32000D0520

KOMISIJOS SPRENDIMAS

2000 m. liepos 26 d.

dėl Europos Parlamento ir Tarybos direktyvos 95/46/EB dėl „saugaus uosto“ privatumo principų teikiamos apsaugos pakankamumo ir su tuo susijusių JAV komercijos departamento pateiktų „Dažnai užduodamų klausimų“

(pranešta dokumentu Nr. C(2000) 2441)

(tekstas svarbus EEE)

(2000/520/EB)

EUROPOS BENDRIJŲ KOMISIJA,

atsižvelgdama į Europos bendrijos steigimo sutartį,

atsižvelgdama į 1995 m. spalio 24 d. Europos Parlamento ir Tarybos direktyvą 95/46/EB dėl asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo [1], ypač į jos 25 straipsnio 6 dalį,

kadangi:

(1) Pagal Direktyvą 95/46/EB valstybės narės privalo imtis priemonių, kad asmens duomenys būtų perduodami trečiajai šaliai tik tuomet, jei ta trečioji šalis užtikrina pakankamą apsaugos lygį ir prieš perduodant duomenis atsižvelgiama į tos valstybės narės įstatymus, įgyvendinančius kitas tos direktyvos nuostatas.

(2) Komisija gali nustatyti, kad trečioji šalis užtikrina pakankamą apsaugos lygį. Tuomet asmens duomenys gali būti perduodami iš valstybių narių nereikalaujant papildomų garantijų.

(3) Pagal Direktyvą 95/46/EB duomenų apsaugos lygį reikia įvertinti atsižvelgiant į visas su duomenų perdavimo operacija arba duomenų perdavimo operacijų rinkiniu susijusias aplinkybes ir esamas sąlygas. Pagal šią direktyvą įkurta Darbo grupė asmenų apsaugai tvarkant asmens duomenis [2] išleido vadovą tokiems įvertinimams [3].

(4) Turint omenyje įvairius požiūrius į duomenų apsaugą trečiosiose šalyse, pakankamumas turėtų būti įvertinamas ir kiekvienas sprendimas, priimtas vadovaujantis Direktyvos 95/46/EB 25 straipsnio 6 dalimi, turėtų būti įgyvendinamas taip, kad savavališkai ar nepagrįstai nediskriminuotų trečiųjų šalių tais atvejais, kai vyrauja panašios sąlygos, nei taptų paslėpta verslo kliūtimi, atsižvelgiant į dabartinius Bendrijos tarptautinius įsipareigojimus.

(5) Šiuo sprendimu pripažįstamas pakankamas duomenų perdavimo iš Bendrijos į Jungtines Valstijas apsaugos lygis yra pasiekiamas, jei organizacijos laikosi iš valstybės narės į Jungtines Valstijas perduodamų asmens duomenų apsaugos „saugaus uosto“ privatumo principų (toliau vadinamų „Principais“) ir „Dažnai užduodamų klausimų“ (toliau vadinamų „FAQ“), nurodančių, kaip laikytis 2000 m. liepos 21 d. Jungtinių Valstijų Vyriausybės išleistų Principų. Be to, organizacijos turi viešai paskelbti savo privatumo taisykles ir joms turi būti taikoma Federalinės prekybos komisijos (FPK) jurisdikcija pagal Federalinės prekybos komisijos akto 5 skirsnį, kuriuo draudžiami komercijoje galimi naudoti ar jai įtakos turėti nesąžiningi ar apgaulingi veiksmai ar metodai, arba kitos įstatyminės institucijos jurisdikcija, kuri veiksmingai užtikrintų, kad būtų laikomasi pagal FAQ įgyvendinamų Principų.

(6) Šis sprendimas netaikomas sektoriams ir (arba) duomenų tvarkymo veiksmams, kurie nepriklauso nė vienos šio sprendimo VII priede išvardytų Jungtinių Valstijų Vyriausybinių institucijų jurisdikcijai.

(7) Tam, kad būtų tinkamai vykdomas šis sprendimas, būtina, kad Principų ir FAQ besilaikančias organizacijas žinotų suinteresuotos šalys, pvz., duomenų subjektai, duomenų eksportuotojai ir duomenų apsaugos institucijos. Tuo tikslu JAV komercijos departamentas ar jo įgaliotas asmuo turi įsipareigoti naudoti ir pateikti visuomenei sąrašą

---

[1] OL L 281, 1995 11 23, p. 31.

[2] Darbo grupės adresas internete: http://www.europa.eu.int/comm/internal_market/en/media/dataprot/wpdocs/index.htm

[3] WP 12: Asmens duomenų perdavimas trečiosioms šalims: 1998 m. liepos 24 d. darbo grupės priimtos ES duomenų apsaugos direktyvos 25 ir 26 straipsnių taikymas.

organizacijų, kurios patvirtina besilaikančios pagal FAQ nustatytų Principų ir kurios priklauso bent vienos šio sprendimo VII priede išvardytų Vyriausybinių institucijų jurisdikcijai.

(8) Siekiant skaidrumo ir norint apsaugoti valstybių narių kompetentingų institucijų gebėjimą užtikrinti asmenų apsaugą tvarkant jų asmens duomenis, šiame sprendime būtina tiksliai apibrėžti išskirtines aplinkybes, kuriomis būtų pateisinamas tam tikrų ypatingų duomenų srautų perdavimo sulaikymas, nepaisant to, kad yra pakankama apsauga.

(9) Principais ir FAQ sukurtą „saugų uostą“ gali reikėti patikslinti atsižvelgiant į patirtį, privatumo apsaugos pažangą, kai dėl technologijų tampa vis lengviau perduoti bei tvarkyti asmens duomenis, ir į vykdymo priežiūros institucijų įgyvendinimo ataskaitas.

(10) Pagal Direktyvos 95/46/EB 29 straipsnio nuostatas įkurta Darbo grupė asmenų apsaugai tvarkant asmens duomenis pareiškė savo nuomonę dėl apsaugos lygio, kurį suteikia „saugaus uosto principai“ Jungtinėse Valstijose, į kurią buvo atsižvelgta rengiat šį sprendimą [1].

(11) Šiame sprendime numatytos priemonės atitinka pagal Direktyvos 95/46/EEB 31 straipsnio nuostatas įkurto komiteto nuomonę.

(12) Remdamasis 2000 m. liepos 5 d. Tarybos sprendimu 1999/468/EB, ypač jo 8 straipsniu, Europos Parlamentas priėmė rezoliuciją A5-0177/2000 dėl Komisijos sprendimo dėl „saugaus uosto privatumo principų“ teikiamos apsaugos ir JAV komercijos departamento pateiktų su jais susijusių dažnai užduodamų klausimų [2] projekto. Komisija dar kartą išnagrinėjo sprendimo projektą, atsižvelgdama į tą rezoliuciją, ir padarė išvadą, kad nors Europos Parlamentas pareiškė nuomonę, kad „saugaus uosto principams“ ir su jais susijusiems DUK reikalingi tam tikri patobulinimai, kad būtų galima spręsti, kad jie suteikia „pakankamą apsaugą“, Parlamentas nenusprendė, kad Komisija viršytų savo įgaliojimus priimdama šį sprendimą,

PRIĖMĖ ŠĮ SPRENDIMĄ:

1 straipsnis

1. Direktyvos 95/46/EB 25 straipsnio 2 dalyje numatytais tikslais, visai tos direktyvos taikymo srityje numatytai veiklai, šio sprendimo I priede pateikti „saugaus uosto privatumo principai“ (toliau vadinami „Principais“) taikomi laikantis šio sprendimo II priede pateiktų 2000 m. liepos 21 d. JAV komercijos departamento išleistų „Dažnai užduodamų klausimų“ (toliau vadinamų „FAQ“) nurodymų ir laikomi užtikrinančiais pakankamą Jungtinėse Valstijose įsikūrusioms organizacijoms iš Bendrijos perduodamų asmens duomenų apsaugos lygį, atsižvelgiant į tokius JAV komercijos departamento išleistus dokumentus:

a) „saugaus uosto“ reikalavimų vykdymo priežiūros apžvalgą, pateiktą III priede;

b) memorandumą dėl JAV teisės aktuose nustatytų nuostolių už privatumo ir aiškių įgaliojimų pažeidimus atlyginimą, pateiktą IV priede;

c) Federalinės prekybos komisijos laišką, pateiktą V priede;

d) JAV transporto departamento laišką, pateiktą VI priede.

2. Vykdant kiekvieną duomenų perdavimo operaciją, būtina įvykdyti tokias sąlygas:

a) duomenis gaunanti organizacija vienareikšmiai ir viešai turi paskelbti apie savo įsipareigojimą laikytis pagal FAQ vykdomų Principų; ir

b) ta organizacija turi priklausyti vienai iš šio sprendimo VII priede išvardytų Jungtinių Valstijų Vyriausybinių institucijų, įgaliotų tirti skundus, ginti nuo nesąžiningų ar apgaulingų veiksmų ir atlyginti žalą asmenims, nesvarbu, kokioje šalyje jie gyvena, ar kokia jų tautybė, patirtą dėl pagal FAQ vykdomų Principų nesilaikymo, jurisdikcijai.

3. Šio straipsnio 2 dalyje nustatytų sąlygų laikomasi, jei organizacija pasiskelbia besilaikanti pagal FAQ vykdomų Principų, nuo dienos, kurią ta organizacija praneša JAV komercijos departamentui (ar jo įgaliotam asmeniui) apie viešą šio straipsnio 2 dalies a punkte nurodyto įsipareigojimo paskelbimą ir nurodo šio straipsnio 2 dalies b punkte nurodytos institucijos tapatybę.

---

[1] WP 15: Nuomonė 1/99 dėl duomenų apsaugos lygio Jungtinėse Valstijose ir vykstančių diskusijų tarp Europos Komisijos ir Jungtinių Valstijų.
WP 19: Nuomonė 2/99 dėl 1999 m. balandžio 19 d. JAV komercijos departamento išleistų „Tarptautinių“ saugaus uosto „principų“ pakankamumo.
WP 21: Nuomonė 4/99 dėl Dažnai užduodamų klausimų, kuriuos JAV komercijos departamentas ruošiasi išleisti remdamasis „saugaus uosto“ principais „dėl“ Tarptautinių „saugaus uosto“ principų „pakankamumo.“
WP 23: Darbinis dokumentas dėl diskusijų, vykstančių tarp Europos Komisijos ir Jungtinių Valstijų Vyriausybės dėl „Tarptautinių“ saugaus uosto „principų“ esamos padėties.
WP 27: Nuomonės 7/99 dėl 1999 m. lapkričio 15 ir 16 d. JAV komercijos departamento išleistų „Saugaus uosto“ principų, „paskelbtų kartu su“ Dažnai užduodamais klausimais „(FAQ)“ ir kitais susijusiais dokumentais.
WP 31: Nuomonė 3/2000 dėl ES ir JAV dialogo dėl „saugaus uosto“ parengimo.
WP 32: Nuomonė 4/2000 dėl „saugaus uosto“ principų „suteikiamo apsaugos lygio.“

[2] Rezoliucija dar nepaskelbta Oficialiajame leidinyje.

2 straipsnis

Šis sprendimas yra susijęs tik su Jungtinėse Valstijose pagal FAQ vykdomų Principų teikiamos apsaugos pakankamumu tam, kad būtų laikomasi Direktyvos 95/46/EB 25 straipsnio 1 dalies reikalavimų ir neturi įtakos kitų su asmens duomenų tvarkymu valstybėse narėse susijusių tos direktyvos nuostatų, ypač jos 4 straipsnio, taikymui.

3 straipsnis

1. Nepažeidžiant valstybių narių kompetentingų institucijų teisių imtis veiksmų, kad būtų laikomasi nacionalinių teisės nuostatų, priimtų pagal Direktyvos 95/46/EB, išskyrus 25 straipsnį, nuostatas, tos institucijos gali pasinaudoti teise sustabdyti duomenų teikimą organizacijai, kuri pasiskelbė besilaikanti pagal FAQ vykdomų Principų, taip apsaugant asmenis, kad jų duomenys nebūtų tvarkomi, jei:

a) šio sprendimo VII priede nurodyta Jungtinių Valstijų Vyriausybinė institucija arba šio sprendimo I priede nustatyto Vykdymo priežiūros principo a punkte numatytas nepriklausomas regreso teisės mechanizmas nustato, kad ta organizacija pažeidžia pagal FAQ vykdomus Principus; arba

b) yra didelė tikimybė, kad Principai yra pažeisti; galima pagrįstai manyti, kad naudojant atitinkamą vykdymo priežiūros mechanizmą nesiimama ar nebus imtasi pakankamų ir savalaikių priemonių išspręsti iškilusią problemą; tęsiant duomenų perdavimą susidarytų neišvengiamas pavojus rimtai pakenkti duomenų subjektams; valstybės narės kompetentingos institucijos ėmėsi pagrįstų pastangų tokiomis aplinkybėmis pranešti apie tai organizacijai ir suteikti jai galimybę nurodyti priežastis.

Duomenų teikimo sustabdymas nutraukiamas, kai tik yra užtikrinama, kad laikomasi pagal FAQ vykdomų Principų ir apie tai pranešama atitinkamoms kompetentingoms institucijoms Bendrijoje.

2. Valstybės narės nedelsdamos praneša Komisijai, kai imamasi priemonių pagal šio straipsnio 1 dalies nuostatas.

3. Valstybės narės ir Komisija taip pat informuoja viena kitą apie atvejus, kai atsakingų už pagal FAQ vykdomų Principų laikymąsi institucijų Jungtinėse Valstijose veiksmai neužtikrina tokio laikymosi.

4. Jei pagal šio straipsnio 1, 2 ir 3 dalių nuostatas sukaupta informacija suteikia įrodymus, kad bet kuri atsakinga už pagal FAQ vykdomų Principų laikymąsi institucija Jungtinėse Valstijose tinkamai neatlieka savo prievolių, Komisija informuoja JAV komercijos departamentą ir, jei būtina, pagal Direktyvos 95/46/EB 31 straipsnyje nustatytą tvarką pateikia numatomų šio sprendimo atšaukimo, sustabdymo ar jos taikymo srities apribojimo priemonių projektą.

4 straipsnis

1. Šis sprendimas gali būti bet kada pakeistas atsižvelgiant į jo vykdymo patirtį ir (arba) tuo atveju, jei JAV teisės aktais būtų reikalaujama didesnio už Principų ir FAQ suteikiamą apsaugos lygį.

Praėjus trejiems metams po sprendimo pranešimo valstybėms narėms, Komisija įvertina kaip šis sprendimas vykdomas ir remdamasi turima informacija praneša susijusias išvadas pagal Direktyvos 95/46/EB 31 straipsnį įsteigtam Komitetui, įskaitant visus įrodymus, kurie gali turėti įtakos vertinant, ar šio sprendimo 1 straipsnio nuostatos suteikia pakankamą apsaugą, kaip numato Direktyvos 95/46/EB 25 straipsnis, ir bet kokius galimus įrodymus, kad taikant šį sprendimą kas nors yra diskriminuojamas.

2. Jei būtina, Komisija pateikia numatomų priemonių projektą laikydamasi Direktyvos 95/46/EB 31 straipsnyje nustatytos tvarkos.

5 straipsnis

Valstybės narės ne vėliau kaip per 90 dienų po pranešimo pateikimo valstybėms narėms imasi visų priemonių, būtinų, kad būtų laikomasi šio sprendimo.

6 straipsnis

Šis sprendimas skirtas valstybėms narėms.

Priimta Briuselyje, 2000 m. liepos 26 d.

Komisijos vardu

Frederik BOLKESTEIN

Komisijos narys

I PRIEDAS

„SAUGAUS UOSTO“ PRIVATUMO PRINCIPAI

2000 m. liepos 21 d. išleisti JAV komercijos departamento

1998 m. spalio 25 d. įsigaliojo Europos Sąjungos išsamus privatumo teisės aktas – Direktyva dėl duomenų apsaugos (Direktyva). Ja reikalaujama, kad asmens duomenys būtų perduodami tik į tas ne ES šalis, kurios suteikia „pakankamą“ privatumo apsaugos lygį. Nors Jungtinės Valstijos ir Europos Sąjunga turi bendrą tikslą pagerinti savo piliečių privatumo apsaugą, Jungtinės Valstijos privatumą traktuoja skirtingai nuo Europos Sąjungos. Jungtinėse Valstijose taikomas sektorinis metodas, paremtas teisės aktų, reguliavimo ir savireguliavimo deriniu. Dėl šių skirtumų daugelis JAV organizacijų išreiškė abejonių dėl ES reikalaujamo „pakankamumo standarto“ perduodant asmens duomenis iš Europos Sąjungos į Jungtines Valstijas.

Šioms abejonėms išsklaidyti ir aiškesnei tokių duomenų perdavimų sistemai sudaryti Komercijos departamentas, turėdamas įstatymų nustatytus įgaliojimus, išleidžia šį dokumentą ir „Dažnai užduodamus klausimus“ („Principus“), skirtus remti, skatinti ir plėsti tarptautinę komerciją. Šie Principai buvo sukurti pasikonsultavus su pramonės ir visuomenės atstovais ir skirti prekybai bei komercijai tarp Jungtinių Valstijų ir Europos Sąjungos palengvinti. Jie tinka naudoti tik JAV organizacijoms, gaunančioms asmens duomenis iš Europos Sąjungos, kad jos galėtų gauti „saugaus uosto“ ir jo sukuriamos „pakankamumo“ prezumpcijos teises. Kadangi Principai skirti tik šiam konkrečiam tikslui, jie gali netikti kitiems tikslams. Principai nepakeičia Direktyvą įgyvendinančių nacionalinių nuostatų, skirtų tvarkyti asmens duomenis valstybėse narėse.

Organizacijos nusprendžia įgyti „saugaus uosto“ teises visiškai savanoriški ir tas teises jos gali įgyti įvairiais būdais. Jei organizacijos nusprendžia laikytis Principų, tai privalo jų laikytis ir viešai apie tai paskelbti, kad galėtų gauti ir naudotis „saugaus uosto“ privilegijomis. Pavyzdžiui, jei organizacija prisijungia prie savireguliacinės privatumo programos, kuri laikosi Principų, ji gauna „saugaus uosto“ teises. Tokias teises organizacijos gali gauti ir sukūrę nuosavas savireguliacines privatumo taisykles, jei jos atitinka Principus. Jei laikydamasi Principų organizacija visiškai ar iš dalies pasikliauja savireguliacija, tuomet už tokios savireguliacijos nesilaikymą taip pat privalo būti baudžiama pagal Federalinės prekybos komisijos aktą, kuriuo draudžiami nesąžiningi ir apgaulingi veiksmai, ar kitą tokius veiksmus draudžiantį įstatymą ar teisės aktą (ES pripažintų JAV įstatyminių institucijų sąrašas pateiktas prieduose). Be to, teises naudotis „saugaus uosto“ privilegijomis gali gauti ir organizacijos, kurias saisto norminiai, administraciniai ar kitokie teisės aktai (ar taisyklės), veiksmingai saugantys asmens privatumą. Visais atvejais „saugaus uosto“ privilegijos užtikrinamos nuo tos dienos, nuo kurios pageidaujanti gauti „saugaus uosto“ teises organizacija patvirtina Komercijos departamentui (ar jo įgaliotam asmeniui) savo įsipareigojimą laikytis Principų pagal nurodymus, pateiktus „Dažnai užduodamuose klausimuose“ dėl įsipareigojimo.

Principų laikymasis gali būti ribojamas: a) tiek, kiek būtina atsižvelgiant į nacionalinio saugumo, visuomenės interesus arba teisės aktų vykdymo reikalavimus; b) įstatymais, Vyriausybės nutarimais arba precedentine teise, dėl kurių atsiranda prieštaringų įsipareigojimų ar aiškių įgaliojimų, jei vykdydama tokius įgaliojimus organizacija gali įrodyti, kad Principų nesilaikoma tik tiek, kiek tai būtina atsižvelgiant į organizacijos palaikomus viršesnius teisėtus interesus; arba c) jei valstybės narės įstatymai dėl Direktyvos numato išimtis ar leidžiančias nukrypti nuostatas ir jei tokios išimtys ar leidžiančias nukrypti nuostatos taikomos dėl panašių priežasčių. Siekdamos privatumo apsaugos stiprinimo, organizacijos turi stengtis visiškai ir skaidriai laikytis šių Principų, o jei ankstesnio sakinio b punkte nurodytos išimtys bus taikomos reguliariai, jos turi tai nurodyti savo privatumo taisyklėse. Dėl tos pačios priežasties pageidaujama, kad tais atvejais, kai pagal Principus ir (arba) JAV taisės aktus galima pasirinkti kelis variantus, organizacijos pasirinktų geriausią apsaugą suteikiantį variantą.

Praktiniais ar kitais sumetimais organizacijos gali pageidauti taikyti Principus visiems savo duomenų tvarkymo veiksmams, tačiau jos privalo juos taikyti tik duomenims, perduodamiems po to, kai jos patenka į „saugų uostą“. Tam, kad gautų „saugaus uosto“ teises, organizacijos neprivalo taikyti šių Principų rankiniu būdu tvarkomose rinkmenų sistemose esančiai asmeninei informacijai. Organizacijos, pageidaujančios pasinaudoti „saugaus uosto“ privilegijomis siekiant gauti informacijos į neautomatiniu būdu tvarkomas rinkmenų sistemas iš ES, privalo taikyti Principus visai

informacijai, perduodamai po to, kai jos patenka į „saugų uostą“. Organizacija, kuri pageidauja praplėsti „saugaus uosto“ privilegijas žmogiškųjų išteklių asmeninei informacijai, perduodamai iš ES ir skirtai naudoti darbo santykiuose, privalo tai nurodyti, kai ji patvirtina Komercijos departamentui (ar jo įgaliotam asmeniui) savo įsipareigojimą laikytis „Dažnai užduodamų klausimų“ dėl įsipareigojimo. Organizacijos galės suteikti Direktyvos 26 straipsnyje reikalaujamą apsaugą ir tuomet, jei įtrauks Principus į rašytines sutartis su šalimis, perduodančiomis duomenis iš ES, vietoj savarankiškų privatumo nuostatų, jei kitoms nuostatoms tokiose tipinėse sutartyse pritartų Komisija ir valstybės narės.

„Saugaus uosto“ principų atitikimo (įskaitant ir Dažnai užduodamus klausimus) ir „saugaus uosto“ organizacijų atitinkamų privatumo taisyklių interpretacijos klausimai bus nagrinėjami pagal JAV teisę, išskyrus atvejus, kai organizacijos įsipareigojo bendradarbiauti su Europos duomenų apsaugos institucijomis. Išskyrus atvejus, kai nurodyta kitaip, visos „saugaus uosto“ principų ir Dažnai užduodamų klausimų nuostatos taikomos pagal paskirtį.

„Asmens duomenys“ ir „asmeninė informacija“ yra JAV organizacijos iš Europos Sąjungos gauti ir bet kuria forma įrašyti duomenys apie nustatytos arba galimos nustatyti tapatybės asmenį, kuriems taikoma Direktyva.

PRANEŠIMAS

Organizacija privalo pranešti asmenims priežastis, dėl kurių ji renka ir naudoja informaciją apie juos, kaip kreiptis į organizaciją su prašymais ar skundais, apie trečiąsias šalis, kurioms ji atskleidžia tą informaciją ir apie informacijos naudojimui ir atskleidimui apriboti skirtas galimybes bei priemones, kurias organizacija siūlo asmenims. Toks pranešimas turi būti pateiktas aiškia ir suprantama kalba tada, kai asmenų pirmą kartą prašoma suteikti asmeninę informaciją organizacijai arba kiek įmanoma greičiau po to, tačiau bet kuriuo atveju prieš organizacijai panaudojant tokią informaciją kitais tikslais, nei tie, dėl kurių duomenis perduodančioji organizacija ją iš pradžių surinko ar tvarkė, arba prieš pirmą kartą ją atskleidžiant trečiajai šaliai ([1]).

PASIRINKIMAS

Organizacija privalo suteikti asmenims galimybę pasirinkti (*opt out* būdu), ar jų asmeninė informacija gali būti: a) atskleista trečiajai šaliai ([1]) arba b) naudojama tikslais, neatitinkančiais tų tikslų, dėl kurių ji buvo iš pradžių surinkta, ar vėliau buvo gautas asmens sutikimas ją naudoti. Asmenims turi būti suteikti aiškūs, suprantami, lengvai naudojami ir prieinami pasirinkimo mechanizmai.

Dėl ypatingos informacijos (t. y. asmeninės informacijos apie sveikatos būklę, rasinę ar etninę kilmę, politines pažiūras, religinius ar filosofinius įsitikinimus, narystę profesinėse sąjungose ar informacijos apie asmens lytinį gyvenimą) turi būti suteikta pritariamoji arba aiški (*opt in* būdu) galimybė pasirinkti, ar informacija gali būti atskleista trečiajai šaliai arba naudojama tikslais, neatitinkančiais tų tikslų, dėl kurių ji buvo iš pradžių surinkta ar vėliau pasirenkant (*opt in* būdu) buvo gautas asmens sutikimas ją naudoti. Bet kuriuo atveju organizacija visuomet turi laikyti iš trečiųjų šalių gautą informaciją ypatinga, jei ta trečioji šalis tą informaciją traktuoja kaip ypatingą.

TOLIMESNIS PERDAVIMAS

Norėdamos atskleisti informaciją trečiajai šaliai, organizacijos privalo taikyti Pranešimo ir Pasirinkimo principus. Jei organizacija pageidauja perduoti informaciją atstovo funkcijas atliekančiai trečiajai šaliai (kaip nurodyta išnašoje), ji gali tai daryti tik įsitikinusi, kad ta trečioji šalis laikosi Principų, Direktyvos ar kitų pakankamumo nuostatų arba sudaro su ta trečiąja šalimi rašytinę sutartį, kurioje reikalaujama, kad trečioji šalis suteiktų ne mažesnį privatumo apsaugos lygį, nei reikalauja atitinkami Principai. Jei organizacija laikosi šių reikalavimų, ji neturi būti laikoma atsakinga (nebent organizacija pripažįsta esant kitaip) už tai, kad trečioji šalis, kuriai ji perduoda tokią informaciją, ją tvarko nepaisydama apribojimų ar nusiskundimų, nebent organizacija iš anksto žinojo arba turėjo žinoti, kad trečioji šalis ją tvarkys tokiu netinkamu būdu ir nesiėmė pagrįstų veiksmų, tam, kad išvengtų tokio tvarkymo ar jį sustabdyti.

([1]) Nebūtina pranešti arba suteikti pasirinkimą, kai informacija atskleidžiama trečiajai šaliai, kuri veikia kaip atstovas vykdydama užduotį (-is) organizacijos vardu ir jai vadovaujant. Tačiau, kita vertus, tokiais atvejais galioja Tolimesnio perdavimo principas.

SAUGUMAS

Asmeninę informaciją formuojančios, laikančios, naudojančios ar platinančios organizacijos privalo imtis pagrįstų apsaugos priemonių, saugančių, kad tokia informacija nebūtų prarasta, naudojama ne pagal paskirtį ar asmenims prieinantiems prie jos neautorizuotu būdu, ji nebūtų, atskleista, pakeista ar sunaikinta.

DUOMENŲ VIENTISUMAS

Laikantis Principų, asmeninė informacija turi atitikti jos panaudojimo tikslus. Organizacija neturi teisės tvarkyti asmeninę informaciją tokiais būdais, kurie neatitinka tikslų, dėl kurių ji buvo surinkta ar vėliau buvo gautas asmens sutikimas ją naudoti. Tiek, kiek būtina tokiems tikslams, organizacija turi imtis pagrįstų priemonių užtikrinti, kad duomenys atitiktų numatomą jų naudojimo paskirtį, būtų tikslūs, išsamūs ir naujausi.

PRIĖJIMAS

Asmenims turi būti suteikta galimybė prieiti prie organizacijos laikomos asmeninės informacijos apie juos, ją pataisyti, pakeisti ar sunaikinti, jei ji būtų netiksli, išskyrus atvejus, kai priėjimo suteikimo sudėtingumas ar išlaidos būtų neproporcingai didelės lyginant su pavojumi to asmens privatumui arba būtų pažeistos kitų asmenų teisės.

VYKDYMAS

Veiksmingai privatumo apsaugai būtini mechanizmai, užtikrinantys Principų laikymąsi, regreso teisę asmenims, kurių duomenims turėjo įtakos Principų nesilaikymas, ir Principų nesilaikančios organizacijos atsakomybė. Būtiniausi mechanizmai turi būti tokie: a) lengvai prieinami ir galimi pasinaudoti nepriklausomi regreso teisės mechanizmai, kuriais būtų tiriami ir laikantis Principų išspręsti kiekvieno asmens skundai bei ginčai ir priteistas žalos atlyginimas, jei tai numato taikytini teisės aktai ar privataus sektoriaus nuostatos, b) atsiliepimų procedūros, skirtos patikrinti, ar įmonių liudijimai ir patikinimai apie privatumo taisykles yra teisingi ir ar tokios privatumo taisyklės yra taikomos taip, kaip skelbiama ir c) įsipareigojimai išspręsti nesklandumus, kylančius dėl to, kad pasiskelbusios besilaikančiomis Principų organizacijos jų nesilaiko, ir tokių organizacijų atsakomybė. Sankcijos turi būti pakankamai griežtos, kad priverstų organizacijas laikytis įsipareigojimų.

Papildymas

Europos Sąjungos pripažįstamų JAV įstatyminių institucijų sąrašas

Europos Sąjungos pripažįstamos kaip turinčios įgaliojimus tirti skundus ir ginti nuo nesąžiningų ar apgaulingų veiksmų, atlyginti žalą asmenims, jei būtų nesilaikyta pagal FAQ vykdomų Principų, tokios JAV įstatyminės institucijos:

— Federalinė prekybos komisija, veikianti pagal Federalinės prekybos komisijos akto 5 skyriuje suteiktus oficialius įgaliojimus,

— Transporto departamentas, veikiantis pagal Jungtinių Valstijų kodekso 41712 skyriaus 49 dalyje suteiktus oficialius įgaliojimus.

II PRIEDAS

DAŽNAI UŽDUODAMI KLAUSIMAI (FAQ)

1 FAQ — Ypatingi duomenys

K.: *Ar organizacijos visada privalo suteikti aiškų pasirinkimą (opt in būdu) dėl ypatingų duomenų?*

A.: Ne, tokio pasirinkimo suteikti nebūtina, jei: 1) duomenys tvarkomi duomenų subjektui ar kitam asmeniui gyvybiškai svarbiais tikslais; 2) duomenis tvarkyti būtina rengiant ieškininius pareiškimus ar gynybą; 3) duomenų reikia medicinos priežiūrai atlikti ar diagnozei nustatyti; 4) duomenys tvarkomi vykdant fondo, asociacijos ar kitos pelno nesiekiančios organizacijos, užsiimančios politine, filosofine, religine ar profsąjungine veikla, teisėtą veiklą, jei tai susiję tik su organizacijos nariais ar reguliariai su jos veikla susijusių reikalų turinčiais asmenimis ir tokie duomenys be duomenų subjekto sutikimo nėra atskleidžiami trečiajai šaliai; 5) duomenys būtini darbo teisinius santykius reglamentuojančiuose teisės aktuose numatytiems organizacijos įsipareigojimams vykdyti arba 6) tai yra duomenys, kuriuos asmuo aiškiai viešai paskelbė.

2 FAQ — Išimtys žurnalistikai

K.: *Turint omenyje JAV spaudos laisvės konstitucinę apsaugą ir Direktyvos išimtį žurnalistinei medžiagai, ar „saugaus uosto" principai galioja žurnalistikos tikslais surinktai, turimai ar platinamai asmeninei informacijai?*

A.: Kai JAV Konstitucijos pirmojoje pataisoje nustatytos laisvos spaudos teisės prieštarauja privatumo apsaugos interesams, JAV asmenų ir organizacijų veiklos interesai derinami taikant Pirmosios pataisos normas. „Saugaus uosto" principai netaikomi asmeninei informacijai, kuri yra surinkta skelbti, transliuoti ar kitoms, žurnalistinės medžiagos, visuomenės informavimo formoms, ar ji būtų panaudota, ar ne, taip pat ir iš žurnalistikos archyvų pasklidusiai anksčiau skelbtai informacijai.

3 FAQ — Netiesioginė atsakomybė

K.: *Ar pagal „saugaus uosto" principus interneto ar telekomunikacijų paslaugų teikėjai ar kitos organizacijos (IPT) yra teisiškai atsakingi, jei kitos organizacijos vardu jie tik perduoda, nukreipia, pakeičia ar saugo informaciją, kuri gali pažeisti Principus?*

A.: Ne. Kaip numatyta ir pačioje Direktyvoje, „saugus uostas" nesukuria netiesioginės atsakomybės. Jei organizacija atlieka tik trečiųjų šalių siunčiamos informacijos perdavimo funkciją ir neapsprendžia tų asmens duomenų tvarkymo tikslų ir priemonių, ji nėra teisiškai atsakinga.

4 FAQ — Investicijų bankininkystė ir auditai

K.: *Vykdydami savo veiklą auditoriai ir investicijų bankininkai gali tvarkyti asmens duomenis be jo sutikimo ar žinios. Kokiomis aplinkybėmis tai leidžiama pagal Pranešimo, Pasirinkimo ir Priėjimo principus?*

A.: Auditoriai ir investicijų bankininkai gali tvarkyti asmens duomenis be jo žinios pirmiausia tuo atveju, kai būtina vykdyti įstatymų ar visuomenės interesų reikalavimus bei esant tokioms aplinkybėms, kai Principai gali pakenkti teisėtiems organizacijos interesams. Tokie teisėti interesai yra kompanijos juridinių įsipareigojimų vykdymo ir teisėtos apskaitybos vedimo monitoringas (stebėsena) ir konfidencialumo reikalavimai, susiję su galimais įmonių įsigijimais, apsijungimais, bendromis įmonėmis ar kitomis auditorių ir investicijų bankininkų vykdomomis operacijomis.

5 FAQ — Duomenų apsaugos institucijų vaidmuo

K.: *Kaip kompanijos, įsipareigojančios bendradarbiauti su Europos Sąjungos duomenų apsaugos institucijomis (DAI), tuos įsipareigojimus prisiima ir kaip jie vykdomi?*

A.: „Saugaus uosto“ sistema įpareigoja JAV organizacijas, gaunančias asmens duomenis iš ES, naudoti veiksmingus mechanizmus, užtikrinančius „saugaus uosto“ principų laikymąsi. Vykdymo priežiūros principas nustato, kad jos privalo užtikrinti: a) regreso teisę asmenims, su kuriais susiję duomenys; b) atsiliepimų procedūras, skirtas patikrinti, ar įmonių liudijimai ir patikinimai apie privatumo taisykles yra teisingi; ir c) įsipareigojimą išspręsti nesklandumus, kylančius dėl to, kad besilaikančios Principų organizacijos iš tikrųjų jų nesilaiko, ir tokių organizacijų atsakomybę. Organizacija gali atitikti Vykdymo priežiūros principo a ir c punktus, jei ji laikosi šio FAQ reikalavimų dėl bendradarbiavimo su DAI.

Organizacija gali įsipareigoti bendradarbiauti su DAI ir tai turi būti įrašyta „saugaus uosto“ liudijime Komercijos departamentui (žr. 6 FAQ dėl įsipareigojimo), kuriame skelbiama, kad ji:

1) įsipareigodama bendradarbiauti su DAI, apsisprendė laikytis Vykdymo priežiūros principo a ir c punktų;

2) bendradarbiaus su DAI tiriant ir sprendžiant skundus „saugaus uosto“ sistemoje ir

3) laikysis visų DAI teikiamų rekomendacijų, kai DAI manymu organizacijai reikia imtis tam tikrų veiksmų norint laikytis „saugaus uosto“ principų, įskaitant teisės gynimo ir kompensacines priemones asmenims, nukentėjusiems dėl Principų bet kokio nesilaikymo, ir raštu patvirtins DAI, kad tokių veiksmų buvo imtasi.

DAI bendradarbiaus suteikdamos informaciją ir teikdamos konsultacijas tokiais būdais:

— DAI konsultacijos bus teikiamos per Europos Sąjungos lygiu įkurtą DAI informacijos grupę, kuri, *inter alia*, padės užtikrinti darnų ir nuoseklų suartėjimą,

— specialistų grupė teiks konsultacijas JAV organizacijoms dėl neišnagrinėtų skundų, kuriuos asmenys pateikia dėl iš ES „saugaus uosto“ sistemoje perduotos asmeninės informacijos tvarkymo. Tokiomis konsultacijomis bus siekiama užtikrinti, kad „saugaus uosto“ principai būtų taikomi teisingai ir būtų suteiktos asmenų teisių gynimo priemonės, kurias DAI laikys tinkamomis,

— grupė teiks tokias konsultacijas atsakydama į organizacijų pranešimus ir (arba) tiesiai iš asmenų gautus nusiskundimus organizacijomis, įsipareigojusiomis bendradarbiauti su DAI „saugaus uosto“ tikslais, paskatindama ir, jei reikia, padėdama tokiems asmenims iš pradžių pasinaudoti vidinėmis skundų nagrinėjimo priemonėmis, kurias gali pasiūlyti organizacija.

— Konsultacijos bus suteikiamos tik abiem šalims susitarimo keliu gavus pagrįstą galimybę aiškinti ir pateikti visus pageidaujamus įrodymus. Grupė sieks suteikti konsultaciją laikantis nustatytos tvarkos reikalavimų kiek įmanoma greičiau. Pagal bendrą taisyklę grupė konsultaciją sieks suteikti per 60 dienų nuo skundo ar pranešimo gavimo, o jei įmanoma — greičiau,

— grupė viešai skelbs jai pateiktų skundų svarstymo rezultatus, jei manys, kad tai reikalinga,

— grupei ar DAI neužtraukia jokios atsakomybės už grupės vardu suteiktas konsultacijas.

Kaip pažymėta anksčiau, šį ginčų sprendimo būdą pasirinkusios organizacijos privalo įsipareigoti laikytis DAI konsultacijų. Jei organizacija per 25 dienas po konsultacijos pateikimo neįvykdo jos reikalavimų ir nepateikia tinkamo paaiškinimo, grupė praneš apie savo ketinimus pateikti klausimą Federalinei prekybos komisijai ar kitai JAV federalinei ar valstybinei institucijai, kad ji imtųsi vykdymo priežiūros veiksmų apgaulės arba klaidinimo atvejais, arba nuspręs, kad bendradarbiavimo sutartis yra rimtai pažeista ir dėl to turi būti pripažinta niekine ir negaliojančia. Pastaruoju atveju grupė informuos Komercijos departamentą (ar jo įgaliotą asmenį), kad būtų atitinkamai pakoreguotas „saugaus uosto“ dalyvių sąrašas. Bet koks įsipareigojimo bendradarbiauti su DAI nevykdymas ir „saugaus uosto“ principų nevykdymas pagal FPK akto 5 skirsnį ar panašų normatyvinį aktą bus laikomas apgaulingais veiksmais.

Šią galimybę pasirinkusios organizacijos privalės mokėti metinį mokestį, skirtą grupės veiklos išlaidoms padengti, ir dar papildomai gali būti paprašyta padengti būtinas vertimo išlaidas, susijusias su pranešimų ar skundų prieš organizacijas svarstymu. Metinis mokestis bus ne didesnis kaip 500 JAV dolerių, o mažesnėms kompanijoms jis bus mažesnis.

Bendradarbiavimo su DAI galimybę galės pasirinkti tos organizacijos, kurios prisijungs prie „saugaus uosto“ per trejų metų laikotarpį. Prieš baigiantis šiam laikotarpiui, DAI persvarstys šią nuostatą, jei ją pasirinkusių JAV organizacijų skaičius pasirodys per didelis.

6 FAQ — Įsipareigojimas

K.: *Kaip organizacija gali įsipareigoti laikytis „saugaus uosto“ principų?*

A.: „Saugaus uosto“ privilegijos suteikiamos nuo dienos, kurią organizacija patvirtina Komercijos departamentui (ar jo įgaliotam asmeniui), kad ji įsipareigoja laikytis Principų pagal toliau pateiktus nurodymus.

Norėdamos patvirtinti savo dalyvavimą „saugiame uoste“, organizacijos gali pateikti Komercijos departamentui (ar jo įgaliotam asmeniui) kompanijos pareigūno organizacijos vardu pasirašytą raštą, kad prisijungiama prie „saugaus uosto“, kuriame būtų pateikta bent jau tokia informacija:

1) organizacijos pavadinimas, pašto adresas, elektroninio pašto adresas, telefono ir fakso numeriai;

2) organizacijos veiklos, susijusios su asmenine informacija, gaunama iš ES, aprašymas ir

3) organizacijos privatumo taisyklių, susijusių su asmenine informacija, aprašymas: a) kur su šiomis privatumo taisyklėmis galima viešai susipažinti; b) jų taikymo pradžios data; c) ryšių palaikymo biuras, kuris svarsto skundus, vertina reikalavimus ir tvarko visus kitus „saugaus uosto“ sistemos reikalus; d) konkreti įstatyminė institucija, turinti jurisdikciją svarstyti bet kokius skundus prieš organizaciją dėl galimų nesąžiningų ar apgaulingų veiksmų ir privatumo teisės aktų ar taisyklių pažeidimų (esanti Principų papildyme pateiktame sąraše); e) privatumo programų, kuriose dalyvauja organizacija, pavadinimai; f) patikrinimo būdas (pvz., vidinis, trečiųjų šalių) ([1]) ir g) nepriklausomas regreso teisės mechanizmas neišspręstiems nusiskundimams tirti.

Organizacijos, kurios pageidauja praplėsti „saugaus uosto“ privilegijas žmogiškųjų išteklių informacijai, perduodamai iš ES ir skirtai naudoti darbo santykiuose, gali tai daryti, jei yra įstatyminė institucija, turinti jurisdikciją svarstyti bet kokius skundus prieš organizaciją dėl informacijos apie žmogiškuosius išteklius ir esanti Principų priede pateiktame sąraše. Be to, organizacija turi tai nurodyti savo rašte ir paskelbti savo įsipareigojimą bendradarbiauti su ES valdžios institucija ar institucijomis, laikydamasi 9 FAQ ir 5 FAQ, ir laikytis tokių institucijų teikiamų konsultacijų.

Departamentas (ar jo įgaliotas asmuo) turės tokius raštus pateikusių visų organizacijų sąrašą ir taip bus užtikrinta galimybė naudotis „saugaus uosto“ privilegijomis. Sąrašas bus atnaujintas pagal kasmetinius raštus ir pranešimus, gautus pagal 11 FAQ nurodymus. Tokie įsipareigojimo raštai turi būti pateikiami ne rečiau kaip kartą per metus. Priešingu atveju organizacija bus išbraukta iš sąrašo ir „saugaus uosto“ privilegijos nebebus suteikiamos. Tiek

([1]) Žr. 7 FAQ dėl tikrinimo.

sąrašas, tiek organizacijų pateikti įsipareigojimo raštai bus skelbiami viešai. Visos savo dalyvavimą „saugiame uoste“ patvirtinusios organizacijos privalo savo privatumo taisyklių pareiškimuose paskelbti, kad jos įsipareigoja laikytis „saugaus uosto“ principų.

Įsipareigojimas laikytis „saugaus uosto“ principų dėl duomenų, gautų per laikotarpį, kurį organizacija naudojasi „saugaus uosto“ privilegijomis, galioja neterminuotai. Toks įsipareigojimas reiškia, kad organizacija ir toliau taikys Principus tokiems duomenims, kol ji juos laiko, naudoja ar atskleidžia, net jei dėl kokios nors priežasties palieka „saugų uostą“.

Organizacija, kuri dėl bendrovių susijungimo ar teisių perėmimo nustoja egzistuoti kaip atskiras juridinis asmuo, apie tai privalo iš anksto informuoti Komercijos departamentą (ar jo įgaliotą asmenį). Informuojant ji kartu turi nurodyti, ar ją įsigijęs juridinis asmuo ar po susijungimo susikūręs juridinis asmuo 1) toliau laikysis „saugaus uosto“ principų pagal bendrovių susijungimą ar teisių perėmimą reglamentuojantį teisės aktą arba 2) nuspręs patvirtinti savo įsipareigojimą laikytis „saugaus uosto“ principų ar imtis kitų apsaugos priemonių, pvz., raštu sudaryti sutartį, kuri užtikrintų, kad bus laikomasi „saugaus uosto“ principų. Jei nepasirenkamas nė vienas iš pirmiau nurodytų variantų, visi „saugaus uosto“ sistemoje gauti duomenys turi būti nedelsiant sunaikinti.

Organizacija neprivalo taikyti „saugaus uosto“ principų visai asmeninei informacijai, tačiau ji privalo juos taikyti visiems asmens duomenims, gautiems iš ES po to, kai ji prisijungia prie „saugaus uosto“.

Už bet kokį visuomenės klaidinimą dėl organizacijos įsipareigojimo laikytis „saugaus uosto“ principų ją gali bausti Federalinė prekybos komisija ar kita atitinkama valstybės institucija. Už melagingus tvirtinimus Komercijos departamentui (ar jo įgaliotam asmeniui) gali būti baudžiama pagal Melagingų parodymų aktą (18 U.S.C. § 1001).

7 FAQ — Patikrinimas

K.: *Kaip organizacijos turi organizuoti atsiliepimų procedūras, skirtas patikrinti, ar jų liudijimai ir patikinimai apie privatumo taisykles yra teisingi, ar šios taisyklės yra taikomos taip, kaip skelbiama, ar laikomasi „saugaus uosto“ principų?*

A.: Siekdama laikytis Vykdymo priežiūros principo reikalavimų dėl tikrinimo, organizacija gali tikrinti tokius liudijimus ir patikinimus saviatestacijos ar išorinių reikalavimų laikymosi patikrinimų būdais.

Naudojant saviatestacijos būdą, tikrinimu turi būti nustatyta, ar organizacijos paskelbtos privatumo taisyklės dėl asmeninės informacijos, gautos iš ES, yra teisingos, visapusės, aiškiai išdėstytos, visiškai vykdomos ir prieinamos. Tikrinimas taip pat turi patvirtinti, kad privatumo taisyklės atitinka „saugaus uosto“ principus; kad asmenys yra informuoti apie vidines skundų nagrinėjimo priemones ir nepriklausomus mechanizmus, kuriais naudodamiesi jie gali reikšti nusiskundimus; kad organizacija yra parengusi darbuotojų mokymo, kaip ją vykdyti, tvarką ir drausminimo priemones, kai jos nesilaikoma; kad yra parengta vidaus tvarka, pagal kurią periodiškai atliekami objektyvūs patikrinimai, kaip laikomasi reikalavimų. Bent kartą per metus turi būti surašyta kompanijos pareigūno ar kito įgalioto organizacijos atstovo pasirašyta saviatestaciją patvirtinanti ataskaita, ji turi būti pateikiama asmenų prašymu atliekant tyrimą arba esant nusiskundimų dėl reikalavimų nesilaikymo.

Organizacijos turi tvarkyti jų „saugaus uosto“ privatumo taisyklių praktinio vykdymo registrus ir pateikti juos už nusiskundimų nagrinėjimą atsakingai nepriklausomai institucijai ar agentūrai, kurios jurisdikcija aprėpia nesąžiningų ir apgaulingų veiksmų tyrimą, kai to pareikalaujama atliekant tyrimą ar esant nusiskundimų dėl reikalavimų nesilaikymo.

Jei organizacija pasirenka išorinius reikalavimų laikymosi patikrinimus, jais turi būti nustatyta, ar organizacijos privatumo taisyklės dėl asmeninės informacijos, gautos iš ES, atitinka „saugaus uosto“ principus, ar jų laikomasi ir ar asmenys yra informuoti apie mechanizmus, kuriais naudodamiesi jie gali reikšti nusiskundimus. Patikrinimai gali būti atliekami tokiais (tačiau nebūtinai vien tokiais) būdais: auditu, atsitiktiniais patikrinimais, panaudojant „spąstų“ metodą arba pasitelkiant technologijos priemones. Bent kartą per metus turi būti surašyta

tikrintojo, kompanijos pareigūno ar kito įgalioto organizacijos atstovo pasirašyta išorinį reikalavimų laikymosi patikrinimą patvirtinanti ataskaita ir ji turi būti pateikiama asmenų prašymu atliekant tyrimą arba esant nusiskundimų dėl reikalavimų nesilaikymo.

8 FAQ — Priėjimas

Priėjimo principas:

Asmenys privalo prieiti prie organizacijos laikomos asmeninės informacijos apie juos ir turėti galimybę ją ištaisyti, pakeisti ar sunaikinti, jei ji būtų netiksli, išskyrus atvejus, kai priėjimo suteikimo sudėtingumas ar išlaidos būtų neproporcingai didelės lyginant su pavojumi to asmens privatumui arba būtų pažeistos kitų asmenų teisės.

1. K.: *Ar priėjimo teisė yra besąlygiška?*

1. A.: Ne. Pagal „saugaus uosto“ principus priėjimo teisė yra esminis privatumo apsaugos principas. Taip leidžiama asmenims patikrinti apie juos saugomos informacijos tikslumą. Nepaisant to, organizacijos įsipareigojimui suteikti asmeniui priėjimą prie jos laikomos informacijos apie jį yra taikomas proporcingumo ar pagrįstumo principas ir tam tikrais atvejais jį reikia apriboti. 1980 m. OECD Privatumo vadovo Aiškinamasis memorandumas aiškiai nurodo, kad organizacijos priėjimo suteikimo įsipareigojimas nėra besąlygiškas. Šiuo įsipareigojimu nereikalaujama itin kruopščios paieškos, kokios gali būti reikalaujama, pvz., šaukime į teismą, taip pat nereikalaujama suteikti priėjimo prie visų organizacijos turimų įvairių informacijos saugojimo formų.

Patirtis parodė, kad, reaguodama į asmens reikalavimą suteikti priėjimą, organizacija iš pradžių turi įvertinti, dėl kokių priežasčių to reikalaujama. Pavyzdžiui, jei priėjimo reikalavimas yra neapibrėžtas ar didelės apimties, organizacija galėtų pabendrauti su asmeniu, kad galėtų geriau suprasti reikalavimo motyvus ir nustatyti tinkamiausią informaciją. Organizacija gali pasiteirauti, su kuriais organizacijos padaliniais asmuo bendravo ir (arba) apie informacijos, prie kurios reikalaujama prieiti, pobūdį (ar panaudojimą). Vis tik asmenys neprivalo pateisinti reikalavimų prieiti prie nuosavų duomenų.

Išlaidos ir sudėtingumas yra svarbūs veiksniai ir į juos reikėtų atsižvelgti, tačiau jie nelemia priėjimo suteikimo pagrįstumo. Pavyzdžiui, jei informacija naudojama sprendimams, kurių įtaka asmeniui didžiulė (pavyzdžiui, atimtų ar suteiktų svarbią naudą, kaip antai, draudimo, hipotekos ar darbo suteikimo reikalais), tuomet, laikydamasi kitų šių FAQ nuostatų, organizacija turėtų atskleisti informaciją net jei ją palyginti sunku ar brangu suteikti.

Jei reikalaujama informacija nėra ypatinga ir nelemia sprendimų, kurių įtaka asmeniui didžiulė (pvz., neypatingi rinkodaros duomenys, naudojami nustatyti, ar išsiųsti asmeniui katalogą), tačiau lengvai prieinama ir ją nebrangu pateikti, organizacija turėtų suteikti priėjimą prie faktinės informacijos, kurią ji laiko apie tą asmenį. Tokią informaciją galėtų sudaryti iš asmens gauti faktai, operacijos metu surinkti faktai ar iš kitų su asmeniu susijusių žmonių gauti faktai.

Kadangi priėjimas yra esminio pobūdžio principas, todėl, organizacijos turėtų visuomet tinkamai pasistengti suteikti priėjimo galimybę. Pavyzdžiui, kai tam tikrą informaciją reikia apsaugoti ir ją galima lengvai atskirti nuo kitos informacijos, prie kurios prašoma prieiti, organizacija turėtų atskirti apsaugotą informaciją ir pateikti tik tą, kurios prašoma. Jei kuriuo nors konkrečiu atveju organizacija nusprendžia, kad prieiti prie informacijos draudžiama, ji turi prašančiam asmeniui nurodyti priežastį, dėl kurios ji taip nusprendė ir pasiūlyti papildomą būdą priėjimui reikalauti.

2. K.: *Kas yra konfidenciali komercinė informacija ir ar organizacijos gali neleisti prieiti prie jos norėdamos ją apsaugoti?*

2. A.: Konfidenciali komercinė informacija (pagal šio termino apibrėžimą, naudojamą Federalinėse civilinio proceso taisyklėse dėl faktų pateikimo teismui) yra tokia informacija, kurią organizacija stengiasi apsaugoti nuo atskleidimo, jei jos atskleidimas padėtų rinkos konkurentams. Konfidencialia komercine informacija gali būti konkreti organizacijos naudojama kompiuterinė programa, pvz., modeliavimo programa ar smulkesnė informacija apie ją. Jei konfidencialią komercinę informaciją galima lengvai atskirti nuo kitos informacijos, prie kurios prašoma prieiti,organizacija turėtųatskirti apsaugotą informaciją ir pateikti nekonfidencialią

informaciją. Organizacijos gali neleisti arba apribotipriėjimą, jei suteikus priėjimą būtų atskleista pirmiau apibrėžta jos pačios konfidenciali komercinė informacija, pvz., organizacijos sudarytos rinkodaros išvados ar klasifikacijos, arba kitų konfidenciali komercinė informacija, kur tokia informacija saistoma sutartinių konfidencialumo įsipareigojimų, tuomet, kai tokie įsipareigojimai tomis aplinkybėmis paprastai būtų prisiimami ar nustatyti.

3. K.: *Ar suteikiant priėjimą organizacija gali atskleisti fizinių asmenų asmeninę informaciją apie juos paimdama ją iš duomenų bazių ar turi suteikti asmenims priėjimą prie pačios duomenų bazės?*

3. A.: Asmeniui galima tik pateikti informaciją ir nebūtina leisti jam naudotis organizacijos duomenų baze.

4. K.: *Ar organizacija privalo restruktūrizuoti savo duomenų bazes, kad galėtų suteikti priėjimą?*

4. A.: Būtina suteikti priėjimą tik prie organizacijos turimos informacijos. Pats priėjimo užtikrinimo principas neįpareigoja išlaikyti, turėti, pertvarkyti ar restruktūrizuoti asmeninės informacijos kompiuterinių bylų.

5. K.: *Iš pateiktų atsakymų aišku, kad tam tikromis aplinkybėmis galima nesuteikti priėjimo. Kokiomis dar aplinkybėmis organizacija turi teisę neleisti asmenims prieiti prie jų asmeninės informacijos?*

5. A.: Tokios aplinkybės ribotos ir bet kokios neleidimo prieiti priežastys turi būti konkrečiai apibrėžtos. Organizacija gali atsisakyti suteikti priėjimą prie informacijos, jei ją atskleidus galėtų būti pažeista svarbių kitų visuomenės interesų apsauga, pvz.: nacionalinio saugumo, gynybos ar visuomenės saugumo. Be to, kai asmeninė informacija yra tvarkoma *vien tik* tyrimo ar statistikos tikslais, priėjimo galima nesuteikti. Kitos priėjimo neleidimo ar ribojimo priežastys yra tokios:

a) trukdymas vykdyti teisės aktus ar prižiūrėti jų vykdymą, įskaitant teisės pažeidimų prevenciją, tyrimą ar atskleidimą arba sąžiningo teismo proceso teisę;

b) prieštaravimas privačios veiklos motyvams, įskaitant teisinių ieškinių prevenciją, tyrimą ar atskleidimą arba sąžiningo teismo proceso teisę;

c) kito asmens (-ų) asmeninės informacijos atskleidimas, jei tokios informacijos negalima atskirti;

d) teisinių ar kitų profesinių lengvatų ar įsipareigojimų pažeidimas;

e) būsimų ar vykstančių derybų, pvz., dėl viešai kotiruojamų kompanijų pirkimo, būtino konfidencialumo pažeidimas;

f) pakenkimas darbuotojų apsaugos tyrimui ar skundų darbovietės administracijai nagrinėjimui;

g) pakenkimas konfidencialumui, kuris gali būti būtinas tam tikrais apibrėžtais laikotarpiais dėl darbuotojų pareigų perėmimo ir įmonių reorganizavimo; arba

h) pakenkimas konfidencialumui, kuris gali būti būtinas monitoringo (stebėsenos), inspektavimo ar kontrolės funkcijomis, susijusiomis su teisėta ekonomine ar finansine vadyba; arba

i) kitos aplinkybės, kuriomis priėjimo suteikimo sudėtingumas ar išlaidos būtų neproporcingai didelės arba būtų pažeistos kitų asmenų teisės ar interesai.

Organizacija, nutarusi taikyti išimtinį apribojimą, dažniausiai privalo įrodyti jo pagrįstumą. Kaip pažymėta pirmiau, asmenims turi būti nurodytos priėjimo nesuteikimo ar apribojimo priežastys ir nurodyti papildomi priėjimo reikalavimo būdai.

6. K.: *Ar gali organizacija imti mokestį priėjimo suteikimo išlaidoms padengti?*

6. A.: Taip. OECD vadove organizacijoms suteikiama teisė imti mokestį, jei jis nėra pernelyg didelis. Naudinga nustatyti mokestį siekiant apriboti per dažnus ar įkyrius reikalavimus.

Viešai prieinama informacija prekiaujančios organizacijos gali imti iš klientų mokestį už prieigos reikalavimus. Asmenys vietoj to gali bandyti prieiti prie savo informacijos per organizaciją, kuri iš pradžių tą informaciją sukaupė.

Negalima atsisakyti suteikti priėjimą dėl su išlaidomis susijusių priežasčių, jei asmuo pasisiūlo apmokėti išlaidas.

7. K.: *Ar organizacija privalo suteikti priėjimą prie asmeninės informacijos, gautos iš viešųjų archyvų?*

7. A.: Visų pirma reikia paaiškinti, kad viešieji archyvai yra bet kokio lygio Vyriausybinių agentūrų ar institucijų saugomi archyvai, kurie apskritai prieinami visuomenei. Tokiai informacijai nebūtina taikyti Priėjimo principo, jei ji nėra susijusi su kita asmenine informacija, išskyrus atvejus, kai nedideli kiekiai neviešųjų archyvų informacijos naudojami viešųjų archyvų informacijai indeksuoti ar organizuoti. Tačiau būtina laikytis atitinkamos jurisdikcijos nustatytų informacijos ieškojimo sąlygų. Kai viešųjų archyvų informacija yra apjungta su kita neviešųjų archyvų informacija (kitokia, nei nurodyta pirmiau), organizacija privalo suteikti priėjimą prie visos tokios informacijos, jei jis neribojamas dėl kitų leistinų išimtinių priežasčių.

8. K.: *Ar Priėjimo principą būtina taikyti viešai prieinamai asmeninei informacijai?*

8. A.: Kaip ir viešųjų archyvų informacijos atveju (žr. 7 FAQ), nebūtina suteikti priėjimo prie plačiajai visuomenei prieinamos informacijos, jei ji neapjungta su viešai neprieinama informacija.

9. K.: *Kaip gali organizacija apsiginti nuo dažnų ar įkyrių priėjimo reikalavimų?*

9. A.: Organizacija neprivalo reaguoti į tokius priėjimo reikalavimus. Dėl šių priežasčių organizacijos gali imti pagrįstą mokestį ir apriboti tenkinamų vieno asmens reikalavimų skaičių per tam tikrą laikotarpį. Nustatydama tokius apribojimus, organizacija turi įvertinti tokius veiksnius: informacijos atnaujinimo dažnumą, informacijos naudojimo paskirtį ir pobūdį.

10. K.: *Kaip organizacija gali apsiginti nuo nesąžiningų priėjimo reikalavimų?*

10. A.: Organizacija neprivalo suteikti priėjimo, jei jai pateikiama nepakankamai informacijos, kad ji galėtų patvirtinti reikalavimą pateikusio asmens tapatybę.

11. K.: *Ar yra nustatytas laikas, per kurį būtina atsakyti į priėjimo reikalavimus?*

11. A.: Taip, organizacijos turi atsakyti per pagrįstą laiko tarpą, ilgai nedelsdamos. Kaip nurodyta 1980 m. OECD Privatumo vadove, šio reikalavimo gali būti laikomasi įvairiais būdais. Pavyzdžiui, duomenų valdytojas, kuris teikia informaciją duomenų subjektams reguliariai, gali būti atleistas nuo įsipareigojimo iškart atsakyti į asmenų reikalavimus.

9 FAQ — Žmogiškieji ištekliai

1. K.: *Ar „saugaus uosto“ sistema taikoma perduodant iš ES į Jungtines Valstijas asmeninę informaciją, renkamą dėl darbo santykių?*

1. A.: Taip, jei ES kompanija perduoda asmeninę informaciją apie savo darbuotojus (buvusius ar esamus), kuri buvo surinkta įdarbinimo reikalams, „saugaus uosto“ sistemoje esančiai motininei įmonei, filialui ar kompanijos

dalimi nesančiam paslaugų teikėjui Jungtinėse Valstijose, tokiai informacijai galioja „saugaus uosto“ privilegijos. Tokiais atvejais informacija, prieš ją perduodant, renkama ir tvarkoma laikantis tos ES šalies, kurioje ji buvo surinkta, teisės aktų ir būtina laikytis visų tuose teisės aktuose numatytų jos perdavimo sąlygų ar apribojimų.

„Saugaus uosto“ principai galioja tik tuomet, kai yra perduodami ar prieinami asmenį identifikuojantys įrašai. Statistiniai pranešimai, sudaryti remiantis bendrais įdarbinimo duomenimis ir (arba) panaudojant anoniminius ar pseudoniminius duomenis, su privatumu nesietini.

2. K.: *Kaip tokiai informacijai taikomi Pranešimo ir Pasirinkimo principai?*

2. A.: JAV organizacija, gavusi informaciją apie darbuotojus iš ES „saugaus uosto“ sistemos, gali atskleisti ją trečiosioms šalims ir (arba) naudoti ją įvairiems tikslams tik laikydamasi Pranešimo ir Pasirinkimo principų. Pavyzdžiui, jei organizacija ketina panaudoti darbo santykių metu surinktą asmeninę informaciją su įdarbinimu nesusijusiais tikslais, pvz., rinkodaros pranešimuose, JAV organizacija prieš tai privalo suteikti susijusiems asmenims pasirinkimo galimybę, nebent jie jau būtų leidę naudoti informaciją tokiems tikslams. Be to, draudžiama atsižvelgiant į pasirinkimą apriboti įdarbinimo galimybes arba imtis kokių nors sankcijų prieš tokius darbuotojus.

Atkreiptinas dėmesys, kad tam tikromis plačiai taikomomis perdavimo iš kai kurių valstybių narių sąlygomis neleidžiama naudoti tokią informaciją kitais tikslais net perdavus ją už ES ribų ir tokias sąlygas būtina vykdyti.

Be to, darbdaviai turi pagrįstai stengtis vykdyti darbuotojų privatumo pageidavimus. Tai, pavyzdžiui, gali būti daroma apribojant priėjimą prie duomenų: kai kuriuos duomenis paverčiant anonimiškais, priskiriant jiems kodus ar pseudonimus, kai tikrieji vardai vadybos tikslams nebūtini.

Laikotarpiui, būtinam, kad nebūtų pakenkta teisėtiems organizacijos interesams, kai paaukštinama pareigose, skiriama į pareigas ar priimami kiti panašūs darbo santykių sprendimai, organizacija neprivalo pranešti ir suteikti pasirinkimą.

3. K.: *Kaip vykdomas Priėjimo principas?*

3. A.: FAQ dėl priėjimo nurodo priežastis, dėl kurių pateisinamas atsisakymas suteikti reikalaujamą priėjimą prie žmogiškųjų išteklių informacijos arba jo apribojimas. Žinoma, darbdaviai Europos Sąjungoje privalo laikytis vietinių teisės aktų ir užtikrinti, kad Europos Sąjungos darbuotojai turėtų priėjimą prie tokios informacijos, kaip reikalaujama jų šalių teisės aktuose, neatsižvelgiant į duomenų tvarkymo ir saugojimo vietą. „Saugaus uosto“ principai reikalauja, kad tokius duomenis tvarkanti organizacija Jungtinėse Valstijose bendradarbiautų suteikiant tokį priėjimą tiesiogiai arba per ES darbdavį.

4. K.: *Kaip pagal „saugaus uosto“ principus bus vykdoma darbuotojų duomenų priežiūra?*

4. A.: Jei informacija naudojama tik darbo santykiams, darbuotojo atžvilgiu už duomenis atsakinga lieka visų pirma ES kompanija. Tai reiškia, kad Europos darbuotojams pasiskundus dėl jų duomenų apsaugos teisių pažeidimų ir jiems nesant patenkintiems vidinio patikrinimo rezultatais, skundo nagrinėjimo ir apeliacijos procedūromis (arba bet kokiomis taikomomis skundų darbovietės administracijai procedūromis pagal sutartį su profsąjunga), tie skundai turi būti adresuoti valstybinei ar nacionalinei duomenų apsaugos ar darbo institucijai, kurios jurisdikcijai priklauso darbuotojo darbovietė. Tai pasakytina ir apie atvejus, kai įtariamas jų asmeninės informacijos tvarkymo pažeidimas įvyko Jungtinėse Valstijose, už jį atsako JAV organizacija, gavusi tą informaciją iš darbdavio, tačiau darbdaviui nepriklausančią, todėl įtariama, kad buvo pažeisti „saugaus uosto“ principai, o ne Direktyvą įgyvendinantys nacionaliniai teisės aktai. Tai yra veiksmingiausias būdas spręsti klausimus dėl dažnai vieni kitiems prieštaraujančių teisių ir įsipareigojimų, nustatytų vietiniais darbo teisės aktais, darbo sutartimis ir duomenų apsaugos teisės aktu.

„Saugaus uosto“ sistemai priklausanti JAV organizacija, naudojanti darbo santykiams iš Europos Sąjungos perduodamus ES žmogiškųjų išteklių duomenis, kuri nori, kad perduodant tokius duomenis būtų taikomi „saugaus uosto“ principai, privalo įsipareigoti bendradarbiauti su kompetentingomis ES institucijomis joms vykdant tyrimus ir laikytis jų konsultacijų. Sutarusios taip bendradarbiauti DAI informuos Europos

Komisiją ir Komercijos departamentą. Jei „saugaus uosto“ sistemai priklausanti JAV organizacija pageidauja perduoti žmogiškųjų išteklių informaciją iš valstybės narės, kur taip nebuvo sutarta su DAI, galioja 5 FAQ nuostatos.

10 FAQ — 17 straipsnis, sutartys

K.: *Ar būtina sudaryti sutartį, kai duomenys iš ES perduodami į JAV vien tvarkymo tikslais, o tvarkantysis priklauso „saugaus uosto“ sistemai?*

A.: Taip. Europos Sąjungoje duomenų valdytojai visuomet privalo sudaryti sutartį, jei duomenys perduodami vien tvarkyti — ar būtų tvarkoma ES, ar už jos ribų. Sutartis skirta duomenų valdytojo, t. y. asmens ar institucijos, kuri nustato tvarkymo tikslus bei būdus ir visiškai atsako prieš asmenis, kurių duomenis tvarko, interesams apsaugoti. Taigi sutartis apibūdina reikiamą tvarkymo operaciją ir priemones, būtinas duomenims apsaugoti.

„Saugaus uosto“ sistemai priklausanti JAV organizacija, kuri gauna iš ES asmeninės informacijos tik tvarkymo tikslais, neprivalo jai taikyti Principų, nes pagal ES teisines nuostatas (kurios gali būti griežtesnės už lygiaverčius „saugaus uosto“ principus) prieš asmenį atsakingu lieka ES duomenų valdytojas.

Kadangi „saugaus uosto“ dalyviai suteikia pakankamą apsaugą, sutarčių su „saugaus uosto“ dalyviais vien tik duomenų tvarkymo tikslais nereikia iš anksto patvirtinti (arba tokį patvirtinimą valstybės narės suteikia automatiškai). Tačiau sudarant sutartis su „saugaus uosto“ sistemai nepriklausančiais ar nesuteikiančiais pakankamos apsaugos gavėjais, tokias sutartis reikėtų iš anksto patvirtinti.

11 FAQ — Ginčų sprendimas ir vykdymo priežiūra

K.: *Kaip turi būti įgyvendinami Vykdymo priežiūros principo ginčų sprendimo reikalavimai ir kas daroma, jei organizacija nuolatos pažeidinėja Principus?*

A.: Vykdymo priežiūros principas nustato „saugaus uosto“ taisyklių vykdymo priežiūros reikalavimus. FAQ dėl tikrinimo (7 FAQ) nurodyta, kaip vykdyti Principo b punkto reikalavimus. Šiame 11 FAQ kalbama apie a ir c punktus, kuriais remiantis reikalingi nepriklausomi regreso teisės mechanizmai. Tokie mechanizmai gali būti įvairūs, tačiau jie privalo atitikti Vykdymo priežiūros principo reikalavimus. Organizacijos gali vykdyti reikalavimus taip: 1) vykdydamos kartu su privačiu sektoriumi sukurtas programas, į kurių taisykles įtraukti „saugaus uosto“ principai ir kuriuose yra veiksmingi vykdymo priežiūros mechanizmai, atitinkantys aprašytuosius Vykdymo priežiūros principe; 2) laikydamosi teisinių ar priežiūros institucijų, nagrinėjančių asmenų skundus ir sprendžiančių ginčus, reikalavimų; arba 3) įsipareigodamos bendradarbiauti su Europos Sąjungoje esančiomis duomenų apsaugos institucijomis arba jų įgaliotais atstovais. Šis sąrašas yra tik paaiškinamasis ir nebaigtinis. Privatus sektorius gali sukurti kitokius vykdymo priežiūros mechanizmus, bet jie privalo atitikti Vykdymo priežiūros principą ir FAQ reikalavimus. Prašome atsižvelgti į tai, kad Vykdymo priežiūros principo reikalavimai papildo Principų aprašymo įvado 3 pastraipos reikalavimus, ir kad pagal Federalinės prekybos komisijos akto 5 straipsnį ar panašų norminį aktą privalo būti numatytos savireguliacijos priemonės.

Regreso teisės mechanizmai

Pirmiausia vartotojai turėtų būti raginami teikti bet kokius galimus skundus pačioms organizacijoms, o tik vėliau pasinaudoti nepriklausomais regreso teisės mechanizmais. Tai, ar regreso teisės mechanizmas yra nepriklausomas, yra faktinis klausimas, į kurį galima atsakyti įvairiais būdais, pavyzdžiui, skaidria sudėtimi ir finansavimu arba profesine patirtimi. Kaip reikalauja Vykdymo priežiūros principas, asmenims skirti

regreso teisės mechanizmai turi būti lengvai prieinami ir galimi pasinaudoti. Ginčų sprendimo institucijos turi nagrinėti visus iš asmenų gautus skundus, nebent jie būtų akivaizdžiai nepagrįsti ar nerimti. Tai nedraudžia regreso teisės mechanizmą naudojančiai organizacijai nustatyti tinkamumo reikalavimų, tačiau tokie reikalavimai turi būti skaidrūs ir pagrįsti (pavyzdžiui, atmetant skundus, kuriems programa netaikoma arba jie skirti svarstyti kitur) ir negali sumažinti įsipareigojimo nagrinėti teisėtus skundus. Asmenims, pateikiantiems skundą regreso teisės mechanizmui, turi būti suteikta visa ir lengvai pasiekiama informacija apie ginčų sprendimo tvarką. Ši informacija turi apimti mechanizmo privatumo praktiką, atitinkančią „saugaus uosto“ principus ([1]). Turi būti sudarytos standartinės skundų formos, kurios palengvintų ginčų sprendimo procesą.

Teisės gynimo priemonės ir sankcijos

Ginčų sprendimo institucijos suteiktos bet kokios teisės gynimo priemonės turėtų užtikrinti, kad organizacija kiek įmanoma panaikintų ar ištaisytų reikalavimų nesilaikymo sukeltus padarinius, toliau tvarkytų informaciją laikydamasi Principų ir nebetvarkytų skundą parašiusio asmens duomenų. Sankcijos turi būti pakankamai griežtos, kad priverstų organizacijas laikytis įsipareigojimų. Įvairaus sunkumo nusižengimus ginčų sprendimo institucijos reikiamai įvertins taikydamos skirtingas griežtumo sankcijas. Sankcijose turi būti numatyta viešai paskelbti išvadas dėl reikalavimų nesilaikymo ir kai kuriais atvejais pareikalauti sunaikinti duomenis ([2]). Kitos sankcijos gali būti veiklos sustabdymas ir licencijos atėmimas, dėl reikalavimų nesilaikymo asmenims padarytos žalos atlyginimas ir draudžiamieji įsakymai. Privataus sektoriaus ginčų sprendimo institucijos ir savireguliacijos institucijos privalo pranešti apie „saugaus uosto“ sistemos organizacijų nuostatų nesilaikymą Vyriausybinei institucijai arba teismams, informuoti Komercijos departamentą (arba jo įgaliotą asmenį).

FPK veikla

FPK įsipareigojo pirmumo tvarka nagrinėti iš privatumo savireguliacijos institucijų, pvz., „BBBOnline“ ir „TRUSTe“, ir iš „saugaus uosto“ principų nesilaikymą įtariančių ES valstybių narių gautus pranešimus, kad nuspręstų, ar buvo pažeistas FPK akto 5 skirsnis, kuriuo komercijoje draudžiami nesąžiningi arba apgaulingi veiksmai ir metodai. Jei FPK nusprendžia, kad yra priežasčių manyti, jog 5 skirsnis buvo pažeistas, ji gali reikalauti sustabdyti administracinę veiklą, paklusti nutraukimo įsakymui, draudžiančiam vykdomą veiklą, paduoti skundą į federalinį apygardos teismą, o šiam priėmus palankų sprendimą jis gali išleisti tokio paties pobūdžio federalinio teismo įsakymą. FPK gali taikyti administracines nuobaudas už administracinio veiklos sustabdymo ir nutraukimo įsakymo nesilaikymą ir persekioti administracine arba baudžiamąja tvarka už federalinio teismo įsakymo nevykdymą. FPK informuos Komercijos departamentą apie visus tokius veiksmus, kurių ji imasi. Komercijos departamentas skatina kitas Vyriausybines institucijas informuoti apie galutinį tokių pranešimų sutvarkymą ir kitus nurodymus, nustatančius „saugaus uosto“ principų laikymąsi.

Nuolatinis reikalavimų nesilaikymas

Jei organizacija nuolatos pažeidinėja Principus, iš jos atimama teisė naudotis „saugaus uosto“ privilegijomis. Nuolatiniai pažeidinėjimai apibrėžiami kaip Komercijos departamentui (arba jo įgaliotam asmeniui) įsipareigojusios organizacijos atsisakymas paklusti bet kurios savireguliacijos ar Vyriausybinės institucijos galutiniam nutarimui arba tokia institucija nustato, kad organizacija taip dažnai pažeidinėja Principus, kad jos pasižadėjimas jų laikytis yra nepatikimas. Tokiais atvejais organizacija privalo nedelsdama informuoti Komercijos departamentą (arba jo įgaliotą asmenį) apie tokius faktus. To nepadarius gali būti baudžiama pagal Melagingų parodymų aktą (18 U.S.C. § 1001).

Departamentas (arba jo įgaliotas asmuo) „saugaus uosto“ principų įsipareigojusių laikytis organizacijų viešajame sąraše pažymės bet kokią informaciją apie nuolatinį pažeidinėjimą, gautą iš pačios organizacijos, savireguliacijos institucijos ar Vyriausybinės institucijos. Tačiau prieš trisdešimt (30) dienų praneš apie tai nusižengusiai organizacijai ir suteiks galimybę jai pasiaiškinti. Tokiu būdu iš Komercijos departamento (arba jo įgalioto asmens) turimo viešojo sąrašo bus aišku, kurios organizacijos turi teisę į „saugaus uosto“ privilegijas ir kurioms ta teisė atimta.

([1]) Ginčų sprendimo institucijos neprivalo atitikti Vykdymo priežiūros principo reikalavimų. Jos taip pat gali nukrypti nuo Principų, jei dėl to vykdant tam tiktas užduotis atsiranda prieštaraujančių vienas kitam įsipareigojimų arba aiškių įpareigojimų.

([2]) Ginčų sprendimo institucijos gali pasirinkti, kokiom aplinkybėm esant jos taikyti tokias sankcijas. Sprendžiant, ar reikėtų reikalauti panaikinti duomenis, reikia įvertinti duomenų ypatingumą ir tai, ar organizacija rinko, naudojo ar atskleidė informaciją akivaizdžiai nepaisydama Principų.

Jei organizacija teikia prašymą dalyvauti savireguliacijos institucijoje, kad galėtų vėl būti priimta į „saugaus uosto“ sistemą, tai privalo pateikti tai institucijai visą informaciją apie savo ankstesnį dalyvavimą „saugaus uosto“ sistemoje.

12 FAQ — Pasirinkimas — *Opt out* būdo pasirinkimo laikas

K.: *Ar Pasirinkimo principas apriboja asmens pasirinkimo laiko laisvę?*

A.: Plačiąja prasme Pasirinkimo principo paskirtis — užtikrinti, kad asmeninė informacija būtų naudojama ir atskleidžiama taip, kaip to tikisi ir pasirenka pats asmuo. Todėl asmuo bet kuriuo metu turi turėti galimybę pasinaudoti *opt out* būdu (ar pasirinkimu), ar jo asmeninė informacija bus naudojama tiesioginei rinkodarai. Tačiau organizacija turėtų pasilikti sau pakankamai laiko pasirinkimui įvykdyti. Organizacija taip pat gali reikalauti pakankamai informacijos, kad galėtų nustatyti *opt out* reikalaujančio asmens tapatybę. Jungtinėse Valstijose asmenys galėtų pasirinkti pasinaudodami centrine *opt out* programa, pvz., „Direct Marketing Association's Mail Preference Service“. Šioje programoje dalyvaujančios organizacijos reklamuoja galimybę ja pasinaudoti klientams, kurie nepageidauja gauti komercinės informacijos. Bet kuriuo atveju asmeniui turi būti suteiktas lengvai prieinamas ir naudojamas pasirinkimo mechanizmas.

Panašiai organizacija gali naudoti informaciją tam tikrais tiesioginės rinkodaros tikslais, kai suteikti asmeniui *opt out* galimybę iki panaudojant informaciją neįmanoma, jei organizacija suteikia asmeniui galimybę iškart (o pareikalavus — bet kuriuo metu) atsisakyti (nemokamai) gauti kitus tiesioginės rinkodaros pranešimus ir įvykdo asmens pageidavimą.

13 FAQ — Kelionių informacija

K.: *Kada ne ES esančioms organizacijoms galima perduoti informaciją apie oro linijų keleivių bilietų rezervaciją ir kitą informaciją apie keliones, pvz., apie dažnai oro linijų paslaugomis besinaudojančius asmenis, viešbučių rezervaciją ar ypatingus aptarnavimo poreikius (religinius reikalavimus atitinkantį maistą ar fizinę pagalbą)?*

A.: Tokia informacija gali būti perduodama keliais atvejais. Pagal Direktyvos 26 straipsnį asmens duomenys „trečiajai šaliai, kuri neužtikrina pakankamo apsaugos lygio, nurodyto 25 straipsnio 2 dalyje“ gali būti perduodami tik tuo atveju, kai 1) būtina suteikti kliento reikalaujamas paslaugas arba vykdyti sutarties, pvz., „dažnai skraidančiojo“ sutarties, sąlygas; arba 2) tam vienareikšmiai pritarė klientas. „Saugaus uosto“ sistemai priklausančios JAV organizacijos suteikia pakankamą apsaugą asmens duomenims ir todėl gali gauti iš ES perduodamus duomenis nesilaikydamos tų sąlygų arba kitų Direktyvos 26 straipsnyje nurodytų sąlygų. Kadangi „saugiame uoste“ numatytos specialios taisyklės ypatingai informacijai apsaugoti, tokią informaciją (kurią gali reikėti surinkti todėl, kad klientui reikia fizinės pagalbos) galima siųsti „saugaus uosto“ dalyviams kartu su kita informacija. Informaciją perduodanti organizacija visuomet privalo laikytis ES valstybės narės, kurioje ji veikia, teisės aktų, kuriuose, *inter alia*, gali būti nustatytos specialios ypatingos informacijos tvarkymo sąlygos.

14 FAQ — Farmaciniai ir medicinos produktai

1. K.: *Ar galioja valstybių narių teisės aktai ar „saugaus uosto“ principai tuomet, kai surinkti asmens duomenys perduodami iš ES į Jungtines Valstijas farmaciniams tyrimams ir (arba) kitais tikslais?*

1. A.: Valstybės narės teisės aktai galioja renkant asmens duomenis ir juos tvarkant iki perduodant į Jungtines Valstijas. Perdavus duomenis į Jungtines Valstijas galioja „saugaus uosto“ principai. Farmaciniams tyrimams ir kitais tikslais naudojami duomenys gali būti pakeisti taip, kad nebūtų galima nustatyti duomenų subjekto tapatybės.

2. K.: *Specialiųjų medicinos ar farmacinių tyrimų studijų metu gauti asmens duomenys dažnai yra labai svarbūs būsimiems moksliniams tyrimams. Jei tokie surinkti asmens duomenys perduodami į „saugaus uosto“ JAV organizaciją, ar gali organizacija tokius duomenis naudoti naujiems moksliniams tyrimams?*

2. A.: Taip, jei iš pradžių buvo atitinkamai pranešta ir leista pasirinkti. Pranešime turi būti pateikta informacija apie bet kokį konkretų būsimą duomenų panaudojimą, pvz., periodinius atsiliepimus, susijusias studijas ar rinkodarą. Suprantama, kad neįmanoma nurodyti visko, kam ateityje gali būti panaudota informacija, nes naujos galimybės panaudoti tyrimams gali susidaryti dėl naujo pirminių duomenų supratimo, naujų medicinos atradimų bei pažangos ir visuomenės sveikatos bei kontrolės plėtros. Todėl pranešime turi būti paaiškinta, kad asmens duomenys gali būti panaudoti būsimiems medicinos ir farmacijos tyrimams, kurių neįmanoma numatyti. Jei duomenis ketinama panaudoti tikslams, kurie neatitinka pirminių bendrųjų tyrimo tikslų ar tų kuriems asmuo vėliau davė sutikimą, būtina gauti naują sutikimą.

3. K.: *Kas atsitinka su asmens duomenimis, jei dalyvis savanoriškai arba reikalaujant rėmėjui atsisako toliau dalyvauti klinikiniuose tyrimuose?*

3. A.: Bet kuriuo metu dalyviai gali nuspręsti arba būti paprašyti nebedalyvauti klinikiniuose tyrimuose. Visi iki to laiko surinkti duomenys ir kiti klinikinio tyrimo metu gauti duomenys gali būti tvarkomi, jei apie tai buvo pranešta dalyviui tuomet, kai jis (ji) sutiko juose dalyvauti.

4. K.: *Farmacinius ir medicinos įrenginius gaminančios kompanijos ES vykdytų klinikinių tyrimų metu gautus asmeninius duomenis gali suteikti tvarkytojams Jungtinėse Valstijose priežiūros ir kontrolės tikslais. Ar panašius duomenis galima perduoti ne tvarkytojams, o kitiems subjektams, pvz., kompanijos ir kitiems tyrėjams?*

4. A.: Taip, laikantis Pranešimo ir Pasirinkimo principų.

5. K.: *Tam, kad būtų užtikrintas daugelio klinikinių tyrimų objektyvumas, dalyviams, o dažnai ir tyrėjams, negalima suteikti priėjimo prie informacijos apie kiekvieno dalyvio gydymą. Taip padarius, kiltų pavojus, kad tyrimų studijos ir jos rezultatai taptų nebepatikimi. Ar tokių klinikinių tyrimų (vadinamų „aklųjų“ studijų) dalyviai tyrimo metu privalo gauti priėjimą prie duomenų apie jų gydymą?*

5. A.: Ne, tokio priėjimo dalyviui suteikti neprivalu, jei šis apribojimas buvo paaiškintas dalyviui pradedant tyrimą ir jei atskleidus tokią informaciją kiltų pavojus pakenkti tyrimui. Sutikimas dalyvauti tyrime tokiomis sąlygomis yra pagrįstas priėjimo teisės atsisakymu. Jei dalyviai pageidauja prieiti prie savo duomenų, tai galima padaryti tik pabaigus tyrimą ir išanalizavus rezultatus. Iš pradžių jie turi to prašyti tyrimo metu juos gydžiusio gydytojo ar kito sveikatos priežiūros teikėjo arba po to — rėmusiosios kompanijos.

6. K.: *Ar farmacijos bei medicinos įrenginius gaminanti kompanija privalo taikyti „saugaus uosto“ principus dėl pranešimų, pasirinkimo, tolimesnio perdavimo ir priėjimo jai vykdant savo gaminių saugos ir veiksmingumo monitoringo (stebėsenos) veiklą, įskaitant pranešimus apie nepalankius atvejus ir vartojančių tam tikrus medikamentus ar naudojančių medicinos įtaisus (pvz., širdies stimuliatorius) pacientų (subjektų) stebėjimą?*

6. A.: Ne, išskyrus tuos atvejus, kai Principai prieštarauja teisės normų reikalavimams. Tai pasakytina apie sveikatos priežiūros teikėjų farmacijos ir medicinos prietaisų gamybos bendrovėms teikiamus pranešimus bei šių bendrovių pranešimus Vyriausybinėms institucijoms, kaip antai Maisto ir vaistų valdybai.

7. K.: *Dažniausiai pagrindinis tyrėjas, tik gavęs tyrimų duomenis, iš karto juos užkoduoja unikaliu kodu, kad nebūtų atskleista atskirų duomenų subjektų tapatybė. Tokį tyrimą remiančios farmacijos kompanijos kodo rakto negauna. Unikalų kodo raktą turi tik tyrėjas, kad tam tikromis aplinkybėmis galėtų nustatyti tyrimų subjekto tapatybę (pvz., jei reikia tęstinės medicininės priežiūros). Ar tokiam užkoduotų asmens duomenų perdavimui iš ES į Jungtines Valstijas taikomi „saugaus uosto“ principai?*

7. A.: Ne. Tokiam asmens duomenų perdavimui netaikytini Principai.

15 FAQ — Viešasis archyvas ir viešai prieinama informacija

K.: *Ar viešųjų archyvų informacijai arba viešai prieinamai informacijai būtina taikyti Pranešimo, Pasirinkimo ir Tolimesnio perdavimo principus?*

A.: Pranešimo, Pasirinkimo ir Tolimesnio perdavimo principų viešųjų archyvų informacijai taikyti nebūtina, jei ji nėra sujungta su neviešųjų archyvų informacija ir laikomasi atitinkamos jurisdikcijos nustatytų jos ieškojimo sąlygų.

Taip pat nebūtina taikyti Pranešimo, Pasirinkimo ir Tolimesnio perdavimo principų viešai prieinamai informacijai, nebent siuntėjas iš Europos nurodo, kad tokiai informacijai taikomi apribojimai, dėl kurių organizacija privalo taikyti Principus. Organizacijos neatsako už tai, kaip tokią informaciją panaudos gaunantieji ją iš paskelbtos medžiagos.

Jei nustatoma, kad organizacija priešingai Principams sąmoningai viešai paskelbė asmeninę informaciją ir kad ji arba kiti gali turėti iš to naudos, ji netenka teisės naudotis „saugaus uosto“ privilegijomis.

III PRIEDAS

„Saugaus uosto“ reikalavimų vykdymo apžvalga

Federalinė ir valstybinė nesąžiningos ir apgaulingos praktikos jurisdikcija ir privatumas

Šiame memorandume apibrėžiama Federalinės prekybos komisijos (FPK) jurisdikcija pagal Federalinės prekybos komisijos akto (15 U.S.C. §§ 41–58 su pakeitimais) 5 skirsnį imtis veiksmų prieš nesugebančius apsaugoti asmeninės informacijos privatumo pagal savo reikalavimus ir (arba) įsipareigojimus tai daryti. Jame taip pat nustatytos tos jurisdikcijos išimtys ir galimybė kitoms federalinėms ir valstybinėms institucijoms imtis veiksmų, kai FPK neturi tam oficialių įgaliojimų ([1]).

FPK jurisdikcija dėl nesąžiningos ir apgaulingos praktikos

Federalinės prekybos komisijos akto 5 skirsnyje nustatyta, kad „komercijoje naudojami ar jai įtakos turintys nesąžiningi ar apgaulingi veiksmai ar metodai“ yra neteisėti (15 U.S.C. § 45(a)(1)). 5 skirsnis suteikia FPK neribotus įgaliojimus užkirsti kelią tokiems veiksmams ir metodams (15 U.S.C. § 45(a)(2)). Todėl FPK, atlikusi oficialų nagrinėjimą, gali išleisti „sustabdymo ir nutraukimo“ įsakymą, skirtą teisę pažeidžiantiems veiksmams sustabdyti (15 U.S.C. § 45(b)). Jei tai atitiktų visuomenės interesus, FPK taip pat gali reikalauti laikino suvaržymo arba laikinojo ar nuolatinio uždraudimo JAV apygardos teisme (15 U.S.C. § 53(b)). Tuomet, kai nesąžiningi bei apgaulingi veiksmai ar metodai yra giliai įsišaknijęs, arba jau išleistas „sustabdymo ir nutraukimo“ įsakymas tuo klausimu, FPK gali paskelbti administracinį sprendimą, ribojantį atitinkamus veiksmus ar metodus (15 U.S.C. § 57(a)).

Nesilaikantieji FPK įsakymo baudžiami 11 000 JAV dolerių dydžio administracine bauda, o kiekviena papildoma diena tęsiant šį pažeidimą laikoma atskiru teisės pažeidimu ([2]) (15 U.S.C. § 45(1)). Lygiai taip pat kiekvienas, kuris žinodamas FPK sprendimą, jį pažeidžia, už kiekvieną pažeidimą baudžiamas 11 000 JAV dolerių dydžio bauda (15 U.S.C. § 45(m)). Vykdymo priežiūros veiksmus atlieka Teisingumo departamentas arba jam pavedus – FPK (15 U.S.C. § 56).

FPK jurisdikcija ir privatumas

Vykdydama 5 skirsnyje jai suteiktus oficialius įgaliojimus FPK nustato, kad klaidingas informavimas apie tai, kodėl informacija renkama iš klientų ar kaip ji bus naudojama, laikomas apgaulinga veika ([3]). Pavyzdžiui, 1998 m. FPK pateikė skundą prieš „GeoCities“ už tai, kad pastaroji negavusi išankstinio sutikimo atskleidė savo interneto svetainėje sukauptą informaciją trečiosioms šalims prekybai per tarpininkus vykdyti, o pati teigė priešingai ([4]). FPK personalas taip pat pareiškė, kad asmeninės informacijos rinkimas iš vaikų ir tokios informacijos pardavimas ir atskleidimas be tėvų sutikimo greičiausiai gali būti traktuojamas kaip nesąžiningos veikos ([5]).

([1]) Mes čia nenagrinėjame visų įvairių federalinių statutų, kurie taikytini tam tikriems privatumo reikalams, ar taikytinų valstybinių statutų ir bendrosios teisės. Federaliniu lygiu asmeninės informacijos rinkimą ir panaudojimą komerciniais tikslais reguliuoja tokie statutai: Kabelinių komunikacijų politikos aktas (47 U.S.C. § 551), Vairuotojų privatumo apsaugos aktas (18 U.S.C. § 2721), Elektroninių komunikacijų privatumo aktas (18 U.S.C. § 2701 *et seq.*), Elektroninio lėšų perdavimo aktas (15 U.S.C. §§ 1693, 1693m), Sąžiningo kreditinių ataskaitų sudarymo aktas (15 U.S.C. § 1681 *et seq.*), Finansinio privatumo teisės aktas (12 U.S.C. § 3401 *et seq.*), Telefono vartotojų apsaugos aktas (47 U.S.C. § 227), Vaizdo privatumo apsaugos aktas (18 U.S.C. § 2710) ir kiti. Daugelis valstijų turi analogiškus šių sričių teisės aktus. Žr., pvz., Mass. Gen. Laws ch. 167B, § 16 (draudžiantis finansinėms institucijoms atskleisti klientų finansinius duomenis trečiajai šaliai be kliento sutikimo ar teisinio proceso vykdytojų leidimo), Niujorko visuomenės sveikatos įstatymo § 17 (ribojantis medicininių ar psichinės sveikatos įrašų panaudojimą bei atskleidimą ir suteikiantis pacientams teisę juos gauti).

([2]) Tokiame procese Jungtinių Valstijų apygardos teismas taip pat gali paskelbti privalomąjį ir nešališką atleidimą nuo prievolės, reikalingą FPK įsakymui vykdyti (15 U.S.C. § 45(1)).

([3]) „Apgaulinga veika“ apibrėžiamas kaip pateikimas, neveikimas ar veiksmas, kuris galėtų iš esmės suklaidinti supratingus vartotojus.

([4]) Žr.: www.ftc.gov/opa/1998/9808/geocitie.htm.

([5]) Žr. personalo raštą Žiniasklaidos švietimo centrui, www.ftc.gov/os/1997/9707/cenmed.htm. Be to, 1998 m. Vaikų interaktyviojo (*on-line*) privatumo apsaugos aktas suteikia FPK specialius teisinius įgaliojimus prižiūrėti, kaip asmeninę informaciją iš vaikų renka interneto svetainės ir interaktyviųjų paslaugų teikėjai (žr. 15 U.S.C. §§ 6501–6506). Šiuo aktu reikalaujama, kad interaktyviųjų paslaugų teikėjai prieš rinkdami, naudodami ar atskleisdami iš vaikų gautą asmeninę informaciją privalo apie tai pranešti tėvams ir gauti iš jų galimą patikrinti sutikimą (*id.*, § 6502(b)). Šis aktas taip pat suteikia tėvams teisę prieiti prie tos informacijos ir uždrausti toliau ją naudoti (*id.*).

FPK pirmininkas Pitofskis savo laiške Europos Komisijos generaliniam direktoriui Johnui Moggui nurodė FPK oficialių įgaliojimų apribojimus ginti privatumą tuomet, kai nebuvo klaidinama (arba buvo nepranešama apskritai) dėl surinktos informacijos panaudojimo (FPK pirmininko Pitofskio laiškas Johnui Moggui (1998 m. rugsėjo 23 d.)). Tačiau bedrovės, norinčios pasinaudoti siūlomu „saugiu uostu“ turės patvirtinti, kad jos saugos surenkamą informaciją pagal nurodytą vadovą. Taigi kai bendrovė patvirtina, kad ji gins informacijos privatumą, o po to nesugebės to padaryti, tai bus laikoma klaidinimu ir „apgaulinga veika“ pagal 5 skirsnio nuostatas.

Nors FPK jurisdikcija aprėpia „komercijoje naudojamus arba jai įtakos turinčius“ nesąžiningus ar apgaulingus veiksmus ar metodus, FPK neturi jurisdikcijos dėl asmeninės informacijos rinkimo ir naudojimo nekomerciniais tikslais, pvz., renkant lėšas labdarai (žr. Pistofskio laišką, p. 3). Tačiau jurisdikcija atsiranda panaudojus asmeninę informaciją bet kokiai komercinei operacijai. Taigi, pvz., darbdaviui pardavus asmeninę informaciją apie jo darbuotojus tiesioginės rinkodaros atstovams, ta operacija patenka į 5 skirsnio taikymo sritį.

5 skirsnio išimtys

5 skirsnyje numatytos FPK oficialių įgaliojimų dėl nesąžiningų ar apgaulingų veiksmų ir metodų išimtys taikomos:

— finansinėms institucijoms, įskaitant taupomuosius bei kredito bankus ir kredito unijas,

— telekomunikacijų ir pervežimų tarp valstijų teikėjams,

— oro vežėjams ir

— maisto produktų paruošimo ir galvijų paskirstymo valdytojams.

(Žr. 15 U.S.C. § 45(a)(2)). Toliau aptarsime kiekvieną išimtį ir kontrolės instituciją, kuri gali pavaduoti FPK.

Finansinės institucijos ([1])

Pirmoji išimtis taikoma „bankams, taupomosioms ir kredito institucijoms, nurodytoms 18 skirsnio f punkto 3 papunktyje (15 U.S.C. § 57a(f)(3))“ ir „Federalinėms kredito sąjungoms, nurodytoms 18 skirsnio f punkto 4 papunktyje (15 U.S.C. § 57a(f)(4))“ ([2]). Šioms finansinėms institucijoms galioja Federalinės rezervo valdybos, Taupymo priežiūros biuro ([3]) ir Nacionalinės kredito sąjungos administracijos valdybos paskelbti nuostatai (žr. 15 U.S.C. § 57a(f)). Šioms priežiūros institucijoms nurodyta parengti teisės aktus, būtinus nesąžiningų ir apgaulingų veiksmų prevencijai šiose finansinėse institucijose ([4]), ir įkurti atskirą padalinį klientų skundams nagrinėti (15 U.S.C. § 57a(f)(1)). Vykdymo priežiūros oficialūs įgaliojimai bankams ir taupomiesiems bei kredito bankams nustatyti Federalinio indėlių draudimo akto (12 U.S.C. § 1818) 8 skirsnyje, o Federalinėms kredito unijoms (15 U.S.C. § 57a(f)(2)–(4)) Federalinės kredito sąjungos akto 120 ir 206 skirsniuose.

Nors draudimo verslas nėra konkrečiai įtrauktas į 5 skirsnio išimčių sąrašą, McCarrano-Fergusono aktu (15 U.S.C. § 1011 *et seq.*) reglamentuoti draudimo verslą dažniausiai paliekama atskiroms valstijoms ([5]). Be to, pagal

([1]) 1999 m. lapkričio 12 d. Prezidentas Klintonas pasirašė įstatymą *Gramm-Leach-Bliley* aktą (Pub. L. 106–102, kodifikuotas kaip 15 U.S.C. § 6801 *et seq.*). Šis aktas apriboja finansinių institucijų galimybes atskleisti asmeninę informaciją apie jų klientus. Aktu reikalaujama, kad finansinės institucijos, *inter alia*, informuotų visus klientus apie savo privatumo taisykles ir praktiką dėl asmeninės informacijos dalijimosi su savo padaliniais ir atskiro kapitalo partneriais. Aktas suteikia oficialius įgaliojimus FPK, Federalinėms bankininkystės institucijoms ir kitoms valdžios institucijoms paskelbti nuostatus, skirtus ginti privatumą pagal įstatymą. Institucijos paskelbė šiam tikslui siūlomas taisykles.

([2]) Pagal savo nuostatas ši išimtis netaikoma vertybinių popierių sektoriui. Todėl brokeriams, platintojams ir kitiems vertybinių popierių sektoriaus subjektams kartu taikoma Vertybinių popierių ir biržos komisijos ir FPK jurisdikcija dėl nesąžiningų ar apgaulingų veikų ir metodų.

([3]) 5 skirsnio išimtis iš pradžių buvo skirta Federalinio vidaus paskolų banko valdybai, kuri buvo panaikinta 1989 m. Finansinių institucijų reformos, atkūrimo ir vykdymo aktu. Jos funkcijos buvo perduotos Taupymo priežiūros biurui ir Atsiskaitymo kreditų korporacijai, Federalinei indėlių draudimo korporacijai ir Gyvenamųjų namų statybos finansavimo valdybai.

([4]) Nors finansinės institucijos išbrauktos iš FPK jurisdikcijos, 5 skirsnis taip pat nustato, kad FPK paskelbus sprendimą dėl nesąžiningų ar apgaulingų veiksmų ir metodų, finansinės priežiūros valdybos turi per 60 dienų priimti atitinkamus teisės aktus (žr. 15 U.S.C. § 57a(f)(1)).

([5]) „Draudimo ir kiekvieno juo užsiimančio asmens verslui galioja keleto valstijų teisės aktai, susiję su tokio verslo reglamentavimu ar apmokestinimu“ (15 U.S.C. § 1012(a)).

McCarrano-Fergusono akto 2 skirsnio b punktą, nė vienas federalinis teisės aktas neanuliuos, nesusilpnins ir nebus viršesnis už valstijų teisės aktą „nebent toks aktas yra konkrečiai skirtas draudimo verslui“ (15 U.S.C. § 1012(b)). Tačiau FPK akto nuostatos taikomos toms draudimo pramonės sritims, kurių nereglamentuoja valstijų teisės aktai (*id*.). Taip pat reikia pažymėti, kad McCarrano-Fergusono aktas palieka pirmenybę valstijoms tik „draudimo versle“. Todėl FPK jurisdikcija dėl draudimo bendrovių nesąžiningų ar apgaulingų veiksmų išlieka, kai jos neužsiima draudimo verslu. Taip galėtų būti tuomet, kai draudikai parduoda asmeninę informaciją apie jų polisų turėtojus ne draudimo produktų tiesioginės rinkodaros atstovams ([1]).

Visuomeniniai vežėjai

Antroji 5 skirsnio išimtis taikoma tiems visuomeniniams vežėjams, kuriems „taikomi komerciją reglamentuojantys aktai“ (15 U.S.C. § 45 (a)(2)). Šiuo atveju „komerciją reglamentuojantys teisės aktai“ apima Jungtinių Valstijų Kodekso 49 skyriaus IV poskyrį ir 1934 m. Komunikacijų aktą (47 U.S.C. § 151 *et seq*.) (Komunikacijų aktas) (žr. 15 U.S.C. § 44).

49 U.S.C. IV poskyris (Pervežimai tarp valstijų) taikomas geležinkelio, motorinių transporto priemonių, vandens transporto vežėjams, brokeriams, krovinių ekspeditoriams ir vamzdynų vežėjams (49 U.S.C. § 10101 *et seq*.). Šiuos įvairius visuomeninius vežėjus reguliuoja Antžeminio transporto valdyba – nepriklausoma Transporto departamento institucija (49 U.S.C. §§ 10501, 13501 ir 15301). Visais atvejais vežėjui draudžiama atskleisti informaciją apie jo krovinio pobūdį, paskirties vietą ir kitus aspektus, kuri gali būti panaudota siuntėjo nenaudai (žr. 49 U.S.C. §§ 11904, 14908 ir 16103). Atkreipiame dėmesį, kad šios nuostatos taikomos informacijai apie siuntėjo krovinį ir todėl neatrodo taikytinos asmeninei informacijai apie siuntėją, kuri nėra susijusi su atitinkama siunta.

Komunikacijų aktas nurodo Federalinės komunikacijų komisijos (FKK) nuostatus dėl „komercijos tarp valstijų ir su užsieniu bendraujant laidinėmis ryšio priemonėmis ir radiju“ (žr. 47 U.S.C. §§ 151 ir 152). Be telekomunikacijų kompanijų, priskiriamų visuomeniniams ryšio paslaugų teikėjams, Komunikacijų aktas taip pat galioja televizijos ir radijo transliacijų kompanijoms, kabelinių paslaugų teikėjams, kurie nėra visuomeniniai ryšio paslaugų teikėjai. Pastarosioms kompanijoms netaikoma FPK akto 5 skirsnio išimtis. Taigi FPK turi jurisdikciją tirti, ar tokios kompanijos neužsiima nesąžininga ir apgaulinga veikla, tuo tarpu FKK turi konkuruojančią jurisdikciją vykdyti savo nepriklausomus įgaliojimus šioje srityje, kaip aprašyta toliau.

Pagal Komunikacijų aktą „kiekvienas telekomunikacijų paslaugų teikėjas“, įskaitant vietines telefono stotis, privalo saugoti klientui priklausančios informacijos privatumą ([2]) (47 U.S.C. § 222(a)). Be šių bendrųjų privatumo apsaugos įgaliojimų, Komunikacijų aktas pakeistas 1984 m. Kabelinių komunikacijų politikos aktu (Kabelinio ryšio aktu) (47 U.S.C. § 551 *et seq*.), specialiai įpareigojant kabelinių paslaugų operatorius saugoti „asmenį identifikuojančią informaciją“ apie kabelinių paslaugų abonentus (47 U.S.C. § 521) ([3]). Kabelinio ryšio aktas riboja kabelinių paslaugų operatorių galimybes rinkti asmeninę informaciją ir reikalauja, kad kabelinių paslaugų operatorius informuotų abonentą apie surinktos informacijos pobūdį ir apie tai, kaip ta informacija bus panaudota. Kabelinio ryšio aktas suteikia abonentams teisę prieiti prie informacijos apie juos ir reikalauja, kad kabelinių paslaugų operatoriai panaikintų tą informaciją, kai ji tampa nebereikalinga.

Komunikacijų aktas suteikia FKK teisę prižiūrėti, kaip vykdomos šios dvi privatumo nuostatos savo iniciatyva arba atsiliepiant į nusiskundimus iš išorės ([4]) (47 U.S.C. §§ 205, 403; *id*. § 208). Jei FKK nustato, kad telekomunikacijų paslaugų teikėjas (įskaitant kabelinių paslaugų operatorius) pažeidė 222 skirsnio arba 551 skirsnio privatumo nuostatas, yra trys pagrindiniai veikimo būdai, kuriais ji gali pasinaudoti. Pirma, Komisija, išnagrinėjusi ir nustačiusi

---

([1]) FPK taikė jurisdikciją draudimo bendrovėms dėl įvairių dalykų. Vienu atveju FPK ėmėsi veiksmų prieš firmą, kuri apgaulingai reklamavosi valstijoje, kurioje verstis neturėjo licencijos. FPK jurisdikcija buvo patvirtinta remiantis tuo, kad nebuvo veiksmingų valstijos teisės aktų, nes firma iš esmės buvo nepasiekiama valstijai. Žr. FPK prieš Keliautojų sveikatos asociaciją, 362 U.S. 293 (1960 m.).

17 valstijų priėmė pavyzdinį „Draudimo informacijos ir privatumo apsaugos aktą“, kurį parengė Nacionalinė draudimo įgaliotinių asociacija (NDĮA). Šiame akte išdėstytos nuostatos dėl pranešimo, naudojimo, atskleidimo ir priėjimo. Be to, beveik visos valstijos priėmė NDĮA pavyzdinį „Nesąžiningų draudimo veiksmų aktą“, kuris skirtas konkretiems nesąžiningiems veiksmams draudimo versle.

([2]) Terminas „kliento nuosava tinkle esanti informacija“ reiškia informaciją, susijusią su kliento „telekomunikacijų paslaugų kiekiu, technine konfigūracija, rūšimi, paskirtimi ir panaudojimo apimtimi“ ir informaciją apie sąskaitas už telefono paslaugas. 47 U.S.C. § 222(f)(1). Tačiau šis terminas neaprėpia abonentų sąrašų informacijos (*id*.).

([3]) Šis teisės aktas aiškiai neapibrėžia „asmenį identifikuojančios informacijos“.

([4]) Šie oficialūs įgaliojimai aprėpia kompensacijos teisę už privatumo pažeidimus pagal Komunikacijų akto 222 skirsnį arba, jei tai kabelinių paslaugų abonentai, pagal to akto pataisos, padarytos Kabelinio ryšio aktu, 551 skirsnį. Taip pat žr. 47 U.S.C. § 551(f)(3) (civilinis ieškinys federaliniam apygardos teismui yra neišimtinė teisės gynimo priemonė, siūloma „kartu su bet kokiomis kitomis teisėtomis teisių gynimo priemonėmis, kuriomis gali pasinaudoti kabelinių paslaugų abonentas“).

pažeidimą, gali nurodyti teikėjui padengti *piniginius nuostolius* [1] (47 U.S.C. § 209). Antra, FKK gali įsakyti teikėjui *sustabdyti ir nutraukti* pažeidžiamuosius veiksmus ar neveikimą (47 U.S.C. § 205(a)). Trečia, Komisija dar gali įsakyti pažeidėjui „*vykdyti ir laikytis (bet kokių) nuostatų ar praktikos*“, kurias jai gali nurodyti FKK (*id.*).

Fiziniai asmenys, manantys, kad telekomunikacijų paslaugų teikėjas ar kabelinių paslaugų operatorius pažeidė atitinkamas Ryšių akto ar Kabelinio ryšio akto nuostatas, gali pateikti skundą FKK arba pateikti ieškinį federaliniam apygardos teismui (47 U.S.C. § 207). Ieškovui, laimėjusiam federalinio teismo procesą prieš telekomunikacijų paslaugų teikėją dėl nesugebėjimo apsaugoti kliento nuosavos informacijos pagal Komunikacijų akto platesnės apimties 222 skirsnį, gali būti priteista atlyginti patirtą žalą ir apmokėti išlaidas advokatui (47 U.S.C. § 206). Bylą dėl privatumo pažeidimo pagal Kabelinio ryšio akto kabeliniam ryšiui skirtą 551 skirsnį, pralaimėjus ieškovui, gali būti priteista ne tik atlyginti patirtą žalą ir išlaidas advokatui, bet ir paskirtas drausminis žalos atlyginimas ir padengtos pagrįstos bylinėjimosi išlaidos (47 U.S.C. § 551(f)).

FKK patvirtino išsamias 222 skirsnio vykdymo taisykles (žr. 47 CFR 64.2001–2009). Šios taisyklės nustato konkrečias apsaugos priemones, skirtas apsaugoti nuo neleistino priėjimo prie asmeninės kliento informacijos tinkle. Taisyklės reikalauja, kad telekomunikacijų paslaugų teikėjai:

— sukurtų ir įdiegtų programinės įrangos sistemas, kurios pažymėtų, ar klientas yra informuotas (patvirtinęs sutikimą), kai klientui suteiktų (-inų) paslaugų įrašai pirmą kartą pasirodo ekrane,

— turėtų elektroninį „audito seklį“, kuris leistų kontroliuoti priėjimą prie kliento sąskaitos, įskaitant tai kada kliento registras buvo atidarytas, kas tai padarė ir dėl kokios priežasties,

— mokytų savo personalą naudoti asmeninę klientų informaciją tinkle tik gavus sutikimą ir taikant reikiamas drausmines priemones,

— sukurti priežiūros patikrinimų tvarką, kuri užtikrintų reikalavimų laikymąsi vykdant prekybos eksportą, ir

— kasmet FKK patvirtintų apie šių taisyklių laikymąsi.

Oro vežėjai

JAV ir užsienio oro vežėjams, kuriems galioja 1958 m. Federalinis aviacijos aktas, taip pat taikoma FPK akto 5 skirsnio išimtis (žr. 15 U.S.C. § 45(a)(2)). Išimtis aprėpia visus, kurie užsiima krovinių, keleivių arba pašto gabenimu orlaiviais tarp valstijų ar tarptautiniais maršrutais (žr. 49 U.S.C. § 40102). Oro vežėjai priklauso Transporto departamento jurisdikcijai. Todėl Transporto ministras turi oficialius įgaliojimus imtis veiksmų „užkertančių kelią nesąžiningiems, apgaulingiems, savanaudiškiems ar antikonkurenciniams veiksmams oro transporto srityje“ (49 U.S.C. § 40101(a)(9)). Jei visuomenės interesai reikalauja, transporto ministras gali tirti, ar JAV arba užsienio oro vežėjas arba bilietų agentūra užsiima nesąžininga ar apgaulinga veikla (49 U.S.C. § 41712). Po nagrinėjimo Transporto ministras gali išleisti įsakymą nelegaliai veiklai sustabdyti (*id.*). Kiek mums žinoma, Transporto ministras nėra naudojęs šių įgaliojimų asmeninės informacijos apie oro linijų klientus privatumui ginti [2].

Yra dvi oro vežėjams taikomos nuostatos, ginančios asmeninės informacijos privatumą tam tikrais atvejais. Pirma, Federalinis aviacijos aktas gina kandidatų į pilotus privatumą (žr. 49 U.S.C. § 44936(f)). Leisdamas oro vežėjams gauti kandidato darbo charakteristiką, Aktas suteikia teisę gauti pranešimą apie charakteristikos pareikalavimą, duoti sutikimą, pataisyti netikslumus ir nurodyti charakteristiką pateikti tik sprendimą dėl įdarbinimo priimsiantiems asmenims. Antra, TD nuostatai reikalauja, kad keleivių deklaracijų informacija, surinkta Vyriausybės naudojimui įvykus aviacijos katastrofai, būtų „laikoma konfidencialia ir atskleidžiama tik JAV valstybės departamentui, Nacionalinei transporto valdybai (NTSB reikalavimu) ir JAV transporto departamentui“ (14 CFR 243 dalis, § 243.9(c) (papildyta 63 FR 8258)).

---

(1) Tačiau tiesioginės žalos skundo pateikėjui nebuvimas nėra priežastis atmesti skundą (47 U.S.C. § 208(a)).

(2) Suprantama, pramonėje stengiamasi spręsti privatumo klausimus. Pramonės atstovai aptarė siūlomus „saugaus uosto“ principus ir galimybę juos pritaikyti oro vežėjams. Aptarime buvo siūlyta patvirtinti pramonės privatumo strategiją. Dalyvaujančios firmos įsipareigoja paklusti TD jurisdikcijai.

Maisto produktų paruošimo ir galvijų paskirstymo įmonės

Kaip numato 1921 m. Maisto produktų paruošimo ir galvijų paskirstymo įmonių aktas (7 U.S.C. § 181 *et seq.*), neteisėta laikoma „bet kurios maisto produktų paruošimo įmonės, susijusios su gyvūnais, mėsa, mėsos produktais ar neapdorotais gyvūnų produktais, prekiautojo gyvais naminiais paukščiais bei su gyvais naminiais paukščiais susijusi veikla ar priemonės, kurios yra nesąžiningos, diskriminacinės arba apgaulingos“ (7 U.S.C. § 192(a); taip pat žr. 7 U.S.C. § 213(a) (draudžiantį „bet kokią nesąžiningą, diskriminacinę arba apgaulingą veiklą ar priemones“, susijusias su gyvūnais). Už šių nuostatų vykdymo priežiūrą visų pirma atsako Žemės ūkio ministras, o FPK turi jurisdikciją mažmeninės veiklos ir su paukštienos pramone susijusioms operacijoms (7 U.S.C. § 227(b)(2)).

Neaišku, ar pagal Maisto produktų paruošimo ir galvijų paskirstymo įmonių aktą Žemės ūkio ministras aiškintų maisto produktų paruošimo ir galvijų paskirstymo įmonės nesugebėjimą apsaugoti asmeninį privatumą pagal aprašytas nuostatas kaip „apgaulingą“ praktiką. Tačiau 5 skirsnio išimtis galioja asmenims, bendrovėms ar įmonėms, kurioms galioja „Maisto produktų paruošimo ir galvijų paskirstymo įmonių aktas“. Todėl, jei asmeninis privatumas nėra Maisto produktų paruošimo ir galvijų paskirstymo įmonių akto taikymo srities dalykas, tuomet gali būti netaikoma 5 skirsnio išimtis ir maisto produktų paruošimo ir galvijų paskirstymo įmonės gali patekti į FPK jurisdikcijos sritį.

Valstybinė jurisdikcija „nesąžiningos ir apgaulingos veiklos“ atžvilgiu

FPK personalo parengta analizė parodė, kad „visos 50 valstijų ir Kolumbijos apygarda, Guamo salos, Puerto Rikas ir Mergelės salos (JAV) priėmė panašius į Federalinės prekybos komisijos aktą (FPKA) nesąžiningos ar apgaulingos prekybos veiklos prevencijos teisės aktus“ (ši FPK informacija perspausdinta iš „Comment, Consumer Protection: The Practical Effectiveness of State Deceptive Trade Practices Legislation“ („Komentaras apie klientų apsaugą – Valstijų apgaulingos veiklos praktiką reglamentuojančių teisės aktų praktinis veiksmingumas“), *59 Tul, L. Rev. 427 (1984 m.)*). Vykdymo priežiūros institucija yra oficialiai įgaliota „tirti panaudojant šaukimus į teismą ar civilinio tyrimo reikalavimus, gauti užtikrinimą apie savanorišką reikalavimų laikymąsi, išleisti veiklos sustabdymo ir nutraukimo įsakymus arba gauti teismo draudimus, draudžiančius vykdyti nesąžiningą arba apgaulingą prekybinę veiklą (*id.*). 46 valstijų jurisdikcijų teisės aktai numato tikrąjį, dvigubą, trigubą arba drausminį žalos atlyginimą, o kai kuriais atvejais – išlaidų ir advokato paslaugų padengimą (*id.*)“.

Pavyzdžiui, Floridos apgaulingos ir nesąžiningos veiklos aktas suteikia įgaliojimus valstijos generaliniam prokurorui tirti ir pateikti civilinius ieškinius prieš „nesąžiningus konkurencijos veiksmus, nesąžiningus arba apgaulingus prekybos metodus“, įskaitant neteisingą arba klaidinančią reklamą, klaidinančius privilegijų ar verslo galimybių siūlymus, apgaulingą tiesioginę rinkodarą telefonu ir piramidines sistemas. Taip pat žr. N.Y. Pagrindinio verslo įstatymo § 349 (draudžiami nesąžiningi veiksmai ir apgaulingi metodai vykdant verslą).

Šiais metais Nacionalinės generalinių prokurorų asociacijos (NGPA) atliktas tyrimas patvirtino šias išvadas. Visos 43 atsakiusios valstijos turi „mini FPK“ įstatymus ar kitus panašią apsaugą suteikiančius įstatymus. Be to, pasak NGPA tyrimo, 39 valstijos nurodė turinčios jurisdikciją nagrinėti ir nenuolatinių gyventojų skundus. Kalbant apie klientų privatumą, 37 iš 41 atsakiusios valstijos nurodė, kad jos reaguotų į skundus dėl to, kad jų jurisdikcijoje esanti bendrovė nesilaiko pačios paskelbtų privatumo taisyklių.

IV PRIEDAS

Nuostolių, atsiradusių dėl privatumo pažeidimo, atlyginimas, teisiniai įgaliojimai ir susijungimai bei įsigijimai pagal JAV įstatymus

Tai – atsakymas į Europos Komisijos prašymą išaiškinti JAV teisės aktus dėl: a) ieškinių dėl privatumo pažeidimo nuostolių atlyginimo; b) „aiškių įgaliojimų" JAV teisės aktuose naudoti asmeninę informaciją „saugaus uosto" principų neatitinkančiu būdu ir c) susijungimų ir įsigijimų poveikio pagal „saugaus uosto" principus prisiimtiems įsipareigojimams.

A. **Privatumo pažeidimo nuostolių atlyginimas**

Prieš „saugaus uosto" principų pažeidėją priklausomai nuo atitinkamų aplinkybių galima pateikti keletą privačių ieškinių. „Saugaus uosto" organizacijos gali būti atsakingos už klaidinimą ir nesugebėjimą laikytis savo paskelbtų privatumo taisyklių. Privačius ieškinius dėl privatumo pažeidimo nuostolių atlyginimo galima teikti ir remiantis bendrąja teise. Daugelyje federalinių ir valstijų teisės aktų dėl privatumo numatytas už pažeidimus padarytos žalos atlyginimas asmenims.

Teisė gauti žalos, patirtos dėl kišimosi į asmens privatų gyvenimą, atlyginimą yra įtvirtinta JAV bendrojoje teisėje.

Už asmeninės informacijos panaudojimą nesilaikant „saugaus uosto" principų numatyta teisinė atsakomybė pagal keletą skirtingų teisės teorijų. Pavyzdžiui, tiek perduodantysis duomenų valdytojas, tiek susiję asmenys gali pateikti ieškinį prieš „saugaus uosto" organizaciją, kuri nesilaiko savo „saugaus uosto" įsipareigojimų dėl klaidinimo. Pagal Antrąjį teisės aktų sąvadą, Deliktai ([1]):

> už klaidingą faktų, nuomonių, ketinimų ar teisės aktų aiškinimą, siekiant paskatinti kitus tuo remiantis veikti arba susilaikyti nuo veikimo, numatoma atsakomybė atlyginti nukentėjusiajam materialinę žalą, kurią jis pateisinamai patyrė pasitikėdamas klaidinimu.

Sąvadas, § 525. Klaidinimas yra „apgaulingas", kai iš anksto žinoma, kad tvirtinimas yra neteisingas (*id.* § 526). Bendra taisyklė yra tokia, kad tas, kas apgaulingai klaidina, yra pilnai teisiškai atsakingas už visų, kuriuos jis ketina arba tikisi suklaidinti, būsimus materialinius nuostolius (*id.* § 531). Šalis, kuri apgaulingai klaidina kitą šalį, gali būti teisiškai atsakinga prieš trečiąją šalį, jei civilinės teisės pažeidėjas ketina arba tikisi, kad jo klaidinimas bus perduotas ir juo vadovausis trečioji šalis (*id.* § 533).

Tvirtinimu laikomas „saugaus uosto" organizacijos viešas pareiškimas, kad ji laikysis „saugaus uosto" principų. Tuomet dėl sąmoningo principų nesilaikymo galima pateikti ieškinį tiems, kurie rėmėsi klaidinimu. Kadangi įsipareigojimas laikytis principų skelbiamas visai visuomenei, tiek informacijos subjektai, tiek ir asmeninę informaciją JAV organizacijai perdavęs duomenų valdytojas Europoje, gali pagrįstai pateikti ieškinius prieš JAV organizaciją dėl klaidinimo ([2]). Be to, JAV organizacija išlieka teisiškai atsakinga prieš juos už „tęstinį klaidinimą" tol, kol jie savo nenaudai pasitiki klaidinimu (Sąvadas, § 535).

([1]) Antrasis teisės aktų sąvadas, Deliktai; Amerikos teisės institutas (1997 m).

([2]) Taip gali būti, kai, pavyzdžiui, asmenys pasitikėjo JAV organizacijos įsipareigojimais laikytis „saugaus uosto" principų, kai sutiko, kad duomenų tvarkytojas perduotų jų asmeninę informaciją į Jungtines Valstijas.

Nukentėję nuo apgaulingo klaidinimo turi teisę į žalos atlyginimą. Pagal Sąvadą:

> nukentėjusysis nuo apgaulingo klaidinimo turi teisę pareikšti ieškinį jį suklaidinusiam asmeniui dėl apgaulės ir reikalauti atlyginti turtinę žalą, kurios priežastis buvo tas klaidinimas.

Sąvadas, § 549. Leidžiama atlyginti tokią žalą: prarastus tiesioginius piniginius nuostolius ir prarastos „sandorio naudos“ komercinėje transakcijoje atlyginimas (*id.* žr., pvz., Boling prieš Tenesio valstijos banką, 890 S.W.2d 32 (1994 m.) (bankas privalėjo atlyginti skolininkams 14 825 JAV dolerius dydžio kompensacinius nuostolius už tai, kad atskleidė skolininkų asmeninę informaciją ir verslo planus banko prezidentui, turėjusiam priešingų interesų).

Nors klaidinimas laikomas apgaulingu tik tuomet, jei žinoma ar bent manoma, kad tvirtinimas yra neteisingas, atsakomybėn gali būti patraukta ir už neatsargų suklaidinimą. Pagal Sąvadą tie, kurie daro melagingus pareiškimus versle, profesinėje veikloje, vykdydami pareigas ar atlikdami bet kokį piniginį sandorį, gali būti patraukti atsakomybėn, jei „gaudami ar perduodami informaciją nebūna pakankamai atidūs ar kompetentingi“ (Sąvadas, § 552(1)). Skirtingai nuo apgaulingo klaidinimo, žalos atlyginimas už neatsargų suklaidinimą apsiriboja žalos grynaisiais pinigais atlyginimu (*id.*, § 552 B(1)).

Pavyzdžiui, nesenoje byloje Konektikuto Aukščiausiasis teismas nusprendė, kad elektros tarnyba, atskleidusi savo ataskaitos apie kliento mokėjimų informaciją nacionalinėms kredito institucijoms, gali būti pagrįstai apkaltinta klaidinimu (žr. „Brouillard“ prieš „United Illuminating Co.“, 1999 m. Conn. Super. LEXIS 1754). Byloje ieškovui buvo atsisakyta suteikti kreditą, nes atsakovas nurodė, kad per trisdešimt dienų po sąskaitos išrašymo nesumokėtos įmokos yra „pavėluotos“. Ieškovas teigė, kad jis nebuvo informuotas apie tokią tvarką, kai pas atsakovą atsidarė rezidentinę elektros paslaugų sąskaitą. Teismas nusprendė, kad „ieškinį neatsargaus suklaidinimo galima paremti tuo, kad atsakovas nepranešė to, ką privalėjo“. Šis atvejis taip pat rodo, kad „sąmoningas“ arba apgaulingas ketinimas nėra būtinas ieškinių elementas neatsargiam suklaidinimui. Taigi JAV organizacija dėl neatsargumo iki galo neatskleidžianti, kaip ji panaudos „saugaus uosto“ sistemoje gautą asmeninę informaciją, gali būti patraukta atsakomybėn už klaidinimą.

Duomenų subjektas gali pateikti ieškinį dėl privatumo pažeidimo atsižvelgiant į tai, kaip „saugaus uosto“ principų pažeidimas susijęs su asmeninės informacijos netinkamu panaudojimu. Amerikos teisė jau seniai pripažįsta su privatumo pažeidimais susijusias ieškinių priežastis. 1905 m. byloje [1] Džordžijos Aukščiausiasis teismas nusprendė, kad prigimtinė ir bendroji teisė į privatumą buvo pažeista, kai gyvybės draudimo bendrovė eilinio piliečio nuotrauką be jo žinios ir sutikimo panaudojo komercinei reklamai. Apibendrindamas plačiai žinomas Amerikos privatumo jurisprudencijos temas, teismas nusprendė, kad nuotrauka panaudota „piktavališkai“, „netinkamai“ ir ketinant „ieškovą apjuokti prieš visą pasaulį“ [2]. Sprendimo *Pavesich* byloje pagrindinės tezės su nedideliais pakeitimais dominavo ir toliau, kol tapo šios srities Amerikos teisės bendruoju principu. Valstijų teismai nuolatos palaikydavo ieškinius dėl privatumo pažeidimų ir dabar mažiausiai 48 valstijos juridiškai pripažįsta juos kaip ieškinių priežastį [3]. Maža to, mažiausiai 12 valstijų yra konstitucinės nuostatos, saugančios jų piliečių teisę nuo kišimosi veiksmų [4], kurios kai kuriais atvejais gali saugoti nuo nevyriausybinių institucijų kišimosi (žr., *pvz.*, Hill prieš NCAA. 865 P.2d 633 (Ca. 1994); taip pat žr. S. Ginder, „Lost and Found in Cyberspace: Information Privacy in the age of the internet“ („Pamestas ir rastas kibernetinėje erdvėje: informacijos privatumas interneto amžiuje“), 34 S.D.L. Rev. 1153 (1997 m.). („Kai kurių valstijų konstitucijose numatyta didesnė privatumo apsauga nei JAV Konstitucijoje. Didesnė privatumo apsauga yra Aliaskoje, Arizonoje, Kalifornijoje, Floridoje, Havajuose, Ilinojuje, Luizianoje, Montanoje, Pietų Karolinoje ir Vašingtone“).

Antrajame deliktų sąvade pateikta autoritetinga šios srities teisės apžvalga. Atspindėdamas bendrąją teisminę praktiką Sąvadas paaiškina, kad „teisė į privatumą“ aprėpia keturias atskiras ieškinių priežastis dėl teisės pažeidimų šioje srityje (žr. Sąvadą, § 652A). Pirma, ieškinys dėl „kišimosi į nuošalumą“ gali būti pateiktas prieš atsakovą, kuris tyčia fiziškai ar kitaip pažeidžia kito asmens vienumą ar nuošalumą arba jo privačius reikalus [5]. Antra, „pasisavinimo“ ieškinys

---

(1) *Pavesich* prieš Naujosios Anglijos gyvybės draudimo bendrovę, 50 S.E. 68 (Ga. 1905).

(2) (Elektroninėje duomenų bazėje *Westlaw* nuo 1995 m. užregistruotos 2 703 su „privatumu“ susijusios civilinių ieškinių bylos valstijų teismuose. Mes anksčiau esame pateikę šios paieškos rezultatus Komisijai.

(3) *Id.*, 69.

(4) Žr., pvz., Aliaskos Konstitucija, 1 straipsnio 22 skirsnis; Arizona, 2 str., 8 sk.; Kalifornija, 1 str., 1 sk.; Florida, 1 str., 23 sk.; Havajai, 1 str., 5 sk.; Ilinojus, 1 str., 6 sk.; Luiziana, 1 str., 5 sk.; Montana, 2 str., 10 sk.; Niujorkas, 1 str., 12 sk.; Pensilvanija, 1 str., 1 sk.; Pietų Karolina, 1 str., 10 sk. ir Vašingtonas, 1 str., 7 sk.

(5) *Id.*, 28 skyrius, 62B skirsnis.

gali būti pateiktas prieš tą, kuris pasisavina kito vardą ar atvaizdą ir panaudoja savo reikmėms ar iš to pasipelno (1). Trečia, baustinas yra „privačių faktų paviešinimas“, kai paskelbta medžiaga įžeidžia atitinkamą asmenį ir nėra pagrįstai svarbi visuomenei (2). Ir pagaliau ieškinys dėl „klaidinančio kėlimo į viešumą“ gali būti pagrįstas, kai atsakovas sąmoningai ar neapgalvotai viešai pateikia neteisingą kito įvaizdį, kas galėtų labai įžeisti supratingą asmenį (3).

„Saugaus uosto“ sistemoje nuošalumo pažeidimas gali aprėpti neleistiną asmeninės informacijos rinkimą, o tokios informacijos panaudojimas komerciniais tikslais galėtų būti pasisavinimo ieškinio pagrindu. Panašiai ir netikslios asmeninės informacijos atskleidimas gali būti deliktu dėl „klaidinančio kėlimo į viešumą“, jei informacija standartiškai laikoma įžeidžiančia supratingą asmenį. Kišimasis į privatumą dėl ypatingos asmeninės informacijos paskelbimo ar atskleidimo gali būti ieškinio dėl „privačių faktų paviešinimo“ pagrindu (žr. toliau pateikiamus paaiškinamųjų bylų pavyzdžius).

Kalbant apie žalos atlyginimą, kišimasis į privatumą suteikia nukentėjusiajai šaliai teisę į kompensaciją už:

a) žalą, sukeltą dėl kišimosi į privačius interesus;

b) moralines kančias, įrodžius, kad jos buvo patirtos ir jei jos yra tokio pobūdžio, koks paprastai būna patyrus tokį kišimąsi, ir

c) ypatingąją žalą, kurios teisinė priežastis yra kišimasis.

Sąvadas, § 652H. Atsižvelgiant į bendrą delikto teisės aktų taikymą ir pagrindų ieškiniams dėl įvairių privatumo interesų aspektų gausumą, dėl „saugaus uosto“ principų nesilaikymo patyrusiems kišimąsi į jų privatumo interesus piniginės kompensacijos dažniausiai būtų išmokamos.

Iš tiesų valstijų teismai pilni bylų dėl kišimosi į privatumą esant panašioms situacijoms. Pavyzdžiui, byloje *ex parte* „AmSaouth Bancorporation“ *et al*., 717 So. 2d 357 buvo pateiktas grupinis ieškinys, kuriame atsakovas buvo kaltinamas „savanaudiškai išnaudojęs banko indėlininkus, nes pranešęs konfidencialią informaciją apie banko indėlininkus ir jų sąskaitas“ tam, kad banko filialas galėtų parduoti bendruosius fondus ir kitas investicijas. Tokiais atvejais dažnai priteisiama atlyginti nuostolius. Byloje Vassiliades prieš Garfinckel's, Brooks Bros., 492 A.2d 580 (D.C.App. 1985 m.) apeliacinis teismas priėmė priešingą sprendimą nei žemesnės instancijos teismas, nustatydamas, kad ieškovo nuotraukų „prieš“ ir „po“ plastinės operacijos panaudojimas skyriaus parduotuvės prezentacijoje yra kišimasis į privatumą dėl privačių faktų paskelbimo. Byloje Candebat prieš Flanagan, 487 So.2d 207 (Miss. 1986 m.) atsakovė draudimo bendrovė savo reklaminėje kampanijoje buvo panaudojusi medžiagą apie avariją, kurioje buvo sunkiai sužeista ieškovo žmona. Ieškovas pateikė ieškinį dėl kišimosi į privatumą. Teismas nustatė, kad ieškovas turi teisę į nuostolių atlyginimą už moralinę žalą ir tapatybės pasisavinimą. Ieškiniai dėl neteisėto pasisavinimo gali būti palaikomi net jei ieškovas nėra garsus. Žr., pvz., bylą Staruski prieš „Continental Telephone Co.“, 154 Vt. 568 (1990 m.) (atsakovas turėjo komercinės naudos iš to, kad panaudojo darbuotojo vardą ir nuotrauką laikraščio reklamoje). Byloje Pulla prieš „Amoco Oil Co.“, 882 F.Supp 836 (S.D Iowa 1995 m.) darbdavys pažeidė ieškovo darbuotojo nuošalumą, kai liepė kitam darbuotojui patikrinti kredito kortelės duomenis ir tokiu būdu sužinoti, ar tikrai darbo dienos buvo praleistos dėl ligos. Teismas palaikė prisiekusiųjų skirtą 2 JAV dolerių atlyginimą už tiesioginę žalą ir 500 000 JAV dolerių drausminio žalos atlyginimo. Kitas darbdavys buvo patrauktas atsakomybėn už tai, kad bendrovės laikraštyje išspausdino straipsnį apie darbuotoją, kuris buvo atleistas už tariamai sufalsifikuotą savo darbo charakteristiką (žr. Zinda prieš „Louisiana-Pacific Corp.“, 140 Wis.2d 277 (Wis.App. 1987 m.). Straipsniu buvo įsikišta į ieškovo privačius reikalus, nes privatūs dalykai buvo išspausdinti bendrijoje platinamame laikraštyje. Net koledžas buvo patrauktas atsakomybėn dėl nuošalumo pažeidimo, kai kraujo mėginiai iš tikrųjų buvo imami dėl ŽIV, o ne raudonukės tyrimams (žr. Doe prieš „High-Tech Institute, Inc.“, 972 P.2d 1060 (Colo.App. 1998 m.). (Kitų registruotos bylos pateiktos: Sąvadas, § 652H, priedas).

Jungtinės Valstijos dažnai kritikuojamos dėl pernelyg didelio pomėgio bylinėtis, tačiau tai liudija, kad asmenys gali imtis ir imasi teisinių veiksmų, kai mano, kad su jais buvo pasielgta neteisingai. Dėl daugelio JAV teisminės sistemos

(1) *Id.*, 28 skyrius, 652C skirsnis.

(2) *Id.*, 28 skyrius, 652D skirsnis.

(3) *Id.*, 28 skyrius, 652E skirsnis.

aspektų ieškovams lengva teikti tiek atskirus, tiek kolektyvinius ieškinius. Dėl gausios advokatūros, kuri yra didesnė nei daugumos šalių, galima lengvai rasti profesionalų gynėją. Asmenis privačių ieškinių bylose atstovaujantys ieškovus advokatai paprastai dirba už atlyginimą, mokamą laimėjus bylą, kas leidžia ieškoti teisingumo net neturtingiems ar nepasiturintiems ieškovams. Tai iškelia svarbų veiksnį – Jungtinėse Valstijose kiekviena pusė paprastai dengia savo advokatų ir kitas išlaidas. Ši tvarka skiriasi nuo Europoje vyraujančios, pagal kurią visas išlaidas kitai pusei atlygina pralaimėjusioji pusė. Nenagrinėjant šių dviejų sistemų privalumų viena kitos atžvilgiu, JAV taisyklės skatina teikti ieškinius asmenis, kurie negalėtų padengti abiejų šalių išlaidų, jei pralaimėtų.

Asmenys gali teikti ieškinius dėl kompensacijų net jei jos yra palyginti nedidelės. Daugelyje, jei ne visose, JAV jurisdikcijose yra smulkių ieškinių teismai, kurie vykdo supaprastintas ir pigesnes procedūras ginčams dėl mažesnių nei įstatymo nustatyta riba sumų ([1]). Galimas drausminis žalos atlyginimas yra galimybė gauti piniginę kompensaciją asmenims, kurie patyrė per mažą tiesioginę žalą, kad galėtų pateikti ieškinį dėl nelestinų veikų. Panašiu būdu nukentėję asmenys gali suvienyti savo išteklius ir ieškinius ir pateikti kolektyvinį ieškinį.

Tinkamas galimybės asmenims pateikti ieškinį dėl kompensacijos pavyzdys yra vykstantis procesas prieš „Amazon.com“ dėl privatumo pažeidimo. „Amazon.com“, stambi mažmeninės prekybos internetu kompanija, yra atsakovė kolektyviniame ieškinyje, kuriame ieškovai teigia, kad jie nebuvo informuoti ir nepritarė asmeninės informacijos apie juos rinkimui jiems naudojantis „Amazon.com“ programa „Alexa“. Ieškovai kaltino pažeidus Kompiuterinio sukčiavimo ir piktnaudžiavimo aktą ir neteisėtai gavus jų sukauptą informaciją bei Elektroninių komunikacijų privatumo aktą – neteisėtai įsikišus į jų elektroninio ir laidinio ryšio bendravimą. Jie taip pat kaltina privatumo pažeidimu pagal bendrąją teisę. Tai nurodyta gruodžio mėnesį interneto apsaugos eksperto surašytame skunde. Ieškinyje reikalaujama atlyginti 1 000 JAV dolerių žalą kiekvienam ieškinio atstovui, išlaidas advokatams ir grąžinti dėl įstatymų pažeidimo gautą pelną. Turint galvoje tai, kad ieškinio atstovų gali būti milijonai, žalos atlyginimo suma gali siekti net milijardus dolerių. FPK taip pat tiria šiuos kaltinimus.

Federaliniuose ir valstijų privatumo teisės aktuose dažnai numatytos privačių ieškinių dėl piniginio žalos atlyginimo galimybės.

Be to, kad tai gali užtraukti administracinę atsakomybę pagal delikto teisės aktus, „saugaus uosto“ principų nesilaikymas gali pažeisti ir vieną ar kitą iš šimtų federalinių ir valstijų privatumo teisės aktų. Daugelis tokių teisės aktų, kuriuose aptariamas asmeninės informacijos tvarkymas tiek Vyriausybinėse, tiek privataus sektoriaus institucijose, leidžia įvykus pažeidimui asmenims pateikti ieškinius dėl žalos atlyginimo. Pavyzdžiui:

1986 m. Elektroninių komunikacijų privatumo aktas. EKPA draudžia neleistinai perimti mobiliųjų telefonų skambučius ir tarp kompiuterių siuntinėjamą informaciją. Už jo pažeidimą gresia administracinė atsakomybė padengti ne mažiau kaip 100 JAV dolerių žalą už kiekvieną pažeidimo dieną. EKPA taip pat saugo laikomas elektronines telekomunikacijas nuo neteisėto priėjimo ar jų atskleidimo. Pažeidėjai atsako už patirtus nuostolius ir dėl pažeidimo negautą pelną.

1996 m. Telekomunikacijų aktas. Pagal 702 skirsnį, tinkle esančios klientams priklausančios informacijos (TEKPI) negalima naudoti jokiais kitais tikslais, išskyrus telekomunikacijų paslaugoms. Paslaugos abonentai gali pateikti skundą Federalinei ryšių komisijai arba ieškinį federaliniam apygardos teismui dėl žalos atlyginimo ir išlaidų advokatams padengimo.

1996 m. Kliento kreditinių ataskaitų sudarymo reformos aktas. 1996 m. aktas iš dalies pakeitė 1970 m. Sąžiningo kreditinių ataskaitų sudarymo aktą (SKASA) – imta reikalauti tikslesnių pranešimų ir priėjimo teisės ataskaitų apie kreditines operacijas subjektams. Reformos aktu buvo nustatyti ir nauji apribojimai kliento kreditinių ataskaitų perpardavėjams. Už pažeidimus klientams gali būti atlyginta žala ir apmokėtos išlaidos advokatams.

([1]) Mes anksčiau esame pateikę Komisijai informaciją apie smulkių ieškinių procesus.

Valstijų teisės aktai taip pat saugo asmenų privatumą labai įvairiose situacijose. Valstijose vyko teismo procesai dėl bankų registrų, kabelinės televizijos abonentų, kreditinių ataskaitų, darbo charakteristikų, Vyriausybinių archyvų, genetinės informacijos ir medicinos registrų, draudimo registrų, mokyklų archyvų, elektroninių komunikacijų ir vaizdajuosčių nuomos ([1]).

B. **Aiškūs teisiniai įgaliojimai**

„Saugaus uosto“ principuose numatyta išimtis, kai įstatymas, kiti teisės aktai ar precedentinė teisė sukuria „prieštaraujančius įsipareigojimus ar aiškius įgaliojimus, jei vykdydama bet kurį iš tokių įgaliojimų organizacija gali įrodyti, kad ji nesilaiko principų tik tiek, kiek tai būtina laikantis svarbesnių teisėtų interesų pagal tokį įgaliojimą“. Akivaizdu, kad tuomet, kai JAV teisės aktai nustato prieštaraujančius įsipareigojimus, tiek „saugaus uosto“ sistemai priklausančios, tiek nepriklausančios JAV organizacijos privalo laikytis teisės aktų. Kalbant apie aiškius įgaliojimus, nors „saugaus uosto“ principai skirti įveikti skirtumus tarp JAV ir Europos privatumo apsaugos režimų, mes gerbiame mūsų išrinktų įstatymų leidėjų teisines prerogatyvas. Tam tikromis griežto „saugaus uosto“ principų laikymosi išimtimis siekiama subalansuoti kiekvienos pusės teisėtus interesus.

Tokios išimtys apsiriboja aiškiais įgaliojimais. Todėl rodikliu yra tai, ar atitinkamas įstatymas, kiti teisės aktai ar teismo sprendimas tvirtai įgalioja „saugaus uosto“ organizacijas elgtis tam tikru būdu ([2]). Kitaip tariant, išimtis negalioja, jei apie tai neparašyta teisės aktuose. Be to, išimtys taikomos tik tuomet, kai aiškus įgaliojimas prieštarauja „saugaus uosto“ principams. Net ir tokiu atveju išimtis taikoma „tik tiek, kiek tai būtina laikantis viršesnių teisėtų interesų pagal tokį įgaliojimą“. Pavyzdžiui, jei teisės aktai tiesiog įgalioja bendrovę pateikti asmeninę informaciją Vyriausybinėms institucijoms, tokia išimtis negalioja. Ir priešingai, jei įstatymas konkrečiai įgalioja kompaniją suteikti asmeninę informaciją Vyriausybinėms institucijoms be asmens sutikimo, tai „aiškus įgaliojimas“ veikti priešingai „saugaus uosto“ principams. Priešingai, aiškiai apibrėžtos išimtys, leidžiančios nesilaikyti patvirtintų reikalavimų pranešti ir gauti sutikimą, priklausys išimties veikimo sričiai (kadangi tai atitinka konkretų įgaliojimą atskleisti informaciją nepranešant ir neprašant sutikimo). Pavyzdžiui, teisės aktas, kuris įgalioja gydytojus suteikti jų pacientų medicininių įrašų korteles sveikatos apsaugos pareigūnams be paciento išankstinio sutikimo, gali leisti išimtinai nesilaikyti pranešimo ir pasirinkimo principų. Toks įgaliojimas neleidžia gydytojui suteikti tų pačių medicininių įrašų kortelių sveikatos priežiūros organizacijoms ar komercinėms farmacinių tyrimų laboratorijoms, kurios nepatenka į teisės akto taikymo sritį ir todėl joms netaikoma išimtis ([3]). Nagrinėjama institucija gali būti „pavieniu“ įgaliojimu panaudoti asmeninę informaciją, tačiau, kaip rodo toliau pateikti pavyzdžiai, tai dažniausiai būna platesnio teisės akto, kuris draudžia asmeninės informacijos rinkimą, naudojimą ar atskleidimą, išimtimi.

1996 m. Telekomunikacijų aktas

Daugeliu atvejų leistini panaudojimai atitinka Direktyvos ir principų reikalavimus arba leidžiami viena iš kitų leistinų išimčių. Pavyzdžiui, Telekomunikacijų akto 702 skirsnyje (susisteminta kaip 47 U.S.C. § 222) telekomunikacijų paslaugų teikėjai įpareigojami išsaugoti gautos jų klientų asmeninės informacijos konfidencialumą. Ši nuostata leidžia telekomunikacijų paslaugų teikėjams:

1) naudoti informaciją apie klientą teikiant telekomunikacijų paslaugas, įskaitant abonentų katalogų skelbimą;

2) raštišku kliento reikalavimu suteikti informaciją apie klientą kitiems ir

3) teikti informaciją apie klientą dalimis.

([1]) *Westlaw* duomenų bazėje užregistruotos 994 bylos, susijusios su žalos atlyginimu dėl privatumo pažeidimo.

([2]) Atitinkama teisinė jurisdikcija neprivalo konkrečiai nurodyti „saugaus uosto“ principų.

([3]) Panašiai gydytojas šiame pavyzdyje, pasiremdamas teisės akto įgaliojimu, negali nekreipti dėmesio į asmens pasirinkimą pasitraukti (*opt out*) iš tiesioginės rinkodaros, kaip nurodyta 12 FAQ. Bet kurios išimties dėl „aiškaus įgaliojimo“ taikymo sritis yra būtinai apribota atitinkamo teisės akto taikymo sritimi.

Žr. 47 U.S.C. § 222(c)(1)-(3). Aktas taip pat leidžia telekomunikacijų paslaugų teikėjams išimties tvarka naudoti informaciją apie klientus:

1) pradėti, suteikti, pateikti sąskaitas ir rinkti ją savo paslaugoms teikti;

2) saugotis nuo apgaulingos, įžeidžiančios ar nelegalios veiklos ir

3) klientui paskambinus, teikti telefonu tiesioginės rinkodaros, persiuntimo ar administracines paslaugas ([1]).

Id., § 222(d)(1)–(3). Telekomunikacijų paslaugų teikėjai privalo pateikti telefonų knygų leidėjams informaciją sąrašais, kuriuose gali būti tik pavardės, adresai, telefono numeriai ir verslo apibūdinimo eilutė komerciniams klientams (*id.*, § 222(e)).

„Aiškių įgaliojimų“ išimtis gali būti taikytina, kai telekomunikacijų paslaugų teikėjai naudoja TEKPI užkirsti kelią apgavystėms ar kitiems neteisėtiems veiksmams. Net ir tokiu atveju teikėjų veiksmai gali būti laikomi atitinkančiais visuomenės interesus ir dėl to leidžiami principų.

Sveikatos ir paslaugų departamento pasiūlytos taisyklės

Sveikatos ir paslaugų departamentas (SPD) pasiūlė taisykles dėl standartų dėl asmenį identifikuojančios informacijos apie sveikatą privatumo (žr. 64 Fed. Reg. 59 918 (1999 m. lapkričio 2 d.) (susisteminta kaip 45 C.F.R. 160–164 punktai). Taisyklės padėtų įgyvendinti 1996 m. Sveikatos draudimo portatyvumo ir atskaitomybės akto (Pub. L. 104–191) privatumo reikalavimus. Siūlomos taisyklės draustų jų paskirties subjektams (t. y. sveikatos planams, sveikatos apsaugos atsiskaitymų kontoroms ir sveikatos paslaugų teikėjams, kurie perdavinėja informacija elektroniniu formatu) naudoti ar atskleisti apsaugotą informaciją apie sveikatą be asmens leidimo (žr. siūlomąjį 45 C.F.R. § 164 506). Remiantis šiomis siūlomomis taisyklėmis, atskleisti apsaugotą informaciją apie sveikatą leidžiama tik dviem tikslais: 1) tam, kad asmenys galėtų patikrinti ir nusikopijuoti informaciją apie savo sveikatą (žr. *id.* § 164 514) ir 2) taisyklėms vykdyti (žr. *id.* § 164 522).

Siūlomos taisyklės tam tikromis aplinkybėmis leistų naudoti ar atskleisti apsaugotą informaciją apie sveikatą be konkretaus asmens leidimo. Tokioms aplinkybėms priskiriama: sveikatos apsaugos sistemos, teisės aktų vykdymo ir kritinių atvejų priežiūra (žr. *id.* § 164 510). Siūlomose taisyklėse išsamiai aprašyti tokių panaudojimo ir atskleidimo atvejų apribojimai. Be to, būtų leidžiama panaudoti ar atskleisti tik būtiniausią reikiamą informacijos kiekį (žr. *id.* § 164 506).

Siūlomuose nuostatuose suteiktos panaudojimo teisės iš esmės atitinka „saugaus uosto“ principus arba yra leistinos kitomis išimtimis. Pavyzdžiui, teisės aktų ir teismo sprendimų vykdymas leidžiamas, kaip ir medicininiai tyrimai. Kitoks panaudojimas, pvz., sveikatos priežiūros sistemos, sveikatos apsaugos funkcionavimo ir Vyriausybinių duomenų apie sveikatą sistemų priežiūrai, tarnauja visuomenei. Atskleisti informaciją sveikatos priežiūros įmokoms ar išmokoms tvarkyti būtina, kad galėtų būti teikiamos sveikatos priežiūros paslaugos. Informacijos panaudojimas kritiniais atvejais, kad būtų galima pasitarti dėl gydymo su artimiausiu giminaičiu, jei paciento sutikimo „negalima gauti praktiškai ar pagrįstai“, arba tapatybei ar mirusiojo mirties priežasčiai nustatyti, apsaugoti gyvybinius duomenų subjekto ir kitų interesus. Informacijos panaudojimas tikrosios karinės tarnybos kariškių ar kitų specialių asmenų kategorijų valdymui padeda tinkamai vykdyti karines užduotis ar panašias neatidėliotinas situacijas; ir bet kuriuo atveju toks panaudojimas retai arba išvis niekada netaikomas eilinių vartotojų atžvilgiu.

Sveikatos priežiūros įstaigoms lieka galimybė panaudoti asmeninę informaciją pacientų kartotekoms sudaryti. Nors tai nėra „gyvybiškai“ svarbi priežastis, tokios kartotekos naudingos pacientams, jų draugams ir giminėms. Be to, tokio

([1]) Šios išimties taikymo sritis yra labai ribota. Pagal jos salygas telekomunikacijų paslaugų teikejai gali naudoti TEKPI tik kliento skambučių metu. Be to, FKK patarė telekomunikacijų paslaugų teikėjui nenaudoti TEKPI parduodant paslaugas, nepatenkančias į kliento pasiteiravimo sritį. Pagaliau, kadangi klientas turi patvirtinti TEKPI naudojimą šiam tikslui, vargu, ar šią nuostatą iš viso galima laikyti „išimtimi“.

leistino panaudojimo taikymo sritis yra natūraliai apribota. Taigi principų išimties taikymas, panaudojant informaciją pagal įstatymo nustatytus „aiškius įgaliojimus“ tokiais tikslais, sukelia minimalią riziką pavojaus pacientų privatumui.

Sąžiningo kreditinių ataskaitų sudarymo aktas

Europos Komisija išreiškė susirūpinimą, kad „aiškių įgaliojimų“ išimtis „iš esmės sukurs tinkamumo išvadą“ Sąžiningo kreditinių ataskaitų sudarymo aktui (SKASA). Taip nebus. Nesant konkrečios SKASA tinkamumo išvados, tos JAV organizacijos, kurios juo vadovautųsi, turės pasižadėti visokeriopai laikytis „saugaus uosto“ principų. Tai reiškia, kad kai SKASA reikalavimais nustatytas apsaugos lygis yra aukštesnis už numatytą principuose, JAV organizacijoms tereikia laikytis SKASA. Ir atvirkščiai, kai SKASA reikalavimai būtų mažiau griežti, tuomet organizacijos turėtų organizuoti savo informacinę veiklą pagal principus. Išimtis nekeičia šios pagrindinės taisyklės. Kaip nurodyta joje pačioje, išimtis taikoma tik tuomet, kai atitinkamas teisės aktas aiškiai įgalioja atlikti veiksmus, kurie neatitinka „saugaus uosto“ principų. Išimtis negalioja tuomet, jei SKASA reikalavimai paprasčiausiai neatitinka „saugaus uosto“ principų ([1]).

Kitaip tariant, mes nenorime pasakyti, kad išimtis reiškia, jog tai, ko nereikalaujama, įvardija „aiškų įgaliojimą“. Išimtis galioja tik tuo atveju, kai iškyla prieštaravimų tarp JAV įstatymų ir „saugaus uosto“ principų reikalavimų. Atitinkamas įstatymas privalo apimti abu šiuos elementus, kad būtų leista nesilaikyti principų.

Pavyzdžiui, SKASA 604 skirsnis aiškiai įgalioja ataskaitas teikiančias institucijas teikti ataskaitas klientams įvairiomis sąraše išvardytomis aplinkybėmis (žr. SKASA, § 604). Jei joms atsiradus 604 skirsnis įgalioja kreditines ataskaitas teikiančias institucijas veikti nesilaikant „saugaus uosto“ principų, tuomet kreditines ataskaitas teikiančioms institucijoms tektų naudotis išimtimi (nebent galiotų kokia nors kita išimtis). Kreditines ataskaitas teikiančios institucijos privalo vykdyti teismo sprendimus ir didžiosios žiuri šaukimus į teismą, o Vyriausybinio licencijavimo, socialinės paramos ir paramos vaikams teikimo institucijos naudoja kreditines ataskaitas visuomenės naudai (*id.*, § 604(a)(1), (3)(D) ir (4)). Taigi šiais tikslais kreditines ataskaitas teikiančiai institucijai nebūtina vadovautis „aiškaus įgaliojimo“ išimtimi. Kai ji veikia laikydamasi klientų raštiškų nurodymų, klientams ataskaitas teikianti institucija visiškai atitiks „saugaus uosto“ principus (*id.*, § 604(a)(2)). Klientų ataskaitas įdarbinimo tikslais galima gauti taip pat tik raštu leidus klientui (*id.*, §§ 604(a)(3)(B) ir (b)(2)(A)(ii)), o kreditinėms ar draudimo operacijoms, kurių neinicijavo klientas – tik jei klientas ne atsisakė (*opt out* būdu) tokių prašymų (*id.*, § 604(c)(1)(B)). Be to, SKASA draudžia kreditines ataskaitas teikiančioms institucijoms teikti informaciją apie sveikatą įdarbinimo tikslais be kliento sutikimo (*id.*, § 604(g)). Tokios panaudojimo teisės dera su pranešimo ir pasirinkimo principais. Kiti tikslai, kuriuos leidžia 604 skyrius, nustato operacijas, kuriose dalyvauja klientas, ir šiuo tikslu leidžiamos pagal principus. Žr. (*id.*, § 604(a)(3)(A) ir (F)).

Likęs 604 skirsniu „įgaliotas“ panaudojimas susijęs su šalutinėmis kredito rinkomis (*id.*, § 604(a)(3)(E)). Klientų ataskaitų panaudojimas šiuo tikslu *per se* neprieštarauja „saugaus uosto“ principams. Teisybė, kad SKASA nereikalauja kreditines ataskaitas teikiančių institucijų, pavyzdžiui, pranešti klientams ir gauti jų sutikimą, kai jos teikia ataskaitas šiuo tikslu. Tačiau mes kartojame esminį dalyką – kad reikalavimo nebuvimas kartu nereiškia „aiškaus įgaliojimo“ veikti kitaip, nei reikalaujama. Štai 608 skirsnis leidžia kreditines ataskaitas teikiančioms institucijoms suteikti tam tikrą asmeninę informaciją Vyriausybinėms institucijoms. Toks „įgaliojimas“ nepateisintų to, kad kreditines ataskaitas teikianti institucija ignoruotų savo įsipareigojimus laikytis „saugaus uosto“ principų. Tai skiriasi nuo kitų mūsų pavyzdžių, kur aiškių pranešimo ir pasirinkimo suteikimo reikalavimų išimtys aiškiai įgalioja panaudoti asmeninę informaciją nepranešus ir nesuteikus pasirinkimo.

Išvada

Net ribotai apžvelgus šiuos teisės aktus išryškėja tokios tendencijos:

— „aiškus įgaliojimas“ teisės akte paprastai leidžia naudoti ar atskleisti asmeninę informaciją be išankstinio asmens sutikimo; taigi tokia išimtis ribojama pranešimo ir pasirinkimo principais,

([1]) Mūsų šio aptarimo nereikia laikyti pripažinimu, kad SKASA nesuteikia „pakankamos“ apsaugos. Vertinant SKASA privalu atsižvelgti į viso teisės akto teikiamą apsaugą, o ne nagrinėti vien išimtis, ką dabar mes darome.

— daugeliu atvejų teisės aktu leidžiamos išimtys yra susiaurintos ir skirtos taikyti tik ypatingomis aplinkybėmis ir ypatingais tikslais. Visais atvejais teisės aktai draudžia neįgaliotą asmeninės informacijos panaudojimą ar atskleidimą, nenumatytą tokiomis išimtimis,

— daugeliu atvejų įgaliotas panaudojimas ar atskleidimas tarnauja visuomenės interesams, o tai rodo jų teisėtumą,

— beveik visais atvejais įgaliotas panaudojimas visiškai atitinka „saugaus uosto“ principus arba kitas leistinas išimtis.

Išvada: „aiškių įgaliojimų“ išimtis teisės aktuose dėl savo pobūdžio gali būti taikytina labai retai.

C. **Susijungimai ir įsigijimai**

29 straipsnio Darbo grupė išreiškė susirūpinimą dėl situacijų, kai „saugaus uosto“ organizaciją įsigyja arba ji susijungia su firma, kuri nėra įsipareigojusi laikytis „saugaus uosto“ principų. Tačiau Darbo grupė, atrodo, padarė prielaidą, kad susikūrusioji firma nebus įpareigota taikyti „saugaus uosto“ principus įsigytos firmos turimai asmeninei informacijai, tačiau pagal JAV teisės aktus taip nebūtinai turi būti. Kalbant apie susijungimus ir įsigijimus, JAV vyrauja pagrindinė taisyklė, kad bendrovė, įsigijusi kitos įmonės išleistas akcijas, paprastai prisiima įsigytos firmos įsipareigojimus ir prievoles (žr. *Privačių įmonių įstatymų Fletčerio enciklopediją* § 7117 (1990 m.); taip pat *Pavyzdinio verslo įmonių akto* § 11.06(3) (1979 m.) („susikūrusioji įmonė turi visus visų susijungime dalyvavusių įmonių įsipareigojimus“). Kitaip tariant, susijungiant ar įsigijus „saugaus uosto“ organizaciją naujai susikūrusi firma būtų saistoma tos organizacijos prisiimtų „saugaus uosto“ įsipareigojimų.

Be to, jei susijungimas ar įsigijimas vykdomas įsigyjant turtą, įsigytos įmonės įsipareigojimai tam tikromis aplinkybėmis vis tiek saisto įsigijusiąją firmą (15 *Fletcher*, § 7122). Net jei susijungus įmonėms neišlieka įsipareigojimų, verta pažymėti, kad jie neišliktų susijungiant ir tuo atveju, jei duomenys būtų perduoti iš Europos pagal sutartį – vienintelę įgyvendinamą „saugaus uosto“ alternatyvą perduodant duomenis į Jungtines Valstijas. Be to, pagal naujai pataisytus „saugaus uosto“ dokumentus bet kuri „saugaus uosto“ organizacija privalo informuoti Komercijos departamentą apie bet kokį įsigijimą ir leisti toliau perdavinėti duomenis į organizaciją perėmėją tik tuomet, jei ji prisijungia prie „saugaus uosto“ (žr. 6 FAQ). Iš tiesų dabar Jungtinės Valstijos pakoregavo „saugaus uosto“ struktūrą ir reikalauja, kad JAV organizacijos, esant tokiai situacijai, panaikintų „saugaus uosto“ sistemoje gautą informaciją, jei ji žada nebesilaikyti „saugaus uosto“ įsipareigojimų arba vietoj to nenaudoja kitų tinkamų apsauginių priemonių.

V PRIEDAS

2000 m. liepos 14 d.

Johnui Moggui
Direktoriui, DG XV
Europos Komisija
Biuras C 107–6/72
Rue de la Loi/Wetstraat 200
B-1049 Briuselis

Gerbiamas p. Moggai,

Suprantu, kad dėl mano 2000 m. kovo 29 d. laiško kilo klausimų. Kad kompetentingai atsakyčiau į iškilusius klausimus, siunčiu šį laišką, kuris papildo ir reziumuoja ankstesnės korespondencijos tekstą.

Lankydamasis mūsų biuruose ir savo laiškuose Jūs iškėlėte keletą klausimų apie Jungtinių Valstijų Federalinės prekybos komisijos oficialius įgaliojimus dėl privatumo interaktyviojo (*on-line*) ryšio srityje. Manau būtų naudinga reziumuoti mano ankstesnius atsakymus dėl FPK veiklos šioje srityje ir suteikti papildomą informaciją apie institucijos jurisdikciją vartotojų privatumo klausimais, iškeltais Jūsų pastarajame laiške. Jūs klausėte ar: 1) FPK turi jurisdikciją perduoti su įdarbinimu susijusius duomenis, jei perduodant pažeidžiami JAV „saugaus uosto“ principai; 2) FPK turi jurisdikciją dėl pelno nesiekiančių privatumo „seal“ programų; 3) FPK aktas vienodai galioja tiek nesant tiesioginio ryšio (*offline*), tiek ir jam esant (*on-line*); ir 4) kas atsitinka, kai FPK jurisdikcija iš dalies sutampa su kitų teisės aktų vykdymo priežiūros institucijų jurisdikcija.

FPK akto taikymas privatumui

Kaip žinote, per pastaruosius penkerius metus FPK ėmėsi vadovaujančio vaidmens skatinant Jungtinių Valstijų pramonės ir vartotojų grupes išsamiai pasisakyti klientų privatumo klausimais, įskaitant asmeninės informacijos rinkimą ir naudojimą internete. Viešuose seminaruose ir nuolatos konsultuodamiesi su pramonės subjektais, vartotojų atstovais ir mūsų kolegomis iš Komercijos departamento bei visos JAV Vyriausybės mes padėjome nustatyti pagrindinius strategijos aspektus ir rasti praktiškus sprendimus.

Federalinės prekybos komisijos teisiniai įgaliojimai šioje srityje nustatyti Federalinės prekybos komisijos akto („FPK akto“) 5 skirsnyje, kuriuo komercijoje draudžiami „nesąžiningi ar apgaulingi veiksmai ar metodai“ ([1]). „Apgaulingas veiksmas“ apibrėžiamas kaip pateikimas, neveikimas ar veiksmas, kuris galėtų iš esmės suklaidinti supratingus vartotojus. Veiksmas yra nesąžiningas, jei neišvengiamai smarkiai pakenkia ar gali pakenkti vartotojui ir to neatsveria privalumai vartotojui ar konkurencijai ([2]).

Tikėtina, kad tam tikri informacijos surinkimo metodai pažeidžia FPK aktą. Pavyzdžiui, jei interneto svetainė melagingai skelbia, kad yra laikomasi paskelbtų privatumo taisyklių arba nustatytų savireguliacijos vadovo, FPK akto 5 skirsnis suteikia teisinį pagrindą suabejoti, ar toks klaidinimas nėra apgaulingas. Iš tiesų, mes sėkmingai vykdėme šį teisės aktą tokiam principui įtvirtinti ([3]). Be to, Komisija kvestionuoja itin drastiškus privatumo metodus kaip nesąžiningus pagal 5 skirsnio nuostatas, jei į juos įtraukiami vaikai arba naudojama labai ypatinga informacija, pvz., finansiniai registrai ([4]) ir medicininių įrašų kortelės. Federalinė prekybos komisija ėmėsi ir toliau imsis tokių teisės aktų vykdymo priežiūros veiksmų ir aktyviai vykdys monitoringą (stebėsena) bei tirs gautus pranešimus iš savireguliacijos ir kitų organizacijų, taip pat ir iš Europos Sąjungos valstybių narių.

([1]) 15 U.S.C. § 45. Sąžiningo kreditinių ataskaitų sudarymo aktas taip pat galioja duomenų rinkimui ir pardavimui internete, kurie atitinka teisės akto nustatytus „kliento ataskaitos“ ir „klientams ataskaitas teikiančios institucijos“ apibrėžimus.

([2]) 15 U.S.C. § 45(n).

([3]) Žr. „GeoCities“, įrašas Nr. C-3849 (1999 m. vasario 12 d. galutinis nuosprendis) (galima surasti adresu: www.ftc.gov/os/1999/9902/9823015d%26o.htm); „Liberty Financial Cos.“, įrašas Nr. C-3891 (1999 m. rugpjūčio 12 d. galutinis sprendimas) (galima surasti adresu: www.ftc.gov/opa/1999/9905/younginvestor.htm). Taip pat žr. Vaikų privatumo *on-line* apsaugos akto taisyklė (COPPA), 16 C.F.R. 312 dalis (galima surasti adresu: www.ftc.gov/opa/1999/9910/childfinal.htm). Praėjusį mėnesį įsigaliojusi COPRA taisyklė reikalauja, kad jaunesniems kaip 13 metų vaikams skirtų interneto svetainių valdytojai arba žinomai renkantieji asmeninę informaciją iš jaunesnių kaip 13 metų vaikų taikytų taisyklėje suformuluotus sąžiningos informacinės praktikos standartus.

([4]) Žr. FPK prieš „Touch Tone, Inc.“, Civilinis ieškinys Nr. 99-WM-783 (D.Co.) (pateiktas 1999 m. balandžio 21 d.) adresu: www.ftc.gov/opa/1999/9904/touchtone.htm. 1997 m. liepos 17 d. personalo nuomonės raštas, paskelbtas atsakant į Žiniasklaidos švietimo centro peticiją, adresu: www.ftc.gov/os/1997/9707/cenmed.htm.

FPK parama savireguliacijai

FPK jau seniai remia pramonės pastangas kurti veiksmingas savireguliacijos programas, skirtas užtikrinti privatumo apsaugą interneto vartotojams. Tačiau jei šios pastangos būtų sėkmingos, programose turėtų visuotinai dalyvauti pramonės subjektai. Savireguliaciją kartu turi paremti ir teisės aktų vykdymo priežiūra. Dėl šių priežasčių FPK teiks pirmenybę pranešimams apie savireguliacijos nurodymų nesilaikymą, gautiems iš tokių organizacijų kaip „BBBOnline“ ir „TRUSTe“. Toks metodas derinsis su mūsų ilgalaikiu bendradarbiavimu su Geresnio verslo biuro Nacionaline reklamos priežiūros valdyba (NRPV), kuri peradresuoja nusiskundimus dėl reklamos į FPK. NRPV Nacionalinės reklamos skyrius (NRS) teisinio nagrinėjimo būdu sprendžia ginčus dėl nacionalinės reklamos. Kai šalis atsisako paklusti NRS sprendimui, pranešama FPK. FPK personalas prioriteto tvarka išnagrinėja ginčijamą reklamą ir nusprendžia, ar ji pažeidžia FPK aktą ir dažnai sėkmingai sustabdo abejotiną veiklą ar įtikina šalį tęsti NRPV procesą.

Tokiu pat būdu FPK teiktų prioritetą pranešimams apie „saugaus uosto“ principų nesilaikymą iš ES valstybių narių. Kaip ir pranešimų iš savireguliacinių JAV organizacijų atveju, mūsų personalas išnagrinės bet kokią informaciją, nurodančią ar apskųsta veikla pažeidžia FPK akto 5 skirsnį. Šis įsipareigojimas taip pat nurodytas „saugaus uosto“ principuose, 11 FAQ dėl vykdymo priežiūros.

„GeoCities“: FPK pirmoji interaktyvaus (on-line) privatumo byla

Federalinės prekybos komisijos pirmoji privatumo internete byla prieš „GeoCities“ buvo pagrįsta Komisijos jurisdikcija pagal 5 skirsnį [1]. Šioje byloje FPK apkaltino „GeoCities“ klaidinus tiek suaugusius, tiek vaikus dėl to, kaip bus panaudota jų asmeninė informacija. Federalinės prekybos komisijos skunde „GeoCities“ buvo kaltinama tvirtinusi, kad jos interneto svetainėje renkama tam tikra asmens tapatybę atskleidžianti informacija bus naudojama vidaus reikmėms arba teikti vartotojams tam tikrus reklaminius pasiūlymus ir jų reikalaujamus produktus ar paslaugas ir kad tam tikra papildoma „neprivalomoji“ informacija nebus pateikta be vartotojo leidimo. Iš tikrųjų ši informacija buvo atskleista trečiosioms šalims, kurios ją naudojo teikti vartotojams siūlymus, dėl kurių šie nebuvo susitarę. Skunde taip pat buvo kaltinimas, kad „GeoCities“ naudojo apgaulingus metodus rinkdama informaciją iš vaikų. Pasak FPK skundo, „GeoCities“ tvirtino, kad ji tvarko interneto svetainės vaikų skyrių ir kad jame surinkta informacija buvo laikoma „GeoCities“. Iš tikrųjų tuos interneto svetainės skyrius tvarkė trečiosios šalys, kurios rinko ir laikė informaciją.

Nuosprendis uždraudė „GeoCities“ klaidingai nurodyti tikslą, kuriuo ji renka ar naudoja asmens tapatybę atskleidžiančią informaciją iš ar apie vartotojus, įskaitant vaikus. Sprendimas reikalauja, kad bendrovė savo interneto svetainėje paskelbtų aiškų ir nuolatinį Privatumo pranešimą, nurodanti vartotojams, kokia informacija ir kokiu tikslu renkama, kam ji bus atskleista ir kaip vartotojai gali ją pasiekti ir pašalinti. Tam, kad būtų užtikrinta tėvų kontrolė, sprendimas taip pat reikalauja, kad prieš rinkdama asmens tapatybę atskleidžiančią informaciją iš jaunesnių kaip 12 metų vaikų „GeoCities“ gautų tėvų sutikimą. Pagal sprendimą „GeoCities“ privalo informuoti savo vartotojus ir suteikti jiems galimybę panaikinti informaciją apie save iš „GeoCities“ ir bet kurios trečiosios šalies duomenų bazių. Sprendimu „GeoCities“ specialiai įpareigota informuoti jaunesnių kaip 12 metų vaikų tėvus ir panaikinti informaciją apie juos, nebent tėvai patvirtintų pritarią jos išlaikymui ir naudojimui. Pagaliau pareikalauta, kad „GeoCities“ susisiektų su trečiosiomis šalimis, kurioms ji anksčiau atskleidė tą informaciją, ir pareikalautų, kad šios šalys taip pat panaikintų tą informaciją [2].

„ReverseAuction.com“

Visai neseniai ši institucija pateikė ieškinį, kuriame apkaltino kitą interaktyviojo (*on-line*) ryšio bendrovę privatumo pažeidimu. 2000 m. sausį Komisija patvirtino skundą prieš ir sutikimo sutartį su „ReverseAuction.*com*“, interaktyviojo (*on-line*) aukciono interneto svetaine, kuri buvo kaltinama gavusi iš konkuruojančios interneto svetainės („eBay.*com*“) vartotojų asmens tapatybę atskleidžiančią informaciją ir savo verslo tikslais elektroniniu paštu išsiuntinėjo tiems vartotojams apgaulingus, neprašytus pranešimus [3]. Mūsų skunde „ReverseAuction“ buvo kaltinama pažeidusi FPK

[1] „GeoCities“, įrašas Nr. C-3849 (1999 m. vasario 12 d. galutinis sprendimas) (galima surasti adresu: www.ftc.gov/os/1999/9902/9823015d%26o.htm).

[2] Komisija vėliau nagrinėjo kitą klausimą dėl asmeninės informacijos rinkimo iš vaikų interaktyviuoju būdu. „Liberty Financial Companies, Inc.“ valdė Jaunojo investuotojo svetainę internete, skirtą vaikams bei paaugliams, ir pagrindinį dėmesį skyrė su pinigais bei investicijomis susijusiems klausimams. Komisija kaltino, kad interneto svetainėje buvo neteisingai tvirtinama, jog iš vaikų tyrime renkama asmeninė informacija bus anoniminė ir kad dalyviams bus išsiųsti elektroninio pašto informaciniai laiškai ir prizai. Iš tikrųjų asmeninė informacija apie vaiką ir šeimos finansus buvo prieinama ir nebuvo išsiuntinėta jokių informacinių laiškų ar prizų. Sutikimo sutartyje uždrausta taip klaidinti ateityje ir „Liberty Financial“ įpareigota paskelbti vaikų interneto svetainėse privatumo pranešimą ir, prieš renkant asmens tapatybę atskleidžiančią informaciją iš vaikų, gauti galimą patikrinti tėvų sutikimą. Įrašas Nr. C-3891 (1999 m. rugpjūčio 12 d. galutinis sprendimas) (galima surasti adresu: www.ftc.gov/opa/1999/9905/younginvestor.htm).

[3] Žr. „ReverseAuction.com, Inc.“, civilinis ieškinys Nr. 000032 (D.D.C.) (pateiktas 2000 m. sausio 6 d.) (pranešimas spaudai ir gynybos pareiškimai pateikti adresu: www.ftc.gov/opa/2000/01/reverse4.htm).

akto 5 skirsnį rinkdama asmenį identifikuojančią informaciją, įskaitant „eBay“ vartotojų elektroninio pašto adresus ir suasmenintus naudotojų identifikavimo vardus („naudotojų ID“) ir išsiuntinėdama apgaulingus pranešimus elektroniniu paštu.

Kaip aprašyta skunde, prieš gaudama informaciją, „ReverseAuction“ užsiregistravo kaip „eBay“ naudotojas ir sutiko laikytis „eBay“ Naudotojų sutarties ir privatumo taisyklių. Ši sutartis ir taisyklės saugo vartotojų privatumą drausdamos „eBay“ naudotojams rinkti ir naudoti asmenį identifikuojančią informaciją neleistinais tikslais, pvz., neprašytiems komerciniams elektroninio pašto pranešimams siųsti. Taigi mūsų skunde „ReverseAuction“ iš pradžių buvo apkaltinta melavusi, kad laikysis „eBay“ Naudotojų sutarties ir privatumo taisyklių, tačiau pagal 5 skirsnio nuostatas tai yra apgaulingas metodas. Alternatyviame skunde „ReverseAuction“ apkaltinta panaudojusi informaciją neprašytiems komerciniams elektroninio pašto pranešimams siųsti pažeidžiant Naudotojų sutartį ir privatumo taisykles, o tai pagal 5 skirsnio nuostatas yra nesąžininga prekybinė veikla.

Antra, skunde buvo kaltinama, kad elektroninio pašto pranešimų vartotojams temos eilutėje buvo įrašyta apgaulinga informacija apie tai, kad „netrukus nustos galioti“ jų „eBay“ naudotojų ID. Pagaliau skunde buvo kaltinama, kad elektroninio pašto pranešimuose buvo neteisingai teigiama, kad „eBay“ tiesiogiai ar netiesiogiai suteikė „ReverseAuction“ savo naudotojų asmenį identifikuojančią informaciją ar kitaip dalyvavo skleidžiant neprašytus elektroninio pašto pranešimus.

FPK inicijuotas sprendimas draudžia „ReverseAuction“ ateityje daryti tokius pažeidimus. Jis taip pat įgalioja „ReverseAuction“ informuoti vartotojus, kurie gavę „ReverseAuction“ elektroninio pašto pranešimą užsiregistravo arba užsiregistruos „ReverseAuction“ interneto svetainėje. Tokie vartotojai turi būti informuoti, kad jų „eBay“ naudotojų ID nenustoja galioti, ir „eBay“ nežinojo ir neįgaliojo ReverseAuction paskleisti neprašytų elektroninio pašto pranešimų. Pranešimu tokiems vartotojams taip pat suteikiama galimybė atšaukti savo registraciją „ReverseAuction“ interneto svetainėje ir panaikinti jų asmenį identifikuojančią informaciją „ReverseAuction“ duomenų bazėje. Be to, sprendime reikalaujama, kad „ReverseAuction“ panaikintų ir atsisakytų naudoti ar atskleisti tų „eBay“ naudotojų, kurie gavo „ReverseAuction“ elektroninio pašto pranešimą, bet neužsiregistravo „ReverseAuction“ interneto svetainėje, asmenį identifikuojančią informaciją. Atsižvelgiant į ankstesnius šios institucijos gautus privatumo nurodymus, galiausiai sprendimu reikalaujama, kad „ReverseAuction“ savo interneto puslapyje atskleistų savo privatumo taisykles ir turėtų išsamų registrą, kad FPK galėtų vykdyti monitoringą (stebėseną), kaip laikomasi reikalavimų.

„ReverseAuction“ byla rodo, kad FPK pasiryžusi naudoti vykdymo priežiūros priemones, kad paremtų pramonės savireguliacijos pastangas interaktyviųjų paslaugų vartotojų privatumo srityje. Iš tiesų ši byla tiesiogiai užkirto kelią veiklai, kuri kenkė vartotojų privatumą ginančioms Privatumo taisyklėms ir Naudotojo sutartims ir galėjo sugriauti vartotojų pasitikėjimą interaktyviųjų (*on-line*) bendrovių naudojamoms privatumo apsaugos priemonėms. Kadangi šioje byloje viena bendrovė neteisėtai pasisavino kitos bendrovės privatumo taisyklėmis apsaugotą informaciją apie vartotojus, ji gali būti labai artima rūpimiems privatumo klausimams, kylantiems perduodant duomenis tarp skirtingose šalyse esančių bendrovių.

Nepaisant Federalinės prekybos komisijos teisės aktų vykdymo priežiūros veiksmų „GeoCities“, „Liberty Financial Cos.“ ir „ReverseAuction“ bylose, institucijos jurisdikcija kai kuriose interaktyviojo (*on-line*) privatumo srityse yra labiau ribota. Kaip pažymėta pirmiau, tam, kad galėtų būti taikomas FPK aktas, asmeninė informacija turi būti renkama ir naudojama be sutikimo tokiu būdu, kad tai galėtų būti laikoma apgaulinga ar nesąžininga komercine veikla. Taigi FPK aktas greičiausiai neturėtų įtakos interneto svetainei, kuri renka asmenį identifikuojančią informaciją iš vartotojų, tačiau neklaidino dėl jos panaudojimo paskirties, nepanaudojo ar neatskleidė informacijos taip, kad rimtai pakenktų vartotojams. Be to, FPK nepajėgi visuotinai reikalauti, kad internete informaciją renkančios įmonės laikytųsi privatumo taisyklių ar kokių nors konkrečių privatumo taisyklių [1]. Tačiau, kaip nurodyta pirmiau, kompanijos nesugebėjimas laikytis paskelbtų privatumo taisyklių greičiausiai gali būti traktuojamas kaip apgaulinga veikla.

---

[1] Dėl šios priežasties Federalinė prekybos komisija liudydama Kongrese pareiškė, kad greičiausiai reikėtų papildomų teisės aktų, kurie reglamentuotų, kad visos klientams skirtos JAV komercinės interneto svetainės laikytųsi nustatytų sąžiningos informacijos taisyklių („Klientų privatumas pasauliniame interneto tinkle“, 1998 m. liepos 21 d., Jungtinių Valstijų Atstovų rūmų Prekybos komiteto Telekomunikacijų, prekybos ir vartotojų apsaugos pakomitetis (liudijimą galima rasti adresu: www.ftc.gov/os/9807/privac98.htm)). FPK atidėliojo tokių teisės aktų prašymą tam, kad suteiktų savireguliaciniams procesams galimybę pademonstruoti, jog sąžiningos informacijos praktika interneto svetainėse plačiai taikoma. Federalinės prekybos komisijos ataskaitoje Kongresui dėl interaktyviojo (*on-line*) privatumo („Interaktyvusis (*on-line*) privatumas. Ataskaita Kongresui“, 1998 m. birželis, ataskaitą galima surasti adresu: www.ftc.gov/reports/privacy3/toc.htm) rekomendavo, kad teisės aktuose būtų reikalaujama gauti tėvų sutikimą, kai renkama asmenį identifikuojanti informacija iš jaunesnių kaip 13 metų vaikų (žr. 3 *supra* išnašą). Praėjusiais metais Komisija ataskaitoje „Interaktyvioji (*on-line*) savireguliacija ir privatumas. Federalinės prekybos komisijos ataskaita Kongresui“, 1999 m. liepa (ataskaitą galima surasti adresu: www.ftc.gov/os/1999/9907/index.htm#13) nurodė pakankamą savireguliacijos pažangą ir todėl tuomet nerekomendavo priimti teisės aktų. Ateinančiomis savaitėmis Komisija vėl teiks ataskaitą Kongresui apie savireguliacijos pažangą.

Be to, FPK jurisdikcija šioje srityje yra taikytina tik tiems nesąžiningiems ar apgaulingiems veiksmams ar metodams, kurie yra „naudojami komercijoje ar turi jai įtakos“. Tai, kad gaminius ar paslaugas siūlančios komercinės įmonės renka informaciją ir panaudoja ją komerciniais tikslais atitiktų šį „komercinį“ reikalavimą. Kita vertus, daug asmenų ar įmonių gali rinkti informaciją *on-line* be jokio komercinio tikslo ir tokiu būdu nepatekti į Federalinės prekybos komisijos jurisdikciją. Tokio apribojimo pavyzdys gali būti nekomercinių įmonių, pvz., labdaros organizacijų „pokalbių svetainės“.

Yra keletas visiškų ar dalinių įstatyminių FPK pagrindinės jurisdikcijos išlygų dėl komercinės veiklos, kurios riboja FPK galimybes visapusiškai reaguoti į privatumo internete problemas. Tokios išlygos aprėpia daugelį didelės informacinės apyvartos verslo rūšių, kaip antai bankai, draudimo bendrovės ir oro linijos. Kaip suprantate, tokias įmones prižiūri kitos federalinės ar valstijų institucijos, pvz., federalinės bankų institucijos ar Transporto departamentas.

Tais atvejais, kai FPK turi jurisdikciją, ji priima ir, jei turi galimybių, reaguoja į vartotojų skundus, kuriuos gauna paštu ir telefonu į savo Vartotojų atsiliepimų centrą (VAC), o pastaruoju metu – savo interneto svetainėje ([1]). VAC priima skundus iš visų vartotojų, įskaitant ir reziduojančius Europos Sąjungos valstybėse narėse. FPK aktas suteikia Federalinei prekybos komisijai nešališkus įgaliojimus imtis teisinių priemonių prieš būsimus FPK akto pažeidimus ir atlyginti žalą nukentėjusiems vartotojams. Tačiau mes nagrinėsime, ar bendrovė dalyvavo netinkamoje veikloje sistemingai, nes nenagrinėjame atskirų vartotojų ginčų. Federalinė prekybos komisija yra pasiekusi, kad žala būtų atlyginta tiek Jungtinių Valstijų, tiek kitų šalių piliečiams ([2]). FPK ir toliau gins savo įgaliojimus atitinkamose bylose, kad būtų atlyginta kitų šalių piliečiams, nukentėjusiems dėl apgaulingos veiklos, kuriai galioja mūsų jurisdikcija.

Įdarbinimo duomenys

Savo paskutiniame laiške Jūs prašėte papildomai paaiškinti FPK jurisdikciją dėl įdarbinimo duomenų. Pirma, klausėte, ar FPK gali imtis veiksmų pagal 5 skirsnį prieš bendrovę, kuri tvirtina besilaikanti JAV „saugaus uosto“ principų, tačiau perdavinėja ar naudoja su darbo santykiais susijusius duomenis pažeisdama šiuos principus. Mes norime užtikrinti Jus, kad atidžiai išnagrinėjome FPK jurisdikciją apibrėžiančius teisės aktus, susijusius dokumentus bei susijusią precedentinę teisę ir padarėme išvadą, kad FPK turi tokią pačią jurisdikciją dėl su darbo santykiais susijusių duomenų, kokią ji turi apskritai pagal FPK akto 5 skirsnį ([3]). Taigi tuomet, kai atvejis atitinka mūsų su privatumu susijusių įstatymų vykdymo priežiūros veiksmų kriterijus (nesąžiningumas ar apgaulė), mes galime imtis veiksmų dėl su darbo santykiais susijusių duomenų aplinkybių.

Mes taip pat norėtume išsklaidyti bet kokias abejones dėl to, kad FPK gali imtis su privatumu susijusių teisės aktų vykdymo priežiūros veiksmų tik tuomet, kai bendrovė apgauna atskirus vartotojus. Iš tikrųjų Komisijos ieškinys dėl „ReverseAuction“ ([4]) rodo, kad FPK vykdo su privatumu susijusius teisės aktų vykdymo priežiūros veiksmus ir tuomet, kai tai susiję su duomenų perdavimu tarp bendrovių ir viena bendrovė kaltinama veikusi neteisėtai kitos bendrovės atžvilgiu, dėl ko gali nukentėti tiek vartotojai, tiek bendrovės. Mes manome, kad būtent tokiomis aplinkybėmis gali greičiausiai iškilti su įdarbinimu susijusių klausimų, kai įdarbinimo duomenys apie europiečius iš Europos bendrovių perduodami į Amerikos bendroves, kurios įsipareigojo laikytis „saugaus uosto“ principų.

Tačiau norėtume atkreipti dėmesį į vieną aplinkybę, kai FPK veiksmai būtų suvaržyti. Taip būtų tuomet, kai reikalas jau svarstomas tradiciniame darbo teisės ginče, greičiausiai per skundą darbovietės administracijai ar arbitražinį

([1]) Federalinės prekybos komisijos skundo formą rasite adresu: http://www.ftc.gov/ftc/complaint.htm.

([2]) Pavyzdžiui, byloje dėl interneto piramidės sistemos, Komisija išreikalavo kompensacijas 15 622 vartotojams, kurių bendra suma sudarė maždaug 5,5 mln. JAV dolerių. Tie vartotojai buvo iš Jungtinių Valstijų ir 70 užsienio valstybių. Žr.: www.ftc.gov/opa/9807/fortunar.htm; www.ftc.gov/opa/9807/ftcrefund01.htm.

([3]) Išskyrus atvejus, kuriuos konkrečiai išskiria FPK jurisdikciją apibrėžiantis įstatymas, FPK jurisdikcija pagal FPK aktą dėl „naudojamų komercijoje ar turinčių jai įtakos“ veiksmų sutampa su Kongreso įgaliojimais pagal Komercijos straipsnį (Jungtinės Valstijos prieš Amerikos statybos priežiūros pramonę, 422 U.S. 271, 277 Nr. 6 (1975 m.)). Taigi FPK jurisdikcija aprėpia su darbo santykiais susijusią tarptautinės komercijos firmų ir pramonės šakų veiklą.

([4]) Žr. „Interaktyviojo aukciono svetainė atsako už FPK pateiktus kaltinimus dėl privatumo pažeidimo“, FPK informacinis biuletenis (2000 m. sausio 6 d.), galima gauti adresu: http://www.ftc.gov/opa/2000/01/reverse4.htm.

skundą arba skundą dėl nesąžiningos darbo praktikos Nacionalinėje darbo santykių taryboje. Taip būtų, jei, pvz., darbdavys kolektyvine sutartimi įsipareigojo dėl asmens duomenų panaudojimo, o darbuotojas ar profsąjunga kaltina darbdavį pažeidus šią sutartį. Komisija greičiausiai paliktų tai spręsti teismui ([1]).

Jurisdikcija dėl „seal“ programų

Antra, klausėte, ar FPK turi jurisdikciją dėl administruojančių ginčų sprendimo mechanizmus Jungtinėse Valstijose „seal“ programų, kurios nesugeba prižiūrėti „saugaus uosto“ principų vykdymo ir nagrinėti atskirų skundų, net jei tokios organizacijos techniškai yra „nesiekiančios pelno“. Spręsdama, ar mūsų jurisdikcija galioja organizacijai, kuri save laiko nesiekiančia pelno, Komisija atidžiai analizuoja, ar organizacija, nors nesiekia pelno sau, neprisideda prie savo narių pelno. Komisija sėkmingai taikė jurisdikciją tokioms organizacijoms, o 1999 m. gegužės 24 d. Jungtinių Valstijų Aukščiausiasis teismas byloje „Kalifornijos dantistų asociacija prieš Federalinę prekybos komisiją“ vienbalsiai patvirtino Komisijos jurisdikciją dėl vietinių dantistų bendrijų savanoriškos pelno nesiekiančios asociacijos svarstant antimonopolinius reikalus. Teismas nusprendė:

> FPK aktu stengiamasi aprėpti ne tik organizacijas, „suburtas vykdyti verslą siekiant pelno sau“ (15 U.S.C. § 44), bet ir tokias, kurios siekia pelno „savo nariams.“… Vargu, ar Kongresas numatė tokią ribotą pagalbines organizacijas aprėpiančią sąvoką, kuri suteiktų galimybę išvengti jurisdikcijos ten, kur FPK akto paskirtis būtų tą jurisdikciją taikyti.

Taigi tam, kad būtų nustatyta, ar jurisdikciją galima taikyti konkrečiai „pelno nesiekiančiai“ organizacijai, kuri prižiūri „seal“ programą, reikia išsiaiškinti, ar organizacija suteikė ekonominę naudą savo pelno siekiantiems nariams. Jei tokia organizacija vykdė „seal“ programą taip, kad suteikė ekonominę naudą savo nariams, FPK greičiausiai taikys savo jurisdikciją. Paminėtina atskirai, kad FPK galėtų taikyti jurisdikciją apgaulingai „seal“ programai, kuri teigia esanti pelno nesiekianti organizacija.

Privatumas realiajame (offline) pasaulyje

Trečia, pastebėjote, kad mūsų korespondencijoje sutelkėme dėmesį į privatumą interaktyviajame (*on-line*) pasaulyje. Nors interaktyvusis (*on-line*) privatumas yra didelis FPK rūpestis, nes yra svarbiausias elektroninės komercijos plėtros komponentas, FPK aktas priimtas 1914 m. ir vienodai galioja realiajame (*offline*) pasaulyje. Taigi mes galime teisiškai persekioti firmas, kurios užsiima nesąžininga ar apgaulinga prekybine veikla vartotojų privatumo atžvilgiu ([2]). Iš tiesų praėjusiais metais Komisijos byloje prieš „TouchTone Information, Inc.“ ([3]) „informacijos brokeris“ buvo apkaltintas neteisėtai gavęs ir pardavęs vartotojų privačią finansinę informaciją. Komisija apkaltino „TouchTone“ gavus vartotojų informaciją „pasinaudodama pretekstu“ (privačių seklių sukurtas specialus terminas, apibūdinantis asmeninės informacijos apie kitus gavimo būdą, kai nurodžius melagingą pretekstą telefonu gaunama informacija). 1999 m. balandžio 21 d. Kolorado federaliniam teismui pateiktame ieškinyje reikalaujama uždrausti veiklą ir grąžinti visą neteisėtai uždirbtą pelną.

Iš dalies sutampanti jurisdikcija

Jūs domėjotės FPK ir kitų teisės aktų vykdymo priežiūros institucijų jurisdikcijų sąveika, kai jos gali potencialiai iš dalies sutapti. Mes suformavome tamprius darbo santykius su daugeliu kitų teisės aktų vykdymo priežiūros institucijų,

([1]) Nustatyti, ar veiksmas yra „nesąžininga darbo praktika“, ar kolektyvinės sutarties pažeidimas patikima atlikti skundus nagrinėsiantiems specializuotiems darbo tribunolams, pvz., arbitrams ir NRLB.

([2]) Kaip žinote iš ankstesnių diskusijų, Sąžiningo kreditinių ataskaitų sudarymo aktas taip pat suteikia FPK įgaliojimus saugoti vartotojų finansinį privatumą Akto numatytose ribose, o Komisija neseniai paskelbė su šiuo klausimu susijusį sprendimą. Žr. „Trans Union“ bylą, įrašo Nr. 9255 (2000 m. kovo 1 d.) (pranešimą spaudai ir nuomonę galima rasti adresu: www.ftc.gov/os/2000/03/index.htm#1).

([3]) Civilinis ieškinys 99-WM-783 (D.Colo.) (galima rasti adresu: http://www.ftc.gov/opa/1999/9904/touchtone.htm) (laukiama preliminaraus pritariamojo sprendimo paskelbimo).

įskaitant federalines bankininkystės institucijas, ir valstijų generaliniais prokurorais. Mes dažnai koordinuojame tyrimus ir siekiame, kad mūsų pajėgos iš dalies sutampančios jurisdikcijos atvejais būtų kuo stipresnės. Neretai perduodame tirti bylas atitinkamoms federalinėms ar valstijų institucijoms.

Tikiuosi, ši apžvalga bus naudinga. Prašome pranešti, jei Jums reikėtų papildomos informacijos.

Nuoširdžiai,

Robertas Pitofskis

VI PRIEDAS

Johnui Moggui
Direktoriui, DG XV
Europos Komisija
Biuras C 107–6/72
Rue de la Loi/Wetstraat 200
B-1049 Briuselis

Gerbiamasis generalinis direktoriau Moggai,

Rašau Jums šį laišką JAV Komercijos departamento prašymu. Prašytume paaiškinti Transporto departamento vaidmenį saugant vartotojų privatumą, kai šie pateikia informaciją oro linijoms.

Transporto departamentas skatina savireguliaciją kaip mažiausiai įkyrų ir veiksmingiausią būdą užtikrinti vartotojų oro linijoms suteikiamos informacijos apsaugą ir todėl remia „saugaus uosto“ sistemos, kuri leistų oro linijoms laikytis Europos Sąjungos privatumo direktyvos reikalavimų dėl perdavimų už ES ribų, sukūrimą. Tačiau Departamentas pripažįsta, kad tam, jog savireguliacija veiktų, būtina, kad įsipareigojusios laikytis „saugaus uosto“ sistemos nustatytų privatumo principų, oro linijos iš tikrųjų jų laikytųsi. Todėl savireguliaciją reikėtų paremti teisės aktų vykdymo priežiūra. Taigi, pasinaudodamas turimais vartotojų apsaugos įstatyminiais įgaliojimais, Departamentas užtikrins, kad oro linijos laikytųsi visuomenei duotų įsipareigojimų dėl privatumo ir nagrinės pranešimus dėl kaltinimų nesilaikymu, kuriuos mes gauname iš savireguliacijos organizacijų ir kitur, įskaitant Europos Sąjungos valstybes nares.

Departamento įgaliojimai imtis teisės aktų vykdymo priežiūros veiksmų apibrėžti 49 U.S.C. 41712 skirsnyje, kuris draudžia vežėjams imtis „nesąžiningų ar apgaulingų veiksmų ar nesąžiningų konkurencijos būdų“ parduodant oro vežimų paslaugas, dėl ko nukenčia ar gali nukentėti vartotojai. 41712 skirsnis yra suformuluotas pagal Federalinės prekybos komisijos akto 5 skirsnį (15 U.S.C. 45). Tačiau oro vežėjams pagal 5 skirsnio nuostatas taikoma išimtis (15 U.S.C. 45(a)(2)).

Mano tarnyba tiria ir palaiko kaltinimą bylose pagal 49 U.S.C. 41712 skirsnį (žr., pvz., TD įsakymus: 1999 m. lapkričio 9 d., 99–11–5; 1999 m. rugpjūčio 23 d., 99–8–23; 1999 m. birželio 1 d., 99–6–1; 1999 m. birželio 22 d., 99–6–24; 1998 m. birželio 19 d., 98–6–21; 1998 m. gegužės 22 d., 98–5–31 ir 1997 m. gruodžio 18 d., 97–12–23). Mes tiriame tokias bylas remdamiesi nuosavais tyrimais ir oficialiais bei neoficialiais skundais, kuriuos gauname iš asmenų, kelionių agentų, oro linijų ir JAV bei užsienio Vyriausybinių institucijų.

Norėčiau pabrėžti, kad vežėjo nesugebėjimas išlaikyti iš keleivių gautos informacijos privatumo *per se* nebus 41712 skirsnio pažeidimu. Tačiau, jei vežėjas oficialiai ir viešai įsipareigoja laikytis „saugaus uosto“ principo ir užtikrinti jo gaunamą vartotojų informaciją, tuomet Departamentas turi teisę panaudoti 41712 skirsnio įstatyminius įgaliojimus užtikrinti tų principų laikymąsi. Todėl, jei keleivis suteikia informaciją vežėjui, kuris įsipareigojo laikytis „saugaus uosto“ principų, bet koks jų nesilaikymas greičiausiai pakenks vartotojui ir pažeis 41712 skirsnį. Mano tarnyba tirtų bet kokį kaltinimą dėl tokios veiklos ir pirmumo tvarka palaikytų kaltinimą bet kokioje byloje, jei būtų tokios veiklos požymių. Mes taip pat informuojame Komercijos departamentą apie visų tokių bylų rezultatus.

Dėl 41712 skirsnio pažeidimų gali būti išleistas veiklos sustabdymo ir nutraukimo įsakymas, o už jo pažeidimą baudžiama administracinėmis nuobaudomis. Nors mes neturime įgaliojimų priteisti nuostolius ar nurodyti atlyginti materialinę žalą atskiriems ieškovams, mes galime patvirtinti atsiskaitymus pagal Departamento atliktus tyrimus ir iškeltas bylas. Tokie atsiskaitymai yra naudingi vartotojams kaip nusižengimo prieš juos sušvelninimas ar kompensacija už šiaip mokamas pinigines baudas. Taip esame darę anksčiau ir darysime ateityje, kai aplinkybės leis taikyti „saugaus uosto“ principus. JAV oro linijai, kuri kelis kartus pažeidė 41712 skirsnį, gali būti skirta nepaklusnumo nuobauda, dėl kurios itin sunkiais atvejais oro linija gali būti pripažinta netinkama vykdyti veiklą ir todėl prarastų ekonominės veiklos licenciją (žr. TD įsakymus: 1993 m. birželio 23, 93–6–24; 1993 m. birželio 9, 93–6–11. Nors

šiame procese nebuvo kaltinimų pažeidus 41712 skirsnį, dėl visiško Federalinio aviacijos akto, dvišalės sutarties ir Departamento taisyklių bei nuostatų nesilaikymo iš vežėjo buvo atimta veiklos licencija).

Tikiuosi, kad ši informacija bus naudinga. Jei turite papildomų klausimų ar Jums reikia daugiau informacijos, prašome kreiptis į mane.

Nuoširdžiai,

Samuelis Podbereskis

Generalinio konsultanto padėjėjas
aviacijos priežiūros ir teismo procesų reikalams

VII PRIEDAS

Kaip numatyta 1 straipsnio 2 dalies b punkte, Jungtinių Valstijų Vyriausybinės institucijos, turinčios įgaliojimus tirti skundus ir naudoti teisių gynimo priemones prieš nesąžiningus ar apgaulingus veiksmus, taip pat ir atlyginti žalą asmenims nepriklausomai nuo šalies, kurioje jie gyvena, ar tautybės, jei nesilaikoma pagal FAQ vykdomų principų, yra tokios:

1) Federalinė prekybos komisija;

2) JAV Transporto departamentas.

Federalinė prekybos komisija veikia pagal Federalinės prekybos komisijos akto 5 skirsnio jai suteiktus įgaliojimus. Federalinės prekybos komisijos jurisdikcija pagal 5 skirsnį negalioja bankams, taupomiesiems bei kredito bankams ir kredito sąjungoms, telekomunikacijų paslaugų teikėjams, pervežimo tarp valstijų visuomeniniams vežėjams, oro vežėjams ir maisto produktų paruošimo ir galvijų paskirstymo įmonėms. Nors draudimo pramonė nėra konkrečiai įtraukta į 5 skirsnio išimčių sąrašą, McCarrano-Fergusono aktu reglamentuoti draudimo verslą dažniausiai paliekama atskiroms valstijoms ([1]). Tačiau FPK akto nuostatos taikomos toms draudimo pramonės sritims, kurių nereglamentuoja valstijų teisės aktai. FPK išlaiko liktinius įgaliojimus dėl draudimo kompanijų nesąžiningų ar apgaulingų veiksmų, kai jos neužsiima draudimo verslu.

JAV Transporto departamentas veikia pagal Jungtinių Valstijų Kodekso 41712 skirsnio 49 dalies jam suteiktus įgaliojimus. JAV Transporto departamentas tiria bylas vadovaudamasis nuosavais tyrimais ir oficialiais bei neoficialiais skundais, kuriuos gauna iš asmenų, kelionių agentų, oro linijų ir JAV bei užsienio Vyriausybinių institucijų.

([1]) 15 U.S.C. § 1011 *et seq*.