 kalendoriniais metais

[54] RISAA 3 straipsnio a punktas.

[55] RISAA 3 straipsnio b punktas. Federalinio tyrimų biuro direktorius gali nuspręsti dėl šios nuostatos taikymo išimties, kai tai reikalinga dėl skubos aplinkybių; apie tokią išimtį turi būti pranešta Kongresui.

[56] Siekiant aiškumo, pažymima, kad, kaip peržiūros susitikime patvirtino JAV, šie pakeitimai nedaro poveikio specialiųjų advokatų statusui ir vaidmeniui Duomenų apsaugos apeliaciniame teisme (angl. *Data Protection Review Court*, DPRC).

[57] RISAA 5 straipsnio b punktas.

[58] 18 straipsnyje konkrečiai reikalaujama, kad šioje komisijoje būtų išorės atstovų ne iš Kongreso.

(paskelbta 2024 m. balandžio mėn.)[59] duomenimis, stebėjimo objektų pagal FISA 702 straipsnį skaičius padidėjo nuo 245 073 2022 kalendoriniais metais iki 268 590 2023 kalendoriniais metais. Ataskaitoje paaiškinta, kad stebėjimo objektų skaičiaus kaitos priežasčių gali būti įvairių, įskaitant tarnybų veiklos prioritetų pokyčius, įvykius pasaulyje, techninius pajėgumus, stebėjimo objekto elgseną ir pokyčius telekomunikacijų sektoriuje. Ataskaitoje taip pat nurodyta, kad tais metais nebuvo stebima jokių ne ES asmenų (2021 m. stebėtas vienas asmuo, 2022 m. – nė vieno) pagal FISA 402 straipsnį (dėl renkamų telefono numerių registro ir gaunamų skambučių sekiklių naudojimo), tačiau buvo duoti šeši nurodymai (2021 ir 2022 m. būta po 11 tokių nurodymų) dėl šešių stebėjimo objektų (2021 m. buvo 13, 2022 m. – 11 stebėjimo objektų) pagal FISA 501 straipsnį (prieiga prie viešojo transporto vežėjų, transporto priemonių nuomos įstaigų ar fizinių saugyklų verslo įrašų), įskaitant 5 412 unikalių identifikatorių (2021 m. jų buvo 23 157, 2022 m. – 55 431), naudojamų pagal tokius nurodymus surinktai informacijai perduoti.

Teisingumo departamento metinėje dėl Užsienio žvalgybos stebėjimo įstatymo parengtoje ataskaitoje Kongresui nurodyta, kad 2023 kalendoriniais metais FISC pateikti 327 prašymai leisti vykdyti elektroninį stebėjimą ir (arba) fizines kratas užsienio žvalgybos tikslais atitinkamai pagal FISA 105 ir 302 straipsnius[60]. Bendras tikslinių asmenų skaičius buvo nuo 500 iki 999. Dėl nacionalinio saugumo raštų (angl. *national security letters*, toliau – NSL) toje ataskaitoje nurodyta, kad buvo pateikta 10 115 prašymų (išskyrus prašymus tik dėl informacijos apie abonentus) dėl informacijos apie ne JAV asmenis, siekiant gauti informacijos apie 3 033 įvairius ne JAV asmenis[61].

Kelios DPS sertifikuotos bendrovės (pvz., „Google“, „Meta“) naudojasi JAV teisėje suteikta galimybe skelbti skaidrumo ataskaitas, kuriose informuojama apie per tam tikrą ataskaitinį laikotarpį jų gautų prašymų pagal FISA ir NSL formos prašymų skaičių. Tuo metu, kai rengta ši ataskaita, dar nebuvo prieinamų statistinių duomenų apie prašymus pagal FISA po 2023 m. liepos mėn. Pavyzdžiui, bendrovė „Google“ pranešė, kad 2023 m. liepos–gruodžio mėn. gavo nuo 500 iki 999 NSL formos prašymų, susijusių su 2 000–2 499 paskyromis[62]. Bendrovė „Meta“ pranešė, kad per tą patį ataskaitinį laikotarpį gavo nuo 0 iki 499 NSL formos prašymų, susijusių su 500–999 paskyromis[63]. Per kelerius pastaruosius metus šie skaičiai išliko gana stabilūs. Siekdamos dar labiau padidinti skaidrumą, kai kurios bendrovės (pvz., „Google“) savo iniciatyva paskelbia gautus NSL formos prašymus, kai tik baigia galioti informacijos atskleidimo apribojimai[64].

2.2.1.4. Kiti pokyčiai

Rengiantis peržiūrai, kelios NVO iškėlė klausimų dėl naujų duomenų įgijimo JAV žvalgybos agentūrose formų, kai duomenys perkami iš komercinių subjektų, visų pirma duomenų tarpininkų. Jos paaiškino, kad nors duomenys, renkami šiuo pagrindu, vis vien turi būti

[59] https://www.dni.gov/files/CLPT/documents/2024_ASTR_for_CY2023.pdf.
[60] https://www.justice.gov/nsd/media/1350236/dl?inline.
[61] Šie skaičiai, palyginti su praėjusiais ataskaitiniais metais (2022 m.), iš esmės nepakito. Palyginimo tikslais galima paminėti, kad 2022 m. buvo pateikta 317 galutinių prašymų FISC leisti vykdyti elektroninį stebėjimą ir (arba) fizines kratas užsienio žvalgybos tikslais. Bendras tikslinių asmenų, dėl kurių išduoti nurodymai vykdyti elektroninį stebėjimą, skaičius buvo nuo 0 iki 499. 2022 m. Federalinis tyrimų biuras pateikė 9 103 prašymus nacionalinio saugumo raštuose (NSL), siekdamas gauti informacijos apie ne JAV asmenis (išskyrus prašymus pateikti informaciją tik apie abonentus). Šaltinis – 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.

tvarkomi laikantis kitų reikalavimų, be kita ko, pavyzdžiui, pagal Vykdomąjį potvarkį Nr. 12333[65], duomenys taip įgyjami netaikant FISA ar Vykdomojo potvarkio Nr. 14086.

Šiuo atžvilgiu reikėtų priminti, kad bet kokiam savanoriškam dalijimuisi duomenimis su trečiosiomis šalimis taikomos kelios išsamiai nustatytos sąlygos pagal DPS. Pirma, sertifikuota organizacija negali dalytis duomenimis su trečiąja šalimi (kuri veikia ne kaip atstovas ar duomenų tvarkytojas), jei ji nėra apie tai pranešusi atitinkamiems asmenims ir nėra suteikusi jiems galimybės pasirinkti[66]. Antra, pagal *atskaitomybės už tolesnį duomenų perdavimą principą*, tolesnis duomenų perdavimas gali būti vykdomas tik 1) ribotais ir konkrečiais tikslais, 2) pagal ES ir JAV DPS organizacijos ir trečiosios šalies sutartį ir 3) tik jei toje sutartyje reikalaujama, kad trečioji šalis užtikrintų tokį patį apsaugos lygį, koks yra garantuojamas pagal DPS principus[67].

Be to, kaip aptarta ir peržiūros susitikime, Federalinė prekybos komisija ėmėsi vykdymo užtikrinimo veiksmų prieš duomenų tarpininkus, parduodančius neskelbtinus vartotojų duomenis. Pavyzdžiui, byloje prieš bendrovę „X-Mode“ ir jos teisių perėmėją „Outlogic“ Federalinė prekybos komisija 2024 m. sausio 9 d. priėmė nutartį, kuria tai bendrovei uždrausta parduoti geografinės buvimo vietos duomenis trečiosioms šalims ir nurodyta ištrinti duomenis, kuriuos ji naudojo ir kuriais ji neteisėtai pasidalijo. Federalinės prekybos komisijos tyrimu, be kita ko, nustatyta, kad ši bendrovė nevisiškai informavo asmenis apie jų geografinės buvimo vietos duomenų naudojimą ir pardavimą, nesuteikė priemonių, kad asmenys galėtų atsisakyti sekimo, leido duomenis naudoti potencialiai diskriminaciniais tikslais ir neapribojo trečiųjų šalių naudojimosi tokia informacija[68]. Komisija tikisi, kad Federalinė prekybos komisija laikysis tokio paties požiūrio tuo atveju, jei DPS sertifikuotos bendrovės, dalydamosi duomenimis, pažeistų minėtas nuostatas.

Galiausiai vertėtų paminėti, kad 2024 m. gegužės mėn. ODNI paskelbė Žvalgybos bendruomenės politikos programą dėl komerciškai prieinamos informacijos[69]. Šioje programoje nustatyti tam tikri principai ir reikalavimai, kurių žvalgybos agentūros turėtų laikytis, be kita ko, siekdamos kuo labiau sumažinti riziką privatumui ir piliečių laisvėms, kai įgyja ir naudoja informaciją pagal komercinį sandorį.

2.2.2. Nepriklausoma priežiūra

JAV žvalgybos agentūrų veiklą prižiūri įvairios įstaigos, įskaitant privatumo ir piliečių laisvių pareigūnus, generalinius inspektorius, Kongresą ir PCLOB. Visų pirma, Vykdomajame potvarkyje Nr. 14086 reikalaujama, kad kiekviena žvalgybos agentūra turėtų vyresniuosius teisės, priežiūros ir atitikties užtikrinimo pareigūnus, kurie užtikrintų, kad būtų laikomasi taikomų JAV teisės aktų. Šią priežiūros funkciją atlieka pareigūnai, kuriems pavesta rūpintis, kad būtų laikomasi reikalavimų, taip pat privatumo ir piliečių laisvių apsaugos pareigūnai ir

[65] Žr., pvz., Vykdomojo potvarkio Nr. 12333 dėl duomenų rinkimo metodų (EO 12333) 2.4 skirsnį.
[66] Žr. sprendimo dėl tinkamumo 40 konstatuojamąją dalį.
[67] Žr. sprendimo dėl tinkamumo 38 konstatuojamąją dalį.
[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. Žvalgybos agentūros privalo laikytis šios programos nuo 2024 m. rugpjūčio mėn.

generaliniai inspektoriai[70]. Jie turi vykdyti periodinę signalų žvalgybos veiklos priežiūrą ir užtikrinti, kad bet koks reikalavimų nesilaikymas būtų ištaisytas. Žvalgybos agentūros privalo tokiems pareigūnams sudaryti sąlygas susipažinti su visa aktualia informacija, kad jie galėtų atlikti priežiūros funkcijas, ir negali imtis veiksmų, kurie jiems kliudytų vykdyti priežiūros veiklą arba tokiai veiklai darytų nederamą įtaką.

Peržiūros susitikime dalyvavo ODNI Žvalgybos bendruomenės generalinio inspektoriaus biuro (ICIG) generalinis juriskonsultas, kuris turi visapusišką jurisdikciją visos žvalgybos bendruomenės atžvilgiu ir yra įgaliotas tirti skundus ar informaciją dėl įtariamų neteisėtų veiksmų ar piktnaudžiavimo įgaliojimais. Jis patvirtino, kad vykdydamas priežiūros veiklą ICIG sistemingai tikrina atitiktį Vykdomajam potvarkiui Nr. 14086. Jis taip pat paminėjo kitų žvalgybos bendruomenės generalinių inspektorių pastaruoju metu vykdytą priežiūros veiklą, kuri išsamiai aprašyta reguliariai teikiamose ataskaitose. Pavyzdžiui, savo 2023 m. balandžio–rugsėjo mėn. pusmečio ataskaitoje Kongresui[71] Nacionalinės saugumo agentūros generalinis inspektorius informavo apie jos vidaus kontrolės sistemos, taikomos sprendimams ir prašymams dėl tikslinio duomenų rinkimo, vertinimą. Jis padarė išvadą, kad ši sistema tinkamai veikia siekiant užtikrinti, kad būtų laikomasi piliečių laisvių ir privatumo apsaugos įstatymų, nurodymų ir politikos. Toje pačioje ataskaitoje taip pat minimas tyrimas, kurį atliekant nustatyta, kad Nacionalinės saugumo agentūros darbuotojas piktnaudžiavo signalų žvalgybos priemone neteisėtais tikslais.

Pagal Vykdomąjį potvarkį Nr. 14086 Privatumo ir piliečių laisvių priežiūros valdybai (PCLOB)[72] pavedamos specialios priežiūros funkcijos[73]. PCLOB pirmininkas ir trys jos nariai dalyvavo peržiūros susitikime ir informavo, kad 2023 m. balandžio mėn. PCLOB pateikė rekomendacijų žvalgybos agentūroms dėl jų politikos ir procedūrų, kuriomis įgyvendinamas Vykdomasis potvarkis Nr. 14086, projektų ir su ja konsultuotasi dėl Duomenų apsaugos apeliacinio teismo (DPRC) teisėjų ir specialiųjų advokatų skyrimo. PCLOB taip pat pradėjo priežiūros projektą, kuriuo siekiama 1) peržiūrėti žvalgybos agentūrų patvirtintos atnaujintos politikos ir procedūrų įgyvendinimą siekiant įsitikinti, kad jos atitinka vykdomąjį potvarkį, ir 2) atlikti metinę naujojo teisių gynimo mechanizmo veikimo peržiūrą (žr. toliau)[74]. PCLOB nariai patvirtino, kad ji planuoja artimiausiu metu atlikti abi peržiūras. Dėl teisių gynimo jie

[70] Kiekvienoje žvalgybos agentūroje yra generalinis inspektorius, kuris yra pagal įstatymus nepriklausomas ir atsakingas už atitinkamos agentūros nacionalinio saugumo tikslais vykdomos veiklos auditą ir tyrimus. Jis turi galimybę (jei reikia, pagal potvarkį) susipažinti su visa aktualia (taip pat įslaptinta) medžiaga ir gali priimti parodymus. Generaliniai inspektoriai įtariamų baudžiamųjų pažeidimų atvejus perduoda baudžiamajam persekiojimui ir agentūrų vadovams teikia rekomendacijas dėl taisomųjų veiksmų. Nors jų rekomendacijų laikytis neprivaloma, jų ataskaitos, be kita ko, dėl tolesnių veiksmų (arba neveikimo), paprastai skelbiamos viešai ir siunčiamos Kongresui. Šiuo klausimu žr. sprendimo dėl tinkamumo 136 išnašą dėl generalinio inspektoriaus vaidmens.

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

[72] PCLOB yra nepriklausoma agentūra, kuriai patikėta atsakomybė kovos su terorizmu politikos ir jos įgyvendinimo srityje, siekiant apsaugoti privatumą ir piliečių laisves. Ji gali susipažinti su visa aktualia (taip pat įslaptinta) informacija, rengti pokalbius ir išklausyti parodymus. Ji gali teikti rekomendacijas teisėsaugos ir žvalgybos institucijoms ir reguliariai teikia ataskaitas Kongresui ir Prezidentui. Jos ataskaitos yra viešai prieinamos ir stengiamasi jas kuo labiau išplatinti.

[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.

[74] https://www.pclob.gov/OversightProjects/Details/1115.

paaiškino, kad skundų negauta, taigi per PCLOB atliekamą peržiūrą dėmesys bus sutelktas į politiką ir procedūras, nustatytas kuriant teisių gynimo mechanizmą.

Dėl kitos priežiūros veiklos pažymima, kad 2023 m. rugsėjo 28 d. PCLOB paskelbė ataskaitą dėl FISA 702 straipsnio[75]. Šioje ataskaitoje, parengtoje po ankstesnės 2014 m. ataskaitos, pateikiama naujausia faktinė ir teisinė informacija apie stebėjimo programų pagal FISA 702 straipsnį veikimą. Ataskaitoje taip pat pateikta rekomendacijų dėl taikomų reikalavimų laikymosi žvalgybos agentūrose ir pasiūlymų Kongresui toliau griežtinti kelis FISA 702 straipsnio aspektus, susijusius su pakartotiniu Kongreso leidimo suteikimu (be kita ko, įforminant Vykdomajame potvarkyje Nr. 14086 nurodytus teisėtus stebėjimo veiklos tikslus)[76]. Peržiūros susitikime PCLOB informavo, kad tikisi greitai gauti žvalgybos agentūrų atsakymus dėl jos rekomendacijų įgyvendinimo ir jie bus įtraukti į būsimą tolesnę ataskaitą. Tarp kitų vykdomų priežiūros projektų yra vienas projektas, skirtas kovai su vietiniu terorizmu ir jos poveikiu privatumui ir piliečių laisvėms ir apimantis Federalinio tyrimų biuro vykdomą duomenų iš atviruųjų šaltinių ar komerciškai prieinamų duomenų rinkimą[77].

Galiausiai, NVO, su kuriomis konsultuotasi per peržiūrą, išreiškė susirūpinimą, kad kelių PCLOB narių kadencija netrukus baigsis ir dėl to PCLOB gali likti be kvorumo. Visų pirma, baigėsi pirmininkės kadencija, o laikotarpis, kuriuo ji gali išlaikyti ankstesnes pareigas, baigiasi 2025 m. sausio mėn.; kita nario vieta yra laisva, o trečia nario vieta taip pat taps laisva kitų metų sausio mėn. Peržiūros susitikime PCLOB nariai paaiškino nemanantys, kad PCLOB liks be kvorumo, nes jau paskelbta kandidatūra į šiuo metu laisvą nario vietą (laukiama Senato patvirtinimo)[78]. Jie taip pat pabrėžė, kad net jei PCLOB liktų be kvorumo, tai nepaveiktų jos gebėjimo toliau vykdyti priežiūros projektus. Vis dėlto, kadangi PCLOB atlieka svarbų vaidmenį peržiūrint Vykdomojo potvarkio Nr. 14086 įgyvendinimą, Komisija ateityje atidžiai stebės laisvų narių vietų ir narių kandidatūrų bei skyrimo padėtį.

2.2.3. Teisių gynimas

Vykdomuoju potvarkiu Nr. 14086, kuris papildytas generalinio prokuroro priimtu reglamentavimo aktu, nustatytas naujas teisių gynimo mechanizmas, skirtas asmenų pateiktiems tinkamiems skundams dėl JAV signalų žvalgybos veiklos nagrinėti ir spręsti[79]. Bet kuris asmuo ES turi teisę pagal šį teisių gynimo mechanizmą pateikti skundą dėl įtariamo JAV teisės nuostatų, kuriomis reglamentuojama signalų žvalgybos veikla, (pvz., Vykdomojo potvarkio Nr. 14086, FISA 702 straipsnio, Vykdomojo potvarkio Nr. 12333) pažeidimo, susijusio su asmens duomenų perdavimu į JAV, kai tai kenkia asmens privatumo ir pilietinių laisvių interesams. Asmenys gali pateikti skundą ES valstybės narės DAI, o ši per EDAV sekretoriatą perduoda skundą nagrinėti pagal teisių gynimo mechanizmą. Šį mechanizmą sudaro du lygmenys: ODNI CLPO atliekamas pirminis skundų tyrimas ir galimybė asmenims apskųsti CLPO sprendimą nepriklausomam Duomenų apsaugos apeliaciniam teismui (DPRC).

---

[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] Komisija pažymi, kad kai kurios iš tų rekomendacijų, įskaitant rekomendaciją dėl netiesioginių duomenų apie pasirinktą stebėjimo objektą rinkimo ir rekomendaciją dėl FISC ekspertų (*amici curiae*) vaidmens didinimo, įtrauktos į RISAA.

[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] Sprendimo dėl tinkamumo 176–194 konstatuojamosios dalys.

Užbaigus ODNI CLPO ar DPRC peržiūrą, asmenys per nacionalinę instituciją informuojami, kad „per peržiūrą atitinkamų pažeidimų nenustatyta arba ODNI CLPO ar DPRC priėmė nutarimą, kuriame reikalaujama tinkamai ištaisyti žalą“. ODNI CLPO ir DPRC sprendimų privalo laikytis žvalgybos agentūros.

Nuo tada, kai priimtas sprendimas dėl tinkamumo, imtasi tolesnių veiksmų siekiant, kad teisių gynimo mechanizmas visapusiškai veiktų.

Dėl DPRC įsteigimo pažymima, kad 2023 m. lapkričio 14 d. į šį teismą paskirti aštuoni teisėjai (t. y. dviem teisėjais daugiau negu privalomas minimalus teisėjų skaičius pagal Vykdomąjį potvarkį Nr. 14086, papildytą generalinio prokuroro priimtais reglamentavimo aktais (28 C.F.R. § 201.3(a))[80]. Teisėjai paskirti pagal Vykdomajame potvarkyje Nr. 14086 nustatytus kriterijus ir laikantis jame nustatyto proceso, be kita ko, pasikonsultavus ir su PCLOB[81]. Tarp jų yra buvusių federalinių apygardos teismų ir apeliacinių teismų teisėjų, buvęs JAV generalinis prokuroras ir buvęs PCLOB narys. Kaip reikalaujama vykdomajame potvarkyje, bent pusė teisėjų turi ankstesnio darbo teismuose patirties. Be to, 2024 m. balandžio mėn. paskirti du specialieji advokatai – ir privatumo, ir nacionalinio saugumo sričių kompetenciją turintys praktikuojantys teisininkai, atstovausiantys asmenų interesams DPRC. Peržiūros susitikime patvirtinta, kad visiems teisėjams ir specialiesiems advokatams išduotas aukščiausio laipsnio patikimumo pažymėjimas, todėl jie, atlikdami savo užduotis DPRC, gali susipažinti su įslaptinta medžiaga. DPRC taip pat paskelbė dažnai užduodamų klausimų (DUK) rinkinį, kuriame pateikta daugiau informacijos apie jo vaidmenį, nepriklausomumą ir veikimą[82].

Dėl skundų nagrinėjimo pažymima, kad 2022 m. gruodžio 6 d. ODNI priėmė Žvalgybos bendruomenės direktyvą Nr. 126, kuria išsamiai reglamentuojami įvairūs skundų tyrimo ir sprendimo proceso aspektai (nustatomi terminai, sukuriama saugi elektroninė duomenų saugykla ir ryšio kanalai, CLPO ir žvalgybos bendruomenės dalyviai įpareigojami bendradarbiauti su PCLOB atliekant metinę teisių gynimo mechanizmo peržiūrą ir t. t.)[83]. Ši direktyva taikoma visai JAV žvalgybos bendruomenei; ją papildo atskirų žvalgybos agentūrų nustatytos vidaus procedūros dėl jų bendradarbiavimo su ODNI CLPO nagrinėjant skundą (pvz., saugios duomenų saugyklos, skirtos skundams ir atsakomiesiems dokumentams perduoti, sukūrimas, saugūs ryšiai tarp atitinkamų agentūrų). Ateinančiais mėnesiais DPRC taip pat paskelbs išsamesnes taisykles dėl skundų nagrinėjimo ir kitų procedūrinių aspektų.

Europos Sąjungoje ir Jungtinėse Amerikos Valstijose imtasi papildomų priemonių siekiant informuoti plačiąją visuomenę, taip pat palengvinti skundų teikimą ir nagrinėjimą. Tai, be kita ko, EDAV priimtas informacinis pranešimas dėl naujojo teisių gynimo mechanizmo[84], parengta pavyzdinė skundo forma (kurią visos DAI turėtų išversti ir paskelbti savo nacionalinėmis kalbomis)[85] ir darbo tvarkos taisyklės, kuriomis reglamentuojamas nacionalinių priežiūros

[80] https://www.justice.gov/opa/pr/attorney-general-merrick-b-garland-announces-judges-data-protection-review-court.
[81] Vykdomojo potvarkio Nr. 14086 (EO 14086) 3 straipsnio d punkto A dalis.
[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
[84] https://www.edpb.europa.eu/our-work-tools/our-documents/other-guidance/information-note-data-protection-framework-redress_en.
[85] https://www.edpb.europa.eu/our-work-tools/our-documents/other-guidance/template-complaint-form-us-office-director-national_en.

institucijų ir EDAV sekretoriato bendradarbiavimas[86]. Be to, ODNI paskelbė dažnai užduodamus klausimus ir informacijos suvestinę apie naująjį teisių gynimo mechanizmą ir vykdė visuomenės informuotumo didinimo veiklą[87].

Be to, praėjusiais metais EDAV ir atitinkamos JAV institucijos glaudžiai bendradarbiavo dėl kelių veiklos aspektų. Visų pirma, kaip patvirtinta peržiūros susitikime, jos sukūrė šifruoto ryšio kanalą, kuriuo skundai iš ES nacionalinių institucijų perduodami EDAV sekretoriatui, iš EDAV sekretoriato – ODNI CLPO ir Teisingumo departamento Privatumo ir piliečių laisvių biurui (OPCL), ir tarp ODNI CLPO ir kitų JAV institucijų (pvz., DPRC). Be to, ODNI CLPO paaiškino, kad yra nustatytos papildomos vidaus procedūros, pagal kurias konkrečios žvalgybos agentūros bendradarbiauja su ODNI CLPO dėl skundų nagrinėjimo.

Galiausiai OPCL, kuris teikia administracinę paramą DPRC, taip pat informavo, kad DPRC veikia pagal jam skirtą biudžeto eilutę ir jam parūpinama reikiamų priemonių jo užduotims atlikti, įskaitant saugius stalinius ir nešiojamuosius kompiuterius, telefonus ir kt. Be to, kaip reikalaujama Vykdomajame potvarkyje Nr. 14086, Prekybos departamentas ėmėsi reikiamų priemonių, be kita ko, sukurdamas šifruoto ryšio su ODNI CLPO kanalą, kad būtų registruojami visi gauti tinkami skundai. Prekybos departamentas periodiškai susisieks su ODNI CLPO siekdamas sužinoti, ar su individualiu skundu susijusi informacija yra išslaptinta. Jei taip, Prekybos departamentas apie tai praneš atitinkamam asmeniui, kad šis galėtų susipažinti su tokia informacija.

Tuo metu, kai vyko peržiūros susitikimas, ES priežiūros institucijos nebuvo gavusios jokių skundų, taigi dar nebuvo pradėta naudotis naujuoju teisių gynimo mechanizmu.

3. IŠVADA

Remdamasi per šią pirmąją peržiūrą surinkta informacija Komisija daro išvadą, kad JAV institucijos yra įdiegusios reikiamas struktūras ir procedūras, skirtas veiksmingam Duomenų privatumo sistemos funkcionavimui užtikrinti. Šiomis aplinkybėmis Komisija labai vertina tai, kad atliekant peržiūrą labai sėkmingai bendradarbiauta su JAV institucijomis.

Per šią pirmąją peržiūrą, žinoma, dėmesys sutelktas į tikrinimą, ar visi sistemą sudarantys elementai yra įdiegti, tačiau patirtis, įgyta praktikoje taikant apsaugos priemones, kurios taikomos ir sertifikuotų bendrovių atliekamam duomenų tvarkymui, ir viešojo sektoriaus institucijų prieigai prie duomenų, neišvengiamai yra ribota, nes sistema veikia dar tik metus. Todėl Komisija atidžiai stebės aktualius pokyčius ateinančiais mėnesiais ir metais, ypač daug dėmesio skirdama 1) būsimoms PCLOB ataskaitoms dėl Vykdomojo potvarkio Nr. 14086 įgyvendinimo ir su signalų žvalgyba susijusio teisių gynimo mechanizmo, visų pirma DPRC, veikimo, 2) galimiems tolesniems FISA 702 straipsnio pakeitimams ir 3) PCLOB narių kandidatūroms ir skyrimui į narių vietas, kurios ateityje taps laisvos.

Be to, siekdama užtikrinti nuolatinį ir veiksmingą sistemos funkcionavimą, Komisija mano, jog yra svarbu, kad:

[86] https://www.edpb.europa.eu/our-work-tools/our-documents/other-guidance/rules-procedure-data-protection-framework-redress_en.
[87] https://www.dni.gov/files/CLPT/documents/Fact_Sheets/The_Role_of_the_ODNI_CLPO_FAQs.pdf ir https://www.dni.gov/files/CLPT/documents/Fact_Sheets/Data_Privacy_Framework.pdf.

- kaip pranešta peržiūros susitikime, Prekybos departamentas daugiau naudotųsi įvairiomis DPS numatytomis priemonėmis, kad būtų galima stebėti, kaip bendrovės laikosi sistemos principų, ir nustatyti neteisingus teiginius apie dalyvavimą,
- Federalinė prekybos komisija toliau plėtotų savo iniciatyvų požiūrį į tyrimą ir užtikrinimą, kad sertifikuotos bendrovės laikytųsi DPS principų, ir
- Prekybos departamentas, Federalinė prekybos komisija ir ES duomenų apsaugos institucijos parengtų bendrus rekomendacinius dokumentus dėl pagrindinių reikalavimų pagal DPS principus, pvz., dėl žmogiškųjų išteklių duomenų ir tolesnio duomenų perdavimo.

Atsižvelgdama į šiuos peržiūros rezultatus ir kaip numatyta sprendimo dėl tinkamumo 211 konstatuojamojoje dalyje, Komisija mano, kad kitą periodinę peržiūrą tikslinga atlikti po trejų metų. Taip turėtų būti galima įgyti daugiau DPS taikymo praktikoje patirties ir atsižvelgti į minėtus būsimus pokyčius. Todėl, pagal sprendimo dėl tinkamumo 3 straipsnio 4 dalį, Komisija dėl būsimų peržiūrų periodiškumo konsultuosis su EDAV ir pagal Bendrojo duomenų apsaugos reglamento 93 straipsnio 1 dalį įsteigtu komitetu.