

II

(Ne teisėkūros procedūra priimami aktai)

SPRENDIMAI

KOMISIJOS ĮGYVENDINIMO SPRENDIMAS (ES) 2022/254

2021 m. gruodžio 17 d.

pagal Europos Parlamento ir Tarybos reglamentą (ES) 2016/679 dėl tinkamos asmens duomenų apsaugos Korėjos Respublikoje pagal Asmeninės informacijos apsaugos įstatymą

(pranešta dokumentu Nr. C(2021) 9316)

(Tekstas svarbus EEE)

EUROPOS KOMISIJA,

atsižvelgdama į Sutartį dėl Europos Sąjungos veikimo,

atsižvelgdama į 2016 m. balandžio 27 d. Europos Parlamento ir Tarybos reglamentą (ES) 2016/679 dėl fizinių asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo ir kuriuo panaikinama Direktyva 95/46/EB (Bendrasis duomenų apsaugos reglamentas) ⁽¹⁾, ypač į jo 45 straipsnio 3 dalį,

kadangi:

1. ĮVADAS

- (1) Reglamente (ES) 2016/679 nustatytos asmens duomenų perdavimo iš Sąjungoje įsikūrusių duomenų valdytojų arba duomenų tvarkytojų į trečiąsias valstybes ir tarptautinėms organizacijoms taisyklės, susijusios su tomis duomenų perdavimo operacijomis, kurioms taikomas minėtas reglamentas. Tarptautinio duomenų perdavimo taisyklės yra nustatytos to reglamento V skyriuje (44–50 straipsniuose). Nors asmens duomenų srautas į Europos Sąjungai nepriklausančias valstybes ir iš jų yra labai svarbus siekiant plėsti tarpvalstybinę prekybą ir tarptautinį bendradarbiavimą, Sąjungoje užtikrinamas asmens duomenų apsaugos lygis negali sumažėti perduodant duomenis į trečiąsias valstybes ⁽²⁾.
- (2) Pagal Reglamento (ES) 2016/679 45 straipsnio 3 dalį Komisija, priimdama įgyvendinimo aktą, gali nuspręsti, kad trečioji valstybė, teritorija arba vienas ar daugiau nurodytų sektorių toje trečiojoje valstybėje, arba tarptautinė organizacija užtikrina tinkamo lygio apsaugą. Tokiu atveju asmens duomenys į trečiąją valstybę gali būti perduodami nereikalaujant jokio papildomo leidimo, kaip nustatyta Reglamento (ES) 2016/679 45 straipsnio 1 dalyje ir 103 konstatuojamojoje dalyje.
- (3) Kaip nurodyta Reglamento (ES) 2016/679 45 straipsnio 2 dalyje, priimant sprendimą dėl tinkamumo, turi būti remiamasi išsamia trečiosios valstybės teisinės sistemos analize, susijusia ir su duomenų importuotojams taikomomis taisyklėmis, ir su apribojimais bei apsaugos priemonėmis, taikomomis valdžios institucijoms gaunant prieigą prie asmens duomenų. Savo vertinime Komisija privalo nustatyti, ar atitinkama trečioji valstybė garantuoja tokio lygio apsaugą, kuri yra „iš esmės lygiavertė“ Europos Sąjungoje užtikrinamai apsaugai (Reglamento (ES) 2016/679 104 konstatuojamoji dalis). Ar tai toks atvejis, turi būti vertinama pagal Sąjungos teisės aktus, visų pirma Reglamentą (ES) 2016/679, taip pat Europos Sąjungos Teisingumo Teismo praktiką ⁽³⁾.

⁽¹⁾ OL L 119, 2016 5 4, p. 1.

⁽²⁾ Žr. Reglamento (ES) 2016/679 101 konstatuojamąją dalį.

⁽³⁾ Žr. naujausią Sprendimą *Facebook Ireland* ir *Schrems*, C-311/18 (Sprendimas *Schrems II*), ECLI:EU:C:2020:559.

- (4) Kaip išaiškino Europos Sąjungos Teisingumo Teismas, pagal šią nuostatą nereikalaujama, kad apsauga būtų tokio paties lygio ⁽⁴⁾. Visų pirma, priemonės, kurių gali imtis atitinkama trečioji valstybė, siekdama apsaugoti asmens duomenis, gali skirtis nuo Sąjungoje taikomų priemonių, jeigu šios priemonės padeda veiksmingai užtikrinti praktinę tinkamo lygio apsaugą ⁽⁵⁾. Todėl pagal tinkamumo kriterijų nėra reikalaujama Sąjungos taisyklės atkartoti papunkčiui. Veikiau pagal šį kriterijų turi būti patikrinta, ar visoje užsienio valstybės sistemoje užtikrinamas reikiamas apsaugos lygis – teisių į privatumą esmė, veiksmingas jų įgyvendinimas, priežiūra ir vykdymo užtikrinimas ⁽⁶⁾. Europos duomenų apsaugos valdybos Orientaciniuose tinkamumo kriterijuose, kuriais siekiama išsamiau paaiškinti šį kriterijų, taip pat pateikiamos gairės šiuo klausimu ⁽⁷⁾.
- (5) Komisija atidžiai išanalizavo Korėjos teisės aktus ir praktiką. Remdamasi (8)–(208) konstatuojamosiose dalyse išdėstytomis išvadomis, Komisija daro išvadą, kad Korėjos Respublika užtikrina tinkamo lygio asmens duomenų, kuriuos Sąjungoje ⁽⁸⁾ veikiantis duomenų valdytojas arba tvarkytojas perduoda subjektams (pvz., fiziniams arba juridiniams asmenims, organizacijoms, viešosioms institucijoms) Korėjoje, kuriems taikomas Asmeninės informacijos apsaugos įstatymas (2011 m. kovo 29 d. Įstatymas Nr. 10465 su paskutiniais pakeitimais, padarytais 2020 m. vasario 4 d. Įstatymu Nr. 16930), apsaugą. Tai apima tiek duomenų valdytojus, tiek tvarkytojus (vadinamuosius „užsakomųjų paslaugų teikėjus“ ⁽⁹⁾), kaip apibrėžta Reglamente (ES) 2016/679. Išvada dėl tinkamumo netaikoma asmens duomenų tvarkymui, kai juos tvarko religinės organizacijos misionierių veiklos tikslais ir politinės partijos keldamos kandidatus, arba kai asmens kredito informaciją pagal Kredito informacijos įstatymą tvarko duomenų valdytojai, kuriuos prižiūri Finansinių paslaugų komisija.
- (6) Šioje išvadoje atsižvelgiama į papildomas apsaugos priemones, nustatytas pranešime Nr. 2021-5 (I priedas) ir Korėjos vyriausybės Komisijai pateiktus oficialius pareiškimus, garantijas ir išipareigojimus (II priedas).
- (7) Pagal šį sprendimą duomenys duomenų valdytojams ir tvarkytojams Korėjos Respublikoje gali būti perduoti be papildomo leidimo. Sprendimas neturi įtakos Reglamento (ES) 2016/679 tiesioginiam taikymui tokiems subjektams, kai tenkinamos teritorinės taikymo srities sąlygos, nustatytos to reglamento 3 straipsnyje.

2. ASMENS DUOMENŲ TVARKYMO TAIKOMOS TAISYKLĖS

2.1. Korėjos Respublikos duomenų apsaugos sistema

- (8) Teisinė sistema, kuria Korėjoje reglamentuojama privatumo ir duomenų apsauga, siejama su 1948 m. liepos 17 d. paskelbta Korėjos Konstitucija. Nepaisant to, kad teisė į asmens duomenų apsaugą Konstitucijoje nėra aiškiai nustatyta, ji pripažįstama pagrindine teise, kylančia iš konstitucinių teisių, kaip antai teisės į žmogaus orumą ir teisės siekti laimės (10 straipsnis), teisės į privatų gyvenimą (17 straipsnis) ir ryšių privatumą (18 straipsnis). Tai patvirtino ir Aukščiausiasis Teismas ⁽¹⁰⁾, ir Konstitucinis Teismas ⁽¹¹⁾. Pagrindinių teisių ir laisvių (įskaitant teisę į privatumą) apribojimai gali būti taikomi tik įstatymu, kai tai būtina nacionaliniam saugumui užtikrinti arba viešajai tvarkai palaikyti siekiant užtikrinti visuomenės gerovę, ir jie negali daryti poveikio atitinkamos teisės ar laisvės esmei (37 straipsnio 2 dalis).

⁽⁴⁾ Sprendimas *Maximilian Schrems* prieš *Data Protection Commissioner* (Sprendimas *Schrems*), C-362/14, ECLI:EU:C:2015:650, 73 punktą.

⁽⁵⁾ Sprendimas *Schrems*, 74 punktą.

⁽⁶⁾ Žr. 2017 m. sausio 10 d. Komisijos komunikato Europos Parlamentui ir Tarybai „Keitimasis asmens duomenimis ir jų apsauga globalizuotame pasaulyje“ (COM(2017) 7) 3.1 skirsnį, 6–7 p.

⁽⁷⁾ Europos duomenų apsaugos valdybos darbinį dokumentą „Orientaciniai tinkamumo kriterijai“ (WP 254, 1-oji peržiūreta versija) galima rasti šiuo adresu: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=614108

⁽⁸⁾ Šis sprendimas svarbus EEE. Europos ekonominės erdvės susitarime (toliau – EEE susitarimas) nustatyta, kad Europos Sąjungos vidaus rinkos taisyklės galioja trijose EEE valstybėse: Islandijoje, Lichtenšteine ir Norvegijoje. 2018 m. liepos 6 d. EEE jungtinis komitetas priėmė Jungtinio komiteto sprendimą, kuriuo Reglamentas (ES) 2016/679 buvo ištrauktas iš EEE susitarimo XI priedą. Šis sprendimas įsigaliojo 2018 m. liepos 20 d. Todėl ta sutartis apima Reglamentą. Šiame sprendime nuorodos į ES ir ES valstybes nares turėtų būti suprantamos kaip apimančios ir EEE valstybes.

⁽⁹⁾ Žr. šio sprendimo 2.2.3 skirsnį.

⁽¹⁰⁾ Žr., pavyzdžiui, 2015 m. spalio 15 d. Aukščiausiojo Teismo sprendimą 2014Da77970 (santrauka anglų kalba pateikiama adresu https://www.privacy.go.kr/eng/enforcement_01.do, spustelėjus nuorodą *Lawmaker's disclosure of teachers' trade union members case*) ir jame minimą teismų praktiką, įskaitant 2014 m. liepos 24 d. Sprendimą 2012Da49933.

⁽¹¹⁾ Žr. visų pirma 2005 m. gegužės 26 d. Konstitucinio Teismo sprendimą 99Hun-ma513 (santrauka anglų kalba pateikiama adresu <http://www.koreanlii.or.kr/w/index.php/99Hun-Ma513?ckattemp=2>) ir 2015 m. gruodžio 23 d. Sprendimą 2014JHun-ma449 2013 Hun-Ba68 (konsoliduota versija) (santrauka anglų kalba pateikiama adresu https://www.privacy.go.kr/eng/enforcement_01.do, spustelėjus nuorodą *Change of resident registration number case*).

- (9) Nepaisant to, kad skirtingose Konstitucijos vietose minimos Korėjos piliečių teisės, Konstitucinis Teismas nusprendė, kad pagrindinės teisės taikomos ir užsienio valstybių piliečiams⁽¹²⁾. Visų pirma Teismas pareiškė, kad teisė į žmogaus orumo ir vertės apsaugą, taip pat teisė siekti laimės yra ne tik piliečių, bet visų žmonių teisės⁽¹³⁾. Be to, remiantis Korėjos vyriausybės oficialiais pareiškimais⁽¹⁴⁾, visuotinai pripažįstama, kad Konstitucijos 12–22 straipsniuose nustatytos pagrindinės žmogaus teisės⁽¹⁵⁾, įskaitant teisę į privatumą. Nors kol kas nėra jokios teismų praktikos, susijusios konkrečiai su užsienio valstybių piliečių teise į privatumą, ši išvada grindžiama teise į žmogaus orumo apsaugą ir teise siekti laimės⁽¹⁶⁾.
- (10) Be to, Korėja priėmė keletą duomenų apsaugos srities įstatymų, kuriuose numatytos apsaugos priemonės visiems asmenims, neatsižvelgiant į jų pilietybę⁽¹⁷⁾. Šio sprendimo tikslais svarbūs šie įstatymai:
- Asmeninės informacijos apsaugos įstatymas (AIAI);
 - Kredito informacijos naudojimo ir apsaugos įstatymas⁽¹⁸⁾;
 - Ryšių privatumo apsaugos įstatymas.
- (11) AIAI nustatomas bendras duomenų apsaugos Korėjos Respublikoje teisinis pagrindas. Jis papildytas Vykdyto uztikrinimo dekretu (2011 m. rugsėjo 29 d. Prezidento dekretas Nr. 23169 su naujaisiais pakeitimais, padarytais 2020 m. rugpjūčio 4 d. Prezidento dekretu Nr. 30892) (AIAI vykdymo uztikrinimo dekretas), kuris, kaip ir AIAI, yra teisiškai privalomas ir vykdytinas.
- (12) Be to, Asmeninės informacijos apsaugos komisijos (AIAK) priimtuose norminiuose pranešimuose pateikiamos papildomos AIAI aiškinimo ir taikymo taisyklės. Remdamasi AIAI 5 straipsniu (Valstybės pareigos) ir 14 straipsniu (Tarptautinis bendradarbiavimas), 2020 m. rugsėjo 1 d. AIAK priėmė pranešimą Nr. 2021-1 (su pakeitimais, padarytais 2021 m. sausio 21 d. pranešimu Nr. 2021-1 ir 2021 m. lapkričio 16 d. pranešimu Nr. 2021-5 (pranešimas Nr. 2021-5)) dėl tam tikrų AIAI nuostatų aiškinimo, taikymo ir vykdymo uztikrinimo. Šiame pranešime pateikiami paaiškinimai, taikomi bet kokiam asmens duomenų tvarkymui pagal AIAI, taip pat papildomos apsaugos priemonės, taikomos pagal šį sprendimą Korėjai perduodamiems asmens duomenims. Pranešimas asmeninės informacijos valdytojams yra teisiškai privalomas, o jo vykdymą uztikrina ir AIAK, ir teismai⁽¹⁹⁾. Pažeidus pranešime nustatytas taisykles pažeidžiamos atitinkamos AIAI nuostatos, kurias jos papildo. Todėl papildomų apsaugos priemonių turinys analizuojamas vertinant atitinkamus AIAI straipsnius. Galiausiai papildomos gairės dėl AIAI ir jo Vykdyto uztikrinimo dekreto, kuriomis remdamasi AIAK taiko duomenų apsaugos taisykles ir uztikrina jų laikymąsi, pateikiamos AIAK priimtame AIAI vadove ir gairėse⁽²⁰⁾.

⁽¹²⁾ 1994 m. gruodžio 29 d. Konstitucinio Teismo sprendimas 93 Hun-MA120.

⁽¹³⁾ 2001 m. lapkričio 29 d. Konstitucinio Teismo sprendimas 99HeonMa494.

⁽¹⁴⁾ Žr. II priedo 1.1 skirsnį.

⁽¹⁵⁾ Taip pat žr. Asmeninės informacijos apsaugos įstatymo 1 straipsnį, kuriame aiškiai nurodomos „asmenų laisvės ir teisės“. Konkrečiau, jame teigiama, kad tokio įstatymo tikslas yra „užtikrinti asmeninės informacijos tvarkymą ir apsaugą siekiant apsaugoti asmenų laisvę ir teises, taip pat užtikrinti asmenų orumo ir vertės apsaugą“. Be to, Asmeninės informacijos apsaugos įstatymo 5 straipsnio 1 dalyje nustatyta valstybės pareiga „formuoti politiką, kuria siekiama užkirsti kelią žalingoms pasekmėms, kylančioms dėl didesnio, nei reikalinga, asmeninės informacijos kiekio rinkimo, piktnaudžiavimo ja ir neteisėto jos naudojimo, neteisėto sekimo ir persekiojimo ir t. t., ir didinti žmonių orumą bei asmens privatumo apsaugą“.

⁽¹⁶⁾ Be to, Konstitucijos 6 straipsnio 2 dalyje numatyta, kad užsienio valstybės piliečio teisės užtikrinamos vadovaujantis tarptautine teise ir sutartimis. Korėja yra kelių tarptautinių susitarimų, kuriais užtikrinama teisė į privatumą, kaip antai Tarptautinio pilietinių ir politinių teisių pakto (17 straipsnis), Neigaliųjų teisių konvencijos (22 straipsnis) ir Vaiko teisių konvencijos (16 straipsnis), šalis.

⁽¹⁷⁾ Tai apima su asmens duomenų apsauga susijusias taisykles, kurios netaikomos tais atvejais, kai asmens duomenys renkami Sąjungoje ir perduodami Korėjai pagal Reglamentą (ES) 2016/679, pavyzdžiui, taisykles, nustatytas Įstatyme dėl informacijos apie buvimą vietą apsaugos, naudojimo ir kt.

⁽¹⁸⁾ Šio įstatymo tikslas – skatinti patikimą kredito informacijos verslą, veiksmingą kredito informacijos naudojimą ir sistemingą valdymą, apsaugoti privatumą nuo grėsmių, kylančių dėl netinkamo kredito informacijos naudojimo ir piktnaudžiavimo ja (įstatymo 1 straipsnis).

⁽¹⁹⁾ Pavyzdžiui, Korėjos teismai keliose bylose priėmė sprendimus dėl teisės aktuose nustatytų pranešimų laikymosi, be kita ko, pripažindami Korėjos duomenų valdytojus atsakingais už pranešimo pažeidimus (žr., pvz., 2018 m. spalio 25 d. Aukščiausiojo Teismo sprendimą 2018Da219406, kuriuo Teismas nurodė duomenų valdytojui atlyginti žalą asmenims, patirtą dėl „Pranešimo dėl asmeninės informacijos saugumo uztikrinimo priemonių standarto“ pažeidimo; taip pat žr. 2018 m. spalio 25 d. Aukščiausiojo Teismo sprendimą 2018Da219352; 2016 m. gegužės 16 d. Aukščiausiojo Teismo sprendimą 2011Da24555; 2016 m. spalio 13 d. Seulo centrinio apylinkės teismo sprendimą 2014Gahap511956; 2010 m. sausio 26 d. Seulo centrinio apylinkės teismo sprendimą 2009Gahap43176.

⁽²⁰⁾ AIAI 12 straipsnio 1 dalis.

- (13) Be to, Kredito informacijos naudojimo ir apsaugos įstatyme (KIĮ) nustatytos specialios taisyklės, taikomos ir įprastiems komercinės veiklos vykdytojams, ir specializuotiems finansų sektoriaus subjektams, jiems tvarkant asmeninę kredito informaciją, t. y. informaciją, būtiną finansinių ar komercinių sandorių šalių kreditingumui nustatyti. Tokia informacija visų pirma apima vardą ir pavardę, kontaktinius duomenis, finansinius sandorius, kredito reitingą, draustumą arba paskolų balansą, kai tokia informacija naudojama asmens kreditingumui nustatyti⁽²¹⁾. Priešingai, kai tokia informacija naudojama kitais tikslais (pvz., žmogiškųjų išteklių tikslais), taikomas visas AIAĮ. Konkrečių KIĮ duomenų apsaugos nuostatų laikymąsi iš dalies prižiūri AIAK (komercinių organizacijų atveju žr. KIĮ 45-3 straipsnį) ir iš dalies Finansinių paslaugų komisija⁽²²⁾ (finansų sektoriaus, įskaitant kredito reitingų agentūras, bankus, draudimo bendroves, savitarpio taupomuosius bankus, specializuotas kredito finansų bendroves, finansinių investicijų paslaugų bendroves, vertybinių popierių finansų bendroves, kredito unijas ir t. t., atveju žr. KIĮ 45 straipsnio 1 dalį kartu su KIĮ vykdymo užtikrinimo dekreto 36-2 straipsniu ir Finansinių paslaugų komisijos įstatymo 38 straipsniu). Šiuo atžvilgiu šis sprendimas taikomas tik komercinės veiklos vykdytojams, kuriuos prižiūri AIAK⁽²³⁾. Šiomis aplinkybėmis taikomos konkrečios KIĮ taisyklės (bendrosios AIAĮ taisyklės taikomos tada, kai nėra taikytinų konkrečių taisyklių), aprašytos 2.3.11 skirsnyje.

2.2. AIAĮ materialinė taikymo sritis ir taikymo sritis asmenų atžvilgiu

- (14) Išskyrus atvejus, kai kituose įstatymuose konkrečiai numatyta kitaip, asmens duomenų apsauga reglamentuojama AIAĮ (6 straipsnyje). Materialinė taikymo sritis ir taikymo sritis asmenų atžvilgiu nustatomos pagal sąvokų „asmeninė informacija“, „duomenų tvarkymas“ ir „asmeninės informacijos valdytojas“ apibrėžtis.

2.2.1. Asmens duomenų apibrėžtis

- (15) AIAĮ 2 straipsnio 1 dalyje asmeninė informacija apibrėžiama kaip su gyvu asmeniu susijusi informacija, kuria remiantis galima nustatyti asmens tapatybę tiesiogiai, pavyzdžiui, jo vardas, pavardė, gyventojų registracijos numeris arba atvaizdas, arba netiesiogiai, t. y. kai informacija, kuria remiantis savaime negalima nustatyti tam tikro asmens tapatybės, šiuo tikslu gali būti derinama su kita informacija. Tai, ar informacija gali būti lengvai derinama su kita informacija, priklauso nuo to, ar toks derinys yra pagrįstai tikėtinas, atsižvelgiant į galimybę gauti kitą informaciją, taip pat į laiką, sąnaudas ir technologijas, kurių reikia asmens tapatybei nustatyti.
- (16) Be to, informacija, kuriai suteikti pseudonimai, t. y. informacija, kuria remiantis negalima nustatyti konkretaus asmens tapatybės, jei ji nenaudojama arba nederinama su papildoma informacija, kad būtų atkurta pradinė jos būklė, pagal AIAĮ laikoma asmens duomenimis (AIAĮ 2 straipsnio 1 dalies c punktas). Tačiau visiškai nuasmeninta informacija nepatenka į AIAĮ taikymo sritį (AIAĮ 58-2 straipsnis). Tai informacija, kuria remiantis konkretaus asmens tapatybę negali būti nustatyta, net jei ji derinama su kita informacija, atsižvelgiant į laiką, sąnaudas ir technologijas, kurių pagrįstai reikia tapatybei nustatyti.
- (17) Tai atitinka Reglamento (ES) 2016/679 materialinę taikymo sritį ir jo sąvokas „asmens duomenys“, „pseudonimų suteikimas“⁽²⁴⁾ ir „nuasmeninta informacija“⁽²⁵⁾.

⁽²¹⁾ KIĮ 2 straipsnio 1 dalis.

⁽²²⁾ Finansinių paslaugų komisija yra Korėjos finansų sektoriaus priežiūros institucija, kuri taip pat užtikrina KIĮ įgyvendinimą.

⁽²³⁾ Jei ateityje tai pasikeistų, pvz., išplečiant AIAK jurisdikciją, kad ji apimtų visą asmeninės kredito informacijos tvarkymą pagal KIĮ, būtų galima apsvaistyti galimybę iš dalies pakeisti sprendimą dėl tinkamumo, kad jis taip pat apimtų subjektus, kuriuos šiuo metu prižiūri Finansinių paslaugų komisija.

⁽²⁴⁾ Pagal AIAĮ „duomenų tvarkymas suteikiant pseudonimus“ – tai duomenų tvarkymas, pavyzdžiui, iš dalies ištrinant asmens duomenis arba iš dalies ar visiškai pakeičiant asmens duomenis taip, kad joks konkretus asmuo negalėtų būti atpažįstamas be papildomos informacijos (AIAĮ 2 straipsnio 1–2 dalys). Tai atitinka pseudonimų suteikimo apibrėžtį, pateiktą Reglamento (ES) 2016/679 4 straipsnio 5 dalyje, kurioje nurodoma, kad tai „asmens duomenų tvarkymas taip, kad asmens duomenys nebegalėtų būti priskirti konkrečiam duomenų subjektui nesinaudojant papildoma informacija, jeigu tokia papildoma informacija yra saugoma atskirai ir jos atžvilgiu taikomos techninės bei organizacinės priemonės siekiant užtikrinti asmens duomenų nepriskyrimą fiziniam asmeniui, kurio tapatybę yra nustatyta arba kurio tapatybę galima nustatyti“.

⁽²⁵⁾ Konkrečiai Reglamento (ES) 2016/679 26 konstatuojamojoje dalyje paaiškinama, kad reglamentas netaikomas nuasmenintai informacijai, t. y. informacijai, kuri nėra susijusi su fiziniu asmeniu, kurio tapatybę nustatyta arba gali būti nustatyta, o tai priklauso nuo visų priemonių, kurias asmens tapatybei tiesiogiai ar netiesiogiai nustatyti, pagrįstai tikėtina, galėtų naudoti duomenų valdytojas ar kitas asmuo. Įsitikinant, ar tokios priemonės, pagrįstai tikėtina, galėtų būti naudojamos, reikėtų atsižvelgti į visus objektyvius veiksnius, pavyzdžiui, sąnaudas ir laiko trukmę, kurių prireiktų tapatybei nustatyti, turint omenyje duomenų tvarkymo metu turimas technologijas bei technologinę plėtrą.

2.2.2. Sąvokos „duomenų tvarkymas“ apibrėžtis

- (18) Sąvoka „duomenų tvarkymas“ AIAI plačiai apibrėžiama kaip apimanti „duomenų rinkimą, generavimą, jungimą, susiejimą, įrašymą, saugojimą, laikymą, apdorojimą kuriant pridėtinę vertę, redagavimą, paiešką, išvedimą, taisymą, atkūrimą, naudojimą, teikimą ir atskleidimą, asmeninės informacijos sunaikinimą ir kitą panašią veiklą“⁽²⁶⁾. Nors tam tikros AIAI nuostatos susijusios tik su konkrečiomis duomenų tvarkymo rūšimis, pavyzdžiui, naudojimu, teikimu arba rinkimu⁽²⁷⁾, sąvoka „naudojimas“ suprantama kaip apimanti bet koki duomenų tvarkymą, išskyrus rinkimą arba teikimą (trečiajai šaliai). Taip plačiai aiškinant sąvoką „naudojimas“ užtikrinama, kad nebūtų apsaugos spragų, susijusių su konkrečia duomenų tvarkymo veikla. Todėl duomenų tvarkymo sąvoka atitinka duomenų tvarkymo sąvoką pagal Reglamentą (ES) 2016/679.

2.2.3. Asmeninės informacijos valdytojas ir „užsakomųjų paslaugų teikėjas“

- (19) AIAI taikomas asmeninės informacijos valdytojams (duomenų valdytojais). Panašiai kaip ir Reglamente (ES) 2016/679, jais gali būti laikomos bet kokios viešosios institucijos, juridiniai asmenys, organizacijos ar fiziniai asmenys, kurie tiesiogiai arba netiesiogiai tvarko asmens duomenis, kad galėtų naudotis asmens duomenų rinkmenomis vykdydami savo veiklą⁽²⁸⁾. Šiomis aplinkybėmis asmeninės informacijos rinkmena – tai „bet koks asmeninės informacijos rinkinys ar rinkiniai, tam tikrų taisyklių pagrindu sistemingai sutvarkyti arba surūšiuoti, kad asmeninė informacija būtų lengvai pasiekiamą“ (AIAI 2 straipsnio 4 dalis)⁽²⁹⁾. Duomenų valdytojas privalo užtikrinti vidinius mokymus su duomenų tvarkymu susijusiems, jam pavaldiems asmenims, pvz., bendrovės pareigūnams arba darbuotojams, ir vykdyti tinkamą kontrolę ir priežiūrą (AIAI 28 straipsnio 1 dalis).
- (20) Kai duomenų valdytojas (užsakomųjų paslaugų gavėjas) perduoda asmens duomenų tvarkymą trečiajai šaliai (užsakomųjų paslaugų teikėjui), taikomos specialios prievolės. Visų pirma užsakomosios paslaugos turi būti reglamentuojamos teisiškai privalomu susitarimu (paprastai sutartimi)⁽³⁰⁾, kuriame būtų nustatyta užsakomųjų darbų apimtis, duomenų tvarkymo tikslas, taikytinos techninės ir valdymo apsaugos priemonės, duomenų valdytojo vykdoma priežiūra, atsakomybė (pavyzdžiui, žalos, patirtos pažeidus sutartinius įsipareigojimus, atlyginimas), taip pat bet kokios duomenų tvarkymo subrangos apribojimai⁽³¹⁾ (AIAI 26 straipsnio 1 ir 2 dalys kartu su Vykdyto užtikrinimo dekretu 28 straipsnio 1 dalimi)⁽³²⁾.
- (21) Be to, duomenų valdytojas turi skelbti ir nuolat atnaujinti informaciją apie užsakomąjį darbą ir užsakomųjų paslaugų teikėjo tapatybę arba, jei užsakomasis duomenų tvarkymas yra susijęs su tiesioginės rinkodaros veikla, tiesiogiai informuoti asmenis jiems pateikdamas atitinkamą informaciją (AIAI 26 straipsnio 2 ir 3 dalys kartu su Vykdyto užtikrinimo dekretu 28 straipsnio 2–5 dalimis)⁽³³⁾.
- (22) Pagal AIAI 26 straipsnio 4 dalį kartu su Vykdyto užtikrinimo dekretu 28 straipsnio 6 dalimi duomenų valdytojas taip pat privalo mokyti užsakomųjų paslaugų teikėją, kaip imtis būtinų saugumo priemonių, ir jį prižiūrėti, be kita ko, tikrinamas, ar jis laikosi visų duomenų valdytojo įsipareigojimų pagal AIAI⁽³⁴⁾ ir įsipareigojimų pagal užsakomųjų paslaugų sutartį. Kai užsakomųjų paslaugų teikėjas pažeidęs AIAI padaro žalą, atsakomybė dėl jo veiksmų ar veiksmų nesiėmimo priskiriama duomenų valdytojui, taip pat kaip ir darbuotojo padarytos žalos atveju (AIAI 26 straipsnio 6 dalis).

⁽²⁶⁾ AIAI 2 straipsnio 2 dalis.

⁽²⁷⁾ Pavyzdžiui, AIAI 15–19 straipsniuose minimas tik asmeninės informacijos rinkimas, naudojimas ir teikimas.

⁽²⁸⁾ AIAI 2 straipsnio 5 dalis. Viešosios institucijos, kaip jos apibrėžtos AIAI, apima visus centrinius administracinius departamentus ar agentūras ir su jomis susijusias įstaigas, vietos valdžios institucijas, mokyklas ir vietos valdžios valdomas viešąsias bendroves, Nacionalinės Asamblėjos ir teisminių institucijų administracinius organus (įskaitant Konstitucinį Teismą) (AIAI 2 straipsnio 6 dalis kartu su AIAI vykdyto užtikrinimo dekretu 2 straipsniu).

⁽²⁹⁾ Tai atitinka Reglamento (ES) 2016/679 materialinę taikymo sritį. Pagal Reglamento (ES) 2016/679 2 straipsnio 1 dalį, reglamentas taikomas „asmens duomenų tvarkymui, visiškai arba iš dalies atliekamam automatizuotomis priemonėmis, ir asmens duomenų, kurie sudaro susisteminto rinkinio dalį ar yra skirti ją sudaryti, tvarkymui ne automatizuotomis priemonėmis“. Reglamento (ES) 2016/679 4 straipsnio 6 dalyje susistemintas rinkinys apibrėžiamas kaip „bet kuris susistemintas pagal specialius kriterijus prieinamų asmens duomenų rinkinys“. Atitinkamai 15 konstatuojamojoje dalyje aiškinama, kad asmenų apsauga turėtų būti taikoma „asmens duomenis tvarkant tiek automatizuotomis priemonėmis, tiek rankiniu būdu, jeigu asmens duomenys laikomi arba juos ketinama laikyti susistemintame rinkinyje. Šis reglamentas neturėtų būti taikomas pagal specialius kriterijus nesusistemintiems rinkiniams ar jų grupėms, taip pat jų tituliniais lapams.“

⁽³⁰⁾ Žr. AIAI Vadovo III skyriaus 2 dalį dėl 26 straipsnio (p. 203–212), kurioje aiškinama, kad AIAI 26 straipsnio 1 dalyje nurodyti privalomi susitarimai, kaip antai sutartys arba panašūs susitarimai.

⁽³¹⁾ Pagal AIAI 26 straipsnio 5 dalį duomenų tvarkytojui draudžiama naudoti bet kokią asmeninę informaciją, kuri nepatenka į užsakomojo darbo sritį, arba teikti asmeninę informaciją trečiajai šaliai. Pagal AIAI 71 straipsnio 2 dalį už šio reikalavimo nesilaikymą gali būti taikoma baudžiamoji sankcija.

⁽³²⁾ Už šio reikalavimo nesilaikymą gali būti taikoma bauda, žr. AIAI 75 straipsnio 4 dalies 4 punktą.

⁽³³⁾ Už šio reikalavimo nesilaikymą gali būti taikoma bauda, žr. AIAI 75 straipsnio 2 dalies 1 punktą ir 4 dalies 5 punktą.

⁽³⁴⁾ Taip pat žr. AIAI 26 straipsnio 7 dalį, pagal kurią 15–25, 27–31, 33–38 straipsniai ir 50 straipsnis duomenų tvarkytojui taikomi *mutatis mutandis*.

- (23) Nors dėl to duomenų valdytojų ir duomenų tvarkytojų sąvokos AIAI neatskiriamos, užsakomųjų paslaugų taisyklėse numatytos prievolės ir apsaugos priemonės iš esmės yra lygiavertės toms, kuriomis reglamentuojami duomenų valdytojų ir duomenų tvarkytojų santykiai pagal Reglamentą (ES) 2016/679.

2.2.4. Specialios nuostatos dėl informacijos ir ryšių paslaugų teikėjų

- (24) Nors AIAI taikomas bet kurio duomenų valdytojo atliekamam asmens duomenų tvarkymui, tam tikrose nuostatose yra konkrečių taisyklių (*lex specialis*) dėl informacijos ir ryšių paslaugų teikėjų tvarkomų naudotojų asmens duomenų⁽³⁵⁾. Naudotojų sąvoka apima asmenis, kurie naudojami informacijos ir ryšių paslaugomis (Informacijos ir ryšių tinklų naudojimo ir duomenų apsaugos skatinimo įstatymo (Tinklų įstatymas) 2 straipsnio 1 dalies 4 punktas). Kad asmuo būtų naudotojas, jis turi naudotis tiesiogiai Korėjos telekomunikacijų operatoriaus teikiama telekomunikacijų paslaugomis arba informacijos paslaugomis⁽³⁶⁾, kurias komerciniais tikslais (t. y. siekdamas pelno) teikia subjektas, kuris teikdamas paslaugas savo ruožtu naudojami telekomunikacijų operatoriaus, turinčio licenciją arba įregistruoto Korėjoje, paslaugomis⁽³⁷⁾. Abiem atvejais konkrečios AIAI nuostatos taikomos tam subjektui, kuris internetinę paslaugą asmeniui (t. y. naudotojui) siūlo tiesiogiai.
- (25) Tačiau tinkamumo išvada susijusi tik su asmens duomenų, kuriuos duomenų valdytojas ir (arba) duomenų tvarkytojas Sąjungoje perduoda subjektui trečiojoje valstybėje (šiuo atveju Korėjos Respublikoje) apsaugos lygiu. Tokiu atveju fiziniai asmenys Sąjungoje paprastai yra tiesiogiai susiję tik su duomenų eksportuotoju Sąjungoje, bet ne su Korėjos informacijos ir ryšių paslaugų teikėju⁽³⁸⁾. Todėl jei konkrečios AIAI nuostatos dėl informacijos ir ryšių paslaugų naudotojų asmens duomenų bus taikomos, tai tik tam tikrais atvejais pagal šį sprendimą perduodamiems asmens duomenims.

2.2.5. Tam tikrų AIAI nuostatų netaikymas

- (26) Pagal AIAI 58 straipsnio 1 dalį, dalis AIAI (t. y. 15–57 straipsniai) netaikoma keturių duomenų tvarkymo kategorijų atveju⁽³⁹⁾. Visų pirma netaikomos AIAI dalys, kuriose nagrinėjami konkretūs duomenų tvarkymo pagrindai, tam tikros duomenų apsaugos prievolės, išsamios naudojimosi individualiomis teisėmis taisyklės, taip pat taisyklės, kuriomis reglamentuojami Tarpininkavimo ginčiuose dėl asmeninės informacijos komiteto sprendžiami ginčai. Kitos pagrindinės AIAI nuostatos yra taikomos, visų pirma bendrosios nuostatos dėl duomenų apsaugos principų (AIAI 3 straipsnis), įskaitant, pavyzdžiui, teisėtumo, tikslo nustatymo ir tikslo apribojimo, duomenų kiekio mažinimo, duomenų tikslumo ir saugumo principus, ir individualių teisių (prieigos, ištaisymo, ištrynimo ir sustabdymo, žr. AIAI 4 straipsnį). Be to, AIAI 58 straipsnio 4 dalyje nustatytos konkrečios prievolės, susijusios su tokia duomenų tvarkymo veikla, t. y. duomenų kiekio mažinimo, riboto duomenų saugojimo, saugumo priemonių užtikrinimo ir skundų nagrinėjimo prievolės⁽⁴⁰⁾. Todėl asmenys vis tiek galėtų pateikti skundą AIK, jei šių principų ir prievolių būtų nesilaikoma, o reikalavimų nesilaikymo atveju AIK būtų įgalios imtis vykdymo užtikrinimo veiksmų.

⁽³⁵⁾ Žr. visų pirma AIAI 18 straipsnio 2 dalį ir VI skyrių.

⁽³⁶⁾ Informacijos paslaugos apima ir informacijos teikimą, ir tarpininkavimo paslaugas teikiant informaciją.

⁽³⁷⁾ Žr. Tinklų įstatymo 2 straipsnio 1 dalies 3 punktą (kartu su 2 straipsnio 1 dalies 2 ir 4 punktais) ir Telekomunikacijų įmonių įstatymo 2 straipsnio 6 ir 8 dalis.

⁽³⁸⁾ Jei Korėjos informacijos ir ryšių paslaugų teikėjai turėtų tiesioginių ryšių su fiziniiais asmenimis ES (siūlydami jiems internetines paslaugas), Reglamentas (ES) 2016/679 galėtų būti tiesiogiai taikomas pagal jo 3 straipsnio 2 dalies a punktą.

⁽³⁹⁾ Be to, AIAI 58 straipsnio 2 dalyje nustatyta, kad 15 ir 22 straipsniai, 27 straipsnio 1 ir 2 dalys, 34 ir 37 straipsniai netaikomi asmens duomenims, tvarkomiems naudojant atvirose vietose įrengtus ir veikiančius vaizdo duomenų apdorojimo įrenginius. Kadangi ši nuostata susijusi su stebėjimu vaizdo kameromis Korėjoje, t. y. su tiesioginiu asmeninės informacijos rinkimu iš asmenų Korėjoje, ji nėra svarbi šio sprendimo, taikomo ES duomenų valdytojų ir (arba) duomenų tvarkytojų subjektams Korėjoje perduodamiems asmens duomenims, tikslu. Be to, pagal AIAI 58 straipsnio 3 dalį 15 straipsnis (asmeninės informacijos rinkimas ir naudojimas), 30 straipsnis (įpareigojimas nustatyti visuomenės privatumo politiką) ir 31 straipsnis (pareiga paskirti privatumo apsaugos pareigūną) netaikomi asmeninei informacijai, kurią tvarko draugystės skatinimo tikslais veikiančios grupės ar asociacijos (pvz., pomėgių klubai). Kadangi tokios grupės yra asmeninio pobūdžio ir nesusijusios su profesine ar komercine veikla, norint rinkti ir naudoti asmenų informaciją šiomis aplinkybėmis nereikia jokio konkretaus teisinio pagrindo (pvz., dalyvaujančių asmenų sutikimo). Tačiau visos kitos AIAI nuostatos yra taikomos (pvz., susijusios su duomenų kiekio mažinimu, tikslo apribojimu, tvarkymo teisėtumu, saugumu ir asmens teisėmis). Be to, išimtis nebūtų taikoma, jei asmeninė informacija būtų tvarkoma viršijant socialinės grupės sukūrimo tikslą.

⁽⁴⁰⁾ Konkrečiau, AIAI 58 straipsnio 4 dalyje nustatyta prievolė tvarkyti tokį asmeninės informacijos kiekį, kuris yra būtinas numatytam tikslui pasiekti, ją tvarkyti minimalų laikotarpį ir imtis būtinų priemonių, kad tokia asmeninė informacija būtų saugiai administruojama ir tinkamai tvarkoma. Tokios priemonės apima technines, valdymo ir fizines apsaugos priemones, taip pat priemones, kuriomis užtikrinamas tinkamas individualių skundų nagrinėjimas.

- (27) Pirma, dalinė išimtis taikoma asmens duomenims, surinktiems pagal Statistikos įstatymą, kad juos tvarkytų viešosios institucijos. Remiantis iš Korėjos vyriausybės gautais paaiškinimais, šiomis aplinkybėmis tvarkomi asmens duomenys paprastai yra susiję su Korėjos piliečiais, o duomenys apie užsienio valstybių piliečius gali būti įtraukti tik išskirtiniais atvejais, t. y. kai tie duomenys susiję su atvykimu į šalies teritoriją ir išvykimu iš jos arba užsienio investicijomis. Tačiau net ir tokiais atvejais tokie duomenys paprastai nėra perduodami Sąjungos duomenų valdytojų ir (arba) duomenų tvarkytojų, bet būtų tiesiogiai renkami Korėjos valdžios institucijų⁽⁴¹⁾. Be to, panašiai, kaip numatyta Reglamento (ES) 2016/679 162 konstatuojamojoje dalyje, duomenų tvarkymui pagal Statistikos įstatymą taikomos kelios sąlygos ir apsaugos priemonės. Visų pirma Statistikos įstatyme nustatyti konkretūs įpareigojimai, kaip antai užtikrinti tikslumą, nuoseklumą ir nešališkumą; garantuoti asmenų konfidencialumą; apsaugoti statistinių užklausų respondentų pateiktą informaciją, be kita ko, siekiant užkirsti kelią tokios informacijos naudojimui kitais nei statistikos rengimo tikslais, ir taikant konfidencialumo reikalavimus darbuotojams⁽⁴²⁾. Statistinius duomenis tvarkančios valdžios institucijos taip pat turi laikytis, *inter alia*, duomenų kiekio mažinimo, tikslo apribojimo ir saugumo principų (AIAĮ 3 straipsnis ir 58 straipsnio 4 dalis) ir leisti asmenims naudotis savo (susipažinimo su informacija, jos ištaisymo, ištyrimo ir rinkimo sustabdymo žr. AIAĮ 4 straipsnį) teisėmis. Galiausiai duomenys turi būti tvarkomi nuasmeninta forma arba suteikus pseudonimus, jei tai leidžia pasiekti duomenų tvarkymo tikslą (AIAĮ 3 straipsnio 7 dalis).
- (28) Antra, AIAĮ 58 straipsnio 1 dalyje nurodomi asmens duomenys, surinkti arba prašomi surinkti, kad būtų galima analizuoti su nacionaliniu saugumu susijusią informaciją. Šios dalinės išimties taikymo sritis ir pasekmės išsamiau aprašytos (149) konstatuojamojoje dalyje.
- (29) Trečia, dalinė išimtis taikoma laikinam asmens duomenų tvarkymui, kai tai skubiai būtina dėl viešojo saugumo, įskaitant visuomenės sveikatą, priešasčių. Šią kategoriją AIAK aiškina griežtai ir, remiantis gauta informacija, ji niekada nebuvo naudojama. Ji taikoma tik tais atvejais, kai reikia imtis skubių veiksmų, pavyzdžiui, siekiant nustatyti infekcijų sukėlėjus arba gelbėti stichinių nelaimių aukas ir joms padėti⁽⁴³⁾. Net ir tokiais atvejais dalinė išimtis taikoma tik asmens duomenų tvarkymui ribotą laikotarpį, kurio reikia tokiam veiksmui atlikti. Galimybės susidaryti situacijai, kurioje ši išimtis galėtų būti taikoma duomenų perdavimui, kuriam taikomas šis sprendimas, yra dar labiau ribotos, nes mažai tikėtina, kad asmens duomenys, iš Sąjungos perduodami Korėjos ekonominės veiklos vykdytojams, būtų tokio pobūdžio, kad dėl tokių ekstremaliųjų situacijų jų tolesnis tvarkymas galėtų būti skubiai būtinas.
- (30) Galiausiai dalinė išimtis taikoma duomenims, kuriuos surenka ir naudoja spaudos subjektai, religinės organizacijos misionierių veiklos tikslu arba politinės partijos kandidatų kėlimo tikslu. Išimtis taikoma tik tada, kai spaudos subjektai, religinės organizacijos arba politinės partijos asmens duomenis tvarko tais konkrečiais tikslais (t. y. žurnalistinei, misionierių veiklai vykdyti ir politinei kandidatūrai kelti). Kai tie subjektai asmens duomenis tvarko kitais tikslais, pavyzdžiui, žmogiškųjų išteklių valdymo ar vidaus administravimo tikslais, AIAĮ taikomas visas.
- (31) Kai spaudos subjektai asmens duomenis tvarko vykdydami žurnalistinę veiklą, pusiausvyra tarp saviraiškos laisvės ir kitų teisių (įskaitant teisę į privatumą) nustatyta Įstatymu dėl arbitražo, teisių gynimo ir kitų priemonių, kai žala padaroma spaudos pranešimais (Spaudos įstatymas)⁽⁴⁴⁾. Visų pirma Spaudos įstatymo 5 straipsnyje nustatyta, kad

⁽⁴¹⁾ Šiuo atžvilgiu Statistikos įstatymo 33 straipsnyje reikalaujama, kad viešosios institucijos apsaugotų statistinių užklausų respondentų pateikiamą informaciją, be kita ko, siekdamas užkirsti kelią tokios informacijos naudojimui kitais nei statistikos rengimo tikslais.

⁽⁴²⁾ Statistikos įstatymo 2 straipsnio 2 ir 3 dalys, 30 straipsnio 2 dalis, 33 ir 34 straipsniai.

⁽⁴³⁾ AIAĮ vadovo skyrius dėl 58 straipsnio.

⁽⁴⁴⁾ Pavyzdžiui, Spaudos įstatymo 4 straipsnyje nustatyta, kad spaudos pranešimai turi būti nešališki ir objektyvūs, grindžiami viešojo interesu, jais turi būti gerbiamas žmogaus orumas ir vertė, negali būti šmeižiami kiti asmenys ir negali būti pažeidžiamos jų teisės, prieštaraujama viešajai moralei ar socialinei etikai.

spaudos subjektas (t. y. bet kuri transliuojančioji organizacija, laikraštis, periodinis leidinys ar internetinis laikraštis), interneto naujienų tarnyba ar transliuojančioji interneto multimedijos organizacija negali pažeisti asmenų teisės į privatumą. Jei teisė į privatumą vis dėlto pažeidžiama, žala turi būti nedelsiant ištaisyta taikant konkrečias įstatyme nustatytas procedūras. Tokiais atvejais asmenims, patyrusiems žalą dėl spaudos pranešimo, įstatymu suteikiamos tam tikros teisės, pavyzdžiui, teisė reikalauti ištaisyti klaidingą pareiškimą ir jį paskelbti, jį ištaisyti paskelbiant paneigiantį pareiškimą arba naują pareiškimą (kai spaudos pranešimas susijęs su įtarimais dėl nusikaltimų, dėl kurių asmuo vėliau išteisinamas) ⁽⁴⁵⁾. Asmenų pretenzijos gali būti sprendžiamos pačių spaudos subjektų (jiems pasitelkiant ombudsmeną) ⁽⁴⁶⁾, taikinimo arba arbitražo būdu (vykdo specializuota spaudos arbitražo komisija) ⁽⁴⁷⁾ arba teismuose. Asmenys taip pat gali gauti kompensaciją, kai dėl neteisėto spaudos subjekto veiksmo (atlikto tyčia arba dėl aplaidumo) jie patiria piniginę žalą, pažeidžiamos jų asmeninės teisės arba sukeliamas bet kokia kita emocinė kančia ⁽⁴⁸⁾. Spaudos subjektai atleidžiami nuo įstatymu nustatytos atsakomybės, jei pranešimu spaudai, kuriuo pažeidžiamos asmens teisės, neprieštarujama socialinėms vertybėms ir jis skelbiamas gavus suinteresuoto asmens sutikimą arba viešojo intereso tikslu (o pagrindas manyti, kad pranešimas atitinka tiesą, yra pakankamas) ⁽⁴⁹⁾.

- (32) Nors spaudos subjektų vykdomam asmens duomenų tvarkymui vykdam žurnalistinę veiklą taikomos specialios apsaugos priemonės, numatytos Spaudos įstatyme, tokių papildomų apsaugos priemonių, ribojančių išimties taikymą duomenis tvarkant religinėms organizacijoms ir politinėms partijoms ir iš dalies panašių į nustatytas Reglamento (ES) 2016/679 85, 89 ir 91 straipsniais, nustatyta nėra. Todėl Komisija mano, kad šio sprendimo tikslinga netaikyti religinėms organizacijoms, jei asmens duomenis jos tvarko savo misionierių veiklos tikslais, ir politinėms partijoms, jei asmens duomenis jos tvarko keldamos kandidatus.

2.3. Apsaugos priemonės, teisės ir prievolės

2.3.1. Duomenų tvarkymo teisėtumas ir sąžiningumas

- (33) Asmens duomenys turėtų būti tvarkomi teisėtai ir sąžiningai.
- (34) Šis principas nustatytas AIAI 3 straipsnio 1 ir 2 dalyse ir sustiprintas AIAI 59 straipsniu, kuriuo draudžiama tvarkyti asmens duomenis „naudojant sukčiavimą, netinkamas arba neteisėtas priemones“, „neturint teisinių įgaliojimų“ arba „peržengiant atitinkamų įgaliojimų ribas“ ⁽⁵⁰⁾. Šie bendrieji teisėto duomenų tvarkymo principai išdėstyti AIAI 15–19 straipsniuose, kuriuose nustatyti skirtingi duomenų tvarkymo (rinkimo, naudojimo ir teikimo trečiosioms šalims) teisiniai pagrindai, įskaitant aplinkybes, kurioms esant tikslas gali būti pakeistas (AIAI 18 straipsnis).

⁽⁴⁵⁾ Spaudos įstatymo 15–17 straipsniai.

⁽⁴⁶⁾ Pagal Spaudos įstatymo 6 straipsnį kiekvienas spaudos ar žiniasklaidos subjektas turi turėti savo ombudsmeną, kuris užkirstų kelią bet kokiai galimai spaudos subjekto padarytai žalai ir ją ištaisyty (pvz., rekomenduodamas ištaisyti spaudos pranešimus, kurie yra neteisingi arba kuriais kenkiama kitų asmenų reputacijai).

⁽⁴⁷⁾ Komisiją sudaro 40–90 arbitražo komisijos narių, kuriuos Kultūros, sporto ir turizmo ministras paskiria rinkdamasis iš asmenų, turinčių bent 10 metų patirtį dirbant teisėju, advokatu, rengiant arba pranešant naujienas, arba kitų asmenų, turinčių patirties, susijusios su spauda. Arbitražo komisijos nariai tuo pačiu metu negali būti valstybės pareigūnais, politinių partijų nariais arba žurnalistais. Pagal Spaudos įstatymo 8 straipsnį arbitražo komisijos nariai turi vykdyti savo pareigas nepriklausomai ir jiems negali būti teikiami jokie su šiomis pareigomis susiję nurodymai ar instrukcijos. Be to, nustatytos konkrečios taisyklės, kuriomis siekiama užkirsti kelią interesų konfliktams, pvz., komisijos nariams draudžiama nagrinėti bylas, kuriose jų sutuoktiniai arba giminaičiai yra bylos šalis (Spaudos įstatymo 10 straipsnis). Komisija gali spręsti ginčus taikinimo arba arbitražo būdu, tačiau taip pat gali pateikti rekomendacijas, kaip ištaisyti pažeidimus (Spaudos įstatymo 5 skirsnis).

⁽⁴⁸⁾ Spaudos įstatymo 30 straipsnis.

⁽⁴⁹⁾ Spaudos įstatymo 5 straipsnis.

⁽⁵⁰⁾ Pagal AIAI 59 straipsnį bet kuriam asmeniui, „kuris tvarko ar kada nors tvarkė asmeninę informaciją“, draudžiama „gauti asmeninę informaciją arba gauti sutikimą dėl asmeninės informacijos tvarkymo naudojant sukčiavimą, netinkamas ar neteisėtas priemones“, „atskleisti asmeninę informaciją, gautą vykdam verslą, arba suteikti ją bet kuriai trečiajai šaliai, kad ji galėtų ją naudoti neturėdama įgaliojimo“ arba „gadinti, naikinti, keisti, klastoti ar atskleisti kitų asmenų asmeninę informaciją neturint teisinio įgaliojimo ar peržengiant atitinkamo įgaliojimo ribas“. Pažeidus šį draudimą gali būti taikomos baudžiamosios sankcijos (žr. AIAI 71 straipsnio 5 ir 6 dalis ir 72 straipsnio 2 dalį). Be to, pagal AIAI 70 straipsnio 2 dalį už asmens duomenų, kuriuos trečiosios šalys tvarko sukčiaudamos ar naudodamos kitas neteisėtas priemones arba būdus, gavimą arba už tokios informacijos pateikimą trečiajai šaliai siekiant pelno ar neteisėtų tikslų, taip pat už bendrininkavimą vykdam tokią veiklą ar jos organizavimą, leidžiama skirti baudžiamąją sankciją.

- (35) Pagal AIAĮ 15 straipsnio 1 dalį yra tik ribotas skaičius teisinių pagrindų, kuriais remdamasis duomenų valdytojas gali rinkti asmens duomenis (tiek, kiek reikalinga jų rinkimo tikslu). Šie pagrindai yra: 1) duomenų subjekto sutikimas⁽⁵¹⁾ (1 punktas); 2) būtinybė, siekiant taikyti ir vykdyti su duomenų subjektu pasirašytą sutartį (4 punktas); 3) konkretus leidimas, nustatytas įstatymu, arba būtinybė, siekiant laikytis teisinės prievolės (2 punktas); būtinybė⁽⁵²⁾, viešajai institucijai siekiant vykdyti įstatymu nustatytas užduotis savo jurisdikcijoje; 4) akivaizdi būtinybė, siekiant apsaugoti duomenų subjekto arba trečiosios šalies gyvybę, fizinius ar turinius interesus nuo gresiančio pavojaus (tik tuo atveju, jei duomenų subjektas negali išreikšti savo ketinimų arba negalima gauti išankstinio sutikimo) (5 punktas); 5) būtinybė, siekiant duomenų valdytojo „pagrįsto intereso“, jei jis yra „akivaizdžiai viršesnis“ už duomenų subjekto interesus (ir tik tada, kai duomenų tvarkymas yra „pagrįstai susijęs“ su teisėtu interesu, ir tvarkomas pagrįstai reikalingas duomenų kiekis) (6 punktas)⁽⁵³⁾. Šie duomenų tvarkymo pagrindai iš esmės atitinka nustatytuosius Reglamento (ES) 2016/679 6 straipsnyje, įskaitant „pagrįsto intereso“ pagrindą, kuris atitinka Reglamento (ES) 2016/679 6 straipsnio 1 dalies f punkte nurodytą „teisėto intereso“ pagrindą.
- (36) Surinktus asmens duomenis galima naudoti tikslu, kuriam jie buvo renkami (AIAĮ 15 straipsnio 1 dalis), arba „tiek, kiek jų naudojimas pagrįstai susijęs“ su tikslu, kuriam duomenys buvo renkami, atsižvelgiant į galimus duomenų subjektui keliamus nepatogumus ir su sąlyga, kad taikomos būtinos saugumo priemonės (pvz., šifravimas) (AIAĮ 15 straipsnio 3 dalis). Kad būtų galima nustatyti, ar naudojimo tikslas yra „pagrįstai susijęs“ su pradiniu rinkimo tikslu, Vykdyto užtikrinimo dekretu nustatyti konkretūs kriterijai, panašūs į pateiktus Reglamento (ES) 2016/679 6 straipsnio 4 dalyje. Visų pirma papildomas naudojimas turi būti labai svarbus įgyvendinant pradinį tikslą, jis turi būti nuspėjamas (pavyzdžiui, atsižvelgiant į aplinkybes, kuriomis informacija buvo surinkta) ir, jei įmanoma, duomenims turi būti suteikti pseudonimai⁽⁵⁴⁾. Konkretūs kriterijai, kuriuos duomenų valdytojas naudoja atlikdamas šį vertinimą, turi būti iš anksto atskleisti privatumo politikoje⁽⁵⁵⁾. Be to, privatumo apsaugos pareigūnas (žr. (94) konstatuojamąją dalį) turi konkrečią prievolę patikrinti, ar duomenys toliau naudojami taikant tuos kriterijus.

⁽⁵¹⁾ Sutikimas turi būti duotas laisva valia, pagrįstas informacija, konkretus ir išreiškiamas vienu iš kelių įstatyme nustatytų būdų. Bet kuriuo atveju sutikimas negali būti gautas sukčiaujant, netinkamai ar kitaip neteisingai elgiantis (AIAĮ 59 straipsnio 1 dalis). Pirma, pagal AIAĮ 4 straipsnio 2 dalį duomenų subjektai turi teisę „sutikti arba nesutikti“ ir „pasirinkti sutikimo taikymo sritį“, ir turėtų būti apie tai informuoti (AIAĮ 15 straipsnio 2 dalis, 16 straipsnio 2 ir 3 dalys, 17 straipsnio 2 dalis ir 18 straipsnio 3 dalis). AIAĮ 22 straipsnio 5 dalyje numatyta papildoma apsaugos priemonė, pagal kurią duomenų valdytojui draudžiama atsakyti tiekti prekes ar teikti paslaugas, jei asmuo negali laisva valia pasirinkti duoti sutikimą. Tai apima atvejus, kai sutikimo reikia tik tam tikrų rūšių duomenų tvarkymui (o kitos duomenų tvarkymo rūšys yra grindžiamos sutartimi), taip pat tolesnį asmens duomenų, surinktų tiekiant prekes ar teikiant paslaugas, tvarkymą. Antra, pagal AIAĮ 15 straipsnio 2 dalį, 17 straipsnio 2 ir 3 dalis ir 18 straipsnio 3 dalį duomenų valdytojas, prašydamas sutikimo, privalo informuoti duomenų subjektą apie asmens duomenų, dėl kurių jis prašo sutikimo, ypatybes (pvz., kad sutikimas susijęs su neskelbtiniais duomenimis, žr. AIAĮ vykdymo užtikrinimo dekretu 17 straipsnio 2 dalies 2 punkto a papunktį), duomenų tvarkymo tikslą, saugojimo laikotarpį ir visus duomenų gavėjus. Toks prašymas turi būti pateikiamas „taip, kad jis būtų aiškiai atpažįstamas“, informaciją, dėl kurios reikalingas sutikimas, atskiriant nuo kitos informacijos (AIAĮ 22 straipsnio 1–4 dalys). Trečia, AIAĮ vykdymo užtikrinimo dekretu 17 straipsnio 1 dalies 1–6 punktuose nustatyti konkretūs būdai, kuriais duomenų valdytojas turi gauti sutikimą, pavyzdžiui, rašytinį sutikimą su duomenų subjekto parašu arba sutikimą elektroniniu paštu (atsakymą į elektroninį laišką). Nors AIAĮ konkrečiai nesuteikia asmenims bendros teisės atšaukti sutikimą, vietoje to asmenys turi teisę į tai, kad su jais susijusių duomenų tvarkymas būtų sustabdytas, ir tuo remiantis duomenų tvarkymas bus nutrauktas, o duomenys ištrinti (žr. 78 konstatuojamąją dalį dėl teisės sustabdyti duomenų tvarkymą).

⁽⁵²⁾ Remiantis iš AIAK gauta informacija, viešosios institucijos šiuo pagrindu gali remtis tik tuo atveju, jei asmens duomenų tvarkymas yra neišvengiamas, t. y. institucijai turi būti neįmanoma arba nepagrįstai sunku atlikti savo funkcijas netvarkant duomenų.

⁽⁵³⁾ AIAĮ 39-3 straipsnyje nustatytos konkrečios (griežtesnės) prievolės informacijos ir ryšių paslaugų teikėjams, susijusios su jų naudotojų asmeninės informacijos rinkimu ir naudojimu. Visų pirma reikalaujama, kad paslaugų teikėjas, pateikęs informaciją apie rinkimo ir (arba) naudojimo tikslą, renkamos asmeninės informacijos kategorijas ir laikotarpį, kuriuo informacija bus tvarkoma, gautų naudotojo sutikimą (AIAĮ 39-3 straipsnio 1 dalis). Tas pats reikalavimas taikomas, kai kuris nors iš šių aspektų pasikeičia. Negavus sutikimo rinkti informaciją taikomos baudžiamosios sankcijos (AIAĮ 71 straipsnio 4–5 dalys). Išimtiniais atvejais informacijos ir ryšių paslaugų teikėjai gali rinkti arba naudoti naudotojų asmeninę informaciją be išankstinio sutikimo. Tai atvejai, kai: 1) dėl ekonominių ir technologinių priežasčių (pvz., kai asmens duomenys neišvengiamai sukuriama vykstant sutartį, kaip antai informacija, reikalinga sąskaitai išrašyti, priegios žurnalas ir mokėjimo įrašai) akivaizdžiai sunku gauti įprastą sutikimą dėl asmeninės informacijos, reikalingos vykdyti sutarčiai, kuria reglamentuojamas informacijos ir ryšių paslaugų teikimas, 2) tai būtina siekiant atlikti apmokėjimą už suteiktas informacijos ir ryšių paslaugas arba 3) tai leidžiama pagal kitus įstatymus (pavyzdžiui, Įstatymo dėl vartotojų apsaugos jiems naudojantis elektronine prekyba 21 straipsnio 1 dalies 6 punkte nustatyta, kad verslo subjektai gali rinkti asmeninę informaciją apie nepilnamečio teisėtus globėjus, kad patvirtintų, ar nepilnamečio vardu gautas galiojantis sutikimas) (AIAĮ 39-3 straipsnio 2 dalis). Visais atvejais informacijos ir ryšių paslaugų teikėjai negali atsakyti teikti paslaugas tik dėl to, kad naudotojas nepateikia daugiau asmeninės informacijos, nei būtina (t. y. informacijos, kuri yra būtina esminiams atitinkamos paslaugos elementams įgyvendinti), žr. AIAĮ 39-3 straipsnio 3 dalį.

⁽⁵⁴⁾ Žr. AIAĮ vykdymo užtikrinimo dekretu 14-2 straipsnį.

⁽⁵⁵⁾ Žr. AIAĮ vykdymo užtikrinimo dekretu 14-2 straipsnio 2 dalį.

- (37) Panašios (tik šiek tiek griežtesnės) taisyklės taikomos duomenų teikimui trečiajai šaliai. Pagal AIAĮ 17 straipsnio 1 dalį asmens duomenys trečiajai šaliai gali būti teikiami gavus sutikimą⁽⁵⁶⁾ arba, jei tai reikalinga siekiant tikslo, kuriam jie buvo renkami, o informacija buvo renkama remiantis vienu iš 15 straipsnio 1 dalies 2, 3 ir 5 punktuose nurodytų teisinių pagrindų. Tai visų pirma netaikoma informacijos atskleidimui, grindžiamam duomenų valdytojo „pagrįstu interesu“. Be to, AIAĮ 17 straipsnio 4 dalyje nustatytas leidimas teikti informaciją trečiajai šaliai, „kiek tai pagrįstai susiję“ su tikslu, kuriuo duomenys buvo renkami, taip pat atsižvelgiant į galimus duomenų subjektui keliamus nepatogumus ir su sąlyga, kad taikomos būtinos saugumo priemonės (pvz., šifravimas). Vertinant, ar informacijos teikimas yra pagrįstai susijęs su tikslu, kuriuo duomenys buvo renkami, reikia atsižvelgti į tuos pačius veiksnius, kurie aprašyti (36) konstatuojamojoje dalyje, ir yra taikomos tos pačios apsaugos priemonės (t. y. dėl skaidrumo, įgyvendinamo privatumo politikoje, ir privatumo apsaugos pareigūno dalyvavimo).
- (38) Kai Korėjos duomenų valdytojas gauna asmens duomenis iš Sąjungos, tai laikoma duomenų rinkimu, kaip jis apibrėžtas AIAĮ 15 straipsnyje. Pranešime Nr. 2021-5 (šio sprendimo I priedo I skirsnis) paaiškinama, kad tikslas, kuriuo atitinkamas ES subjektas perdavė duomenis, yra tikslas, kuriuo Korėjos duomenų valdytojas renka duomenis. Todėl pagal AIAĮ 17 straipsnį iš Sąjungos asmens duomenis gaunantys Korėjos duomenų valdytojai iš esmės turi tvarkyti tokią informaciją tuo tikslu, kuriuo jie perduodami.
- (39) Konkretūs apribojimai taikomi tuo atveju, kai duomenų valdytojas siekia naudoti asmens duomenis arba pateikti juos trečiajai šaliai kitu tikslu nei tikslas, kuriuo jie buvo renkami⁽⁵⁷⁾. Pagal AIAĮ 18 straipsnio 2 dalį privatus duomenų valdytojas išimtiniais atvejais⁽⁵⁸⁾ gali naudoti asmens duomenis arba pateikti juos trečiajai šaliai kitu tikslu: 1) remdamasis duomenų subjekto papildomu (t. y. atskiru) sutikimu, 2) kai tai numatyta konkrečiose įstatymų nuostatose arba 3) kai tai akivaizdžiai būtina, siekiant apsaugoti duomenų subjekto arba trečiosios šalies gyvybę, fizinius ar turtinius interesus nuo gresiančio pavojaus (tik tuo atveju, jei duomenų subjektas negali išreikšti savo ketinimų arba negalima gauti išankstinio sutikimo)⁽⁵⁹⁾.
- (40) Viešosios institucijos tam tikrais atvejais taip pat gali naudoti asmens duomenis arba teikti juos trečiajai šaliai kitu tikslu. Tai apima ir tas aplinkybes, kai kitu atveju viešosios institucijos negalėtų vykdyti įstatymuose nustatytų pareigų (turi gauti AIAK leidimą). Be to, viešosios institucijos gali teikti asmens duomenis kitai institucijai ar teismui, jei tai būtina siekiant atlikti nusikalstamų veikų tyrimus ir už jas patraukti baudžiamojon atsakomybėn arba pareikšti kaltinimus, siekiant, kad būtų vykdomos teismo funkcijos, susijusios su vykstančiais teismo procesais arba siekiant užtikrinti baudžiamųjų sankcijų ar globos orderių vykdymą⁽⁶⁰⁾. Jos taip pat gali teikti asmens duomenis užsienio vyriausybei arba tarptautinei organizacijai, kad įvykdytų teisinį išipareigojimą pagal sutartį arba tarptautinę konvenciją (tokiu atveju jos taip pat turi laikytis tarpvalstybinio duomenų perdavimo reikalavimų (žr. (90) konstatuojamąją dalį).
- (41) Todėl duomenų tvarkymo teisėtumo ir sąžiningumo principai Korėjos teisinėje sistemoje įgyvendinami tokiu būdu, kuris iš esmės yra lygiavertis numatytam Reglamente (ES) 2016/679, leidžiant tvarkyti duomenis tik remiantis teisėtais ir aiškiai apibrėžtais pagrindais. Be to, visais minėtais atvejais tvarkyti duomenis leidžiama tik tuo atveju, jei nėra tikėtina, kad duomenų subjekto arba trečiosios šalies interesai bus „nepagrįstai pažeisti“, o tam reikalinga suderinti interesus. Be to, AIAĮ 18 straipsnio 5 dalyje nustatytos papildomos apsaugos priemonės, kai duomenų valdytojas pateikia asmens duomenis trečiajai šaliai, įskaitant prašymą apriboti naudojimo tikslą ir būdą arba nustatyti konkrečias saugumo priemones. Trečioji šalis savo ruožtu privalo įgyvendinti prašomas priemones.

⁽⁵⁶⁾ Už AIAĮ 17 straipsnio 1 dalies 1 punkto pažeidimą gali būti taikomos baudžiamosios sankcijos (AIAĮ 71 straipsnio 1 dalis).

⁽⁵⁷⁾ Numatytas tikslas – tai tikslas, kuriuo informacija buvo surinkta. Pavyzdžiui, kai informacija renkama atitinkamo asmens sutikimo pagrindu, numatytas tikslas yra tikslas, apie kurį asmeniui pranešama pagal AIAĮ 15 straipsnio 2 dalį.

⁽⁵⁸⁾ Žr. AIAĮ 18 straipsnio 1 dalį. Už AIAĮ 18 straipsnio 1 ir 2 dalies pažeidimą gali būti taikomos baudžiamosios sankcijos (AIAĮ 71 straipsnio 2 dalis).

⁽⁵⁹⁾ Informacijos ir ryšių paslaugų teikėjai gali naudoti asmeninę informaciją arba teikti ją trečiajai šaliai kitu nei pradinio tikslu tik AIAĮ 18 straipsnio 2 dalies 1 ir 2 punktuose nurodytais pagrindais (t. y. kai gaunamas papildomas sutikimas arba kai teisės aktuose numatytos konkrečios nuostatos). Žr. AIAĮ 18 straipsnio 2 dalį.

⁽⁶⁰⁾ Išskyrus atvejus, kai duomenų tvarkymas yra būtinas siekiant atlikti nusikalstamų veikų tyrimus, pareikšti kaltinimus ir patraukti baudžiamojon atsakomybėn, viešosios institucijos, kurios naudoja asmeninę informaciją arba teikia ją trečiajai šaliai kitu tikslu nei tikslas, kuriuo duomenys buvo renkami (pavyzdžiui, kai tai konkrečiai leidžiama pagal įstatymą arba būtina sutarčiai vykdyti), privalo savo interneto svetainėje arba oficialiajame leidinyje paskelbti duomenų tvarkymo teisinius pagrindus, tikslą ir apimtį ir saugoti įrašus (AIAĮ 18 straipsnio 4 dalis kartu su AIAĮ vykdymo užtikrinimo dekretu 15 straipsniu).

- (42) Galiausiai pagal AIAĮ 28-2 straipsnį informaciją, kuriai suteikti pseudonimai, be atitinkamo asmens sutikimo viešojo intereso pagrindu leidžiama (toliau) tvarkyti statistikos, mokslinių tyrimų⁽⁶¹⁾ ir archyvavimo tikslais, taikant specialias apsaugos priemones. Todėl AIAĮ, panašiai kaip ir Reglamente (ES) 2016/679⁽⁶²⁾, numatytas (tolesnis) asmens duomenų tvarkymas tokiais tikslais taikant sistemą, kurioje numatytos tinkamos asmenų teisių apsaugos priemonės. Užtuot pseudonimų suteikimą numačius kaip galimą apsaugos priemonę, jis AIAĮ nustatytas kaip būtina sąlyga siekiant viešojo intereso pagrindu vykdyti tam tikrą duomenų tvarkymo veiklą statistikos, mokslinių tyrimų ir archyvavimo tikslais (pavyzdžiui, siekiant tvarkyti duomenis be sutikimo arba sujungti skirtingus duomenų rinkinius).
- (43) Be to, AIAĮ nustatyta keletas konkrečių apsaugos priemonių, visų pirma susijusių su reikalingomis techninėmis ir organizacinėmis priemonėmis, įrašų saugojimu, dalijimosi duomenimis apribojimais ir galimos duomenų reidentifikavimo rizikos šalinimu. Derinant įvairias apsaugos priemones, aprašytas (44)–(48) konstatuojamosiose dalyse, užtikrinama, kad asmens duomenų tvarkymui šiomis aplinkybėmis būtų taikoma iš esmės lygiavertė apsauga, palyginti su apsauga, kurios būtų reikalaujama pagal Reglamentą (ES) 2016/679.
- (44) Pirma ir svarbiausia, pagal AIAĮ 28-5 straipsnio 1 dalį draudžiama tvarkyti informaciją, kuriai suteikti pseudonimai, siekiant nustatyti tam tikro asmens tapatybę. Jei informacija, kurią naudojant būtų galima nustatyti asmens tapatybę, vis dėlto būtų gauta tvarkant informaciją, kuriai suteikti pseudonimai, duomenų valdytojas privalo nedelsdamas sustabdyti tokios informacijos tvarkymą ir ją sunaikinti (AIAĮ 28-5 straipsnio 2 dalis). Šių nuostatų nesilaikymas yra nusikalstama veika ir už ją skiriamos administracinės baudos⁽⁶³⁾. Tai reiškia, kad net ir tais atvejais, kai *praktiškai* būtų įmanoma reidentifikuoti asmenį, toks reidentifikavimas yra *teisiškai* draudžiamas.
- (45) Antra, kai tokiais tikslais informacija, kuriai suteikti pseudonimai, (toliau) tvarkoma, duomenų valdytojas turi taikyti konkrečias technologines, valdymo ir fizines priemones, skirtas informacijos saugumui užtikrinti (įskaitant atskirą informacijos, būtinos atkurti informacijos, kuriai suteikti pseudonimai, pradinę būseną, saugojimą ir tvarkymą)⁽⁶⁴⁾. Be to, turi būti saugomi įrašai apie tvarkomą informaciją, kuriai suteikti pseudonimai, tvarkymo tikslą, naudojimo istoriją ir bet kokias ją gavusias trečiąsias šalis (AIAĮ vykdymo užtikrinimo dekreto 29-5 straipsnio 2 dalis).
- (46) Galiausiai trečia, AIAĮ numatytos specialios apsaugos priemonės, kurias taikant trečiosioms šalims užkertamas kelias nustatyti asmenų tapatybę tuo atveju, kai informacija dalijamasi. Visų pirma teikdami informaciją, kuriai suteikti pseudonimai, trečiajai šaliai viešojo intereso pagrindu tvarkyti statistikos, mokslinių tyrimų arba archyvavimo tikslais, duomenų valdytojai negali į ją įtraukti informacijos, kuri galėtų būti naudojama konkrečiam asmeniui identifikuoti (AIAĮ 28-2 straipsnio 2 dalis)⁽⁶⁵⁾.
- (47) Konkrečiai, nors pagal AIAĮ sujungti informaciją, kuriai suteikti pseudonimai, su kita informacija (tvarkoma kitų duomenų valdytojų), siekiant viešojo intereso pagrindu ją tvarkyti statistikos, mokslinių tyrimų arba archyvavimo tikslais, leidžiama, toks įgaliojimas suteikiamas tik specializuotoms institucijoms, galinčioms taikyti specialias saugumo priemones (AIAĮ 28-3 straipsnio 1 dalis)⁽⁶⁶⁾. Prašydamas leidimo sujungti duomenis, kuriems suteikti pseudonimai, su kitais duomenimis, duomenų valdytojas turi pateikti dokumentus, susijusius, be kita ko, su

⁽⁶¹⁾ AIAĮ 2 straipsnio 8 dalyje moksliniai tyrimai apibrėžiami kaip „tyrimai, kuriuose taikomi moksliniai metodai, pavyzdžiui, technologijų kūrimas ir demonstravimas, fundamentiniai moksliniai tyrimai, taikomieji moksliniai tyrimai ir privačiomis lėšomis finansuojami moksliniai tyrimai“. Šios kategorijos atitinka Reglamento (ES) 2016/679 159 konstatuojamojoje dalyje nustatytas kategorijas.

⁽⁶²⁾ Žr. Reglamento (ES) 2016/679 5 straipsnio 1 dalies b punktą, 89 straipsnio 1–2 dalis ir 50 bei 157 konstatuojamąsias dalis.

⁽⁶³⁾ Žr. AIAĮ 28-6 straipsnio 1 dalį, 71 straipsnio 4-3 dalį ir 75 straipsnio 2 dalies 4-4 punktą.

⁽⁶⁴⁾ AIAĮ 28-4 straipsnis ir AIAĮ vykdymo užtikrinimo dekreto 29-5 straipsnis. Už šio reikalavimo nesilaikymą gali būti taikomos administracinės arba baudžiamosios sankcijos (žr. AIAĮ 73 straipsnio 1 dalį ir 75 straipsnio 2 dalies 6 punktą).

⁽⁶⁵⁾ Už šių reikalavimų pažeidimą gali būti taikomos baudžiamosios sankcijos (AIAĮ 71 straipsnio 2 dalis). AIK nedelsdama ėmėsi užtikrinti šių naujų taisyklių taikymą, pvz., savo 2021 m. balandžio 28 d. sprendimu, kuriame numatyta, kad bendrovei, kuri, be kitų AIAĮ pažeidimų, nesilaikė AIAĮ 28-2 straipsnio 2 dalyje nustatyto reikalavimo, skiriama bauda ir taikomi taisomieji veiksmai (žr. <https://www.pipc.go.kr/np/cop/bbs/selectBoardArticle.do?bbsId=BS074&mCode=C020010000&ntId=7298&fbclid=IwAR3SKcMQi6G5pR9k4I7j6GNXtc8aBVDOwcURevvzQtYI7AS40UKYXoOXo8>).

⁽⁶⁶⁾ Institucija, siekianti būti paskirta tokia specializuota institucija (Duomenų sujungimo ekspertų agentūra), turi AIK pateikti prašymą kartu su patvirtinamaisiais dokumentais, kuriuose, be kita ko, turėtų būti pateikta išsami informacija apie priemones ir įrangą, įdiegtą siekiant saugiai sujungti duomenis, kuriems suteikti pseudonimai, ir patvirtinama, kad prašymą teikiantis subjektas yra įdarbinęs bent tris visą darbo dieną dirbančius darbuotojus, turinčius kvalifikaciją arba patirties, susijusios su asmens duomenų apsauga (AIAĮ vykdymo užtikrinimo dekreto 29-2 straipsnio 1 ir 2 dalys). Išsamūs reikalavimai, pvz., susiję su darbuotojų kvalifikacija, turima įranga, saugumo priemonėmis, vidaus politika ir procedūromis, taip pat finansiniais reikalavimais, nustatyti AIK pranešime 2020-9 dėl informacijos, kuriai suteikti pseudonimai, sujungimo ir teikimo (I sąrašas). Turėdama tam tikrą pagrindą AIK, surengusi klausymą, gali atšaukti Duomenų sujungimo ekspertų agentūros paskyrimą, pvz., jei agentūra nebeatitinka paskyrimui būtinų saugumo standartų arba jei duomenų sujungimo metu buvo pažeistas duomenų saugumas (AIAĮ vykdymo užtikrinimo dekreto 29-2 straipsnio 5 ir 6 dalys). AIK privalo paskelbti apie kiekvieną Duomenų sujungimo ekspertų agentūros paskyrimą (arba paskyrimo atšaukimą) (AIAĮ vykdymo užtikrinimo dekreto 29-2 straipsnio 7 dalis).

duomenimis, kurie turi būti sujungti su kitais duomenimis, jų sujungimo tikslu, taip pat su siūlomomis saugumo priemonėmis, taikomomis tvarkant sujungtus duomenis⁽⁶⁷⁾. Kad duomenis būtų galima sujungti su kitais duomenimis, duomenis, kuriuos reikia sujungti, duomenų valdytojas turi siųsti specializuotai institucijai ir pateikti duomenų sujungimo raktą (t. y. informaciją, kuri buvo naudojama pseudonimų suteikimui) Korėjos interneto ir saugumo agentūrai⁽⁶⁸⁾. Pastaroji sukuria duomenų sujungimo rakto susiejimo duomenis (kuriuos naudojant galima susieti skirtingų prašymus sujungti duomenis pateikusių asmenų duomenų sujungimo raktus, kad būtų galima sujungti duomenų rinkinius) ir teikia juos specializuotai institucijai⁽⁶⁹⁾.

- (48) Informaciją sujungti prašantis duomenų valdytojas gali analizuoti sujungtą informaciją specializuotos institucijos patalpose, erdvėje, kurioje taikomos specialios techninės, fizinės ir administracinės saugumo priemonės (AIAI vykdymo užtikrinimo dekreto 29-3 straipsnis). Duomenų valdytojai, kurie pateikia duomenų rinkinį tokiam sujungimui atlikti, sujungtus duomenis iš specializuotos institucijos patalpų išsinešti gali tik po to, kai sujungtiems duomenims yra suteikti pseudonimai arba jie yra nuasmeninti, ir gavę tos institucijos sutikimą (AIAI 28-3 straipsnio 2 dalis)⁽⁷⁰⁾. Svarstydama, ar suteikti tokį sutikimą, institucija įvertins ryšį tarp sujungtų duomenų ir tvarkymo tikslo ir ar tokiems duomenims naudoti buvo parengtas specialus saugumo planas⁽⁷¹⁾. Teikti sujungtą informaciją už institucijos ribų draudžiama, jei joje yra duomenų, kuriuos naudojant būtų galima nustatyti asmens tapatybę⁽⁷²⁾. Galiausiai specializuotos institucijos atliekamą duomenų, kuriems suteikti pseudonimai, sujungimą ir pateikimą prižiūri AIAK (AIAI vykdymo užtikrinimo dekreto 29-4 straipsnio 3 dalis).

2.3.2. Specialių kategorijų asmens duomenų tvarkymas

- (49) Kai tvarkomi „specialių kategorijų“ duomenys, turėtų būti taikomos specialios apsaugos priemonės.
- (50) AIAI nustatytos konkrečios taisyklės dėl neskelbtinų duomenų⁽⁷³⁾, kurie apibrėžiami kaip asmens duomenys, atskleidžiantys informaciją apie ideologiją, įsitikinimus, priėmimą į profesinę sąjungą ar politinę partiją ar pasitraukimą iš jos, politines pažiūras, asmens sveikatą ir seksualinį gyvenimą, taip pat kitą asmeninę informaciją, kuri „akivaizdžiai“ gali kelti grėsmę duomenų subjekto privatumui ir kuri Prezidento dekretu nurodyta kaip neskelbtina informacija, tvarkymo⁽⁷⁴⁾. Remiantis AIAK pateiktais paaiškinimais, seksualinis gyvenimas taip pat suprantamas kaip apimantis asmens seksualinę orientaciją⁽⁷⁵⁾. Be to, Vykdymo užtikrinimo dekreto 18 straipsnyje neskelbtinų duomenų apimtis išplečiama pridodant papildomų neskelbtinų duomenų kategorijų, visų pirma DNR informaciją, gautą atlikus genetinius tyrimus, ir duomenis apie teistumą. Neseniai iš dalies pakeitus AIAI vykdymo užtikrinimo dekretą dar labiau išplesta neskelbtinų duomenų sąvoka, įtraukiant asmens duomenis, atskleidžiančius rasę ar etninę kilmę ir biometrinę informaciją⁽⁷⁶⁾. Priėmus šį pakeitimą neskelbtinų duomenų sąvoka pagal AIAI iš esmės atitinka Reglamento (ES) 2016/679 9 straipsnyje vartojamą neskelbtinų duomenų sąvoką.
- (51) Pagal AIAI 23 straipsnio 1 dalį, panašiai kaip numatyta Reglamento (ES) 2016/679 9 straipsnio 1 dalyje, neskelbtinų duomenų tvarkymas paprastai draudžiamas, išskyrus atvejus, kai taikoma viena iš išvardytų išimčių⁽⁷⁷⁾. Jas taikant duomenų tvarkymas apribojamas juos tvarkant tik tais atvejais, kai duomenų valdytojas

⁽⁶⁷⁾ Pranešimo 2020-9 dėl informacijos, kuriai suteikti pseudonimai, sujungimo ir teikimo 8 straipsnio 1 ir 2 dalys.

⁽⁶⁸⁾ Pranešimo 2020-9 dėl informacijos, kuriai suteikti pseudonimai, sujungimo ir teikimo 2 straipsnio 3 ir 6 dalys ir 9 straipsnio 1 dalis.

⁽⁶⁹⁾ Pranešimo 2020-9 dėl informacijos, kuriai suteikti pseudonimai, sujungimo ir teikimo 2 straipsnio 4 dalis ir 9 straipsnio 2 ir 3 dalys. Duomenis sujungus specializuota institucija turi nedelsdama sunaikinti duomenų sujungimo rakto susiejimo duomenis (pranešimo 9 straipsnio 4 dalis).

⁽⁷⁰⁾ Už duomenų rinkinių sujungimo reikalavimų pažeidimą gali būti taikomos baudžiamosios sankcijos (AIAI 71 straipsnio 4-2 dalis). Žr. AIAI vykdymo užtikrinimo dekreto 29-2 straipsnio 4 dalį.

⁽⁷¹⁾ Sujungtų duomenų pateikimo patvirtinimo procedūra nustatyta pranešimo 2020-9 dėl informacijos, kuriai suteikti pseudonimai, sujungimo ir teikimo 11 straipsnyje. Visų pirma specializuota institucija turi įsteigti „pateikimo peržiūros komitetą“, sudarytą iš narių, turinčių pakankamai žinių ir patirties duomenų apsaugos srityje.

⁽⁷²⁾ AIAI vykdymo užtikrinimo dekreto 29-2 straipsnio 4 dalis ir pranešimo Nr. 2020-9 11 straipsnis.

⁽⁷³⁾ Korėjos Konstitucinis Teismas taip pat pripažino, kad tvarkant neskelbtinus duomenis, pavyzdžiui, duomenis apie sveikatą ar seksualinę elgseną, reikia taikyti specialią apsaugą (žr. 2007 m. gegužės 31 d. Konstitucinio Teismo sprendimą HunMa 1139).

⁽⁷⁴⁾ AIAI 23 straipsnio 1 dalis.

⁽⁷⁵⁾ Taip pat žr. AIAI Vadovo III skyriaus 2 dalį dėl 23 straipsnio (p. 157–164).

⁽⁷⁶⁾ T. y. asmeninę informaciją, gautą duomenis, susijusius su asmens fizinėmis, fiziologinėmis ar elgesio savybėmis, tvarkant specialiomis techninėmis priemonėmis konkrečiai siekiant identifikuoti tą asmenį.

⁽⁷⁷⁾ Dėl šių reikalavimų nesilaikymo gali būti taikomos sankcijos pagal AIAI 71 straipsnio 3 dalį.

informuoja duomenų subjektą pagal AIAĮ 15 ir 17 straipsnius ir gauna atskirą sutikimą (t. y. atskirą nuo sutikimo tvarkyti kitus asmens duomenis) arba kai duomenų tvarkymas yra privalomas arba leidžiamas pagal įstatymus. Viešosios institucijos taip pat gali tvarkyti biometrinę informaciją, DNR informaciją, gautą atlikus genetinius tyrimus, asmeninę informaciją, atskleidžiančią rasę ar etninę kilmę, ir duomenis apie teistumą, remdamosi tik tais pagrindais, kuriuos jos gali taikyti (pavyzdžiui, kai tai būtina nusikalstamai veikai tirti arba kai tai būtina, kad teismas galėtų nagrinėti bylą) ⁽⁷⁸⁾. Taigi neskelbtinų duomenų tvarkymo teisiniai pagrindai yra labiau riboti nei tie, kurie taikomi kitų rūšių asmens duomenų tvarkymui, ir Korėjos teisėje jie dar griežtesni nei teisiniai pagrindai, nustatyti Reglamento (ES) 2016/679 9 straipsnio 2 dalyje.

- (52) Be to, AIAĮ 23 straipsnio 2 dalyje, už kurios nesilaikymą gali būti taikomos sankcijos ⁽⁷⁹⁾, pabrėžiama, kad ypač svarbu užtikrinti tinkamą saugumą tvarkant neskelbtinus duomenis, kad jie „nebūtų prarasti, pavogti, atskleisti, suklastoti, pakeisti ar sugadinti“. Nors tai bendrasis reikalavimas pagal AIAĮ 29 straipsnį, 3 straipsnio 4 dalyje aiškiai nurodyta, kad saugumo lygis turi būti pritaikytas prie tvarkomų asmens duomenų rūšies, o tai reiškia, kad reikia atsižvelgti į ypatingą riziką, susijusią su neskelbtinų duomenų tvarkymu. Be to, duomenys visada tvarkomi „taip, kad būtų kuo labiau sumažinta galimybė pažeisti“ duomenų subjekto privatumą, ir, jei įmanoma, „anoniמיškai“ (AIAĮ 3 straipsnio 6 ir 7 dalys). Šie reikalavimai ypač svarbūs tais atvejais, kai tvarkomi neskelbtini duomenys.

2.3.3. Tikslų apribojimas

- (53) Asmens duomenys turėtų būti renkami konkrečiu tikslu ir tokiu būdu, kuris nebūtų nesuderinamas su jų tvarkymo tikslu.
- (54) Šis principas užtikrinamas AIAĮ 3 straipsnio 1 ir 2 dalimis, pagal kurias duomenų valdytojas „tiksliai ir aiškiai nurodo“ duomenų tvarkymo tikslą, asmens duomenis tvarko tinkamai, kaip būtina šiam tikslui pasiekti, ir nenaudoja jų kitu tikslu. Bendrasis tikslo apribojimo principas taip pat patvirtintas 15 straipsnio 1 dalyje, 18 straipsnio 1 dalyje, 19 straipsnyje, o duomenų tvarkytojų (vadinamųjų „užsakomųjų paslaugų teikėjų“) atžvilgiu – AIAĮ 26 straipsnio 1 dalies 1 punkte ir 5 ir 7 dalyse. Visų pirma asmens duomenys iš esmės gali būti naudojami ir teikiami trečiosioms šalims tik tuo tikslu, kuriuo jie buvo renkami (15 straipsnio 1 dalis ir 17 straipsnio 1 dalies 2 punktas). Duomenų tvarkymas suderinamu tikslu, t. y. „tokiu, kuris pagrįstai susijęs su pradiniu rinkimo tikslu“, gali būti atliekamas tik tuo atveju, jei tai nedaro neigiamo poveikio atitinkamiems duomenų subjektams ir jei taikomos būtinos saugumo priemonės (pavyzdžiui, šifravimas) (AIAĮ 15 straipsnio 3 dalis ir 17 straipsnio 4 dalis). Siekiant nustatyti, ar tolesnio duomenų tvarkymo tikslas yra suderinamas, naudojami AIAĮ vykdymo užtikrinimo dekretu nurodyti konkretūs kriterijai, kurie yra panašūs į tuos, kurie nustatyti Reglamento (ES) 2016/679 6 straipsnio 4 dalyje (žr. (36) konstatuojamąją dalį).

- (55) Kaip paaiškinta (38) konstatuojamojoje dalyje, Korėjos duomenų valdytojams asmens duomenis gaunant iš Sąjungos jų rinkimo tikslas yra tikslas, kuriuo duomenys perduodami. Duomenų valdytojas gali keisti tikslą tik konkrečiais išimtiniais (išvardytais) atvejais (AIAĮ 18 straipsnio 2 dalies 1–3 punktai, taip pat žr. (39) konstatuojamąją dalį). Atsižvelgiant į aplinkybes, kurioms esant pagal įstatymą leidžiama keisti tikslą, tokiais įstatymais savo ruožtu turi būti gerbiama pagrindinė teisė į privatumą ir duomenų apsaugą, taip pat laikomasi Korėjos Konstitucijoje nustatytų būtinumo ir proporcingumo principų. Be to, AIAĮ 18 straipsnio 2 ir 5 dalyse numatytos papildomos apsaugos priemonės, visų pirma reikalavimas, kad atliekant tokį tikslo pakeitimą negalima „nepagrįstai pažeisti duomenų subjekto interesų“, todėl visada būtina suderinti interesus. Taip nustatomas apsaugos lygis, kuris yra iš esmės lygiavertis apsaugos lygiui, numatytam pagal Reglamento (ES) 2016/679 5 straipsnio 1 dalies b punktą ir 6 straipsnį kartu su 50 konstatuojamąja dalimi.

2.3.4. Duomenų tikslumas ir kiekio mažinimas

- (56) Asmens duomenys turėtų būti tikslūs ir prareikūs atnaujinami. Duomenys taip pat privalo būti tinkami, susiję ir nepertekliniai atsižvelgiant į tikslus, kuriais jie tvarkomi.

⁽⁷⁸⁾ AIAĮ vykdymo užtikrinimo dekretu 18 straipsnyje nustatyta, kad ten išvardytoms duomenų kategorijoms netaikoma įstatymo 23 straipsnio 1 dalies nuostata, kai duomenis tvarko viešoji institucija pagal AIAĮ 18 straipsnio 2 dalies 5–9 punktus.

⁽⁷⁹⁾ Žr. AIAĮ 73 straipsnio 1 dalį ir 75 straipsnio 2 dalies 6 punktą.

- (57) Tikslumo principas panašiai pateikiamas AIAĮ 3 straipsnio 3 dalyje, kurioje reikalaujama, kad asmens duomenys būtų „tikslūs, išsamūs ir atnaujinti tiek, kiek tai būtina tikslams“, kuriais duomenys tvarkomi, pasiekti. Duomenų kiekio mažinimo reikalavimas nustatytas AIAĮ 3 straipsnio 1 ir 6 dalyse ir 16 straipsnio 1 dalyje, kuriose nurodyta, kad duomenų valdytojas renka asmens duomenis (tik) „tiek, kiek tai būtina“ numatytam tikslui pasiekti, ir kad šiuo atžvilgiu jam tenka prievolė įrodyti. Jei tikslą, kuriuo duomenys renkami, įmanoma pasiekti tvarkant nuasmenintą informaciją, duomenų valdytojai turėtų stengtis taip daryti (AIAĮ 3 straipsnio 7 dalis).

2.3.5. Saugojimo ribojimas

- (58) Iš esmės asmens duomenys turėtų būti saugomi ne ilgiau, nei reikia tikslams, kuriais asmens duomenys tvarkomi, pasiekti.
- (59) Saugojimo ribojimo principas taip pat numatytas AIAĮ 21 straipsnio 1 dalyje⁽⁸⁰⁾, kurioje reikalaujama, kad duomenų valdytojas, pasiekęs duomenų tvarkymo tikslą arba pasibaigus saugojimo laikotarpiui (priklausomai nuo to, kuri data ankstesnė), nedelsdamas „sunaikintų“⁽⁸¹⁾ asmens duomenis, išskyrus atvejus, kai pagal įstatymą asmens duomenis reikalaujama toliau saugoti⁽⁸²⁾. Pastaruoju atveju atitinkami asmens duomenys „saugomi ir administruojami atskirai nuo kitos asmeninės informacijos“ (AIAĮ 21 straipsnio 3 dalis).
- (60) AIAĮ 21 straipsnio 1 dalis netaikoma, kai duomenys, kuriems suteikti pseudonimai, viešojo intereso pagrindu tvarkomi statistikos, mokslinių tyrimų ar archyvavimo tikslais⁽⁸³⁾. Siekiant užtikrinti duomenų saugojimo ribojimo principo taikymą ir šiuo atveju, pranešime 2021-5 reikalaujama, kad duomenų valdytojai nuasmenintų informaciją pagal AIAĮ 58-2 straipsnį, jei duomenys nebuvo sunaikinti pasiekus konkretų tvarkymo tikslą⁽⁸⁴⁾.

2.3.6. Duomenų saugumas

- (61) Asmens duomenys turėtų būti tvarkomi taip, kad būtų užtikrintas jų saugumas, įskaitant apsaugą nuo neleistino ar neteisėto tvarkymo ir netyčinio praradimo, sunaikinimo ar sugadinimo. Todėl verslo subjektai turėtų imtis tinkamų techninių ir organizacinių priemonių, kad asmens duomenis apsaugotų nuo galimų grėsmių. Šios priemonės turėtų būti vertinamos atsižvelgiant į techninių galimybių išsivystymo lygį, susijusias sąnaudas ir duomenų tvarkymo pobūdį, aprėptį, aplinkybes ir tikslus, taip pat į asmenų teisėms kylančius pavojus.
- (62) Panašus saugumo principas nustatytas AIAĮ 3 straipsnio 4 dalyje, pagal kurią reikalaujama, kad duomenų valdytojai „saugiai tvarkytų asmeninę informaciją taikydami asmeninės informacijos tvarkymo metodus, rūšis ir t. t., atsižvelgdami į duomenų subjektų teisių pažeidimo galimybę ir susijusių pavojų mastą“. Be to, duomenų valdytojas „asmeninę informaciją tvarko taip, kad būtų kuo labiau sumažinta galimybė pažeisti duomenų subjekto privatumą“, ir šiomis aplinkybėmis stengiasi asmens duomenis tvarkyti anonimiškai arba, jei įmanoma, jiems suteikdamas pseudonimus (AIAĮ 3 straipsnio 6 ir 7 dalys).
- (63) Šie bendrieji reikalavimai išsamiau išdėstyti AIAĮ 29 straipsnyje, pagal kurį kiekvienas duomenų valdytojas „taiko technines, valdymo ir fizines priemones, kaip antai vidaus valdymo plano parengimas, registracijos įrašų saugojimas ir kt., kurios yra būtinos siekiant užtikrinti saugumą, kaip nustatyta Prezidento dekretu, kad asmeninė informacija nebūtų prarasta, pavogta, atskleista, suklastota, pakeista ar sugadinta“. AIAĮ vykdymo užtikrinimo

⁽⁸⁰⁾ 8 straipsnis (kartu su Vykdyto užtikrinimo dekretu 8-2 straipsniu), 11 straipsnis (kartu su Vykdyto užtikrinimo dekretu 12 straipsnio 2 dalimi).

⁽⁸¹⁾ Dėl asmeninės informacijos sunaikinimo būdų žr. AIAĮ vykdymo užtikrinimo dekretu 16 straipsnį. AIAĮ 21 straipsnio 2 dalyje paaiškinama, kad tai apima „būtiną atkūrimo ir atstatymo blokavimo priemones“.

⁽⁸²⁾ Už šių reikalavimų nesilaikymą gali būti taikomos baudžiamosios sankcijos (AIAĮ 73 straipsnio 1–2 dalys). AIAĮ 39-6 straipsnyje nustatytas papildomas reikalavimas informacijos ir ryšių paslaugų teikėjams ištrinti naudotojų, kurie mažiausiai vienus metus nesinaudojo siūlomomis informacijos ir ryšių paslaugomis, asmeninę informaciją (išskyrus atvejus, kai tolesnis jos saugojimas yra privalomas pagal įstatymą arba asmens prašymu). Asmenys turi būti informuoti apie numatomą jų informacijos ištrynimą likus 30 dienų iki vieno metų termino pabaigos (AIAĮ 39-6 straipsnio 2 dalis ir AIAĮ vykdymo užtikrinimo dekretu 48-5 straipsnio 3 dalis). Jei pagal įstatymą duomenis reikalaujama toliau saugoti, jie turi būti saugomi atskirai nuo kitos naudotojų informacijos ir gali būti naudojami arba atskleidžiami tik vadovaujantis šiuo įstatymu (AIAĮ vykdymo užtikrinimo dekretu 48-5 straipsnio 1 ir 2 dalys).

⁽⁸³⁾ AIAĮ 28-7 straipsnis.

⁽⁸⁴⁾ Pranešimo 2021-5 (I priedas) 4 skirsnis.

dekreto 30 straipsnio 1 dalyje šios priemonės patikslinamos nurodant, kad turi būti: 1) parengtas ir įgyvendinamas vidaus valdymo planas saugiam asmens duomenų tvarkymui, 2) kontroliuojama ir ribojama prieiga, 3) įdiegtos šifravimo technologijos, skirtos saugiai saugoti ir perduoti asmens duomenis, 4) saugomi prisijungimo įrašai, 5) taikomos saugumo programos ir 6) fizinės priemonės, kaip antai saugaus saugojimo arba užrakinimo sistema⁽⁸⁵⁾.

- (64) Be to, duomenų saugumo pažeidimo atveju taikomos specialios prievolės (AIAĮ 34 straipsnis kartu su AIAĮ vykdymo užtikrinimo dekretu 39 ir 40 straipsniais)⁽⁸⁶⁾. Visų pirma duomenų valdytojas turi nedelsdamas pateikti nukentėjusiems duomenų subjektams išsamią informaciją apie pažeidimą⁽⁸⁷⁾, įskaitant informaciją apie (privalomas) atsakomąsias priemones, kurių duomenų valdytojas ėmėsi, ir apie tai, kaip duomenų subjektai galėtų kuo labiau sumažinti žalos riziką (AIAĮ 34 straipsnio 1 ir 2 dalys)⁽⁸⁸⁾. Kai duomenų saugumo pažeidimas susijęs su ne mažiau kaip 1 000 duomenų subjektų, duomenų valdytojas apie duomenų saugumo pažeidimą ir atsakomąsias priemones taip pat nedelsdamas praneša AIAK ir Korėjos interneto ir saugumo agentūrai, kurios gali suteikti techninę pagalbą (AIAĮ 34 straipsnio 3 dalis kartu su AIAĮ vykdymo užtikrinimo dekretu 39 straipsniu). Duomenų valdytojai atsako už žalą, padarytą dėl duomenų saugumo pažeidimų, pagal Civilinio įstatymo dėl deliktinės atsakomybės nuostatas (taip pat žr. 2.5 skirsnį dėl teisių gynimo)⁽⁸⁹⁾.
- (65) Vykdyti saugumo išipareigojimus duomenų valdytojui turi padėti privatumo apsaugos pareigūnas, kurio užduotys, be kita ko, apima vidaus kontrolės sistemos sukūrimą, siekiant „užkirsti kelią asmens duomenų atskleidimui, piktnaudžiavimui jais ir netinkamam jų naudojimui“ (AIAĮ 31 straipsnio 2 dalies 4 punktas). Be to, duomenų valdytojas privalo taikyti „tinkamą kontrolę ir priežiūrą“ asmens duomenis tvarkantiems darbuotojams, be kita ko, siekiant užtikrinti saugų asmens duomenų valdymą, įskaitant būtiną darbuotojų mokymą („švietimą“) (AIAĮ 28 straipsnio 1 ir 2 dalys). Galiausiai duomenų tvarkymo subrangos atveju duomenų valdytojas „užsakomųjų paslaugų teikėjui“ turi taikyti reikalavimus, be kita ko, susijusius su saugiu asmens duomenų tvarkymu („techninės ir valdymo apsaugos priemonės“), ir prižiūrėti, kaip jie įgyvendinami atlikdamas patikrinimus (AIAĮ 26 straipsnio 1 ir 4 dalys kartu su AIAĮ vykdymo užtikrinimo dekretu 28 straipsnio 1 dalies 3 ir 4 punktais ir 6 dalimi).

2.3.7. Skaidrumas

- (66) Duomenų subjektai turėtų būti informuoti apie pagrindinius jų asmens duomenų tvarkymo aspektus.

⁽⁸⁵⁾ Kiek tai susiję su informacijos ir ryšių paslaugų teikėjų atliekamu asmens duomenų tvarkymu, AIAĮ 39-5 straipsnyje aiškiai nustatyta, kad asmenų, tvarkančių naudotojų asmeninę informaciją, skaičius turi būti kuo mažesnis. Be to, informacijos ir ryšių paslaugų teikėjai užtikrina, kad naudotojų asmeninė informacija nebūtų viešai prieinama per informacijos ir ryšių tinklą (AIAĮ 39-10 straipsnio 1 dalis). AIAK prašymu viešai prieinama informacija turi būti ištrinta arba prieiga prie jos turi būti užblokuota (AIAĮ 39-10 straipsnio 2 dalis). Apskritai informacijos ir ryšių paslaugų teikėjams (ir trečiosioms šalims, gaunančioms naudotojų asmens duomenis) taikomos papildomos saugumo prievolės, nurodytos AIAĮ vykdymo užtikrinimo dekretu 48-2 straipsnyje, pvz., vidaus valdymo plano dėl saugumo priemonių, parengimas ir įgyvendinimas, prieigos kontrolės užtikrinimo priemonės, šifravimas, programinės įrangos naudojimas kenkimo programinei įrangai aptikti ir kt.

⁽⁸⁶⁾ Be to, taikomas bendras draudimas gadinti, naikinti, keisti, klastoti ar nutekinti asmeninę informaciją neturint teisinio įgaliojimo (žr. AIAĮ 59 straipsnio 3 dalį).

⁽⁸⁷⁾ Reikalavimas pranešti asmeniui apie pažeidimą netaikomas, kai pažeidžiamas viešojo intereso pagrindu statistikos, mokslinių tyrimų ar archyvavimo tikslais tvarkomos informacijos, kuriai suteikti pseudonimai, saugumas (AIAĮ 28-7 straipsnis, kuriame numatyta išimtis dėl AIAĮ 34 straipsnio 1 dalies ir 39-4 straipsnio). Norėdamas užtikrinti, kad asmenims būtų pranešta individualiai, atitinkama duomenų valdytojas turėtų nustatyti asmenų tapatybę iš duomenų rinkinio, kuriam suteikti pseudonimai, o tai aiškiai draudžiama pagal AIAĮ 28-5 straipsnį. Tačiau bendrasis reikalavimas pranešti (AIAK) apie duomenų saugumo pažeidimą taikomas ir toliau.

⁽⁸⁸⁾ Pranešimo reikalavimai, įskaitant jo pateikimo laiką ir galimybę pranešti „palaipsniui“, išsamiau išdėstyti AIAĮ vykdymo užtikrinimo dekretu 40 straipsnyje. Griežtesnės taisyklės taikomos informacijos ir ryšių paslaugų teikėjams, kurie duomenų subjektui ir AIAK privalo pranešti per 24 valandas nuo tada, kai sužinojo apie asmeninės informacijos praradimą, vagystę ar nutekinimą (AIAĮ 39-4 straipsnio 1 dalis). Šiame pranešime turi būti pateikta išsami informacija apie nutekintą asmeninę informaciją, nurodytas šio įvykio laikas, priemonės, kurių gali imtis naudotojas, paslaugų teikėjo priimtoms atsakomosios priemonės ir departamento, kuriam naudotojas gali pateikti klausimus, kontaktiniai duomenys (AIAĮ 39-4 straipsnio 1 dalies 1–5 punktai). Jei yra pagrįsta priežastis, pvz., neturint naudotojo kontaktinių duomenų, gali būti naudojamos kitos pranešimo priemonės, pvz., viešai paskelbiant informaciją interneto svetainėje (AIAĮ 39-4 straipsnio 1 dalis kartu su AIAĮ vykdymo užtikrinimo dekretu 48-4 straipsnio 4 ir tolesnėmis dalimis). Tokiu atveju AIAK turi būti pranešama apie priežastis (AIAĮ 34-4 straipsnio 3 dalis).

⁽⁸⁹⁾ Žr., pvz., 2012 m. gruodžio 26 d. Aukščiausiojo Teismo sprendimus 2011Da59834, 2011Da59858 ir 2011Da59841. Santrauka anglų kalba pateikiama adresu http://library.scourt.go.kr/SCLIB_data/decision/9-69%202012.12.26.2011Da59834.htm.

- (67) Korėjos sistemoje tai užtikrinama įvairiais būdais. Be teisės į informaciją pagal AIAĮ 4 straipsnio 1 dalį (apskritai ir 20 straipsnio 1 dalį (susijusios su asmens duomenimis, surinktais iš trečiųjų šalių), taip pat teisės susipažinti su duomenimis pagal AIAĮ 35 straipsnį, AIAĮ numatytas bendras skaidrumo reikalavimas, susijęs su duomenų tvarkymo tikslu (AIAĮ 3 straipsnio 1 dalis), ir konkretūs skaidrumo reikalavimai tuo atveju, kai duomenų tvarkymas grindžiamas sutikimu (AIAĮ 15 straipsnio 2 dalis, 17 straipsnio 2 dalis ir 18 straipsnio 3 dalis) ⁽⁹⁰⁾. Be to, AIAĮ 20 straipsnio 2 dalyje nustatytas reikalavimas tam tikriems duomenų valdytojams (pasiekusiems atitinkamas duomenų tvarkymo ribas ⁽⁹¹⁾) pranešti duomenų subjektui, kurio asmens duomenis jie gavo iš trečiosios šalies, apie informacijos šaltinį, tvarkymo tikslą ir duomenų subjekto teisę reikalauti sustabdyti duomenų tvarkymą, nebent toks pranešimas būtų neįmanomas dėl to, kad nėra jokios kontaktinės informacijos. Išimtys taikomos tam tikroms valdžios institucijų turimoms asmens duomenų byloms, visų pirma byloms, kuriose yra duomenų, tvarkomų siekiant užtikrinti nacionalinį saugumą, apsaugoti kitus ypač svarbius nacionalinius interesus arba baudžiamosios teisės saugos tikslais, arba kai pranešus gali kilti grėsmė kito asmens gyvybei ar fizinei sveikatai arba gali būti nepagrįstai pakenkta kito asmens turtui ir kitiems interesams, tačiau tik tais atvejais, kai atitinkami viešieji ar privatieji interesai yra „akivaizdžiai viršesni“ už atitinkamų duomenų subjektų teises (AIAĮ 20 straipsnio 4 dalis). Todėl reikia suderinti interesus.
- (68) Be to, AIAĮ 3 straipsnio 5 dalyje nustatyta, kad duomenų valdytojai viešai skelbia savo privatumo politiką (ir kitą su asmens duomenų tvarkymu susijusią informaciją). Šis reikalavimas išsamiau apibrėžtas AIAĮ 30 straipsnyje kartu su AIAĮ vykdymo užtikrinimo dekretu 31 straipsniu. Pagal šias nuostatas viešai skelbiama privatumo politika, be kita ko, turi apimti: 1) tvarkomų asmens duomenų rūšis, 2) duomenų tvarkymo tikslą, 3) saugojimo laikotarpį, 4) informaciją apie tai, ar asmens duomenys teikiami trečiajai šaliai ⁽⁹²⁾, 5) informaciją apie bet kokią duomenų tvarkymo subrangą, 6) informaciją apie duomenų subjekto teises ir tai, kaip jomis naudotis, ir 7) kontaktinę informaciją (įskaitant privatumo apsaugos pareigūno vardą ir pavardę arba už duomenų apsaugos taisyklių laikymosi užtikrinimą ir skundų nagrinėjimą atsakingo vidaus departamento pavadinimą). Privatumo politika turi būti viešai skelbiama taip, kad duomenų subjektai ją galėtų „lengvai atpažinti“ (AIAĮ 30 straipsnio 2 dalis) ⁽⁹³⁾, ir ji turi būti nuolat atnaujinama (AIAĮ vykdymo užtikrinimo dekretu 31 straipsnio 2 dalis).
- (69) Viešosioms institucijoms taikoma papildoma pareiga AIAK pateikti visų pirma šią informaciją, kad ji ją galėtų užregistruoti: 1) viešosios institucijos pavadinimą, 2) asmens duomenų bylų tvarkymo pagrindus ir tikslus, 3) išsamią informaciją apie užregistruotus asmens duomenis, 4) informaciją apie duomenų tvarkymo būdą, 5) saugojimo laikotarpį, 6) duomenų subjektų, kurių asmens duomenys saugomi, skaičių, 7) duomenų subjekto prašymus tvarkantį departamentą ir 8) asmens duomenų gavėjus, kai duomenys teikiami reguliariai arba pakartotinai (AIAĮ 32 straipsnio 1 dalis) ⁽⁹⁴⁾. Užregistruotas asmens duomenų bylas AIAK skelbia viešai, o viešosios institucijos taip pat turi jas nurodyti savo privatumo politikoje (AIAĮ 30 straipsnio 1 dalis ir 32 straipsnio 4 dalis).
- (70) Siekiant padidinti skaidrumą Sąjungos duomenų subjektų, kurių asmens duomenys perduodami Korėjai remiantis šiuo sprendimu, atžvilgiu, pranešimo 2021-5 (I priedas) 3 skirsnio i ir ii punktuose nustatyti papildomi skaidrumo reikalavimai. Pirma, šio sprendimo pagrindu asmens duomenis iš Sąjungos gavę Korėjos duomenų valdytojai nepagrįstai nedelsdami (ir bet kuriuo atveju ne vėliau kaip per vieną mėnesį nuo duomenų gavimo) turi pateikti atitinkamiems duomenų subjektams perduodančių ir gaunančių subjektų pavadinimus ir kontaktinius

⁽⁹⁰⁾ Visų pirma, kai asmeninė informacija yra tvarkoma asmens sutikimu, duomenų valdytojas turi informuoti asmenį apie tvarkymo tikslą, pateikti jam išsamią informaciją apie tvarkytiną informaciją, informacijos gavėją, asmeninės informacijos saugojimo ir naudojimo laikotarpį, taip pat apie tai, kad asmuo turi teisę atsisakyti duoti sutikimą (ir bet kokius nepatogumus, kurie gali dėl to kilti).

⁽⁹¹⁾ Pagal AIAĮ vykdymo užtikrinimo dekretu 15-2 straipsnio 1 dalį reikalavimas taikomas duomenų valdytojams, tvarkantiems neskelbtiną informaciją apie ne mažiau kaip 50 000 duomenų subjektų arba įprastą asmens informaciją apie ne mažiau kaip 1 mln. duomenų subjektų. AIAĮ vykdymo užtikrinimo dekretu 15-2 straipsnio 2 dalyje nustatyti pranešimo būdai ir laikas, o 15-2 straipsnio 3 dalyje – reikalavimas saugoti tam tikrus su jais susijusius įrašus. Be to, konkrečios taisyklės taikomos tam tikrų kategorijų informacijos ir ryšių paslaugų teikėjams (per praėjusius metus uždirbusiems ne mažiau kaip 10 mlrd. vonų pardavimo pajamų arba praėjusių metų paskutinius tris mėnesius vidutiniškai saugojusiems ir (arba) tvarkiusiems ne mažiau kaip vieno milijono naudotojų asmens duomenis per dieną), kurie privalo reguliariai pranešti naudotojams apie jų asmeninės informacijos naudojimo istoriją, išskyrus atvejus, kai to padaryti neįmanoma dėl kontaktinės informacijos trūkumo (AIAĮ 39-8 straipsnis ir AIAĮ vykdymo užtikrinimo dekretu 48-6 straipsnis).

⁽⁹²⁾ Remiantis iš Korėjos vyriausybės gauta informacija, tai reiškia, kad kiekvienas gavėjas viešosios privatumo politikos sąraše privalo būti nurodytas atskirai.

⁽⁹³⁾ Papildomos sąlygos nustatytos AIAĮ vykdymo užtikrinimo dekretu 31 straipsnio 3 dalyje.

⁽⁹⁴⁾ Reikalavimas užregistruoti informaciją netaikomas tam tikrų rūšių asmeninės informacijos byloms, pavyzdžiui, toms, kuriose registruojama informacija, susijusi su nacionaliniu saugumu, diplomatinėmis paslaptimis, baudžiamaisiais tyrimais, baudžiamuoju persekiojimu, sankcijomis, nusikaltimų, susijusių su mokesčiais, tyrimais, arba byloms, kurios susijusios tik su vidaus darbo rezultatais (AIAĮ 32 straipsnio 2 dalis).

duomenis, informaciją apie perduotus asmens duomenis (arba asmens duomenų kategorijas), Korėjos duomenų valdytojo atliekamo duomenų rinkimo tikslą, saugojimo laikotarpį ir pagal AIAĮ suteikiamas teises. Antra, šio sprendimo pagrindu iš Sąjungos gautus asmens duomenis teikiant trečiosioms šalims duomenų subjektams turi būti pateikta informacija, *inter alia*, apie duomenų gavėją, asmens duomenis arba teiktinų asmens duomenų kategorijas, valstybę, kuriai duomenys teikiami (atitinkamais atvejais), taip pat apie pagal AIAĮ suteikiamas teises⁽⁹⁵⁾. Taip pranešimu užtikrinama, kad asmenys ES ir toliau būtų informuojami apie konkrečius jų informaciją tvarkančius duomenų valdytojus ir galėtų naudotis savo teisėmis atitinkamų subjektų atžvilgiu.

- (71) Pagal pranešimo 3 skirsnio iii punktą (I priedas) leidžiama taikyti tam tikras ribotas ir sąlygines šių papildomų skaidrumo prievolių išimtis, kurios iš esmės atitinka Reglamente (ES) 2016/679 nustatytas išimtis. Visų pirma, pranešti duomenų subjektams Sąjungoje nereikalaujama: 1) tais atvejais ir tol, kol dėl tam tikrų su viešuoju interesu susijusių priežasčių (pavyzdžiui, kai informacija tvarkoma nacionalinio saugumo arba vykdomų nusikaltamų veikų tyrimų tikslais) būtina apriboti pranešimą tiek, kiek šie viešojo intereso tikslai yra akivaizdžiai viršesni už duomenų subjekto teises, 2) kai duomenų subjektas jau turi informacijos, 3) kai ir tol, kol pranešus gali kilti grėsmė asmens ar kito žmogaus gyvybei ar fizinei sveikatai arba gali būti nepagrįstai pažeisti kito žmogaus turtiniai interesai, kai tos teisės ar interesai yra akivaizdžiai viršesni už duomenų subjekto teises, arba 4) kai neturimi atitinkamų asmenų kontaktiniai duomenys arba siekiant jiems pranešti turėtų būti dedamos neproporcingai didelės pastangos. Nustatant, ar įmanoma susisiekti su duomenų subjektu ir ar dėl to reikia dėti pernelyg daug pastangų, atsižvelgiama į galimybę bendradarbiauti su duomenų eksportuotoju Sąjungoje.
- (72) Todėl, kiek tai susiję su skaidrumu, (67)–(71) konstatuojamosiose dalyse išdėstytomis taisyklėmis užtikrinamas iš esmės lygiavertis apsaugos lygis numatytam Reglamente (ES) 2016/679.

2.3.8. Asmens teisės

- (73) Duomenų subjektai turėtų turėti tam tikras teises, kurias būtų galima įgyvendinti duomenų valdytojo arba duomenų tvarkytojo atžvilgiu, visų pirma teisę susipažinti su duomenimis, teisę reikalauti ištaisyti duomenis, teisę nesutikti su duomenų tvarkymu ir teisę reikalauti ištrinti duomenis. Tokios teisės taip pat gali būti ribojamos, jei šie apribojimai yra būtini ir proporcingi siekiant apsaugoti svarbius bendro viešojo intereso tikslus.
- (74) Pagal AIAĮ 3 straipsnio 5 dalį duomenų valdytojas užtikrina AIAĮ 4 straipsnyje išvardytas ir AIAĮ 35–37, 39 ir 39-2 straipsniuose išsamiau išdėstytas duomenų subjekto teises.
- (75) Pirma, asmenys turi teisę į informaciją ir teisę susipažinti su ja. Kai duomenų valdytojas surenka asmens duomenis iš trečiosios šalies (o taip bus visada tuo atveju, kai duomenys perduodami iš Sąjungos), duomenų subjektai paprastai turi teisę gauti informaciją apie 1) surinktų asmens duomenų „šaltinį“ (t. y. duomenų perdavėją), 2) duomenų tvarkymo tikslą ir 3) tai, kad duomenų subjektas turi teisę reikalauti sustabdyti duomenų tvarkymą (AIAĮ 20 straipsnio 1 dalis). Taikomos ribotos išimties, t. y. kai pranešus gali kilti grėsmė kito asmens gyvybei ar fizinei sveikatai arba gali būti „nepagrįstai pakenkta kito asmens turtui ir kitiems interesams“, tačiau tik tais atvejais, kai šie trečiųjų šalių interesai yra „aiškiai viršesni“ už duomenų subjekto teises (AIAĮ 20 straipsnio 4 dalies 2 punktą).
- (76) Be to, AIAĮ 35 straipsnio 1 ir 3 dalyse kartu su AIAĮ vykdymo užtikrinimo dekreto 41 straipsnio 4 dalimi duomenų subjektams suteikiama teisė susipažinti su savo asmenine informacija⁽⁹⁶⁾. Teisė susipažinti su duomenimis taikoma duomenų tvarkymo patvirtinimui, informacijai apie tvarkomų duomenų rūšį, tvarkymo tikslą, saugojimo laikotarpį, taip pat informacijai apie bet kokią informacijos atskleidimą trečiajai šaliai ir tvarkomos

⁽⁹⁵⁾ Pranešimo 2021-5 3 skirsnio ii punktas (I priedas).

⁽⁹⁶⁾ Pagal AIAĮ 35 straipsnio 3 dalį kartu su AIAĮ vykdymo užtikrinimo dekreto 42 straipsnio 2 dalimi duomenų valdytojas gali pavélini galimybés susipažinti su duomenimis suteikimą dėl „rimtos priežasties“ (t. y. dėl pagrįstų priežasčių, pvz., jei reikia daugiau laiko įvertinti, ar galima suteikti galimybę susipažinti su duomenimis), tačiau privalo per 10 dienų pranešti duomenų subjektui apie tokį pagrindimą ir pateikti informaciją apie tai, kaip šį sprendimą galima apskųsti. Kai pagrindo nesuteikti galimybės susipažinti su duomenimis nebelieka, galimybė susipažinti su duomenimis turi būti suteikta.

asmeninės informacijos kopijos pateikimą (AIAĮ 4 straipsnio 3 dalis kartu su AIAĮ vykdymo užtikrinimo dekretu 41 straipsnio 1 dalimi) ⁽⁹⁷⁾. Galimybė susipažinti su duomenimis gali būti ribojama (dalinis susipažinimas su duomenimis) ⁽⁹⁸⁾ arba nesuteikiama tik tada, kai tai numatyta įstatyme ⁽⁹⁹⁾, kai tai gali kelti grėsmę trečiosios šalies gyvybei ar fizinei sveikatai arba nepagrįstai pažeisti kito asmens turtinius ir kitus interesus (AIAĮ 35 straipsnio 4 dalis) ⁽¹⁰⁰⁾. Tai reiškia, kad turėtų būti derinamos asmens ir kitų asmenų Konstitucijoje nustatytos teisės ir laisvės. Kai galimybė susipažinti su duomenimis ribojama arba nesuteikiama, duomenų valdytojas privalo informuoti duomenų subjektą apie tokio sprendimo pagrindus ir pateikti informaciją apie tai, kaip tokį sprendimą galima apskųsti (AIAĮ vykdymo užtikrinimo dekretu 41 straipsnio 5 dalis ir 42 straipsnio 2 dalis).

- (77) Antra, duomenų subjektai turi teisę reikalauti, kad jų asmens duomenys būtų ištaisyti arba ištrinti ⁽¹⁰¹⁾, „išskyrus atvejus, kai kituose įstatymuose konkrečiai numatyta kitaip“ (AIAĮ 36 straipsnio 1 ir 2 dalys) ⁽¹⁰²⁾. Gavęs prašymą, duomenų valdytojas turi nedelsdamas iširti atvejį, imtis būtinų priemonių ⁽¹⁰³⁾ ir apie tai pranešti duomenų subjektui per 10 dienų. Kai prašymas negali būti patenkintas, į reikalavimą pranešti įtraukiama atsakymo priežastis ir informacija apie tai, kaip pateikti skundą (žr. AIAĮ 36 straipsnio 4 dalį kartu su AIAĮ vykdymo užtikrinimo dekretu 43 straipsnio 3 dalimi) ⁽¹⁰⁴⁾.
- (78) Galiausiai duomenų subjektai turi teisę į tai, kad būtų nedelsiant sustabdytas jų asmens duomenų tvarkymas ⁽¹⁰⁵⁾, išskyrus atvejus, kai taikoma viena iš išvardytų išimčių (AIAĮ 37 straipsnio 1 ir 2 dalys) ⁽¹⁰⁶⁾. Duomenų valdytojas gali atmesti prašymą sustabdyti duomenų tvarkymą: 1) kai tai konkrečiai leidžiama pagal įstatymą arba būtina („neišvengiama“) siekiant vykdyti teisinės prievolės, 2) kai dėl sustabdymo gali kilti grėsmė trečiosios šalies gyvybei ar fizinei sveikatai arba gali būti nepagrįstai pažeidžiami kito asmens turtiniai ir kiti interesai, 3) kai netvarkydama informacijos viešoji institucija negalėtų vykdyti savo funkcijos, kaip nustatyta teisės aktuose, arba 4) kai duomenų subjektas aiškiai nenutraukia pagrindinės sutarties su duomenų valdytoju, net jei vykdyti sutartį be tokio duomenų tvarkymo būtų neįmanoma. Šiuo atveju duomenų valdytojas turi nedelsdamas informuoti duomenų subjektą apie prašymo atmetimo priežastis ir pateikti informaciją apie tai, kaip sprendimą galima apskųsti (AIAĮ 37 straipsnio 2 dalis kartu su AIAĮ vykdymo užtikrinimo dekretu 44 straipsnio 2 dalimi). Pagal AIAĮ 37 straipsnio 4 dalį duomenų valdytojas, vykdydamas prašymą sustabdyti duomenų tvarkymą, turi nedelsdamas „imtis būtinų priemonių, įskaitant atitinkamos asmeninės informacijos sunaikinimą“ ⁽¹⁰⁷⁾.
- (79) Teisė sustabdyti duomenų tvarkymą taip pat taikoma tais atvejais, kai asmens duomenys naudojami tiesioginės rinkodaros tikslais, t. y. siekiant reklamuoti prekes ar paslaugas arba siūlyti jas pirkti. Be to, tokiam tolesniam duomenų tvarkymui paprastai reikalingas konkretus (papildomas) duomenų subjekto sutikimas (žr. AIAĮ 15 straipsnio 1 dalies 1 punktą ir 17 straipsnio 2 dalies 1 punktą) ⁽¹⁰⁸⁾. Prašydamas šio sutikimo, duomenų

⁽⁹⁷⁾ Galimybę susipažinti su viešosios institucijos tvarkoma asmenine informacija gali suteikti pati institucija arba ji gali būti suteikta pateikus prašymą AIAK, kuri prašymą nedelsdama perduoda (AIAĮ 35 straipsnio 2 dalis ir AIAĮ vykdymo užtikrinimo dekretu 41 straipsnio 3 dalis).

⁽⁹⁸⁾ Pagal AIAĮ vykdymo užtikrinimo dekretu 42 straipsnio 1 dalį duomenų valdytojas privalo suteikti galimybę susipažinti su dalimi informacijos, jei bent daliai informacijos netaikomas pagrindas, kurį taikant galimybė nesuteikiama.

⁽⁹⁹⁾ Tokiame įstatyme savo ruožtu turi būti gerbiama pagrindinė teisė į privatumą ir duomenų apsaugą, taip pat laikomasi Korėjos Konstitucijoje nustatytų būtinumo ir proporcingumo principų.

⁽¹⁰⁰⁾ Be to, viešosios institucijos gali atsakyti suteikti galimybę susipažinti su duomenimis, jei dėl to kiltų didelių sunkumų atliekant tam tikras funkcijas, įskaitant audito atlikimą arba mokesčių taikymą, surinkimą arba grąžinimą (AIAĮ 35 straipsnio 4 dalis).

⁽¹⁰¹⁾ Tokiu atveju duomenų valdytojas turi imtis priemonių, kad būtų užkirstas kelias asmeninės informacijos atkūrimui (žr. AIAĮ 36 straipsnio 3 dalį).

⁽¹⁰²⁾ Tokie įstatymai turi atitikti Konstitucijos reikalavimus, pagal kuriuos pagrindinė teisė gali būti apribota tik tada, kai tai būtina nacionaliniam saugumui užtikrinti arba viešajai tvarkai palaikyti siekiant užtikrinti visuomenės gerovę, ir negali turėti įtakos esminių laisvės ar teisės aspektų įgyvendinimui (Konstitucijos 37 straipsnio 2 dalis).

⁽¹⁰³⁾ AIAĮ vykdymo užtikrinimo dekretu 43 straipsnio 2 dalyje numatyta speciali procedūra tuo atveju, kai duomenų valdytojas tvarko kito duomenų valdytojo pateiktas asmens duomenų bylas.

⁽¹⁰⁴⁾ Už būtinų priemonių asmens informacijai ištaisyti ar ištrinti nesėdimą ir tos informacijos tolesnį naudojimą arba teikimą trečiajai šaliai gali būti taikomos baudžiamosios sankcijos (AIAĮ 73 straipsnio 2 dalis).

⁽¹⁰⁵⁾ Pagal AIAĮ vykdymo užtikrinimo dekretu 44 straipsnio 2 dalį duomenų valdytojas per 10 dienų nuo prašymo gavimo informuoja duomenų subjektą apie tai, kad jis tinkamai sustabdė duomenų tvarkymą.

⁽¹⁰⁶⁾ Viešųjų institucijų atveju teisė į duomenų tvarkymo sustabdymą gali būti taikoma dėl užregistruotose asmens duomenų bylose esančios informacijos (AIAĮ 37 straipsnis kartu su 32 straipsniu). Tokios duomenų registracijos nereikalaujama tik tam tikrais atvejais, pvz., kai asmens duomenų bylos yra susijusios su nacionaliniu saugumu, baudžiamaisiais tyrimais, diplomatiniais santykiais ir t. t. (AIAĮ 32 straipsnio 2 dalis).

⁽¹⁰⁷⁾ Už prašymo sustabdyti duomenų tvarkymą nevykdymą gali būti taikomos baudžiamosios sankcijos (AIAĮ 73 straipsnio 3 dalis).

⁽¹⁰⁸⁾ Tarpininkavimo ginčiuose komitetas (žr. 133 konstatuojamąją dalį) nagrinėjo keletą atvejų, kai asmenys skundėsi dėl jų duomenų naudojimo tiesioginės rinkodaros tikslais be sutikimo, dėl kurių, pavyzdžiui, atitinkamas duomenų valdytojas sumokėjo kompensaciją ir ištyrė asmens duomenis (žr., pvz., Tarpininkavimo ginčiuose komiteto 20R10-024(2020.11.18), 20R08-015(2020.8.28), 20R07-031(2020.9.1)).

valdytojas visų pirma privalo informuoti duomenų subjektą apie numatomą duomenų naudojimą tiesioginės rinkodaros tikslais (t. y. apie tai, kad su juo gali būti susisiekta siekiant reklamuoti prekes ar paslaugas arba siūlyti jas pirkti), tokiu būdu, kad informavimas būtų „aiškiai atpažįstamas“ (AIAĮ 22 straipsnio 2 ir 4 dalys kartu su AIAĮ vykdymo užtikrinimo dekreto 17 straipsnio 2 dalies 1 punktu).

- (80) Kad asmenims būtų sudarytos palankesnės sąlygos naudotis savo teisėmis, duomenų valdytojas turi nustatyti specialias procedūras ir jas viešai paskelbti (AIAĮ 38 straipsnio 4 dalis) ⁽¹⁰⁹⁾. Tai apima procedūras, skirtas prieštaravimams dėl prašymo atmetimo pareikšti (AIAĮ 38 straipsnio 5 dalis). Duomenų valdytojas turi užtikrinti, kad procedūra, kuria sudaromos sąlygos naudotis teisėmis, būtų „patogi duomenų subjektams“ ir nebūtų sudėtingesnė nei renkant asmens duomenis taikoma procedūra, taip pat vykdyti pareigą pateikti informaciją apie procedūrą savo interneto svetainėje (AIAĮ vykdymo užtikrinimo dekreto 41 straipsnio 2 dalis, 43 straipsnio 1 dalis ir 44 straipsnio 1 dalis) ⁽¹¹⁰⁾. Asmenys gali įgalioti atstovą pateikti tokį prašymą (AIAĮ 38 straipsnio 1 dalis kartu su AIAĮ vykdymo užtikrinimo dekreto 45 straipsniu). Duomenų valdytojas turi teisę reikalauti padengti mokesčių (ir, jei asmens duomenų kopijas prašoma atsiųsti, pašto išlaidas), bet jo suma turi būti nustatyta „atsižvelgiant į faktines [prašymo] tvarkymo išlaidas“. Reikalauti padengti mokesčių (arba pašto išlaidas) negalima, jei prašymas teikiamas dėl duomenų valdytojo kaltės (AIAĮ 38 straipsnio 3 dalis kartu su AIAĮ vykdymo užtikrinimo dekreto 47 straipsniu).
- (81) AIAĮ ir jo Vykdymo užtikrinimo dekrete nėra bendrųjų nuostatų, susijusių su sprendimais, turinčiais pasekmių duomenų subjektui ir grindžiamais tik automatizuotu asmens duomenų tvarkymu. Tačiau asmens duomenų, surinktų Sąjungoje, atveju bet koki automatizuotu duomenų tvarkymu grindžiamą sprendimą paprastai priims duomenų valdytojas Sąjungoje (kuris turi tiesioginį ryšį su atitinkamu duomenų subjektu), todėl jų tvarkymui taikomas Reglamentas (ES) 2016/679 ⁽¹¹¹⁾. Tai apima perdavimo atvejus, kai duomenis tvarko užsienio valstybės (pavyzdžiui, Korėjos) verslo subjektas, veikiantis kaip ES duomenų valdytojo atstovas (duomenų tvarkytojas) arba kaip pagalbinis duomenų tvarkytojas, veikiantis ES duomenų tvarkytojo, gavusio duomenis iš ES duomenų valdytojo, kuris juos surinko, vardu), todėl šiuo pagrindu sprendimą priima ES duomenų valdytojas. Todėl mažai tikėtina, kad tai, jog AIAĮ nėra konkrečių automatizuoto sprendimų priėmimo taisyklių, turės įtakos pagal sprendimą perduotų asmens duomenų apsaugos lygiui.
- (82) Išimties tvarka nuostatos dėl skaidrumo įgyvendinant prašymų teikimo (20 straipsnis) ir asmens teises (35–37 straipsniai), taip pat informacijos ir ryšių paslaugų teikėjams taikomas individualaus pranešimo reikalavimas (AIAĮ 39-8 straipsnis) netaikomi, jei tai susiję su informacija, kuriai suteikti pseudonimai, ir ji viešojo intereso pagrindu tvarkoma statistikos, mokslinių tyrimų ar archyvavimo tikslu (AIAĮ 28-7 straipsnis) ⁽¹¹²⁾. Laikantis Reglamento (ES) 2016/679 11 straipsnio 2 dalies (kartu su 57 konstatuojamąja dalimi) požiūriu, tai pateisinama tuo, kad, siekdamas užtikrinti skaidrumą arba suteikti individualias teises, duomenų valdytojas turėtų nustatyti, ar (o jei taip, kurie) duomenys yra susiję su prašymą teikiančiu asmeniu, o tai aiškiai draudžiama pagal AIAĮ (AIAĮ 28-5 straipsnio 1 dalis). Be to, kai toks reidentifikavimas apima viso duomenų rinkinio (kuriam suteikti pseudonimai) pseudonimų panaikinimą, visų kitų susijusių asmenų asmeninei informacijai kiltų didesnė rizika. Reglamente (ES) 2016/679 nurodomi atvejai, kai duomenų reidentifikavimas praktiškai neįmanomas, tačiau AIAĮ laikomasi griežtesnio požiūrio aiškiai uždraudžiant reidentifikuoti duomenis visais atvejais, kai tvarkoma informacija, kuriai suteikti pseudonimai.
- (83) Todėl, kaip aprašyta (74)–(82) konstatuojamosiose dalyse, Korėjos sistemoje nustatytos su duomenų subjektų teisėmis susijusios taisyklės, kuriomis užtikrinamas iš esmės toks pat apsaugos lygis, koks nustatytas pagal Reglamentą (ES) 2016/679.

⁽¹⁰⁹⁾ Taip pat žr. AIAĮ 30 straipsnio 1 dalies 5 punktą dėl privatumo politikos, kurioje, be kita ko, pateikiama informacija apie asmens teises ir apie tai, kaip jomis naudotis.

⁽¹¹⁰⁾ Taip pat žr. AIAĮ 39-7 straipsnio 2 dalį dėl informacijos ir ryšių paslaugų teikėjų.

⁽¹¹¹⁾ Išskirtiniu atveju tiesioginį ryšį su duomenų subjektu ES Korėjos ekonominės veiklos vykdytojas gali turėti greičiausiai dėl to, kad jis asmeniui Europos Sąjungoje siūlė prekes ar paslaugas arba stebėjo jo elgesį. Šiuo atveju Korėjos ekonominės veiklos vykdytojui bus taikomas Reglamentas (ES) 2016/679 (3 straipsnio 2 dalis), todėl jis turės tiesiogiai laikytis ES duomenų apsaugos teisės nuostatų.

⁽¹¹²⁾ Taip pat žr. pranešimą 2021-5, kuriuo patvirtinama, kad AIAĮ III skirsnis (įskaitant 28-7 straipsnį) taikomas tik tada, kai informacija, kuriai suteikti pseudonimai, viešojo intereso pagrindu tvarkoma mokslinių tyrimų, statistikos arba archyvavimo tikslu (žr. šio sprendimo I priedo 4 skirsnį).

2.3.9. Tolesnis perdavimas

- (84) Asmens duomenims, perduodamiems iš Sąjungos duomenų valdytojams Korėjoje, užtikrinamas apsaugos lygis neturėtų sumažėti tokius duomenis toliau perduodant gavėjams trečiojoje valstybėje.
- (85) Korėjos duomenų valdytojo atžvilgiu tokie „tolesni pervedimai“ yra tarptautiniai pervedimai iš Korėjos Respublikos. Šiuo atžvilgiu AIAI atskiria duomenų tvarkymo perdavimą užsakomųjų paslaugų teikėjui (t. y. duomenų tvarkytojui) ir asmens duomenų teikimą trečiosioms šalims ⁽¹¹³⁾.
- (86) Pirma, kai asmens duomenų tvarkymas perduodamas trečiojoje valstybėje esančiam subjektui, Korėjos duomenų valdytojas turi užtikrinti, kad būtų laikomasi AIAI nuostatų dėl užsakomųjų paslaugų (AIAI 26 straipsnis). Tai apima teisiškai privalomas priemones (kuria, be kita ko, užsakomųjų paslaugų teikėjo atliekamas duomenų tvarkymas apribojamas tik duomenų tvarkymu užsakomojo darbo tikslu, nustatomos techninės ir valdymo apsaugos priemonės ir apribojimai, susiję su duomenų tvarkymo subranga (žr. AIAI 26 straipsnio 1 dalį)) taikymą ir informacijos apie užsakomąjį darbą skelbimą. Duomenų valdytojas taip pat privalo mokyti užsakomųjų paslaugų teikėją, kaip imtis būtinų saugumo priemonių, ir jį prižiūrėti, be kita ko, tikrinant, ar užsakomųjų paslaugų teikėjas laikosi visų duomenų valdytojo įsipareigojimų pagal AIAI ⁽¹¹⁴⁾ ir įsipareigojimų pagal užsakomųjų paslaugų sutartį.
- (87) Jeigu asmens duomenis tvarkantis užsakomųjų paslaugų teikėjas pažeidęs AIAI padaro žalą, atsakomybė už ją priskiriama duomenų valdytojui, taip pat kaip ir duomenų valdytojo darbuotojo padarytos žalos atveju (AIAI 26 straipsnio 6 dalis). Todėl Korėjos duomenų valdytojas lieka atsakingas už asmens duomenis, kurie buvo perduoti su tikslu gauti užsakomąsias paslaugas, ir privalo užtikrinti, kad užsienio valstybės duomenų tvarkytojas informaciją tvarkytų vadovaudamasis AIAI. Jeigu užsakomųjų paslaugų teikėjas tvarko informaciją pažeisdamas AIAI, Korėjos duomenų valdytojas gali būti laikomas atsakingu už savo prievolės užtikrinti, kad būtų laikomasi AIAI, pavyzdžiui, vykdant užsakomųjų paslaugų teikėjo priežiūrą, nevykdymą. Užsakomųjų paslaugų sutartyje numatytais apsaugos priemonėmis ir Korėjos duomenų valdytojo atsakomybe už užsakomųjų paslaugų teikėjo veiksmus užtikrinamas apsaugos tęstinumas, kai asmens duomenys tvarkomi ne Korėjoje esančio užsakomųjų paslaugų teikėjo.
- (88) Antra, Korėjos duomenų valdytojai gali teikti asmens duomenis ne Korėjoje esančiai trečiajai šaliai. Nors AIAI yra numatyta keletas teisinių pagrindų, kuriais remiantis apskritai leidžiama pateikti duomenis trečiosioms šalims, jei trečioji šalis yra ne Korėjoje, iš esmės ⁽¹¹⁵⁾ duomenų valdytojas turi gauti duomenų subjekto sutikimą ⁽¹¹⁶⁾ jam pateikęs informaciją apie: 1) asmens duomenų rūšį, 2) asmens duomenų gavėją, 3) duomenų perdavimo tikslą, t. y. gavėjo siekiamą duomenų tvarkymo tikslą, 4) laikotarpį, kurį duomenų gavėjas duomenis saugo duomenų tvarkymo tikslu, ir 5) tai, kad duomenų subjektas gali atsisakyti duoti sutikimą (AIAI 17 straipsnio 2 ir 3 dalys). Pranešimo 2021-5 skirsnyje dėl skaidrumo (žr. (70) konstatuojamąją dalį) reikalaujama, kad asmenys būtų informuojami apie trečiąją valstybę, į kurią bus teikiami jų duomenys. Taip užtikrinama, kad duomenų subjektai Sąjungoje galėtų priimti visapusiškai informacija pagrįstą sprendimą dėl to, ar sutikti su nuostata dėl informacijos teikimo užsienio valstybių trečiosioms šalims. Be to, duomenų valdytojas negali sudaryti sutarties su trečiaja šalimi (gavėju), jei taip pažeidžiamas AIAI, o tai reiškia, kad sutartyje negali būti numatyta prievolių, kuriomis prieštaraujama duomenų valdytojui AIAI nustatytiems reikalavimams ⁽¹¹⁷⁾.

⁽¹¹³⁾ Informacijos ir ryšių paslaugų teikėjams taikomos specialios taisyklės. Pagal AIAI 39-12 straipsnį informacijos ir ryšių paslaugų teikėjai iš esmės turi gauti naudotojo sutikimą dėl bet kokio asmeninės informacijos perdavimo į užsienio valstybę. Tais atvejais, kai asmeninė informacija perduodama siekiant gauti duomenų tvarkymo operacijų užsakomąsias paslaugas, įskaitant duomenų saugojimą, sutikimo nereikalaujama, jei atitinkami asmenys tiesiogiai arba viešai pranešant informuojami tokiu būdu, kad būtų galima lengvai susipažinti su: 1) perduotinos informacijos ypatybėmis, 2) valstybe, į kurią informacija bus perduota (taip pat perdavimo data ir būdu), 3) gavėjo pavadinimu ir 4) gavėjo naudojimo ir saugojimo tikslu (AIAI 39-12 straipsnio 3 dalis). Be to, tokiu atveju bus taikomi bendrieji užsakomųjų paslaugų reikalavimai. Kiekvienam perdavimui turi būti taikomos specialios apsaugos priemonės, susijusios su saugumu, skundų ir ginčų nagrinėjimu, taip pat kitos priemonės, būtinos naudotojų informacijai apsaugoti (AIAI vykdymo užtikrinimo dekreto 48-10 straipsnis).

⁽¹¹⁴⁾ Taip pat žr. AIAI 26 straipsnio 7 dalį, pagal kurią 15–25, 27–31, 33–38 ir 50 straipsnis duomenų tvarkytojui taikomi *mutatis mutandis*.

⁽¹¹⁵⁾ Informacijos ir ryšių paslaugų teikėjams naudotojų asmeninę informaciją teikiant trečiosioms šalims naudotojo sutikimas reikalingas visada (AIAI 39-12 straipsnio 2 dalis).

⁽¹¹⁶⁾ Kaip išsamiau paaiškinta 51 išnašoje, kad toks sutikimas galiotų, jis turi būti duotas laisva valia, pagrįstas informacija ir konkretus.

⁽¹¹⁷⁾ Taip pat žr. AIAI 39-12 straipsnio 1 dalį dėl informacijos ir ryšių paslaugų teikėjų.

- (89) Be asmens sutikimo asmens duomenys trečiajai šaliai (užsienio valstybėje) gali būti teikiami, kai atskleidimo tikslas yra „pakankamai susijęs“ su pradiniu rinkiniu tikslu (AIAI 17 straipsnio 4 dalis, žr. (36) konstatuojamąją dalį). Tačiau sprendamas, ar atskleisti asmens duomenis „susijusiu“ tikslu, duomenų valdytojas turi atsižvelgti į tai, ar dėl atskleidimo asmuo patiria nepatogumų ir ar imtasi būtinų saugumo priemonių (pavyzdžiui, šifravimo). Atsižvelgiant į tai, kad trečioji valstybė, į kurią perduodami asmens duomenys, negali suteikti apsaugos, panašios į apsaugą, numatytą pagal AIAI, pranešimo 2021-5 2 skirsnyje pripažįstama, kad tokių nepatogumų gali kilti ir jų galima išvengti tik tuo atveju, jei Korėjos duomenų valdytojas ir užsienio valstybės duomenų gavėjas teisiškai įpareigojančia priemone (pavyzdžiui, sutartimi) užtikrina tokį apsaugos lygį, kuris būtų lygiavertis nustatytam AIAI, be kita ko, duomenų subjektų teisių atžvilgiu.
- (90) Specialios taisyklės taikomos atskleidimui „kitu tikslu“, t. y. duomenų teikimui trečiajai šaliai nauju (nesusijusiu) tikslu, ir toks atskleidimas gali būti atliekamas tik remiantis vienu iš AIAI 18 straipsnio 2 dalyje nurodytų pagrindų, kaip aprašyta (39) konstatuojamojoje dalyje. Tačiau net taikant tokias sąlygas duomenų teikimas trečiajai šaliai neleidžiamas, jei yra tikėtina, kad bus „nepagrįstai pažeisti“ duomenų subjekto arba trečiosios šalies interesai, o tam reikalinga suderinti interesus. Be to, pagal AIAI 18 straipsnio 5 dalį duomenų valdytojas turi taikyti papildomas apsaugos priemones, įskaitant galimybę reikalauti, kad trečioji šalis apribotų duomenų tvarkymo tikslą ir būdą, arba nustatyti specialias saugumo priemones. Vėlgi atsižvelgiant į tai, kad trečioji valstybė, į kurią perduodami asmens duomenys, negali suteikti apsaugos, panašios į apsaugą, numatytą pagal AIAI, pranešimo 2021-5 2 skirsnyje pripažįstama, kad toks asmens arba trečiosios šalies interesų „nepagrįstas pažeidimas“ gali įvykti ir jo galima išvengti tik tuo atveju, jei Korėjos duomenų valdytojas ir užsienio valstybės duomenų gavėjas teisiškai įpareigojančia priemone (pavyzdžiui, sutartimi) užtikrina tokį apsaugos lygį, kuris būtų lygiavertis nustatytam AIAI, be kita ko, duomenų subjektų teisių atžvilgiu.
- (91) Todėl kai asmens duomenys iš Korėjos Respublikos perduodami toliau (užsakomųjų paslaugų teikėjui arba trečiajai šaliai), (86)–(90) konstatuojamosiose dalyse išdėstytais taisyklėmis užtikrinamas apsaugos tęstinumas, kuris iš esmės atitinka apsaugą, numatytą pagal Reglamentą (ES) 2016/679.

2.3.10. Atskaitomybė

- (92) Pagal atskaitomybės principą duomenis tvarkantys subjektai privalo nustatyti tinkamas technines ir organizacines priemones, kad veiksmingai laikytųsi savo duomenų apsaugos prievolių ir galėtų įrodyti (visų pirma kompetentingai priežiūros institucijai), kad jų laikosi.
- (93) Pagal AIAI 3 straipsnio 6 ir 8 dalis duomenų valdytojas turi tvarkyti asmens duomenis „taip, kad būtų sumažinta galimybė pažeisti“ duomenų subjekto privatumą, ir stengiasi pelnyti duomenų subjekto pasitikėjimą atsižvelgdamas į tokias pareigas ir užduotis ir jas vykdydamas, kaip numatyta AIAI ir kituose įstatymuose. Tai apima vidaus valdymo plano parengimą (AIAI 29 straipsnis), taip pat tinkamą darbuotojų mokymą ir priežiūrą (AIAI 28 straipsnis).
- (94) Siekiant užtikrinti atskaitomybę, AIAI 31 straipsniu kartu su AIAI vykdymo užtikrinimo dekretu 32 straipsniu duomenų valdytojai įpareigojami paskirti privatumo apsaugos pareigūną, kuris „visapusiškai prisiima atsakomybę už asmeninės informacijos tvarkymą“. Visų pirma tokiam privatumo apsaugos pareigūnui pavedama atlikti šias funkcijas: 1) parengti ir įgyvendinti asmens duomenų apsaugos planą ir parengti privatumo politiką, 2) reguliariai atlikti asmens duomenų tvarkymo būklės ir praktikos tyrimus, siekiant pašalinti trūkumus, 3) nagrinėti skundus ir skirti žalos atlyginimo kompensacijas, 4) sukurti vidaus kontrolės sistemą, skirtą užkirsti kelią asmens duomenų atskleidimui, piktnaudžiavimui jais ar netinkamam jų naudojimui, 5) parengti ir įgyvendinti mokymo programą, 6) įgyvendinti asmens duomenų bylų apsaugą, kontrolę ir valdymą ir 7) sunaikinti asmens duomenis pasiekus tvarkymo tikslą arba pasibaigus saugojimo laikotarpiui. Vykdydamas šias pareigas privatumo apsaugos pareigūnas gali tikrinti asmens duomenų tvarkymo ir susijusių sistemų būklę ir prašyti apie juos informacijos (AIAI 31 straipsnio 3 dalis). Jei privatumo apsaugos pareigūnas sužino apie bet kokią AIAI ar kitų atitinkamų duomenų apsaugos įstatymų pažeidimą, jis nedelsdamas imasi taisomųjų veiksmų ir prirėkęs apie tokius veiksmus praneša duomenų valdytojo vadovybei (vadovui) (AIAI 31 straipsnio 4 dalis). Pagal AIAI 31 straipsnio 5 dalį privatumo apsaugos pareigūnas dėl šių funkcijų vykdymo neturi patirti nepagrįstų nepatogumų.

- (95) Be to, duomenų valdytojai turi aktyviai stengtis atlikti poveikio privatumui vertinimą tuo atveju, kai naudojant asmens duomenų bylas kyla pavojus privatumui (AIAĮ 33 straipsnio 8 dalis). Remiantis AIAĮ 33 straipsnio 1 ir 2 dalimis kartu su AIAĮ vykdymo užtikrinimo dekretu 35, 36 ir 38 straipsniais, vertinant duomenų subjektų teisėms kylančios rizikos laipsnį bus svarbūs tokie veiksniai kaip tvarkomų duomenų rūšis ir pobūdis (visų pirma, ar tai neskelbtina informacija), jų apimtis, saugojimo laikotarpis ir duomenų saugumo pažeidimų tikimybė. Poveikio privatumui vertinimo tikslas – užtikrinti, kad būtų analizuojami su privatumu susiję rizikos veiksniai, taip pat saugumo ar kitos atsakomosios priemonės, ir nurodytos tobulintinos sritys (žr. AIAĮ 33 straipsnio 1 dalį kartu su AIAĮ vykdymo užtikrinimo dekretu 38 straipsniu).
- (96) Tvarkydamos tam tikras asmens duomenų bylas, kurių atžvilgiu kyla didesnė galimų privatumo pažeidimų rizika, viešosios institucijos privalo atlikti poveikio vertinimą (AIAĮ 33 straipsnio 1 dalis). Pagal AIAĮ vykdymo užtikrinimo dekretu 35 straipsnį tai taikoma, be kita ko, byloms, kuriose yra neskelbtinos informacijos apie ne mažiau kaip 50 000 duomenų subjektų, byloms, kurios bus sujungtos su kitomis bylomis ir dėl to jose bus informacijos apie ne mažiau kaip 500 000 duomenų subjektų, arba byloms, kuriose yra informacijos apie ne mažiau kaip vieną milijoną duomenų subjektų. Apie viešosios institucijos atlikto poveikio vertinimo rezultatus turi būti pranešta AIAK (AIAĮ 33 straipsnio 1 dalis), kuri gali pateikti savo nuomonę (AIAĮ 33 straipsnio 3 dalis).
- (97) Galiausiai AIAĮ 13 straipsnyje nustatyta, kad AIAK nustato politiką, būtiną duomenų valdytojų „savarankiškai reguliuojamai duomenų apsaugos veiklai“ skatinti ir remti, be kita ko, šviečiant duomenų apsaugos klausimais, skatinant ir remiant duomenų apsaugą vykdančias organizacijas ir padedant duomenų valdytojams nustatyti ir įgyvendinti savarankiško reguliavimo taisyklės. Be to, ji įdiegia ePRIVACY vertinimo sistemą ir palengvina jos taikymą. Šiuo atžvilgiu AIAĮ 32-2 straipsnyje kartu su AIAĮ vykdymo užtikrinimo dekretu 34-2–34-8 straipsniais numatyta galimybė suteikti sertifikatą, kuriuo patvirtinama, kad duomenų valdytojo asmens duomenų tvarkymo ir apsaugos sistema (-os) atitinka AIAĮ reikalavimus. Remiantis šiomis taisyklėmis, sertifikatas ⁽¹¹⁸⁾ gali būti suteiktas (3 metų laikotarpiui), jei duomenų valdytojas atitinka AIAK nustatytus sertifikavimo kriterijus, įskaitant valdymo, techninių ir fizinių apsaugos priemonių taikymo asmens duomenims apsaugoti kriterijų ⁽¹¹⁹⁾. Kad būtų išlaikytas sertifikato patikimumas, AIAK bent kartą per metus turi patikrinti su sertifikatu susijusias duomenų valdytojo sistemas, todėl sertifikatas gali būti atšauktas (AIAĮ 32 straipsnio 4 dalis kartu su AIAĮ vykdymo užtikrinimo dekretu 34-5 straipsniu; vadinamasis „tęstinis valdymas“).
- (98) Todėl Korėjos sistemoje atskaitomybės principas įgyvendinamas taip, kad būtų užtikrintas iš esmės toks pat apsaugos lygis, koks užtikrinamas pagal Reglamentą (ES) 2016/679, be kita ko, numatant įvairius mechanizmus, kuriais užtikrinama ir įrodoma, kad laikomasi AIAĮ.

2.3.11. Specialios taisyklės dėl asmeninės kredito informacijos tvarkymo

- (99) Kaip aprašyta (13) konstatuojamojoje dalyje, KIĮ nustatytos specialios taisyklės, kuriomis vadovaudamiesi komercinės veiklos vykdytojai tvarko asmeninę kredito informaciją. Todėl tvarkydami asmeninę kredito informaciją komercinės veiklos vykdytojai turi laikytis AIAĮ bendrųjų reikalavimų, išskyrus atvejus, kai KIĮ nustatytos konkrečios taisyklės. Taip bus, pavyzdžiui, komercinio sandorio su asmeniu metu jiems tvarkant informaciją, susijusią su kredito kortele arba banko sąskaita. KIĮ, kaip sektorių teisės aktu dėl kredito informacijos (tiek asmeninės, tiek neasmeninės) tvarkymo, nustatomos ne tik konkrečios duomenų apsaugos priemonės (pavyzdžiui, dėl skaidrumo ir saugumo), bet ir apskritai reglamentuojamos konkrečios aplinkybės, kurioms esant gali būti tvarkoma asmeninė kredito informacija. Tai visų pirma atspindėta išsamiuose tokių duomenų naudojimo, teikimo trečiajai šaliai ir saugojimo reikalavimuose.
- (100) Kaip ir AIAĮ, KIĮ nustatyti teisėtumo ir proporcingumo principai. Pirma, KIĮ 15 straipsnio 1 dalyje numatytas bendras reikalavimas, kad asmeninę kredito informaciją galima rinkti tik pagrįstomis ir sąžiningomis priemonėmis ir tik tokį jos kiekį, koks yra būtinas konkrečiam tikslui pasiekti pagal AIAĮ 3 straipsnio 1 ir 2 dalis. Antra, KIĮ konkrečiai reglamentuojamas asmeninės kredito informacijos tvarkymo teisėtumas apribojant jos rinkimą, naudojimą bei teikimą trečiajai šaliai ir paprastai susiejant šią duomenų tvarkymo veiklą su atitinkamo asmens sutikimo reikalavimu.

⁽¹¹⁸⁾ Be to, jei duomenų valdytojas ketina nurodyti sertifikatą vykdydamas verslo veiklą arba skatinti jį naudoti, jis gali naudoti AIAK nustatytą asmeninės informacijos apsaugos ženklą. Žr. AIAĮ vykdymo užtikrinimo dekretu 34-7 straipsnį.

⁽¹¹⁹⁾ Nuo 2018 m. lapkričio mėn. veikia Asmeninės informacijos ir informacijos saugumo valdymo sistema (ISMS-P), skirta patvirtinti, kad duomenų valdytojai naudoja išsamią valdymo sistemą.

- (101) Asmeninė kredito informacija gali būti renkama remiantis vienu iš AIAI nurodytų pagrindų arba KIĮ nurodytais specialiais pagrindais. Atsižvelgiant į tai, kad Reglamento (ES) 2016/679 45 straipsnyje suponuojama, kad asmens duomenis perduoda duomenų valdytojas arba duomenų tvarkytojas Sąjungoje, tačiau jis neapima duomenų valdytojo Korėjoje vykdomo tiesioginio duomenų rinkimo (pvz., iš asmens arba interneto svetainės), šio sprendimo atžvilgiu svarbus tik sutikimas ir AIAI nustatyti duomenų rinkimo pagrindai. Šie pagrindai visų pirma apima atvejus, kai perdavimas yra būtinas sutarčiai su asmeniu įvykdyti arba dėl Korėjos duomenų valdytojo teisėtų interesų (AIAI 15 straipsnio 1 dalies 4 ir 6 punktai) ⁽¹²⁰⁾.
- (102) Surinkta asmeninė kredito informacija gali būti naudojama 1) siekiant pradinio tikslo, kuriuo asmuo ją (tiesiogiai) pateikė ⁽¹²¹⁾, 2) siekiant tikslo, suderinamo su pradiniu duomenų rinkimo tikslu ⁽¹²²⁾, 3) siekiant nustatyti, ar užmegzti arba palaikyti komercinius santykius, dėl kurių asmuo kreipėsi ⁽¹²³⁾, 4) viešojo intereso pagrindu statistikos, mokslinių tyrimų ir archyvavimo tikslais ⁽¹²⁴⁾, jei informacijai yra suteikti pseudonimai ⁽¹²⁵⁾, 5) jei gautas papildomas sutikimas arba 6) pagal įstatymą.
- (103) Jeigu komercinės veiklos vykdytojas ketina atskleisti asmeninę kredito informaciją trečiajai šaliai, jis turi gauti asmens sutikimą ⁽¹²⁶⁾ prieš tai suteikęs asmeniui informaciją apie duomenų gavėją, duomenų gavėjo tvarkymo tikslą, teiktinų duomenų ypatybes, duomenų gavėjo duomenų saugojimo laikotarpį ir teisę atsisakyti duoti sutikimą (KIĮ 32 straipsnio 1 dalis ir KIĮ vykdymo užtikrinimo dekreto 28 straipsnio 2 dalis) ⁽¹²⁷⁾. Šis sutikimo reikalavimas netaikomas konkrečiais atvejais, t. y. kai asmeninė kredito informacija atskleidžiama ⁽¹²⁸⁾: 1) užsakomųjų paslaugų teikėjui užsakomųjų paslaugų teikimo tikslu ⁽¹²⁹⁾, 2) trečiajai šaliai verslo perdavimo, skaidymo arba jungimo atveju, 3) viešojo intereso pagrindu statistikos, mokslinių tyrimų ir archyvavimo tikslais, kai informacijai yra suteikti pseudonimai, 4) siekiant tikslo, suderinamo su pradiniu duomenų rinkimo tikslu, 5) trečiajai šaliai, kuri naudoja informaciją asmens skolai susigrąžinti ⁽¹³⁰⁾, 6) siekiant vykdyti teismo nutartį,

⁽¹²⁰⁾ KIĮ taip pat apima kitus teisinius duomenų rinkimo pagrindus, t. y. kai to reikalaujama įstatymais, kai informaciją viešai skelbia viešoji institucija pagal teisės aktus dėl informacijos laisvės arba kai informacija prieinama socialiniame tinkle. Kad komercinės veiklos vykdytojas galėtų remtis paskutiniu nurodytu pagrindu, jis turi galėti įrodyti, kad duomenų rinkimas patenka į duomenų subjekto sutikimo taikymo sritį, remdamasis pagrįstu („objektyviu“) aiškinimu ir atsižvelgdamas į duomenų pobūdį, jų pateikimo socialiniame tinkle ketinimą ir tikslą, į tai, ar rinkimo tikslas yra „labai svarbus“ tam tikslui ir t. t. (KIĮ vykdymo užtikrinimo dekreto 13 straipsnis). Tačiau, kaip paaiškinta (101) konstatuojamojoje dalyje, šie pagrindai iš esmės nebus svarbūs perdavimo atveju.

⁽¹²¹⁾ Pavyzdžiui, kai kredito informacija sukuriama ir (arba) teikiama vykdant komercinį sandorį su asmeniu. Tačiau šiuo pagrindu negalima remtis siekiant asmeninę kredito informaciją naudoti tiesioginiais rinkodaros tikslais (žr. KIĮ 33 straipsnio 1 dalies 3 punktą).

⁽¹²²⁾ Siekiant nustatyti, ar naudojimo tikslas yra suderinamas su pradiniu rinkimo tikslu, reikia atsižvelgti į šiuos veiksnius: 1) šių dviejų tikslų ryšį („svarbą“ vienas kitam), 2) informacijos rinkimo būdą, 3) naudojimo poveikį asmeniui ir 4) ar buvo įgyvendintos tinkamos saugumo priemonės, pavyzdžiui, pseudonimų suteikimas (žr. KIĮ 32 straipsnio 6 dalies 9-4 punktą).

⁽¹²³⁾ Pavyzdžiui, duomenų valdytojui gali reikėti atsižvelgti į iš asmens gautą asmeninę kredito informaciją, kad nuspręstų, ar pratęsti to asmens paskolos terminą.

⁽¹²⁴⁾ KIĮ 33 straipsnis kartu su KIĮ 32 straipsnio 6 dalies 9-2, 9-4 ir 10 punktais.

⁽¹²⁵⁾ KIĮ 2 straipsnio 15 dalyje pseudonimų suteikimas apibrėžiamas kaip asmens kredito informacijos tvarkymas taip, kad remiantis informacija nebebūtų galima nustatyti asmens tapatybės, nebent naudojant ją kartu su papildoma informacija. Nors KIĮ numatytos specialios apsaugos priemonės, taikomos viešojo intereso pagrindu tvarkant informaciją, kuriai suteikti pseudonimai, statistikos, mokslinių tyrimų ir archyvavimo tikslais (KIĮ 40-2 straipsnis), šios taisyklės netaikomos komercinėms organizacijoms. Pastarosioms ir toliau taikomi specialūs AIAI III skirsnio reikalavimai, kaip aprašyta (42)–(48) konstatuojamosiose dalyse. Be to, KIĮ 40-3 straipsnyje nustatyta, kad kredito informacijos, kuriai suteikti pseudonimai, tvarkymui, kai tai daroma viešojo intereso pagrindu statistikos, mokslinių tyrimų ar archyvavimo tikslais, netaikomi skaidrumo ir asmens teisių reikalavimai, panašiai kaip nustatyta AIAI 28-7 straipsnyje, ir taikomos AIAI III skirsnyje nustatytos apsaugos priemonės, kaip išsamiau aprašyta (42)–(48) konstatuojamosiose dalyse.

⁽¹²⁶⁾ Tai netaikoma tais atvejais, kai informacija trečiajai šaliai teikiama siekiant užtikrinti asmeninės kredito informacijos tikslumą ir aktualumą, jei tokio jos teikimo siekiama pradinio tvarkymo tikslo (KIĮ 32 straipsnio 1 dalis). Taip gali būti, pavyzdžiui, kai kredito reitingų agentūrai pateikiama naujausia informacija, siekiant užtikrinti, kad jos įrašai būtų tikslūs.

⁽¹²⁷⁾ Jei pirmiau minėtos informacijos pateikti neįmanoma, gali pakakti nurodyti asmeniui dėl reikalingos informacijos kreiptis į informaciją gaunantį trečiąjį asmenį.

⁽¹²⁸⁾ Atsižvelgiant į tai, kad KIĮ konkrečiai neregulmentuojami atvejai, kai užsienio valstybės subjektas atskleidžia asmeninę kredito informaciją, toks atskleidimas turi atitikti pranešimo Nr. 2021-5 2 skirsnyje nustatytas tolesnio perdavimo apsaugos priemones.

⁽¹²⁹⁾ Užsakomųjų paslaugų teikėjas tvarkyti asmeninę kredito informaciją gali tik rašytinės sutarties pagrindu ir jei laikomasi AIAI 26 straipsnio 1–3 ir 5 dalių reikalavimų, kaip nurodyta (20) konstatuojamojoje dalyje (KIĮ 17 straipsnis ir KIĮ vykdymo užtikrinimo dekreto 14 straipsnis). Užsakomųjų paslaugų teikėjas negali naudoti informacijos tokiu būdu, kuris viršija užsakomųjų paslaugų teikimą, o užsakomųjų paslaugų bendrovė turi nustatyti specialius saugumo reikalavimus (pvz., šifravimą) ir šviesti užsakomųjų paslaugų teikėją, kaip išvengti kredito informacijos praradimo, pavogimo, atskleidimo, keitimo ar pavojaus saugumui kėlimo.

⁽¹³⁰⁾ Taip pat žr. KIĮ vykdymo užtikrinimo dekreto 28 straipsnio 10 dalies 1, 2 ir 6 punktus.

- 7) prokurorui ir (arba) teismo policijos pareigūnui ekstremaliosios situacijos atveju, kai gresia pavojus asmens gyvybei arba tikėtina, kad jis patirs kūno sužalojimą, ir nėra laiko išduoti teismo orderį⁽¹³¹⁾, 8) kompetentingoms mokesčių institucijoms siekiant laikytis mokesčių įstatymų arba 9) vadovaujantis kitais įstatymais. Jeigu informacija atskleidžiama remiantis vienu iš šių pagrindų, duomenų subjektui apie tai turi būti pranešta iš anksto (KIĮ 32 straipsnio 7 dalis).
- (104) KIĮ taip pat konkrečiai reglamentuojama asmeninės kredito informacijos tvarkymo, remiantis vienu iš tų naudojimo ar pateikimo trečiajai šaliai pagrindų, trukmė pasibaigus komerciniams santykiams su asmeniu⁽¹³²⁾. Gali būti saugoma tik ta informacija, kuri buvo būtina šiems santykiams užmegzti arba išlaikyti, taikant papildomas apsaugos priemones (ji turi būti saugoma atskirai nuo kredito informacijos, susijusios su asmenimis, su kuriais palaikomi komerciniai santykiai, apsaugota taikant specialias saugumo priemones ir prieinama tik įgaliotiems asmenims)⁽¹³³⁾. Visi kiti duomenys turi būti ištrinti (KIĮ vykdymo užtikrinimo dekreto 17-2 straipsnio 1 dalies 2 punktas). Siekiant nustatyti, kurie duomenys buvo reikalingi komerciniams santykiams įgyvendinti, reikia atsižvelgti į įvairius veiksnius, įskaitant tai, ar būtų buvę įmanoma užmegzti santykius neturint šių duomenų ir ar jie tiesiogiai susiję su asmeniui teiktomis prekėmis ar paslaugomis (KIĮ vykdymo užtikrinimo dekreto 17-2 straipsnio 2 dalis).
- (105) Tais atvejais, kai asmeninė kredito informacija iš esmės galėtų būti saugoma pasibaigus komerciniams santykiams, ji vis tiek turėtų būti ištrinta per tris mėnesius nuo tada, kai buvo pasiektas tolesnis duomenų tvarkymo tikslas⁽¹³⁴⁾, arba bet kuriuo atveju po penkerių metų (KIĮ 20-2 straipsnis). Tam tikromis aplinkybėmis asmeninė kredito informacija gali būti saugoma ilgiau nei penkerius metus, visų pirma tais atvejais, kai tai būtina siekiant įvykdyti teisinę prievolę, kai tai būtina siekiant patenkinti gyvybiškai svarbius asmens gyvybės išsaugojimo, fizinius ar turtinius interesus, kai reikia archyvuoti informaciją, kuriai suteikti pseudonimai (kuri viešojo intereso pagrindu buvo naudojama mokslinių tyrimų, statistikos ar archyvavimo tikslais), arba kai informacija saugoma draudimo tikslais (visų pirma draudimo mokėjimų atveju arba siekiant užkirsti kelią sukčiavimui draudimo srityje)⁽¹³⁵⁾. Šiais išimtiniais atvejais taikomos specialios apsaugos priemonės (kaip antai pranešimas asmeniui apie tolesnį naudojimą, saugomos informacijos atskyrimas nuo informacijos, susijusios su asmenimis, su kuriais vis dar palaikomi komerciniai santykiai, priegos teisių apribojimas, žr. KIĮ vykdymo užtikrinimo dekreto 17-2 straipsnio 1–2 dalis).
- (106) KIĮ taip pat patikslinami tikslumo ir duomenų kokybės principai, reikalaujant, kad asmeninė kredito informacija būtų „registruojama, keičiama ir tvarkoma“ taip, kad ji išliktų tiksli ir aktuali (KIĮ 18 straipsnio 1 dalis ir KIĮ vykdymo užtikrinimo dekreto 15 straipsnio 3 dalis)⁽¹³⁶⁾. Komercinės veiklos vykdytojams kredito informaciją teikiant tam tikriems kitiems subjektams (kaip antai kredito reitingų agentūroms) jiems taikoma konkreti prievolė patikrinti informacijos tikslumą, siekiant užtikrinti, kad gavėjas užregistruotų ir tvarkytų tik tikslią informaciją (KIĮ vykdymo užtikrinimo dekreto 15 straipsnio 1 dalis kartu su KIĮ 18 straipsnio 1 dalimi). Apskritai KIĮ reikalaujama saugoti įrašus apie asmeninės kredito informacijos rinkimą, naudojimą, atskleidimą trečiosioms šalims ir sunaikinimą (KIĮ 20 straipsnio 2 dalis)⁽¹³⁷⁾.
- (107) Be to, asmeninės kredito informacijos tvarkymui taikomi specialūs duomenų saugumo reikalavimai. Visų pirma KIĮ reikalaujama įgyvendinti technologines, fizines ir organizacines priemones, kuriomis būtų užkirstas kelias neteisėtai prieigai prie kompiuterinių sistemų, taip pat tvarkomų duomenų keitimui, sunaikinimui ar kitokiam duomenims kylančiam pavojui (pavyzdžiui, taikant priegos kontrolę, žr. KIĮ 19 straipsnį ir KIĮ vykdymo užtikrinimo dekreto 16 straipsnį). Be to, asmenine kredito informacija keičiantis su trečiaja šalimi turi būti sudarytas susitarimas, kuriame būtų nustatytos specialios saugumo priemonės (KIĮ 19 straipsnio 2 dalis). Įvykus asmeninės kredito informacijos saugumo pažeidimui turi būti imtasi priemonių bet kokiai žalai sumažinti ir apie tai turi būti nedelsiant pranešta atitinkamiems asmenims (KIĮ 39-4 straipsnio 1 ir 2 dalys). Be to, AIAK turi būti informuojama apie fiziniams asmenims pateiktą pranešimą ir įgyvendintas priemones (KIĮ 39-4 straipsnio 4 dalis).

⁽¹³¹⁾ Tokiu atveju išduoti orderį turi būti prašoma nedelsiant. Jei orderis neišduodamas per 36 valandas, gauti duomenys turi būti nedelsiant ištrinti (KIĮ 32 straipsnio 6 dalies 6 punktas).

⁽¹³²⁾ Pavyzdžiui, kai įvykdžius sutartinius įsipareigojimus viena iš šalių pasinaudojo savo teise nutraukti sutartį ir t. t., žr. KIĮ vykdymo užtikrinimo dekreto 17-2 straipsnio 5 dalį.

⁽¹³³⁾ KIĮ 20-2 straipsnio 1 dalis ir KIĮ vykdymo užtikrinimo dekreto 17-2 straipsnio 1 dalies 1 punktas.

⁽¹³⁴⁾ Nustatant šį laikotarpį atsižvelgiama į tai, kad ištrinti duomenis nedelsiant dažnai bus neįmanoma, nes paprastai tam reikia imtisi tam tikrų veiksmų (pvz., atskirti ištrintinus duomenis nuo kitų duomenų ir atlikti ištyrimą nedarant poveikio informacinių sistemų stabilumui), kuriems įgyvendinti reikia šiek tiek laiko.

⁽¹³⁵⁾ KIĮ 20-2 straipsnio 2 dalis.

⁽¹³⁶⁾ KIĮ 18 straipsnio 2 dalyje ir KIĮ vykdymo užtikrinimo dekreto 15 straipsnio 4 dalyje nustatytos konkretnės taisyklės dėl šio įrašų saugojimo reikalavimo, pvz., dėl įrašų, kurie susiję su informacija, kuri gali pakenkti asmeniui, pavyzdžiui, informacija apie nusikalstamumą ir bankrotą.

⁽¹³⁷⁾ Kitų atskaitomybės mechanizmų atžvilgiu KIĮ reikalaujama, kad tam tikros organizacijos (pvz., kooperatinės bendrovės ir viešosios bendrovės, žr. KIĮ vykdymo užtikrinimo dekreto 21 straipsnio 2 dalį) paskirtų „kredito informacijos administratorių ir (arba) sergėtoją“, kuris būtų atsakingas už KIĮ laikymosi stebėseną ir atliktų „privatumo apsaugos pareigūno“ funkcijas pagal AIAĮ (KIĮ 20 straipsnio 3 ir 4 dalys).

- (108) KIĮ taip pat nustatytos specialios skaidrumo prievolės, kai siekiama gauti sutikimą naudoti arba teikti asmeninę kredito informaciją (KIĮ 32 straipsnio 4 dalis, 34-2 straipsnis ir KIĮ vykdymo užtikrinimo dekreto 30-3 straipsnis) ir apskritai prieš pateikiant informaciją trečiajai šaliai (KIĮ 32 straipsnio 7 dalis) ⁽¹³⁸⁾. Be to, asmenys turi teisę paprašę gauti informaciją apie jų kredito informacijos naudojimą ir teikimą trečiosioms šalims trejus metus iki prašymo pateikimo (įskaitant tokio naudojimo ir (arba) teikimo tikslą ir datą) ⁽¹³⁹⁾.
- (109) Pagal KIĮ asmenys taip pat turi teisę susipažinti su savo asmenine kredito informacija (KIĮ 38 straipsnio 1 dalis) ir reikalauti ištaisyti netikslius duomenis (KIĮ 38 straipsnio 2 ir 3 dalys) ⁽¹⁴⁰⁾. Be to, be AIAĮ nustatytos bendros teisės prašyti ištrinti duomenis (žr. (77) konstatuojamąją dalį), KIĮ numatyta konkrečiai teisė prašyti ištrinti asmeninę kredito informaciją, kuri buvo saugoma pasibaigus saugojimo laikotarpiams, nurodytiems (104) konstatuojamojoje dalyje, t. y. penkeriems metams (asmeninės kredito informacijos, kuri buvo būtina komerciniams santykiams užmegzti ar išlaikyti, atveju) arba trimis mėnesiais (kitų rūšių asmeninės kredito informacijos atveju) ⁽¹⁴¹⁾. Išimtiniais atvejais, kai duomenis būtina toliau saugoti esant (105) konstatuojamojoje dalyje aprašytoms aplinkybėms, prašymas ištrinti duomenis gali būti atmestas. Jei asmuo prašo ištrinti duomenis, tačiau jiems taikoma viena iš išimčių, kredito informacijai turi būti taikomos specialios apsaugos priemonės (KIĮ 38-3 straipsnio 3 dalis ir KIĮ vykdymo užtikrinimo dekreto 33-3 straipsnis). Pavyzdžiui, informacija turi būti saugoma atskirai nuo kitos informacijos, su ja gali susipažinti tik įgaliotas asmuo ir jai turi būti taikomos specialios saugumo priemonės.
- (110) Be (109) konstatuojamojoje dalyje minėtų teisių, KIĮ asmenims garantuojama teisė reikalauti, kad duomenų valdytojas nebandytų su jais susisiekti tiesioginės rinkodaros tikslais (įstatymo 37 straipsnio 2 dalis), ir teisė į duomenų perkeliamumą. Pastarosios teisės atveju KIĮ nustatytas leidimas asmenims prašyti jų asmeninę kredito informaciją perduoti jiems patiems arba tam tikroms trečiosioms šalims (kaip antai finansų įstaigoms ir kredito reitingų bendrovėms). Asmeninė kredito informacija turi būti tvarkoma ir perduodama trečiajai šaliai tokiu formatu, kuriame pateikta informacija gali būti tvarkoma naudojant informacijos apdorojimo priemonę (kaip antai kompiuterį).
- (111) Palyginti su AIAĮ, KIĮ nustatytos taisyklės yra konkretesnės, todėl Komisija mano, kad šiomis taisyklėmis taip pat užtikrinamas toks apsaugos lygis, kuris yra iš esmės lygiavertis pagal Reglamentą (ES) 2016/679 užtikrinamam apsaugos lygiui.

2.4. Priežiūra ir vykdymo užtikrinimas

- (112) Siekiant užtikrinti, kad tinkamas duomenų apsaugos lygis būtų užtikrinamas praktiškai, reikalinga nepriklausoma priežiūros institucija, kuriai suteikti įgaliojimai stebėti, kaip laikomasi duomenų apsaugos taisyklių, ir užtikrinti, kad jų būtų laikomasi. Atlikdama savo pareigas ir naudodamasi savo įgaliojimais ši institucija turėtų veikti visiškai nepriklausomai ir nešališkai.

2.4.1. Nepriklausoma priežiūra

- (113) Korėjos Respublikoje už AIAĮ laikymosi stebėseną ir jo vykdymo užtikrinimą atsakinga nepriklausoma institucija yra AIAK. AIAK sudaro pirmininkas, pirmininko pavaduotojas ir septyni komisijos nariai. Pirmininką ir pirmininko pavaduotoją skiria Prezidentas, remdamasis Ministro Pirmininko rekomendacija. Du iš Komisijos narių Prezidentas skiria remdamasis pirmininko rekomendacija, o penkis – remdamasis Nacionalinės Asamblėjos rekomendacija (iš jų du skiriami vadovaujantis politinės partijos, kuriai priklauso Prezidentas, rekomendacija ir trys rekomendavus kitoms politinėms partijoms (AIAĮ 7-2 straipsnio 2 dalis), o tai padeda kovoti su šališkumu

⁽¹³⁸⁾ Tai apima bendrą reikalavimą informuoti (KIĮ 32 straipsnio 7 dalis) ir konkrečią prievolę dėl skaidrumo, kai informacija, kuria remiantis gali būti nustatytas asmens kreditingumas, pateikiama tam tikriems subjektams, pavyzdžiui, kredito reitingų agentūroms ir kredito informacijos rinkimo agentūroms (KIĮ 35-3 straipsnis ir KIĮ vykdymo užtikrinimo dekreto 30-3 straipsnis), arba kai atsisakoma užmegzti komercinių sandorių santykius arba jie nutraukiami remiantis iš trečiosios šalies gauta asmenine kredito informacija (KIĮ 36 straipsnis ir KIĮ vykdymo užtikrinimo dekreto 31 straipsnis).

⁽¹³⁹⁾ KIĮ 35 straipsnis. Tam tikroms komercinėms organizacijoms, pvz., kooperatinėms bendrovėms ir viešosioms bendrovėms (KIĮ vykdymo užtikrinimo dekreto 21 straipsnio 2 dalis), taikomi papildomi skaidrumo reikalavimai, pvz., viešai skelbti tam tikrą informaciją (KIĮ 31 straipsnis) ir informuoti asmenis apie galimus jų kredito reitingo trūkumus jiems sudarant finansinius sandorius, dėl kurių kyla kredito rizika (KIĮ 35-2 straipsnis).

⁽¹⁴⁰⁾ Sąlygų ir išimčių dėl teisių susipažinti su informacija ir prašyti ją ištaisyti atveju taikomos AIAĮ taisyklės (apibūdintos (76)–(77) konstatuojamosiose dalyse). Be to, papildomos sąlygos nustatytos KIĮ 38 straipsnio 4–8 dalyse ir KIĮ vykdymo užtikrinimo dekreto 33 straipsnyje. Visų pirma, komercinės veiklos vykdytojas ištaišęs arba ištrynęs netikslią kredito informaciją turi apie tai pranešti asmeniui. Be to, apie tai turi būti pranešta bet kuriai trečiajai šaliai, kuriai ši informacija buvo atskleista per pastaruosius šešis mėnesius, ir apie tai turi būti informuotas atitinkamas asmuo. Jei asmuo nėra patenkintas tuo, kaip buvo išnagrinėtas prašymas ištaisyti informaciją, jis gali pateikti prašymą AIAK, kuri patikrina duomenų valdytojo veiksmus ir gali taikyti taisomuosius veiksmus.

⁽¹⁴¹⁾ KIĮ 38-3 straipsnis.

skyrimo procese)⁽¹⁴²⁾. Ši procedūra atitinka duomenų apsaugos institucijų narių skyrimo Sąjungoje reikalavimus (Reglamento (ES) 2016/679 53 straipsnio 1 dalis). Be to, nė vienas komisijos narys negali vykdyti jokios su pelnu susijusios veiklos, politinės veiklos ir užimti pareigų viešojo administravimo srityje arba Nacionalinėje Asamblėjoje (AIAĮ 7-6 straipsnis ir 7-7 straipsnio 1 dalies 3 punktas)⁽¹⁴³⁾. Komisijos nariams taikomos specialios taisyklės, draudžiančios dalyvauti svarstymuose, jei galimas interesų konfliktas (AIAĮ 7-11 straipsnis). AIAK padeda sekretoriatas (7-13 straipsnis), o jos nariai gali sudaryti mažesnes komisijas (sudarytas iš trijų komisijos narių) smulkiems pažeidimams ir pasikartojantiems klausimams spręsti (AIAĮ 7-12 straipsnis).

- (114) Visi AIAK nariai skiriami trejiems metams ir gali būti paskirti dar vienai kadencijai (AIAĮ 7-4 straipsnio 1 dalis). Komisijos nariai gali būti atleisti tik ypatingomis aplinkybėmis, t. y. jei jie nebegali vykdyti savo pareigų dėl ilgalaikio psichikos sutrikimo ar fizinės negalios, veikia pažeisdami įstatymą arba atitinka vieną iš pagrindų, dėl kurių jie negali eiti pareigų⁽¹⁴⁴⁾ (AIAĮ 7-5 straipsnis). Tai suteikia jiems institucinę apsaugą vykdamas savo funkcijas.
- (115) Apskritai AIAĮ 7 straipsnio 1 dalimi aiškiai garantuojamas AIAK nepriklausomumas, o AIAĮ 7-5 straipsnio 2 dalyje reikalaujama, kad komisijos nariai savo pareigas vykdytų nepriklausomai, pagal įstatymą ir remdamiesi savo sąžine⁽¹⁴⁵⁾. Aprašytomis institucinėmis ir procedūrinėmis apsaugos priemonėmis, įskaitant susijusias su AIAK narių skyrimu ir atleidimu, užtikrinama, kad AIAK veiktų visiškai nepriklausomai, neveikiama išorės įtakos ar nurodymų. Be to, AIAK, kaip centrinė administracinė agentūra, kasmet siūlo savo biudžetą (jį Finansų ministerija peržiūri kaip bendro nacionalinio biudžeto dalį prieš jį patvirtinant Nacionalinėje Asamblėjoje) ir yra atsakinga už savo personalo valdymą. AIAK biudžetas šiuo metu sudaro apie 35 milijonus eurų, o joje dirba 154 darbuotojai (40 darbuotojų, besispecializuojančių informacinių ir ryšių technologijų srityje, 32 darbuotojai, daugiausia dėmesio skiriantys tyrimams, ir 40 teisės ekspertų).
- (116) AIAK užduotys ir įgaliojimai daugiausia numatyti AIAĮ 7-8 ir 7-9 straipsniuose, taip pat AIAĮ 61–66 straipsniuose⁽¹⁴⁶⁾. Visų pirma AIAK užduotys apima konsultavimą dėl įstatymų ir kitų teisės aktų, susijusių su duomenų apsauga, duomenų apsaugos politikos ir gairių rengimą, asmens teisių pažeidimų tyrimą, skundų nagrinėjimą ir tarpininkavimą sprendžiant ginčus, AIAĮ laikymosi užtikrinimą, švietimo duomenų apsaugos srities klausimais ir jos propagavimo užtikrinimą, keitimąsi informacija ir bendradarbiavimą su trečiųjų valstybių duomenų apsaugos institucijomis⁽¹⁴⁷⁾.
- (117) Remiantis AIAĮ 68 straipsniu kartu su AIAĮ vykdymo užtikrinimo dekretu 62 straipsniu, tam tikros AIAK užduotys buvo pavestos Korėjos interneto ir saugumo agentūrai, kaip antai: 1) švietimas ir viešieji ryšiai, 2) specialistų mokymas ir poveikio privatumui vertinimo kriterijų rengimas, 3) prašymų paskirti vadinamąja poveikio privatumui vertinimo institucija tvarkymas, 4) prašymų suteikti netiesioginę prieigą prie valdžios

⁽¹⁴²⁾ AIAK komisijos nariais asmenys gali būti skiriami tik tada, jei jie yra: vyresnieji valstybės tarnautojai, atsakingi už asmeninės informacijos reikalus, buvę teisėjai, prokurorai arba advokatai, savo profesiją praktikavę bent 10 metų, buvę vadovai, turintys patirties duomenų apsaugos srityje ir dirbę viešojoje institucijoje arba organizacijoje ilgiau nei trejus metus arba kuriuos rekomendavo tokia institucija arba organizacija, ir buvę docentai, turintys profesinių žinių duomenų apsaugos srityje, kurie bent penkerius metus dirbo akademinėje institucijoje (AIAĮ 7-2 straipsnis).

⁽¹⁴³⁾ Žr. AIAĮ vykdymo užtikrinimo dekretu 4-2 straipsnį.

⁽¹⁴⁴⁾ Žr. AIAĮ 7-7 straipsnį, pagal kurį ne Korėjos piliečiai ir politinių partijų nariai negali tapti AIAK nariais. Tas pats taikytina ir asmenims, kuriems buvo skirtos tam tikros baudžiamosios sankcijos, kurie per pastaruosius penkerius metus buvo atleisti iš pareigų dėl drausminių nuobaudų ir t. t. (AIAĮ 7-7 straipsnis kartu su Valstybės pareigūnų įstatymo 33 straipsniu).

⁽¹⁴⁵⁾ Nors AIAĮ 7 straipsnio 2 dalyje nurodomi bendri Ministro Pirmininko įgaliojimai pagal Vyriausybės organizavimo įstatymo 18 straipsnį sustabdyti ar atšaukti, Prezidentui pritarus, bet kokį neteisėtą ar nepagrįstą centrinės administracinės agentūros sprendimą, tokie įgaliojimai nesuteikiami AIAK tyrimo arba vykdymo užtikrinimo įgaliojimų atveju (žr. AIAĮ 7 straipsnio 2 dalies 1 ir 2 punktus). Remiantis iš Korėjos vyriausybės gautais paaiškinimais, Vyriausybės organizavimo įstatymo 18 straipsniu siekiama Ministrui Pirmininkui suteikti galimybę veikti ypatingų aplinkybių atveju, pvz., tarpininkauti sprendžiant skirtingų vyriausybinių agentūrų nesutarimus. Tačiau nuo 1963 m., kai buvo priimta ši nuostata, Ministras Pirmininkas niekada nepasinaudojo šia galia.

⁽¹⁴⁶⁾ Kai tai būtina užduotims pagal AIAĮ 7-9 straipsnio 1 dalį atlikti, AIAK gali kreiptis į atitinkamus valstybės pareigūnus, duomenų apsaugos ekspertus, pilietines organizacijas ir atitinkamus verslo subjektus dėl jų nuomonės. Be to, AIAK gali prašyti atitinkamos medžiagos, gali teikti rekomendacijas dėl tobulinimo ir tikrinti, ar jos įgyvendinamos (AIAĮ 7-9 straipsnio 2–5 dalys).

⁽¹⁴⁷⁾ Taip pat žr. AIAĮ 9 straipsnį (asmeninės informacijos apsaugos trejų metų pagrindinis planas), AIAĮ 12 straipsnį (Standartinės asmeninės informacijos apsaugos gairės), AIAĮ 13 straipsnį (savireguliacijos skatinimo ir rėmimo politika).

institucijų turimų asmens duomenų tvarkymas (AIAĮ 35 straipsnio 2 dalis) ir 5) prašyti medžiagos ir atlikti patikrinimus, susijusius su skundais, gautais per vadinamąjį privatumo apsaugos skambučių centrą. Jei nagrinėjama skundas, gautus per privatumo apsaugos skambučių centrą, Korėjos interneto ir saugumo agentūra nustato, kad buvo pažeistas įstatymas, ji perduoda bylą AIAK arba prokuratūrai. Galimybė pateikti skundą per privatumo apsaugos skambučių centrą neužkerta kelio asmenims pateikti skundą tiesiogiai AIAK arba kreiptis į AIAK, jei jie mano, kad Korėjos interneto ir saugumo agentūra jų skundo tinkamai neišnagrinėjo.

2.4.2. Vykdyto užtikrinimas, įskaitant sankcijas

- (118) Siekdamas užtikrinti, kad būtų laikomasi AIAĮ, teisės aktų leidėjas suteikė AIAK tyrimo ir vykdyto užtikrinimo įgaliojimus, pradedant rekomendacijų teikimu ir baigiant administracinių baudų skyrimu. Šie įgaliojimai dar papildyti baudžiamųjų sankcijų tvarka.
- (119) Dėl turimų tyrimo įgaliojimų, tais atvejais, kai įtariamas AIAĮ pažeidimas arba apie jį buvo pranešta, arba kai tai būtina siekiant apsaugoti duomenų subjekto teises nuo pažeidimų, AIAK gali atlikti patikrinimus vietoje ir prašyti asmens duomenų valdytojų pateikti visą susijusią medžiagą (pvz., straipsnius ir dokumentus) (AIAĮ 63 straipsnis kartu su AIAĮ vykdyto užtikrinimo dekreto 60 straipsniu) ⁽¹⁴⁸⁾.
- (120) Turėdama vykdyto užtikrinimo įgaliojimus, pagal AIAĮ 61 straipsnio 2 dalį AIAK gali patarti duomenų valdytojams, kaip pagerinti konkrečios duomenų tvarkymo veiklos asmens duomenų apsaugos lygį. Duomenų valdytojai turi sąžiningai stengtis įgyvendinti tokius patarimus ir privalo informuoti AIAK apie rezultatus. Be to, kai yra pagrįsto pagrindo manyti, kad buvo padarytas AIAĮ pažeidimas, o nesiėmus veiksmų gali būti padaryta sunkiai atitaisoma žala, AIAK gali taikyti taisomuosius veiksmus (AIAĮ 64 straipsnio 1 dalis) ⁽¹⁴⁹⁾. Pranešimo 2021-5 5 skirsnyje (I priedas) paaiškinama, kad šios sąlygos privalomai taikomos dėl bet kurios AIAĮ nuostatos, kuria apsaugomos asmenų privatumo teisės, susijusios su asmenine informacija, pažeidimo ⁽¹⁵⁰⁾. Priemonės, kurių AIAK turi teisę imtis, apima nurodymą sustabdyti elgesį, dėl kurio buvo padarytas pažeidimas, laikinai sustabdyti duomenų tvarkymą ar kitas būtinas priemones. Jei taisomieji veiksmai nevykdomi, gali būti skirta sankcija, skiriant ne didesnę kaip 50 mln. vonų baudą (AIAĮ 75 straipsnio 2 dalies 13 punktą).
- (121) Tam tikrų valdžios institucijų (pvz., Nacionalinės Asamblėjos, centrinių administracinių agentūrų, vietos valdžios institucijų ir teismų) atžvilgiu AIAĮ 64 straipsnio 4 dalyje nustatyta, kad AIAK gali „rekomenduoti“ bet kurį iš (120) konstatuojamojoje dalyje nurodytų taisomųjų veiksmų ir kad šios institucijos privalo laikytis tokios rekomendacijos, išskyrus atvejus, kai egzistuoja ypatingos aplinkybės. Pagal pranešimo 2021-5 5 skirsnį tai susiję su ypatingomis faktinėmis ar teisinėmis aplinkybėmis, apie kurias AIAK teikdama savo rekomendaciją nežinojo. Suinteresuotoji valdžios institucija gali remtis tokiomis ypatingomis aplinkybėmis tik tuo atveju, jei ji aiškiai įrodo, kad nebuvo padarytas joks pažeidimas, o AIAK nustato, kad iš tikrųjų taip yra. Priešingu atveju valdžios institucija turi laikytis AIAK rekomendacijos ir „imtis taisomųjų veiksmų, įskaitant nedelsiant sustabdyti veiką ir atlyginti žalą tokiu išskirtiniu atveju, kai vis dėlto buvo vykdoma neteisėta veika“.
- (122) AIAK taip pat gali prašyti kitų administracinių agentūrų, turinčių konkrečią kompetenciją pagal sektorių teisės aktus (pvz., sveikatos, švietimo), atskirai arba kartu su AIAK atlikti tyrimą dėl (įtariamų) duomenų valdytojų, veikiančių šiuose jų jurisdikcijai priklausančiuose sektoriuose, privatumo pažeidimų ir nustatyti taisomuosius veiksmus (AIAĮ 63 straipsnio 4–5 dalys). Tokiu atveju AIAK nustato tyrimo pagrindus, objektą ir apimtį ⁽¹⁵¹⁾. Savo ruožtu atitinkama administracinė agentūra turi pateikti AIAK patikrinimo planą ir pranešti AIAK apie patikrinimo rezultatus. AIAK gali rekomenduoti konkretų taisomąjį veiksma, kurį turi įgyvendinti atitinkama agentūra. Bet kuriuo atveju, toks prašymas neapriboja AIAK kompetencijos atlikti savo tyrimą ar taikyti sankcijas.

⁽¹⁴⁸⁾ Be to, AIAK gali pateikti į duomenų valdytojo patalpas, kad patikrintų verslo operacijų būklę, įrašus, dokumentus ir t. t. (AIAĮ 63 straipsnio 2 dalis). Taip pat žr. KII 45-3 straipsnį ir KII vykdyto užtikrinimo dekreto 36-4 straipsnį dėl AIAK įgaliojimų pagal tą įstatymą.

⁽¹⁴⁹⁾ Taip pat žr. KII 45-4 straipsnį dėl AIAK įgaliojimų pagal KII.

⁽¹⁵⁰⁾ Pranešimo 5 skirsnyje nustatyta, kad „pagrįstas pagrindas manyti, kad buvo padarytas pažeidimas, susijęs su asmenine informacija, ir galima sunkiai atitaisoma žala, jei nesiimama veiksmų, kaip tai suprantama pagal AIAĮ 64 straipsnio 1 ir 2 dalis, reiškia bet kurio iš įstatyme numatytų principų, teisių ir pareigų, skirtų asmenų teisėms į asmeninę informaciją apsaugoti, pažeidimą“. Tas pats taikoma AIAK įgaliojimams pagal KII 45-4 straipsnį.

⁽¹⁵¹⁾ AIAĮ vykdyto užtikrinimo dekreto 60 straipsnis.

- (123) AIAK gali skirti ne tik taisomuosius veiksmus, bet ir 10–50 mln. vonų administracines baudas už įvairių AIAI reikalavimų pažeidimus (AIAI 75 straipsnis) ⁽¹⁵²⁾. Tai, be kita ko, yra duomenų tvarkymo teisėtumo reikalavimų nesilaikymas, būtinų saugumo priemonių nesiėmimas, duomenų subjektų neinformavimas duomenų saugumo pažeidimo atveju, duomenų tvarkymo subrangos reikalavimų nesilaikymas, privatumo politikos nenustatymas ir neatskleidimas, privatumo apsaugos pareigūno nepaskyrimas arba duomenų subjekto prašymo, pateikto asmens teisių pagrindu, nepatenkinimas, taip pat tam tikri procedūriniai pažeidimai (nebendradarbiavimas tyrimo metu). Jei tas pats duomenų valdytojas pažeidžia kelias AIAI nuostatas, už kiekvieną pažeidimą gali būti skiriama bauda, o nustatant baudos dydį atsižvelgiama į nukentėjusių asmenų skaičių.
- (124) Be to, jei yra pagrįsto pagrindo įtarti AIAI ar bet kokių kitų su duomenų apsauga susijusių įstatymų pažeidimą, AIAK gali pateikti skundą dėl nusikalstamos veikos kompetentingai tyrimo agentūrai (pvz., prokurorui, žr. AIAI 65 straipsnio 1 dalį). Be to, AIAK gali patarti duomenų valdytojui taikyti drausmines priemones atsakingam asmeniui (įskaitant atsakingą vadovą, žr. AIAI 65 straipsnio 2 dalį). Duomenų valdytojas, gavęs tokį patarimą, privalo jo laikytis ⁽¹⁵³⁾ ir apie rezultatą raštu pranešti AIAK (AIAI 65 straipsnis kartu su AIAI vykdymo užtikrinimo dekretu 58 straipsniu).
- (125) Kai teikiami patarimai pagal AIAI 61 straipsnį, taikomi taisomieji veiksmai pagal 64 straipsnį, teikiami kaltinimai arba patarimai dėl drausminių priemonių taikymo pagal 65 straipsnį ir skiriamos administracinės baudos pagal 75 straipsnį, AIAK gali viešai nurodyti faktus, t. y. pažeidimą, įstatymą pažeidusį subjektą ir taikytiną (-us) veiksmą (-us), skelbdama juos savo interneto svetainėje arba bendro pobūdžio nacionaliniame dienraštyje (AIAI 66 straipsnis kartu su AIAI vykdymo užtikrinimo dekretu 61 straipsnio 1 dalimi) ⁽¹⁵⁴⁾.
- (126) Galiausiai AIAI (taip pat kitų „su duomenų apsauga susijusių įstatymų“) duomenų apsaugos reikalavimų laikymasis sustiprinamas baudžiamųjų sankcijų tvarkos taikymu. Šiuo atžvilgiu į AIAI 70–73 straipsnius įtrauktos nuostatos dėl sankcijų, kuriose numatyta galimybė skirti baudą (nuo 20 iki 100 mln. vonų) arba laisvės atėmimą (didžiausia bausmė – nuo 2 iki 10 metų). Susiję pažeidimai, be kita ko, apima asmens duomenų naudojimą arba tokių duomenų teikimą trečiajai šaliai neturint būtino sutikimo, neskelbtinos informacijos tvarkymą pažeidžiant AIAI 23 straipsnio 1 dalyje nustatytą draudimą, taikomų saugos reikalavimų nesilaikymą, dėl kurio asmens duomenys prarandami, pavagiami, atskleidžiami, suklastojami, pakeičiami arba sugadinami, būtinų priemonių asmens duomenims ištaisyti, ištrinti arba sustabdyti jų tvarkymą ar neteisėtą asmens duomenų perdavimą į trečiąją valstybę nesiėmimą ⁽¹⁵⁵⁾. Pagal AIAI 74 straipsnį kiekvienu iš šių atvejų atsako duomenų valdytojo darbuotojas, įgaliotas asmuo arba atstovas, taip pat pats duomenų valdytojas ⁽¹⁵⁶⁾.
- (127) Be AIAI numatytų baudžiamųjų sankcijų, piktnaudžiavimas asmens duomenimis taip pat gali būti laikomas nusikalstama veika pagal Baudžiamąjį įstatymą. Tai atvejai, kai pažeidžiamas laišku, dokumentų ar elektroninių įrašų slaptumas (316 straipsnis), atskleidžiama informacija, kuriai taikomas profesinės paslapties principas (317 straipsnis), sukčiaujama naudojant kompiuterius (347-2 straipsnis), taip pat kai pasisavinamas turtas ir pažeidžiamas pasitikėjimas (355 straipsnis).
- (128) Todėl Korėjos sistemoje derinamos įvairių rūšių sankcijos – nuo taisomųjų veiksmų ir administracinių baudų skyrimo iki baudžiamųjų sankcijų taikymo, – kurių atgrasomasis poveikis duomenų valdytojams ir duomenis tvarkantiems asmenims gali būti ypač didelis. AIAK pradėjo naudotis savo įgaliojimais iš karto po jos įsteigimo 2020 m. Iš 2021 m. AIAK metinės ataskaitos matyti, kad AIAK jau paskelbė daug rekomendacijų, administracinių

⁽¹⁵²⁾ Be to, kai buvo suteiktas sertifikatas, kuriuo patvirtinama, kad duomenų valdytojo naudojamos asmeninės informacijos tvarkymo ir apsaugos sistemos atitinka AIAI reikalavimus, bet kai AIAI vykdymo užtikrinimo dekretu 34-2 straipsnio 1 dalyje nustatyti sertifikavimo kriterijai iš tiesų nebuvo patenkinti arba jei buvo šiuose kriterijuose pažeisti kokie nors „su [asmeninės] informacijos apsauga susiję įstatymai“, AIAK gali atšaukti sertifikatą (AIAI 32-2 straipsnio 3 ir 5 dalys). AIAK apie tokį atšaukimą praneša duomenų valdytojui ir viešai apie jį paskelbia arba pateikia apie jį informaciją savo interneto svetainėje arba Oficialiajame leidinyje (AIAI vykdymo užtikrinimo dekretu 34-4 straipsnis). Už KIĮ pažeidimus taip pat numatytos administracinės baudos (KIĮ 52 straipsnis) ir baudžiamosios sankcijos (KIĮ 50 straipsnis).

⁽¹⁵³⁾ Pagal AIAI vykdymo užtikrinimo dekretu 58 straipsnio 2 dalį, jei dėl ypatingų aplinkybių patarimo vykdymas tampa „neįmanomas“, duomenų valdytojas turi pateikti AIAK pagrįstą paaiškinimą.

⁽¹⁵⁴⁾ Spręsdama, ar viešai atskleisti tokią informaciją, AIAK atsižvelgia į pažeidimo esmę ir sunkumą, jo trukmę ir dažnumą, taip pat į jo pasekmes (žalos mastą). Atitinkamam subjektui apie tai iš anksto pranešama ir suteikiama galimybė apsiginti. Žr. AIAI vykdymo užtikrinimo dekretu 61 straipsnio 2 ir 3 dalis.

⁽¹⁵⁵⁾ Žr. AIAI 71 straipsnio 2 dalį kartu su 18 straipsnio 1 dalimi (sąlygų, nustatytų AIAI 17 straipsnio 3 dalyje, nesilaikymas, nurodytas 18 straipsnio 1 dalyje). Taip pat žr. AIAI 75 straipsnio 2 dalies 1 punktą kartu su 17 straipsnio 2 dalimi (būtinų informacijos atitinkamam asmeniui nesuteikimas pagal AIAI 17 straipsnio 2 dalį, nurodytas 17 straipsnio 3 dalyje).

⁽¹⁵⁶⁾ Be to, AIAI 74-2 straipsnyje numatytas leidimas konfiskuoti bet kokius pinigus, prekes ar kitokį pelną, gautus dėl pažeidimo, arba, jei konfiskavimas neįmanomas, „susigrąžinti“ neteisėtai gautą naudą.

baudų ir taisomųjų įsakymų tiek viešajam sektoriui (apie 34 valdžios institucijoms), tiek privatiems veiklos vykdytojams (apie 140 bendrovių) ⁽¹⁵⁷⁾. Pavyzdžiui, pažymėtina, kad 2020 m. gruodžio mėn. AIAK vienai bendrovei skyrė 6,7 mlrd. vonų baudą už įvairių AIAI nuostatų (be kita ko, susijusių su saugumo reikalavimais, reikalavimais dėl sutikimo teikiant informaciją trečiajai šaliai ir skaidrumo) pažeidimą ⁽¹⁵⁸⁾, o 2021 m. balandžio mėn. vienai dirbtinio intelekto technologijų bendrovei skyrė 103,3 mln. vonų baudą (be kita ko, už duomenų tvarkymo teisėtumo, visų pirma susijusio su sutikimo gavimu, ir informacijos, kuriai suteikti pseudonimai, tvarkymo taisyklių pažeidimą) ⁽¹⁵⁹⁾. 2021 m. rugpjūčio mėn. AIAK užbaigė dar vieną trijų bendrovių veiklos tyrimą, po kurio buvo nustatyti taisomieji veiksmai ir skirta iki 6,47 mlrd. EUR bauda (be kita ko, dėl asmenų neinformavimo apie asmens duomenų atskleidimą trečiosioms šalims, įskaitant perdavimą trečiosioms šalims) ⁽¹⁶⁰⁾. Be to, dar prieš įgyvendinant naują reformą Pietų Korėjoje pasiekta gerų rezultatų vykdymo užtikrinimo srityje: atsakingos institucijos taikė visus vykdymo užtikrinimo veiksmus, įskaitant administracines baudas, taisomuosius veiksmus ir „įvardijimą ir dalijimąsi“ įvairių duomenų valdytojų atžvilgiu, įskaitant ryšių paslaugų teikėjus (Korėjos ryšių komisija), taip pat komercinės veiklos vykdytojus, finansų įstaigas, valdžios institucijas, universitetus ir ligonines (Vidaus reikalų ir saugumo ministerija) ⁽¹⁶¹⁾. Tuo remdamasi Komisija daro išvadą, kad Korėjos sistema užtikrinamas veiksmingas duomenų apsaugos taisyklių praktinis vykdymas, todėl užtikrinamas toks apsaugos lygis, kuris iš esmės yra lygiavertis nustatytam Reglamente (ES) 2016/679.

2.5. Teisių gynimas

- (129) Siekiant užtikrinti tinkamą apsaugą ir, visų pirma, asmens teisių įgyvendinimą, duomenų subjektui turėtų būti suteikta veiksmingų administracinių ir teisminių teisių gynimo priemonių, įskaitant kompensaciją už patirtą žalą.
- (130) Pagal Korėjos sistemą asmenys gali naudotis įvairiais mechanizmais, siekdami veiksmingai įgyvendinti savo teises ir naudotis (teisminėmis) teisių gynimo priemonėmis.
- (131) Pirmiausia asmenys, manantys, kad jų duomenų apsaugos teisės ar interesai buvo pažeisti, gali kreiptis į atitinkamą duomenų valdytoją. Pagal AIAI 30 straipsnio 1 dalies 5 punktą duomenų valdytojo privatumo politika apima, be kita ko, informaciją apie duomenų subjektų teises ir apie tai, kaip jomis naudotis. Be to, joje pateikiama kontaktinė informacija, pavyzdžiui, privatumo apsaugos pareigūno vardas ir pavardė arba už duomenų apsaugą atsakingo departamento pavadinimas ir jų telefono numeriai, kad būtų galima pateikti skundus. Duomenų valdytojo organizacijoje privatumo apsaugos pareigūnas atsako už skundų nagrinėjimą, taisomųjų veiksmų nustatymą privatumo pažeidimo atveju ir taisomųjų kompensacijų taikymą (AIAI 31 straipsnio 2 dalies 3 punktas ir 4 dalis). Pastaroji funkcija svarbi, pavyzdžiui, duomenų saugumo pažeidimo atveju, nes duomenų valdytojas turi informuoti duomenų subjektą apie kontaktinį (-ius) punktą (-us), į kuriuos jis gali kreiptis, be kita ko, norėdamas pranešti apie bet kokią patirtą žalą (AIAI 34 straipsnio 1 dalies 5 punktas).
- (132) Be to, AIAI asmenims siūloma keletas teisių gynimo būdų jiems nukentėjus dėl duomenų valdytojų veiklos. Pirmia, bet kuris asmuo, manantis, kad duomenų valdytojas pažeidė jo duomenų apsaugos teises ar interesus, apie tokį pažeidimą gali tiesiogiai pranešti AIAK ir (arba) vienai iš specializuotų institucijų, AIAK paskirtų priimti ir nagrinėti skundus, įskaitant Korėjos interneto ir saugumo agentūrai, kuri tuo tikslu yra įsteigusi asmeninės informacijos apsaugai skirtą skambučių centrą (vadinamąjį privatumo apsaugos skambučių centrą) (AIAI 62 straipsnio 1 ir 2 dalys kartu su AIAI vykdymo užtikrinimo dekretu 59 straipsniu). Privatumo apsaugos skambučių

⁽¹⁵⁷⁾ Žr. 2021 m. AIAK metinę ataskaitą, p. 50–55 (pateikiama tik korėjiečių kalba) <https://www.pipc.go.kr/np/cop/bbs/selectBoardArticle.do?bbsId=BS074&mCode=C020010000&ntId=7511#LINK>.

⁽¹⁵⁸⁾ Žr. adresu (pateikiama tik korėjiečių kalba) <https://www.pipc.go.kr/np/cop/bbs/selectBoardArticle.do?bbsId=BS074&mCode=C020010000&ntId=6954#LINK>.

⁽¹⁵⁹⁾ Žr. adresu (pateikiama tik korėjiečių kalba) <https://www.pipc.go.kr/np/cop/bbs/selectBoardArticle.do?bbsId=BS074&mCode=C020010000&ntId=7298&fbclid=IwAR3SKcMQi6G5pR9k4I7j6GNXtc8aBVDOWcURvzvzQtYI7AS40UKYXoXo8>.

⁽¹⁶⁰⁾ Žr. adresu (pateikiama tik korėjiečių kalba) <https://www.pipc.go.kr/np/cop/bbs/selectBoardArticle.do?bbsId=BS074&mCode=C020010000&ntId=7497#LINK>.

⁽¹⁶¹⁾ Žr., pvz., 2020 m. metinę ataskaitą (pateikiama tik korėjiečių kalba) <https://www.pipc.go.kr/np/cop/bbs/selectBoardList.do?bbsId=BS079&mCode=D070020000> ir pavyzdžius anglų kalba https://www.privacy.go.kr/eng/enforcement_02.do.

centras tiria ir nustato pažeidimus, teikia konsultacijas asmens duomenų tvarkymo klausimais (AIAĮ 62 straipsnio 3 dalis) ir gali pranešti apie pažeidimus AIAK (tačiau pats negali imtis vykdymo užtikrinimo priemonių). Privatumo apsaugos skambučių centras gauna labai daug skundų ir prašymų (pvz., 2020 m. – 177 457, 2019 m. – 159 255, o 2018 m. – 164 497) ⁽¹⁶²⁾. Remiantis iš AIAK gauta informacija, nuo 2020 m. rugpjūčio mėn. iki 2021 m. rugpjūčio mėn. pati AIAK gavo apie 1 000 skundų. Atsakydama į skundą, AIAK gali kompetentingai tyrimo agentūrai (įskaitant prokurorą) pateikti tobulinimo patarimą, nustatyti taisomuosius veiksmus, pateikti „kaltinimą“ arba patarimą dėl drausminių priemonių (žr. AIAĮ 61, 64 ir 65 straipsnius). AIAK sprendimai (kaip antai atsisakymas nagrinėti skundą arba apskritai skundo atmetimas) gali būti ginčijami pagal Administracinių ginčų įstatymą ⁽¹⁶³⁾.

- (133) Antra, pagal AIAĮ 40–50 straipsnius kartu su AIAĮ vykdymo užtikrinimo dekretu 48-14-57 straipsniais duomenų subjektai gali kreiptis į vadinamąjį tarpininkavimo ginčiuose komitetą, kurį sudaro AIAK pirmininko iš AIAK vyresniosios vykdomosios tarnybos narių paskirti atstovai ir asmenys, paskirti iš tam tikrų reikalavimus atitinkančių grupių remiantis jų patirtimi duomenų apsaugos srityje (žr. AIAĮ 40 straipsnio 2, 3 ir 7 dalis, AIAĮ vykdymo užtikrinimo dekretu 48-14 straipsnį) ⁽¹⁶⁴⁾. Galimybė pasinaudoti tarpininkavimu Tarpininkavimo ginčiuose komitete suteikia alternatyvų teisių gynimo būdą, tačiau neriboja asmens teisės vietoje to kreiptis į AIAK arba teismus. Siekdamas išnagrinėti atvejį, komitetas gali prašyti ginčo šalių pateikti reikiamą medžiagą ir (arba) pakviesti atitinkamus liudytojus liudyti komitete (AIAĮ 45 straipsnis). Išsprendęs klausimą komitetas parengia tarpininkavimo sprendimo projektą ⁽¹⁶⁵⁾, kuriam turi pritarti jo narių dauguma. Tarpininkavimo sprendimo projekte gali būti numatyta sustabdyti veiklą, dėl kurios buvo atliktas pažeidimas, taikyti būtinas teisių gynimo priemones (įskaitant restituciją ar kompensaciją) ir bet kokias priemones, būtinas siekiant užkirsti kelią to paties ar panašaus pažeidimo ar pažeidimų pasikartojimui (AIAĮ 47 straipsnio 1 dalis). Jei abi šalys pritaria tarpininkavimo sprendimui, jo poveikis toks pats kaip ir susitarimo teisme (AIAĮ 47 straipsnio 5 dalis). Vykstant tarpininkavimui nė vienai iš šalių neužkertamas kelias kreiptis į teismą. Tokiu atveju tarpininkavimas sustabdomas (žr. AIAĮ 48 straipsnio 2 dalį) ⁽¹⁶⁶⁾. AIAK paskelbti metiniai duomenys rodo, kad asmenys reguliariai naudojami procedūra Tarpininkavimo ginčiuose komitete, o tai dažnai lemia sėkmingą rezultatą. Pavyzdžiui, 2020 m. komitetas išnagrinėjo 126 bylas, iš kurių 89 buvo išspręstos komitete (77 atvejai, kai šalys jau pasiekė susitarimą iki tarpininkavimo proceso pabaigos, ir 12 atvejų, kai šalys pritarė tarpininkavimo pasiūlymui), taigi tarpininkavimo rodiklis siekė 70,6 proc. ⁽¹⁶⁷⁾. 2019 m. Komitetas nagrinėjo 139 bylas, iš kurių 92 buvo išspręstos, taigi tarpininkavimo rodiklis siekė 62,2 proc.

- (134) Be to, tais atvejais, kai dėl to paties įvykio (įvykio tipo) žalą patiria ne mažiau kaip 50 asmenų arba jų duomenų apsaugos teisės pažeidžiamos tokiu pačiu ar panašiu būdu ⁽¹⁶⁸⁾, duomenų subjektas arba duomenų apsaugos organizacija tokios nukentėjusiųjų grupės vardu gali kreiptis dėl tarpininkavimo kolektyvinio ginčo sprendime. Kiti duomenų subjektai gali kreiptis dėl prisijungimo prie tokio tarpininkavimo, apie kurį viešai skelbs tarpininkavimo ginčiuose komitetas (AIAĮ 49 straipsnio 1–3 dalys kartu su AIAĮ vykdymo užtikrinimo dekretu 52–54 straipsniais) ⁽¹⁶⁹⁾. Tarpininkavimo ginčiuose komitetas kaip atstovaujancią šalį gali pasirinkti mažiausiai vieną

⁽¹⁶²⁾ Žr. 2021 m. AIAK metinę ataskaitą, p. 174. 2020 m. tokie skundai buvo susiję, pavyzdžiui, su duomenų rinkimu be sutikimo, skaidrumo prievolių nesilaikymu, duomenų tvarkytojų padarytais AIAĮ pažeidimais, nepakankamomis saugumo priemonėmis, neatsakymu į duomenų subjektų prašymus ir bendro pobūdžio užklausomis.

⁽¹⁶³⁾ Visų pirma asmenys gali apskusti tai, kaip administracinė agentūra naudoja viešuosius įgaliojimus, arba jos atsisakymą juos vykdyti (Administracinių ginčų įstatymo 2 straipsnio 1 dalies 1 punktą ir 3 straipsnio 1 dalis). Išsamesnė informacija apie procedūrinius aspektus, įskaitant skundo priimtinumą reikalavimus, pateikta (181) konstatuojamojoje dalyje.

⁽¹⁶⁴⁾ Visų narių kadencija terminuota, o atleisti jie gali būti tik dėl pateisinamų priežasčių (žr. AIAĮ 40 straipsnio 5 dalį ir 41 straipsnį). Be to, AIAĮ 42 straipsnyje nustatytos nuo interesų konfliktų apsaugoti skirtos priemonės.

⁽¹⁶⁵⁾ Žr. AIAĮ 44 straipsnį. Be to, jis gali pasiūlyti susitarimo projektą ir rekomenduoti susitarimą be tarpininkavimo (žr. AIAĮ 46 straipsnį).

⁽¹⁶⁶⁾ Be to, komitetas gali atsakyti tarpininkauti, jei mano, kad tarpininkauti ginče yra netinkama dėl jo pobūdžio arba dėl to, kad prašymas taikyti tarpininkavimą buvo pateiktas nesąžiningai (AIAĮ 48 straipsnis).

⁽¹⁶⁷⁾ Žr. 2021 m. AIAK metinę ataskaitą, p. 179–180. Šios bylos, *inter alia*, buvo susijusios su reikalavimu gauti sutikimą duomenų rinkimui, tikslo apribojimo principo ir duomenų subjektų teisių pažeidimais.

⁽¹⁶⁸⁾ Žr. AIAĮ 49 straipsnio 1 dalį, pagal kurią duomenų subjektų patirta žala turi būti „tokia pati arba panaši“ arba jų teisės turi būti pažeistos „tokiu pačiu arba panašiu būdu“, ir AIAĮ vykdymo užtikrinimo dekretu 52 straipsnio 2 dalį, pagal kurią reikalaujama, kad „svarbiausios su įvykiu susijusios problemos būtų faktiškai arba teisiškai bendros“.

⁽¹⁶⁹⁾ Be to, duomenų valdytojo sutikimas su kolektyvinio ginčo sprendimu gali būti naudingas ir tiems asmenims, kurie nėra ginčo šalis, nes tarpininkavimo ginčiuose komitetas gali patarti duomenų valdytojui parengti ir pateikti žalos atlyginimo planą, į kurį būtų įtraukti (ir) šie asmenys (AIAĮ 49 straipsnio 5 dalis).

asmenį, kuris tinkamiausiai atstovauja bendram interesui (AIAĮ 49 straipsnio 4 dalis). Jeigu duomenų valdytojas nesutinka, kad kolektyviniuose ginčiuose būtų tarpininkaujama, arba nesutinka su tarpininkavimo sprendimu, tam tikros organizacijos⁽¹⁷⁰⁾ gali pateikti kolektyvinį ieškinį dėl pažeidimo (AIAĮ 51–57 straipsniai).

(135) Trečia, privatumo pažeidimo, dėl kurio asmeniui padaroma „žala“, atveju duomenų subjektas turi teisę į tinkamą teisių gynimą taikant „savalaikę ir sąžiningą procedūrą“ (AIAĮ 4 straipsnio 5 dalis kartu su 39 straipsniu)⁽¹⁷¹⁾. Duomenų valdytojas gali būti išteisintas, jei įrodo, kad jo kaltės („blogų ketinimų“ arba nerūpestingumo) nėra. Tais atvejais, kai duomenų subjektas patiria žalą dėl jo asmens duomenų praradimo, vagystės, atskleidimo, klastojimo, pakeitimo ar sugadinimo, teismas, atsižvelgdamas į atitinkamus veiksnius, gali nustatyti kompensaciją, kuri būtų iki trijų kartų didesnė už faktinę žalą (AIAĮ 39 straipsnio 3 ir 4 dalys). Kitu atveju duomenų subjektas gali reikalauti „pagrįstos“ kompensacijos sumos, neviršijančios 3 mln. vonų (AIAĮ 39-2 straipsnio 1 ir 2 dalys). Be to, pagal Civilinį įstatymą kompensacijos gali būti reikalaujama iš bet kurio asmens, „dėl kurio neteisėtų veiksmų, tyčinių arba atliktų dėl neatsargumo, kitas asmuo patiria žalą arba fizinį sužalojimą“⁽¹⁷²⁾, arba iš asmens, „sužeidusio kitą asmenį, padariusio žalą jo laisvei ar reputacijai arba sukėlusio kito asmens psichinę kančią“⁽¹⁷³⁾. Tokią deliktinę atsakomybę dėl duomenų apsaugos taisyklių pažeidimo patvirtino Aukščiausiasis Teismas⁽¹⁷⁴⁾. Jeigu žala padaryta dėl neteisėtų valdžios institucijos veiksmų, reikalavimas atlyginti žalą taip pat gali būti pateiktas pagal Valstybės kompensacijų įstatymą⁽¹⁷⁵⁾. Reikalavimas atlyginti žalą pagal Valstybės kompensacijų įstatymą gali būti pateiktas specializuotai „kompensacijos tarybai“ arba tiesiogiai Korėjos teismams⁽¹⁷⁶⁾. Valstybės atsakomybė taip pat apima neturtinę žalą (pvz., psichinę kančią)⁽¹⁷⁷⁾. Jei nukentėjusysis yra užsienio valstybės pilietis, Valstybės kompensacijų įstatymas jam taikomas tada, kai jo kilmės šalis taip pat užtikrina valstybės kompensaciją Korėjos piliečiams⁽¹⁷⁸⁾.

(136) Ketvirta, Aukščiausiasis Teismas pripažino, kad asmenys turi teisę reikalauti uždrausti vykdyti veiklą, dėl kurios pažeidžiamos jų teisės pagal Konstituciją, įskaitant teisę į asmens duomenų apsaugą⁽¹⁷⁹⁾. Tokiomis aplinkybėmis teismas gali, pavyzdžiui, nurodyti duomenų valdytojams sustabdyti bet kokią neteisėtą veiklą arba jos nebevykdyti. Be to, duomenų apsaugos teisių, įskaitant AIAĮ saugomas teises, įgyvendinimas gali būti užtikrinamas civiliniais ieškiniais. Aukščiausiasis Teismas pripažino šį horizontalų konstitucinės privatumo apsaugos taikymą privačių asmenų santykiams⁽¹⁸⁰⁾.

⁽¹⁷⁰⁾ Būtent vartotojų grupės arba ne pelno nevyriausybinių organizacijos, kurios turi atitinkamą skaičių narių ir kurių nurodytas tikslas yra duomenų apsauga (nors pastarųjų organizacijų atveju taikomas papildomas reikalavimas, kad bent 100 duomenų subjektų, patyrusių tokį patį (to pačio tipo) pažeidimą, būtų pateikę prašymą pateikti kolektyvinį ieškinį). Žr. AIAĮ 51 straipsnį.

⁽¹⁷¹⁾ KIĮ 43–43-3 straipsniuose taip pat nustatyta atsakomybė kompensuoti žalą, padarytą dėl to įstatymo pažeidimo.

⁽¹⁷²⁾ Civilinio įstatymo 750 straipsnis.

⁽¹⁷³⁾ Civilinio įstatymo 751 straipsnio 1 dalis.

⁽¹⁷⁴⁾ Žr., pavyzdžiui, 2018 m. gegužės 30 d. Aukščiausiojo Teismo sprendimą 2015Da251539, 251546, 251553, 251560, 251577. Be to, Aukščiausiasis Teismas patvirtino, kad už duomenų saugumo pažeidimą pagal Civilinį įstatymą gali būti priteistas žalos atlyginimas, žr. 2012 m. gruodžio 26 d. Aukščiausiojo Teismo sprendimą 2011Da59834, 59858, 59841 (santrauka anglų kalba pateikiama adresu http://library.scourt.go.kr/SCLIB_data/decision/9-69%202012.12.26.2011Da59834.htm). Šiuo atveju Aukščiausiasis Teismas paaiškino, kad siekiant įvertinti, ar asmuo patyrė emocinį sukrėtimą, laikomą atlygintina žala, reikėtų atsižvelgti į kelis veiksnius, kaip antai nutekintos informacijos rūšį ir ypatybes, asmens tapatybės nustatymo galimybę dėl pažeidimo, galimybę trečiosioms šalims susipažinti su duomenimis, asmeninės informacijos platinimo mastą, tai, ar dėl to atsirado kokių nors papildomų asmens teisių pažeidimų, kaip asmeninė informacija buvo tvarkoma ir saugoma ir t. t.

⁽¹⁷⁵⁾ Remdamiesi Valstybės kompensacijų įstatymu, asmenys gali prašyti kompensacijos už žalą, kurią valstybės pareigūnai padarė pažeidę įstatymą, kai vykdė savo oficialias pareigas (įstatymo 2 straipsnio 1 dalis).

⁽¹⁷⁶⁾ Valstybės kompensacijų įstatymo 9 ir 12 straipsniai. Įstatymu įsteigiamos apygardų tarybos (kurioms pirmininkauja atitinkamos prokuratūros prokuroro pavaduotojas), centrinė taryba (kurai pirmininkauja Teisingumo ministro pavaduotojas) ir specialioji taryba (atsakinga už reikalavimus atlyginti žalą, padarytą karinio personalo arba civilių kariuomenės darbuotojų, kuriai pirmininkauja Nacionalinės gynybos ministro pavaduotojas). Prašymus atlyginti žalą iš esmės nagrinėja apygardų tarybos, kurios esant tam tikroms aplinkybėmis bylas turi perduoti centrinei arba specialiajai tarybai, pvz., jei kompensacija viršija tam tikrą sumą arba jei asmuo kreipiasi dėl pakartotinio svarstymo. Visas tarybas sudaro Teisingumo ministro paskirti nariai (pvz., iš Teisingumo ministerijos valstybės pareigūnų, teismų pareigūnų, advokatų ir asmenų, turinčių patirties valstybės kompensacijų srityje) ir jems taikomos specialios taisyklės dėl interesų konflikto (žr. Valstybės kompensacijų įstatymo 7 straipsnį).

⁽¹⁷⁷⁾ Žr. Valstybės kompensacijų įstatymo 8 straipsnį (kuriame nurodomas Civilinis įstatymas), taip pat Civilinio įstatymo 751 straipsnį.

⁽¹⁷⁸⁾ Valstybės kompensacijų įstatymo 7 straipsnis.

⁽¹⁷⁹⁾ Aukščiausiojo Teismo 1996 m. balandžio 12 d. Sprendimas 93Da40614 ir 2011 m. rugsėjo 2 d. Sprendimas 2008Da42430 (santrauka anglų kalba pateikiama adresu <https://www.scourt.go.kr/eng/supreme/decisions/NewDecisionsView.work?seq=696&pageIndex=1&mode=6&searchWord=>).

⁽¹⁸⁰⁾ Žr., pavyzdžiui, 2011 m. rugsėjo 2 d. Aukščiausiojo Teismo sprendimą 2008Da42430 (santrauka anglų kalba pateikiama adresu <https://www.scourt.go.kr/eng/supreme/decisions/NewDecisionsView.work?seq=696&pageIndex=1&mode=6&searchWord=>).

- (137) Galiausiai asmenys pagal Baudžiamojo proceso įstatymą (223 straipsnis) skundą dėl nusikalstamos veiklos gali pateikti prokurorui arba teismo policijos pareigūnui ⁽¹⁸¹⁾.
- (138) Todėl Korėjos sistemoje siūlomi įvairūs teisių gynimo būdai, nuo lengvai prieinamų ir nebrangių galimybių (pvz., kreiptis į privatumo apsaugos skambučių centrą arba naudoti (kolektyvinį) tarpininkavimą) iki administracinių (AIAK) ir teisminių priemonių, įskaitant galimybę gauti kompensaciją už žalą.

3. KORĖJOS RESPUBLIKOS VALDŽIOS INSTITUCIJŲ SUSIPAŽINIMAS SU ASMENS DUOMENIMIS, PERDUOTAIŠ IŠ EUROPOS SAJUNGOS, IR JŲ NAUDOJIMAS

- (139) Komisija taip pat įvertino apribojimus ir apsaugos priemones, įskaitant pagal Korėjos teisės aktus galimus priežiūros ir asmens teisių gynimo priemonių mechanizmus Korėjos valdžios institucijoms renkanti ir vėliau naudojanti asmens duomenis, perduotus duomenų valdytojams Korėjoje viešojo intereso pagrindu, visų pirma, baudžiamosios teisėsaugos ir nacionalinio saugumo tikslais (vyriausybės susipažinimas su informacija). Atsižvelgiant į tai, Korėjos vyriausybė Komisijai pateikė aukščiausiu ministerijų ir įstaigų lygmeniu pasirašytus oficialius pareiškimus, garantijas ir išsipareigojimus, kurie pateikiami šio sprendimo II priede.
- (140) Vertindama, ar sąlygos, kuriomis vyriausybė gauna prieigą prie duomenų, perduotų Korėjai pagal šį sprendimą, atitinka „esminio lygiavertiškumo“ kriterijų pagal Reglamento (ES) 2016/679 45 straipsnio 1 dalį, kaip jį išaiškino Europos Sąjungos Teisingumo Teismas, atsižvelgdamas į Pagrindinių teisių chartiją, Komisija visų pirma atsižvelgė į toliau išvardytus kriterijus.
- (141) Pirma, bet koks teisės į asmens duomenų apsaugą apribojimas turi būti numatytas įstatyme, o pačiame teisiniame pagrindu, kuriuo remiantis leidžiama apriboti tokią teisę, turi būti apibrėžta apribojimo taikymo atitinkamos teisės įgyvendinimui sritis ⁽¹⁸²⁾.
- (142) Antra, siekiant įvykdyti proporcingumo reikalavimą, pagal kurį nuo asmens duomenų apsaugos nukrypti leidžiančios nuostatos ir asmens duomenų apsaugos apribojimai turi būti taikomi tik tiek, kiek tai griežtai būtina demokratinėje visuomenėje siekiant konkrečių viešojo intereso tikslų, kurie yra lygiavertiški Sąjungos pripažintiems tikslams, atitinkamos trečiosios valstybės, kurioje leidžiami apribojimai, teisės aktuose turi būti nustatytos aiškios ir tikslios taisyklės, kuriomis reglamentuojamas atitinkamų priemonių mastas ir taikymas, ir nustatomos būtinosios apsaugos priemonės, kad asmenys, kurių duomenys buvo perduoti, turėtų pakankamai garantijų ir galėtų veiksmingai apsaugoti savo asmens duomenis nuo piktnaudžiavimo rizikos ⁽¹⁸³⁾. Teisės akte visų pirma turi būti nurodyta, kokiomis aplinkybėmis ir sąlygomis galima priimti priemonę, kurią įgyvendinant numatyta tvarkyti tokius duomenis ⁽¹⁸⁴⁾, taip pat tokiai priemonei taikomi nepriklausomos priežiūros reikalavimai ⁽¹⁸⁵⁾.
- (143) Trečia, tas teisės aktas ir jame nustatyti reikalavimai turi būti teisiškai privalomi pagal nacionalinę teisę. Tai visų pirma susiję su atitinkamos trečiosios valstybės valdžios institucijomis, tačiau šie teisiniai reikalavimai šių institucijų atžvilgiu taip pat turi būti įgyvendinami teisme ⁽¹⁸⁶⁾. Duomenų subjektai visų pirma privalo turėti galimybę imtis teisinių veiksmų nepriklausomame ir nešališkame teisme, kad galėtų susipažinti su savo asmens duomenimis arba reikalauti ištaisyti arba ištrinti tokius duomenis ⁽¹⁸⁷⁾.

3.1. Bendroji teisinė sistema

- (144) Apribojimai ir apsaugos priemonės, taikomi Korėjos valdžios institucijoms renkanti asmens duomenis ir vėliau juos naudojanti, kyla iš visa apimančios konstitucinės sistemos, konkrečių įstatymų, kuriais reglamentuojama jų veikla baudžiamosios teisėsaugos ir nacionalinio saugumo srityse, taip pat taisyklių, kurios taikomos konkrečiai asmens duomenų tvarkymui.

⁽¹⁸¹⁾ Kaip paaiškinta (127) konstatuojamojoje dalyje, piktnaudžiavimas duomenimis pagal Baudžiamąjį įstatymą gali būti laikomas nusikalstama veika.

⁽¹⁸²⁾ Žr. Sprendimo *Schrems II* 174–175 punktus ir juose minimą teismo praktiką. Dėl valstybių narių valdžios institucijų prieigos prie duomenų taip pat žr. Sprendimo *Privacy International*, C-623/17, ECLI:EU:C:2020:790, 65 punktą ir Sprendimo *La Quadrature du Net* ir kt., sujungtos bylos C-511/18, C-512/18 ir C-520/18, ECLI:EU:C:2020:791, 175 punktą.

⁽¹⁸³⁾ Žr. Sprendimo *Schrems II* 176 ir 181 punktus, taip pat juose minimą teismo praktiką. Dėl valstybių narių valdžios institucijų prieigos prie duomenų taip pat žr. Sprendimo *Privacy International* 68 punktą ir Sprendimo *La Quadrature du Net* ir kt. 132 punktą.

⁽¹⁸⁴⁾ Žr. Sprendimo *Schrems II* 176 punktą. Dėl valstybių narių valdžios institucijų prieigos prie duomenų taip pat žr. Sprendimo *Privacy International* 68 punktą ir Sprendimo *La Quadrature du Net* ir kt. 132 punktą.

⁽¹⁸⁵⁾ Žr. Sprendimo *Schrems II* 179 punktą.

⁽¹⁸⁶⁾ Žr. Sprendimo *Schrems II* 181–182 punktus.

⁽¹⁸⁷⁾ Žr. Sprendimo *Schrems I* 95 punktą ir Sprendimo *Schrems II* 194 punktą. Šiuo atžvilgiu ESTT visų pirma pažymėjo, kad Pagrindinių teisių chartijos 47 straipsnio, kuriame garantuojama teisė į veiksmingą teisinę gynybą nepriklausomame ir nešališkame teisme, laikymasis yra „svarbus užtikrinant Sąjungos teisėje reikalaujamą apsaugos lygį ir kurio laikymąsi Komisija turi konstatuoti prieš priimdama sprendimą dėl tinkamumo pagal Reglamento (ES) 2016/679 45 straipsnio 1 dalį“ (Sprendimo *Schrems II* 186 punktas).

- (145) Pirma, Korėjos valdžios institucijų prieiga prie asmens duomenų reglamentuojama bendraisiais teisėtumo, būtinumo ir proporcingumo principais, nustatytais Korėjos Konstitucijoje⁽¹⁸⁸⁾. Visų pirma pagrindinės teisės ir laisvės (įskaitant teisę į privatumą ir teisę į susirašinėjimo privatumą)⁽¹⁸⁹⁾ gali būti ribojamos tik įstatymais ir tik tada, kai tai būtina nacionaliniam saugumui užtikrinti arba viešajai tvarkai palaikyti siekiant užtikrinti visuomenės gerovę. Tokie apribojimai negali turėti įtakos esminių atitinkamos teisės ar laisvės aspektų įgyvendinimui. Kalbant konkrečiai apie kratą ir poėmį, Konstitucijoje numatyta, kad jie gali būti atliekami tik įstatymų nustatyta tvarka, remiantis teisėjo išduotu orderiu ir užtikrinant tinkamą teisinį procesą⁽¹⁹⁰⁾. Galiausiai asmenys savo teisėmis ir laisvėmis gali pasinaudoti Konstituciniame Teisme, jei mano, kad valdžios institucijos, vykdydamos savo įgaliojimus, juos pažeidė⁽¹⁹¹⁾. Be to, asmenys, patyrę žalą dėl valstybės pareigūno neteisėtų veiksmų jam vykdanant tarnybines pareigas, turi teisę reikalauti teisingo žalos atlyginimo⁽¹⁹²⁾.
- (146) Antra, kaip išsamiau aprašyta 3.2.1 ir 3.3.1 skirsniuose, (145) konstatuojamojoje dalyje nurodyti bendrieji principai taip pat atspindimi specialiuose įstatymuose, kuriais reglamentuojami teisėsaugos ir nacionalinio saugumo institucijų įgaliojimai. Pavyzdžiui, baudžiamųjų bylų tyrimo atveju Baudžiamojo proceso įstatyme (BPI) numatyta, kad priverstinių priemonių galima imtis tik tuo atveju, jei tai aiškiai numatyta BPI, ir tik tiek, kiek tai būtina tyrimo tikslui pasiekti⁽¹⁹³⁾. Be to, Rysių privatumo apsaugos įstatymo (RPAĮ) 3 straipsniu draudžiama susipažinti su privačiai perduodama informacija, išskyrus atvejus, kai tai daroma remiantis įstatymu ir taikant jame nustatytus apribojimus ir apsaugos priemones. Nacionalinio saugumo srityje Nacionalinės žvalgybos tarnybos įstatymu (NŽT įstatymas) nustatyta, kad bet kokia galimybė susipažinti su ryšių ar buvimų vietos informacija turi būti suteikta pagal įstatymus, o už piktnaudžiavimą įgaliojimais ir įstatymų pažeidimą taikomos baudžiamosios sankcijos⁽¹⁹⁴⁾.
- (147) Trečia, valdžios institucijų vykdomam asmens duomenų tvarkymui, be kita ko, teisėsaugos ir nacionalinio saugumo tikslais, taikomos AIAĮ nustatytos duomenų apsaugos taisyklės⁽¹⁹⁵⁾. AIAĮ 5 straipsnio 1 dalyje nustatytas bendras reikalavimas valdžios institucijoms parengti politiką, kuria būtų užkertamas kelias „piktnaudžiavimui asmenine informacija ir neteisėtam jos naudojimui, neteisėtam sekimui ir persekiojimui ir t. t., ir didinti žmonių orumą bei asmens privatumo apsaugą.“ Be to, bet kuris duomenų valdytojas turi tvarkyti asmens duomenis taip, kad būtų kuo labiau sumažinta galimybė pažeisti duomenų subjekto privatumą (AIAĮ 3 straipsnio 6 dalis).
- (148) Visi 2 skirsnyje išsamiai aprašyti AIAĮ reikalavimai taikomi asmens duomenų tvarkymui teisėsaugos tikslais. Tai apima pagrindinius principus (pavyzdžiui, teisėtumo ir sąžiningumo, tikslo apribojimo, tikslumo, duomenų kiekio mažinimo, saugojimo apribojimo, saugumo ir skaidrumo), prievoles (pavyzdžiui, susijusias su pranešimu apie duomenų saugumo pažeidimą ir neskelbtiniais duomenimis) ir teises (gauti prieigą, reikalauti duomenis ištaisyti, ištrinti ir sustabdyti jų tvarkymą).
- (149) Nors asmens duomenų tvarkymui nacionalinio saugumo tikslais pagal AIAĮ taikoma mažiau nuostatų, pagrindiniai principai, taip pat priežiūros, vykdymo užtikrinimo ir teisių gynimo taisyklės, yra taikomi⁽¹⁹⁶⁾. Konkrečiau, AIAĮ 3 ir 4 straipsniuose nustatyti bendrieji duomenų apsaugos principai (teisėtumas ir sąžiningumas, tikslo apribojimas, tikslumas, duomenų kiekio mažinimas, saugumas ir skaidrumas) ir asmens teisės (teisė būti informuotam, teisė susipažinti su duomenimis ir teisė į duomenų ištaisymą, ištrynimą ir jų tvarkymo sustabdymą)⁽¹⁹⁷⁾. Be to, AIAĮ 4 straipsnio 5 dalyje asmenims suteikiama teisė į tinkamą žalą, sukeltą tvarkant jų asmens duomenis, atlyginimą taikant savalaikę ir sąžiningą procedūrą. Tai papildyta konkretesnėmis prievolėmis tvarkyti

⁽¹⁸⁸⁾ Žr. II priedo 1.1 skirsnį.

⁽¹⁸⁹⁾ Konstitucijos 37 straipsnio 2 dalis.

⁽¹⁹⁰⁾ Konstitucijos 16 straipsnis ir 12 straipsnio 3 dalis. Be to, Konstitucijos 12 straipsnio 3 dalyje nustatytos išimtinės aplinkybės, kurioms esant galima atlikti kratą ar poėmį neturint orderio (nors *ex post* orderis vis tiek reikalingas), t. y. *in flagrante delicto* atveju arba už nusikaltimus, už kuriuos skiriama ne trumpesnė kaip trejų metų laisvės atėmimo bausmė, jei yra pavojus, kad įrodymai bus sunaikinti arba įtariamasis pabėgs.

⁽¹⁹¹⁾ Konstitucinio Teismo įstatymo 68 straipsnio 1 dalis.

⁽¹⁹²⁾ Konstitucijos 29 straipsnio 1 dalis.

⁽¹⁹³⁾ BPI 199 straipsnio 1 dalis. Apskritai valdžios institucijos, naudodamosi savo įgaliojimais pagal BPI, privalo gerbti nusikalstama veika įtariamų asmenų ir visų kitų susijusių asmenų pagrindines teises (BPI 198 straipsnio 2 dalis).

⁽¹⁹⁴⁾ NŽT įstatymo 14 straipsnis.

⁽¹⁹⁵⁾ Žr. II priedo 1.2 skirsnį.

⁽¹⁹⁶⁾ AIAĮ 58 straipsnio 1 dalies 2 punktas. Taip pat žr. pranešimo Nr. 2021-5 6 skirsnį (I priedas). Tam tikros AIAĮ nuostatos netaikomos tik tais atvejais, kai asmens duomenys tvarkomi „nacionalinio saugumo tikslais“. Pasibaigus nacionalinio saugumo padėčiai, kuria grindžiamas duomenų tvarkymas, nebeįmanoma remtis išimtimi ir taikomi visi AIAĮ reikalavimai.

⁽¹⁹⁷⁾ Tokios teisės gali būti ribojamos tik tada, kai tai numatyta teisės aktuose, tiek ir tol, kol tai būtina svarbiam viešojo intereso tikslui apsaugoti ir ribojamas yra proporcingas jo atžvilgiu, arba kai teisės suteikimas gali kelti grėsmę trečiosios šalies gyvybei ar fizinei sveikatai arba nepagrįstai pažeisti trečiosios šalies turtinius ir kitus interesus. Žr. pranešimo Nr. 2021-5 6 skirsnį.

asmens duomenis tik tiek, kiek tai būtina numatytam tikslui pasiekti, ir minimalų laikotarpį, nustatyti būtinas priemones, kuriomis būtų užtikrinama, kad duomenys būtų saugiai valdomi ir tinkamai tvarkomi (pvz., technines, valdymo ir fizines apsaugos priemones), taip pat nustatyti priemones, kad būtų tinkamai nagrinėjami individualūs skundai ⁽¹⁹⁸⁾. Galiausiai Korėjos Konstitucijoje nustatyti bendrieji teisėtumo, būtinumo ir proporcingumo principai (žr. (145) konstatuojamąją dalį) taip pat taikomi asmens duomenų tvarkymui nacionalinio saugumo tikslais.

- (150) Šiais bendraisiais apribojimais ir apsaugos priemonėmis asmenys gali remtis nepriklausomose priežiūros institucijose (pvz., AIAK ir (arba) Nacionalinėje žmogaus teisių komisijoje, žr. (177)–(178) konstatuojamąsias dalis) ir teismuose (žr. (179)–(183) konstatuojamąsias dalis), kad apgintų savo teises.

3.2. Korėjos valdžios institucijų galimybė susipažinti su duomenimis ir jų naudojimas baudžiamosios teisės saugos tikslais

- (151) Korėjos Respublikos teisėje nustatyti įvairūs galimybės susipažinti su asmens duomenimis ir juos naudoti baudžiamosios teisės saugos tikslais apribojimai, ir numatyti priežiūros ir teisių gynimo mechanizmai, kurie atitinka šio sprendimo (141)–(143) konstatuojamosiose dalyse nurodytus reikalavimus. Sąlygos, kuriomis tokia prieiga gali būti suteikta, ir tų įgaliojimų naudojimui taikomos apsaugos priemonės išsamiai įvertinamos kituose skirsniuose.

3.2.1. Teisiniai pagrindai, apribojimai ir apsaugos priemonės

- (152) Korėjos duomenų valdytojų tvarkomi asmens duomenys, kurie būtų perduodami iš Sąjungos pagal šį sprendimą ⁽¹⁹⁹⁾, Korėjos valdžios institucijų baudžiamosios teisės saugos tikslais gali būti renkami atliekant kratą arba poėmį (pagal BPI), gaunant prieigą prie ryšių informacijos (pagal RPAI) arba gaunant abonento duomenis teikiant prašymus savanoriškai atskleisti informaciją (remiantis Telekomunikacijų įmonių įstatymu, TII) ⁽²⁰⁰⁾.

3.2.1.1. Krata ir poėmis

- (153) BPI nustatyta, kad krata ar poėmis gali būti atliekami tik tuo atveju, jei asmuo įtariamasis nusikaltimu, tai būtina tyrimui ir nustatomas ryšys tarp tyrimo ir asmens, kuris turi būti apieškotas, arba daiktų, kuriuos reikia patikrinti ar paimiti ⁽²⁰¹⁾. Be to, krata ar poėmis (kaip bet kuri priverstinė priemonė) gali būti leidžiami ir (arba) atliekami tik tiek, kiek tai būtina ⁽²⁰²⁾. Jei krata susijusi su kompiuterio disku ar kita duomenų laikmena, iš esmės bus paimiti tik būtini duomenys (nukopijavus arba atspausdinus), o ne visa laikmena ⁽²⁰³⁾. Pastarosios gali būti paimitos tik tada, kai manoma, kad iš esmės neįmanoma atspausdinti ar nukopijuoti tik reikalingų duomenų arba kad kitaip kratos tikslo pasiekti iš esmės neįmanoma ⁽²⁰⁴⁾. Todėl BPI nustatomos aiškios ir tikslios šių priemonių taikymo masto ir taikymo taisyklės, taip užtikrinant, kad asmenų teisių apribojimas kratos ar poėmio atveju neviršytų to, kas būtina konkrečiam baudžiamajam tyrimui, ir būtų proporcingas siekiamam tikslui.

⁽¹⁹⁸⁾ AIAI 58 straipsnio 4 dalis.

⁽¹⁹⁹⁾ Žr. II priedo 2.1 skirsnį. Korėjos vyriausybės oficialiame pareiškime (II priedo 2.1 skirsnis) taip pat nurodyta galimybė rinkti informaciją apie finansinius sandorius pinigų plovimo ir terorizmo finansavimo prevencijos tikslais, remiantis Įstatymu dėl konkrečios finansinių sandorių informacijos teikimo ir naudojimo (IKFSITN). Tačiau IKFSITN nustatomos tik duomenų valdytojų, kurie tvarko asmeninę kredito informaciją pagal KIĮ ir kuriems taikoma FPK priežiūra (žr. (13) konstatuojamąją dalį), informacijos atskleidimo prievolės. Kadangi tokių duomenų valdytojų vykdomam asmeninės kredito informacijos tvarkymui šis sprendimas netaikomas, IKFSITN šiam vertinimui nėra svarbus.

⁽²⁰⁰⁾ RPAI 3 straipsnyje kaip galimas ryšių duomenų rinkimo teisinis pagrindas taip pat nurodomas Karinio teismo įstatymas. Tačiau tuo įstatymu reglamentuojamas informacijos apie karinį personalą rinkimas ir civiliams jis gali būti taikomas tik ribotais atvejais (pvz., jei karinis personalas ir civiliai asmenys nusikaltimą padarytų kartu arba jei asmuo padaro nusikaltimą, dėl kurio nukenčia karinis personalas, pažeidimo nagrinėjimo procedūra gali būti pradėta karo teisme, žr. Karinio teismo įstatymo 2 straipsnį). Bet kurio atveju jame nustatomos bendrosios nuostatos, kuriomis reglamentuojama krata ir poėmis ir kurios yra panašios į BPI (žr., pvz., Karinio teismo įstatymo 146–149 ir 153–156 straipsnius), ir jose numatyta, pavyzdžiui, kad pašto korespondencija gali būti renkama tik tada, kai tai būtina tyrimui atlikti ir remiantis Karinio teismo orderiu. Jei elektroninė korespondencija būtų renkama remiantis šiuo įstatymu, būtų taikomi RPAI nustatyti apribojimai ir apsaugos priemonės. Žr. II priedo 2.2.2 skirsnį ir 50 išnašą.

⁽²⁰¹⁾ BPI 215 straipsnio 1 ir 2 dalys. Taip pat žr. BPI 106 straipsnio 1 dalį, 107 ir 109 straipsnius, kuriuose nustatyta, kad teismai gali atlikti kratas ir poėmius, jei atitinkami daiktai ar asmenys laikomi susijusiais su konkrečia byla. Žr. II priedo 2.2.1.2 skirsnį.

⁽²⁰²⁾ BPI 199 straipsnio 1 dalis.

⁽²⁰³⁾ BPI 106 straipsnio 3 dalis.

⁽²⁰⁴⁾ BPI 106 straipsnio 3 dalis.

- (154) Procedūrinių apsaugos priemonių atžvilgiu BPI reikalaujama, kad teismas išduotų orderį atlikti kratą ar poėmį⁽²⁰⁵⁾. Kratos ar poėmio atlikimas neturint orderio leidžiami tik išimtiniais atvejais, t. y. kai aplinkybės reikalauja skubiai veikti⁽²⁰⁶⁾: nusikalstama veika įtariamo asmens suėmimo ar sulaikymo metu (*in loco*)⁽²⁰⁷⁾ arba kai daiktas buvo išmestas ar savanoriškai pateiktas nusikalstama veika įtariamo asmens arba trečiojo asmens (asmens duomenų atveju, pačio su duomenimis susijusio asmens)⁽²⁰⁸⁾. Už neteisėtai atliktą kratą ir poėmį taikomos baudžiamosios sankcijos⁽²⁰⁹⁾, o bet kokie įrodymai, surinkti pažeidžiant BPI, laikomi netinkamais⁽²¹⁰⁾. Galiausiai atitinkamiems asmenims visada turi būti nedelsiant pranešama apie kratą ar poėmį (įskaitant jų duomenų poėmį)⁽²¹¹⁾, o taip atitinkamai bus palengvinamas naudojimas asmens materialinėmis teisėmis ir teisių gynimo teise (žr. visų pirma galimybę užginčyti poėmio orderio vykdymą, žr. (180) konstatuojamąją dalį).

3.2.1.2. Galimybė susipažinti su ryšių informacija

- (155) Remdamosi RPAI, Korėjos baudžiamosios teisėsaugos institucijos gali imtis dviejų rūšių priemonių⁽²¹²⁾: viena vertus, rinkti „ryšių patvirtinimo duomenis“⁽²¹³⁾, apimančius telekomunikacinių ryšių datą, jų pradžios ir pabaigos laiką, atliktų ir gautų skambučių skaičių, taip pat kitos šalies abonento numerį, naudojimo dažnumą, telekomunikacijų paslaugų naudojimo žurnalo failus ir vietos nustatymo informaciją (pavyzdžiui, atsižvelgiant į perdavimo bokštus, į kuriuos gaunami signalai), ir, kita vertus, taikyti „ryšius ribojančias priemones“, kurios apima tiek tradicinio pašto korespondencijos turinio rinkimą, tiek tiesioginių telekomunikacinių ryšių turinio perėmimą⁽²¹⁴⁾.
- (156) Su ryšių patvirtinimo duomenimis galima susipažinti tik tada, kai tai būtina baudžiamajam tyrimui atlikti arba nuosprendžiui priimti⁽²¹⁵⁾, remiantis teismo išduotu orderiu⁽²¹⁶⁾. Šiuo atžvilgiu RPAI reikalaujama, kad išsami informacija būtų pateikta ir prašyme išduoti orderį (pvz., apie prašymo priežastis, ryšį su taikymo sritimi ir (arba) abonentu ir reikalingais duomenimis) ir pačiame orderyje (pvz., apie priemonės tikslą, taikymo sritį ir mastą)⁽²¹⁷⁾. Rinkti duomenis neturint orderio galima tik tada, kai dėl aplinkybių, kurios reikalauja skubos, neįmanoma gauti

⁽²⁰⁵⁾ BPI 215 straipsnio 1 ir 2 dalys ir 113 straipsnis. Prašydama orderio atitinkama institucija turi pateikti medžiagą, kurioje įrodomas nusikalstama veika įtariamo asmens įtarimo pagrindas, įrodoma, kad atlikti kratą, patikrinimą ar poėmį yra būtina ir kad yra atitinkamų daiktų, kurie turi būti paimti (Baudžiamojo proceso reglamento 108 straipsnio 1 dalis). Pačiame orderyje, be kita ko, turi būti nurodyti nusikalstama veika įtariamo asmens vardas ir pavardė ir nusikalstama veika, vieta, asmuo ar daiktai, kurie yra kratos objektas, arba daiktai, kurie turi būti paimti, išdavimo data ir galiojimo laikotarpis (BPI 114 straipsnio 1 dalis kartu su 219 straipsniu). Žr. II priedo 2.2.1.2 skirsnį.

⁽²⁰⁶⁾ Tokiu atveju, kai orderio neįmanoma gauti, nes nusikaltimo vietos aplinkybės reikalauja skubiai veikti (BPI 216 straipsnio 3 dalis), orderis paskui vis tiek turi būti nedelsiant gautas (BPI 216 straipsnio 3 dalis).

⁽²⁰⁷⁾ BPI 216 straipsnio 1 ir 2 dalys.

⁽²⁰⁸⁾ BPI 218 straipsnis. Be to, kaip paaiškinta II priedo 2.2.1.2 skirsnyje, savanoriškai pateikti daiktai įrodymais teismo procese pripažįstami tik tuo atveju, jei nekyla pagrįstų abejonų dėl informacijos atskleidimo savanoriško pobūdžio, o tai turi įrodyti prokuroras.

⁽²⁰⁹⁾ Baudžiamojo įstatymo 321 straipsnis.

⁽²¹⁰⁾ BPI 308-2 straipsnis. Be to, asmuo (ir jo advokatas) gali dalyvauti vykdamas kratos ar poėmio orderį, todėl pareikšti prieštaravimą jis taip pat gali orderio vykdymo metu (BPI 121 ir 219 straipsniai).

⁽²¹¹⁾ BPI 121 ir 122 straipsniai (dėl kratos) ir 219 straipsnis kartu su BPI 106 straipsnio 4 dalimi (dėl poėmio).

⁽²¹²⁾ Taip pat žr. II priedo 2.2.2.1 skirsnį. Siekiant imtis tokių priemonių būtinas telekomunikacijų paslaugų teikėjų sutikimas padėti, kai jiems pateikiamas raštiškas teismo leidimas (RPAI 9 straipsnio 2 dalis), kurį paslaugų teikėjai turi saugoti (RPAI 15-2 straipsnis ir RPAI vykdymo užtikrinimo dekretu 12 straipsnis). Telekomunikacijų paslaugų teikėjai gali atsisakyti bendradarbiauti, kai teismo rašytiniame leidime nurodyta informacija apie asmenį, kurio informaciją norima rinkti, yra neteisinga (pavyzdžiui, asmens telefono numeris), ir jiems draudžiama, nepaisant aplinkybių, atskleisti slaptažodžius, naudojamus naudojantis telekomunikacijų paslaugomis (RPAI 9 straipsnio 4 dalis).

⁽²¹³⁾ RPAI 2 straipsnio 11 dalis.

⁽²¹⁴⁾ Žr. RPAI 2 straipsnio 6 dalį, kurioje nurodoma „cenzūra“ (korespondencijos atidarymas neturint atitinkamos šalies sutikimo arba informacijos apie jos turinį sužinojimas, įrašymas ar nuslėpimas taikant kitas priemones), ir RPAI 2 straipsnio 7 dalis, kurioje nurodomas „slaptas pokalbių klausymasis“ (telekomunikacinių ryšių turinio gavimas arba įrašymas, išklausanč ar kartu skaitant pranešimų garsus, žodžius, simbolius ar vaizdus taikant elektronines ir mechanines priemones neturint atitinkamos šalies sutikimo arba trukdymas jos perdavimui ir gavimui).

⁽²¹⁵⁾ RPAI 13 straipsnio 1 dalis. Taip pat žr. II priedo 2.2.2.3 skirsnį. Be to, buvimo vietos nustatymo realiuoju laiku duomenys ir ryšių patvirtinimo duomenys, susiję su konkrečia bazine stotimi, gali būti renkami tik sunkių nusikaltimų tyrimo tikslais arba tais atvejais, kai kitaip būtų sunku užkirsti kelią nusikalstamos veikos vykdymui arba surinkti įrodymus (RPAI 13 straipsnio 2 dalis). Tai rodo, kad reikia numatyti papildomas apsaugos priemones visų pirma privatumo ribojimo priemonių atveju, laikantis proporcingumo principo.

⁽²¹⁶⁾ RPAI 13 ir 6 straipsniai.

⁽²¹⁷⁾ Žr. RPAI 13 straipsnio 3 ir 9 dalis kartu su 6 straipsnio 4 ir 6 dalimis.

teismo leidimo ir tokiu atveju orderis turi būti gautas ir apie jį turi būti pranešta telekomunikacijų paslaugų teikėjui iš karto po to, kai paprašoma pateikti duomenis⁽²¹⁸⁾. Jeigu paskui teismas atsisako išduoti leidimą, surinkta informacija turi būti sunaikinta⁽²¹⁹⁾.

- (157) Papildomų apsaugos priemonių, susijusių su ryšių patvirtinimo duomenų rinkimu, atžvilgiu RPAĮ nustatyti konkretūs įrašų saugojimo ir skaidrumo reikalavimai⁽²²⁰⁾. Visų pirma ir baudžiamosios teisėsaugos institucijos⁽²²¹⁾, ir telekomunikacijų paslaugų teikėjai⁽²²²⁾ privalo registruoti pateiktus prašymus ir informacijos atskleidimo faktus. Be to, iš esmės baudžiamosios teisėsaugos institucijos privalo informuoti asmenis apie tai, kad buvo surinkti jų ryšių patvirtinimo duomenys⁽²²³⁾. Toks pranešimas gali būti atidėtas tik išimtinėmis aplinkybėmis, gavus kompetentingos apygardos prokuratūros direktoriaus leidimą⁽²²⁴⁾. Toks leidimas gali būti suteiktas tik tada, kai pranešus gali 1) kilti pavojus nacionaliniam saugumui, visuomenės saugumui ir tvarkai joje, 2) gali būti sukelta mirtis ar kūno sužalojimas, 3) gali būti trukdoma teisingam teismo procesui (pavyzdžiui, jei pranešus būtų sunaikinti įrodymai arba grasinama liudytojams) arba 4) gali būti apšmeižtas įtariamasis asmuo, aukos ar kiti su byla susiję asmenys arba gali būti pažeistas jų privatumas. Tokiais atvejais pranešimas turi būti pateiktas per 30 dienų nuo tos dienos, kai išnyksta atidėjimo pagrindas (-ai)⁽²²⁵⁾. Gavę pranešimą, asmenys turi teisę gauti informaciją apie jų duomenų rinkimo priežastis⁽²²⁶⁾.
- (158) Griežtesnės taisyklės taikomos ryšius ribojančioms priemonėms, kurios gali būti taikomos tik tada, kai yra svarių priežasčių įtarti, kad planuojami, vykdomi arba buvo įvykdyti tam tikri konkrečiai RPAĮ išvardyti sunkūs nusikaltimai⁽²²⁷⁾. Be to, ryšius ribojančių priemonių galima imtis tik kraštutiniu atveju ir kai kitaip sunku užkirsti kelią nusikaltimui, suimti nusikaltėlių arba surinkti įrodymus⁽²²⁸⁾. Jos turi būti nedelsiant nutrauktos, kai jos neberekalingos, siekiant užtikrinti, kad ryšių privatumo pažeidimas būtų kuo labiau ribotas⁽²²⁹⁾. Informacija, kuri buvo neteisėtai gauta taikant ryšius ribojančias priemones, nėra pripažįstama kaip įrodymas teismo ar drausminėse procedūrose⁽²³⁰⁾.
- (159) Procedūrinių apsaugos priemonių atžvilgiu RPAĮ reikalaujama, kad ryšius ribojančių priemonių taikymui teismas išduotų orderį⁽²³¹⁾. Be to, RPAĮ reikalaujama, kad prašyme išduoti orderį ir pačiame orderyje būtų pateikta išsami informacija⁽²³²⁾, įskaitant informaciją apie prašymo pagrindimą, taip pat perduodamą ir gaunamą informaciją, kurią reikia surinkti (tai turi būti įtariamojo, dėl kurio atliekamas tyrimas, perduodama arba gaunama informacija)⁽²³³⁾. Tokių priemonių imtis neturint orderio galima tik gresiant neišvengiamam organizuoto nusikalstamumo

⁽²¹⁸⁾ RPAĮ 13 straipsnio 2 dalis.

⁽²¹⁹⁾ RPAĮ 13 straipsnio 3 dalis.

⁽²²⁰⁾ Žr. II priedo 2.2.2.3 skirsnį.

⁽²²¹⁾ RPAĮ 13 straipsnio 5 ir 6 dalys.

⁽²²²⁾ RPAĮ 13 straipsnio 7 dalis. Be to, telekomunikacijų paslaugų teikėjai privalo du kartus per metus pranešti apie ryšių patvirtinimo duomenų atskleidimą Mokslo ir IRT ministerijai.

⁽²²³⁾ Žr. RPAĮ 13-3 straipsnio 7 dalį kartu su 9-2 straipsniu. Visų pirma asmenims turi būti pranešta per 30 dienų nuo sprendimo patraukti (nepatraukti) baudžiamojon atsakomybėn priėmimo arba per 30 dienų nuo sprendimo nutraukti kaltinimus priėmimo (nors pranešimas bet koku atveju turi būti pateiktas per 30 dienų praėjus metams nuo tos dienos, kai buvo surinkta informacija) (žr. RPAĮ 13-3 straipsnio 1 dalį).

⁽²²⁴⁾ RPAĮ 13-3 straipsnio 2 ir 3 dalys.

⁽²²⁵⁾ RPAĮ 13-3 straipsnio 4 dalis.

⁽²²⁶⁾ RPAĮ 13-3 straipsnio 5 dalis. Asmens prašymu prokuroras arba teismo policijos pareigūnas per 30 dienų nuo prašymo gavimo turi raštu nurodyti priežastis, išskyrus atvejus, kai taikoma viena iš pranešimo atidėjimo išimčių (RPAĮ 13-3 straipsnio 6 dalis).

⁽²²⁷⁾ Pavyzdžiui, maištas, su narkotikais susiję nusikaltimai, su sprogmenimis susiję nusikaltimai, taip pat nusikaltimai, susiję su nacionaliniu saugumu, diplomatiniais santykiais arba karinėmis bazėmis ir įrenginiais (žr. RPAĮ 5 straipsnio 1 dalį). Taip pat žr. II priedo 2.2.2.2 skirsnį.

⁽²²⁸⁾ RPAĮ 3 straipsnio 2 dalis ir 5 straipsnio 1 dalis.

⁽²²⁹⁾ RPAĮ vykdymo užtikrinimo dekreto 2 straipsnis.

⁽²³⁰⁾ RPAĮ 4 straipsnis.

⁽²³¹⁾ RPAĮ 6 straipsnio 1, 2, 5 ir 6 dalys.

⁽²³²⁾ Prašyme išduoti orderį turi būti nurodytos 1) esminės priežastys, dėl kurių įtariama (*prima facie*), kad vienas iš išvardytų nusikaltimų yra planuojamas, vykdomas ar įvykdytas, taip pat bet kokia patvirtinanti medžiaga, 2) ryšius ribojančios priemonės, taip pat jų taikymo sritis, mastas, tikslas ir galiojimo laikotarpis ir 3) vieta, kurioje priemonės bus įgyvendinamos, ir jų įgyvendinimo būdas (RPAĮ 6 straipsnio 4 dalis ir RPAĮ vykdymo užtikrinimo dekreto 4 straipsnio 1 dalis). Pačiame orderyje turi būti nurodytos priemonės ir jų taikymo sritis, mastas, galiojimo laikotarpis, įgyvendinimo vieta ir būdas (RPAĮ 6 straipsnio 6 dalis).

⁽²³³⁾ Ryšius ribojančios priemonės taikymo sritis turi būti konkretūs pašto korespondencijos arba telekomunikacijų ryšių vienetai, kuriuos siunčia arba gauna įtariamasis, arba pašto korespondencijos arba telekomunikacijų ryšių vienetai, kuriuos per nustatytą laikotarpį siunčia arba gauna įtariamasis (RPAĮ 5 straipsnio 2 dalis).

pavojui arba kitam sunkiam nusikaltimui, kuris gali tiesiogiai sukelti mirtį ar sunkų sužalojimą, ir egzistuoja ekstremalioji situacija, dėl kurios neįmanoma taikyti įprastos procedūros⁽²³⁴⁾. Tačiau tokiu atveju prašymas išduoti orderį turi būti pateiktas iš karto po to, kai buvo imtasi priemonės⁽²³⁵⁾. Ryšius ribojančios priemonės gali būti taikomos ne ilgesnį kaip dviejų mėnesių laikotarpį⁽²³⁶⁾ ir teismui pritarus gali būti pratęšiamos tik tuo atveju, jei tebesilaikoma priemonių įgyvendinimo sąlygų⁽²³⁷⁾. Pratęstas laikotarpis negali būti ilgesnis kaip vieni metai, o tam tikrų ypač sunkių nusikaltimų atveju – treji metai (kaip antai nusikaltimų, susijusių su maištu, užsienio valstybės agresija, nacionaliniu saugumu)⁽²³⁸⁾.

- (160) Kaip ir ryšių patvirtinimo duomenų rinkimo atveju, RPAĮ reikalaujama, kad telekomunikacijų paslaugų teikėjai⁽²³⁹⁾ ir teisėsaugos institucijos⁽²⁴⁰⁾ saugotų įrašus apie ryšius ribojančių priemonių taikymą, ir numatoma, kad atitinkamam asmeniui turi būti pranešama apie priemonių taikymą, su galimybe šį pranešimą išimties tvarka atidėti dėl svarbių viešojo intereso priežasčių⁽²⁴¹⁾.
- (161) Galiausiai už kelių RPAĮ apribojimų ir apsaugos priemonių nesilaikymą (įskaitant, pavyzdžiui, prievoles gauti orderį, saugoti įrašus ir pranešti asmeniui apie duomenų rinkimą) ir ryšių patvirtinimo duomenų rinkimo atveju, ir ryšius ribojančių priemonių taikymo atveju taikomos baudžiamosios sankcijos⁽²⁴²⁾.
- (162) Todėl baudžiamosios teisėsaugos institucijų įgaliojimai rinkti ryšių duomenis pagal RPAĮ (ir duomenis apie ryšių turinį, ir ryšių patvirtinimo duomenis) yra apriboti aiškiais ir tiksliais taisyklėmis ir jiems taikomos tam tikros apsaugos priemonės. Šiomis apsaugos priemonėmis visų pirma užtikrinama tokių priemonių vykdymo priežiūra tiek *ex ante* (gaunant išankstinį teismo leidimą), tiek *ex post* (taikant įrašų saugojimo ir informacijos teikimo reikalavimus) ir sudaromos palankesnės sąlygos asmenims naudotis veiksmingomis teisių gynimo priemonėmis (užtikrinant, kad jie būtų informuoti apie jų duomenų rinkimą).

3.2.1.3. Prašymai savanoriškai atskleisti abonentų duomenis

- (163) Korėjos teisėsaugos institucijos gali ne tik taikyti (153)–(162) konstatuojamosiose dalyse aprašytas priverstines priemones, bet ir prašyti telekomunikacijų paslaugų teikėjus savanoriškai pateikti „ryšių duomenis“, kuriais būtų remiamasi nagrinėjant baudžiamąją bylą, atliekant tyrimą arba skiriant bausmę (TĮ 83 straipsnio 3 dalis). Ši galimybė taikoma tik ribotiems duomenų rinkiniams, t. y. naudotojų vardui ir pavardai, gyventojų registracijos numeriui, adresui ir telefono numeriui, abonemento užsisakymo arba atsisakymo datoms, taip pat naudotojo identifikavimo kodams (t. y. kodams, naudojamiems teisėtam kompiuterinių sistemų ar ryšių tinklų naudotojui identifikuoti)⁽²⁴³⁾. Kadangi „naudotojais“ laikomi tik tie asmenys, kurie paslaugų sutartį sudaro tiesiogiai su Korėjos telekomunikacijų paslaugų teikėju⁽²⁴⁴⁾, šiai kategorijai paprastai nepriskiriami ES asmenys, kurių duomenys buvo perduoti į Korėjos Respubliką⁽²⁴⁵⁾.
- (164) Tokiam savanoriškam informacijos atskleidimui taikomi skirtingi apribojimai teisėsaugos institucijos naudojimosi įgaliojimais atžvilgiu ir telekomunikacijų operatoriaus bendradarbiavimo atžvilgiu. Paprastai teisėsaugos institucijos turi veikti laikydamosi konstitucinių būtinumo ir proporcingumo principų (Konstitucijos 12 straipsnio 1 dalis ir 37 straipsnio 2 dalis), įskaitant atvejus, kai jos prašo savanoriškai pateikti informaciją. Be to, jos turi

⁽²³⁴⁾ RPAĮ 8 straipsnio 1 dalis. Tačiau ekstremaliųjų situacijų atvejais informacija visada turi būti renkama remiantis „neišvengiamos cenzūros ir (arba) slapto pokalbių klausymosi pareiškimu“, o rinkimą atliekanti institucija privalo registruoti visas neatidėliotinas priemones (RPAĮ 8 straipsnio 4 dalis).

⁽²³⁵⁾ Informacijos rinkimą reikia nedelsiant nutraukti, jei teisėsaugos institucija per 36 valandas negauna teismo leidimo (RPAĮ 8 straipsnio 2 dalis), ir tokiu atveju, kaip paaiškinta II priedo 2.2.2.2 skirsnelyje, surinkta informacija iš esmės bus sunaikinta. Teismui taip pat turi būti pranešta apie atvejus, kai neatidėliotinos priemonės buvo įgyvendintos per tokį trumpą laiką, kad buvo išvengta būtinybės gauti leidimą (pvz., jei įtariamasis suimamas vos pradėjus vykdyti informacijos perėmimą (žr. RPAĮ 8 straipsnio 5 dalį). Tokiu atveju teismui turi būti pateikta informacija apie priemonės taikymo tikslą, sritį, mastą, laikotarpį, įgyvendinimo vietą ir rinkimo būdą, taip pat prašymo dėl teismo leidimo nepateikimo priežastis (RPAĮ 8 straipsnio 6–7 dalys).

⁽²³⁶⁾ RPAĮ 6 straipsnio 7 dalis. Jei priemonių taikymo tikslas pasiekiamas anksčiau nei baigiasi tas laikotarpis, priemonių taikymas turi būti nedelsiant nutrauktas.

⁽²³⁷⁾ RPAĮ 6 straipsnio 7–8 dalys.

⁽²³⁸⁾ RPAĮ 6 straipsnio 8 dalis.

⁽²³⁹⁾ RPAĮ 9 straipsnio 3 dalis.

⁽²⁴⁰⁾ RPAĮ vykdymo užtikrinimo dekreto 18 straipsnio 1 dalis.

⁽²⁴¹⁾ Visų pirma prokuroras privalo apie tai pranešti asmeniui per 30 dienų nuo kaltinimų pateikimo arba sprendimo kaltinimų nepateikti arba nesuimti (RPAĮ 9-2 straipsnio 1 dalis). Pranešimas gali būti atidėtas, pritarus apygardos prokuratūros vadovui, jei pranešus galėtų kilti didelis pavojus nacionaliniam saugumui arba būtų sutrikdytas visuomenės saugumas ir viešoji tvarka, arba kai tikėtina, kad pranešus kiltų grėsmė kitų asmenų gyvybėms ir fizinei sveikatai (RPAĮ 9-2 straipsnio 4–6 dalys).

⁽²⁴²⁾ RPAĮ 16 ir 17 straipsniai.

⁽²⁴³⁾ TĮ 83 straipsnio 3 dalis. Taip pat žr. II priedo 2.2.3 skirsnį.

⁽²⁴⁴⁾ TĮ 2 straipsnio 9 dalis.

⁽²⁴⁵⁾ Taip pat žr. II priedo 2.2.3 skirsnį.

laikytis AIAĮ, visų pirma rinkdamos asmens duomenis tik tiek, kiek tai būtina teisėtam tikslui pasiekti, kad būtų kuo labiau sumažintas poveikis asmenų privatumui (kaip antai laikantis AIAĮ 3 straipsnio 1 ir 6 dalių). Konkrečiau, prašymai gauti ryšių duomenis remiantis TĮI turi būti pateikiami raštu ir juose turi būti nurodytos prašymo priežastys, ryšys su atitinkamu naudotoju ir prašomų duomenų apimtis ⁽²⁴⁶⁾.

- (165) Telekomunikacijų paslaugų teikėjai neprivalo patenkinti tokių prašymų, o juos patenkinti gali tik laikydamiesi AIAĮ. Tai visų pirma reiškia, kad jie turi suderinti skirtingus susijusius interesus ir negali pateikti duomenų, jei tai galėtų nepagrįstai pažeisti asmens ar trečiosios šalies interesus ⁽²⁴⁷⁾. Taip būtų tokiu atveju, kai, pavyzdžiui, būtų aišku, kad prašančioji institucija piktnaudžiavo savo įgaliojimais ⁽²⁴⁸⁾. Telekomunikacijų paslaugų teikėjai privalo saugoti atskleidimo įrašus pagal TĮI ir du kartus per metus teikti ataskaitas Mokslo ir IRT ministrui ⁽²⁴⁹⁾.
- (166) Be to, pagal pranešimo Nr. 2021-5 3 skirsnį (I priedas) telekomunikacijų paslaugų teikėjai iš esmės turi pranešti atitinkamam asmeniui, kai jie patenkina prašymą savanoriškai teikti duomenis ⁽²⁵⁰⁾. Taip asmeniui atitinkamai suteikiama galimybė pasinaudoti savo teisėmis, o jei jo duomenys atskleidžiami neteisėtai, ginti savo teises nukentėjus dėl duomenų valdytojo veiksmų (pavyzdžiui, jam dėl duomenų atskleidimo pažeidus AIAĮ arba patenkinus akivaizdžiai neproporcingą prašymą) arba teisėsaugos institucijos veiksmų (pavyzdžiui, dėl to, kad ji ėmėsi veiksmų, viršijančių tai, kas būtina ir proporcinga, arba nesilaikė TĮI procedūrinių reikalavimų).

3.2.2. Tolesnis surinktos informacijos naudojimas

- (167) Korėjos baudžiamosios teisėsaugos institucijų surinktų asmens duomenų tvarkymui taikomi visi AIAĮ reikalavimai, be kita ko, susiję su tikslo apribojimu (AIAĮ 3 straipsnio 1 ir 2 dalys), naudojimo ir duomenų teikimo trečiosioms šalims teisėtumu (AIAĮ 15, 17 ir 18 straipsniai), tarptautiniu perdavimu (AIAĮ 17 ir 18 straipsniai kartu su pranešimo 2021-5 2 skirsniu) ⁽²⁵¹⁾, proporcingumu ir (arba) duomenų kiekio mažinimu (AIAĮ 3 straipsnio 1 ir 6 dalys) ir saugojimo apribojimais (AIAĮ 21 straipsnis) ⁽²⁵²⁾.
- (168) Ryšių turinio, gauto taikant ryšius ribojančias priemones, atžvilgiu RPAĮ nustatyti konkretūs apribojimai dėl galimo jų naudojimo vykdant sunkių nusikaltimų tyrimus, baudžiamąjį persekiojimą už juos ar jų prevenciją ⁽²⁵³⁾, taikant drausmines procedūras dėl tų pačių nusikaltimų, nagrinėjant ieškinius dėl žalos atlyginimo, kuriuos iškėlė ryšių šalis, arba kai tai konkrečiai leidžiama pagal kitus įstatymus ⁽²⁵⁴⁾. Be to, surinktas internetu perduodamų telekomunikacinių ryšių turinys gali būti saugomas tik gavus teismo, kuris išdavė leidimą taikyti ryšius ribojančias priemones ⁽²⁵⁵⁾, sutikimą, siekiant jį naudoti sunkių nusikaltimų tyrimui, baudžiamajam persekiojimui ar prevencijai ⁽²⁵⁶⁾. Apskritai RPAĮ draudžiama atskleisti konfidencialią informaciją, gautą taikant ryšius ribojančias priemones, ir naudoti tokią informaciją siekiant pakenkti asmenų, kuriems taikomos priemonės, reputacijai ⁽²⁵⁷⁾.

3.2.3. Priežiūra

- (169) Korėjoje baudžiamosios teisėsaugos institucijų veiklą prižiūri įvairios įstaigos ⁽²⁵⁸⁾.

⁽²⁴⁶⁾ TĮI 83 straipsnio 4 dalis. Kai dėl aplinkybių, kurios reikalauja skubos, neįmanoma pateikti rašytinio prašymo, rašytinis prašymas turi būti pateiktas iš karto skubos priežastiai išnykus (TĮI 83 straipsnio 4 dalis).

⁽²⁴⁷⁾ AIAĮ 18 straipsnio 2 dalis.

⁽²⁴⁸⁾ 2016 m. kovo 10 d. Aukščiausiojo Teismo sprendimas Nr. 2012Da105482. Taip pat žr. II priedo 2.2.3 skirsnį dėl šio Aukščiausiojo Teismo sprendimo.

⁽²⁴⁹⁾ TĮI 83 straipsnio 5–6 dalys.

⁽²⁵⁰⁾ Šiam reikalavimui taikomos ribotos ir sąlyginės išimtys, visų pirma, jei pranešus būtų kliudoma vykstančiam baudžiamajam tyrimui arba galėtų kilti pavojus kito asmens gyvybei ar fizinei sveikatai ir tol, kol tokie pavojai kiltų, kai tos teisės ar interesai yra akivaizdžiai viršesni už duomenų subjekto teises. Žr. pranešimo 3 skirsnio iii dalies 1 punktą.

⁽²⁵¹⁾ Visų pirma reikalaujama, kad Korėjos valdžios institucijos, priimdamos teisiškai privalomą dokumentą, užtikrintų apsaugos lygį, lygiavertį AIAĮ, taip pat žr. (90) konstatuojamąją dalį.

⁽²⁵²⁾ Taip pat žr. II priedo 1.2 skirsnį.

⁽²⁵³⁾ Žr. (158) konstatuojamąją dalį.

⁽²⁵⁴⁾ RPAĮ 12 straipsnis. Žr. II priedo 2.2.2.2 skirsnį.

⁽²⁵⁵⁾ Ryšius ribojančias priemones taikantis prokuroras arba policijos pareigūnas per 14 dienų nuo priemonių taikymo pabaigos turi pasirinkti saugotinus telekomunikacinius ryšius ir prašyti teismo sutikimo (policijos pareigūno atveju prašymas turi būti pateiktas prokurorui, kuris tuomet prašymą pateikia teismui) (žr. RPAĮ 12-2 straipsnio 1 ir 2 dalis).

⁽²⁵⁶⁾ Prašyme išduoti tokį leidimą turi būti pateikta informacija apie ryšius ribojančias priemones, priemonių rezultatų santrauka, saugojimo priežastys (kartu su patvirtinančia medžiaga) ir nurodyti saugotini telekomunikaciniai ryšiai (RPAĮ 12-2 straipsnio 3 dalis). Jei prašymas nepateikiamas, gauti duomenys turi būti ištrinti per 14 dienų nuo ryšių ribojančių priemonių taikymo pabaigos (RPAĮ 12-2 straipsnio 5 dalis), o jei prašymas atmetamas – per septynias dienas (RPAĮ 12-2 straipsnio 5 dalis). Abiem atvejais teismui, kuris suteikė leidimą rinkti duomenis, per septynias dienas turi būti pateikta ataskaita apie ištrynimą.

⁽²⁵⁷⁾ RPAĮ vykdymo užtikrinimo dekreto 11 straipsnio 2 dalis.

⁽²⁵⁸⁾ Žr. II priedo 2.3 skirsnį.

- (170) Pirmą, policijai taikoma vidaus priežiūra, kurią įgyvendina generalinis inspektorius⁽²⁵⁹⁾ vykdydamas teisėtumo kontrolę, be kita ko, galimų žmogaus teisių pažeidimų atžvilgiu. Generalinio inspektoriaus pareigybė įsteigta siekiant įgyvendinti Viešojo sektoriaus audito įstatymą, kuriuo skatinama steigti savikontrolės įstaigas ir nustatomi konkretūs jų sudėties ir užduočių reikalavimai. Visų pirma įstatyme reikalaujama, kad savikontrolės įstaigos vadovas nebūtų skiriamas iš susijusios institucijos (būtų, pvz., buvęs teisėjas, profesorius) ir būtų skiriamas laikotarpiui nuo dvejų iki penkerių metų⁽²⁶⁰⁾, nustatyta, kad jis gali būti atleistas iš pareigų tik dėl pagrįstų priežasčių (pavyzdžiui, kai negali eiti pareigų dėl su sveikata susijusių priežasčių arba kai jam taikomos drausminės priemonės)⁽²⁶¹⁾ ir kad turi būti užtikrinamas kuo didesnis jo nepriklausomumas⁽²⁶²⁾. Už trukdymą įgyvendinti savikontrolę skiriamos administracinės baudos⁽²⁶³⁾. Audito ataskaitos (kurios gali apimti rekomendacijas, prašymus taikyti drausmines priemones ir prašymus skirti kompensacijas ar ištaisyti) perduodamos atitinkamos valdžios institucijos vadovui, Audito ir inspektavimo valdybai (AIV)⁽²⁶⁴⁾ ir paprastai viešai skelbiamos⁽²⁶⁵⁾. Apie ataskaitos įgyvendinimo rezultatus taip pat turi būti pranešta AIV⁽²⁶⁶⁾ (žr. (173) konstatuojamąją dalį dėl AIV priežiūros vaidmens ir įgaliojimų).
- (171) Antra, AIAK prižiūri, kad baudžiamosios teisėsaugos institucijos tvarkytų duomenis pagal AIAĮ ir kitus teisės aktus, kuriais saugomas asmenų privatumas, įskaitant įstatymus, kuriais reglamentuojamas (elektroninių) įrodymų rinkimas baudžiamosios teisėsaugos tikslais, kaip aprašyta 3.2.1 skirsnyje⁽²⁶⁷⁾. Visų pirma AIAK vykdoma priežiūra apima duomenų rinkimo ir tvarkymo teisėtumo ir sąžiningumo (AIAĮ 3 straipsnio 1 dalis), kurie bus pažeisti, jei asmens duomenys bus gauti ir naudojami pažeidžiant tuos teisės aktus⁽²⁶⁸⁾, užtikrinimą, todėl AIAK taip pat gali atlikti tyrimus ir užtikrinti 3.2.1 skirsnyje aprašytų apribojimų ir apsaugos priemonių laikymąsi⁽²⁶⁹⁾. Vykdydama šį priežiūros vaidmenį AIAK gali naudotis visais savo tyrimų atlikimo ir taisomųjų veiksmų taikymo įgaliojimais, kaip išsamiai aprašyta 2.4.2 skirsnyje. Dar prieš įgyvendinant naują AIAĮ reformą (t. y. vykdydama savo ankstesnę viešojo sektoriaus priežiūros funkciją) AIAK vykdė keletą priežiūros veiksmų, susijusių su baudžiamosios teisėsaugos institucijų vykdomu asmens duomenų tvarkymu, pvz., susijusių su įtariamųjų apklausa (2013 m. rugpjūčio 26 d. byla Nr. 2013-16), su pranešimu asmenims apie administracinių baudų skyrimą (2015 m. sausio 26 d. byla Nr. 2015-02-04), su dalijimusi duomenimis su kitomis institucijomis (2018 m. liepos 9 d. byla Nr. 2018-15-146, 2018 m. gruodžio 10 d. byla Nr. 2018-25-308, 2019 m. sausio 29 d. byla Nr. 2019-02-015), su pirštų atspaudų ar nuotraukų rinkimu (2019 m. rugsėjo 9 d. byla Nr. 2019-17-273), su bepiločių orlaivių naudojimu (2020 m. sausio 13 d. byla Nr. 2020-01-004). Tokiais atvejais AIAK atliko tyrimus siekdama nustatyti, ar laikomasi kelių AIAĮ nuostatų (pvz., duomenų tvarkymo teisėtumo, tikslo apribojimo ir duomenų kiekio mažinimo principų), taip pat atitinkamų kitų įstatymų, pavyzdžiui, Baudžiamojo proceso įstatymo, nuostatų, ir prireikus teikė rekomendacijas, kaip tvarkyti duomenis laikantis duomenų apsaugos reikalavimų.
- (172) Trečia, nepriklausomą priežiūrą vykdo Nacionalinė žmogaus teisių komisija (NŽTK)⁽²⁷⁰⁾, kuri, vykdydama savo bendrusius įgaliojimus apsaugoti Konstitucijos 10–22 straipsniuose nustatytas pagrindines teises, gali tirti teisės į privatumą ir ryšių privatumą pažeidimus. NŽTK sudaro 11 komisijos narių, kurie turi turėti specialią kvalifikaciją⁽²⁷¹⁾ ir kuriuos įstatymų nustatyta tvarka skiria Prezidentas. Visų pirma keturis komisijos narius siūlo Nacionalinė Asamblėja, keturis narius – Prezidentas ir tris – Aukščiausiojo Teismo vyriausiasis teisėjas⁽²⁷²⁾. Pirmininką iš komisijos narių skiria Prezidentas, o šį paskyrimą patvirtinti turi Nacionalinė Asamblėja⁽²⁷³⁾. Komisijos nariai

⁽²⁵⁹⁾ Žr. II priedo 2.3.1 skirsnį. Taip pat žr. <https://www.police.go.kr/eng/knpa/org/org01.jsp>.

⁽²⁶⁰⁾ Auditoriai taip pat skiriami remiantis konkrečiomis įstatyme nustatytomis sąlygomis (žr. Viešojo sektoriaus audito įstatymo 16 ir tolesnius straipsnius).

⁽²⁶¹⁾ Viešojo sektoriaus audito įstatymo 8–11 straipsniai.

⁽²⁶²⁾ Viešojo sektoriaus audito įstatymo 7 straipsnis.

⁽²⁶³⁾ Viešojo sektoriaus audito įstatymo 41 straipsnis.

⁽²⁶⁴⁾ Viešojo sektoriaus audito įstatymo 23 straipsnio 1 dalis.

⁽²⁶⁵⁾ Viešojo sektoriaus audito įstatymo 26 straipsnis.

⁽²⁶⁶⁾ Viešojo sektoriaus audito įstatymo 23 straipsnio 3 dalis.

⁽²⁶⁷⁾ Žr. AIAĮ 7-8 straipsnio 3 ir 4 dalis ir 7-9 straipsnio 5 dalį.

⁽²⁶⁸⁾ Žr. AIAK pranešimo Nr. 2021-5 6 skirsnį (I priedas).

⁽²⁶⁹⁾ Taip pat žr. II priedo 2.3.4 skirsnį.

⁽²⁷⁰⁾ Žmogaus teisių komisijos įstatymo (NŽTK įstatymas) 1 straipsnis.

⁽²⁷¹⁾ Kad būtų paskirtas komisijos nariu asmuo turi būti 1) bent dešimt metų dirbęs universitete arba įgaliotame mokslinių tyrimų institute, ne žemesnėse kaip docento pareigose, 2) bent dešimt metų dirbęs teisėju, prokuroru ar advokatu, 3) bent dešimt metų dalyvavęs veikloje, susijusioje su žmogaus teisėmis (pvz., ne pelno siekiančioje, nevyriausybinėje organizacijoje arba tarptautinėje organizacijoje), arba 4) rekomenduotas pilietinės visuomenės grupės (NŽTK įstatymo 5 straipsnio 3 dalis). Be to, paskirtiems komisijos nariams draudžiama tuo pačiu metu eiti pareigas Nacionalinėje Asamblėjoje, vietos tarybose arba bet kurioje valstybės ar vietos valdžios institucijoje (valstybės pareigūno pareigas) (žr. NŽTK įstatymo 10 straipsnį).

⁽²⁷²⁾ NŽTK įstatymo 5 straipsnio 1 ir 2 dalys.

⁽²⁷³⁾ NŽTK įstatymo 5 straipsnio 5 dalis.

(įskaitant pirmininką) skiriami trejų metų kadencijai, kuri gali būti pratęsta, o atleisti jie gali būti tik tada, kai jiems skiriama laisvės atėmimo bausmė arba jie nebegali vykdyti savo pareigų dėl užsitęsios fizinės ar psichinės negalios (tokiu atveju du trečdaliai komisijos narių turi sutikti su atleidimu iš pareigų) (274). Atlikdama tyrimą, NŽTK gali prašyti pateikti atitinkamą medžiagą, atlikti patikrinimus ir kviesti asmenis liudyti (275). Vykdydama taisomųjų veiksmų taikymo įgaliojimus NŽTK gali teikti (viešas) rekomendacijas dėl konkrečios politikos ir praktikos tobulinimo arba taisymo, į kurias atsižvelgusios valdžios institucijos turi siūlyti įgyvendinimo planą (276). Jei atitinkama institucija rekomendacijų neįgyvendina, ji apie tai turi pranešti komisijai (277), kuri savo ruožtu gali apie tai pranešti Nacionalinei Asamblėjai ir (arba) viešai apie tai paskelbti. Remiantis Korėjos vyriausybės oficialiu pareiškimu (II priedo 2.3.5 skirsnis), Korėjos valdžios institucijos iš esmės laikosi NŽTK rekomendacijų ir turi rimtų paskatų tai daryti, nes jų įgyvendinimas buvo vertinamas atliekant bendrą nuolatinį vertinimą, kuriam vadovavo Ministro Pirmininko kanceliarija. Iš metinių duomenų apie NŽTK veiklą matyti, kad ji aktyviai prižiūri baudžiamosios teisėsaugos institucijų veiklą atskirų peticijų arba *ex officio* tyrimų pagrindu (278).

- (173) Ketvirta, bendrą viešosios valdžios institucijų veiklos teisėtumo kontrolę vykdo AIV, kuri nagrinėja valstybės pajamas ir išlaidas, tačiau apskritai prižiūri, kaip valdžios institucijos vykdo savo pareigas, siekdama gerinti viešojo administravimo veiklą (279). AIV yra oficialiai įsteigta Korėjos Respublikos Prezidento, tačiau vykdydama savo pareigas yra nepriklausoma (280). Be to, ji visiškai nepriklausomai samdo, atleidžia ir organizuoja savo žmogiškuosius išteklius ir sudaro savo biudžetą (281). AIV sudaro pirmininkas (skiria Prezidentas, pritarus Nacionalinei Asamblėjai) (282) ir šeši komisijos nariai (skiria Prezidentas pirmininko siūlymu) (283), kurie turi turėti konkrečią įstatymų nustatytą kvalifikaciją (284) ir gali būti atleisti tik apkaltos, nuteisimo laisvės atėmimo bausme ar negalėjimo atlikti savo pareigų dėl ilgalaikės psichinės ar fizinės negalios atveju (285). AIV kasmet atlieka bendrą auditą, tačiau taip pat gali atlikti specialų auditą, susijusį su ypatingos svarbos klausimais. Atlikdama auditą ar inspektuodama, AIV gali prašyti pateikti dokumentus ir dalyvauti konkrečius asmenis (286). AIV gali teikti rekomendacijas, prašyti taikyti drausmines priemones arba pateikti baudžiamąjį skundą (287).

- (174) Galiausiai Nacionalinė Asamblėja vykdo parlamentinę valdžios institucijų priežiūrą atlikdama jų veiklos (288) tyrimus ir patikrinimus (289). Ji gali prašyti atskleisti dokumentus, įpareigoti liudytojus liudyti (290), rekomenduoti

(274) NŽTK įstatymo 7 straipsnio 1 dalis ir 8 straipsnis.

(275) NŽTK įstatymo 36 straipsnis. Pagal įstatymo 6 straipsnio 7 dalį gali būti atsisakyta pateikti medžiagą ar daiktinius įrodymus, jei taip būtų atskleista konfidenciali valstybinė informacija, o tai galėtų turėti esminės įtakos valstybės saugumui ar diplomatiniam santykiams arba dėl to kiltų didelių kliūčių vykdant baudžiamąjį tyrimą ar būsima teismo procesą. Tokiais atvejais komisija gali prašyti atitinkamos agentūros vadovo papildomos informacijos (jis turi gera valia ją pateikti), jei tai būtina siekiant patikrinti, ar atsisakymas suteikti informaciją yra pagrįstas.

(276) NŽTK įstatymo 25 straipsnio 1 ir 3 dalys.

(277) NŽTK įstatymo 25 straipsnio 4 dalis.

(278) Pavyzdžiui, 2015–2019 m. NŽTK kasmet gavo 1 380–1 699 peticijas prieš baudžiamosios teisėsaugos institucijas ir išnagrinėjo toki pat didelį jų skaičių (pvz., 2018 m. ji išnagrinėjo 1 546 skundus prieš policiją, o 2019 m. – 1 249 skundus); ji taip pat atliko keletą *ex officio* tyrimų, kaip išsamiau aprašyta NŽTK 2018 m. metinėje ataskaitoje (paskelbta adresu <https://www.humanrights.go.kr/site/program/board/basicboard/view?menuid=002003003001&pagesize=10&boardtypeid=7017&boardid=7602641>) ir 2019 m. metinėje ataskaitoje (paskelbta adresu <https://www.humanrights.go.kr/site/program/board/basicboard/view?menuid=002003003001&pagesize=10&boardtypeid=7017&boardid=7606217>).

(279) Audito ir inspektavimo valdybos įstatymo (AIV įstatymas) 20 ir 24 straipsniai. Žr. II priedo 2.3.2 skirsni.

(280) AIV įstatymo 2 straipsnio 1 dalis.

(281) AIV įstatymo 2 straipsnio 2 dalis.

(282) AIV įstatymo 4 straipsnio 1 dalis.

(283) AIV įstatymo 5 straipsnio 1 dalis ir 6 straipsnis.

(284) Pavyzdžiui, ne mažiau kaip dešimt metų teisėjo, prokuroro ar advokato pareigose, ne mažiau kaip aštuoneri metai valstybės tarnautojo, universiteto dėstytojo ar aukštesnės pareigose universitete arba bent dešimt metų darbo biržinėje bendrovėje ar vyriausybės valdomoje institucijoje (iš kurių bent penkeri metai vykdomojo pareigūno pareigose) (žr. AIV įstatymo 7 straipsnį). Be to, komisijos nariams draudžiama dalyvauti politinėje veikloje ir tuo pačiu metu eiti pareigas Nacionalinėje Asamblėjoje, administracinėse agentūrose, organizacijose, kurių auditą ir inspektavimą atlieka AIV, arba bet kurioje kitoje įstaigoje ar pareigose už atlygį (AIV įstatymo 9 straipsnis).

(285) AIV įstatymo 8 straipsnis.

(286) Žr., pvz., AIV įstatymo 27 straipsnį.

(287) AIV įstatymo 24 ir 31–35 straipsniai.

(288) Žr. priedo 2.2.3 skirsni.

(289) Nacionalinės Asamblėjos įstatymo 128 straipsnis ir Valstybės administracijos inspektavimo ir tyrimo įstatymo 2, 3 ir 15 straipsniai. Tai apima ne tik kasmetinius vyriausybės veiklos visumos patikrinimus, bet ir tyrimus, susijusius su konkrečiais klausimais.

(290) Valstybės administracijos inspektavimo ir tyrimo įstatymo 10 straipsnio 1 dalis. Taip pat žr. Nacionalinės Asamblėjos įstatymo 128 ir 129 straipsnius.

taisomojus veiksmus (jei padaro išvadą, kad buvo vykdoma neteisėta ar netinkama veikla) ⁽²⁹¹⁾ ir viešai paskelbti savo išvadų rezultatus ⁽²⁹²⁾. Kai Nacionalinė Asamblėja nurodo imtis taisomųjų veiksmų, kuriuos, pavyzdžiui, galėtų sudaryti kompensacijos skyrimas, drausminių priemonių taikymas arba vidaus procedūrų tobulinimas, atitinkama valdžios institucija privalo nedelsdama imtis veiksmų ir apie rezultatus pranešti Nacionalinei Asamblėjai ⁽²⁹³⁾.

3.2.4. Teisių gynimas

- (175) Korėjos sistemoje siūlomi skirtingi (teisminiai) teisių gynimo būdai, įskaitant žalos atlyginimą.
- (176) Pirma, AIAI asmenims suteikiama teisė susipažinti su asmens duomenimis, tvarkomais baudžiamosios teisės saugos tikslais, juos taisyti, ištrinti ir sustabdyti jų tvarkymą ⁽²⁹⁴⁾.
- (177) Antra, asmenys gali pasinaudoti įvairiais AIAI siūlomais teisių gynimo mechanizmais, jei tvarkydama jų duomenis baudžiamosios teisės saugos institucija pažeidė AIAI arba kituose teisės aktuose (t. y. BPI arba RPAI, žr. (171) konstatuojamąją dalį) nustatytus asmens duomenų rinkimo apribojimus ir apsaugos priemones. Visų pirma asmenys gali pateikti skundą AIAK (be kita ko, per Korėjos interneto ir saugumo agentūros administruojamą privatumo apsaugos skambučių centrą ⁽²⁹⁵⁾) arba Tarpininkavimo ginčiuose dėl asmeninės informacijos komitetui ⁽²⁹⁶⁾. Šioms teisių gynimo galimybėms tolesni priimtinumai reikalavimai netaikomi. Be to, remdamiesi Administracinių ginčų įstatymu, asmenys gali apskusti AIAK sprendimus arba neveikimą (žr. (132) konstatuojamąją dalį).
- (178) Trečia, bet kuris asmuo ⁽²⁹⁷⁾ gali pateikti skundą NŽTK dėl Korėjos baudžiamosios teisės saugos institucijos padaryto teisės į privatumą ir duomenų apsaugą pažeidimo. NŽTK gali rekomenduoti taisyti ar tobulinti atitinkamą įstatymą, instituciją, politiką ar praktiką ⁽²⁹⁸⁾ arba įgyvendinti teisių gynimo priemones, kaip antai tarpininkavimą ⁽²⁹⁹⁾, žmogaus teisių pažeidimo nutraukimą, žalos atlyginimą ir priemones, kuriomis siekiama užkirsti kelią tokių pačių ar panašių pažeidimų pasikartojimui ⁽³⁰⁰⁾. Remiantis oficialiu Korėjos vyriausybės pareiškimu (II priedo 2.4.2 skirsnis), tai taip pat gali būti neteisėtai surinktų asmens duomenų ištrynimasis. Nors NŽTK neturi įgaliojimų priimti privalomai taikomų sprendimų, ji siūlo neoficialesnę, pigesnę ir lengvai prieinamą teisių gynimo priemonę, visų pirma dėl to, kad, kaip paaiškinta II priedo 2.4.2 skirsnyje, tam, kad skundas būtų tiriamas, nereikalaujama faktiškai įrodyti žalą ⁽³⁰¹⁾. Taip užtikrinama, kad asmenų skundai dėl jų duomenų rinkimo galėtų būti tiriami, net jei asmuo negali įrodyti, kad jo duomenys iš tikrųjų buvo surinkti (pvz., dėl to, kad asmeniui dar nepranešta). Iš NŽTK metinių veiklos ataskaitų matyti, kad asmenys taip pat naudojami šia galimybe praktikoje siekdami užginčyti baudžiamosios teisės saugos institucijų veiksmus, be kita ko, susijusius su asmens duomenų tvarkymu ⁽³⁰²⁾. Jei asmuo nepatenkintas NŽTK vykdomos procedūros rezultatais, jis gali

⁽²⁹¹⁾ Valstybės administracijos inspektavimo ir tyrimo įstatymo 16 straipsnio 2 dalis.

⁽²⁹²⁾ Valstybės administracijos inspektavimo ir tyrimo įstatymo 12-2 straipsnis.

⁽²⁹³⁾ Valstybės administracijos inspektavimo ir tyrimo įstatymo 16 straipsnio 3 dalis.

⁽²⁹⁴⁾ Šia teise gali būti naudojama tiesiogiai kompetentingos institucijos atžvilgiu arba netiesiogiai per AIAK (AIAI 35 straipsnio 2 dalis). Kaip išsamiau aprašyta (76)–(78) konstatuojamosiose dalyse, išimties dėl šių teisių bus taikomos tik tada, kai tai bus būtina svarbiems (viešiesiems) interesams apsaugoti.

⁽²⁹⁵⁾ AIAI 62 straipsnis.

⁽²⁹⁶⁾ AIAI 40–50 straipsniai ir AIAI vykdymo užtikrinimo dekretu 48–57 straipsniai. Taip pat žr. II priedo 2.4.1 skirsnį.

⁽²⁹⁷⁾ Kaip paaiškinta II priedo 2.4.2 skirsnyje, NŽTK įstatymo 4 straipsnyje nurodomi Korėjos Respublikoje gyvenantys piliečiai ir užsienio valstybių piliečiai, bet terminu „gyvenantys“ atspindima jurisdikcijos, o ne teritorijos sąvoka. Todėl, jei nacionalinės institucijos Korėjoje pažeidžia už Korėjos ribų esančio užsienio valstybės piliečio pagrindines teises, tas asmuo gali pateikti skundą NŽTK. Taip būtų tais atvejais, kai Korėjos valdžios institucijos neteisėtai susipažintų su į Korėją perduotais užsienio valstybės piliečio asmens duomenimis. Visų pirma žr. paaiškinimus, paskelbtus adresu <https://www.humanrights.go.kr/site/program/board/basicboard/list?boardtypeid=7025&menuid=002004005001&pagesize=10¤tpage=2>.

⁽²⁹⁸⁾ NŽTK įstatymo 44 straipsnis.

⁽²⁹⁹⁾ Asmuo taip pat gali prašyti skundą išspręsti tarpininkaujant (žr. NŽTK įstatymo 42 ir tolesnius straipsnius).

⁽³⁰⁰⁾ NŽTK įstatymo 42 straipsnio 4 dalis. Be to, NŽTK gali taikyti skubias paramos priemones, jei vykdomas pažeidimas, dėl kurio gali būti padaryta sunkiai atitaisoma žala nesilaikant priemonių (žr. NŽTK įstatymo 48 straipsnį).

⁽³⁰¹⁾ Skundas iš esmės turi būti pateiktas per vienus metus nuo pažeidimo įvykdymo, tačiau NŽTK gali nuspręsti nagrinėti skundą, pateiktą jau pasibaigus šiam terminui, jei dar nepasiektas senaties terminas pagal baudžiamąją arba civilinę teisę (NŽTK įstatymo 32 straipsnio 1 dalies 4 punktą).

⁽³⁰²⁾ Pavyzdžiui, NŽTK anksčiau nagrinėjo skundus ir pateikė rekomendacijas dėl neteisėto poėmio ir reikalavimo informuoti asmenis apie poėmį pažeidimo (žr. NŽTK 2018 m. metinės ataskaitos 80 ir 91 p.; ji paskelbta adresu <https://www.humanrights.go.kr/site/program/board/basicboard/view?menuid=002003003001&pagesize=10&boardtypeid=7017&boardid=7604746>), taip pat dėl neteisėto policijos, prokuratūros ir teismų atliekamo asmeninės informacijos tvarkymo (žr. NŽTK 2019 m. metinės ataskaitos 157–158 p.; ji paskelbta adresu <https://www.humanrights.go.kr/site/program/board/basicboard/view?menuid=002003003001&pagesize=10&boardtypeid=7017&boardid=7603308>, ir 2019 m. metinės ataskaitos 76 p.; ji paskelbta adresu <https://www.humanrights.go.kr/site/program/board/basicboard/view?menuid=002003003001&pagesize=10&boardtypeid=7017&boardid=7606217>).

apskusti NŽTK sprendimus (kaip antai sprendimą nebetęsti skundo nagrinėjimo⁽³⁰³⁾) ir rekomendacijas Korėjos teismuose pagal Administracinių ginčų įstatymą (žr. (181) konstatuojamąją dalį)⁽³⁰⁴⁾. Be to, taikant NŽTK procedūrą gali būti palengvintas kreipimasis į teismus, nes asmuo galėtų siekti tolesnių teisių gynimo veiksmų valdžios institucijos, kuri neteisėtai tvarkė jo duomenis, atžvilgiu remdamasis NŽTK išvadomis pagal (181)–(183) konstatuojamosiose dalyse aprašytas procedūras.

- (179) Galiausiai asmenys gali naudotis įvairiomis teisminėmis teisių gynimo priemonėmis, kad galėtų apginti savo teises pasinaudodami 3.2.1 skirsnyje aprašytais apribojimais ir apsaugos priemonėmis⁽³⁰⁵⁾.
- (180) Poėmio (įskaitant duomenų) atžvilgiu BPI numatyta galimybė nesutikti su orderio vykdymu arba užginčyti jo vykdymą pateikiant „kvaziskundą“, t. y. kreipiantis į kompetentingą teisimą su prašymu panaikinti arba pakeisti prokuroro ar policijos pareigūno sprendimą⁽³⁰⁶⁾.
- (181) Apskritai asmenys gali užginčyti valdžios institucijų (įskaitant baudžiamosios teisėsaugos institucijas) veiksmus⁽³⁰⁷⁾ ar neveikimą⁽³⁰⁸⁾ pagal Administracinių ginčų įstatymą⁽³⁰⁹⁾. Administracinis veiksmas laikomas „užginčijamu sprendimu“, jei juo daromas tiesioginis poveikis pilietinėms teisėms ir pareigoms⁽³¹⁰⁾, o taip yra, kaip patvirtino Korėjos vyriausybė (II priedo 2.4.3 skirsnis), taikant asmens duomenų rinkimo priemonės nepaisant to, ar duomenys būtų renkami tiesiogiai (pvz., perimant ryšius), pateikus privalomo atskleidimo prašymus (pavyzdžiui, paslaugų teikėjui) ar prašymus savanoriškai atskleisti informaciją. Kad skundas pagal Administracinių ginčų įstatymą būtų priimtinas, asmuo turi turėti teisinį interesą pareikšti reikalavimą⁽³¹¹⁾. Pagal Aukščiausiojo Teismo praktiką „teisinis interesas“ suprantamas kaip „teisiškai saugomas interesas“, t. y. tiesioginis ir konkretus interesas, saugomas įstatymais ir kitais teisės aktais, kuriais grindžiami administraciniai sprendimai (t. y. jais negali būti bendri, netiesioginiai ir abstraktūs visuomenės interesai)⁽³¹²⁾. Asmenys turi tokį teisinį interesą tuo atveju, kai pažeidžiami apribojimai ir apsaugos priemonės, taikomos jų asmens duomenų rinkimui baudžiamosios teisėsaugos tikslais (pagal specialius įstatymus arba AIAI). Teismas, remdamasis Administracinių ginčų įstatymu, gali nuspręsti panaikinti arba pakeisti neteisėtą sprendimą, paskelbti jį negaliojančiu (t. y. pateikti išvadą, kad sprendimas neturi teisinės galios arba kad jis neegzistuoja teisinėje sistemoje) arba paskelbti, kad neveikimas yra neteisėtas⁽³¹³⁾. Pagal Administracinių ginčų įstatymą šalis privalo įgyvendinti galutinį teismo sprendimą⁽³¹⁴⁾.

⁽³⁰³⁾ Pavyzdžiui, jei išimtinu atveju NŽTK negali tikrinti tam tikros medžiagos ar priemonių dėl to, kad jos susijusios su valstybės paslaptimis, galinčiomis turėti didelį poveikį valstybės saugumui ar diplomatiniais santykiams, arba jei tikrinant būtų sukurtos rimtos kliūtys baudžiamajam tyrimui ar būsimam teismo procesui ir jei tai trukdo NŽTK atlikti tyrimą, būtiną gautos peticijos pagrįstumui įvertinti, ji informuoja asmenį apie priežastis, dėl kurių skundas buvo atmestas pagal NŽTK įstatymo 39 straipsnį. Tokiu atveju asmuo galėtų užginčyti NŽTK sprendimą pagal Administracinių ginčų įstatymą.

⁽³⁰⁴⁾ Žr., pvz., 2008 m. balandžio 18 d. Seulo Aukštojo Teismo sprendimą 2007Nu27259, patvirtintą 2008 m. spalio 9 d. Aukščiausiojo Teismo sprendimu 2008Du7854; 2018 m. vasario 2 d. Seulo Aukštojo Teismo sprendimą 2017Nu69382.

⁽³⁰⁵⁾ Žr. II priedo 2.4.3 skirsnį.

⁽³⁰⁶⁾ BPI 417 straipsnis kartu su BPI 414 straipsnio 2 dalimi. Taip pat žr. 1997 m. rugsėjo 29 d. Aukščiausiojo Teismo sprendimą Nr. 97Mo66.

⁽³⁰⁷⁾ Administracinių ginčų įstatyme nurodomas „sprendimas“ reiškia viešosios valdžios vykdymą arba atsisakymą ją vykdyti konkrečiu atveju.

⁽³⁰⁸⁾ Pagal Administracinių ginčų įstatymą tai reiškia, kad administracinė agentūra ilgai nepriėmė tam tikro sprendimo, o tai prieštarauja teisei prievolei.

⁽³⁰⁹⁾ Administracinis skundas pirmiausia gali būti pateikiamas administracinėms apeliacinėms komisijoms, įsteigtoms tam tikrų valdžios institucijų (pvz., NŽT, NŽTK), arba Centrinei administracinei apeliacinei komisijai, įsteigtai Kovos su korupcija ir pilietinių teisių komisijoms (Administracinių skundų įstatymo 6 straipsnis ir Administracinių ginčų įstatymo 18 straipsnio 1 dalis), jei siekiama taikyti ne tokias oficialias teisių gynimo priemones. Tačiau reikalavimas taip pat gali būti pateikiamas tiesiogiai Korėjos teismuose Administracinių ginčų įstatymo pagrindu.

⁽³¹⁰⁾ 1999 m. spalio 22 d. Aukščiausiojo Teismo sprendimas 98Du18435, 2000 m. rugsėjo 8 d. Aukščiausiojo Teismo sprendimas 99Du1113 ir 2012 m. rugsėjo 27 d. Aukščiausiojo Teismo sprendimas 2010Du3541.

⁽³¹¹⁾ Administracinių ginčų įstatymo 12, 35 ir 36 straipsniai. Be to, prašymas panaikinti (pakeisti) sprendimą ir prašymas patvirtinti neveikimo neteisėtumą turi būti pateiktas per 90 dienų nuo tos dienos, kai asmuo sužinojo apie sprendimą arba neveikimą, ir iš esmės ne vėliau kaip per vienus metus nuo sprendimo paskelbimo arba neveikimo dienos, išskyrus atvejus, kai tam yra pagrįstų priežasčių (Administracinių ginčų įstatymo 20 straipsnis ir 38 straipsnio 2 dalis). „Pagrįstų priežasčių“ sąvoką Aukščiausiasis Teismas aiškino plačiai ir ją taikant reikalauja įvertinti, ar socialiai priimtina leisti pateikti skundą pavėluotai, atsižvelgiant į visas bylos aplinkybes (1991 m. birželio 28 d. Aukščiausiojo Teismo sprendimas 90Nu6521). Kaip patvirtino Korėjos vyriausybė II priedo 2.4.3 skirsnyje, tai apima vėlavimo priežastis (bet jomis neapsiriboja), už kurias susijusi šalis negali būti laikoma atsakinga (t. y. situacijas, kurių skundo pateikėjas negali kontroliuoti, pavyzdžiui, kai jam nebuvo pranešta apie jo asmeninės informacijos rinkimą), arba *force majeure* (pvz., stichinė nelaimė, karas).

⁽³¹²⁾ 2006 m. kovo 26 d. Aukščiausiojo Teismo sprendimas Nr. 2006Du330.

⁽³¹³⁾ Administracinių ginčų įstatymo 2 ir 4 straipsniai.

⁽³¹⁴⁾ Administracinių ginčų įstatymo 30 straipsnio 1 dalis.

- (182) Asmenys gali ne tik užginčyti vyriausybės veiksmus iškeldami administracinę bylą, bet ir pateikti konstitucinį skundą Konstituciniam Teismui dėl bet kokio jų pagrindinių teisių pažeidimo, susijusio su naudojimu vyriausybiniais įgaliojimais arba jų nevykdymu (išskyrus teismų sprendimus) ⁽³¹⁵⁾. Jei yra kitų teisių gynimo priemonių, pirmiausia turi būti pasinaudota jomis. Pagal Konstitucinio Teismo praktiką užsienio valstybių piliečiai gali pateikti konstitucinį skundą tais atvejais, kai jų pagrindinės teisės pripažįstamos pagal Korėjos Konstituciją (žr. 1.1 skirsnyje pateiktus paaiškinimus) ⁽³¹⁶⁾. Konstitucinis Teismas gali panaikinti vyriausybės įgaliojimų vykdymą, dėl kurio buvo padarytas pažeidimas, arba patvirtinti, kad tam tikras neveikimas prieštarauja Konstitucijai ⁽³¹⁷⁾. Tokiu atveju atitinkama institucija privalo imtis priemonių, kad būtų įvykdytas Teismo sprendimas.
- (183) Be to, asmenys gali reikalauti žalos atlyginimo Korėjos teismuose. Visų pirma tai apima galimybę reikalauti kompensacijos už AIAI pažeidimus, kuriuos padarė baudžiamosios teisėsaugos institucijos, pagal 39 straipsnį (taip pat žr. (135) konstatuojamąją dalį). Apskritai asmenys, remdamiesi Valstybės kompensacijų įstatymu, gali prašyti kompensacijos už žalą, kurią patyrė dėl to, kad valstybės pareigūnai vykdydami savo oficialias pareigas pažeidė įstatymą (taip pat žr. (135) konstatuojamąją dalį) ⁽³¹⁸⁾.
- (184) (176)–(183) konstatuojamosiose dalyse aprašytais mechanizmais duomenų subjektams suteikiamos veiksmingos administracinės ir teisminės teisių gynimo priemonės, kuriomis jiems sudaromos sąlygos visų pirma užtikrinti savo teises, įskaitant teisę susipažinti su savo asmens duomenimis arba ištaisyti ar ištrinti tokius duomenis.

3.3. Korėjos valdžios institucijų galimybė susipažinti su duomenimis ir jų naudojimas nacionalinio saugumo tikslais

- (185) Korėjos Respublikos teisėje nustatyti įvairūs galimybės susipažinti su asmens duomenimis ir juos naudoti nacionalinio saugumo tikslais apribojimai ir apsaugos priemonės, ir numatyti priežiūros ir teisių gynimo mechanizmai, kurie atitinka šio sprendimo (141)–(143) konstatuojamosiose dalyse nurodytus reikalavimus. Sąlygos, kuriomis tokia prieiga gali būti suteikta, ir tų įgaliojimų naudojimui taikomos apsaugos priemonės išsamiai įvertinamos kituose skirsniuose.

3.3.1. Teisiniai pagrindai, apribojimai ir apsaugos priemonės

- (186) Korėjos Respublikoje galimybė susipažinti su asmens duomenimis nacionalinio saugumo tikslais gali būti suteikiama RPAI, TIĮ ir Įstatymu dėl kovos su terorizmu siekiant apsaugoti piliečius ir užtikrinti viešąjį saugumą pagrindu (Kovos su terorizmu įstatymas) ⁽³¹⁹⁾. Pagrindinė institucija ⁽³²⁰⁾, turinti kompetencijos nacionalinio saugumo srityje, yra Nacionalinė žvalgybos tarnyba (NŽT) ⁽³²¹⁾. Rinkdama ir naudodama asmens duomenis

⁽³¹⁵⁾ Konstitucinio Teismo įstatymo 68 straipsnio 1 dalis. Konstituciniai skundai turi būti pateikti per 90 dienų nuo tos dienos, kai asmuo sužinojo apie pažeidimą, ir per vienus metus nuo tada, kai buvo įvykdytas pažeidimas. Kaip paaiškinta ir II priedo 2.4.3 skirsnyje, atsižvelgiant į tai, kad pagal Konstitucinio Teismo įstatymo 40 straipsnį ginčų nagrinėjimui pagal Konstitucinio Teismo įstatymą taikoma Administracinių ginčų įstatyme nustatyta procedūra, skundas vis tiek bus priimtinas, jei yra „pagrįstų priežasčių“, kaip aiškinama atsižvelgiant į 312 išnašoje aprašytą Aukščiausiojo Teismo praktiką. Jei pirmiausia reikia naudotis kitomis teisių gynimo priemonėmis, konstitucinis skundas turi būti pateiktas per 30 dienų nuo galutinio sprendimo dėl tokios teisių gynimo priemonės priėmimo (Konstitucinio Teismo įstatymo 69 straipsnis).

⁽³¹⁶⁾ 2001 m. lapkričio 29 d. Konstitucinio Teismo sprendimas Nr. 99HeonMa194.

⁽³¹⁷⁾ Konstitucinio Teismo įstatymo 75 straipsnio 3 dalis.

⁽³¹⁸⁾ Valstybės kompensacijų įstatymo 2 straipsnio 1 dalis.

⁽³¹⁹⁾ Žr. II priedo 3.1 skirsnį.

⁽³²⁰⁾ Išimtiniais atvejais policija ir prokuratūra taip pat gali rinkti asmeninę informaciją nacionalinio saugumo tikslais (žr. 327 išnašą ir II priedo 3.2.1.2 skirsnį). Be to, Korėjos karinės žvalgybos agentūra (Paramos saugumui gynybos vadavietė, įsteigta prie Gynybos ministerijos) turi įgaliojimų nacionalinio saugumo srityje. Tačiau, kaip paaiškinta II priedo 3.1 skirsnyje, ji yra atsakinga tik už karinę žvalgybą ir civilių gyventojų sekimą vykdo tik tais atvejais, kai tai būtina jos karinėms funkcijoms vykdyti. Visų pirma ji gali vykdyti tik karinio personalo, civilių kariuomenės darbuotojų, karinius mokymus atliekančių asmenų, asmenų kariniame rezerve arba samdomųjų karių ir karo belaisvių tyrimą (Karinio teismo įstatymo 1 straipsnis). Paramos saugumui gynybos vadavietei renkant ryšių informaciją nacionalinio saugumo tikslais jai taikomi RPAI ir jo vykdymo užtikrinimo dekretu nustatyti apribojimai ir apsaugos priemonės.

⁽³²¹⁾ NŽT įgaliota rinkti, rengti ir platinti informaciją apie užsienio šalis (t. y. bendrą informaciją apie tendencijas ir pokyčius, susijusius su užsienio šalimis, arba apie valstybinių subjektų veiklą), žvalgybos informaciją, susijusią su kovos su šnipinėjimu (įskaitant karinį ir pramoninį šnipinėjimą), terorizmu ir tarptautiniais nusikalstamais sindikatais veikla, žvalgybos informaciją apie tam tikrų rūšių nusikaltimus, nukreiptus prieš viešąjį ir nacionalinį saugumą (pvz., vidaus sukilimus, užsienio agresiją), ir žvalgybos informaciją, susijusią su kibernetinio saugumo užtikrinimo ir kibernetinių išpuolių ir grėsmių prevencijos arba kovos su jais užduotimis (NŽT įstatymo 4 straipsnio 2 dalis). Taip pat žr. II priedo 3.1 skirsnį.

NŽT turi laikytis atitinkamų teisinių reikalavimų (įskaitant AIAĮ ir RPAĮ) ⁽³²²⁾ ir bendrųjų gairių, parengtų Prezidento ir peržiūrėtų Nacionalinės Asamblėjos ⁽³²³⁾. Apskritai NŽT turi išlaikyti politinį neutralumą ir apsaugoti asmenų laisvę ir teises ⁽³²⁴⁾. Be to, NŽT darbuotojai negali piktnaudžiauti savo oficialiais įgaliojimais siekdami priversti bet kurią instituciją, organizaciją ar asmenį daryti tai, ko jie neprivalo daryti (pagal įstatymą), ir negali trukdyti jokiame asmeniui naudotis savo teisėmis ⁽³²⁵⁾.

3.3.1.1. Galimybė susipažinti su ryšių informacija

- (187) Remdamosi RPAĮ, Korėjos valdžios institucijos ⁽³²⁶⁾ gali rinkti ryšių patvirtinimo duomenis (t. y. telekomunikacinių ryšių datą, jų pradžios ir pabaigos laiką, atliktų ir gautų skambučių skaičių, taip pat kitos šalies abonento numerį, naudojimo dažnumą, telekomunikacijų paslaugų naudojimo žurnalo failus ir vietos nustatymo informaciją (žr. (155) konstatuojamąją dalį)) ir ryšių turinį (taikydamos ryšius ribojančias priemones (žr. (155) konstatuojamąją dalį)) nacionalinio saugumo tikslais (kaip nustatyta NŽT įgaliojimuose (žr. 322 išnašą)). Šie įgaliojimai taikytini dviejų rūšių informacijai: 1) ryšiams, kurių viena arba abi šalys yra Korėjos piliečiai ⁽³²⁷⁾, ir 2) ryšiams a) valstybių, kurios yra priešiškos nusiteikusios Korėjos Respublikos atžvilgiu, b) užsienio šalių agentūrų, grupių ar piliečių, įtariamų vykdant prieš Korėją nukreiptą veiklą ⁽³²⁸⁾ arba c) grupių, veikiančių Korėjos pusiasalyje, tačiau faktiškai esančių už Korėjos Respublikos suvereniteto ribų, ir joms priklausančių grupių, įsikūrusių užsienio šalyse, narių ⁽³²⁹⁾. Todėl pagal šį sprendimą iš Sąjungos į Korėjos Respubliką perduota ES asmenų ryšių informacija gali būti renkama nacionalinio saugumo tikslais tik pagal RPAĮ (laikantis (188)–(192) konstatuojamosiose dalyse nustatytų sąlygų), jei tai ES asmens ir Korėjos piliečio ryšių informacija arba, tuo atveju, kai ji susijusi tik su ne Korėjos piliečiais, ji priskiriama vienai iš trijų ryšių informacijos kategorijų, nurodytų 2 punkto a, b ir c papunkčiuose.
- (188) Abiem atvejais ryšių patvirtinimo duomenys gali būti renkami tik siekiant užkirsti kelią nacionaliniam saugumui kylančioms grėsmėms ⁽³³⁰⁾, o ryšius ribojančios priemonės gali būti taikomos tik tada, kai kyla didelis pavojus nacionaliniam saugumui ir duomenų rinkimas yra būtinas jam išvengti ⁽³³¹⁾. Be to, prieiga prie ryšių turinio gali būti suteikiama tik kraštutiniu atveju ir turi būti dedamos pastangos kuo labiau vengti ryšių privatumo pažeidimo ⁽³³²⁾, taip užtikrinant, kad jis išliktų proporcingas siekiamam nacionalinio saugumo tikslui. Ryšių turinio ir ryšių patvirtinimo duomenų rinkimas gali trukti ne ilgiau kaip keturis mėnesius ir turi būti nedelsiant nutrauktas, jei siekiamas tikslas pasiekiamas anksčiau ⁽³³³⁾. Jei atitinkamos sąlygos ir toliau tenkinamos, laikotarpis gali būti pratęstas iki keturių mėnesių gavus išankstinį teismo (dėl (189) konstatuojamojoje dalyje aprašytų priemonių) arba Prezidento (dėl (190) konstatuojamojoje dalyje aprašytų priemonių) leidimą ⁽³³⁴⁾.
- (189) Tos pačios procedūrinės apsaugos priemonės taikomos ryšių patvirtinimo duomenų ir ryšių turinio rinkimui ⁽³³⁵⁾. Visų pirma, kai bent viena iš ryšių šalių yra Korėjos pilietis, žvalgybos agentūra turi pateikti rašytinį prašymą Vyriausiajai prokuratūrai, o pastaroji atitinkamai turi prašyti Aukštojo Teismo vyriausiąjį teisėją išduoti

⁽³²²⁾ Taip pat žr. NŽT įstatymo 14, 22 ir 23 straipsnius.

⁽³²³⁾ NŽT įstatymo 4 straipsnio 2 dalis.

⁽³²⁴⁾ NŽT įstatymo 3 straipsnio 1 dalis, 6 straipsnio 2 dalis, 11 ir 21 straipsniai. Taip pat žr. taisyklės dėl interesų konfliktų, visų pirma NŽT įstatymo 10 ir 12 straipsnius.

⁽³²⁵⁾ NŽT įstatymo 13 straipsnis.

⁽³²⁶⁾ Tai apima žvalgybos agentūras (t. y. NŽT ir Paramos saugumui gynybos vadavietė) ir policiją bei prokuratūrą.

⁽³²⁷⁾ RPAĮ 7 straipsnio 1 dalies 1 punktą.

⁽³²⁸⁾ Kaip Korėjos vyriausybė paaiškino II priedo 244 išnašoje, tai reiškia veiklą, kuri kelia grėsmę tautos egzistavimui ir saugumui, demokratinei tvarkai arba žmonių išlikimui ir laisvei.

⁽³²⁹⁾ RPAĮ 7 straipsnio 1 dalies 2 punktą.

⁽³³⁰⁾ RPAĮ 13-4 straipsnis.

⁽³³¹⁾ RPAĮ 7 straipsnio 1 dalis.

⁽³³²⁾ RPAĮ 3 straipsnio 2 dalis. Be to, ryšius ribojančios priemonės turi būti nedelsiant nutrauktos, kai jos tampa nebereikalingos, taip užtikrinant, kad bet koks asmens ryšių slaptumo pažeidimas būtų kuo mažesnis (RPAĮ vykdymo užtikrinimo dekreto 2 straipsnis).

⁽³³³⁾ RPAĮ 7 straipsnio 2 dalis.

⁽³³⁴⁾ Prašymas pratęsti sekimo priemonių taikymą turi būti pateiktas raštu, nurodant priežastis, dėl kurių prašoma jį pratęsti, ir pateikiant patvirtinančios medžiagos (RPAĮ 7 straipsnio 2 dalis ir RPAĮ vykdymo užtikrinimo dekreto 5 straipsnis).

⁽³³⁵⁾ Žr. RPAĮ 13-4 straipsnio 2 dalį ir RPAĮ vykdymo užtikrinimo dekreto 37 straipsnio 4 dalį, pagal kurias ryšių turinio rinkimui taikomos procedūros taip pat taikomos ryšių patvirtinimo duomenų rinkimui. Taip pat žr. II priedo 3.2.1.1.1 skirsnį.

orderį⁽³³⁶⁾. RPAĮ išvardijama informacija, kuri turi būti pateikta prašyme prokurorui, prašyme išduoti orderį ir pačiame orderyje, kuriame visų pirma pateikiamas prašymo pagrindimas ir pagrindinės įtarimo priežastys, patvirtinanti medžiaga, taip pat informacija apie tikslą, taikymo sritį (t. y. asmenį arba asmenis, kuriems jis bus taikomas), siūlomos priemonės taikymo mastą ir trukmę⁽³³⁷⁾. Rinkti duomenis neturint orderio galima tik tuo atveju, jei vykdomas sąmokslas, kuriuo keliama grėsmė nacionaliniam saugumui, ir dėl ekstremaliosios situacijos neįmanoma atlikti minėtų procedūrų⁽³³⁸⁾. Tačiau ir tokiu atveju prašymas išduoti orderį turi būti pateiktas iš karto po to, kai buvo imtasi priemonės⁽³³⁹⁾. Todėl RPAĮ aiškiai apibrėžtas tokio duomenų rinkimo mastas ir sąlygos ir jo vykdymo atžvilgiu nustatytos konkrečios (procedūrinės) apsaugos priemonės (įskaitant išankstinį teismo leidimą), kuriomis užtikrinama, kad tokios priemonės būtų naudojamos tik tiek, kiek būtina ir kol laikomasi proporcingumo principo. Be to, reikalaujant pateikti išsamią informaciją ir prašyme išduoti orderį, ir pačiame orderyje pašalinama galimybė beatodairiškai susipažinti su duomenimis.

- (190) Ryšių tarp ne Korėjos piliečių, patenkančių į vieną iš trijų konkrečių kategorijų, išvardytų (187) konstatuojamojoje dalyje, atveju prašymas turi būti pateiktas NŽT direktoriui, o pastarasis, peržiūrėjęs siūlomų priemonių tinkamumą, turi prašyti Korėjos Respublikos Prezidento išankstinio raštiško patvirtinimo⁽³⁴⁰⁾. Žvalgybos agentūros parengtame prašyme turi būti pateikta tokia pati išsami informacija kaip ir prašyme išduoti teismo orderį (žr. (189) konstatuojamąją dalį), visų pirma informacija apie prašymo pagrindimą ir pagrindines įtarimo priežastis, patvirtinanti medžiaga ir informacija apie tikslus, asmenį arba asmenis, kuriems bus taikomos priemonės, siūlomų priemonių taikymo mastą ir trukmę⁽³⁴¹⁾. Ekstremaliųjų situacijų atveju⁽³⁴²⁾ turi būti gautas išankstinis ministro, kurio įgaliojimų sričiai priklauso atitinkama žvalgybos agentūra, patvirtinimas, bet iš karto po to, kai buvo imtasi neatidėliotinių priemonių, žvalgybos agentūra turi kreiptis dėl Prezidento patvirtinimo⁽³⁴³⁾. Be to, ryšių tik tarp ne Korėjos piliečių informacijos rinkimo atžvilgiu RPAĮ nustatytas apribojimas taikyti tokias priemones tik tiek, kiek būtina, ir tol, kol jos atitinka proporcingumo principą, aiškiai apibrėžiant ribotas asmenų, kuriems gali būti taikomos tokios priemonės, kategorijas ir nustatant išsamius kriterijus, kurie turi būti įvykdyti, kad žvalgybos tarnybos galėtų pateisinti prašymą rinkti informaciją. Be to, taip vėlgi atmetama galimybė beatodairiškai susipažinti su duomenimis. Nors išankstinis nepriklausomas tokių priemonių patvirtinimas netaikomas, nepriklausomą *ex post* priežiūrą užtikrina visų pirma AIAK ir NŽTK (žr., pavyzdžiui, (199)–(200) konstatuojamąsias dalis).
- (191) Be to, RPAĮ nustatomos kelios papildomos apsaugos priemonės, kuriomis prisidedama prie *ex post* priežiūros ir sudaromos palankesnės sąlygos asmenims pasinaudoti veiksmingomis teisių gynimo priemonėmis. Pirma, visų rūšių duomenų rinkimo nacionalinio saugumo tikslais atžvilgiu RPAĮ numatyti skirtingi duomenų saugojimo ir ataskaitų teikimo reikalavimai. Visų pirma prašydamos privačių paslaugų teikėjų bendradarbiauti žvalgybos tarnybos turi pateikti teismo orderį, Prezidento leidimą arba neišvengiamos cenzūros pareiškimo titulinio puslapio kopiją, kurią prašomas subjektas turi saugoti⁽³⁴⁴⁾. Kai privačių veiklos vykdytojų bendradarbiavimas yra būtinas,

⁽³³⁶⁾ RPAĮ 6 straipsnio 5 ir 8 dalys, 7 straipsnio 1 dalies 1 punktą ir 3 dalis kartu su RPAĮ vykdymo užtikrinimo dekretu 7 straipsnio 3 ir 4 dalimis.

⁽³³⁷⁾ Žr. RPAĮ 7 straipsnio 3 dalį ir 6 straipsnio 4 dalį (dėl žvalgybos agentūros prašymo), RPAĮ vykdymo užtikrinimo dekretu 4 straipsnį (dėl prokuroro prašymo) ir RPAĮ 7 straipsnio 3 dalį ir 6 straipsnio 6 dalį (dėl orderio).

⁽³³⁸⁾ RPAĮ 8 straipsnis.

⁽³³⁹⁾ RPAĮ 8 straipsnio 2 ir 8 dalys. Jei teismo leidimas negaunamas per 36 valandas nuo priemonių taikymo pradžios, duomenų rinkimas turi būti nedelsiant nutrauktas. Tais atvejais, kai stebėjimas užbaigiamas per trumpą laiką nespėjus gauti teismo leidimo, kompetentingos Vyriausiosios prokuratūros vadovas turi nusiųsti žvalgybos agentūros parengtą pranešimą dėl neatidėliotinos priemonės kompetentingo teismo vadovui, kuris šiuo pagrindu gali išnagrinėti duomenų rinkimo teisėtumą (RPAĮ 8 straipsnio 5 ir 7 dalys). Šiame pranešime turi būti nurodytas stebėjimo tikslas, sritis, mastas, laikotarpis, vykdymo vieta ir stebėjimo būdas, taip pat priežastis, dėl kurios prašymas nebuvo pateiktas prieš imantis priemonės (RPAĮ 8 straipsnio 6 dalis). Apskritai žvalgybos agentūros gali imtis neatidėliotinių priemonių tik remdamosi „neatidėliotinos cenzūros ir (arba) slapto pokalbių klausymosi pareiškimu“ ir privalo saugoti įrašus apie tokių priemonių taikymą (RPAĮ 8 straipsnio 4 dalis).

⁽³⁴⁰⁾ RPAĮ vykdymo užtikrinimo dekretu 8 straipsnio 1 ir 2 dalys.

⁽³⁴¹⁾ RPAĮ vykdymo užtikrinimo dekretu 8 straipsnio 3 dalis kartu su RPAĮ 6 straipsnio 4 dalimi.

⁽³⁴²⁾ Tai tokie atvejai, kai priemone siekiama užkirsti kelią sąmokslui, dėl kurio kyla grėsmė nacionaliniam saugumui, nėra laiko gauti Prezidento pritarimą, o neįgyvendinus neatidėliotinių priemonių gali būti pakenkta nacionaliniam saugumui (RPAĮ 8 straipsnio 8 dalis).

⁽³⁴³⁾ RPAĮ 8 straipsnio 9 dalis. Jei leidimas negaunamas per 36 valandas nuo prašymo pateikimo, duomenų rinkimas turi būti nedelsiant nutrauktas.

⁽³⁴⁴⁾ RPAĮ 9 straipsnio 2 dalis ir RPAĮ vykdymo užtikrinimo dekretu 12 straipsnis. Žr. RPAĮ vykdymo užtikrinimo dekretu 13 straipsnį dėl galimybės prašyti pašto įstaigų ir telekomunikacijų paslaugų teikėjų pagalbos. Privatūs veiklos vykdytojai, kurių prašoma atskleisti informaciją, gali atsakyti tai padaryti, kai orderio (leidimo) arba neišvengiamos cenzūros pareiškime nurodomas neteisingas identifikatorius (pvz., telefono numeris, priklausantis kitam asmeniui nei nurodytasis). Bet kuriuo atveju jiems draudžiama atskleisti slaptą žodžius, naudojamus naudojantis telekomunikacijų paslaugomis (RPAĮ 9 straipsnio 4 dalis).

prašančioji valdžios institucija ir atitinkamas veiklos vykdytojas turi saugoti įrašus apie priemonių tikslą ir objektą, taip pat jų įgyvendinimo datą⁽³⁴⁵⁾. Be to, žvalgybos agentūros turi pranešti NŽT direktoriui apie surinktą informaciją ir stebėjimo veiklos rezultatus⁽³⁴⁶⁾.

- (192) Antra, asmenims turi būti pranešta apie jų duomenų (ryšių patvirtinimo duomenų arba ryšių turinio) rinkimą nacionalinio saugumo tikslais, jei jie susiję su ryšiais, kuriuose bent viena iš šalių yra Korėjos pilietis⁽³⁴⁷⁾. Apie tai turi būti pranešta raštu per 30 dienų nuo duomenų rinkimo pabaigos (įskaitant atvejus, kai duomenys buvo gauti taikant ekstremaliosios situacijos tvarką), o pranešimas gali būti atidėtas tik tuo atveju, jei pranešus kiltų pavojus nacionaliniam saugumui arba žmonių gyvybėms ir fiziniam saugumui, ir tik tol, kol toks pavojus kiltų⁽³⁴⁸⁾. Nepriklausomai nuo to, ar buvo pranešta, asmenys gali naudotis skirtingais teisių gynimo būdais, kaip išsamiau paaiškinta 3.3.4 skirsnyje.

3.3.1.2. Informacijos apie asmenis, įtariamus teroristine veikla, rinkimas

- (193) Kovos su terorizmu įstatyme nustatyta, kad NŽT gali rinkti duomenis apie teroristine veikla įtariamus asmenis⁽³⁴⁹⁾, laikydami kituose įstatymuose nustatytų apribojimų ir apsaugos priemonių⁽³⁵⁰⁾. Visų pirma NŽT gali gauti ryšių duomenis (RPAĮ pagrindu) ir kitą asmeninę informaciją (pateikdama prašymą savanoriškai atskleisti informaciją)⁽³⁵¹⁾. Ryšių informacijos rinkimui (t. y. ryšių turinio arba ryšių patvirtinimo duomenų rinkimui) taikomi 3.3.1.1 skirsnyje aprašyti apribojimai ir apsaugos priemonės, įskaitant reikalavimą gauti teismo patvirtintą orderį. NŽT teikiamais prašymais savanoriškai atskleisti kitų rūšių asmens duomenis apie teroristine veikla įtariamus asmenis turi būti laikomasi Konstitucijoje ir AIAĮ nustatytų būtinumo ir proporcingumo reikalavimų (žr. (164) konstatuojamąją dalį)⁽³⁵²⁾. Tokius prašymus gaunantys duomenų valdytojai gali savanoriškai juos vykdyti AIAĮ nustatytais sąlygomis (pvz., laikydamiesi duomenų kiekio mažinimo principo ir ribodami poveikį asmens privatumui)⁽³⁵³⁾. Šiuo atveju jos taip pat turi laikytis reikalavimo pranešti atitinkamam asmeniui pagal pranešimą Nr. 2021-5 (žr. (166) konstatuojamąją dalį).

⁽³⁴⁵⁾ Ryšius ribojančių priemonių taikymo atveju tokie įrašai turi būti saugomi trejus metus (žr. RPAĮ 9 straipsnio 3 dalį ir RPAĮ vykdymo užtikrinimo dekreto 17 straipsnio 2 dalį). Ryšių patvirtinimo duomenų rinkimo atveju žvalgybos agentūros turi saugoti įrašus apie tai, kad buvo pateiktas prašymas pateikti tokius duomenis, taip pat patį rašytinį prašymą ir įrašą apie instituciją, kuri jį pateikė (RPAĮ 13 straipsnio 5 dalis ir 13-4 straipsnio 3 dalis). Telekomunikacijų paslaugų teikėjai turi saugoti įrašus septynerius metus ir du kartus per metus pranešti Mokslo ir IRT ministrui apie tokios informacijos atskleidimo dažnumą (RPAĮ 9 straipsnio 3 dalis kartu su RPAĮ 13 straipsnio 7 dalimi ir RPAĮ vykdymo užtikrinimo dekreto 37 straipsnio 4 dalimi ir 39 straipsniu).

⁽³⁴⁶⁾ RPAĮ vykdymo užtikrinimo dekreto 18 straipsnio 3 dalis.

⁽³⁴⁷⁾ RPAĮ 9-2 straipsnio 3 dalis ir 13-4 straipsnis. Pranešime turi būti nurodyta: 1) tai, kad informacija buvo surinkta, 2) vykdančioji agentūra ir 3) vykdymo laikotarpis.

⁽³⁴⁸⁾ RPAĮ 9-2 straipsnio 4 dalis. Tokiu atveju pranešimas turi būti pateiktas per 30 dienų nuo tada, kai išnyksta atidėjimo pagrindai (žr. RPAĮ 13-4 straipsnio 2 dalį ir 9-2 straipsnio 6 dalį).

⁽³⁴⁹⁾ Tai teroristinės grupės nariai (kaip juos apibrėžia Jungtinės Tautos, žr. Kovos su terorizmu įstatymo 2 straipsnio 2 dalį), asmenys, kurie propaguoja ir platina teroristinės grupės idėjas ar taktiką, renka teroristinei veiklai skirtas lėšas arba prisideda prie jų rinkimo arba dalyvauja kitoje veikloje, susijusioje su teroristinės veiklos planavimu, sąmokslu ją vykdyti, jos propaganda ar kurtymu, arba asmenys, kurių atžvilgiu yra pagrįstų priežasčių įtarti, kad jie tokią veiklą vykdė (Kovos su terorizmu įstatymo 2 straipsnio 3 dalis). Kovos su terorizmu įstatymo 2 straipsnio 1 dalyje terminas „terorizmas“ apibrėžiamas kaip elgesys, kuriuo siekiama trukdyti valstybei, vietos valdžios institucijai ar užsienio vyriausybei (įskaitant tarptautines organizacijas) vykdyti savo įgaliojimus arba priversti jas imtis veiksmų neturint jokios teisinės prievolės, arba kelti grėsmę visuomenei. Toks elgesys gali būti, pavyzdžiui, žudymas, pagrobimas ar asmens laikymas įkaitu, laivo ar orlaivio užgrobimas (paėmimas), sunaikinimas ar sugadinimas, biocheminių, sprogstamųjų ar padegamųjų ginklų naudojimas siekiant mirties, sunkaus sužalojimo ar žalos ir branduolinių ar radioaktyviųjų medžiagų naudojimas piktavališkais tikslais.

⁽³⁵⁰⁾ Kovos su terorizmu įstatymo 9 straipsnio 1 ir 3 dalys.

⁽³⁵¹⁾ Nors Kovos su terorizmu įstatyme taip pat nurodoma galimybė rinkti informaciją apie atvykimą į Korėjos Respubliką ir išvykimą iš jos remiantis Imigracijos įstatymu ir Muitų įstatymu, tuose įstatymuose toks įgaliojimas šiuo metu nenumatytas (žr. II priedo 3.2.2.1 skirsnį). Bet kuriuo atveju šie įgaliojimai iš esmės nebūtų taikomi duomenims, perduotiems remiantis šiuo sprendimu, nes jie paprastai būtų susiję su informacija, kurią Korėjos valdžios institucijos rinktų tiesiogiai (o ne naudodamosi prieiga prie duomenų, kurie iš Sąjungos anksčiau buvo perduoti Korėjos duomenų valdytojams). Be to, Kovos su terorizmu įstatyme ĮKFSITN nurodytas kaip teisinis pagrindas informacijai apie finansinius sandorius rinkti. Tačiau, kaip paaiškinta 200 išnašoje, duomenų, kuriuos galima gauti šio įstatymo pagrindu, rūšys nepatenka į šio sprendimo taikymo sritį. Galiausiai Kovos su terorizmu įstatyme taip pat nustatyta, kad NŽT gali rinkti buvimo vietos nustatymo informaciją teikdama neįpareigojančius prašymus; tokiu atveju buvimo vietos informacijos teikėjai galėtų savanoriškai atskleisti tokią informaciją laikydamiesi AIAĮ (kaip aprašyta (193) konstatuojamojoje dalyje) ir Informacijos apie buvimo vietą įstatyme nustatytų sąlygų. Tačiau, kaip paaiškinta 17 išnašoje, buvimo vietos nustatymo informacija nebūtų perduodama iš Sąjungos Korėjos duomenų valdytojams remiantis šiuo sprendimu, bet būtų renkama Korėjoje.

⁽³⁵²⁾ Žr. II priedo 3.2.2.2 skirsnį.

⁽³⁵³⁾ Žr. AIAĮ 58 straipsnio 4 dalį, pagal kurią reikalaujama, kad asmeninė informacija būtų tvarkoma tik tiek, kiek būtina numatytam tikslui pasiekti, ir AIAĮ 3 straipsnio 6 dalį, kurioje numatyta, kad asmeninė informacija turi būti tvarkoma taip, kad būtų kuo labiau sumažinta galimybė pažeisti asmens privatumą. Taip pat žr. AIAĮ 59 straipsnio 2 ir 3 dalis, pagal kurias duomenų valdytojams draudžiama atskleisti asmeninę informaciją trečiosioms šalims, neturinčioms įgaliojimų ją gauti.

3.3.1.3. Prašymai savanoriškai atskleisti abonentų duomenis

- (194) Remdamiesi TII, telekomunikacijų paslaugų teikėjai gali savanoriškai atskleisti abonento duomenis (žr. (163) konstatuojamąją dalį) žvalgybos agentūros, kuri ketina rinkti tokią informaciją, prašymu, kad užkirstų kelią nacionaliniam saugumui kylančiam pavojui ⁽³⁵⁴⁾. Tokiems NŽT prašymams taikomi tie patys apribojimai (pagal Konstituciją, AIAĮ ir TII) kaip ir baudžiamosios teisės saugos atveju, kaip nurodyta (164) konstatuojamojoje dalyje ⁽³⁵⁵⁾. Telekomunikacijų paslaugų teikėjai prašymų vykdyti neprivalo, o juos vykdyti gali tik AIAĮ nustatytomis sąlygomis (visų pirma laikydamiesi duomenų kiekio mažinimo principo ir ribodami poveikį asmens privatumui (taip pat žr. (193) konstatuojamąją dalį)). Taikomi tie patys įrašų saugojimo ir pranešimo atitinkamam asmeniui reikalavimai, kaip ir baudžiamosios teisės saugos atveju (žr. (165) ir (166) konstatuojamąsias dalis).

3.3.2. Tolesnis surinktos informacijos naudojimas

- (195) Asmens duomenų, kuriuos Korėjos valdžios institucijos renka nacionalinio saugumo tikslais, tvarkymui taikomi tikslo apribojimo (AIAĮ 3 straipsnio 1 ir 2 dalys), duomenų tvarkymo teisėtumo ir sąžiningumo (AIAĮ 3 straipsnio 1 dalis), proporcingumo ir duomenų kiekio mažinimo (AIAĮ 3 straipsnio 1 ir 6 dalys ir 58 straipsnis), tikslumo (AIAĮ 3 straipsnio 3 dalis), skaidrumo (AIAĮ 3 straipsnio 5 dalis), saugumo (AIAĮ 58 straipsnio 4 dalis) ir saugojimo apribojimo (AIAĮ 58 straipsnio 4 dalis) principai ⁽³⁵⁶⁾. Asmens duomenys trečiosioms šalims (įskaitant trečiąsias valstybes) gali būti atskleidžiami tik laikantis šių principų (visų pirma tikslo apribojimo ir duomenų kiekio mažinimo), įvertinus, ar laikomasi būtinumo ir proporcingumo principų (Konstitucijos 37 straipsnio 2 dalis) ir atsižvelgiant į poveikį atitinkamų asmenų teisėms (AIAĮ 3 straipsnio 6 dalis).
- (196) Ryšių turinio ir ryšių patvirtinimo duomenų atžvilgiu RPAĮ taip pat nustatyti apribojimai, tokius duomenis leidžiant naudoti teismo procesuose, kai su ryšiais susijusi šalis jais remiasi teikdama reikalavimą dėl žalos atlyginimo, arba pagal kitus įstatymus numatytoms paskirtims ⁽³⁵⁷⁾.

3.3.3. Priežiūra

- (197) Korėjos nacionalinio saugumo institucijų veiklą prižiūri įvairios įstaigos ⁽³⁵⁸⁾.
- (198) Pirma, Kovos su terorizmu įstatyme numatyti specialūs kovos su terorizmu veiklos priežiūros mechanizmai, įskaitant duomenų apie teroristine veikla įtariamus asmenis rinkimą. Visų pirma vykdomosios valdžios lygmeniu kovos su terorizmu veiklą prižiūri Kovos su terorizmu komisija ⁽³⁵⁹⁾, kuriai NŽT direktorius turi pranešti apie tyrimus ir teroristine veikla įtariamų asmenų sekimą siekiant surinkti kovos su terorizmu veiklai reikalingą informaciją ar medžiagą ⁽³⁶⁰⁾. Be to, žmogaus teisių apsaugos pareigūnas (ŽTAP) konkrečiai prižiūri, kad vykdytą kovos su terorizmu veiklą nebūtų pažeistos pagrindinės teisės ⁽³⁶¹⁾. Kovos su terorizmu komisijos pirmininkas ŽTAP skiria iš asmenų, kurie turi konkrečias kvalifikacijas, išvardytas Kovos su terorizmu įstatymo vykdymo užtikrinimo dekretu ⁽³⁶²⁾, dvejų metų kadencijai (kuria galima pratęsti), o atleistas iš pareigų jis gali būti tik dėl konkrečių, ribotų priežasčių ir rimtu pagrindu ⁽³⁶³⁾. Vykdydamas priežiūros funkciją ŽTAP gali teikti bendras

⁽³⁵⁴⁾ TII 83 straipsnio 3 dalis.

⁽³⁵⁵⁾ Taip pat žr. II priedo 3.2.3 skirsnį.

⁽³⁵⁶⁾ Žr. II priedo 1.2 skirsnį.

⁽³⁵⁷⁾ RPAĮ 5 straipsnio 1 ir 2 dalys, 12 ir 13-5 straipsniai.

⁽³⁵⁸⁾ Žr. II priedo 3.3 skirsnį.

⁽³⁵⁹⁾ Kovos su terorizmu įstatymo 5 straipsnio 3 dalis. Komisijai pirmininkauja Ministras Pirmininkas, o ją sudaro keli ministrai ir vyriausybinių agentūrų vadovai, pavyzdžiui, Užsienio reikalų, Teisingumo, Nacionalinės gynybos, Vidaus reikalų ir saugumo ministrai, NŽT direktorius ir Nacionalinės policijos agentūros generalinis komisaras (Kovos su terorizmu įstatymo vykdymo užtikrinimo dekretu 3 straipsnio 1 dalis).

⁽³⁶⁰⁾ Kovos su terorizmu įstatymo 9 straipsnio 4 dalis.

⁽³⁶¹⁾ Kovos su terorizmu įstatymo 7 straipsnis.

⁽³⁶²⁾ Tai asmenys, turintys bent dešimties metų advokato darbo patirtį arba turintys profesinių žinių žmogaus teisių apsaugos srityje ir bent dešimt metų (mažiausiai) eję docento pareigas, arba asmenys, eję vyresniojo valstybės pareigūno pareigas valstybės institucijose ar vietos valdžios institucijose, arba asmenys, turintys bent dešimties metų darbo patirtį žmogaus teisių apsaugos srityje, pvz., nevyriausybinėje organizacijoje (Kovos su terorizmu įstatymo vykdymo užtikrinimo dekretu 7 straipsnio 1 dalis).

⁽³⁶³⁾ Pavyzdžiui, kai jam pareikšti kaltinimai baudžiamojoje byloje, susijusioje su jo pareigomis, kai jis atskleidžia konfidencialią informaciją arba dėl ilgalaikės psichinės ar fizinės negalios (Kovos su terorizmu įstatymo vykdymo užtikrinimo dekretu 7 straipsnio 3 dalis).

rekomendacijas dėl žmogaus teisių apsaugos gerinimo ⁽³⁶⁴⁾ ir konkrečias rekomendacijas dėl taisomųjų veiksmų taikymo, jei nustatomas žmogaus teisių pažeidimas ⁽³⁶⁵⁾. Valdžios institucijos privalo informuoti ŽTAP apie veiksmus, kurių imtasi atsižvelgiant į jo rekomendacijas ⁽³⁶⁶⁾.

- (199) Antra, AIAK prižiūri, kaip nacionalinės saugumo institucijos laikosi duomenų apsaugos taisyklių, kurias sudaro ir taikomos AIAI nuostatos (žr. (149) konstatuojamąją dalį), ir apribojimai ir apsaugos priemonės, taikomi asmens duomenų rinkimui pagal kitus teisės aktus (RPAI, Kovos su terorizmu įstatymą ir TII, taip pat žr. (171) konstatuojamąją dalį) ⁽³⁶⁷⁾. Vykdydama šį priežiūros vaidmenį AIAK gali naudotis visais savo tyrimų atlikimo ir taisomųjų veiksmų taikymo įgaliojimais, kaip išsamiai aprašyta 2.4.2 skirsnyje.
- (200) Trečia, nacionalinių saugumo institucijų veiklai taikoma nepriklausoma NŽTK priežiūra remiantis (172) konstatuojamojoje dalyje aprašytomis procedūromis ⁽³⁶⁸⁾.
- (201) Ketvirta, AIV priežiūros funkcija taip pat apima nacionalines saugumo institucijas, nors išimtinėmis aplinkybėmis NŽT gali atsisakyti suteikti tam tikrą informaciją ar medžiagą, t. y. kai ji susijusi su valstybės paslaptimis ir jų atskleidimas turėtų didelį poveikį nacionaliniam saugumui ⁽³⁶⁹⁾.
- (202) Galiausiai parlamentinę NŽT veiklos priežiūrą vykdo Nacionalinė Asamblėja (per specializuotą žvalgybos komitetą) ⁽³⁷⁰⁾. RPAI nustatomas specialus Nacionalinės Asamblėjos priežiūros vaidmuo, susijęs su ryšius ribojančių priemonių taikymu nacionalinio saugumo tikslais ⁽³⁷¹⁾. Visų pirma Nacionalinė Asamblėja gali atlikti slapto pokalbių klausymosi įrangos patikrinimus vietoje ir reikalauti, kad ir NŽT, ir telekomunikacijų paslaugų teikėjai, kurie atskleidė ryšių turinį, apie tai praneštų. Nacionalinė Asamblėja taip pat gali vykdyti savo bendrąsias priežiūros funkcijas (remdamasi (174) konstatuojamojoje dalyje aprašytomis procedūromis). NŽT įstatyme reikalaujama, kad Žvalgybos komitetui paprašius pateikti ataskaitą konkrečiu klausimu NŽT direktorius nedelsdamas vykdytų prašymą ⁽³⁷²⁾, taikydamas konkrečias taisykles dėl tam tikros neskelbtinos informacijos. Atsisakyti vykdyti prašymą arba duoti parodymus komitete NŽT direktorius gali tik išskirtinėmis aplinkybėmis, t. y. jei prašymas susijęs su valstybės paslaptimis, susijusiomis su kariniais, diplomatiniais ar Šiaurės Korėjos klausimais, kai jų atskleidimas gali turėti didelį poveikį šalies „nacionaliniam likimui“ ⁽³⁷³⁾. Tokiu atveju Žvalgybos komitetas gali prašyti Ministro Pirmininko pateikti paaiškinimą ir, jei paaiškinimas nepateikiamas per septynias dienas, atsisakyti vykdyti prašymą arba duoti parodymus negalima.

3.3.4. Teisių gynimas

- (203) Nacionalinio saugumo atžvilgiu Korėjos sistemoje taip pat siūlomi skirtingi (teisminiai) teisių gynimo būdai, įskaitant žalos atlyginimą. Šiais mechanizmais duomenų subjektams suteikiamos veiksmingos administracinės ir teisminės teisių gynimo priemonės, kuriomis jiems sudaromos sąlygos visų pirma užtikrinti savo teises, įskaitant teisę susipažinti su savo asmens duomenimis arba ištaisyti ar ištrinti tokius duomenis.
- (204) Pirma, pagal AIAI 3 straipsnio 5 dalį ir 4 straipsnio 1, 3 ir 4 dalis asmenys gali naudotis savo susipažinimo su informacija, jos ištaisymo, ištrynimo ir rinkimo sustabdymo teisėmis nacionalinių saugumo institucijų atžvilgiu. Pranešimo Nr. 2021-5 6 skirsnyje (šio sprendimo I priedas) išsamiau paaiškinama, kaip šios teisės taikomos, kai duomenys tvarkomi nacionalinio saugumo tikslais. Visų pirma nacionalinė saugumo institucija gali apriboti šią

⁽³⁶⁴⁾ Kovos su terorizmu įstatymo vykdymo užtikrinimo dekreto 8 straipsnio 1 dalis.

⁽³⁶⁵⁾ Kovos su terorizmu įstatymo vykdymo užtikrinimo dekreto 9 straipsnio 1 dalis. ŽTAP rekomendacijas teikia savarankiškai, tačiau apie tokias rekomendacijas turi pranešti Kovos su terorizmu komisijos pirmininkui.

⁽³⁶⁶⁾ Kovos su terorizmu įstatymo vykdymo užtikrinimo dekreto 9 straipsnio 2 dalis. Remiantis oficialiu Korėjos vyriausybės pareiškimu, neįgyvendinus ŽTAP rekomendacijos atvejis būtų perduodamas Kovos su terorizmu komisijai, įskaitant Ministrą Pirmininką, tačiau iki šiol nebuvo atvejų, kad ŽTAP rekomendacijos būtų neįgyvendintos (žr. II priedo 3.3.1 skirsnį).

⁽³⁶⁷⁾ Žr. II priedo 3.3.4 skirsnį.

⁽³⁶⁸⁾ Konkrečiai NŽT atveju NŽTK yra vykdžiusi *ex officio* tyrimų ir nagrinėjusi kelis individualius skundus. Žr., pvz., NŽTK 2018 m. metinės ataskaitos 128 p. (paskelbta adresu <https://www.humanrights.go.kr/site/program/board/basicboard/view?menuid=002003003001&pagesize=10&boardtypeid=7017&boardid=7604746>) ir NŽTK 2019 m. metinės ataskaitos 70 p. (paskelbta adresu <https://www.humanrights.go.kr/site/program/board/basicboard/view?menuid=002003003001&pagesize=10&boardtypeid=7017&boardid=7606217>).

⁽³⁶⁹⁾ NŽT įstatymo 13 straipsnio 1 dalis.

⁽³⁷⁰⁾ Nacionalinės Asamblėjos įstatymo 36 straipsnis ir 37 straipsnio 1 dalies 15 punktas.

⁽³⁷¹⁾ RPAI 15 straipsnis.

⁽³⁷²⁾ NŽT įstatymo 15 straipsnio 2 dalis.

⁽³⁷³⁾ NŽT įstatymo 17 straipsnio 2 dalis. „Valstybės paslaptys“ – tai (įslaptinti) faktai, prekės ar žinios, kurie negali būti atskleisti jokiai kitai valstybei ar organizacijai, kad būtų išvengta rimtų kliūčių siekiant užtikrinti nacionalinį saugumą, ir su kuriais leidžiama susipažinti tik ribotam asmenų skaičiui. Žr. NŽT įstatymo 13 straipsnio 4 dalį.

teisę arba neleisti ja naudotis tik tiek ir tol, kol tai būtina siekiant apsaugoti svarbų viešojo intereso tikslą ir kai šie veiksmai yra jam proporcingi (pavyzdžiui, tiek ir tol, kol teisės suteikimu būtų trukdoma vykstančiam tyrimui arba dėl jo kultū grėsmė nacionaliniam saugumui), arba kai teisės suteikimas galėtų kelti pavojų trečiojo asmens gyvybei ar fizinei sveikatai. Taigi norint taikyti tokį apribojimą reikia suderinti asmens teises ir interesus su atitinkamu viešuoju interesu ir toks apribojimas jokių atveju negali turėti įtakos esminių šios teisės aspektų įgyvendinimui (Konstitucijos 37 straipsnio 2 dalis). Jei prašymas atmetamas arba apribojamas, asmeniui turi būti nedelsiant pranešta apie priežastis.

- (205) Antra, asmenys turi teisę ginti savo teises pagal AIAĮ, jei tvarkydama jų duomenis nacionalinė saugumo institucija pažeidė AIAĮ arba kituose asmens duomenų rinkimą reglamentuojančiuose įstatymuose (visų pirma RPAĮ (žr. (171) konstatuojamąją dalį) nustatytus apribojimus ir apsaugos priemones⁽³⁷⁴⁾). Šia teise galima pasinaudoti pateikus skundą AIAK (be kita ko, per Korėjos interneto ir saugumo agentūros administruojamą privatumo apsaugos skambučių centrą)⁽³⁷⁵⁾. Be to, siekiant sudaryti palankesnes sąlygas ginti savo teises nukentėjus dėl Korėjos nacionalinių saugumo institucijų veiksmų, ES esantiems asmenims suteikiamos galimybės skundą AIAK pateikti per savo nacionalinę duomenų apsaugos instituciją⁽³⁷⁶⁾. Tokiu atveju, kai tyrimas baigiamas, AIAK informuoja asmenį (įskaitant, kai taikoma, pateikdama informaciją apie taikomus taisomuosius veiksmus) per nacionalinę duomenų apsaugos instituciją. Be to, remdamiesi Administracinių ginčų įstatymu, asmenys gali apskusti AIAK sprendimus arba neveikimą (žr. (132) konstatuojamąją dalį).
- (206) Trečia, asmenys gali pateikti skundą ŽTAP dėl jų teisės į privatumą ir (arba) duomenų apsaugą pažeidimo vykdant kovos su terorizmu veiklą (t. y. remdamiesi Kovos su terorizmu įstatymu)⁽³⁷⁷⁾, o pastarasis gali rekomenduoti taisomuosius veiksmus. Teikiant skundą ŽTAP nėra taikomi priimtino reikalavimai, todėl skundas bus nagrinėjamas net jei atitinkamas asmuo negali įrodyti, kad jis iš tikrųjų patyrė žalą (pavyzdžiui, dėl to, kad nacionalinė saugumo institucija tariamai neteisėtai rinko jo duomenis)⁽³⁷⁸⁾. Atitinkama institucija turi informuoti ŽTAP apie visas priemones, kurių ėmėsi jo rekomendacijoms įgyvendinti.
- (207) Ketvirta, asmenys gali pateikti skundą NŽTK dėl to, kad nacionalinės saugumo institucijos renka jų duomenis, ir ginti savo teises pagal (178) konstatuojamojoje dalyje aprašytą procedūrą⁽³⁷⁹⁾.
- (208) Galiausiai asmenys gali naudotis įvairiomis teisminėmis teisių gynimo priemonėmis⁽³⁸⁰⁾, kad galėtų apginti savo teises pasinaudodami 3.3.1 skirsnyje aprašytais apribojimais ir apsaugos priemonėmis. Visų pirma asmenys gali užginčyti nacionalinių saugumo institucijų veiksmų teisėtumą pagal Administracinių ginčų įstatymą ((181) konstatuojamojoje dalyje nustatyta tvarka) arba Konstitucinio Teismo įstatymą (žr. (182) konstatuojamąją dalį). Be to, jiems gali būti atlyginama žala pagal Valstybės kompensacijų įstatymą (kaip išsamiau aprašyta (183) konstatuojamojoje dalyje).

4. IŠVADA

- (209) Komisija mano, kad taikant AIAĮ, specialias taisykles, taikomas tam tikriems sektoriams (kaip analizuojama 2 skirsnyje), ir papildomas apsaugos priemones, numatytas pranešime Nr. 2021-5 (I priedas), Korėjos Respublikoje užtikrinama tokio lygio iš Europos Sąjungos perduotų asmens duomenų apsauga, kuri yra iš esmės lygiavertė Reglamentu (ES) 2016/679 garantuojamai apsaugai.
- (210) Be to, Komisija mano, kad pagal Korėjos teisę numatytais priežiūros mechanizmais ir teisių gynimo galimybėmis, vertinant juos kaip visumą, sudaromos galimybės praktiškai nustatyti Korėjos duomenų valdytojų padarytus duomenų apsaugos taisyklių pažeidimus ir jų atžvilgiu imtis veiksmų, o duomenų subjektui suteikiama teisių gynimo priemonių, kad jis galėtų susipažinti su savo asmens duomenimis ir vėliau pasiekti, kad šie duomenys būtų ištaisyti arba ištrinti.

⁽³⁷⁴⁾ AIAĮ 58 straipsnio 4 dalis ir 4 straipsnio 5 dalis. Žr. II priedo 3.4.2 skirsnį.

⁽³⁷⁵⁾ AIAĮ 62 straipsnis ir 63 straipsnio 2 dalis.

⁽³⁷⁶⁾ Pranešimas Nr. 2021-5 (I priedo 6 skirsnis).

⁽³⁷⁷⁾ Kovos su terorizmu įstatymo vykdymo užtikrinimo dekreto 8 straipsnio 1 dalies 2 punktą.

⁽³⁷⁸⁾ Žr. II priedo 3.4.1 skirsnį.

⁽³⁷⁹⁾ Pavyzdžiui, NŽTK reguliariai gauna skundus dėl Nacionalinės žvalgybos tarnybos (žr. duomenis apie 2015–2019 m. gautų skundų skaičių NŽTK 2019 m. metinės ataskaitos 70 p. (paskelbta adresu <https://www.humanrights.go.kr/site/program/board/basicboard/view?menuid=002003003001&pagesize=10&boardtypeid=7017&boardid=7606217>)).

⁽³⁸⁰⁾ Žr. II priedo 3.4.4 skirsnį.

- (211) Galiausiai Komisija, remdamasi turima informacija apie Korėjos teisinę tvarką, įskaitant Korėjos vyriausybės pareiškimus, garantijas ir įsipareigojimus, pateiktus II priede, mano, kad bet koks Korėjos valdžios institucijų vykdomas asmenų, kurių asmens duomenys iš Europos Sąjungos perduodami į Korėjos Respubliką, pagrindinių teisių ribojimas viešojo intereso tikslais, visų pirma baudžiamosios teisėsaugos ir nacionalinio saugumo tikslais, bus griežtai apribojamas jį taikant tik tada, kai būtina atitinkamam teisėtam tikslui pasiekti, ir kad egzistuoja veiksminga teisinė apsauga tokio ribojimo atžvilgiu.
- (212) Todėl atsižvelgiant į šio sprendimo išvadas turėtų būti nuspręsta, kad Korėjos Respublika užtikrina tinkamą apsaugos lygį, kaip jis apibrėžtas Reglamento (ES) 2016/679 45 straipsnyje, kuris aiškinamas atsižvelgiant į Europos Sąjungos pagrindinių teisių chartiją asmens duomenų, perduodamų iš Europos Sąjungos į Korėjos Respubliką Korėjos Respublikos asmens duomenų valdytojams, kuriems taikoma AIAI, tvarkymo atžvilgiu, išskyrus asmens duomenis, kuriuos religinės organizacijos tvarko misionierių veiklos tikslais, politinės partijos tvarko keldamos kandidatus, ir asmens kredito informaciją, kurią duomenų valdytojai, kuriuos prižiūri Finansinių paslaugų komisija, tvarko pagal Kredito informacijos įstatymą, jei jie tokią informaciją tvarko.

5. ŠIO SPRENDIMO PADARINIAI IR DUOMENŲ APSAUGOS INSTITUCIJŲ VEIKSMAI

- (213) Valstybės narės ir jų institucijos privalo imtis priemonių, kurios yra būtinos siekiant užtikrinti atitiktį Sąjungos institucijų aktams, nes preziumuojama, kad Sąjungos institucijų teisės aktai yra teisėti, todėl sukelia teisinių pasekmių, kol nėra pripažinti netekusiais galios, panaikinti patenkinus ieškinį dėl panaikinimo, paskelbti negaliojančiais išnagrinėjus prašymą priimti prejudicinį sprendimą arba neteisėtumu grindžiamą prieštaravimą.
- (214) Todėl Komisijos sprendimas dėl tinkamumo, kurį ji priėmė pagal Reglamento (ES) 2016/679 45 straipsnio 3 dalį, yra privalomas visoms valstybių narių, kurioms jis skirtas, institucijoms, įskaitant šių valstybių narių nepriklausomas priežiūros institucijas. Visų pirma Europos Sąjungoje esantys duomenų valdytojai arba duomenų tvarkytojai duomenis duomenų valdytojams Korėjos Respublikoje gali perduoti be papildomo leidimo.
- (215) Reikėtų priminti, kad pagal Reglamento (ES) 2016/679 58 straipsnio 5 dalį ir kaip išaiškinta Teisingumo Teismo sprendime *Schrems* ⁽³⁸¹⁾, jeigu nacionalinė duomenų apsaugos institucija abejoja, įskaitant tuos atvejus, kai pateikiamas skundas, dėl Komisijos sprendimo dėl tinkamumo derėjimo su asmens pagrindinėmis teisėmis į privatumą ir duomenų apsaugą, nacionalinėje teisėje jai turi būti numatyta teisinė teisių gynimo priemonė, kad ji šiuos prieštaravimus galėtų pareikšti nacionaliniame teisme, kuriam gali pririnkti pateikti Teisingumo Teismui prašymą priimti prejudicinį sprendimą ⁽³⁸²⁾.

6. ŠIO SPRENDIMO STEBĖSENA IR PERŽIŪRA

- (216) Remiantis Teisingumo Teismo praktika ⁽³⁸³⁾, ir, kaip pripažįstama Reglamento (ES) 2016/679 45 straipsnio 4 dalyje, Komisija turėtų nuolat stebėti atitinkamus pokyčius trečiojoje valstybėje po sprendimo dėl tinkamumo priėmimo, kad įvertintų, ar trečioji valstybė vis dar užtikrina iš esmės lygiavertį apsaugos lygį. Toks patikrinimas turi būti atliekamas visais atvejais, kai Komisija gauna informacijos, dėl kurios jai šiuo atžvilgiu kyla pagrįstų abejonių.
- (217) Todėl Komisija turėtų nuolat stebėti teisinės sistemos ir esamos asmens duomenų tvarkymo praktikos, kaip įvertinta šiame sprendime, situaciją Korėjos Respublikoje, įskaitant tai, kaip Korėjos institucijos laikosi II priede pateiktų pareiškimų, garantijų ir įsipareigojimų. Kad šis procesas vyktų sklandžiau, Korėjos institucijos turėtų nedelsdama informuoti Komisiją apie esminius su šiuo sprendimu susijusius pokyčius dėl verslo subjektų ir valdžios institucijų atliekamo asmens duomenų tvarkymo, taip pat dėl apribojimų bei apsaugos priemonių, taikomų valdžios institucijų priegai prie asmens duomenų.

⁽³⁸¹⁾ Sprendimo *Schrems* 65 punktas.

⁽³⁸²⁾ Sprendimo *Schrems* 65 punktas: „Šiuo atžvilgiu nacionalinis teisės aktų leidėjas turi numatyti teisių gynimo priemones, leidžiančias atitinkamai nacionalinei priežiūros institucijai remtis nacionaliniuose teismuose prieštaravimais, kurie, jos nuomone, yra pagrįsti, tam, kad šie teismai, vertindami Komisijos sprendimo galiojimą, pateiktų prašymą priimti prejudicinį sprendimą, jei, kaip ir ši institucija, turėtų abejonių dėl šio sprendimo galiojimo.“

⁽³⁸³⁾ Sprendimo *Schrems* 76 punktas.

- (218) Taip pat pažymėtina, jog tam, kad Komisija galėtų veiksmingai vykdyti stebėsenos funkciją, valstybės narės turėtų Komisijai pranešti apie visus atitinkamus veiksmus, kurių ėmėsi nacionalinės duomenų apsaugos institucijos, visų pirma dėl ES duomenų subjektų užklausų ar skundų, susijusių su asmens duomenų perdavimu iš Europos Sąjungos duomenų valdytojams Korėjos Respublikoje. Komisijai taip pat reikėtų pranešti apie bet kokius požymius, kad Korėjos valdžios institucijų, atsakingų už nusikalstamų veikų prevenciją, tyrimą, atskleidimą ar baudžiamąjį persekiojimą už jas, arba atsakingų už nacionalinį saugumą, įskaitant bet kokias priežiūros įstaigas, veiksmais nėra užtikrinama reikiamo lygio apsauga.
- (219) Komisija, taikydama Reglamento (ES) 2016/679 45 straipsnio 3 dalį ⁽³⁸⁴⁾ ir atsižvelgdama į tai, kad pagal Korėjos teisinę tvarką suteikiamas apsaugos lygis gali pasikeisti, po šio sprendimo priėmimo turėtų periodiškai tikrinti, ar išvados dėl Korėjos Respublikos užtikrinamos apsaugos lygio tinkamumo vis dar yra faktiškai ir teisiškai pagrįstos.
- (220) Todėl šis sprendimas pirmą kartą turėtų būti peržiūrimas per trejus metus po jo įsigaliojimo. Po šios pirmosios peržiūros ir atsižvelgdama į jos rezultatus, Komisija, glaudžiai konsultuodamasi su komitetu, įsteigtu pagal Reglamento (ES) 2016/679 93 straipsnio 1 dalį, nuspręš, ar reikėtų išlaikyti trejų metų ciklą. Bet kuriuo atveju vėlesnės peržiūros turėtų būti atliekamos ne rečiau kaip kas ketverius metus ⁽³⁸⁵⁾. Peržiūra turėtų apimti visus šio sprendimo veikimo aspektus, visų pirma šio sprendimo I priede nustatytų papildomų apsaugos priemonių taikymą, ypatingą dėmesį skiriant apsaugai, užtikrinamai tolesnio perdavimo atveju; atitinkamiems teismų praktikos pokyčiams; informacijos, kuriai suteikti pseudonimai, tvarkymo viešojo intereso pagrindu statistikos, mokslinių tyrimų ir archyvavimo tikslais, taip pat AIAI 28 straipsnio 7 dalyje nustatytų išimčių taikymo taisyklėms; naudojimosi asmens teisėmis veiksmingumui, be kita ko, jas įgyvendinant neseniai pertvarkytoje AIAK, ir šių teisių išimčių taikymui; dalinių išimčių pagal AIAI taikymui; taip pat apribojimams ir apsaugos priemonėms, susijusiems su vyriausybės prieiga prie informacijos (kaip nustatyta šio sprendimo II priede), įskaitant AIAK bendradarbiavimą su ES duomenų apsaugos institucijomis dėl asmenų skundų. Ji taip pat turėtų apimti priežiūros ir vykdymo užtikrinimo (visų pirma vykdomų AIAK ir NŽTK) veiksmingumą taikant AIAI ir baudžiamosios teisėsaugos bei nacionalinio saugumo srityje.
- (221) Komisija, atlikdama šią peržiūrą, turėtų susitikti su AIAK, kurią lydėtų (jei reikia) kitos už vyriausybės galimybę susipažinti su informacija atsakingos Korėjos institucijos, įskaitant atitinkamas priežiūros institucijas. Turėtų būti suteiktos galimybės šiame susitikime dalyvauti Europos duomenų apsaugos valdybos atstovams. Atlikdama peržiūrą Komisija turėtų AIAK prašyti pateikti išsamią informaciją apie visus su sprendimu dėl tinkamumo susijusius aspektus, įskaitant apribojimus ir apsaugos priemones, susijusias su vyriausybės galimybe susipažinti su duomenimis ⁽³⁸⁶⁾. Komisija taip pat turėtų prašyti pateikti paaiškinimus dėl bet kokios gautos informacijos, susijusios su šiuo sprendimu, įskaitant viešas Korėjos institucijų ar kitų suinteresuotųjų subjektų Korėjoje, Europos duomenų apsaugos valdybos, atskirų duomenų apsaugos institucijų, pilietinės visuomenės grupių, žiniasklaidos ataskaitas ar bet kokius kitus informacijos šaltinius.
- (222) Remdamasi peržiūra, Komisija turėtų parengti viešą ataskaitą, kuri bus teikiama Europos Parlamentui ir Tarybai.

7. SPRENDIMO GALIOJIMO SUSTABDYMAS, PANAIKINIMAS ARBA KEITIMAS

- (223) Jeigu iš turimos informacijos, ypač iš informacijos, surinktos vykdant stebėseną pagal šį sprendimą, arba iš informacijos, kurią pateikia Korėjos arba valstybių narių institucijos, paaiškėja, kad Korėjos Respublikoje užtikrinamas duomenų apsaugos lygis nebėra pakankamas, Komisija turėtų apie tai nedelsdama informuoti kompetentingas Korėjos institucijas ir paprašyti per nustatytą protingą terminą imtis tinkamų priemonių.
- (224) Jeigu, pasibaigus tam konkrečiam terminui, Korėjos kompetentingos institucijos nesiima tų priemonių arba kitaip įtikinamai neįrodo, kad šis sprendimas toliau grindžiamas tinkamu apsaugos lygiu, Komisija inicijuos Reglamento (ES) 2016/679 93 straipsnio 2 dalyje nurodytą procedūrą, siekdama iš dalies arba visiškai sustabdyti šio sprendimo galiojimą arba jį panaikinti.
- (225) Kitu atveju Komisija pradeda procedūrą, siekdama iš dalies pakeisti sprendimą, visų pirma nustatydama, kad duomenų perdavimui turi būti taikomos papildomos sąlygos, arba apribodama išvadą dėl duomenų apsaugos tinkamumo taip, kad ji būtų taikoma tik tam duomenų perdavimui, kurį vykdant užtikrinamas tinkamo lygio duomenų apsaugos tęstinumas.

⁽³⁸⁴⁾ Pagal Reglamento (ES) 2016/679 45 straipsnio 3 dalį „[i]gyvendinimo akte numatomas periodinės peržiūros, [...] kuria atsižvelgiama į visus atitinkamus pokyčius trečiojoje valstybėje ar tarptautinėje organizacijoje, mechanizmas.“

⁽³⁸⁵⁾ Reglamento (ES) 2016/679 45 straipsnio 3 dalyje nustatyta, kad periodinė peržiūra turi būti atliekama „bent kas ketverius metus“. Taip pat žr. Europos duomenų apsaugos valdybos darbinį dokumentą „Orientaciniai tinkamumo kriterijai“, WP 254, 1-oji peržiūrėta versija.

⁽³⁸⁶⁾ Žr. šio sprendimo II priedą.

- (226) Komisija galiojimo sustabdymo arba panaikinimo procedūrą visų pirma turėtų inicijuoti tuo atveju, kai yra požymių, kad verslo subjektai, gaunantys asmens duomenis pagal šį sprendimą, netaiko I priede pateiktų papildomų apsaugos priemonių ir (arba) ne iki galo užtikrinamas jų taikymas, arba kad Korėjos institucijos nesilaiko pareiškimų, garantijų ir įsipareigojimų, pateiktų šio sprendimo II priede.
- (227) Komisija taip pat turėtų apsvarstyti galimybę pradėti procedūrą dėl šio sprendimo pakeitimo, jo galiojimo sustabdymo arba panaikinimo, jeigu atliekant peržiūrą arba kitu metu kompetentingos Korėjos institucijos nepateikia informacijos arba paaiškinimų, kurie yra būtini norint įvertinti iš Europos Sąjungos į Korėjos Respubliką perduodamiems asmens duomenims užtikrinamą apsaugos lygį arba tai, kaip laikomasi šio sprendimo. Šiuo atžvilgiu Komisija turėtų atsižvelgti į tai, kiek atitinkamos informacijos ji gali gauti iš kitų šaltinių.
- (228) Remdamasi tinkamai pagrįsta privalomos skubos priežastimi, Komisija pasinaudos galimybe pagal Reglamento (ES) 2016/679 93 straipsnio 3 dalyje nustatytą procedūrą priimti nedelsiant taikytinus įgyvendinimo aktus, kuriais sprendimo galiojimas sustabdomas, sprendimas panaikinamas arba iš dalies pakeičiamas.

8. BAIGIAMOSIOS PASTABOS

- (229) Europos duomenų apsaugos valdyba paskelbė savo nuomonę ⁽³⁸⁷⁾, į kurią buvo atsižvelgta rengiant šį sprendimą.
- (230) Šiame sprendime numatytos priemonės atitinka pagal Reglamento (ES) 2016/679 93 straipsnio 1 dalį įsteigto komiteto nuomonę,

PRIĖMĖ ŠĮ SPRENDIMĄ:

1 straipsnis

1. Atsižvelgdama į Reglamento (ES) 2016/679 45 straipsnį Korėjos Respublika užtikrina tinkamą asmens duomenų, iš Europos Sąjungos perduodamų subjektams Korėjos Respublikoje, apsaugos lygį pagal Asmeninės informacijos apsaugos įstatymą, kurį papildo I priede išdėstytos papildomos apsaugos priemonės kartu su II priede pateiktais oficialiais pareiškimais, garantijomis ir įsipareigojimais.

2. Šis sprendimas netaikomas asmens duomenims, perduodamiems vienai iš toliau nurodytų kategorijų priklausančioms gavėjams, kai visi arba dalis asmens duomenų tvarkymo tikslų atitinka vieną iš nurodytų tikslų, atitinkamai:

- (a) religinėms organizacijoms, kai jos tvarko asmens duomenis misionierių veiklos tikslais;
- (b) politinėms partijoms, kai jos tvarko asmens duomenis iškeldamos kandidatus;
- (c) subjektams, kuriuos prižiūri Finansinių paslaugų komisija, kai jie tvarko asmeninę kredito informaciją pagal Kredito informacijos įstatymą, jei jie tvarko tokią informaciją.

2 straipsnis

Jei valstybių narių kompetentingos institucijos, siekdamos apsaugoti asmenis tvarkant jų asmens duomenis, įgyvendina savo įgaliojimus pagal Reglamento (ES) 2016/679 58 straipsnį dėl duomenų perdavimo, kuris patenka į šio sprendimo 1 straipsnyje nustatytą taikymo sritį, atitinkama valstybė narė turi nedelsdama apie tai informuoti Komisiją.

3 straipsnis

1. Komisija nuolat stebi teisinės sistemos, kuria grindžiamas šis sprendimas, taikymą, įskaitant sąlygas, kuriomis vykdomas tolesnis duomenų perdavimas, įgyvendinamos asmens teisės ir Korėjos valdžios institucijoms suteikiama prieiga prie duomenų, kurie buvo perduoti pagal šį sprendimą, siekdama įvertinti, ar Korėjos Respublika ir toliau užtikrina tinkamą 1 straipsnyje nurodytą apsaugos lygį.

⁽³⁸⁷⁾ Nuomonė 32/2021 dėl Europos Komisijos įgyvendinimo sprendimo pagal Reglamentą (ES) 2016/679 dėl tinkamos asmens duomenų apsaugos Korėjos Respublikoje projekto, kurią galima rasti adresu https://edpb.europa.eu/our-work-tools/our-documents/opinion-art-70/opinion-322021-regarding-european-commission-draft_en.

2. Valstybės narės ir Komisija viena kitą turi informuoti apie atvejus, kai Asmeninės informacijos apsaugos komisija arba bet kokia kita kompetentinga Korėjos institucija neužtikrina, kad būtų laikomasi teisinės sistemos, kuria grindžiamas šis sprendimas.
3. Valstybės narės ir Komisija viena kitą turi informuoti apie bet kokius požymius, kad Korėjos valdžios institucijos riboja asmenų teisę į jų asmens duomenų apsaugą viršydamos tai, kas yra būtina, arba apie tai, kad tokio ribojimo atžvilgiu nėra suteikiama jokios veiksmingos teisinės apsaugos.
4. Po trejų metų nuo pranešimo apie šį sprendimą valstybėms narėms, o paskui – ne rečiau kaip kas ketverius metus, Komisija turi įvertinti 1 straipsnio 1 dalyje pateiktą išvadą remdamasi visa turima informacija, įskaitant informaciją, gautą peržiūros, kuri atliekama kartu su atitinkamomis Korėjos institucijomis, metu.
5. Jei Komisija nustato, kad yra požymių, kad tinkamas apsaugos lygis daugiau nebeužtikrinamas, Komisija turi apie tai informuoti kompetentingas Korėjos institucijas. Prireikus, Komisija gali nuspręsti laikinai sustabdyti šio sprendimo taikymą, jį iš dalies pakeisti ar panaikinti, arba apriboti jo taikymo sritį pagal Reglamento (ES) 2016/679 45 straipsnio 5 dalį, visų pirma, jei yra požymių, kad:
 - (a) duomenų valdytojai Korėjoje, kurie gavo asmens duomenis iš Europos Sąjungos pagal šį sprendimą, netaiko šio sprendimo I priede pateiktų papildomų apsaugos priemonių, arba jų taikymo priežiūra ir užtikrinimas yra nepakankami;
 - (b) Korėjos valdžios institucijos nesilaiko II priede pateiktų pareiškimų, garantijų ir įsipareigojimų, įskaitant dėl sąlygų ir ribojimų, taikomų Korėjos valdžios institucijoms renkant pagal šį sprendimą perduotus asmens duomenis ir su jais susipažįstant baudžiamosios teisėsaugos arba nacionalinio saugumo tikslais.

Komisija taip pat gali taikyti tokias priemones, jei dėl nepakankamo Korėjos vyriausybės bendradarbiavimo Komisija negali nustatyti, ar Korėjos Respublikoje ir toliau užtikrinamas tinkamas apsaugos lygis.

4 straipsnis

Šis sprendimas skirtas valstybėms narėms.

Priimta Briuselyje 2021 m. gruodžio 17 d.

Komisijos vardu
Didier REYNDERS
Komisijos narys

I PRIEDAS

PAPILDOMOS TAISYKLĖS DĖL ASMENINĖS INFORMACIJOS APSAUGOS ĮSTATYMO AIŠKINIMO IR
TAIKYMO, SUSIJUSIOS SU Į KORĖJĄ PERDUOTŲ ASMENS DUOMENŲ TVARKYMU

Turinys

I.	Apžvalga	54
II.	Sąvokų apibrėžtys	55
III.	Papildomos taisyklės	55
1.	Asmeninės informacijos naudojimo ir teikimo ne pagal tikslą apribojimas (įstatymo 3, 15 ir 18 straipsniai)	55
2.	Asmens duomenų tolesnio perdavimo apribojimas (įstatymo 17 straipsnio 3 ir 4 dalys, 18 straipsnis)	57
3.	Pranešimas apie duomenų naudojimą, kai asmens duomenys nebuvo gauti iš duomenų subjekto (įstatymo 20 straipsnis)	58
4.	Informacijai, kuriai suteikti pseudonimai, taikomos specialios išimties taikymo sritis (įstatymo 28-2, 28-3, 28-4, 28-5, 28-6 ir 28-7 straipsniai, 3 ir 58-2 straipsniai)	60
5.	Taisomieji veiksmai ir kt. (įstatymo 64 straipsnio 1, 2 ir 4 dalys)	61
6.	AIAI taikymas tvarkant asmens duomenis nacionalinio saugumo tikslais, įskaitant pažeidimų tyrimą ir vykdymo užtikrinimą pagal AIAI (AIAI 7-8, 7-9, 58, 3, 4 ir 62 straipsniai)	62

I. Apžvalga

Po Korėjos ir Europos Sąjungos (toliau – ES) diskusijų dėl tinkamumo Europos Komisija nustatė, kad Korėja užtikrina tinkamą asmens duomenų apsaugos lygį, kaip numatyta BDAR 45 straipsnyje.

Atsižvelgdama į šias aplinkybes, Asmeninės informacijos apsaugos komisija priėmė šį pranešimą remdamasi Asmeninės informacijos apsaugos įstatymo 5 straipsniu (Valstybės pareigos ir kt.) ir 14 straipsniu (Tarptautinis bendradarbiavimas) ⁽¹⁾, siekdama paaiškinti tam tikrų įstatymo nuostatų aiškinimą, taikymą ir vykdymo užtikrinimą, be kita ko, asmens duomenų, perduotų į Korėją remiantis ES sprendimu dėl tinkamumo, tvarkymo atžvilgiu.

Kadangi šis pranešimas turi administracinės taisyklės, kurią kompetentinga administracinė agentūra nustato ir paskelbia, siekdama paaiškinti Asmeninės informacijos apsaugos įstatymo aiškinimo, taikymo ir vykdymo užtikrinimo Korėjos teisinėje sistemoje standartus, statusą, asmeninės informacijos valdytojui jis turi privalomą teisinę galią, o tai reiškia, kad bet koks šio pranešimo pažeidimas gali būti laikomas atitinkamų AIAI nuostatų pažeidimu. Be to, jei pažeidus šį pranešimą pažeidžiamos asmeninės teisės ir interesai, atitinkami asmenys gali ginti savo teises kreipdamiesi į Asmeninės informacijos apsaugos komisiją arba teismą.

Taigi asmeninės informacijos valdytojui, kuris tvarko į Korėją pagal ES sprendimą dėl tinkamumo perduotą asmeninę informaciją, nesimant šiame pranešime nustatytų priemonių bus laikoma, kad „yra svarių priežasčių manyti, kad buvo padarytas pažeidimas, susijęs su asmenine informacija, o nesėdimus veiksnių gali būti padaryta sunkiai atitaisoma žala“, kaip nustatyta įstatymo 64 straipsnio 1 ir 2 dalyse. Tokiais atvejais Asmeninės informacijos apsaugos komisija arba

⁽¹⁾ Asmeninės informacijos apsaugos įstatymo 14 straipsnyje nustatyta, kad Korėjos Vyriausybė turi įgaliojimą nustatyti politiką, kuria siekiama gerinti asmeninės informacijos apsaugos lygį tarptautinėje aplinkoje ir užkirsti kelią duomenų subjektų teisių pažeidimams dėl tarpvalstybinio asmeninės informacijos perdavimo.

susijusios centrinės administracinės agentūros remdamosi šioje nuostatoje nustatytais įgaliojimais gali nurodyti atitinkamam asmeninės informacijos valdytojui imtis taisomųjų ir kt. veiksmų, o atsižvelgiant į konkrečius įstatymo pažeidimus taip pat gali būti skiriamos atitinkamos baudmės (sankcijos, administracinės baudos ir t. t.).

II. Sąvokų apibrėžtys

Šioje nuostatoje vartojamų sąvokų apibrėžtys:

- (i) įstatymas – Asmeninės informacijos apsaugos įstatymas (įstatymas Nr. 16930, iš dalies pakeistas 2020 m. vasario 4 d. ir įsigaliojęs 2020 m. rugpjūčio 5 d.);
- (ii) Prezidento dekretas – Asmeninės informacijos apsaugos įstatymo vykdymo užtikrinimo dekretas (2020 m. kovo 3 d. Prezidento dekretas Nr. 30509, kuriuo iš dalies keičiami kiti įstatymai);
- (iii) duomenų subjektas – asmuo, kurio tapatybę galima nustatyti tvarkant informaciją ir kuris tampa tos informacijos objektu;
- (iv) asmeninės informacijos valdytojas – viešoji įstaiga, juridinis asmuo, organizacija, fizinis asmuo ir t. t., kuris vykdydamas veiklą tiesiogiai ar netiesiogiai tvarko asmeninę informaciją;
- (v) ES – ES (2020 m. vasario mėn. pabaigoje – 27 valstybės narės ⁽²⁾), įskaitant Belgiją, Vokietiją, Prancūziją, Italiją, Liuksemburgą, Nyderlandus, Daniją, Airiją, Graikiją, Portugaliją, Ispaniją, Austriją, Suomiją, Švediją, Kiprą, Čekijos Respubliką, Estiją, Vengriją, Latviją, Lietuvą, Maltą, Lenkiją, Slovakiją, Slovėniją, Rumuniją, Bulgariją ir Kroatiją) ir su ES pagal EEE susitarimą susijusios šalys (Islandija, Lichtenšteinas ir Norvegija);
- (vi) BDAR – ES bendrasis asmeninės informacijos apsaugos teisės aktas, Bendrasis duomenų apsaugos reglamentas (Reglamentas (ES) 2016/679);
- (vii) Sprendimas dėl tinkamumo – remiantis BDAR 45 straipsnio 3 dalimi, Europos Komisijos sprendimas, kad trečioji valstybė, trečiosios valstybės teritorija arba vienas ar daugiau sektorių joje, arba tarptautinė organizacija užtikrina asmeninės informacijos apsaugą, kuri yra tinkamo lygio.

III. Papildomos taisyklės

1. Asmeninės informacijos naudojimo ir teikimo ne pagal tikslą apribojimas (įstatymo 3, 15 ir 18 straipsniai)

<Asmeninės informacijos apsaugos įstatymas

(įstatymas Nr. 16930, iš dalies pakeistas 2020 m. vasario 4 d.)>

3 straipsnis (Asmeninės informacijos apsaugos principai). 1) Asmeninės informacijos valdytojas aiškiai nurodo, kokiais tikslais tvarkoma asmeninė informacija, ir teisėtai bei sąžiningai renka tokį asmeninės informacijos kiekį, kuris yra būtinas tokiems tikslams pasiekti.

2) Asmeninės informacijos valdytojas asmeninę informaciją tvarko tinkamai, kaip būtina tikslams, kurių pagrindu ji tvarkoma, pasiekti, ir nenaudoja jos jokiais kitais tikslais.

15 straipsnis (Asmeninės informacijos rinkimas ir naudojimas). 1) Asmeninės informacijos valdytojas asmeninę informaciją gali rinkti bet kuriomis iš šių aplinkybių ir gali ją naudoti rinkimo tikslu:

1. gavęs duomenų subjekto sutikimą;
2. kai tai numatyta specialiomis teisės aktų nuostatomis arba neišvengiama siekiant įvykdyti teisinius įsipareigojimus;
3. kai tai neišvengiama viešajai institucijai siekiant vykdyti savo pareigas, priskirtas jos jurisdikcijai, kaip nustatyta įstatymuose ir pan.;
4. kai tai neišvengiamai būtina siekiant taikyti ir vykdyti su duomenų subjektu pasirašytą sutartį;

⁽²⁾ Iki pereinamojo laikotarpio pabaigos viena jų taip pat buvo Jungtinė Karalystė, kaip numatyta Susitarimo dėl Jungtinės Didžiosios Britanijos ir Šiaurės Airijos Karalystės išstojimo iš Europos Sąjungos ir Europos atominės energijos bendrijos (2019/C 384 I/01) 126, 127 ir 132 straipsniuose.

5. kai tai akivaizdžiai būtina siekiant apsaugoti duomenų subjekto arba trečiosios šalies gyvybę, fizinius ar turtinius interesus nuo gresiančio pavojaus, jei duomenų subjektas ar jo teisėtas atstovas negali išreikšti savo ketinimų arba neįmanoma gauti jo išankstinio sutikimo, nes nežinomi jo adresai ir kt.;
6. kai tai būtina siekiant asmeninės informacijos valdytojo pagrįsto intereso, jei toks interesas yra akivaizdžiai viršesnis už duomenų subjekto teises. Tokiais atvejais duomenis leidžiama tvarkyti tik tiek, kiek tvarkymas yra pagrįstai susijęs su asmeninės informacijos valdytojo pagrįstu interesu, ir tvarkomas toks duomenų kiekis, koks yra pagrįstai reikalingas.

18 straipsnis (Asmeninės informacijos naudojimo ir teikimo ne pagal tikslą apribojimas). 1) Asmeninės informacijos valdytojas nenaudoja asmeninės informacijos kitais tikslais nei nurodyti 15 straipsnio 1 dalyje ir 39-3 straipsnio 1 ir 2 dalyse arba neteikia jos jokiai trečiajai šaliai kitais tikslais nei nurodyti 17 straipsnio 1 ir 3 dalyse.

2) Nepaisant 1 dalies, tais atvejais, kai taikomas kuris nors iš toliau nurodytų punktų, asmeninės informacijos valdytojas gali naudoti asmeninę informaciją arba ją teikti trečiajai šaliai kitais tikslais, išskyrus atvejus, kai taip galėtų būti nepagrįstai pažeisti duomenų subjekto ar trečiosios šalies interesai (atsižvelgiant į tai, kad informacijos ir ryšių paslaugų teikėjams [kaip nustatyta Informacijos ir ryšių tinklų naudojimo ir duomenų apsaugos skatinimo įstatymo 2 straipsnio 1 dalies 3 punkte ir kt.; toliau taikoma ta pati nuostata], tvarkantiems naudotojų asmeninę informaciją [kaip nustatyta Informacijos ir ryšių tinklų naudojimo ir duomenų apsaugos skatinimo įstatymo 2 straipsnio 1 dalies 4 punkte ir kt.; toliau taikoma ta pati nuostata], taikomi tik 1 ir 2 punktai, o 5–9 punktai taikomi tik viešosioms institucijoms):

1. kai gaunamas papildomas duomenų subjekto sutikimas;
2. kai tai numatyta kitose konkrečiose teisės aktų nuostatose;
3. kai tai akivaizdžiai būtina siekiant apsaugoti duomenų subjekto arba trečiosios šalies gyvybę, fizinius ar turtinius interesus nuo gresiančio pavojaus, jei duomenų subjektas ar jo teisėtas atstovas negali išreikšti savo ketinimų arba neįmanoma gauti jo išankstinio sutikimo, nes nežinomi jo adresai;
4. ištrinta <2020 m. vasario 4 d. įstatymu Nr. 16930>;
5. kai neįmanoma vykdyti jo jurisdikcijai priskirtų pareigų, kaip numatyta bet kuriame teisės akte, išskyrus atvejus, kai asmeninės informacijos valdytojas asmeninę informaciją naudoja kitais tikslais nei numatytasis, arba teikia ją trečiajai šaliai, ir tai apsvarstyti ir dėl to sprendimą priimti turi Komisija;
6. kai asmeninę informaciją būtina teikti užsienio valstybės vyriausybei arba tarptautinei organizacijai, kad ji galėtų vykdyti sutartį ar kitą tarptautinę konvenciją;
7. kai tai būtina nusikaltimo tyrimui, kaltinimų pateikimui ir baudžiamajam persekiojimui;
8. kai tai būtina, kad teismas galėtų vykdyti su teismo procesu susijusias pareigas;
9. kai tai būtina bausmės, probacijos skyrimui ir sulaukymui.

3–4 punktai praleisti

5) Kai asmeninės informacijos valdytojas asmeninę informaciją trečiajai šaliai teikia kitais tikslais nei numatyti ir bet kuriuo iš 2 dalyje nurodytu atveju, asmeninės informacijos valdytojas nurodo asmeninės informacijos gavėjui apriboti naudojimo tikslą ir būdą bei kitus būtinus aspektus arba parengti būtinas apsaugos priemones, kad būtų užtikrintas asmeninės informacijos saugumas. Tokiais atvejais tokį nurodymą gavęs asmuo imasi būtinų priemonių, kad užtikrintų asmeninės informacijos saugumą.

- i) Įstatymo 3 straipsnio 1 ir 2 dalyse nustatytas principas, pagal kurį asmeninės informacijos valdytojas privalo rinkti tik teisėto tvarkymo tikslu būtiną asmeninę informaciją ir neturėtų jos naudoti kitais tikslais, nei numatyta ⁽³⁾.
- ii) Vadovaujantis šiuo principu įstatymo 15 straipsnio 1 dalyje nustatyta, kad asmeninės informacijos valdytojo renkama asmeninė informacija gali būti naudojama rinkimo tikslu, o 18 straipsnio 1 dalyje nustatyta, kad asmeninė informacija neturėtų būti naudojama kitu tikslu nei jos rinkimo tikslas arba teikiama trečiajai šaliai.

⁽³⁾ Šiose nuostatose nustatyti bendrieji principai taikomi bet kokiam asmeninės informacijos tvarkymui, įskaitant atvejus, kai tokį tvarkymą konkrečiai reglamentuoja kiti teisės aktai, todėl šiame skirsnyje pateikti paaiškinimai taip pat taikomi tais atvejais, kai asmens duomenys tvarkomi remiantis kitais įstatymais (žr., pvz., Kredito informacijos įstatymo 15 straipsnio 1 dalį, kurioje nurodomos konkrečiai šios nuostatos).

- iii) Be to, net jei išimtiniais atvejais, nurodytais įstatymo 18 straipsnio 2 dalyje ⁽⁴⁾, asmeninė informacija gali būti naudojama kitais tikslais nei numatytasis arba teikiama trečiajai šaliai, turi būti reikalaujama apriboti naudojimo tikslą ar būdą, kad asmeninė informacija galėtų būti saugiai tvarkoma pagal 5 dalį, arba imtis priemonių, būtinų asmeninės informacijos saugumui užtikrinti.
- iv) Anksčiau nurodytos nuostatos vienodai taikomos tvarkant visą asmeninę informaciją, į Korėjos teisinės jurisdikcijos teritoriją gautą iš trečiosios valstybės, neatsižvelgiant į duomenų subjekto pilietybę.
- v) Pavyzdžiui, jei asmeninės informacijos valdytojas ES perduoda asmeninę informaciją asmeninės informacijos valdytojui Korėjoje pagal Europos Komisijos sprendimą dėl tinkamumo, asmeninės informacijos valdytojo ES asmeninės informacijos perdavimo tikslas laikomas asmeninės informacijos valdytojo Korėjoje asmeninės informacijos rinkimo tikslu ir tokiais atvejais asmeninės informacijos valdytojas Korėjoje gali naudoti asmeninę informaciją arba teikti ją trečiajai šaliai tik rinkimo tikslu, išskyrus įstatymo 18 straipsnio 2 dalyje nurodytus išimtinis atvejus.

2. Asmens duomenų tolesnio perdavimo apribojimas (įstatymo 17 straipsnio 3 ir 4 dalys, 18 straipsnis)

<Asmeninės informacijos apsaugos įstatymas

(įstatymas Nr. 16930, iš dalies pakeistas 2020 m. vasario 4 d.)>

17 straipsnis (Asmeninės informacijos teikimas). 1) praleistas

2) Gavęs sutikimą pagal 1 dalies 1 punktą, asmeninės informacijos valdytojas informuoja duomenų subjektą apie toliau nurodytus aspektus. Tas pats taikoma, kai bet kuris iš šių aspektų pasikeičia:

1. asmeninės informacijos gavėjas;
2. tikslas, kurio pagrindu asmeninės informacijos gavėjas tokią informaciją naudoja;
3. teiktinos asmeninės informacijos ypatybės;
4. laikotarpis, kurio metu gavėjas saugo ir naudoja asmeninę informaciją;
5. duomenų subjekto teisė atsakyti duoti sutikimą ir dėl šio atsakymo jam kilsiantys nepatogumai, jei jų kiltų.

3) Asmeninės informacijos valdytojas informuoja duomenų subjektą apie 2 dalyje numatytus aspektus ir gauna duomenų subjekto sutikimą, kad galėtų teikti asmeninę informaciją užsienio valstybėje esančiai trečiajai šaliai; ir nesudaro sutarties dėl tarpvalstybinio asmeninės informacijos perdavimo, jei taip pažeidžiamas šis įstatymas.

4) Asmeninės informacijos valdytojas gali teikti asmeninę informaciją be duomenų subjekto sutikimo tada, kai tai pagrįstai susiję su pradiniais asmeninės informacijos rinkimo tikslais, atsižvelgiant į aspektus, nustatytus Prezidento dekretu, ir į tai, ar duomenų subjektui kyla nepatogumų, ar imtasi būtinų saugumo užtikrinimo priemonių, pvz., šifravimo, ir t. t.

※ Dėl su 18 straipsniu susijusios informacijos žr. 3, 4 ir 5 puslapius.

<Asmeninės informacijos apsaugos įstatymo vykdymo užtikrinimo dekretas

([įsigaliojimo data: 2021 m. vasario 5 d.] [2020 m. rugpjūčio 4 d. Prezidento dekretas Nr. 30892, kuriuo iš dalies keičiami kiti įstatymai])>

14-2 straipsnis (Standartai dėl asmeninės informacijos papildomo naudojimo ir (arba) teikimo, ir kt.).

1) Jei asmeninės informacijos valdytojas naudoja arba teikia asmeninę informaciją (toliau – asmeninės informacijos papildomas naudojimas arba teikimas) be duomenų subjekto sutikimo vadovaudamasis įstatymo 15 straipsnio 3 dalimi arba 17 straipsnio 4 dalimi, asmeninės informacijos valdytojas atsižvelgia į šiuos aspektus:

1. ar papildomas asmeninės informacijos naudojimas arba teikimas pagrįstai susijęs su pradiniu asmeninės informacijos rinkimo tikslu,
2. ar papildomą asmeninės informacijos naudojimą arba teikimą galima numatyti atsižvelgiant į aplinkybes, kuriomis asmeninė informacija buvo renkama, ir tvarkymo praktiką,
3. ar papildomas asmeninės informacijos naudojimas arba teikimas nepagrįstai nepažeidžia duomenų subjekto interesų ir
4. ar imtasi priemonių, reikalingų saugumui užtikrinti, kaip antai pseudonimų suteikimo arba šifravimo.

⁽⁴⁾ Informacijos ir ryšių paslaugų teikėjams taikomi tik 18 straipsnio 2 dalies 1 ir 2 punktai. 5–9 punktai taikomi tik viešosioms įstaigoms.

2) Asmeninės informacijos valdytojas iš anksto atskleidžia 1 dalies punktuose nurodytų aspektų vertinimo kriterijus Privatumo politikoje pagal įstatymo 30 straipsnio 1 dalį, o privatumo pareigūnas pagal įstatymo 31 straipsnio 1 dalį tikrina, ar asmeninės informacijos valdytojas asmeninę informaciją papildomai naudoja arba teikia laikydamasis atitinkamų standartų.

i) Jei asmeninės informacijos valdytojas teikia asmeninę informaciją trečiajai šaliai užsienio valstybėje, jis turi iš anksto informuoti duomenų subjektus apie visus įstatymo 17 straipsnio 2 dalyje nurodytus aspektus ir gauti jų sutikimą, išskyrus atvejus, numatytus 1 arba 2 punktuose. Neturėtų būti sudaroma jokia sutartis dėl tarpvalstybinio asmens duomenų teikimo, jei taip pažeidžiamas šis įstatymas.

(1) Jei asmeninė informacija teikiama tokiu tikslu, kuris pagrįstai susijęs su pradiniu rinkimo tikslu pagal Įstatymo 17 straipsnio 4 dalį. Tačiau ši nuostata gali būti taikoma tik tais atvejais, kai laikomasi vykdymo užtikrinimo dekreto 14-2 straipsnyje nustatytų asmeninės informacijos papildomo naudojimo ir teikimo standartų. Be to, asmeninės informacijos valdytojas turi atsižvelgti į tai, ar asmeninės informacijos teikimas gali sukelti nepatogumų duomenų subjektams ir ar imtasi būtinų priemonių saugumui užtikrinti, kaip antai šifravimo.

(2) Jei asmeninė informacija gali būti teikiama trečiajai šaliai išimtiniais atvejais, nurodytais įstatymo 18 straipsnio 2 dalyje (žr. 3–5 p.). Tačiau net ir tokiais atvejais, jei tokios asmeninės informacijos teikimas gali nepagrįstai pažeisti duomenų subjekto ar trečiosios šalies interesus, asmeninė informacija negali būti teikiama trečiajai šaliai. Be to, asmeninės informacijos teikėjas privalo reikalauti, kad asmeninės informacijos gavėjas apribotų asmeninės informacijos naudojimo tikslą ar būdą arba imtųsi priemonių, būtinų jos saugumui užtikrinti, kad asmeninė informacija būtų tvarkoma saugiai.

ii) Jei asmeninė informacija teikiama trečiajai šaliai užsienio valstybėje, dėl skirtumų tarp skirtingose valstybėse taikomų asmeninės informacijos apsaugos sistemų šiai asmeninei informacijai taikomos apsaugos lygis gali neatitikti apsaugos lygio, kuris Korėjoje garantuojamas Asmeninės informacijos apsaugos įstatymu. Atitinkamai, tokie atvejai bus laikomi įstatymo 17 straipsnio 4 dalyje nurodytais „atvejais, kai duomenų subjektui gali būti sukelta nepatogumų“, arba įstatymo 18 straipsnio 2 dalyje arba to paties įstatymo vykdymo užtikrinimo dekreto 14-2 straipsnyje nurodytais „atvejais, kai nepagrįstai pažeidžiami duomenų subjekto ar trečiosios šalies interesus“⁽⁵⁾. Kad įvykdytų šių nuostatų reikalavimus, asmeninės informacijos valdytojas ir trečioji šalis turi aiškiai užtikrinti įstatymui lygiavertį apsaugos lygį, įskaitant garantiją, kad duomenų subjektas galės naudotis savo teisėmis, numatytomis teisiškai įpareigojančiuose dokumentuose, kaip antai sutartyse, netgi tada, kai asmeninė informacija perduodama į užsienio valstybę.

3. Pranešimas apie duomenų naudojimą, kai asmens duomenys nebuvo gauti iš duomenų subjekto (įstatymo 20 straipsnis)

<Asmeninės informacijos apsaugos įstatymas

(įstatymas Nr. 16930, iš dalies pakeistas 2020 m. vasario 4 d.)>

20 straipsnis (Pranešimas apie iš trečiųjų šalių surinktos asmeninės informacijos šaltinius ir kt.). 1) Kai asmeninės informacijos valdytojas tvarko iš trečiųjų šalių surinktą asmeninę informaciją, duomenų subjekto prašymu asmeninės informacijos valdytojas nedelsdamas praneša tokiam duomenų subjektui apie šiuos aspektus:

1. surinktos asmeninės informacijos šaltinį;
2. asmeninės informacijos tvarkymo tikslą;
3. duomenų subjekto teisę reikalauti sustabdyti asmeninės informacijos tvarkymą, kaip numatyta 37 straipsnyje.

2) Nepaisant 1 dalies, kai asmeninės informacijos valdytojas, atitinkantis Prezidento dekretu nustatytus kriterijus, kuriais atsižvelgiama į tvarkomos asmeninės informacijos rūšis ir kiekį, darbuotojų skaičių, pardavimų apimtį ir kt., renka asmeninę informaciją iš trečiųjų šalių ir ją tvarko pagal 17 straipsnio 1 dalies 1 punktą, asmeninės informacijos valdytojas praneša duomenų subjektui apie 1 punkte nurodytus aspektus; su sąlyga, kad tai netaikoma, kai asmeninės informacijos valdytojo surinktoje informacijoje nėra jokios asmeninės informacijos, pavyzdžiui, kontaktinės informacijos, kurią naudojant būtų galima informuoti duomenų subjektą.

⁽⁵⁾ Pagal AIAĮ 18 straipsnio 2 dalies 2 punktą tai taip pat taikoma, kai asmeninė informacija trečiosioms šalims užsienio valstybėje atskleidžiama remiantis kitų įstatymų (pvz., Kredito informacijos įstatymo) nuostatomis.

3) Būtinai aspektai, susiję su pranešimo duomenų subjektui pagal 2 punkto pagrindinį sakinį laiku, būdu ir tvarka, nustatomi Prezidento dekretu.

4) 1 punktas ir pagrindinė 2 punkto sąlyga netaikomi šioms aplinkybėmis (su sąlyga, kad taip yra tik tuo atveju, kai tai akivaizdžiai viršija duomenų subjekto teises pagal šį įstatymą):

1. kai asmeninė informacija, apie kurią reikia pranešti, įtraukta į asmeninės informacijos bylas, nurodytas bet kuriame 32 straipsnio 2 dalies punkte;
2. kai dėl tokio pranešimo gali kilti grėsmė bet kurio kito asmens gyvybei ar fizinei sveikatai arba gali būti nepagrįstai pakenkta bet kurio kito asmens turciniams ir kitiems interesams.

(i) Jei asmeninės informacijos valdytojas gauna asmeninę informaciją, perduotą iš ES remiantis joje priimtu sprendimu dėl tinkamumo ⁽⁶⁾, jis privalo nedelsdamas ir bet kuriuo atveju ne vėliau kaip per vieną mėnesį nuo informacijos perdavimo duomenų subjektui pateikti informaciją, nurodytą 1–5 punktuose:

- (1) vardą, pavardę arba pavadinimą, taip pat kontaktinę informaciją asmenų, kurie perduoda ir gauna asmeninę informaciją;
- (2) perduotos asmeninės informacijos vienetus ar kategorijas;
- (3) asmeninės informacijos rinkimo ir naudojimo tikslą (duomenų eksportuotojo nustatytą pagal šio pranešimo 1 punktą);
- (4) asmeninės informacijos saugojimo laikotarpį;
- (5) informaciją apie duomenų subjekto teises, susijusias su asmeninės informacijos tvarkymu, naudojimosi teisėmis būdą ir tvarką bei bet kokius nepatogumus, jei naudojimas jomis jų sukelia.

(ii) Be to, jei asmeninės informacijos valdytojas teikia i punkte nurodytą asmeninę informaciją trečiajai šaliai Korėjos Respublikoje arba užsienio valstybėje, prieš teikdamas asmeninę informaciją jis turi pateikti duomenų subjektui 1–5 punktuose nurodytą informaciją:

- (1) vardą, pavardę arba pavadinimą, taip pat kontaktinę informaciją asmenų, kurie teikia ir gauna asmeninę informaciją;
- (2) teikiamos asmeninės informacijos vienetus ar kategorijas;
- (3) šalį, į kurią asmeninė informacija bus teikiama, numatomą jos teikimo laikotarpį ir būdą (tik tais atvejais, kai asmeninė informacija teikiama trečiajai šaliai užsienio valstybėje);
- (4) asmeninės informacijos teikėjo tikslą ir teisinį pagrindą, kurį taikant asmeninė informacija teikiama;
- (5) informaciją apie duomenų subjekto teises, susijusias su asmeninės informacijos tvarkymu, naudojimosi teisėmis būdą ir tvarką bei bet kokius nepatogumus, jei naudojimas jomis jų sukelia.

(iii) Asmeninės informacijos valdytojas negali taikyti i arba ii punktų bet kuriuo iš 1–4 punktuose nurodytų atvejų:

- (1) jei asmeninė informacija, kurią tvarkant reikia informuoti duomenų subjektą, yra įtraukta į bet kurią iš įstatymo 32 straipsnio 2 dalyje nurodytų asmeninės informacijos bylų, jei šios nuostatos saugomi interesai yra akivaizdžiai viršesni už duomenų subjekto teises ir tik tol, kol informavimas keltų grėsmę tų interesų įgyvendinimui, būtų kliudoma vykstantiems kriminaliniams tyrimams arba keliama grėsmė nacionaliniam saugumui;
- (2) jei ir tol, kol pranešus gali kilti grėsmė asmens ar kito subjekto gyvybei ar fizinei sveikatai arba gali būti nepagrįstai pažeisti kito subjekto turciniai interesai, kai tos teisės ar interesai yra akivaizdžiai viršesni už duomenų subjekto teises;
- (3) jei duomenų subjektas jau turi informaciją, kurią asmeninės informacijos valdytojas privalo jam pateikti pagal i arba ii punktus;
- (4) jei asmeninės informacijos valdytojas neturi jokios duomenų subjekto kontaktinės informacijos arba jam reikėtų dėti nepagrįstai dideles pastangas, kad susisiektų su duomenų subjektu, įskaitant atvejus, kai duomenys tvarkomi AIAI 3 skirsnyje nustatytais sąlygomis. Nustatant, ar įmanoma susisiekti su duomenų subjektu ir ar dėl to reikia dėti nepagrįstai dideles pastangas, atsižvelgiama į galimybę bendradarbiauti su duomenų eksportuotoju ES.

⁽⁶⁾ Prievolės pagal i, ii ir iii punktus taip pat taikomos, kai duomenų valdytojas, kuris gauna asmeninę informaciją iš ES remiantis sprendimu dėl tinkamumo, tokią informaciją tvarko remdamasis kitais teisės aktais, pavyzdžiui, Kredito informacijos įstatymu.

4. **Informacijai, kuriai suteikti pseudonimai, taikomos specialios išimties taikymo sritis (įstatymo 28-2, 28-3, 28-4, 28-5, 28-6 ir 28-7 straipsniai, 3 ir 58-2 straipsniai)**

<Asmeninės informacijos apsaugos įstatymas

(įstatymas Nr. 16930, iš dalies pakeistas 2020 m. vasario 4 d.)>

III skyrius. Asmeninės informacijos tvarkymas

3 SKIRSNIS. Ypatingi atvejai, susiję su duomenimis, kuriems suteikti pseudonimai

28-2 straipsnis (Duomenų, kuriems suteikti pseudonimai, tvarkymas). 1) Asmeninės informacijos valdytojas gali tvarkyti informaciją, kuriai suteikti pseudonimai, be duomenų subjektų sutikimo, kai ji tvarkoma viešojo intereso pagrindu statistikos, mokslinių tyrimų ir archyvavimo tikslais, ir kt.

2) Asmeninės informacijos valdytojas, trečiajai šaliai teikdamas informaciją, kuriai suteikti pseudonimai, pagal 1 dalį, į ją neįtraukia informacijos, kuri gali būti naudojama tam tikro asmens tapatybei nustatyti.

28-3 straipsnis (Duomenų, kuriems suteikti pseudonimai, sujungimo apribojimas). 1) Nepaisant 28-2 straipsnio, skirtingų asmeninės informacijos valdytojų tvarkomos informacijos, kuriai suteikti pseudonimai, sujungimą siekiant ją viešojo intereso pagrindu tvarkyti statistikos, mokslinių tyrimų, įrašų saugojimo tikslais ir kt. atlieka Apsaugos komisijos arba susijusios centrinės administracinės įstaigos vadovo paskirta specializuota institucija.

2) Asmeninės informacijos valdytojas, ketinantis sujungtą informaciją paskelbti už informaciją sujungusios organizacijos ribų, sutvarkęs informaciją suteikdamas jai pseudonimus arba 58-2 straipsnyje nurodytą formą, turi gauti specializuotos institucijos vadovo sutikimą.

3) Būtinai aspektai, įskaitant sujungimo procedūras ir metodus pagal 1 dalį, standartus ir procedūras, kurias taikant valdymo ir priežiūros tikslais paskiriama arba atšaukiama specializuota institucija, ir eksportavimo bei patvirtinimo standartus ir procedūras pagal 2 dalį, nustatomi Prezidento dekretu.

28-4 straipsnis (Pareiga imtis saugumo priemonių dėl duomenų, kuriems suteikti pseudonimai). 1) Tvarkydamas informaciją, kuriai suteikti pseudonimai, asmeninės informacijos valdytojas imasi tokių techninių, organizacinių ir fizinių priemonių, kaip antai atskiras papildomos informacijos, reikalingos siekiant atkurti pradinę jos būklę, saugojimas ir tvarkymas, kurių gali prireikti siekiant užtikrinti jos saugumą, kaip nurodyta Prezidento dekretu, užkertant kelią asmeninės informacijos praradimui, pavogimui, atskleidimui, suklastojimui, pakeitimui ar sugadinimui.

2) Asmeninės informacijos valdytojas, ketinantis tvarkyti informaciją, kuriai suteikti pseudonimai, rengia ir saugo įrašus, susijusius su Prezidento dekretu nustatytais aspektais, įskaitant apie informacijos, kuriai suteikti pseudonimai, tvarkymo tikslą, ir trečiąją šalimi, kai informacija, kuriai suteikti pseudonimai, jai teikiama, kad galėtų valdyti informacijos, kuriai suteikti pseudonimai, tvarkymą.

28-5 straipsnis (Draudžiami veiksmai tvarkant informaciją, kuriai suteikti pseudonimai). 1) Niekas negali tvarkyti informacijos, kuriai suteikti pseudonimai, su tikslu nustatyti tam tikro asmens tapatybę.

2) Kai apdorojant informaciją, kuriai suteikti pseudonimai, sukuriama informacija, kurią naudojant galima nustatyti tam tikro asmens tapatybę, asmeninės informacijos valdytojas turi nutraukti informacijos tvarkymą, informaciją nedelsiant atgauti ir sunaikinti.

28-6 straipsnis (Papildomų administracinių mokesčių taikymas už informacijos, kuriai suteikti pseudonimai, tvarkymą). 1) Duomenų valdytojui, kuris tvarkė duomenis siekdamas nustatyti konkretaus asmens tapatybę pažeisdamas 28-5 straipsnio 1 dalį, Komisija gali skirti baudą, kurios suma mažesnė nei trys šimtosios visų jo pardavimų sumos; su sąlyga, kad tuo atveju, kai pardavimų nėra arba sunku apskaičiuoti pardavimų pajamas, duomenų valdytojui gali būti skirta bauda, lygi didesniajai iš dviejų sumų: 400 milijonų vonų arba trys šimtosios kapitalo sumos.

2) 34-2 straipsnio 3–5 dalys *mutatis mutandis* taikomos aspektams, būtiniams siekiant taikyti ir surinkti papildomus administracinius mokesčius.

28-7 straipsnis (Taikymo sritis). 20, 21 ir 27 straipsniai, 34 straipsnio 1 dalis, 35–37 straipsniai, 39-3 ir 39-4 straipsniai, 39-6–39-8 straipsniai netaikomi informacijai, kuriai suteikti pseudonimai.

I skyrius. Bendrosios nuostatos

3 straipsnis (Asmeninės informacijos apsaugos principai). 1) Asmeninės informacijos valdytojas aiškiai nurodo, kokiais tikslais tvarkoma asmeninė informacija; ir teisėtai bei sąžiningai renka tokią asmeninės informacijos kiekį, kuris yra būtinas tokiems tikslams pasiekti.

2) Asmeninės informacijos valdytojas asmeninę informaciją tvarko tinkamai, kaip būtina tikslams, kurių pagrindu ji tvarkoma, pasiekti, ir nenaudoja jos jokiais kitais tikslais.

- 3) Asmeninės informacijos valdytojas užtikrina, kad asmeninė informacija būtų tiksli, išsami ir atnaujinta tiek, kiek tai būtina, atsižvelgiant į asmeninės informacijos tvarkymo tikslus.
- 4) Asmeninės informacijos valdytojas asmeninę informaciją tvarko saugiai, taikydamas asmeninės informacijos tvarkymo metodus, rūšis ir t. t. bei atsižvelgdamas į duomenų subjektų teisių pažeidimo galimybę ir susijusių pavojų mastą.
- 5) Asmeninės informacijos valdytojas viešai skelbia savo privatumo politiką ir kitą su asmeninės informacijos tvarkymu susijusią informaciją; ir užtikrina duomenų subjekto teisių, kaip antai teisės susipažinti su savo asmenine informacija, įgyvendinimą.
- 6) Asmeninės informacijos valdytojas asmeninę informaciją tvarko taip, kad galimybė pažeisti duomenų subjekto privatumą būtų kuo mažesnė.
- 7) Jei tvarkant nuasmenintą informaciją arba informaciją, kuriai suteikti pseudonimai, vis tiek įmanoma pasiekti asmeninės informacijos rinkimo tikslus, asmeninės informacijos valdytojas turi stengtis asmeninę informaciją tvarkyti ją nuasmeninęs, jei ją įmanoma nuasmeninti, arba jai suteikęs pseudonimus, jei asmeninės informacijos rinkimo tikslų neįmanoma pasiekti tvarkant nuasmenintą informaciją.
- 8) Asmeninės informacijos valdytojas turi stengtis įgyti duomenų subjektų pasitikėjimą atsižvelgdamas į tokias pareigas ir užduotis ir jas vykdydamas, kaip numatyta šiame įstatyme ir kituose susijusiuose įstatymuose.

IX skyrius. Papildomos nuostatos

58-2 straipsnis (Atleidimas nuo taikymo). Šis įstatymas netaikomas informacijai, kurią sujungus su kita informacija nebeįmanoma nustatyti tam tikro asmens tapatybės, pagrįstai atsižvelgiant į laiką, sąnaudas, technologijas ir kt. <Šis straipsnis naujai įtrauktas 2020 m. vasario 4 d. įstatymu Nr. 16930>

- i) Pagal III skyriaus 3 skirsnį (Ypatingi atvejai, susiję su duomenimis, kuriems suteikti pseudonimai) (28-2–28-7 straipsniai) leidžiama be duomenų subjekto sutikimo tvarkyti informaciją, kuriai suteikti pseudonimai, statistikos rengimo, mokslinių tyrimų vykdymo, viešųjų įrašų saugojimo tikslais ir kt. (28-2 straipsnis), tačiau tokiais atvejais privaloma užtikrinti atitinkamas apsaugos priemones ir taikyti draudimus, būtinus duomenų subjektų teisėms apsaugoti (28-4 ir 28-5 straipsniai), pažeidėjams gali būti taikomos baudos (28-6 straipsnis), o tam tikros apsaugos priemonės, kitais atvejais taikomos pagal AIAĮ, nėra taikomos (28-7 straipsnis).
- ii) Šios nuostatos netaikomos tais atvejais, kai informacija, kuriai suteikti pseudonimai, tvarkoma kitais tikslais nei statistikos rengimo, mokslinių tyrimų vykdymo, viešųjų įrašų saugojimo ir kt. Pavyzdžiui, jei ES esančio asmens asmeninei informacijai, kuri buvo perduota į Korėją pagal Europos Komisijos sprendimą dėl tinkamumo, yra suteikti pseudonimai kitais nei statistikos rengimo, mokslinių tyrimų vykdymo, viešųjų įrašų saugojimo ir kt. tikslais, specialiosios III skyriaus 3 skirsnio nuostatos netaikomos (7).
- iii) Kai asmeninės informacijos valdytojas tvarko informaciją, kuriai suteikti pseudonimai, statistikos rengimo, mokslinių tyrimų vykdymo, viešųjų įrašų saugojimo ir kt. tikslais ir jei informacija, kuriai suteikti pseudonimai, nebuvo sunaikinta pasiekus konkretų tvarkymo tikslą pagal Konstitucijos 37 straipsnį ir įstatymo 3 straipsnį (Asmeninės informacijos apsaugos principai), jis nuasmenina informaciją siekdamas užtikrinti, kad ją naudojant, vieną ar sujungtą su kita informacija, nebebūtų įmanoma nustatyti konkretaus asmens tapatybės, pagrįstai atsižvelgiant į tam reikalingą laiką, išlaidas, technologijas ir kt. pagal AIAĮ 58-2 straipsnį.

5. Taisomieji veiksmai ir kt. (įstatymo 64 straipsnio 1, 2 ir 4 dalys)

<Asmeninės informacijos apsaugos įstatymas

(įstatymas Nr. 16930, iš dalies pakeistas 2020 m. vasario 4 d.)>

64 straipsnis (Taisomieji veiksmai). 1) Jei Apsaugos komisija turi rimtą pagrindą manyti, kad buvo padarytas su asmenine informacija susijęs pažeidimas, o nesiėmus veiksmų gali būti padaryta žala, kurią sunku ištaisyti, ji gali įpareigoti šio įstatymo pažeidėją (išskyrus centrinės administracinės agentūros, vietos valdžios institucijas, Nacionalinę Asamblėją, teismą, Konstitucinį Teismą ir Nacionalinę rinkimų komisiją) imtis šių veiksmų:

1. nebevykdyti su asmenine informacija susijusio pažeidimo;
2. laikinai sustabdyti asmeninės informacijos tvarkymą;

(7) Kredito informacijos įstatymo 40-3 straipsnio išimtis taip pat taikoma tik tada, kai kredito informacija, kuriai suteikti pseudonimai, tvarkoma statistikos rengimo, mokslinių tyrimų vykdymo ir viešųjų įrašų saugojimo tikslais.

3. kitų veiksmų, būtinų asmeninei informacijai apsaugoti ir užkirsti kelią asmeninės informacijos pažeidimui.

2) Jei susijusios centrinės administracinės agentūros vadovas turi rimtą pagrindą manyti, kad buvo pažeistas asmeninės informacijos saugumas, o nesiėmus veiksmų gali būti padaryta žala, kurią sunku ištaisyti, jis gali įpareigoti asmeninės informacijos valdytoją imtis bet kurių 1 dalyje numatytų veiksmų pagal įstatymus, priklausančius tokios susijusios centrinės administracinės agentūros jurisdikcijai.

4) Jei centrinė administracinė agentūra, vietos valdžios institucija, Nacionalinė Asamblėja, teismas, Konstitucinis Teismas ar Nacionalinė rinkimų komisija pažeidžia šį įstatymą, Apsaugos komisija gali rekomenduoti atitinkamos įstaigos vadovui imtis bet kurių iš 1 dalyje numatytų veiksmų. Tokiais atvejais agentūra gavusi rekomendaciją ją vykdo, išskyrus atvejus, kai tai neįmanoma dėl ypatingų aplinkybių.

- i) Visų pirma teismų praktikoje ⁽⁸⁾ ⁽⁹⁾ „žala, kurią sunku ištaisyti“ aiškinama kaip atvejis, kai galima pakenkti asmens asmeninėms teisėms arba privatumui.
- ii) Todėl 64 straipsnio 1 ir 2 dalyse nustatyta, kad „turi rimtą pagrindą manyti, kad buvo pažeistas asmeninės informacijos saugumas, o nesiėmus veiksmų gali būti padaryta žala, kurią sunku ištaisyti“ reiškia atvejus, kai pažeidus įstatymą gali būti pažeistos asmenų teisės ir laisvė, susiję su asmenine informacija. Tai bus taikoma visais atvejais, kai bus pažeisti bet kokie įstatyme nustatyti principai, teisės ir pareigos, kuriais siekiama apsaugoti asmeninę informaciją ⁽¹⁰⁾.
- iii) Pagal Asmeninės informacijos apsaugos įstatymo 64 straipsnio 4 dalį tai veiksma, skirtas taikyti „šio įstatymo pažeidimo“ atveju, t. y. veiksma, taikytinas AIAI pažeidimo atveju.

Centrinė administracinė agentūra ir kt., būdamos valdžios institucijomis, kurios privalo laikytis teisinės valstybės principo, negali pažeisti jokio įstatymo ir privalo imtis taisomųjų veiksmų, įskaitant nedelsiant nutraukti veiksmus ir atlyginti žalą, jei išimtinu atveju neteisėtai veiklos vis dėlto buvo imtasi.

Atitinkamai, net ir nesikišant Apsaugos komisijai, pagal AIAI 64 straipsnio 4 dalį centrinė administracinė agentūra ir kt., sužinojusios apie įstatymo pažeidimą, privalo imtis su pažeidimu susijusių taisomųjų veiksmų.

Visų pirma tais atvejais, kai Apsaugos komisija rekomendavo taisomąją priemonę, centrinei administracinei agentūrai ir kt. paprastai bus objektyviai aišku, kad jos pažeidė įstatymą. Taigi centrinė administracinė agentūra ir kt., siekdamos pagrįsti, kodėl jų manymu neturėtų būti vykdoma Apsaugos komisijos rekomendacija, turi pateikti aiškų pagrindą, kuriuo remiantis įrodoma, kad jos nepažeidė įstatymo. Rekomendacija turi būti vykdoma, išskyrus atvejus, kai Apsaugos komisija nusprendžia, kad įstatymas iš tiesų nepažeistas.

Atsižvelgiant į tai, Asmeninės informacijos apsaugos įstatymo 64 straipsnio 4 dalyje nurodytos „ypatingos aplinkybės“ turi būti griežtai taikomos tik ypatingomis aplinkybėmis, kurioms esant centrinės administracinės agentūros ir kt. turi aiškų pagrindą, kuriuo remiantis galima įrodyti, kad „šis įstatymas iš tiesų nebuvo pažeistas“, pavyzdžiui, „atvejai, kai yra ypatingų (faktinių ar teisinių) aplinkybių“, kurių Apsaugos komisija, pateikdama savo rekomendaciją, nežinojo, o Apsaugos komisija nustato, kad pažeidimas iš tikrųjų nebuvo padarytas.

6. AIAI taikymas tvarkant asmens duomenis nacionalinio saugumo tikslais, įskaitant pažeidimų tyrimą ir vykdymo užtikrinimą pagal AIAI (AIAI 7-8, 7-9, 58, 3, 4 ir 62 straipsniai)

<Asmeninės informacijos apsaugos įstatymas

(įstatymas Nr. 16930, iš dalies pakeistas 2020 m. vasario 4 d.)>

7-8 straipsnis (Apsaugos komisijos funkcijos). 1) Apsaugos komisija atlieka šias funkcijas: [...]

3. vykdo su duomenų subjektų teisių pažeidimu susijusius tyrimus ir priima su jais susijusius sprendimus;

4. nagrinėja su asmeninės informacijos tvarkymu susijusius skundus arba taiko taisomąsias procedūras ir tarpininkauja ginčuose dėl asmeninės informacijos;

[...]

⁽⁸⁾ (1999 m. sausio 26 d. Aukščiausiojo Teismo sprendimas 97Da10215,10222). Žiniasklaidai atskleidus informaciją apie kaltinamojo įvykdytą nusikalstamą veiklą gali būti padaryta nepataisoma psichinė ir fizinė žala ne tik nukentėjusiajam, t. y. ieškovui, bet ir jo aplinkai priklausantiems asmenims, įskaitant šeimas.

⁽⁹⁾ (2008 m. sausio 16 d. Seulo Aukštojo Teismo sprendimas 2006Na92006). Išleidus straipsnį, kuriame asmuo apšmeižiamas, tam asmeniui gali būti padaryta didelė nepataisoma žala.

⁽¹⁰⁾ Tokie patys principai, kaip nustatyti ši punkte, taikomi Kredito informacijos įstatymo 45-4 straipsnio atveju.

7-9 straipsnis (Apsaugos komisijos sprendimai ir nutarimai). 1) Apsaugos komisija sprendžia ir priima nutarimus dėl šių klausimų: [...]

5. teisės aktų, susijusių su asmeninės informacijos apsauga, aiškinimo ir įgyvendinimo;

[...]

58 straipsnis (Dalinis netaikymas). 1) III–VII skyriai netaikomi šiems asmens duomenims:

1. asmeninei informacijai, kuri renkama pagal Statistikos įstatymą, kad ją galėtų tvarkyti viešosios institucijos;
2. asmeninei informacijai, kuri renkama arba kurią prašoma pateikti siekiant analizuoti su nacionaliniu saugumu susijusią informaciją;
3. asmeninei informacijai, kuri laikinai tvarkoma, kai tai neišvengiamai būtina, siekiant užtikrinti visuomenės saugumą, sveikatą ir pan.;
4. asmeninei informacijai, kuri surinkta arba naudojama atitinkamai spaudos atstovų vykdant žurnalistinę veiklą, religinių organizacijų vykdant misionierių veiklą ir politinių partijų keliant kandidatus.

[2 ir 3 punktai praleisti]

4) Asmeninės informacijos valdytojas, tvarkydamas asmeninę informaciją pagal 1 punktą, ją tvarko tiek, kiek tai būtina numatytam tikslui pasiekti per trumpiausią laikotarpį; taip pat imasi būtinų priemonių, pavyzdžiui, techninių, valdymo ir fizinių apsaugos priemonių, individualių skundų nagrinėjimo ir kitų būtinų priemonių, kad tokia asmeninė informacija būtų saugiai valdoma ir tinkamai tvarkoma.

3 straipsnis (Asmeninės informacijos apsaugos principai). 1) Asmeninės informacijos valdytojas aiškiai nurodo, kokiais tikslais tvarkoma asmeninė informacija; ir teisėtai bei sąžiningai renka tokį asmeninės informacijos kiekį, kuris yra būtinas tokiems tikslams pasiekti.

2) Asmeninės informacijos valdytojas asmeninę informaciją tvarko tinkamai, kaip būtina tikslams, kurių pagrindu ji tvarkoma, pasiekti, ir nenaudoja jos jokiais kitais tikslais.

3) Asmeninės informacijos valdytojas užtikrina, kad asmeninė informacija būtų tiksli, išsami ir atnaujinta tiek, kiek tai būtina, atsižvelgiant į asmeninės informacijos tvarkymo tikslus.

4) Asmeninės informacijos valdytojas asmeninę informaciją tvarko saugiai, taikydamas asmeninės informacijos tvarkymo metodus, rūšis ir t. t. bei atsižvelgdamas į duomenų subjektų teisių pažeidimo galimybę ir susijusių pavojų mastą.

5) Asmeninės informacijos valdytojas viešai skelbia savo privatumo politiką ir kitą su asmeninės informacijos tvarkymu susijusią informaciją; ir užtikrina duomenų subjekto teisių, kaip antai teisės susipažinti su savo asmenine informacija, įgyvendinimą.

6) Asmeninės informacijos valdytojas asmeninę informaciją tvarko taip, kad galimybė pažeisti duomenų subjekto privatumą būtų kuo mažesnė.

7) Jei tvarkant nuasmenintą informaciją arba informaciją, kuriai suteikti pseudonimai, vis tiek įmanoma pasiekti asmeninės informacijos rinkimo tikslus, asmeninės informacijos valdytojas turi stengtis asmeninę informaciją tvarkyti ją nuasmeninęs, jei ją įmanoma nuasmeninti, arba jai suteikęs pseudonimus, jei asmeninės informacijos rinkimo tikslų neįmanoma pasiekti tvarkant nuasmenintą informaciją.

8) Asmeninės informacijos valdytojas turi stengtis įgyti duomenų subjektų pasitikėjimą atsižvelgdamas į tokias pareigas ir užduotis ir jas vykdydamas, kaip numatyta šiame įstatyme ir kituose susijusiuose įstatymuose.

4 straipsnis (Duomenų subjektų teisės). Duomenų subjektas turi šias su jo asmens informacijos tvarkymu susijusias teises:

1. teisę būti informuotam apie tokios asmeninės informacijos tvarkymą;
2. teisę duoti arba neduoti sutikimą ir nustatyti sutikimo dėl tokios asmens informacijos tvarkymo taikymo sritį;
3. teisę gauti patvirtinimą, ar asmeninė informacija yra tvarkoma, ir prašyti susipažinti su tokia asmenine informacija (įskaitant pateikti kopijas; toliau taikoma tas pats);
4. teisę sustabdyti tokios asmeninės informacijos tvarkymą ir reikalauti ištaisyti, ištrinti ir sunaikinti tokią asmeninę informaciją;
5. teisę į tinkamą žalą, sukeltą tvarkant tokią asmeninę informaciją, atlyginimą taikant savalaikę ir sąžiningą procedūrą.

62 straipsnis (Pranešimas apie pažeidimus). 1) Bet koks asmuo, kurio teisės ar interesai, susiję su jo asmenine informacija, buvo pažeisti asmens duomenų valdytojui tvarkant asmeninę informaciją, gali pranešti apie tokį pažeidimą Apsaugos komisijai.

2) Siekdama, kad skundų, pateiktų pagal 1 dalį, gavimas ir tvarkymas būtų veiksmingas, Apsaugos komisija gali paskirti specializuotą instituciją, kaip nustatyta Prezidento dekretu. Tokiais atvejais tokia specializuota institucija įsteigta ir valdo asmeninės informacijos pažeidimams skirtą skambučių centrą (toliau – privatumo apsaugos skambučių centras).

3) Privatumo apsaugos skambučių centras atlieka šias pareigas:

1. priima skundus ir teikia konsultacijas asmeninės informacijos tvarkymo klausimais;
2. tiria ir patvirtina atvejus bei išklauso susijusių šalių nuomones;
3. atlieka pareigas, susijusias su pareigomis, nurodytomis 1 ir 2 punktuose.

4) Prireikus pagal Valstybės pareigūnų įstatymo 32-4 straipsnį Apsaugos komisija gali skirti valstybės pareigūną, kad specializuotoje institucijoje, paskirtoje vadovaujantis 2 punktu, pagal 3 straipsnio 2 dalį būtų veiksmingai iširti ir patvirtinti atvejai.

- i) Asmeninės informacijos rinkimas nacionalinio saugumo tikslais reglamentuojamas specialiais įstatymais, kuriais kompetentingoms institucijoms (pvz., Nacionalinei žvalgybos tarnybai) suteikiami įgaliojimai perimti ryšių informaciją arba prašyti atskleisti informaciją taikant tam tikras sąlygas ir apsaugos priemones (toliau – nacionalinio saugumo įstatymai). Šie nacionalinio saugumo įstatymai yra, pavyzdžiui, Ryšių privatumo apsaugos įstatymas, Įstatymas dėl kovos su terorizmu siekiant apsaugoti piliečius ir užtikrinti viešąjį saugumą arba Telekomunikacijų įmonių įstatymas. Be to, asmeninės informacijos rinkimas ir tolesnis tvarkymas turi atitikti AIAĮ reikalavimus. Šiuo atžvilgiu AIAĮ 58 straipsnio 1 dalies 2 punkte numatoma, kad III–VII skyriai netaikomi asmeninei informacijai, kuri renkama arba kurią prašoma pateikti siekiant analizuoti su nacionaliniu saugumu susijusią informaciją. Todėl ši dalinė išimtis taikoma asmeninę informaciją tvarkant nacionalinio saugumo tikslais.

Tuo pat metu tvarkant tokią asmeninę informaciją taikomi AIAĮ I skyrius (Bendrosios nuostatos), II skyrius (Asmeninės informacijos apsaugos politikos nustatymas ir kt.), VIII skyrius (Kolektyvinis ieškinys dėl duomenų saugumo pažeidimo), IX skyrius (Papildomos nuostatos) ir X skyrius (Nuostatos dėl sankcijų). Tai apima bendruosius duomenų apsaugos principus, nustatytus AIAĮ 3 straipsnyje (Asmeninės informacijos apsaugos principai), ir asmens teises, užtikrinamas 4 straipsniu (Duomenų subjektų teisės).

Be to, AIAĮ 58 straipsnio 4 dalyje nustatyta, kad tokia informacija turi būti tvarkoma tiek, kiek būtina numatytam tikslui pasiekti per trumpiausią laikotarpį; joje taip pat nustatytas reikalavimas asmeninės informacijos valdytojui taikyti reikiamas priemones, kad būtų užtikrinamas saugus duomenų valdymas ir tinkamas jų tvarkymas, pavyzdžiui, technines, valdymo ir fizines apsaugos priemones, taip pat priemones, kuriomis būtų užtikrinamas tinkamas individualių skundų nagrinėjimas.

Galiausiai taikomos nuostatos, kuriomis reglamentuojamos AIAK užduotys ir įgaliojimai (įskaitant AIAĮ 60-65 straipsnį dėl skundų nagrinėjimo ir rekomendacijų bei taisomųjų veiksmų priėmimo), taip pat nuostatos dėl administracinių ir baudžiamųjų sankcijų (AIAĮ 70 ir tolesni straipsniai). Pagal AIAĮ 7-8 straipsnio 1 dalies 3 ir 4 punktus ir 7-9 straipsnio 1 dalies 5 punktą šie tiriamojo ir taisomojo pobūdžio įgaliojimai, įskaitant atvejus, kai jie naudojami nagrinėjant skundus, taip pat taikomi galimų konkrečiuose įstatymuose, kaip antai nacionalinio saugumo įstatymuose, pateiktų taisyklių, kuriomis nustatomi apribojimai ir apsaugos priemonės, susijusios su asmeninės informacijos rinkimu, pažeidimų atveju. Atsižvelgiant į AIAĮ 3 straipsnio 1 dalyje nustatytus reikalavimus dėl teisėto ir sąžiningo asmeninės informacijos rinkimo, toks pažeidimas taip pat yra „šio įstatymo“ pažeidimas, kaip tai apibrėžta 63 ir 64 straipsniuose, todėl AIAK leidžiama atlikti tyrimą ir taikyti taisomuosius veiksmus⁽¹⁾. Šiais AIAK įgaliojimais papildomi, bet ne pakeičiami Nacionalinės žmogaus teisių komisijos įgaliojimai pagal Žmogaus teisių komisijos įstatymą.

Pagrindiniais AIAĮ principais, teisėmis ir pareigomis, taikomais tvarkant asmeninę informaciją nacionalinio saugumo tikslais, atspindimos Konstitucijoje įtvirtintos garantijos dėl asmens teisės valdyti savo asmeninę informaciją apsaugos. Kaip pripažįsta Konstitucinis Teismas, tai, be kita ko, yra asmens teisė⁽²⁾ „asmeniškai nuspręsti, kada ir kam jo asmeninė informacija gali būti atskleista arba ja leidžiama naudotis arba kas ir koku mastu ją gali atskleisti arba naudoti. Tai yra pagrindinė teisė⁽³⁾, [...], kuria siekiama apsaugoti asmens apsisprendimo laisvę nuo grėsmės, kylančios dėl valstybės funkcijų išplėtimo ir informacinių ryšių technologijų“. Norint taikyti bet kokią tos teisės apribojimą, pavyzdžiui, kai tai būtina nacionaliniam saugumui užtikrinti, reikia suderinti asmens teises ir interesus su atitinkamu viešuoju interesu ir toks apribojimas negali turėti įtakos esminių šios teisės aspektų įgyvendinimui (Konstitucijos 37 straipsnio 2 dalis).

⁽¹⁾ Dėl taisomųjų veiksmų pagal 64 straipsnį taip pat žr. 5 skirsnį.

⁽²⁾ 2005 m. gegužės 26 d. Konstitucinio Teismo sprendimas 99HunMa513, 2004HunMa190.

⁽³⁾ 2005 m. liepos 21 d. Konstitucinio Teismo sprendimas 2003HunMa282.

Todėl tvarkydamas asmeninę informaciją nacionalinio saugumo tikslais duomenų valdytojas (pvz., NŽT) privalo, *inter alia*:

- 1) aiškiai nurodyti tikslus, kurių pagrindu asmeninė informacija tvarkoma, ir teisėtai bei sąžiningai rinkti tokią asmeninės informacijos kiekį, kokio reikia tokiems tikslams pasiekti (AIAĮ 3 straipsnio 1 dalis); konkrečiai, jis renka ir toliau tvarko asmeninę informaciją tik tam, kad atliktų pareigas pagal atitinkamus įstatymus, kaip antai Nacionalinės žvalgybos tarnybos įstatymą;
 - 2) tvarkyti tik tokią asmeninės informacijos kiekį ir tik tol, kol tai būtina numatytam tikslui pasiekti (AIAĮ 58 straipsnio 4 dalis); pasiekęs tvarkymo tikslą duomenų valdytojas negrįžtamai sunaikina asmeninę informaciją, išskyrus atvejį, kai jis įstatymu konkrečiai įpareigojamas ją toliau saugoti; tokiu atveju atitinkama asmeninė informacija saugoma ir tvarkoma atskirai nuo kitos asmeninės informacijos, nenaudojama kitais nei įstatyme nurodytais tikslais ir sunaikinama pasibaigus saugojimo laikotarpiui;
 - 3) tinkamai tvarkyti asmeninę informaciją, kaip būtina tikslams, kurių pagrindu ji tvarkoma, pasiekti, ir nenaudoja jos jokiais kitais tikslais (AIAĮ 3 straipsnio 2 dalis);
 - 4) užtikrinti, kad asmeninė informacija būtų tiksli, išsami ir atnaujinta tiek, kiek tai būtina, atsižvelgiant į asmeninės informacijos tvarkymo tikslus (AIAĮ 3 straipsnio 3 dalis);
 - 5) saugiai tvarkyti asmeninę informaciją, taikant asmeninės informacijos tvarkymo metodus, rūšis ir t. t. bei atsižvelgiant į duomenų subjektų teisių pažeidimo galimybę ir susijusių pavojų mastą (AIAĮ 3 straipsnio 4 dalis);
 - 6) paskelbti savo privatumo politiką ir kitą su asmeninės informacijos tvarkymu susijusią informaciją (AIAĮ 3 straipsnio 5 dalis);
 - 7) tvarkyti asmeninę informaciją tokiu būdu, kad būtų kuo labiau sumažinta galimybė pažeisti duomenų subjekto privatumą (AIAĮ 3 straipsnio 6 dalis).
- ii) Pagal AIAĮ 58 straipsnio 4 dalį duomenų valdytojas (pvz., už nacionalinį saugumą atsakingos institucijos, kaip antai NŽT) imasi reikiamų priemonių, pavyzdžiui, taiko technines, valdymo ir fizines apsaugos priemones, kad užtikrintų šių principų laikymąsi ir tinkamą asmeninės informacijos tvarkymą. Tai, pavyzdžiui, gali apimti specialias priemones, kuriomis užtikrinamas asmeninės informacijos saugumas, kaip antai priegios prie asmeninės informacijos apribojimą, priegios kontrolę ir žurnalus, tikslinį darbuotojų mokymą asmeninės informacijos tvarkymo tema ir kt.

Be to, pagal AIAĮ 3 straipsnio 5 dalį ir 4 straipsnį duomenų subjektai, *inter alia*, turi šias teises, susijusias su nacionalinio saugumo tikslais tvarkoma asmenine informacija:

- 1) teisę gauti patvirtinimą, ar jo asmeninė informacija yra tvarkoma, taip pat informaciją apie tvarkymą, ir susipažinti su ta informacija, įskaitant gauti jos kopijas (AIAĮ 4 straipsnio 1 ir 3 dalys);
 - 2) teisę sustabdyti asmeninės informacijos tvarkymą ir reikalauti ją ištaisyti, ištrinti bei sunaikinti (AIAĮ 4 straipsnio 4 dalis).
- iii) Duomenų subjektas, naudodamasis šiomis teisėmis, gali pateikti prašymą tiesiogiai duomenų valdytojui arba netiesiogiai per Apsaugos komisiją ir tai padaryti gali įgalioti savo atstovą. Duomenų subjektui pateikus prašymą, duomenų valdytojas nedelsdamas suteikia teisę; su sąlyga, kad jis gali laikinai neleisti, apriboti arba neleisti naudotis teise, jei tai numatyta kituose įstatymuose arba būtina siekiant jų laikytis, tiek ir tol, kol tai būtina siekiant apsaugoti svarbų viešojo intereso tikslą ir kai šie veiksmai yra jam proporcingi (pavyzdžiui, tiek ir tol, kol teisės suteikimu būtų trukdoma vykstančiam tyrimui arba dėl jo kiltų grėsmė nacionaliniam saugumui), arba kai teisės suteikimas galėtų kelti pavojų trečiosios šalies gyvybei ar fizinei sveikatai arba ją suteikus būtų nepagrįstai pažeidžiami trečiosios šalies turtiniai ir kiti interesai. Jei prašymas atmetamas arba apribojamas, duomenų subjektui turi būti nedelsiant pranešama apie to priežastis. Duomenų valdytojas nustato duomenų subjektams skirtą prašymų teikimo būdą ir parengia jų teikimo tvarką ir juos viešai paskelbia, kad apie juos sužinotų duomenų subjektai.

Be to, pagal AIAĮ 58 straipsnio 4 dalį (reikalavimas užtikrinti tinkamą individualių skundų nagrinėjimą) ir AIAĮ 4 straipsnio 5 dalį (teisė į tinkamą teisių gynimą patyrus žalą dėl asmeninės informacijos tvarkymo, taikant savalaikę ir sąžiningą procedūrą) duomenų subjektai turi teisę į teisių gynimą. Tai, be kita ko, yra teisė apie tariamą pažeidimą pranešti Pranešimų apie asmeninės informacijos saugumo pažeidimą centrui (pagal AIAĮ 62 straipsnio 3 dalį), pateikti skundą AIAK pagal AIAĮ 62 straipsnį dėl bet kokio teisių ar interesų, susijusių su asmens asmenine informacija, pažeidimo ir ginti savo teises teisme, apskundžiant AIAK sprendimą ar neveikimą pagal Administracinių ginčų įstatymą. Be to, duomenų subjektai gali ginti savo teises teisme pagal Administracinių ginčų įstatymą, jei dėl duomenų valdytojo sprendimo ar neveikimo buvo pažeistos jų teisės ar interesai (pvz., neteisėtai renkant asmens duomenis), arba gauti žalos atlyginimą pagal Valstybės kompensacijų įstatymą. Šiomis teisių gynimo priemonėmis galima pasinaudoti ir tuo atveju, jei pažeidžiamos taisyklės, nustatytos konkrečiuose įstatymuose, kuriais nustatomi apribojimai ir apsaugos priemonės, susijusios su asmeninės informacijos rinkimu, kaip antai nacionalinio saugumo įstatymuose, ir AIAĮ.

Asmuo iš ES gali pateikti skundą AIAK per savo nacionalinę duomenų apsaugos instituciją, o kai tyrimas baigiamas ir pritaikomi taisomieji veiksmai (jei taikomi), AIAK informuos asmenį per nacionalinę duomenų apsaugos instituciją.

II PRIEDAS

2021 m. gegužės 18 d.

Jo Ekscelencijai p. Didier Reynders, už teisingumą atsakingam Europos Komisijos nariui

Jūsų Ekscelencija,

Palankiai vertinu konstruktyvias Korėjos ir Europos Komisijos diskusijas, kuriomis siekiama sukurti asmens duomenų perdavimo iš ES į Korėją sistemą.

Europos Komisijos Korėjos Vyriausybei nusiųstu prašymu pateikiu pridedamą dokumentą, kuriame apžvelgiama Korėjos Vyriausybės prieigos prie informacijos teisinė sistema.

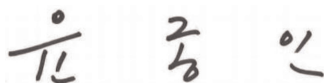
Šis dokumentas susijęs su ne viena Korėjos Vyriausybės ministerija ir agentūra, todėl už atskirų šio dokumento turinio dalių parengimą, atsižvelgiant į jų atitinkamas kompetencijos sritis, atsakingos atitinkamos ministerijos ir agentūros (Asmeninės informacijos apsaugos komisija, Teisingumo ministerija, Nacionalinė žvalgybos tarnyba, Korėjos nacionalinė žmogaus teisių komisija, Nacionalinis kovos su terorizmu centras, Korėjos finansinės žvalgybos padalinys). Toliau pateikiamas susijusių ministerijų bei agentūrų sąrašas ir atitinkami parašai.

Asmeninės informacijos apsaugos komisija priima visus su šiuo dokumentu susijusius klausimus ir užtikrins, kad visos atitinkamos ministerijos ir agentūros pateiktų į juos atsakymus.

Tikiuosi, kad šis dokumentas bus naudingas priimant sprendimus Europos Komisijoje.

Labai vertinu Jūsų iki šiol įneštą didžiulį indėlį.

Pagarbiai



Yoon Jong In
Asmeninės informacijos apsaugos komisijos pirmininkas

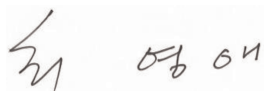
Šį dokumentą parengė Asmeninės informacijos apsaugos komisija ir šios susijusios ministerijos ir agentūros.



Park Jie Won
Nacionalinės žvalgybos tarnybos pirmininkas (direktorius)



Lee Jung Soo
Teisingumo ministerijos generalinis direktorius



Choi Young Ae
Korėjos nacionalinės žmogaus teisių komisijos pirmininkas



Kim Hyuck Soo
Nacionalinio kovos su terorizmu centro direktorius



Kim, Jeong Kag
Korėjos finansinės žvalgybos padalinio komisaras

Korėjos valdžios institucijų atliekamo asmens duomenų rinkimo ir naudojimo teisėsaugos ir nacionalinio saugumo tikslais teisinė sistema

Šiame dokumente apžvelgiama Korėjos valdžios institucijų atliekamo asmens duomenų rinkimo ir naudojimo baudžiamosios teisėsaugos ir nacionalinio saugumo tikslais teisinė sistema (toliau – *vyriausybės prieiga*), visų pirma, kiek tai susiję su galiojančiu teisiniu pagrindu, taikomomis sąlygomis (apribojimais) ir apsaugos priemonėmis, įskaitant nepriklausomą priežiūrą ir individualių teisių gynimo galimybes.

1. BENDRIEJI TEISĖS PRINCIPAI, SUSIJĘ SU VYRIAUSYBĖS PRIEIGA

1.1. Konstitucinė sistema

Korėjos Respublikos Konstitucijoje nustatyta bendra teisė į privatumą (17 straipsnis) ir konkreti teisė į ryšių privatumą (18 straipsnis). Valstybės pareiga – užtikrinti šias pagrindines teises⁽¹⁾. Konstitucijoje taip pat nustatyta, kad piliečių teisės ir laisvės gali būti ribojamos tik įstatymais ir tik tada, kai tai būtina nacionaliniam saugumui užtikrinti arba viešajai tvarkai palaikyti siekiant užtikrinti visuomenės gerovę⁽²⁾. Net kai tokie apribojimai taikomi, jie negali turėti įtakos esminiams laisvės ar teisės aspektams⁽³⁾. Korėjos teismai taikė šias nuostatas nagrinėjant bylas dėl vyriausybės atliekamo teisių į privatumą ribojimo. Pavyzdžiui, Aukščiausiasis Teismas konstatavo, kad stebint civilius gyventojus pažeidžiama pagrindinė teisė į privatumą, ir pabrėžė, kad piliečiai turi „teisę patys nuspręsti, ar informacija yra asmeninė“⁽⁴⁾. Kitoje byloje Konstitucinis Teismas konstatavo, kad privatumas yra pagrindinė teisė, kuria suteikiama apsauga nuo valstybės kišimosi į privatų piliečių gyvenimą ir jo stebėjimą⁽⁵⁾.

Be to, Korėjos Konstitucija garantuoja, kad asmuo gali būti suimamas, sulaikomas, apieškomas, tardomas arba jo daiktai gali būti paimami tik tada, kai tai nustatyta įstatymu⁽⁶⁾. Be to, kratos ir poėmiai gali būti atliekami tik remiantis prokuroro prašymu išduotu teisėjo orderiu ir užtikrinant tinkamą teisinį procesą⁽⁷⁾. Išskirtinėmis aplinkybėmis, t. y., kai nusikaltimu įtariamas asmuo sulaikomas darant nusikaltimą (*flagrante delicto*) arba kai kyla pavojus, kad asmuo, įtariamas nusikaltimu, už kurį baudžiama trejų metų ir didesne laisvės atėmimo bausme, gali pasprukti ar sunaikinti įkalčius, tyrimą atliekančios institucijos gali atlikti kratą arba poėmį neturėdamos orderio ir tokiu atveju turi pateikti *ex post* prašymą dėl orderio⁽⁸⁾. Šie bendrieji principai plačiau apibrėžti konkrečiuose įstatymuose, kuriais reglamentuojamas baudžiamasis procesas ir ryšių apsauga (išsamią apžvalgą žr. toliau).

Užsienio valstybių piliečių atžvilgiu Konstitucijoje nustatyta, kad jų teisės užtikrinamos tarptautine teise ir sutartimis⁽⁹⁾. Korėja yra kelių tarptautinių susitarimų, kuriais užtikrinama teisė į privatumą, kaip antai Tarptautinio pilietinių ir politinių teisių pakto (17 straipsnis), Neįgalųjų teisių konvencijos (22 straipsnis) ir Vaiko teisių konvencijos (16 straipsnis), šalis. Be to, nors Konstitucijoje iš esmės minimos „piliečių“ teisės, Konstitucinis Teismas nusprendė, kad pagrindinės teisės taikomos ir užsienio valstybių piliečiams⁽¹⁰⁾. Visų pirma Teismas pareiškė, kad teisė į žmogaus orumo ir vertės

⁽¹⁾ 1948 m. liepos 17 d. paskelbtos Korėjos Respublikos Konstitucijos (toliau – Konstitucija) 10 straipsnis.

⁽²⁾ Konstitucijos 37 straipsnio 2 dalis.

⁽³⁾ Konstitucijos 37 straipsnio 2 dalis.

⁽⁴⁾ 1998 m. liepos 24 d. Korėjos Aukščiausiojo Teismo sprendimas Nr. 96DA42789.

⁽⁵⁾ 2003 m. spalio 30 d. Konstitucinio Teismo sprendimas Nr. 2002Hun- Ma51. Konstitucinis Teismas 2005 m. gegužės 26 d. sprendime 99Hun-Ma513 ir 2004Hun-Ma190 (sujungtas) taip pat išaiškino, kad „teisė valdyti savo asmeninę informaciją tai informacijos subjekto teisė asmeniškai nuspręsti, kada ir kam jo asmeninė informacija gali būti atskleista arba ja leidžiama naudotis arba kas ir kokių mastu ją gali atskleisti arba naudoti. Tai yra pagrindinė teisė, net jei Konstitucijoje ji nenurodyta, kuria siekiama apsaugoti asmens apsisprendimo laisvę nuo grėsmės, kylančios dėl valstybės funkcijų išplėtimo ir informacinių ryšių technologijų“.

⁽⁶⁾ Konstitucijos 12 straipsnio 1 dalies pirmas sakiny.

⁽⁷⁾ Konstitucijos 16 straipsnis ir 12 straipsnio 3 dalis.

⁽⁸⁾ Konstitucijos 12 straipsnio 3 dalis.

⁽⁹⁾ Konstitucijos 6 straipsnio 2 dalis.

⁽¹⁰⁾ 1994 m. gruodžio 29 d. Konstitucinio Teismo sprendimas Nr. 93Hun- MA120. Taip pat žr., pavyzdžiui, Konstitucinio Teismo sprendimą Nr. 2014Hun-Ma346 (2018 m. gegužės 31 d.), kuriame Teismas nustatė, kad buvo pažeista oro uoste laikomo Sudano piliečio konstitucinė teisė gauti teisinės konsultacijos. Kitoje byloje Konstitucinis Teismas konstatavo, kad laisvė pasirinkti teisėtą darbo vietą yra glaudžiai susijusi su teise siekti laimės, taip pat su žmogaus orumu ir verte, todėl ji nėra tik piliečių teisė, bet gali būti užtikrinama ir užsienio valstybių piliečiams, teisėtai dirbantiems Korėjos Respublikoje (2011 m. rugsėjo 29 d. Konstitucinio Teismo sprendimas Nr. 2007Hun-Ma1083).

apsaugą, taip pat teisė siekti laimės yra ne tik piliečių, bet visų žmonių teisės⁽¹¹⁾. Teismas taip pat išaiškino, kad teisė valdyti savo informaciją yra laikoma pagrindine teise, pagrįsta teise į orumą ir laimės siekį bei teise į privatų gyvenimą⁽¹²⁾. Teismų praktikoje iki šiol nebuvo nagrinėjama konkrečiai ne Korėjos piliečių teisė į privatumą, bet mokslininkai plačiai pripažįsta, kad Konstitucijos 12–22 straipsniuose (kuriuose, be kita ko, numatyta teisė į privatumą ir asmens laisvę) nustatytos „žmogaus teisės“.

Galiausiai Konstitucijoje taip pat numatoma teisė reikalauti teisingos kompensacijos iš valdžios institucijų⁽¹³⁾. Be to, remiantis Konstitucinio Teismo įstatymu, bet kuris asmuo, kurio Konstitucija garantuojamos pagrindinės teisės yra pažeidžiamos valdžios institucijoms naudojantis savo įgaliojimais (išskyrus teismų sprendimus), gali Konstituciniam Teismui pateikti konstitucinį skundą⁽¹⁴⁾.

1.2. Bendrosios duomenų apsaugos taisyklės

Korėjos Respublikos bendrasis duomenų apsaugos įstatymas – Asmeninės informacijos apsaugos įstatymas (toliau – AIAĮ) – taikomas ir privačiam, ir viešajam sektoriui. Valdžios institucijų atžvilgiu AIAĮ konkrečiai nurodyta prievolė parengti politiką, kuria būtų užkertamas kelias „piktnaudžiavimui asmenine informacija ir neteisėtam jos naudojimui, neteisėtam sekimui ir persekiojimui ir t. t., ir būtų didinamas žmonių orumas bei asmens privatumo apsauga.“⁽¹⁵⁾

Asmens duomenis tvarkant teisėsaugos tikslais taikomi visi AIAĮ reikalavimai. Tai reiškia, kad, pavyzdžiui, baudžiamosios teisėsaugos institucijos privalo laikytis su teisėtu tvarkymu susijusių prievolių, t. y. remtis vienu iš AIAĮ išvardytų teisiųjų pagrindų rinkdamos, naudodamos ar teikdamos asmeninę informaciją (AIAĮ 15–18 straipsniai), taip pat tikslo apribojimo principu (AIAĮ 3 straipsnio 1 ir 2 dalys), proporcingumo ir (arba) duomenų kiekio mažinimo principais (AIAĮ 3 straipsnio 1 ir 6 dalys), riboto duomenų saugojimo principu (AIAĮ 21 straipsnis), duomenų saugumo principu, įskaitant pranešimą apie duomenų saugumo pažeidimus (AIAĮ 3 straipsnio 4 dalis, 29 ir 34 straipsniai), ir skaidrumo principu (AIAĮ 3 straipsnio 1 ir 5 dalys, 20, 30 ir 32 straipsniai). Neskelbtinai informacijai taikomos specialios apsaugos priemonės (AIAĮ 23 straipsnis). Be to, pagal AIAĮ 3 straipsnio 5 dalį ir 4 straipsnį, taip pat 35–39-2 straipsnius asmens gali naudotis savo prieigos prie informacijos, jos ištaisymo, ištrynimo ir rinkimo sustabdymo teisėmis baudžiamosios teisėsaugos institucijų atžvilgiu.

Taigi AIAĮ visapusiškai taikomas, kai asmens duomenys tvarkomi baudžiamosios teisėsaugos tikslais, tačiau jame numatyta išimtis, kai asmens duomenys tvarkomi nacionalinio saugumo tikslais. Pagal AIAĮ 58 straipsnio 1 dalies 2 punktą AIAĮ 15–50 straipsniai netaikomi asmeninei informacijai, kuri renkama arba kurią prašoma pateikti siekiant analizuoti su nacionaliniu saugumu susijusią informaciją⁽¹⁶⁾. Tačiau taikomi AIAĮ I skyrius (Bendrosios nuostatos), II skyrius (Asmeninės informacijos apsaugos politikos nustatymas ir kt.), VIII skyrius (Kolektyvinis ieškinys dėl duomenų saugumo pažeidimo), IX skyrius (Papildomos nuostatos) ir X skyrius (Nuostatos dėl sankcijų). Tai apima bendruosius duomenų apsaugos principus, nustatytus 3 straipsnyje (Asmeninės informacijos apsaugos principai), ir asmens teises, užtikrinamas AIAĮ 4 straipsniu (Duomenų subjektų teisės). Tai reiškia, kad šioje srityje taip pat užtikrinamas pagrindinių principų ir teisių įgyvendinimas. Be to, AIAĮ 58 straipsnio 4 dalyje nustatyta, kad tokia informacija turi būti tvarkoma tiek, kiek būtina numatytam tikslui pasiekti per trumpiausią laikotarpį; joje taip pat nustatytas reikalavimas asmeninės informacijos valdytojiui taikyti reikiamas priemones, kad būtų užtikrinamas saugus duomenų valdymas ir tinkamas jų tvarkymas, pavyzdžiui, technines, valdymo ir fizinės apsaugos priemones, taip pat priemones, kuriomis būtų užtikrinamas tinkamas individualių skundų nagrinėjimas.

Pranešime Nr. 2021-1 dėl papildomų taisyklių dėl Asmeninės informacijos apsaugos įstatymo aiškinimo ir taikymo Asmeninės informacijos apsaugos komisija (toliau – AIAK) išsamiau paaiškino, kaip AIAĮ taikomas, kai asmens duomenys tvarkomi nacionalinio saugumo tikslais, atsižvelgiant į šią dalinę išimtį⁽¹⁷⁾. Tai visų pirma taikoma asmenų teisėms (prieigos, ištaisymo, sustabdymo ir ištrynimo) ir galimo jų suvaržymo pagrindams bei apribojimams. Remiantis pranešimu, pagrindiniais AIAĮ principais, teisėmis ir pareigomis, taikomais tvarkant asmeninę informaciją nacionalinio

⁽¹¹⁾ 2001 m. lapkričio 29 d. Konstitucinio Teismo sprendimas Nr. 99HeonMa494.

⁽¹²⁾ Žr., pavyzdžiui, Konstitucinio Teismo sprendimą Nr. 99HunMa513.

⁽¹³⁾ Konstitucijos 29 straipsnio 1 dalis.

⁽¹⁴⁾ Konstitucinio Teismo įstatymo 68 straipsnio 1 dalis.

⁽¹⁵⁾ AIAĮ 5 straipsnio 1 dalis.

⁽¹⁶⁾ AIAĮ 58 straipsnio 1 dalies 2 punktą.

⁽¹⁷⁾ AIAK pranešimo Nr. 2021-1 dėl papildomų taisyklių dėl Asmeninės informacijos apsaugos įstatymo aiškinimo ir taikymo III skirsnio 6 dalis.

saugumo tikslais, atspindimos Konstitucijoje įtvirtintos garantijos dėl asmens teisės valdyti savo asmeninę informaciją apsaugos. Norint taikyti bet kokią tos teisės apribojimą, pavyzdžiui, kai tai būtina nacionaliniam saugumui užtikrinti, reikia suderinti asmens teises ir interesus su atitinkamu viešuoju interesu ir toks apribojimas negali turėti įtakos esminių šios teisės aspektų įgyvendinimui (Konstitucijos 37 straipsnio 2 dalis).

2. VYRIAUSYBĖS GALIMYBĖ SUSIPAŽINTI SU INFORMACIJA TEISĖSAUGOS TIKSLAIS

2.1. Teisėsaugos srityje kompetentingos valdžios institucijos

Policija, prokurorai ir teismai gali rinkti asmens duomenis baudžiamosios teisėsaugos tikslais remdamiesi Baudžiamojo proceso įstatymu (toliau – BPI), Ryšių privatumo apsaugos įstatymu (toliau – RPAI) ir Telekomunikacijų įmonių įstatymu (toliau – TIĮ). Tiek, kiek Nacionalinės žvalgybos tarnybos įstatymu šie įgaliojimai suteikiami ir Nacionalinei žvalgybos tarnybai (toliau – NŽT), ji turi laikytis pirmiau minėtų įstatymų⁽¹⁸⁾. Galiausiai įstatymu dėl konkrečios finansinių sandorių informacijos teikimo ir naudojimo (toliau – ĮKFSITN) nustatytas teisinis pagrindas finansų įstaigoms atskleisti informaciją Korėjos finansinės žvalgybos padaliniui (toliau – KFŽP) pinigų plovimo ir terorizmo finansavimo prevencijos tikslais. Ši specializuota agentūra savo ruožtu gali teikti tokią informaciją teisėsaugos institucijoms. Tačiau šie informacijos atskleidimo įpareigojimai taikomi tik tiems duomenų valdytojams, kurie tvarko asmens kredito informaciją pagal Kredito informacijos įstatymą ir kuriuos prižiūri Finansinių paslaugų komisija. Kadangi tokių duomenų valdytojų atliekamas asmens kredito informacijos tvarkymas nepatenka į sprendimo dėl tinkamumo taikymo sritį, pagal ĮKFSITN taikomi apribojimai ir apsaugos priemonės šiame dokumente išsamiau neapibūdinti.

2.2. Teisiniai pagrindai ir apribojimai

BPI (žr. 2.2.1 skirsnį), RPAI (žr. 2.2.2 skirsnį) ir Telekomunikacijų įmonių įstatymu (žr. 2.2.3 skirsnį) suteikiamas teisinis pagrindas rinkti asmeninę informaciją teisėsaugos tikslais ir nustatomi taikytini apribojimai ir apsaugos priemonės.

2.2.1. Krata ir poėmis

2.2.1.1. Teisinis pagrindas

Prokurorai ir vyresnieji teismo policijos pareigūnai gali tikrinti daiktus, apieškoti asmenis arba paimti daiktus: 1) jei asmuo įtariamas padaręs nusikaltimą (yra įtariamasis tiriant nusikalstamą veiką), 2) jei tai būtina tyrimui atlikti ir 3) jei tikrintini daiktai, apieškotini asmenys ir bet kokie paimti daiktai laikomi susijusiais su byla⁽¹⁹⁾. Teismai taip pat gali atlikti kratą ir paimti bet kokius daiktus, naudotinus kaip įrodymai arba konfiskuotinus, jeigu tokie daiktai ar asmenys laikomi susijusiais su konkrečia byla⁽²⁰⁾.

2.2.1.2. Apribojimai ir apsaugos priemonės

Prokurorams ir teismo policijos pareigūnams taikoma bendra prievolė gerbti įtariamojo, taip pat bet kurio kito susijusio asmens žmogaus teises⁽²¹⁾. Be to, imtis priverstinių priemonių tyrimo tikslui pasiekti galima tik tuo atveju, jei tai aiškiai numatyta BPI ir tiek, kiek tai būtina⁽²²⁾.

Vykdydami baudžiamąjį tyrimą policijos pareigūnai arba prokurorai gali atlikti kratą, patikrinimą ar poėmį tik remdamiesi teismo išduotu orderiu⁽²³⁾. Orderio prašanti institucija turi pateikti medžiagą, kurioje įrodomas nusikalstama veika įtariamo asmens įtarimo nusikaltimu pagrindas, įrodoma, kad atlikti kratą, patikrinimą ar poėmį yra būtina ir kad yra atitinkamų daiktų, kurie turi būti paimti⁽²⁴⁾. Pačiame orderyje, be kita ko, turi būti nurodyti nusikalstama veika įtariamo asmens vardas ir pavardė ir nusikalstama veika, vieta, asmuo ar daiktai, kurie yra kratos objektas, arba daiktai, kurie turi būti paimti, išdavimo data ir galiojimo laikotarpis⁽²⁵⁾. Jei teismo proceso metu krata ir poėmis atliekami ne viešame teismo posėdyje, teismo išduotas orderis taip pat turi būti gautas iš anksto⁽²⁶⁾. Atitinkamam asmeniui ir jo gynyba užsiimančiam asmeniui iš anksto pranešama apie kratą ar poėmį ir jie gali dalyvauti vykdam orderį⁽²⁷⁾.

⁽¹⁸⁾ Žr. NŽT įstatymo 3 straipsnį (įstatymas Nr. 12948), kuriame nurodyti baudžiamosios veikos tyrimai tam tikrų nusikaltimų, pavyzdžiui, sukilimo, maišto ir su nacionaliniu saugumu susijusių nusikaltimų (pvz., šnipinėjimo) atveju. Tokiomis aplinkybėmis būtų taikomos BPI numatytos procedūros dėl kratos ir poėmio, o RPAI būtų reglamentuojamas ryšių duomenų rinkimas (žr. 3 dalį dėl nuostatų, susijusių su prieiga prie ryšių nacionalinio saugumo tikslais).

⁽¹⁹⁾ BPI 215 straipsnio 1 ir 2 dalys.

⁽²⁰⁾ BPI 106 straipsnio 1 dalis ir 107 ir 109 straipsniai.

⁽²¹⁾ BPI 198 straipsnio 2 dalis.

⁽²²⁾ BPI 199 straipsnio 1 dalis.

⁽²³⁾ BPI 215 straipsnio 1 ir 2 dalys.

⁽²⁴⁾ Baudžiamojo proceso reglamento 108 straipsnio 1 dalis.

⁽²⁵⁾ BPI 114 straipsnio 1 dalis kartu su BPI 219 straipsniu.

⁽²⁶⁾ BPI 113 straipsnis.

⁽²⁷⁾ BPI 121 ir 122 straipsniai.

Kai atliekama krata arba poėmis ir kai apieškomas daiktas yra kompiuterio diskas arba kita duomenų laikmena, iš esmės bus paimti tik duomenys (juos nukopijavus arba atspausdinus), o ne visa laikmena ⁽²⁸⁾. Pati duomenų laikmena gali būti paimta tik tada, kai manoma, kad iš esmės neįmanoma atspausdinti ar nukopijuoti tik reikalingų duomenų arba kad kitaip kratos tikslo pasiekti iš esmės neįmanoma ⁽²⁹⁾. Atitinkamam asmeniui turi būti nedelsiant pranešama apie poėmį ⁽³⁰⁾. Reikalavimo pranešti atžvilgiu BPI nenustatyta jokių išimčių.

Neturint orderio kratos, patikrinimai ir poėmiai gali būti atliekami tik tam tikrais atvejais. Pirma, taip yra tuo atveju, kai orderio neįmanoma gauti, nes nusikaltimo vietos aplinkybės reikalauja skubiai veikti ⁽³¹⁾. Tačiau po to orderis turi būti nedelsiant gautas ⁽³²⁾. Antra, neturint orderio kratos ir patikrinimai gali būti atliekami *in loco* suimant arba sulaikant įtariamąjį ⁽³³⁾. Galiausiai prokuroras arba vyresnysis teismo policijos pareigūnas gali paimti daiktą neturėdamas orderio, kai nusikaltimu įtariamasis asmuo arba trečiasis asmuo daiktą išmetė arba savanoriškai pateikė ⁽³⁴⁾.

Įrodymai, gauti pažeidžiant BPI, bus laikomi netinkamais ⁽³⁵⁾. Be to, Baudžiamuoju įstatymu nustatyta, kad už neteisėtą asmenų apieškojimą arba asmens gyvenamosios vietos, saugomo pastato, statinio, automobilio, laivo, lėktuvo ar kambario, kuriame jis gyvena, kratą baudžiama laisvės atėmimu iki trejų metų ⁽³⁶⁾. Todėl ši nuostata taip pat taikoma tais atvejais, kai vykdamas neteisėtą kratą paimami tokie daiktai kaip duomenų saugojimo įrenginiai.

2.2.2. Ryšių informacijos rinkimas

2.2.2.1. Teisinis pagrindas

Ryšių informacijos rinkimas reglamentuojamas specialiu įstatymu – RPAĮ. Visų pirma RPAĮ nustatomas draudimas bet kuriam asmeniui cenzūruoti bet kokį pašta, slapta stebėti ryšius bet kokioje telekomunikacijų terpėje, teikti ryšių patvirtinimo duomenis arba įrašyti ar klausytis kitų asmenų viešai neskelbiamų pokalbių, išskyrus atvejus, kai galima remtis BPI, RPAĮ ar Karinio teismo įstatymu ⁽³⁷⁾. Pagal RPAĮ sąvoka „ryšiai“ yra ir tradicinis paštas, ir telekomunikaciniai ryšiai ⁽³⁸⁾. Šiuo atžvilgiu „ryšius ribojančios priemonės“ ⁽³⁹⁾ ir „ryšių patvirtinimo duomenų“ rinkimas RPAĮ atskiriami.

Ryšius ribojančių priemonių sąvoka apima „cenzūrą“, t. y. tradicinio pašto turinio rinkimą, taip pat „slaptą pokalbių klausymąsi“, t. y. tiesioginių telekomunikacinių ryšių turinio perėmimą (gavimą ar įrašymą) ⁽⁴⁰⁾. Ryšių patvirtinimo duomenų sąvoka apima „įrašų apie telekomunikacinius ryšius duomenis“, kuriuos sudaro telekomunikacinių ryšių data, jų pradžios ir pabaigos laikas, atliktų ir gautų skambučių skaičius, taip pat kitos šalies abonento numeris, naudojimo dažnumas, telekomunikacijų paslaugų naudojimo žurnalo failai ir vietos nustatymo informacija (pvz., atsižvelgiant į perdavimo bokštus, į kuriuos gaunami signalai) ⁽⁴¹⁾.

⁽²⁸⁾ BPI 106 straipsnio 3 dalis.

⁽²⁹⁾ BPI 106 straipsnio 3 dalis.

⁽³⁰⁾ BPI 219 straipsnis kartu su BPI 106 straipsnio 4 dalimi.

⁽³¹⁾ BPI 216 straipsnio 3 dalis.

⁽³²⁾ BPI 216 straipsnio 3 dalis.

⁽³³⁾ BPI 216 straipsnio 1 ir 2 dalys.

⁽³⁴⁾ BPI 218 straipsnis. Asmeninės informacijos atveju tai taikoma tik tuomet, kai ją savanoriškai pateikia atitinkamas asmuo, o ne asmeninės informacijos valdytojas, turintis tokią informaciją (tokiu atveju reikėtų specialaus teisinio pagrindo pagal Asmeninės informacijos apsaugos įstatymą). Savanoriškai pateikti daiktai įrodymais teismo procese pripažįstami tik tuo atveju, jei nekyla pagrįstų abejonių dėl informacijos atskleidimo savanoriško pobūdžio, o tai turi įrodyti prokuroras. Žr. 2016 m. kovo 10 d. Aukščiausiojo Teismo sprendimą 2013Do11233.

⁽³⁵⁾ BPI 308-2 straipsnis.

⁽³⁶⁾ Baudžiamuoju įstatymu 321 straipsnis.

⁽³⁷⁾ RPAĮ 3 straipsnis. Karinio teismo įstatymu iš esmės reglamentuojamas informacijos apie karinį personalą rinkimas ir civiliams jis gali būti taikomas tik ribotais atvejais (pvz., jei karinis personalas ir civiliai asmenys nusikaltimą padarytų kartu arba jei asmuo padaro nusikaltimą, dėl kurio nukenčia karinis personalas, pažeidimo nagrinėjimo procedūra gali būti pradėta kariniame teisme (žr. Karinio teismo įstatymo 2 straipsnį)). Bendrosios nuostatos, kuriomis reglamentuojama krata ir poėmis, yra panašios į BPI nuostatas (žr., pvz., Karinio teismo įstatymo 146–149 ir 153–156 straipsnius). Pavyzdžiui, pašto korespondencija gali būti paimama tik tada, kai tai būtina tyrimui atlikti, ir remiantis Karinio teismo išduotu orderiu. Renkant elektroninę korespondenciją būtų taikomi RPAĮ nustatyti apribojimai ir apsaugos priemonės.

⁽³⁸⁾ RPAĮ 2 straipsnio 1 dalis, t. y. „visų rūšių garsų, žodžių, simbolių ar vaizdų perdavimas arba priėmimas laidais, belaidžiu ryšiu, optiniu skaiduliniu kabeliu ar kita elektromagnetine sistema, įskaitant telefoną, el. pašta, informacijos teikimo paslaugą narystės pagrindu, faksimilę ir radijo iešką“.

⁽³⁹⁾ RPAĮ 2 straipsnio 7 dalis ir 3 straipsnio 2 dalis.

⁽⁴⁰⁾ „Cenzūra“ apibrėžiama kaip „korespondencijos atidarymas neturint atitinkamos šalies sutikimo arba informacijos apie jos turinį sužinojimas, įrašymas ar nuslėpimas taikant kitas priemones“ (RPAĮ 2 straipsnio 6 dalis). „Slaptas pokalbių klausymasis“ reiškia „telekomunikacinių ryšių turinio gavimą arba įrašymą, išklausančiant ar kartu skaitant pranešimų garsus, žodžius, simbolius ar vaizdus taikant elektrones ir mechanines priemones neturint atitinkamos šalies sutikimo, arba trukdymas jo perdavimui ir gavimui“ (RPAĮ 2 straipsnio 7 dalis).

⁽⁴¹⁾ RPAĮ 2 straipsnio 11 dalis.

RPAĮ nustatyti apribojimai ir apsaugos priemonės abiejų rūšių duomenų rinkimo atžvilgiu, o už kelių iš šių reikalavimų nesilaikymą taikomos baudžiamosios sankcijos ⁽⁴²⁾.

2.2.2.2. Apribojimai ir apsaugos priemonės, taikomi renkant ryšių turinį (taikant ryšius ribojančias priemones)

Ryšių turinio rinkimas gali būti tik papildoma priemonė baudžiamajam tyrimui palengvinti (t. y. kraštutinė priemonė) ir turi būti dedamos pastangos kuo labiau sumažinti kišimasi į privačius žmonių ryšius ⁽⁴³⁾. Vadovaujantis šiuo bendroju principu ryšius ribojančios priemonės gali būti taikomos tik tais atvejais, kai jų netaikant sunku užkirsti kelią nusikaltimo įvykdymui, suimti nusikaltėlių arba surinkti įrodymus ⁽⁴⁴⁾. Ryšių turinį renkančios teisėsaugos institucijos turi nedelsdamos nustoti tai daryti, kai nuolatinės prieigos prie informacijos nebereikia, taip užtikrinant, kad ryšių privatumo pažeidimas būtų kuo mažesnis ⁽⁴⁵⁾.

Be to, ryšius ribojančios priemonės gali būti taikomos tik tada, kai yra svarių priežasčių įtarti, kad planuojami, vykdomi arba buvo įvykdyti tam tikri konkrečiai RPAĮ išvardyti sunkūs nusikaltimai. Šie nusikaltimai, be kita ko, yra, pavyzdžiui, maištas, su narkotikais susiję nusikaltimai, su sprogmenimis susiję nusikaltimai, taip pat nusikaltimai, susiję su nacionaliniu saugumu, diplomatiniais santykiais arba karinėmis bazėmis ir įrenginiais ⁽⁴⁶⁾. Ryšius ribojančios priemonės taikymo sritis turi būti konkretūs pašto korespondencijos arba telekomunikacinių ryšių vienetai, kuriuos siunčia arba gauna įtariamasis, arba pašto korespondencijos arba telekomunikacinių ryšių vienetai, kuriuos per nustatytą laikotarpį siunčia arba gauna įtariamasis ⁽⁴⁷⁾.

Net jei šie reikalavimai įvykdomi, turinio duomenys gali būti renkami tik remiantis teismo išduotu orderiu. Visų pirma prokuroras gali prašyti teismo leisti rinkti turinio duomenis, susijusius su įtariamuoju arba tiriamu asmeniu ⁽⁴⁸⁾. Be to, teismo policijos pareigūnas gali prašyti prokurorą išduoti leidimą, o šis savo ruožtu gali prašyti teismą išduoti orderį ⁽⁴⁹⁾. Prašymas išduoti orderį turi būti pateiktas raštu ir jame turi būti nurodyta konkreti informacija. Visų pirma jame turi būti nurodytos 1) esminės priežastys, dėl kurių įtariama, kad vienas iš išvardytų nusikaltimų yra planuojamas, vykdomas ar įvykdytas, taip pat bet kokia medžiaga, kuria įrodomas *prima facie* pagrindas įtarimams, 2) ryšius ribojančios priemonės, taip pat jų taikymo sritis, mastas, tikslas ir galiojimo laikotarpis ir 3) vieta, kurioje priemonės bus įgyvendinamos, ir jų įgyvendinimo būdas ⁽⁵⁰⁾.

Jeigu laikomasi teisinių reikalavimų, teismas gali suteikti rašytinį leidimą taikyti ryšius ribojančias priemones įtariamajam arba tiriamam asmeniui ⁽⁵¹⁾. Šiame orderyje nurodomos taikytinų priemonių rūšys ir jų taikymo sritis, mastas, galiojimo laikotarpis, įgyvendinimo vieta ir būdas ⁽⁵²⁾.

Ryšius ribojančios priemonės gali būti taikomos tik dviejų mėnesių laikotarpį ⁽⁵³⁾. Jei priemonių taikymo tikslas pasiekiamas anksčiau nei baigiasi tas laikotarpis, priemonių taikymas turi būti nedelsiant nutrauktas. Tais atvejais, kai reikiamos sąlygos vis dar tenkinamos, prašymas pratęsti ryšius ribojančių priemonių taikymo laikotarpį gali būti pateiktas per du mėnesius. Į tokį prašymą turi būti įtraukta medžiaga, kuria įrodomas *prima facie* pagrindas pratęsti priemonių taikymą ⁽⁵⁴⁾. Pratęstas laikotarpis negali būti ilgesnis kaip vieni metai, o tam tikrų ypač sunkių nusikaltimų atveju – treji metai (pvz., nusikaltimų, susijusių su sukilimu, užsienio agresija, nacionaliniu saugumu ir t. t., atveju) ⁽⁵⁵⁾.

Pateikusias rašytinį teismo leidimą teisėsaugos institucijos gali reikalauti ryšių paslaugų teikėjų pagalbos ⁽⁵⁶⁾. Ryšių paslaugų teikėjai privalo bendradarbiauti ir saugoti pateiktą leidimą savo byloje ⁽⁵⁷⁾. Jie gali atsisakyti bendradarbiauti, kai teismo rašytiniame leidime nurodyta informacija apie asmenį, kurio informaciją norima rinkti, yra neteisinga (pavyzdžiui, asmens telefono numeris). Be to, jiems draudžiama, nepaisant aplinkybių, atskleisti slaptažodžius, naudojamus naudojantis telekomunikacijų paslaugomis ⁽⁵⁸⁾.

⁽⁴²⁾ RPAĮ 16 ir 17 straipsniai. Jos taikomos, pavyzdžiui, jei renkami duomenys neturint orderio, netvarkomi įrašai, nenutraukiamas duomenų rinkimas pasibaigus ekstremaliajai situacijai arba apie duomenų rinkimą nepranešama atitinkamam asmeniui.

⁽⁴³⁾ RPAĮ 3 straipsnio 2 dalis.

⁽⁴⁴⁾ RPAĮ 5 straipsnio 1 dalis.

⁽⁴⁵⁾ RPAĮ vykdymo užtikrinimo dekreto 2 straipsnis.

⁽⁴⁶⁾ RPAĮ 5 straipsnio 1 dalis.

⁽⁴⁷⁾ RPAĮ 5 straipsnio 2 dalis.

⁽⁴⁸⁾ RPAĮ 6 straipsnio 1 dalis.

⁽⁴⁹⁾ RPAĮ 6 straipsnio 2 dalis.

⁽⁵⁰⁾ RPAĮ 6 straipsnio 4 dalis ir RPAĮ vykdymo užtikrinimo dekreto 4 straipsnio 1 dalis.

⁽⁵¹⁾ RPAĮ 6 straipsnio 5 dalis ir 6 straipsnio 8 dalis.

⁽⁵²⁾ RPAĮ 6 straipsnio 6 dalis.

⁽⁵³⁾ RPAĮ 6 straipsnio 7 dalis.

⁽⁵⁴⁾ RPAĮ 6 straipsnio 7 dalis.

⁽⁵⁵⁾ RPAĮ 6 straipsnio 8 dalis.

⁽⁵⁶⁾ RPAĮ 9 straipsnio 2 dalis.

⁽⁵⁷⁾ RPAĮ 15-2 straipsnis ir RPAĮ vykdymo užtikrinimo dekreto 12 straipsnis.

⁽⁵⁸⁾ RPAĮ 9 straipsnio 4 dalis.

Bet kuris ryšius ribojančias priemones taikantis arba bendradarbiauti prašantis asmuo turi saugoti įrašus, kuriuose turi būti nurodomi priemonių tikslai, jų taikymo laikotarpis, bendradarbiavimo data ir sritis⁽⁵⁹⁾. Ryšius ribojančias priemones taikančios teisėsaugos institucijos taip pat turi saugoti įrašus ir juose pateikti išsamią informaciją ir nurodyti pasiektus rezultatus⁽⁶⁰⁾. Baigę tyrimą teismo policijos pareigūnai privalo šią informaciją ataskaitos forma pateikti prokurorui⁽⁶¹⁾.

Kai prokuroras pateikia kaltinimus byloje, kurioje buvo taikytos ryšius ribojančios priemonės, arba paskelbia sprendimą atitinkamam asmeniui nepateikti kaltinimų arba jo nesuimti (t. y. ne tik sustabdyti baudžiamąjį persekiojimą), prokuroras privalo pranešti asmeniui, kuriam buvo taikytos ryšius ribojančios priemonės, apie tai, kad jam buvo taikytos ryšius ribojančios priemonės, nurodant jas taikiusią agentūrą ir taikymo laikotarpį. Toks pranešimas turi būti pateiktas raštu per 30 dienų nuo sprendimo priėmimo⁽⁶²⁾. Pranešimas gali būti atidėtas, jei pranešus galėtų kilti didelis pavojus nacionaliniam saugumui arba būtų sutrikdytas visuomenės saugumas ir viešoji tvarka, arba kai tikėtina, kad pranešus kiltų grėsmė kitų asmenų gyvybėms ir fizinei sveikatai⁽⁶³⁾. Pranešimą atidėti ketinantis prokuroras arba teismo policijos pareigūnas turi gauti apygardos prokuratūros vadovo sutikimą⁽⁶⁴⁾. Pranešimas turi būti pateiktas per 30 dienų nuo tada, kai išnyksta atidėjimo pagrindai⁽⁶⁵⁾.

RPAĮ taip pat nustatoma speciali tvarka, kai ryšių turinys renkamas ekstremaliųjų situacijų atveju. Visų pirma teisėsaugos institucijos gali rinkti ryšių turinį tuo atveju, kai dėl planuojamo ar vykdomo organizuoto nusikalstamumo ar kito sunkaus nusikaltimo kyla neišvengiama tiesioginė mirties ar sunkaus sužalojimo grėsmė, ir susidaro ekstremalioji situacija, dėl kurios neįmanoma taikyti įprastos procedūros (kaip nurodyta pirmiau)⁽⁶⁶⁾. Tokios ekstremaliosios situacijos atveju policijos pareigūnas arba prokuroras gali taikyti ryšius ribojančias priemones be išankstinio teismo leidimo, bet privalo pateikti teismui prašymą dėl leidimo iš karto pritaikęs priemones. Jei teisėsaugos institucija negauna teismo leidimo per 36 valandas nuo to momento, kai buvo imtasi neatidėliotinių priemonių, duomenų rinkimas turi būti nedelsiant nutrauktas, o surinkta informacija paprastai sunaikinama⁽⁶⁷⁾. Policijos pareigūnai sekimą ekstremaliųjų situacijų atveju atlieka prižiūrimi prokuroro, o jei prokuroro nurodymų iš anksto gauti neįmanoma dėl būtinybės imtis skubių veiksmų, policija turi gauti prokuroro sutikimą iš karto po to, kai pradėdama vykdyti veiksmus⁽⁶⁸⁾. Kaip aprašyta pirmiau, taisyklės dėl asmens informavimo apie informacijos rinkimą taip pat taikomos, kai ryšių turinys renkamas ekstremaliųjų situacijų atveju.

Ekstremaliųjų situacijų atvejais informacija visada turi būti renkama remiantis „neišvengiamos cenzūros ir (arba) slapto pokalbių klausymosi pareiškimu“, o rinkimą atliekanti institucija privalo registruoti visas neatidėliotinas priemones⁽⁶⁹⁾. Prie prašymo teismui suteikti leidimą taikyti neatidėliotinas priemones turi būti pridėtas rašytinis dokumentas, kuriame turi būti nurodytos būtinos ryšius ribojančios priemonės, jų taikymo sritis, objektas, taikymo mastas, vykdymo vieta, būdas ir paaiškinimas, kaip atitinkamos ryšius ribojančios priemonės atitinka RPAĮ 5 straipsnio 1 dalį⁽⁷⁰⁾, taip pat patvirtinamieji dokumentai.

Tais atvejais, kai neatidėliotinos priemonės taikomos trumpai ir nespėjama gauti teismo leidimo (pvz., jei įtariamasis suimamas iš karto pradėjus informacijos perėmimą ir dėl to jis sustabdomas), kompetentingos prokuratūros vadovas kompetentingam teismui pateikia pranešimą apie taikytą neatidėliotinę priemonę⁽⁷¹⁾. Pranešime turi būti pateikta informacija apie priemonės taikymo tikslą, sritį, mastą, laikotarpį, įgyvendinimo vietą ir rinkimo būdą, taip pat prašymo dėl teismo leidimo nepateikimo priežastis⁽⁷²⁾. Pateikus šį pranešimą jį gavęs teismas gali patikrinti rinkimo teisėtumą ir jis turi būti įtrauktas į pranešimų apie neatidėliotinas priemones registrą.

⁽⁵⁹⁾ RPAĮ 9 straipsnio 3 dalis.

⁽⁶⁰⁾ RPAĮ vykdymo užtikrinimo dekreto 18 straipsnio 1 dalis.

⁽⁶¹⁾ RPAĮ vykdymo užtikrinimo dekreto 18 straipsnio 2 dalis.

⁽⁶²⁾ RPAĮ 9-2 straipsnio 1 dalis.

⁽⁶³⁾ RPAĮ 9-2 straipsnio 4 dalis.

⁽⁶⁴⁾ RPAĮ 9-2 straipsnio 5 dalis.

⁽⁶⁵⁾ RPAĮ 9-2 straipsnio 6 dalis.

⁽⁶⁶⁾ RPAĮ 8 straipsnio 1 dalis.

⁽⁶⁷⁾ RPAĮ 8 straipsnio 2 dalis.

⁽⁶⁸⁾ RPAĮ 8 straipsnio 3 dalis ir RPAĮ vykdymo užtikrinimo dekreto 16 straipsnio 3 dalis.

⁽⁶⁹⁾ RPAĮ 8 straipsnio 4 dalis.

⁽⁷⁰⁾ T. y., kad yra sviri priežastis įtarti, kad tam tikri sunkūs nusikaltimai yra planuojami, vykdomi ar įvykdyti, ir kitaip neįmanoma užkirsti kelio nusikaltimo įvykdymui, suimti nusikaltėlių ar surinkti įrodymus.

⁽⁷¹⁾ RPAĮ 8 straipsnio 5 dalis.

⁽⁷²⁾ RPAĮ 8 straipsnio 6 ir 7 dalys.

Paprastai ryšių, RPAĮ pagrindu gautų taikant ryšius ribojančias priemones, turinys gali būti naudojamas tik konkrečių pirmiau išvardytų nusikaltimų tyrimui, juos atlikusių asmenų baudžiamajam persekiojimui ar jų prevencijai, kai taikomos drausminės procedūros dėl tų pačių nusikaltimų, kai ryšių šalis pateikia reikalavimą atlyginti žalą arba tais atvejais, kai tai leidžiama pagal kitus įstatymus ⁽⁷³⁾.

Renkant internetu perduodamus telekomunikacinius ryšius taikomos specialios apsaugos priemonės ⁽⁷⁴⁾. Tokia informacija gali būti naudojama tik RPAĮ 5 straipsnio 1 dalyje išvardytiems sunkiems nusikaltimams tirti. Jei informaciją norima saugoti, reikia gauti teismo, leidusio taikyti ryšius ribojančias priemones, sutikimą ⁽⁷⁵⁾. Prašyme leisti saugoti informaciją turi būti pateikta informacija apie ryšius ribojančias priemones, priemonių rezultatų santrauka, saugojimo priežastys (kartu su patvirtinančia medžiaga) ir nurodyti saugotini telekomunikaciniai ryšiai ⁽⁷⁶⁾. Jei toks prašymas nepateikiamas, gauti telekomunikaciniai ryšiai turi būti ištrinami per 14 dienų nuo ryšių ribojančių priemonių taikymo pabaigos ⁽⁷⁷⁾. Jei prašymas atmetamas, telekomunikaciniai ryšiai turi būti sunaikinami per septynias dienas ⁽⁷⁸⁾. Kai telekomunikaciniai ryšiai ištrinami, apie tai turi būti per septynias dienas pranešta teismui, kuris davė leidimą taikyti ryšius ribojančias priemones, nurodant ištrynimo priežastis, taip pat pateikiant išsamią informaciją apie ištrynimą ir nurodant jo laiką.

Apskritai, jei informacija buvo gauta neteisėtai taikant ryšius ribojančias priemones, ji nebus pripažįstama kaip įrodymai teismo ar drausminėse procedūrose ⁽⁷⁹⁾. Be to, pagal RPAĮ bet kuriam asmeniui, kuris taiko ryšius ribojančias priemones, draudžiama atskleisti konfidencialią informaciją, gautą taikant tokias priemones, ir naudoti gautą informaciją siekiant pakenkti asmenų, kuriems taikomos priemonės, reputacijai ⁽⁸⁰⁾.

2.2.2.3. Apribojimai ir apsaugos priemonės, taikomi ryšius patvirtinančios informacijos rinkimui

Remdamosi RPAĮ teisėsaugos institucijos gali prašyti, kad telekomunikacijų paslaugų teikėjai pateiktų ryšių patvirtinimo duomenis, kai tai būtina tyrimui atlikti arba nuosprendžiui priimti ⁽⁸¹⁾. Kitaip nei renkant turinio duomenis, galimybė rinkti ryšių patvirtinimo duomenis neapribojama ją suteikiant tik tam tikrų konkrečių nusikaltimų atveju. Tačiau, kaip ir turinio duomenų atveju, ryšių patvirtinimo duomenų rinkimui reikalingas išankstinis rašytinis teismo leidimas, taikant tas pačias, anksčiau aprašytas sąlygas ⁽⁸²⁾. Kai teismo leidimo neįmanoma gauti, nes reikia skubiai imtis veiksmų, ryšių patvirtinimo duomenys gali būti renkami neturint orderio; tokiu atveju leidimas turi būti gautas iš karto po to, kai paprašoma duomenų, ir turi būti perduotas telekomunikacijų paslaugų teikėjui ⁽⁸³⁾. Jei vėliau leidimas negaunamas, surinkta informacija turi būti sunaikinama ⁽⁸⁴⁾.

Prokurorai, teismo policijos pareigūnai ir teismai privalo registruoti prašymus rinkti ryšių patvirtinimo duomenis ⁽⁸⁵⁾. Be to, telekomunikacijų paslaugų teikėjai apie ryšių patvirtinimo duomenų atskleidimą privalo du kartus per metus pranešti Mokslo ir IRT ministrui ir įrašus apie tai saugoti septynerius metus nuo duomenų atskleidimo dienos ⁽⁸⁶⁾.

Asmenims iš esmės pranešama apie tai, kad buvo surinkti ryšių patvirtinimo duomenys ⁽⁸⁷⁾. Tokio pranešimo laikas priklauso nuo tyrimo aplinkybių ⁽⁸⁸⁾. Priėmus sprendimą asmenį patraukti (nepatraukti) baudžiamajon atsakomybėn, pranešimas turi būti pateiktas per 30 dienų. Jei kaltinimų pateikimas sustabdomas, pranešimas turi būti pateiktas per 30 dienų praėjus metams nuo tokio sprendimo priėmimo. Bet kuriuo atveju pranešimas turi būti pateiktas per 30 dienų praėjus metams nuo informacijos rinkimo.

Pranešimas gali būti atidėtas, jei pranešus 1) gali kilti pavojus nacionaliniam saugumui, visuomenės saugumui ir viešajai tvarkai, 2) gali būti sukelta mirtis ar kūno sužalojimas, 3) gali būti trukdoma teisingam teismo procesui (pvz., jei

⁽⁷³⁾ RPAĮ 12 straipsnis.

⁽⁷⁴⁾ RPAĮ 12-2 straipsnis.

⁽⁷⁵⁾ Ryšius ribojančias priemones taikantis prokuroras arba policijos pareigūnas per 14 dienų nuo priemonių taikymo pabaigos turi pasirinkti saugotinus telekomunikacinius ryšius ir prašyti teismo sutikimo (policijos pareigūno atveju prašymas turi būti pateiktas prokurorui, kuris tuomet prašymą pateikia teismui) (žr. RPAĮ 12-2 straipsnio 1 ir 2 dalis).

⁽⁷⁶⁾ RPAĮ 12-2 straipsnio 3 dalis.

⁽⁷⁷⁾ RPAĮ 12-2 straipsnio 5 dalis.

⁽⁷⁸⁾ RPAĮ 12-2 straipsnio 5 dalis.

⁽⁷⁹⁾ RPAĮ 4 straipsnis.

⁽⁸⁰⁾ RPAĮ vykdymo užtikrinimo dekreto 11 straipsnio 2 dalis.

⁽⁸¹⁾ RPAĮ 13 straipsnio 1 dalis.

⁽⁸²⁾ RPAĮ 13 ir 6 straipsniai.

⁽⁸³⁾ RPAĮ 13 straipsnio 2 dalis. Kaip ir neatidėliotinių ryšių ribojančių priemonių atveju, turi būti parengtas dokumentas, kuriame turi būti išsamiai aprašyta byla (įtariamasis, taikytinos priemonės, nusikaltimas, kurio įvykdymu asmuo įtariamasis, ir skubumas). Žr. RPAĮ vykdymo užtikrinimo dekreto 37 straipsnio 5 dalį.

⁽⁸⁴⁾ RPAĮ 13 straipsnio 3 dalis.

⁽⁸⁵⁾ RPAĮ 13 straipsnio 5 ir 6 dalys.

⁽⁸⁶⁾ RPAĮ 13 straipsnio 7 dalis.

⁽⁸⁷⁾ RPAĮ 13-3 straipsnio 7 dalis kartu su RPAĮ 9-2 straipsniu.

⁽⁸⁸⁾ RPAĮ 13-3 straipsnio 1 dalis.

pranešus būtų sunaikinti įrodymai arba grasinama liudytojams) arba 4) gali būti apšmeižtas įtariamasis asmuo, aukos ar kiti su byla susiję asmenys arba gali būti pažeistas jų privatumas⁽⁸⁹⁾. Norint atidėti pranešimą dėl vienos iš pirmiau nurodytų priežasčių, reikalingas kompetentingos apygardos prokuratūros vadovo leidimas⁽⁹⁰⁾. Pranešimas turi būti pateiktas per 30 dienų nuo tada, kai išnyksta atidėjimo pagrindai⁽⁹¹⁾.

Asmenys, kuriems pranešama, gali pateikti prokurorui arba teismo policijos pareigūnui rašytinį prašymą nurodyti ryšių patvirtinimo duomenų rinkimo priežastis⁽⁹²⁾. Tokiu atveju prokuroras arba teismo policijos pareigūnas per 30 dienų nuo prašymo gavimo turi raštu nurodyti priežastis, išskyrus atvejus, kai taikoma viena iš pirmiau nurodytų priežasčių (išimties dėl pranešimo atidėjimo)⁽⁹³⁾.

2.2.3. Telekomunikacijų paslaugų teikėjų savanoriškas informacijos atskleidimas

Pagal TII 83 straipsnio 3 dalį telekomunikacijų paslaugų teikėjams leidžiama savanoriškai vykdyti teismo, prokuroro arba tyrimų agentūros vadovo prašymą (pateiktą siekiant paremti baudžiamąjį procesą, tyrimą ar baumės skyrimą) atskleisti „ryšių duomenis“. Pagal TII „ryšių duomenis“ sudaro naudotojų vardas ir pavardė, gyventojų registracijos numeris, adresas ir telefono numeris, abonemento užsakyto arba atsisakymo datos, taip pat naudotojo identifikavimo kodas (t. y. kodas, naudojamas teisėtam kompiuterinių sistemų ar ryšių tinklų naudotojui identifikuoti)⁽⁹⁴⁾. TII tikslais vartotojais laikomi tik tie asmenys, kurie sudaro paslaugų sutartis tiesiogiai su Korėjos telekomunikacijų paslaugų teikėju⁽⁹⁵⁾. Todėl tikėtina, kad atvejai, kai asmenys ES, kurių duomenys buvo perduoti į Korėjos Respubliką, būtų laikomi naudotojais pagal TII, pasitaikys retai, nes tie asmenys paprastai nesudarys sutarties tiesiogiai su Korėjos telekomunikacijų operatoriumi.

Prašymai gauti ryšių duomenis remiantis TII turi būti pateikiami raštu ir juose turi būti nurodytos prašymo priežastys, ryšys su atitinkamu naudotoju ir prašomų duomenų apimtis⁽⁹⁶⁾. Kai dėl aplinkybių, kurios reikalauja skubos, neįmanoma pateikti rašytinio prašymo, rašytinis prašymas turi būti pateiktas iš karto skubos priežastiai išnykus⁽⁹⁷⁾. Prašymus atskleisti ryšių duomenis vykdytys telekomunikacijų paslaugų teikėjai privalo saugoti žurnalus su įrašais, kuriuose turi būti nurodyta, kad buvo pateikti ryšių duomenys, taip pat susijusią medžiagą, pavyzdžiui, rašytinį prašymą⁽⁹⁸⁾. Be to, telekomunikacijų paslaugų teikėjai apie ryšių duomenų teikimą turi du kartus per metus pranešti Mokslo ir IRT ministru⁽⁹⁹⁾.

Telekomunikacijų paslaugų teikėjai neprivalo vykdyti prašymų atskleisti ryšių duomenis remiantis TII. Todėl kiekvieną prašymą paslaugų teikėjas turi įvertinti atsižvelgdamas į pagal AIAI taikomus duomenų apsaugos reikalavimus. Visų pirma telekomunikacijų paslaugų teikėjas turi atsižvelgti į duomenų subjekto interesus ir negali atskleisti informacijos, jei tikėtina, kad dėl to galėtų būti nepagrįstai pažeisti asmens arba trečiosios šalies interesai⁽¹⁰⁰⁾. Be to, pagal pranešimą Nr. 2021-1 dėl papildomų taisyklių dėl Asmeninės informacijos apsaugos įstatymo aiškinimo ir taikymo atitinkamam asmeniui turi būti pranešama apie informacijos atskleidimą. Ypatingais atvejais pranešimas gali būti atidedamas, visų pirma, jei pranešus būtų kliudoma vykstančiam baudžiamajam tyrimui arba galėtų kilti pavojus kito asmens gyvybei ar fizinei sveikatai ir tol, kol tokie pavojai kiltų, kai tos teisės ar interesai yra akivaizdžiai viršesni už duomenų subjekto teises⁽¹⁰¹⁾.

2016 m. Aukščiausiasis Teismas patvirtino, kad savanorišku telekomunikacijų paslaugų teikėjų ryšių duomenų teikimu pagal TII negavus orderio savaime nepažeidžiama telekomunikacijų paslaugos naudotojo teisė į informaciją pagrįstą apsisprendimą. Tačiau Teismas paaiškino, kad toks pažeidimas būtų padarytas, jei būtų akivaizdu, kad prašančioji agentūra piktnaudžiavo savo įgaliojimais prašydama atskleisti ryšių duomenis, taip pažeisdama atitinkamo asmens ar trečiojo asmens interesus⁽¹⁰²⁾. Apskritai bet koks teisėsaugos institucijos prašymas savanoriškai atskleisti informaciją turi atitikti Korėjos Konstitucijoje nustatytus teisėtumo, būtinumo ir proporcingumo principus (12 straipsnio 1 dalis ir 37 straipsnio 2 dalis).

⁽⁸⁹⁾ RPAI 13-3 straipsnio 2 dalis.

⁽⁹⁰⁾ RPAI 13-3 straipsnio 3 dalis.

⁽⁹¹⁾ RPAI 13-3 straipsnio 4 dalis.

⁽⁹²⁾ RPAI 13-3 straipsnio 5 dalis.

⁽⁹³⁾ RPAI 13-3 straipsnio 6 dalis.

⁽⁹⁴⁾ TII 83 straipsnio 3 dalis.

⁽⁹⁵⁾ TII 2 straipsnio 9 dalis.

⁽⁹⁶⁾ TII 83 straipsnio 4 dalis.

⁽⁹⁷⁾ TII 83 straipsnio 4 dalis.

⁽⁹⁸⁾ TII 83 straipsnio 5 dalis.

⁽⁹⁹⁾ TII 83 straipsnio 6 dalis.

⁽¹⁰⁰⁾ AIAI 18 straipsnio 2 dalis.

⁽¹⁰¹⁾ AIAK pranešimo Nr. 2021-1 dėl papildomų taisyklių dėl Asmeninės informacijos apsaugos įstatymo aiškinimo ir taikymo III skirsnio 2 dalies iii punktą.

⁽¹⁰²⁾ 2016 m. kovo 10 d. Aukščiausiojo Teismo sprendimas Nr. 2012Da105482.

2.3. Priežiūra

Baudžiamosios teisėsaugos institucijų priežiūra vykdoma naudojantis skirtingais mechanizmais, tiek viduje, tiek išorės įstaigų.

2.3.1. Savikontrolė

Pagal Viešojo sektoriaus audito įstatymą valdžios institucijos raginamos steigti savikontrolės įstaigas, kurioms, be kita ko, būtų pavesta vykdyti teisėtumo tikrinimą⁽¹⁰³⁾. Turi būti užtikrinamas kuo didesnis tokių savikontrolės įstaigų vadovų nepriklausomumas⁽¹⁰⁴⁾. Konkrečiau, laikotarpiui nuo dvejų iki penkerių metų skiriami su atitinkama institucija nesusiję asmenys (pvz., buvę teisėjai, profesoriai) ir iš pareigų jie gali būti atleidžiami tik dėl pagrįstų priežasčių (pvz., kai jie negali atlikti pareigų dėl psichikos sutrikimo ar fizinės negalios, kai jiems taikomos drausminės priemonės)⁽¹⁰⁵⁾. Auditoriai taip pat skiriami atsižvelgiant į specialius įstatyme nustatytus reikalavimus⁽¹⁰⁶⁾. Audito ataskaitose gali būti pateikiamos rekomendacijos ar prašymai dėl kompensacijų ar pataisų, taip pat papeikimai ir rekomendacijos arba prašymai taikyti drausmines priemones⁽¹⁰⁷⁾. Apie jas per 60 dienų nuo audito pabaigos pranešama valdžios institucijos, kurios auditas atliekamas, vadovui, taip pat Audito ir inspektavimo valdybai (žr. 2.3.2 skirsnį)⁽¹⁰⁸⁾. Atitinkama institucija turi įgyvendinti reikiamas priemones ir rezultatus pateikti Audito ir inspektavimo valdybai⁽¹⁰⁹⁾. Be to, audito rezultatai paprastai skelbiami viešai⁽¹¹⁰⁾. Už atsisakymą atlikti savikontrolę arba trukdymą ją atlikti skiriamos administracinės baudos⁽¹¹¹⁾. Baudžiamosios teisėsaugos srityje Nacionalinė policijos agentūra, siekdama laikytis pirmiau minėtų teisės aktų, įgyvendina generalinio inspektoriaus sistemą, skirtą vykdyti savikontrolę, įskaitant galimų žmogaus teisių pažeidimų atveju⁽¹¹²⁾.

2.3.2. Audito ir inspektavimo valdyba

Audito ir inspektavimo valdyba (toliau – AIV) gali tikrinti valdžios institucijų veiklą ir, remdamasi tokiais patikrinimais, teikti rekomendacijas, prašyti taikyti drausmines priemones arba pateikti skundą dėl nusikalstamos veikos⁽¹¹³⁾. AIV yra įsteigta Korėjos Respublikos Prezidento, tačiau vykdydama savo pareigas yra nepriklausoma⁽¹¹⁴⁾. Be to, įstatyme, kuriuo įsteigta AIV, reikalaujama, kad AIV būtų kuo labiau nepriklausoma jai priimant, atleidžiant ir organizuojant savo žmogiškuosius išteklius, taip pat sudarant savo biudžetą⁽¹¹⁵⁾. AIV pirmininką skiria Prezidentas, gavęs Nacionalinės Asamblėjos sutikimą⁽¹¹⁶⁾. Likusius šešis komisijos narius ketverių metų kadencijai skiria pirmininkas, remdamasis Prezidento rekomendacija⁽¹¹⁷⁾. Komisijos nariai (įskaitant pirmininką) turi turėti įstatymų nustatytą konkrečią kvalifikaciją⁽¹¹⁸⁾ ir atleisti jie gali būti tik tada, jei jiems vykdoma apkalta, skiriama laisvės atėmimo bausmė arba jie nebegali vykdyti savo pareigų dėl užsitiesusios fizinės ar psichinės negalios⁽¹¹⁹⁾. Be to, komisijos nariams draudžiama dalyvauti politinėje veikloje ir tuo pačiu metu eiti pareigas Nacionalinėje Asamblėjoje, administracinėse agentūrose, organizacijose, kurių auditą ir inspektavimą atlieka AIV, arba bet kurioje kitoje įstaigoje ar pareigose už atlygį⁽¹²⁰⁾.

AIV kasmet atlieka bendrą auditą, tačiau taip pat gali atlikti specialų auditą, susijusį su ypatingos svarbos klausimais. Inspektavimo metu AIV gali prašyti, kad būtų pateikti dokumentai ir kad dalyvautų konkretūs asmenys⁽¹²¹⁾. Atliekdama auditą AIV tikrina valstybės pajamas ir išlaidas, taip pat prižiūri, kaip bendrai valdžios institucijos ir valstybės pareigūnai

⁽¹⁰³⁾ Viešojo sektoriaus audito įstatymo 3 ir 5 straipsniai.

⁽¹⁰⁴⁾ Viešojo sektoriaus audito įstatymo 7 straipsnis.

⁽¹⁰⁵⁾ Viešojo sektoriaus audito įstatymo 8–11 straipsniai.

⁽¹⁰⁶⁾ Viešojo sektoriaus audito įstatymo 16 ir tolesni straipsniai.

⁽¹⁰⁷⁾ Viešojo sektoriaus audito įstatymo 23 straipsnio 2 dalis.

⁽¹⁰⁸⁾ Viešojo sektoriaus audito įstatymo 23 straipsnio 1 dalis.

⁽¹⁰⁹⁾ Viešojo sektoriaus audito įstatymo 23 straipsnio 3 dalis.

⁽¹¹⁰⁾ Viešojo sektoriaus audito įstatymo 26 straipsnis.

⁽¹¹¹⁾ Viešojo sektoriaus audito įstatymo 41 straipsnis.

⁽¹¹²⁾ Visų pirma žr. Audito ir inspektavimo generaliniam direktoriui atskaitingus skyrius: <https://www.police.go.kr/eng/knpa/org/org01.jsp>.

⁽¹¹³⁾ Audito ir inspektavimo valdybos įstatymo (toliau – AIV įstatymas) 24 ir 31–35 straipsniai.

⁽¹¹⁴⁾ AIV įstatymo 2 straipsnio 1 dalis.

⁽¹¹⁵⁾ AIV įstatymo 2 straipsnio 2 dalis.

⁽¹¹⁶⁾ AIV įstatymo 4 straipsnio 1 dalis.

⁽¹¹⁷⁾ AIV įstatymo 5 straipsnio 1 dalis ir 6 straipsnis.

⁽¹¹⁸⁾ Pvz., ne mažiau kaip dešimt metų teisėjo, prokuroro ar advokato pareigose, ne mažiau kaip aštuoneri metai valstybės tarnautojo, universiteto dėstytojo ar aukštesnėse pareigose universitete arba bent dešimt metų darbo biržinėje bendrovėje ar vyriausybės valdomoje institucijoje (iš kurių bent penkeri metai vykdomojo pareigūno pareigose) (žr. AIV įstatymo 7 straipsnį).

⁽¹¹⁹⁾ AIV įstatymo 8 straipsnis.

⁽¹²⁰⁾ AIV įstatymo 9 straipsnis.

⁽¹²¹⁾ Žr., pvz., AIV įstatymo 27 straipsnį.

vykdo savo pareigas, siekdama pagerinti viešojo administravimo veikimą⁽¹²²⁾. Todėl jos atliekama priežiūra apima ne tik biudžeto aspektus, bet ir teisėtumo tikrinimą.

2.3.3. Nacionalinė Asamblėja

Nacionalinė Asamblėja gali tirti ir tikrinti valdžios institucijas⁽¹²³⁾. Tyrimo ar inspektavimo metu Nacionalinė Asamblėja gali prašyti atskleisti dokumentus ir įpareigoti liudytojus liudyti⁽¹²⁴⁾. Bet kuriam asmeniui Nacionalinės Asamblėjos tyrimo metu pateikiamam melagingus parodymus taikomos baudžiamosios sankcijos (iki dešimties metų laisvės atėmimo bausmė)⁽¹²⁵⁾. Inspektavimo procesas ir rezultatai gali būti skelbiami viešai⁽¹²⁶⁾. Jei Nacionalinė Asamblėja nustato neteisėtą ar netinkamą veiklą, ji gali prašyti, kad atitinkama valdžios institucija imtųsi taisomųjų veiksmų, be kita ko, skirtų kompensacijas, taikytų drausmines priemones ir tobulintų savo vidaus procedūras⁽¹²⁷⁾. Gavusi tokią prašymą, institucija turi nedelsdama imtis veiksmų ir Nacionalinei Asamblėjai pranešti apie rezultatus⁽¹²⁸⁾.

2.3.4. Asmeninės informacijos apsaugos komisija

Asmeninės informacijos apsaugos komisija (toliau – AIAK) prižiūri, kad baudžiamosios teisėsaugos institucijos tvarkytų asmeninę informaciją pagal AIAĮ. Be to, pagal AIAĮ 7-8 straipsnio 3 ir 4 dalis ir 7-9 straipsnio 5 dalį AIAK priežiūra taip pat apima galimus taisyklių, kuriomis nustatomi asmeninės informacijos rinkimo apribojimai ir apsaugos priemonės, įskaitant nustatytus konkrečiuose įstatymuose, reglamentuojančiuose (elektroninių) įrodymų rinkimą baudžiamosios teisėsaugos tikslais, pažeidimus (žr. 2.2 skirsnį). Atsižvelgiant į AIAĮ 3 straipsnio 1 dalyje nustatytus reikalavimus dėl teisėto ir sąžiningo asmeninės informacijos rinkimo, toks pažeidimas taip pat yra AIAĮ pažeidimas, todėl AIAK leidžiama atlikti tyrimą ir taikyti taisomuosius veiksmus⁽¹²⁹⁾.

Vykdydama priežiūros funkciją AIAK turi prieigą prie visos aktualios informacijos⁽¹³⁰⁾. AIAK gali teikti teisėsaugos institucijoms konsultacijas dėl jų taikomo asmeninės informacijos apsaugos lygio gerinimo joms vykdant duomenų tvarkymo veiklą, taisomųjų veiksmų taikymo (pvz., sustabdyti duomenų tvarkymą arba imtis būtinų priemonių asmens informacijai apsaugoti) arba patarti institucijai imtis drausminių priemonių⁽¹³¹⁾. Galiausiai numatytos baudžiamosios sankcijos už tam tikrus AIAĮ pažeidimus, pavyzdžiui, už neteisėtą asmeninės informacijos naudojimą ar atskleidimą trečiosioms šalims arba neteisėtą neskelbtinos informacijos tvarkymą⁽¹³²⁾. Tokiu atveju AIAK gali perduoti klausimą nagrinėti kompetentingai tyrimo agentūrai (įskaitant prokurorą)⁽¹³³⁾.

2.3.5. Nacionalinė žmogaus teisių komisija

Nacionalinė žmogaus teisių komisija (toliau – NŽTK) – nepriklausoma institucija, kuriai pavesta saugoti ir remti pagrindines teises⁽¹³⁴⁾ – turi įgaliojimus tirti ir ištaisyti Konstitucijos 10–22 straipsnių, įskaitant teisės į privatumą ir susirašinėjimo privatumą, pažeidimus. NŽTK sudaro 11 komisijos narių, kuriuos siūlo Nacionalinė Asamblėja (keturis), Prezidentas (keturis) ir Aukščiausiojo Teismo vyriausiasis teisėjas (tris)⁽¹³⁵⁾. Kad būtų paskirtas komisijos nariu asmuo turi būti 1) bent dešimt metų dirbęs universitete arba įgaliotame mokslinių tyrimų institute, ne žemesnėse kaip docento pareigose, 2) bent dešimt metų dirbęs teisėju, prokuroru ar advokatu, 3) bent dešimt metų dalyvavęs veikloje, susijusioje su žmogaus teisėmis (pvz., ne pelno siekiančioje, nevyriausybinėje organizacijoje arba tarptautinėje organizacijoje) arba 4) rekomenduotas pilietinės visuomenės grupės⁽¹³⁶⁾. Pirmininką iš komisijos narių skiria Prezidentas, o šį paskyrimą turi

⁽¹²²⁾ AIV įstatymo 20 ir 24 straipsniai.

⁽¹²³⁾ Nacionalinės Asamblėjos įstatymo 128 straipsnis ir Valstybės administracijos inspektavimo ir tyrimo įstatymo 2, 3 ir 15 straipsniai. Tai apima kasmetinius vyriausybės veiklų visumos patikrinimus ir tyrimus, susijusius su konkrečiais klausimais.

⁽¹²⁴⁾ Valstybės administracijos inspektavimo ir tyrimo įstatymo 10 straipsnio 1 dalis. Taip pat žr. Nacionalinės Asamblėjos įstatymo 128 ir 129 straipsnius.

⁽¹²⁵⁾ Įstatymo dėl liudijimo, vertinimo ir kt. Nacionalinėje Asamblėjoje 14 straipsnis.

⁽¹²⁶⁾ Valstybės administracijos inspektavimo ir tyrimo įstatymo 12-2 straipsnis.

⁽¹²⁷⁾ Valstybės administracijos inspektavimo ir tyrimo įstatymo 16 straipsnio 2 dalis.

⁽¹²⁸⁾ Valstybės administracijos inspektavimo ir tyrimo įstatymo 16 straipsnio 3 dalis.

⁽¹²⁹⁾ Žr. AIAK pranešimą Nr. 2021-1 dėl papildomų taisyklių dėl Asmeninės informacijos apsaugos įstatymo aiškinimo ir taikymo.

⁽¹³⁰⁾ AIAĮ 63 straipsnis.

⁽¹³¹⁾ AIAĮ 61 straipsnio 2 dalis, 65 straipsnio 1 ir 2 dalys ir 64 straipsnio 4 dalis.

⁽¹³²⁾ AIAĮ 70–74 straipsniai.

⁽¹³³⁾ AIAĮ 65 straipsnio 1 dalis.

⁽¹³⁴⁾ Žmogaus teisių komisijos įstatymo (toliau – NŽTK įstatymas) 1 straipsnis.

⁽¹³⁵⁾ NŽTK įstatymo 5 straipsnio 1 ir 2 dalys.

⁽¹³⁶⁾ NŽTK įstatymo 5 straipsnio 3 dalis.

patvirtinti Nacionalinė Asamblėja⁽¹³⁷⁾. Komisijos nariai (įskaitant pirmininką) skiriami trejų metų kadencijai, kuri gali būti pratęsta, o atleisti jie gali būti tik tada, kai jiems skiriama laisvės atėmimo bausmė arba jie nebegali vykdyti savo pareigų dėl užsitęsusių fizinės ar psichinės negalios (tokiu atveju du trečdaliai komisijos narių turi pritarti atleidimui iš pareigų)⁽¹³⁸⁾. NŽTK nariams draudžiama tuo pačiu metu eiti pareigas Nacionalinėje Asamblėjoje, vietos tarybose arba bet kurioje valstybės ar vietos valdžios institucijoje (valstybės pareigūno pareigas)⁽¹³⁹⁾.

NŽTK gali pradėti tyrimą savo iniciatyva arba remdamasi asmens peticija. Atlikdama tyrimą, NŽTK gali prašyti pateikti atitinkamą medžiagą, atlikti patikrinimus ir kvieisti asmenis liudyti⁽¹⁴⁰⁾. Atlikusi tyrimą, NŽTK gali teikti rekomendacijas, kaip tobulinti arba taisyti konkrečią politiką ir praktiką, ir gali jas paskelbti viešai⁽¹⁴¹⁾. Valdžios institucijos turi pateikti NŽTK tokių rekomendacijų įgyvendinimo planą per 90 dienų nuo jų gavimo⁽¹⁴²⁾. Be to, jei rekomendacijos neįgyvendinamos, atitinkama institucija apie tai turi pranešti komisijai⁽¹⁴³⁾. NŽTK savo ruožtu gali pranešti apie tokių nevykdymą Nacionalinei Asamblėjai ir (arba) apie jį paskelbti viešai. Valdžios institucijos iš esmės laikosi NŽTK rekomendacijų ir turi rimtų paskatų tai daryti, nes jų įgyvendinimas vertinamas Vyriausybės politikos koordinavimo biurui atliekant bendrą vertinimą, kuriam vadovauja Ministro Pirmininko kanceliarija.

2.4. Individualios teisių gynimo priemonės

2.4.1. AIAĮ nustatyti teisių gynimo mechanizmai

Pagal AIAĮ asmenys turi teisę susipažinti su baudžiamosios teisėsaugos institucijų tvarkoma asmenine informacija, reikalauti ją ištaisyti, ištrinti ir sustabdyti jos tvarkymą. Prašyti susipažinti su informacija galima tiesiogiai atitinkamos institucijos arba netiesiogiai per AIAK⁽¹⁴⁴⁾. Kompetentinga institucija gali apriboti susipažinimą su informacija arba jį uždrausti tik tais atvejais, kai tai numatyta teisės aktuose, kai dėl to gali kilti grėsmė trečiosios šalies gyvybei ar fizinei sveikatai arba kai tikėtina, kad bus padarytas nepagrįstas kito asmens turinių ir kitų interesų pažeidimas (t. y. kai kito asmens interesai būtų viršesni už prašymą pateikusių asmens interesus)⁽¹⁴⁵⁾. Jei prašymas leisti susipažinti su informacija atmetamas, asmeniui turi būti nurodomos atmetimo priežastys ir pateikiama informacija apie tai, kaip tokių sprendimų galima apskūsti⁽¹⁴⁶⁾. Be to, prašymas ištaisyti ar ištrinti duomenis gali būti atmetamas, jei tokia galimybė numatyta kituose teisės aktuose; tokiu atveju asmeniui turi būti nurodytos prašymo atmetimo priežastys ir pateikiama informacija apie galimybę tokių sprendimų apskūsti⁽¹⁴⁷⁾.

Teisių gynimo atžvilgiu asmenys gali pateikti skundą AIAK, be kita ko, per Korėjos interneto ir saugumo agentūros administruojamą privatumo apsaugos skambučių centrą⁽¹⁴⁸⁾. Be to, asmuo gali kreiptis į Tarpininkavimo ginčiuose dėl asmeninės informacijos komitetą⁽¹⁴⁹⁾. Šiomis teisių gynimo priemonėmis galima pasinaudoti, jei pažeidžiamos taisyklės, nustatytos konkrečiuose įstatymuose, kuriais nustatomi apribojimai ir apsaugos priemonės, susijusios su asmeninės informacijos rinkimu (2.2 skirsnis), ir jei pažeidžiamas AIAĮ. Be to, asmenys gali užginčyti AIAK sprendimus arba neveikimą pagal Administracinių ginčų įstatymą (žr. 2.4.3 skirsnį).

⁽¹³⁷⁾ NŽTK įstatymo 5 straipsnio 5 dalis.

⁽¹³⁸⁾ NŽTK įstatymo 7 straipsnio 1 dalis ir 8 straipsnis.

⁽¹³⁹⁾ NŽTK įstatymo 10 straipsnis.

⁽¹⁴⁰⁾ NŽTK įstatymo 36 straipsnis. Pagal įstatymo 36 straipsnio 7 dalį gali būti atsisakyta pateikti medžiagą ar daiktinius įrodymus, jei taip būtų atskleista konfidenciali valstybinė informacija, o tai galėtų turėti esminės įtakos valstybės saugumui ar diplomatiniam santykiams arba dėl to kiltų didelių kliūčių vykdant baudžiamąjį tyrimą ar būsimą teismo procesą. Tokiais atvejais komisija gali prašyti atitinkamos agentūros vadovo papildomos informacijos (kuris turi gera valia ją pateikti), jei tai būtina siekiant patikrinti, ar atsakymas suteikti informaciją yra pagrįstas.

⁽¹⁴¹⁾ NŽTK įstatymo 25 straipsnio 1 dalis.

⁽¹⁴²⁾ NŽTK įstatymo 25 straipsnio 3 dalis.

⁽¹⁴³⁾ NŽTK įstatymo 25 straipsnio 4 dalis.

⁽¹⁴⁴⁾ AIAĮ 35 straipsnio 2 dalis.

⁽¹⁴⁵⁾ AIAĮ 35 straipsnio 4 dalis.

⁽¹⁴⁶⁾ AIAĮ vykdymo užtikrinimo dekreto 42 straipsnio 2 dalis.

⁽¹⁴⁷⁾ AIAĮ 36 straipsnio 1–2 dalys ir AIAĮ vykdymo užtikrinimo dekreto 43 straipsnio 3 dalis.

⁽¹⁴⁸⁾ AIAĮ 62 straipsnis.

⁽¹⁴⁹⁾ AIAĮ 40–50 straipsniai ir AIAĮ vykdymo užtikrinimo dekreto 48–57 straipsniai.

2.4.2. Teisių gynimas Nacionalinėje žmogaus teisių komisijoje

NŽTK nagrinėja asmenų (tiek Korėjos, tiek užsienio valstybių piliečių) skundus dėl valdžios institucijų padarytų žmogaus teisių pažeidimų⁽¹⁵⁰⁾. Asmenims nebūtina skundą pateikti NŽTK⁽¹⁵¹⁾. Skundą NŽTK nagrinėja net jei nagrinėjant skundo priimtinumą atitinkamas asmuo negali įrodyti, kad buvo padaryta žala. Todėl kai asmens duomenys renkami baudžiamosios teisėsaugos tikslais, asmuo, siekdamas, kad jo skundą priimtų nagrinėti NŽTK, neprivalo įrodyti, kad Korėjos valdžios institucijos iš tikrųjų susipažino su jo asmenine informacija. Asmuo taip pat gali prašyti skundą išspręsti tarpininkaujant⁽¹⁵²⁾.

Norėdama iširti skundą NŽTK gali naudotis savo tyrimo įgaliojimais, be kita ko, prašyti pateikti atitinkamą medžiagą, atlikti patikrinimus ir kviesti asmenis liudyti⁽¹⁵³⁾. Jeigu atlikus tyrimą nustatoma, kad buvo pažeisti atitinkami teisės aktai, NŽTK gali rekomenduoti įgyvendinti teisių gynimo priemones arba taisyti ar tobulinti atitinkamą įstatymą, instituciją, politiką ar praktiką⁽¹⁵⁴⁾. Siūlomos teisių gynimo priemonės gali apimti tarpininkavimą, žmogaus teisių pažeidimo nutraukimą, žalos atlyginimą ir priemones, kuriomis siekiama užkirsti kelią tokių pačių ar panašių pažeidimų pasikartojimui⁽¹⁵⁵⁾. Neteisėto asmeninės informacijos rinkimo pagal taikomas taisykles atveju teisių gynimo priemonės gali apimti ir surinktos asmeninės informacijos ištrynimą. Jei manoma, kad labai tikėtina, jog pažeidimas yra tęstinio pobūdžio, ir kad tikėtina, jog nesiėmus veiksmų, būtų padaryta sunkiai atitaisoma žala, NŽTK gali taikyti skubias paramos priemones⁽¹⁵⁶⁾.

Nors NŽTK neturi įgaliojimų įpareigoti, jos sprendimai (pvz., sprendimas netęsti skundo nagrinėjimo)⁽¹⁵⁷⁾ ir rekomendacijos gali būti ginčijami Korėjos teismuose pagal Administracinių ginčų įstatymą (žr. 2.4.3 skirsnį)⁽¹⁵⁸⁾. Be to, jei iš NŽTK išvadų matyti, kad valdžios institucija neteisėtai rinko asmens duomenis, asmuo gali siekti tolesnių teisių gynimo veiksmų tos valdžios institucijos atžvilgiu Korėjos teismuose, pvz., užginčyti duomenų rinkimą pagal Administracinių ginčų įstatymą, pateikti konstitucinį skundą pagal Konstitucinio Teismo įstatymą arba prašyti atlyginti žalą pagal Valsybės kompensacijų įstatymą (žr. 2.4.3 skirsnį).

2.4.3. Teisminis teisių gynimas

Asmenys gali remtis ankstesniuose skirsniuose aprašytais apribojimais ir apsaugos priemonėmis siekdami įvairiais būdais ginti savo teises Korėjos teismuose.

Visų pirma pagal BPI atitinkamas asmuo ir jo advokatas gali dalyvauti, kai vykdomas kratos ar poėmio orderis, todėl jis gali pareikšti prieštaravimą orderio vykdymo metu⁽¹⁵⁹⁾. Be to, BPI numatytas vadinamojo „kvaziskundo“ mechanizmas, kuriuo asmenims sudaromos sąlygos kreiptis į kompetentingą teismą su prašymu panaikinti arba pakeisti prokuroro ar policijos pareigūno priimtą sprendimą dėl poėmio⁽¹⁶⁰⁾. Taip asmenims sudaromos sąlygos užginčyti priemones, kurių buvo imtasi siekiant įvykdyti poėmio orderį.

⁽¹⁵⁰⁾ NŽTK įstatymo 4 straipsnyje nurodomi Korėjos Respublikoje gyvenantys piliečiai ir užsienio valstybių piliečiai, bet terminu „gyvenantys“ atspindima jurisdikcijos, o ne teritorijos sąvoka. Todėl, jei nacionalinės institucijos Korėjoje pažeidžia už Korėjos ribų esančio užsienio valstybės piliečio pagrindines teises, tas asmuo gali pateikti skundą NŽTK. Žr., pavyzdžiui, atitinkamą klausimą NŽTK dažnai užduodamų klausimų puslapyje, kurį galima rasti adresu <https://www.humanrights.go.kr/site/program/board/basicboard/list?boardtypeid=7025&menuid=002004005001&pagesize=10¤tpage=2>. Taip būtų tais atvejais, kai Korėjos valdžios institucijos neteisėtai susipažintų su į Korėją perduotais užsienio valstybės piliečio asmens duomenimis.

⁽¹⁵¹⁾ Skundas iš esmės turi būti pateiktas per vienus metus nuo pažeidimo įvykdymo, tačiau NŽTK gali nuspręsti nagrinėti skundą, pateiktą jau pasibaigus šiam terminui, jei dar nepasiektas senaties terminas pagal baudžiamąją arba civilinę teisę (NŽTK įstatymo 32 straipsnio 1 dalies 4 punktas).

⁽¹⁵²⁾ NŽTK įstatymo 42 ir tolesni straipsniai.

⁽¹⁵³⁾ NŽTK įstatymo 36 ir 37 straipsniai.

⁽¹⁵⁴⁾ NŽTK įstatymo 44 straipsnis.

⁽¹⁵⁵⁾ NŽTK įstatymo 42 straipsnio 4 dalis.

⁽¹⁵⁶⁾ NŽTK įstatymo 48 straipsnis.

⁽¹⁵⁷⁾ Pavyzdžiui, jei išimtinu atveju NŽTK negali tikrinti tam tikros medžiagos ar priemonių dėl to, kad jos susijusios su valstybės paslaptimis, galinčiomis turėti didelį poveikį valstybės saugumui ar diplomatiniais santykiams, arba jei tikrinant būtų sukurtos rimtos kliūtys baudžiamajam tyrimui ar būsimam teismo procesui (žr. 166 išnašą) ir jei tai trukdo NŽTK atlikti tyrimą, būtiną gautos peticijos pagrįstumui įvertinti, ji informuoja asmenį apie priežastis, dėl kurių skundas buvo atmestas pagal NŽTK įstatymo 39 straipsnį. Tokiu atveju asmuo galėtų užginčyti NŽTK sprendimą pagal Administracinių ginčų įstatymą.

⁽¹⁵⁸⁾ Žr., pvz., 2008 m. balandžio 18 d. Seulo Aukštojo Teismo sprendimą 2007Nu27259, patvirtintą 2008 m. spalio 9 d. Aukščiausiojo Teismo sprendimu 2008Du7854; 2018 m. vasario 2 d. Seulo Aukštojo Teismo sprendimą 2017Nu69382.

⁽¹⁵⁹⁾ BPI 121 ir 219 straipsniai.

⁽¹⁶⁰⁾ BPI 417 straipsnis kartu su BPI 414 straipsnio 2 dalimi. Taip pat žr. 1997 m. rugsėjo 29 d. Aukščiausiojo Teismo sprendimą 97Mo66.

Be to, asmenys gali reikalauti žalos atlyginimo Korėjos teismuose. Remdamiesi Valstybės kompensacijų įstatymu, asmenys gali prašyti kompensacijos už žalą, kurią valstybės pareigūnai padarė pažeidę įstatymą, kai vykdė savo oficialias pareigas⁽¹⁶¹⁾. Reikalavimas atlyginti žalą pagal Valstybės kompensacijų įstatymą gali būti pateiktas specializuotai „kompensacijos tarybai“ arba tiesiogiai Korėjos teismuose⁽¹⁶²⁾. Jei nukentėjusysis yra užsienio valstybės pilietis, Valstybės kompensacijų įstatymas jam taikomas tada, kai to piliečio kilmės šalis taip pat užtikrina valstybės kompensaciją Korėjos piliečiams⁽¹⁶³⁾. Remiantis teismų praktika, ši sąlyga laikoma įvykdyta, jei reikalavimai prašant kompensacijos kitoje šalyje „nėra labai skirtingi Korėjoje ir kitoje šalyje“ ir „bendrai nėra griežtesni už reikalavimus, nustatytus Korėjoje, nėra reikšmingai ir iš esmės skirtingi“⁽¹⁶⁴⁾. Civiliniu įstatymu reglamentuojama valstybės atsakomybė atlyginti žalą, todėl ji apima ir neturtinę žalą (pvz., psichinę kančią)⁽¹⁶⁵⁾.

Duomenų apsaugos taisyklių pažeidimo atveju AIAĮ numatyta papildoma teisinė teisių gynimo priemonė. Pagal AIAĮ 39 straipsnį kiekvienas asmuo, patyręs žalą dėl AIAĮ pažeidimo arba dėl jo asmeninės informacijos praradimo, vagystės, atskleidimo, suklastojimo, pakeitimo ar sugadinimo, gali reikalauti žalos atlyginimo teisme. Abipusiškumo reikalavimas, panašus į nustatytą Valstybės kompensacijų įstatymu, nėra taikomas.

Be žalos atlyginimo, pagal Administracinių ginčų įstatymą numatytas administracinis teisių gynimas nukentėjus nuo administracinių įstaigų veiksmų ar neveikimo. Kiekvienas asmuo gali užginčyti sprendimą (t. y. viešųjų įgaliojimų naudojimą ar atsakymą juos naudoti konkrečiu atveju) arba neveikimą (administracinei agentūrai ilgą laiką nepriimant tam tikro sprendimo, kai tai prieštarauja teisei prievolei tai daryti), o tai gali lemti neteisėto sprendimo panaikinimą (pakeitimą), pripažinimą niekiniu (t. y. konstatavimą, kad sprendimas neturi teisinės galios arba kad ji neegzistuoja teisinėje sistemoje) arba neveikimo pripažinimą neteisėtu⁽¹⁶⁶⁾. Kad būtų galima užginčyti administracinį sprendimą, jis turi daryti tiesioginį poveikį civilinėms teisėms ir pareigoms⁽¹⁶⁷⁾. Tai, be kita ko, yra priemonės, skirtos asmens duomenims rinkti, kai jie renkami tiesiogiai (pvz., perimant ryšius) arba pateikiant atskleidimo prašymą (pvz., paslaugų teikėjui).

Anksčiau nurodyti reikalavimai gali būti pirmiausia pateikti administracinėms apeliacinėms komisijoms, įsteigtoms tam tikrų valdžios institucijų (pvz., NŽT, NŽTK), arba Centrinei administracinei apeliacinei komisijai, įsteigtai Kovos su korupcija ir pilietinių teisių komisijoms⁽¹⁶⁸⁾. Toks administracinis skundas yra alternatyvus, mažiau oficialus būdas užginčyti valdžios institucijos sprendimą arba neveikimą. Tačiau reikalavimas taip pat gali būti pateikiamas tiesiogiai Korėjos teismuose, remiantis Administracinių ginčų įstatymu.

Prašymą panaikinti (pakeisti) sprendimą pagal Administracinių ginčų įstatymą gali pateikti bet kuris asmuo, turintis teisinį interesą siekti, kad jis būtų panaikintas (pakeistas) arba kad jo teisės būtų atkurtos panaikinant arba pakeičiant sprendimą, jei sprendimas nebeturi galios⁽¹⁶⁹⁾. Reikalavimą sprendimą pripažinti negaliojančiu taip pat gali pateikti asmuo, turintis teisinį interesą siekti tokio pripažinimo, o reikalavimą pripažinti neveikimą neteisėtu gali pateikti bet kuris asmuo, pateikęs prašymą priimti sprendimą ir turintis teisinį interesą siekti, kad neveikimas būtų pripažintas neteisėtu⁽¹⁷⁰⁾. Pagal Aukščiausiojo Teismo praktiką „teisinis interesas“ suprantamas kaip „teisiškai saugomas interesas“, t. y. tiesioginis ir konkretus interesas, saugomas įstatymais ir kitais teisės aktais, kuriais grindžiami administraciniai sprendimai (t. y. jais negali būti bendri, netiesioginiai ir abstraktūs visuomenės interesai)⁽¹⁷¹⁾. Todėl asmenys tokį teisinį interesą turi tuo atveju, kai pažeidžiami apribojimai ir apsaugos priemonės, taikomos jų asmens duomenų rinkimui baudžiamosios teisės saugos tikslais (pagal specialius įstatymus arba AIAĮ). Pagal Administracinių ginčų įstatymą šalis privalo įgyvendinti galutinį sprendimą⁽¹⁷²⁾.

Prašymas panaikinti (pakeisti) sprendimą ir prašymas pripažinti neveikimą neteisėtu turi būti pateiktas per 90 dienų nuo tos dienos, kai asmuo sužinojo apie sprendimą arba neveikimą, ir iš esmės ne vėliau kaip per vienus metus nuo

⁽¹⁶¹⁾ Valstybės kompensacijų įstatymo 2 straipsnio 1 dalis.

⁽¹⁶²⁾ Valstybės kompensacijų įstatymo 9 ir 12 straipsniai. Įstatymu įsteigiamos apygardų tarybos (kurioms pirmininkauja atitinkamos prokuratūros prokuroro pavaduotojas), centrinė taryba (kurai pirmininkauja Teisingumo ministro pavaduotojas) ir specialioji taryba (kurai pirmininkauja Nacionalinės gynybos ministro pavaduotojas ir kuri atsakinga už reikalavimus atlyginti žalą, padarytą karinio personalo arba civilių kariuomenės darbuotojų). Prašymus atlyginti žalą iš esmės nagrinėja apygardų tarybos, kurios esant tam tikroms aplinkybėmis bylas turi perduoti centrinei arba specialiajai tarybai, pvz., jei kompensacija viršija tam tikrą sumą arba jei asmuo kreipiasi dėl pakartotinio svarstymo. Visas tarybas sudaro Teisingumo ministro paskirti nariai (pvz., iš Teisingumo ministerijos valstybės pareigūnų, teismų pareigūnų, teisininkų ir asmenų, turinčių patirties valstybės kompensacijų srityje) ir jiems taikomos specialios taisyklės dėl interesų konflikto (žr. Valstybės kompensacijų įstatymo vykdymo užtikrinimo dekretu 7 straipsnį).

⁽¹⁶³⁾ Valstybės kompensacijų įstatymo 7 straipsnis.

⁽¹⁶⁴⁾ 2015 m. birželio 11 d. Aukščiausiojo Teismo sprendimas Nr. 2013Da208388.

⁽¹⁶⁵⁾ Žr. Valstybės kompensacijų įstatymo 8 straipsnį, taip pat Civilinio įstatymo 751 straipsnį.

⁽¹⁶⁶⁾ Administracinių ginčų įstatymo 2 ir 4 straipsniai.

⁽¹⁶⁷⁾ 1999 m. spalio 22 d. Aukščiausiojo Teismo sprendimas 98Du18435, 2000 m. rugsėjo 8 d. Aukščiausiojo Teismo sprendimas 99Du1113 ir 2012 m. rugsėjo 27 d. Aukščiausiojo Teismo sprendimas 2010Du3541.

⁽¹⁶⁸⁾ Administracinių skundų įstatymo 6 straipsnis ir Administracinių ginčų įstatymo 18 straipsnio 1 dalis.

⁽¹⁶⁹⁾ Administracinių ginčų įstatymo 12 straipsnis.

⁽¹⁷⁰⁾ Administracinių ginčų įstatymo 35 ir 36 straipsniai.

⁽¹⁷¹⁾ 2006 m. kovo 26 d. Aukščiausiojo Teismo sprendimas Nr. 2006Du330.

⁽¹⁷²⁾ Administracinių ginčų įstatymo 30 straipsnio 1 dalis.

sprendimo paskelbimo arba neveikimo dienos, išskyrus atvejus, kai tam yra pagrįstų priežasčių⁽¹⁷³⁾. Pagal Aukščiausiojo Teismo praktiką „pagrįstų priežasčių“ sąvoka turi būti aiškinama plačiai ir ją taikant reikalaujama įvertinti, ar socialiai priimtina leisti pateikti skundą pavėluotai, atsižvelgiant į visas bylos aplinkybes⁽¹⁷⁴⁾. Tai yra, pavyzdžiui, vėlavimo priežastys (jomis neapsiribojant), už kurias susijusi šalis negali būti laikoma atsakinga (t. y. situacijos, kurių skundo teikėjas negali kontroliuoti, pavyzdžiui, kai jam nebuvo pranešta apie jo asmeninės informacijos rinkimą), arba *force majeure* (pvz., stichinė nelaimė, karas).

Galiausiai asmenys taip pat gali pateikti konstitucinį skundą Konstituciniam Teismui⁽¹⁷⁵⁾. Remiantis Konstitucinio Teismo įstatymu, bet kuris asmuo, kurio Konstitucija garantuojamos pagrindinės teisės yra pažeidžiamos valdžios institucijoms naudojantis savo įgaliojimais arba jų nevykdant (išskyrus teismų sprendimus), gali prašyti priimti sprendimą dėl konstitucinio skundo. Jei yra kitų teisių gynimo priemonių, pirmiausia turi būti naudojamos jomis. Pagal Konstitucinio Teismo praktiką užsienio valstybių piliečiai gali pateikti konstitucinį skundą tais atvejais, kai jų pagrindinės teisės pripažįstamos pagal Korėjos Konstituciją (žr. 1.1 skirsnyje pateiktus paaiškinimus)⁽¹⁷⁶⁾. Konstituciniai skundai turi būti pateikti per 90 dienų nuo tos dienos, kai asmuo sužinojo apie pažeidimą, ir per vienus metus nuo tada, kai buvo įvykdytas pažeidimas. Atsižvelgiant į tai, kad ginčų nagrinėjimui pagal Konstitucinio Teismo įstatymą taikoma Administracinių ginčų įstatyme nustatyta procedūra,⁽¹⁷⁷⁾ skundas vis tiek bus priimtinas, jei yra „pagrįstų priežasčių“, kaip aiškinama remiantis anksčiau aprašyta Aukščiausiojo Teismo praktika.

Jei pirmiausia reikia naudotis kitomis teisių gynimo priemonėmis, konstitucinis skundas turi būti pateiktas per 30 dienų nuo galutinio sprendimo dėl tokios teisių gynimo priemonės priėmimo⁽¹⁷⁸⁾. Konstitucinis Teismas gali panaikinti vyriausybės įgaliojimų vykdymą, dėl kurio buvo padarytas pažeidimas, arba patvirtinti, kad tam tikras neveikimas prieštarauja Konstitucijai⁽¹⁷⁹⁾. Tokiu atveju atitinkama institucija privalo imtis priemonių, kad būtų įvykdytas Teismo sprendimas.

3. VYRIAUSYBĖS GALIMYBĖ SUSIPAŽINTI SU INFORMACIJA NACIONALINIO SAUGUMO TIKSLAIS

3.1. Nacionalinio saugumo srityje kompetentingos valdžios institucijos

Korėjos Respublikoje yra dvi specialios žvalgybos agentūros – NŽT ir Paramos saugumui gynybos vadavietė. Be to, policija ir prokuratūra taip pat gali rinkti asmeninę informaciją nacionalinio saugumo tikslais.

NŽT įsteigta Nacionalinės žvalgybos tarnybos įstatymu (toliau – NŽT įstatymas) ir jos veikla priklauso tiesiogiai Prezidento jurisdikcijai bei jai taikoma jo priežiūra⁽¹⁸⁰⁾. Visų pirma NŽT renka, rengia ir teikia informaciją apie užsienio šalis (ir Šiaurės Korėją)⁽¹⁸¹⁾, žvalgybos informaciją, susijusią su užduotimis dėl kovos su šnipinėjimu (įskaitant karinį ir pramoninį šnipinėjimą), terorizmu ir tarptautinių nusikalstamų sindikatų veikla, žvalgybos informaciją apie tam tikrų rūšių nusikaltimus, nukreiptus prieš viešąjį ir nacionalinį saugumą (pvz., vidaus sukilimus, užsienio agresiją), ir žvalgybos informaciją, susijusią su kibernetinio saugumo užtikrinimo ir kibernetinių išpuolių ir grėsmių prevencijos arba kovos su jais užduotimis⁽¹⁸²⁾. NŽT įstatyme, kuriuo įsteigiama NŽT ir nustatomos jos užduotys, taip pat nustatyti bendrieji principai, kuriais grindžiama visa jos veikla. Apskritai NŽT turi išlaikyti politinį neutralumą ir apsaugoti asmenų laisvę ir teises⁽¹⁸³⁾. NŽT pirmininkui pavesta parengti bendrąsias gaires, kuriose būtų nustatyti NŽT pareigų, susijusių su informacijos rinkimu ir naudojimu, vykdymo principai, apimtis ir procedūros, ir apie jas jis turi informuoti Nacionalinę Asamblėją⁽¹⁸⁴⁾. Nacionalinė Asamblėja (per savo žvalgybos komitetą) gali reikalauti, kad gairės būtų pataisytos arba papildytos, jei mano, kad jos yra neteisėtos arba neteisingo pobūdžio. Apskritai vykdydami savo pareigas NŽT direktorius ir darbuotojai negali versti jokios institucijos, organizacijos ar asmens daryti tai, ko jie neprivalo daryti, ir negali trukdyti jokiam asmeniui naudotis savo teisėmis piktnaudžiaudami savo oficialiais įgaliojimais⁽¹⁸⁵⁾. Be to, taikant pašto cenzūrą, perimant telekomunikacinius ryšius, renkant buvimo vietos nustatymo informaciją, ryšių patvirtinimo duomenis arba

⁽¹⁷³⁾ Administracinių ginčų įstatymo 20 straipsnis. Šis terminas taip pat taikomas reikalavimui pripažinti neveikimą neteisėtu (žr. Administracinių ginčų įstatymo 38 straipsnio 2 dalį).

⁽¹⁷⁴⁾ 1991 m. birželio 28 d. Aukščiausiojo Teismo sprendimas 90Nu6521.

⁽¹⁷⁵⁾ Konstitucinio Teismo įstatymo 68 straipsnio 1 dalis.

⁽¹⁷⁶⁾ 2001 m. lapkričio 29 d. Konstitucinio Teismo sprendimas Nr. 99HeonMa194.

⁽¹⁷⁷⁾ Konstitucinio Teismo įstatymo 40 straipsnis.

⁽¹⁷⁸⁾ Konstitucinio Teismo įstatymo 69 straipsnis.

⁽¹⁷⁹⁾ Konstitucinio Teismo įstatymo 75 straipsnio 3 dalis.

⁽¹⁸⁰⁾ NŽT įstatymo 2 straipsnis ir 4 straipsnio 2 dalis.

⁽¹⁸¹⁾ Į šią sąvoką neįtraukiama informacija apie asmenis, tik bendra informacija apie užsienio valstybes (tendencijas, pokyčius) ir trečiųjų valstybių valstybinių subjektų veiklą.

⁽¹⁸²⁾ NŽT įstatymo 3 straipsnio 1 dalis.

⁽¹⁸³⁾ 3 straipsnio 1 dalis, 6 straipsnio 2 dalis, 11 ir 21 straipsniai. Taip pat žr. taisyklės dėl interesų konfliktų, visų pirma 10 ir 12 straipsnius.

⁽¹⁸⁴⁾ NŽT įstatymo 4 straipsnio 2 dalis.

⁽¹⁸⁵⁾ NŽT įstatymo 13 straipsnis.

NŽT įrašant privačius ryšius arba jų klausantis būtina laikytis RPAĮ, Informacijos apie buvimo vietą įstatymo arba BPI reikalavimų⁽¹⁸⁶⁾. Už bet kokią piktnaudžiavimą įgaliojimais ar informacijos rinkimą pažeidžiant šiuos įstatymus taikomos baudžiamosios sankcijos⁽¹⁸⁷⁾.

Paramos saugumui gynybos vadavieta yra Gynybos ministerijos įsteigta karinės žvalgybos agentūra. Ji atsakinga už saugumo klausimus vykdant karinę veiklą, karinių nusikalstamų veikų tyrimus (taikant Karinio teismo įstatymą) ir karinę žvalgybą. Apskritai Paramos saugumui gynybos vadavieta nevykdo civilių gyventojų sekimo, nebent tai būtina jos karinėms funkcijoms vykdyti. Gali būti vykdomi karinio personalo, civilių kariuomenės darbuotojų, karinius mokymus atliekančių asmenų, asmenų kariniame rezerve arba samdomųjų karių ir karo belaisvių tyrimai⁽¹⁸⁸⁾. Paramos saugumui gynybos vadavietai renkant ryšių informaciją nacionalinio saugumo tikslais jai taikomi RPAĮ ir jo vykdymo užtikrinimo dekretu nustatyti apribojimai ir apsaugos priemonės.

3.2. Teisiniai pagrindai ir apribojimai

RPAĮ, Įstatymu dėl kovos su terorizmu siekiant apsaugoti piliečius ir užtikrinti viešąją saugumą (toliau – Kovos su terorizmu įstatymas) ir TII suteikiami teisiniai pagrindai asmeninės informacijos rinkimui nacionalinio saugumo tikslais ir nustatomi taikytini apribojimai ir apsaugos priemonės⁽¹⁸⁹⁾. Šiais apribojimais ir apsaugos priemonėmis užtikrinama, kaip aprašyta tolesniuose skirsniuose, kad informacija būtų renkama ir tvarkoma tik tiek, kiek būtina teisėtam tikslui pasiekti. Tai neapima masinio ir nesirinktinai atliekamo asmeninės informacijos rinkimo nacionalinio saugumo tikslais.

3.2.1. Ryšių informacijos rinkimas

3.2.1.1. Žvalgybos agentūrų atliekamas ryšių informacijos rinkimas

3.2.1.1.1. Teisinis pagrindas

RPAĮ žvalgybos agentūroms suteikiamas įgaliojimas rinkti ryšių duomenis, o ryšių paslaugų teikėjams nustatomas reikalavimas bendradarbiauti toms agentūroms paprašius⁽¹⁹⁰⁾. Kaip aprašyta 2.2.2.1 skirsnyje, RPAĮ ryšių turinio rinkimas (t. y. „ryšius ribojančios priemonės“, kaip antai „slapto pokalbių klausymosi“ arba „cenzūros“⁽¹⁹¹⁾ priemonės) atskiriamas nuo „ryšių patvirtinimo duomenų“ rinkimo⁽¹⁹²⁾.

Šių dviejų rūšių informacijos rinkimo ribos skiriasi, tačiau taikomos procedūros ir apsaugos priemonės iš esmės yra vienodos⁽¹⁹³⁾. Ryšių patvirtinimo duomenys (arba metaduomenys) gali būti renkami siekiant užkirsti kelią nacionaliniam saugumui kylančioms grėsmėms⁽¹⁹⁴⁾. Siauresnės ribos taikomos, kai imamasi ryšius ribojančių priemonių (t. y. renkamas ryšių turinys), kurios gali būti taikomos tik tada, kai numatoma, kad nacionaliniam saugumui kils didelis pavojus, o žvalgybos duomenų rinkimas yra būtinas siekiant užkirsti kelią tokiam pavojui (t. y. jei nacionaliniam saugumui kyla didelis pavojus ir duomenų rinkimas yra būtinas siekiant užkirsti kelią tokiam pavojui)⁽¹⁹⁵⁾. Be to, prieiga prie ryšių turinio gali būti suteikiama tik kraštutiniu atveju, kai siekiama užtikrinti nacionalinį saugumą, ir turi būti dedamos pastangos kuo mažiau pažeisti ryšių privatumą⁽¹⁹⁶⁾. Net gavus atitinkamą patvirtinimą ir (arba) leidimą, tokių priemonių taikymas turi būti nedelsiant sustabdomas, kai jos nebereikalingos, taip užtikrinant, kad bet koks privačių asmens ryšių pažeidimas būtų kuo mažesnis⁽¹⁹⁷⁾.

3.2.1.1.2. Apribojimai ir apsaugos priemonės, taikomi renkant ryšių, kuriuose dalyvauja bent vienas Korėjos pilietis, informaciją

Ryšių, kuriuose viena arba abi šalys yra Korėjos piliečiai, informacija (tiek turinys, tiek metaduomenys) gali būti renkama

⁽¹⁸⁶⁾ NŽT įstatymo 14 straipsnis.

⁽¹⁸⁷⁾ NŽT įstatymo 22 ir 23 straipsniai.

⁽¹⁸⁸⁾ Karinio teismo įstatymo 1 straipsnis.

⁽¹⁸⁹⁾ Tirdamos nusikaltimus, susijusius su nacionaliniu saugumu policija ir NŽT remiasi BPI, o Paramos saugumui gynybos vadavietai taikomas Karinio teismo įstatymas.

⁽¹⁹⁰⁾ RPAĮ 15-2 straipsnis.

⁽¹⁹¹⁾ RPAĮ 2 straipsnio 6 ir 7 dalys.

⁽¹⁹²⁾ RPAĮ 2 straipsnio 11 dalis.

⁽¹⁹³⁾ Taip pat žr. RPAĮ 13-4 straipsnio 2 dalį ir RPAĮ vykdymo užtikrinimo dekretu 37 straipsnio 4 dalį, kuriuose numatyta, kad ryšių turinio rinkimui taikomos procedūros *mutatis mutandis* taikomos ryšių patvirtinimo duomenų rinkimui.

⁽¹⁹⁴⁾ RPAĮ 13-4 straipsnis.

⁽¹⁹⁵⁾ RPAĮ 7 straipsnio 1 dalis.

⁽¹⁹⁶⁾ RPAĮ 3 straipsnio 2 dalis.

⁽¹⁹⁷⁾ RPAĮ vykdymo užtikrinimo dekretu 2 straipsnis.

tik gavus Aukštojo Teismo vyriausiojo teisėjo leidimą⁽¹⁹⁸⁾. Žvalgybos agentūros prašymas turi būti pateiktas raštu prokurorui arba Vyriausiajai prokuratūrai⁽¹⁹⁹⁾. Jame turi būti nurodomos rinkimo priežastys (t. y. kad tikėtina, jog nacionaliniam saugumui kils didelis pavojus arba kad rinkimas yra būtinas siekiant užkirsti kelią nacionaliniam saugumui kylančioms grėsmėms), pateikiamos kartu su medžiaga, kuria tos priežastys pagrindžiamos ir įrodomas *prima facie* pagrindas, taip pat pateikiama išsami informacija apie prašymą (t. y. tikslai, asmuo (asmenys), kurio (-ių) duomenis siekiama rinkti, taikymo mastas, rinkimo laikotarpis, taip pat rinkimo vieta ir būdas)⁽²⁰⁰⁾. Savo ruožtu prokuroras arba Vyriausioji prokuratūra prašo Aukštojo teismo vyriausiojo teisėjo leidimo⁽²⁰¹⁾. Vyriausiasis teisėjas rašytinį leidimą gali suteikti tik tada, kai mano, kad prašymas yra pagrįstas, ir prašymą atmeta, kai mano, kad jis nepagrįstas⁽²⁰²⁾. Orderyje nurodoma rinkimo rūšis, tikslas, taikymo sritis, mastas ir laikotarpis, taip pat vieta ir būdas⁽²⁰³⁾.

Specialios taisyklės taikomos tuomet, kai taikant priemonę siekiama tirti sąmokslą, kuriuo keliami grėsmė nacionaliniam saugumui, esant ekstremaliajai situacijai, dėl kurios neįmanoma atlikti minėtų procedūrų⁽²⁰⁴⁾. Esant šioms sąlygoms žvalgybos tarnybos gali taikyti sekimo priemones be išankstinio teismo leidimo⁽²⁰⁵⁾. Tačiau įvykdžiusi neatidėliotinas priemones žvalgybos agentūra turi nedelsiant prašyti teismo leidimo. Jei leidimas negaunamas per 36 valandas nuo priemonių taikymo pradžios, jų taikymas turi būti nedelsiant nutraukiamas⁽²⁰⁶⁾. Ekstremaliųjų situacijų atvejais informacija visada turi būti renkama remiantis „neišvengiamos cenzūros ir (arba) slapto pokalbių klausymosi pareiškimu“, o rinkimą atliekanti žvalgybos agentūra privalo registruoti visas neatidėliotinas priemones⁽²⁰⁷⁾.

Tais atvejais, kai sekimas užbaigiamas per trumpą laiką nespėjus gauti teismo leidimo, kompetentingos Vyriausiosios prokuratūros vadovas turi nusiųsti žvalgybos agentūros parengtą pranešimą dėl neatidėliotinos priemonės kompetentingo teismo vadovui, kuris registruoja neatidėliotinas priemones⁽²⁰⁸⁾. Taip teismui sudaromos sąlygos išnagrinėti duomenų rinkimo teisėtumą.

3.2.1.1.3. Apribojimai ir apsaugos priemonės, taikomi renkant ryšių, kuriuose dalyvauja tik ne Korėjos piliečiai, informaciją

Žvalgybos agentūros, siekdamos rinkti ryšių tik tarp ne Korėjos piliečių informaciją, turi gauti išankstinį raštišką Prezidento sutikimą⁽²⁰⁹⁾. Tokie ryšiai nacionalinio saugumo tikslais bus renkami tik tuo atveju, jei jie priklauso vienai iš kelių išvardytų kategorijų, t. y. ryšiai tarp vyriausybės pareigūnų ar kitų asmenų šalyse, kurios yra priešiška nusiteikusi Korėjos Respublikos atžvilgiu, užsienio šalių agentūrų, grupių ar piliečių, įtariamų vykdant prieš Korėją nukreiptą veiklą⁽²¹⁰⁾, arba grupių, veikiančių Korėjos pusiasalyje, tačiau faktiškai esančių už Korėjos Respublikos suvereniteto ribų, ir joms priklausančių grupių, įsikūrusių užsienio šalyse, narių⁽²¹¹⁾. Tačiau jei viena ryšių šalis yra Korėjos pilietis, o kita – ne Korėjos pilietis, reikia gauti teismo sutikimą 3.2.1.1.2 skirsnyje aprašyta tvarka.

Žvalgybos agentūros vadovas turi pateikti NŽT direktoriui priemonių, kurių ketinama imtis, planą⁽²¹²⁾. NŽT direktorius peržiūri planą ir, jei nustato, kad jis yra tinkamas, pateikia jį tvirtinti Prezidentui⁽²¹³⁾. Į planą turi būti įtraukta ta pati informacija, kurią reikalaujama pateikti prašant teismo leidimo rinkti informaciją apie Korėjos piliečius (aprašyta pirmiau)⁽²¹⁴⁾. Visų pirma jame turi būti nurodomos rinkimo priežastys (t. y. kad tikėtina, jog nacionaliniam saugumui kils didelis pavojus arba kad rinkimas yra būtinas siekiant užkirsti kelią nacionaliniam saugumui kylančioms grėsmėms) ir pagrindinės įtarimo priežastys, pateikiamos kartu su medžiaga, kuria tos priežastys pagrindžiamos ir įrodomas

⁽¹⁹⁸⁾ RPAĮ 7 straipsnio 1 dalies 1 punktą. Kompetentingas teismas yra aukštasis teismas, kurio jurisdikcijoje yra vienos ar abiejų stebimų šalių nuolatinė gyvenamoji vieta arba buveinė.

⁽¹⁹⁹⁾ RPAĮ vykdymo užtikrinimo dekreto 7 straipsnio 3 dalis.

⁽²⁰⁰⁾ RPAĮ 7 straipsnio 3 dalis ir 6 straipsnio 4 dalis.

⁽²⁰¹⁾ RPAĮ vykdymo užtikrinimo dekreto 7 straipsnio 4 dalis. Prokuroro prašyme teismui turi būti nurodytos pagrindinės įtarimo priežastys ir pagrindimas, jei tuo pačiu metu prašoma kelių leidimų (žr. RPAĮ vykdymo užtikrinimo dekreto 4 straipsnį).

⁽²⁰²⁾ RPAĮ 7 straipsnio 3 dalis, 6 straipsnio 5 ir 9 dalys.

⁽²⁰³⁾ RPAĮ 7 straipsnio 3 dalis ir 6 straipsnio 6 dalis.

⁽²⁰⁴⁾ RPAĮ 8 straipsnis.

⁽²⁰⁵⁾ RPAĮ 8 straipsnio 1 dalis.

⁽²⁰⁶⁾ RPAĮ 8 straipsnio 2 dalis.

⁽²⁰⁷⁾ RPAĮ 8 straipsnio 4 dalis. Dėl neatidėliotinių priemonių teisėsaugos srityje žr. anksčiau pateiktą 2.2.2.2 skirsnį.

⁽²⁰⁸⁾ RPAĮ 8 straipsnio 5 ir 7 dalys. Šiame pranešime turi būti nurodytas stebėjimo tikslas, sritis, mastas, laikotarpis, vykdymo vieta ir stebėjimo būdas, taip pat priežastis, dėl kurios prašymas nebuvo pateiktas prieš imantis priemones (RPAĮ 8 straipsnio 6 dalis).

⁽²⁰⁹⁾ RPAĮ 7 straipsnio 1 dalies 2 punktą.

⁽²¹⁰⁾ Tai yra veikla, kuria keliami grėsmė tautos egzistavimui ir saugumui, demokratinei tvarkai arba žmonių išlikimui ir laisvei.

⁽²¹¹⁾ Be to, jei viena iš šalių yra RPAĮ 7 straipsnio 1 dalies 2 punkte apibūdintas asmuo, o kita yra nežinoma arba negali būti nurodyta, taikoma 7 straipsnio 1 dalies 2 punkte nustatyta procedūra.

⁽²¹²⁾ RPAĮ vykdymo užtikrinimo dekreto 8 straipsnio 1 dalis. NŽT direktorių skiria Prezidentas, gavęs Parlamento patvirtinimą (NŽT įstatymo 7 straipsnis).

⁽²¹³⁾ RPAĮ vykdymo užtikrinimo dekreto 8 straipsnio 2 dalis.

⁽²¹⁴⁾ RPAĮ vykdymo užtikrinimo dekreto 8 straipsnio 3 dalis kartu su RPAĮ 6 straipsnio 4 dalimi.

prima facie pagrindas, taip pat pateikiama išsami informacija apie prašymą (t. y. tikslai, asmuo (asmenys), kurio (-ių) duomenis siekiama rinkti, taikymo mastas, rinkimo laikotarpis, taip pat rinkimo vieta ir būdas). Jei tuo pačiu metu prašoma išduoti kelis leidimus, nurodomas jų prašymo tikslas ir priežastys ⁽²¹⁵⁾.

Ekstremaliųjų situacijų atveju ⁽²¹⁶⁾ turi būti gautas išankstinis ministro, kurio jurisdikcijai priklauso atitinkama žvalgybos agentūra, sutikimas. Tačiau tokiu atveju po to, kai buvo imtasi neatidėliotinių priemonių, žvalgybos agentūra turi nedelsiant gauti Prezidento patvirtinimą. Jei žvalgybos agentūra negauna patvirtinimo per 36 valandas nuo prašymo pateikimo, duomenų rinkimas turi būti nedelsiant nutraukiamas ⁽²¹⁷⁾. Tokiais atvejais surinkta informacija bus visada sunaikinama.

3.2.1.1.4. Bendrieji apribojimai ir apsaugos priemonės

Prašydamos privačių bendrovių bendradarbiauti žvalgybos tarnybos turi pateikti teismo orderį, Prezidento leidimą arba neišvengiamos cenzūros pareiškimo titulinio puslapio kopiją, kurią prašomas subjektas turi saugoti ⁽²¹⁸⁾. Bendrovės, kurių žvalgybos agentūros RPAĮ pagrindu prašo atskleisti informaciją, gali atsisakyti tai padaryti, kai orderyje arba neišvengiamos cenzūros pareiškime nurodytas neteisingas identifikatorius (pvz., telefono numeris, priklausantis kitam asmeniui nei nurodytasis). Be to, nepaisant aplinkybių, negalima atskleisti slaptažodžių, naudojamų naudojantis ryšių paslaugomis ⁽²¹⁹⁾.

Žvalgybos agentūros gali patikėti ryšius ribojančių priemonių taikymą arba ryšių patvirtinimo informacijos rinkimą pašto tarnybai arba telekomunikacijų paslaugų teikėjui (kaip apibrėžta Telekomunikacijų įmonių įstatyme) ⁽²²⁰⁾. Atitinkama žvalgybos agentūra ir prašymą bendradarbiauti gaunantis paslaugų teikėjas turi trejus metus saugoti įrašus, kuriuose nurodomas prašymo imtis priemonių tikslas, vykdymo ar bendradarbiavimo data ir priemonių objektas (pvz., paštas, telefonas, e. paštas) ⁽²²¹⁾. Ryšių patvirtinimo duomenis teikiantys telekomunikacijų paslaugų teikėjai turi septynerius metus savo bylose saugoti informaciją apie rinkimo dažnumą ir du kartus per metus teikti ataskaitas Mokslo ir IRT ministrui ⁽²²²⁾.

Žvalgybos agentūros turi pranešti NŽT direktoriui apie surinktą informaciją ir stebėjimo veiklos rezultatus ⁽²²³⁾. Ryšių patvirtinimo duomenų rinkimo atveju turi būti saugomi įrašai apie tai, kad buvo pateiktas prašymas pateikti tokius duomenis, taip pat pats rašytinis prašymas ir įrašas apie instituciją, kuri juo rėmėsi ⁽²²⁴⁾.

Ryšių turinio ir ryšių patvirtinimo duomenų rinkimas gali trukti ne ilgiau kaip keturis mėnesius, o kai siekiamas tikslas pasiekiamas anksčiau, rinkimas turi būti nutraukiamas nedelsiant ⁽²²⁵⁾. Jei leidimo išdavimo sąlygos toliau tenkinamos, teismui leidus arba Prezidentui pritarus terminas gali būti pratęsiamas iki keturių mėnesių. Prašymas leisti pratęsti stebėjimo priemonių taikymą turi būti pateikiamas raštu, nurodant pratęsimo prašymo priežastis ir pateikiant patvirtinančią medžiagą ⁽²²⁶⁾.

Priklausomai nuo duomenų rinkimo teisinio pagrindo, asmenims paprastai pranešama, kai renkama jų ryšių informacija. Visų pirma, nepriklausomai nuo to, ar surinkta informacija yra susijusi su ryšių turiniu, ar su ryšių patvirtinimo duomenimis, ir neatsižvelgiant į tai, ar informacija buvo gauta taikant įprastą procedūrą, ar esant ekstremaliajai situacijai, žvalgybos agentūros vadovas turi raštu pranešti atitinkamam asmeniui apie stebėjimo priemonės taikymą per 30 dienų nuo stebėjimo priemonės taikymo pabaigos ⁽²²⁷⁾. Pranešime turi būti nurodyta: 1) tai, kad informacija buvo surinkta,

⁽²¹⁵⁾ RPAĮ vykdymo užtikrinimo dekreto 8 straipsnio 3 dalis ir 4 straipsnis.

⁽²¹⁶⁾ Tai tokie atvejai, kai priemone siekiama užkirsti kelią šamokslui, dėl kurio kyla grėsmė nacionaliniam saugumui, nėra laiko gauti Prezidento patvirtinimą, o neįgyvendinus neatidėliotinių priemonių gali būti pakenkta nacionaliniam saugumui (RPAĮ 8 straipsnio 8 dalis).

⁽²¹⁷⁾ RPAĮ 8 straipsnio 9 dalis.

⁽²¹⁸⁾ RPAĮ 9 straipsnio 2 dalis ir RPAĮ vykdymo užtikrinimo dekreto 12 straipsnis.

⁽²¹⁹⁾ RPAĮ 9 straipsnio 4 dalis.

⁽²²⁰⁾ RPAĮ vykdymo užtikrinimo dekreto 13 straipsnis.

⁽²²¹⁾ RPAĮ 9 straipsnio 3 dalis ir RPAĮ vykdymo užtikrinimo dekreto 17 straipsnio 2 dalis. Šis terminas netaikomas ryšių patvirtinimo duomenims (žr. RPAĮ vykdymo užtikrinimo dekreto 39 straipsnį).

⁽²²²⁾ RPAĮ 13 straipsnio 7 dalis ir RPAĮ vykdymo užtikrinimo dekreto 39 straipsnis.

⁽²²³⁾ RPAĮ vykdymo užtikrinimo dekreto 18 straipsnio 3 dalis.

⁽²²⁴⁾ RPAĮ 13 straipsnio 5 dalis ir 13-4 straipsnio 3 dalis.

⁽²²⁵⁾ RPAĮ 7 straipsnio 2 dalis.

⁽²²⁶⁾ RPAĮ 7 straipsnio 2 dalis ir RPAĮ vykdymo užtikrinimo dekreto 5 straipsnis.

⁽²²⁷⁾ RPAĮ 9-2 straipsnio 3 dalis. Pagal RPAĮ 13-4 straipsnį tai taikoma tiek ryšių turinio rinkimui, tiek ryšių patvirtinimo duomenų rinkimui.

2) informaciją renkanti agentūra ir 3) rinkimo laikotarpis. Tačiau jei tikėtina, kad pranešus galėtų kilti pavojus nacionaliniam saugumui arba galėtų kilti grėsmė žmonių gyvybėms ir fiziniam saugumui, pranešimas gali būti atidedamas ⁽²²⁸⁾. Pranešimas turi būti pateikiamas per 30 dienų nuo tada, kai išnyksta atidėjimo pagrindai ⁽²²⁹⁾.

Tačiau šis reikalavimas pranešti taikomas tik tada, kai bent viena iš renkamos informacijos šalių yra Korėjos pilietis. Todėl ne Korėjos piliečiams bus pranešama tik tada, kai bus renkami jų ryšių su Korėjos piliečiais informacija. Taigi reikalavimas pranešti netaikomas, kai renkama tik ne Korėjos piliečių ryšių informacija.

Bet kokių ryšių turinys ir ryšių patvirtinimo duomenys, gauti vykdant stebėjimą pagal RPAĮ, gali būti naudojami tik 1) vykdant tam tikrų nusikaltimų tyrimą, baudžiamąjį persekiojimą už juos ar jų prevenciją, 2) taikant drausmines procedūras, 3) vykdant teismo procesą, kai su ryšiais susijusi šalis jais remiasi pateikdama ieškinį dėl žalos atlyginimo, arba 4) remiantis kitais įstatymais ⁽²³⁰⁾.

3.2.1.2. Policijos ir (arba) prokurorų vykdomas ryšių informacijos rinkimas nacionalinio saugumo tikslais

Policija ir (arba) prokuroras gali rinkti ryšių informaciją (tiek ryšių turinį, tiek ryšių patvirtinimo duomenis) nacionalinio saugumo tikslais tomis pačiomis sąlygomis, kurios aprašytos 3.2.1.1 skirsnyje. Ekstremaliosios situacijos atveju ⁽²³¹⁾ taikoma anksčiau aprašyta procedūra, taikoma, kai ryšių turinys renkamas teisėsaugos tikslais ekstremaliųjų situacijų atveju (t. y. RPAĮ 8 straipsnis).

3.2.2. Informacijos apie asmenis, įtariamus teroristine veikla, rinkimas

3.2.2.1. Teisinis pagrindas

Kovos su terorizmu įstatymu NŽT direktoriui suteikiami įgaliojimai rinkti informaciją apie teroristine veikla įtariamus asmenis ⁽²³²⁾. „Teroristine veikla įtariamasis asmuo“ apibrėžiamas kaip teroristinės grupės narys ⁽²³³⁾, asmuo, kuris remia teroristinę grupę (propaguodamas ir platindamas teroristinės grupės idėjas ar taktiką), renka teroristinei veiklai skirtas lėšas arba jų skiria ⁽²³⁴⁾ arba dalyvauja kitoje veikloje, susijusioje su teroristinės veiklos planavimu, sąmokslu ją vykdyti, jos propaganda ar kurstyti, arba asmuo, kurio atžvilgiu yra pagrįstų priežasčių įtarti, kad jis tokią veiklą vykdo ⁽²³⁵⁾. Paprastai bet kuris valstybės pareigūnas, užtikrinantis Kovos su terorizmu įstatymo įgyvendinimą, privalo gerbti pagrindines teises, įtvirtintas Korėjos Konstitucijoje ⁽²³⁶⁾.

Pačiu Kovos su terorizmu įstatymu konkretūs įgaliojimai, apribojimai ir apsaugos priemonės, susijusios su informacijos apie teroristine veikla įtariamus asmenis rinkimu, nenustatomi, jame veikiau nurodomos kitais įstatymais nustatytos procedūros. Visų pirma remdamasis Kovos su terorizmu įstatymu NŽT direktorius gali rinkti 1) informaciją apie atvykimą į Korėjos Respubliką ir išvykimą iš jos, 2) informaciją apie finansinius sandorius ir 3) informaciją apie ryšius. Atsižvelgiant į informacijos, kurią siekiama gauti, rūšį, atitinkami procedūriniai reikalavimai nustatyti atitinkamai Imigracijos įstatymu ir Muitų įstatymu, ĮKFSITN arba RPAĮ ⁽²³⁷⁾. Dėl informacijos apie atvykimą į Korėją ir išvykimą iš jos rinkimo Kovos su terorizmu įstatyme daroma nuoroda į Imigracijos įstatymu ir Muitų įstatymu nustatytas procedūras.

⁽²²⁸⁾ RPAĮ 9-2 straipsnio 4 dalis.

⁽²²⁹⁾ RPAĮ 13-4 straipsnio 2 dalis ir 9-2 straipsnio 6 dalis.

⁽²³⁰⁾ RPAĮ 5 straipsnio 1 ir 2 dalys, 12 ir 13-5 straipsniai.

⁽²³¹⁾ Tai atvejai, kai priemone siekiama užkirsti kelią sąmokslui, dėl kurio kyla grėsmė nacionaliniam saugumui, esant ekstremaliajai situacijai, dėl kurios neįmanoma taikyti įprastos patvirtinimo procedūros (RPAĮ 8 straipsnio 1 dalis).

⁽²³²⁾ Kovos su terorizmu įstatymo 9 straipsnis.

⁽²³³⁾ „Teroristinė grupė“ – tai asmenų, užsiimančių teroristine veikla, grupė, kaip ją apibrėžia Jungtinės Tautos (Kovos su terorizmu įstatymo 2 straipsnio 2 dalis).

⁽²³⁴⁾ Kovos su terorizmu įstatymo 2 straipsnio 1 dalyje terminas „terorizmas“ apibrėžiamas kaip elgesys, kuriuo siekiama trukdyti valstybei, vietos valdžios institucijai ar užsienio vyriausybei (įskaitant vietos valdžios institucijas ir tarptautines organizacijas) vykdyti savo įgaliojimus arba priversti ją imtis veiksmų, kurių imtis ji neturi jokios prievolės, arba kelti grėsmę visuomenei. Tai gali būti a) asmens nužudymas arba grėsmės jo gyvybei sukėlimas jį fiziškai sužalojus, asmens sulaikymas, uždarymas, pagrobimas ar laikymas įkaitu, b) tam tikras elgesys, susijęs su orlaiviais (skrendančio orlaivio sudaužymas, užgrobimas arba sugadinimas), c) tam tikras elgesys, susijęs su laivais (pvz., naudojimo laivo arba jūrinio statinio užėmimas, naudojamo laivo arba jūrinio statinio sunaikinimas arba toks jo sugadinimas, kad kiltų pavojus dėl jo saugumo, įskaitant krovinių, esančių naudojamame laive ar jūriniame statinyje, sugadinimą), d) biocheminių, sprogstamųjų ar padegamųjų ginklų ar prietaisų priverstinis, susprogdinimas arba kitoks jų naudojimas siekiant mirties, sunkaus sužalojimo ar rimtos materialinės žalos arba tokio poveikio siekiant atitinkamų rūšių transporto priemonėse ar objektuose (pvz., traukiniuose, tramvajuose, variklinėse transporto priemonėse, viešosiose stovėjimo aikštelėse ir stotyse, objektuose, susijusiuose su elektros energijos, dujų ir telekomunikacijų paslaugų tiekimu, ir t. t.), e) tam tikras elgesys, susijęs su branduolinėmis ir radioaktyviosiomis medžiagomis arba branduoliniais objektais (pvz., grėsmės žmonių gyvybėms, jų fizinei sveikatai ar turtui kelimas arba kitoks viešojo saugumo trikdymas sunaikinant branduolinį reaktorių arba neteisėtai valdant radioaktyviasias medžiagas ir t. t.).

⁽²³⁵⁾ Kovos su terorizmu įstatymo 2 straipsnio 3 dalis.

⁽²³⁶⁾ Kovos su terorizmu įstatymo 3 straipsnio 3 dalis.

⁽²³⁷⁾ Kovos su terorizmu įstatymo 9 straipsnio 1 dalis.

Tačiau šiuo metu šiais teisės aktais tokie įgaliojimai nenumatomi. Dėl ryšių informacijos ir finansinių sandorių informacijos rinkimo Kovos su terorizmu įstatyme nurodomi apribojimai ir apsaugos priemonės, nustatyti RPAĮ (išsamiau aprašyti toliau) ir ĮKFSITN (kuris, kaip paašškinta 2.1 skirsnyje, nėra svarbus vertinant sprendimą dėl tinkamumo).

Be to, Kovos su terorizmu įstatymo 9 straipsnio 3 dalyje nurodyta, kad NŽT direktorius gali prašyti, kad asmeninės informacijos valdytojas ⁽²³⁸⁾ arba buvimo vietos nustatymo informacijos teikėjas ⁽²³⁹⁾ pateiktų teroristine veikla įtariamo asmens asmeninę informaciją arba jo buvimo vietos nustatymo informaciją. Naudotis šia galimybe įmanoma tik teikiant prašymus savanoriškai atskleisti informaciją, kurių asmeninės informacijos valdytojai ir buvimo vietos nustatymo informacijos teikėjai neprivalo vykdyti, ir bet kuriuo atveju juos vykdyti gali tik remdamiesi AIAĮ ir Informacijos apie buvimo vietą įstatymu (žr. 3.2.2.2 skirsnį).

3.2.2.2. Apribojimai ir apsaugos priemonės, taikomi savanoriškai atskleidžiant informaciją pagal AIAĮ ir Informacijos apie buvimo vietą įstatymą

Savanoriško bendradarbiavimo atveju pagal Kovos su terorizmu įstatymą gali būti prašoma tik informacijos apie teroristine veikla įtariamą asmenį (žr. 3.2.2.1 skirsnį). NŽT teikiant tokius prašymus turi būti laikomasi teisėtumo, būtinumo ir proporcingumo principų, nustatytų Korėjos Konstitucijoje (12 straipsnio 1 dalis ir 37 straipsnio 2 dalis) ⁽²⁴⁰⁾, taip pat AIAĮ reikalavimų dėl asmeninės informacijos rinkimo (AIAĮ 3 straipsnio 1 dalis, žr. 1.2 skirsnį). Be to, NŽT įstatyme nurodyta, kad piktnaudžiaudama savo oficialiais įgaliojimais NŽT negali priversti jokios institucijos, organizacijos ar asmens daryti nieko, ko jie neprivalo daryti, ir negali trukdyti jokiam asmeniui naudotis savo teisėmis ⁽²⁴¹⁾. Dėl šio draudimo pažeidimo gali būti taikomos baudžiamosios sankcijos ⁽²⁴²⁾.

Asmeninės informacijos valdytojai ir informacijos apie buvimo vietą teikėjai neprivalo vykdyti Kovos su terorizmu įstatymo pagrindu iš NŽT gautų prašymų. Juos vykdyti jie gali savanorišku pagrindu, tačiau tai daryti gali tik vadovaudamiesi AIAĮ ir Informacijos apie buvimo vietą įstatymu. Dėl AIAĮ laikymosi, visų pirma duomenų valdytojas turi atsizvelgti į duomenų subjekto interesus ir negali atskleisti informacijos, jei tikėtina, kad dėl to galėtų būti nepagrįstai pažeisti asmens arba trečiosios šalies interesai ⁽²⁴³⁾. Be to, pagal pranešimą Nr. 2021-1 dėl papildomų taisyklių dėl Asmeninės informacijos apsaugos įstatymo aiškinimo ir taikymo atitinkamam asmeniui turi būti pranešama apie informacijos atskleidimą. Ypatingais atvejais pranešimas gali būti atidedamas, visų pirma, jei pranešus būtų kliudoma vykstančiam baudžiamajam tyrimui arba galėtų kilti pavojus kito asmens gyvybei ar fizinei sveikatai ir tol, kol tokie pavojai kiltų, kai tos teisės ar interesai yra akivaizdžiai viršesni už duomenų subjekto teises ⁽²⁴⁴⁾.

3.2.2.3. RPAĮ nustatyti apribojimai ir apsaugos priemonės

Remdamasi Kovos su terorizmu įstatymu, žvalgybos agentūros gali rinkti ryšių informaciją (tiek ryšių turinį, tiek ryšių patvirtinimo duomenis) tik tada, kai tai būtina vykdant kovos su terorizmu veiklą, t. y. veiklą, susijusią su teroristinės veiklos prevencija ir atsakomosiomis priemonėmis jos atžvilgiu. 3.2.1 skirsnyje aprašytos RPAĮ procedūros taikomos tada, kai ryšių informacija renkama kovos su teroristine veikla tikslais.

3.2.3. Telekomunikacijų paslaugų teikėjų savanoriškas informacijos atskleidimas

Remdamiesi TĮ, telekomunikacijų paslaugų teikėjai gali vykdyti žvalgybos agentūros prašymą atskleisti „ryšių duomenis“, kai ji siekia rinkti tokią informaciją ketindama užkirsti kelią nacionaliniam saugumui kylančiam pavojui ⁽²⁴⁵⁾. Teikiant tokius prašymus turi būti laikomasi teisėtumo, būtinumo ir proporcingumo principų, nustatytų Korėjos Konstitucijoje (12 straipsnio 1 dalis ir 37 straipsnio 2 dalis) ⁽²⁴⁶⁾, taip pat AIAĮ reikalavimų dėl asmeninės informacijos rinkimo (AIAĮ 3 straipsnio 1 dalis (žr. 1.2 skirsnį)). Be to, taikomi tie patys apribojimai ir apsaugos priemonės, kurie taikomi savanoriškai atskleidžiant informaciją teisėsaugos tikslais (žr. 2.2.3 skirsnį) ⁽²⁴⁷⁾.

⁽²³⁸⁾ Kaip apibrėžta AIAĮ 2 straipsnyje, tai viešoji įstaiga, juridinis asmuo, organizacija, fizinis asmuo ir t. t., tiesiogiai ar netiesiogiai tvarkantys asmeninę informaciją, siekdami naudoti asmens duomenų bylas oficialiais ar verslo tikslais.

⁽²³⁹⁾ Kaip apibrėžta įstatymo dėl informacijos apie buvimo vietą apsaugos, naudojimo ir kt. (toliau – Informacijos apie buvimo vietą įstatymas) 5 straipsnyje, tai bet kuris asmuo, gavęs Korėjos ryšių komisijos leidimą užsiimti informacijos apie buvimo vietą rinkimo veikla.

⁽²⁴⁰⁾ Kovos su terorizmu įstatymo 3 straipsnio 2 ir 3 dalys.

⁽²⁴¹⁾ NŽT įstatymo 11 straipsnio 1 dalis.

⁽²⁴²⁾ NŽT įstatymo 19 straipsnis.

⁽²⁴³⁾ AIAĮ 18 straipsnio 2 dalis.

⁽²⁴⁴⁾ AIAK pranešimo Nr. 2021-1 dėl papildomų taisyklių dėl Asmeninės informacijos apsaugos įstatymo aiškinimo ir taikymo III skirsnio 2 dalies iii punktas.

⁽²⁴⁵⁾ TĮ 83 straipsnio 3 dalis.

⁽²⁴⁶⁾ Kovos su terorizmu įstatymo 3 straipsnio 2 ir 3 dalys.

⁽²⁴⁷⁾ Visų pirma prašymas turi būti pateikiamas raštu ir jame turi būti nurodytos prašymo priežastys, taip pat ryšys su atitinkamu vartotoju ir prašomos informacijos apimtis, o telekomunikacijų paslaugų teikėjas turi saugoti įrašus ir du kartus per metus teikti ataskaitas Mokslo ir IRT ministrui.

Telekomunikacijų paslaugų teikėjai neprivalo vykdyti prašymo, tačiau gali tai daryti savanoriškai ir būtinai laikydamiesi AIAI reikalavimų. Šiuo atžvilgiu telekomunikacijų verslo operatoriams taikomos tos pačios prievolės, be kita ko, susijusios su pranešimu asmeniui, kaip ir tuo atveju, kai jie gauna prašymus iš baudžiamosios teisėsaugos institucijų, kaip išsamiau paaiškinta 2.2.3 skirsnyje.

3.3. Priežiūra

Korėjos žvalgybos agentūrų veiklą prižiūri įvairios įstaigos. Paramos saugumui gynybos vadavietės priežiūrą vykdo Nacionalinės gynybos ministerija, vadovaudamasi ministerijos direktyva dėl vidaus audito įgyvendinimo. Kaip išsamiau paaiškinta toliau, NŽT veiklą prižiūri vadovas, Nacionalinė Asamblėja ir kitos nepriklausomos įstaigos.

3.3.1. Žmogaus teisių apsaugos pareigūnas

Kovos su terorizmu įstatyme numatyta, kad žvalgybos agentūroms renkant informaciją apie teroristine veikla įtariamus asmenis jų priežiūrą vykdo Kovos su terorizmu komisija ir žmogaus teisių apsaugos pareigūnas (toliau – ŽTAP) ⁽²⁴⁸⁾.

Kovos su terorizmu komisija, *inter alia*, rengia kovos su terorizmu veiklos politiką ir prižiūri kovos su terorizmu priemonių įgyvendinimą, taip pat įvairių kompetentingų institucijų veiklą kovos su terorizmu srityje ⁽²⁴⁹⁾. Komisijai pirmininkauja Ministras Pirmininkas, o ją sudaro keli ministrai ir vyriausybinių agentūrų vadovai, kaip antai Užsienio reikalų ministras, Teisingumo ministras, Nacionalinės gynybos ministras, Vidaus reikalų ir saugumo ministras, NŽT direktorius, Nacionalinės policijos agentūros generalinis komisaras ir Finansinių paslaugų komisijos pirmininkas ⁽²⁵⁰⁾. Atlikdamas tyrimus kovos su terorizmu srityje ir sekdamas teroristine veikla įtariamus asmenis, kad surinktų kovos su terorizmu veiklai reikalingą informaciją ar medžiagą, NŽT direktorius turi teikti ataskaitas Kovos su terorizmu komisijos pirmininkui (t. y. Ministrui Pirmininkui) ⁽²⁵¹⁾.

Be to, Kovos su terorizmu įstatymu įsteigiama ŽTAP pareigybė, siekiant apsaugoti pagrindines asmenų teises nuo pažeidimų, daromų vykdant kovos su terorizmu veiklą ⁽²⁵²⁾. Kovos su terorizmu komisijos pirmininkas ŽTAP skiria iš asmenų, kurie turi konkrečias kvalifikacijas, išvardytas Kovos su terorizmu įstatymo vykdymo užtikrinimo dekretu (t. y. iš asmenų, turinčių bent dešimties metų advokato darbo patirtį arba turinčių profesinių žinių žmogaus teisių apsaugos srityje ir bent dešimt metų ėjusių (mažiausiai) docento pareigas, arba asmenų, ėjusių vyresniojo valstybės pareigūno pareigas valstybės institucijose ar vietos valdžios institucijose, arba asmenų, turinčių bent dešimties metų darbo patirtį žmogaus teisių apsaugos srityje, pvz., nevyriausybiniame organizacijoje) ⁽²⁵³⁾. ŽTAP skiriamas dvejimms metams (su galimybe pratęsti kadenciją), o atleistas iš pareigų jis gali būti tik dėl konkrečių, ribotų priežasčių ir rimtu pagrindu, pvz., kai jam pareiškiami kaltinimai baudžiamojoje byloje, susijusioje su jo pareigomis, kai jis atskleidžia konfidencialią informaciją arba dėl ilgalaikės psichinės ar fizinės negalios ⁽²⁵⁴⁾.

ŽTAP turi įgaliojimus teikti rekomendacijas kovos su terorizmu veiklą vykdančioms agentūroms dėl žmogaus teisių apsaugos gerinimo ir nagrinėti civilines peticijas (žr. 3.4.3 skirsnį) ⁽²⁵⁵⁾. Jeigu pagrįstai nustatoma, kad vykdant oficialias pareigas pažeidžiamos žmogaus teisės, ŽTAP gali rekomenduoti atsakingos agentūros vadovui ištaisyti tokių pažeidimą ⁽²⁵⁶⁾. Savo ruožtu atsakinga agentūra turi pranešti ŽTAP apie veiksmus, kurių imtasi šiai rekomendacijai įgyvendinti ⁽²⁵⁷⁾. Agentūrai neįgyvendinus ŽTAP rekomendacijos, atvejis perduodamas komisijai, įskaitant jos pirmininką, kurio pareigas eina Ministras Pirmininkas. Atveju, kai ŽTAP rekomendacijos nebuvo įgyvendintos, kol kas nebuvo.

3.3.2. Nacionalinė Asamblėja

Kaip aprašyta 2.3.2 skirsnyje, Nacionalinė Asamblėja gali tirti ir tikrinti valdžios institucijas ir šiuo tikslu gali prašyti atskleisti dokumentus ir įgalioti liudininkus liudyti. NŽT jurisdikcijai priklausančios veiklos parlamentinę priežiūrą vykdo Nacionalinės Asamblėjos žvalgybos komitetas ⁽²⁵⁸⁾. NŽT direktorius, kuris prižiūri, kaip agentūra vykdo savo pareigas,

⁽²⁴⁸⁾ Kovos su terorizmu įstatymo 7 straipsnis.

⁽²⁴⁹⁾ Kovos su terorizmu įstatymo 5 straipsnio 3 dalis.

⁽²⁵⁰⁾ Kovos su terorizmu įstatymo vykdymo užtikrinimo dekretu 3 straipsnio 1 dalis.

⁽²⁵¹⁾ Kovos su terorizmu įstatymo 9 straipsnio 4 dalis.

⁽²⁵²⁾ Kovos su terorizmu įstatymo 7 straipsnis.

⁽²⁵³⁾ Kovos su terorizmu įstatymo vykdymo užtikrinimo dekretu 7 straipsnio 1 dalis.

⁽²⁵⁴⁾ Kovos su terorizmu įstatymo vykdymo užtikrinimo dekretu 7 straipsnio 3 dalis.

⁽²⁵⁵⁾ Kovos su terorizmu įstatymo vykdymo užtikrinimo dekretu 8 straipsnio 1 dalis.

⁽²⁵⁶⁾ Kovos su terorizmu įstatymo vykdymo užtikrinimo dekretu 9 straipsnio 1 dalis. ŽTAP rekomendacijas teikia savarankiškai, tačiau apie tokias rekomendacijas turi pranešti Kovos su terorizmu komisijos pirmininkui.

⁽²⁵⁷⁾ Kovos su terorizmu įstatymo vykdymo užtikrinimo dekretu 9 straipsnio 2 dalis.

⁽²⁵⁸⁾ Nacionalinės Asamblėjos įstatymo 36 straipsnis ir 37 straipsnio 1 dalies 16 punktas.

Žvalgybos komitetui (taip pat Prezidentui) teikia ataskaitas⁽²⁵⁹⁾. Pateikti ataskaitą konkrečiu klausimu taip pat gali prašyti pats Žvalgybos komitetas, o NŽT direktorius turi nedelsdamas tokį prašymą vykdyti⁽²⁶⁰⁾. Atsisakyti vykdyti prašymą arba duoti parodymus komitete jis gali tik tada, jei prašymas susijęs su valstybės paslaptimis, susijusiomis su kariniais, diplomatiniais ar Šiaurės Korėjos klausimais, kai jų atskleidimas gali turėti didelį poveikį šalies nacionaliniam likimui⁽²⁶¹⁾. Tokiu atveju Žvalgybos komitetas gali prašyti Ministro Pirmininko pateikti paaiškinimą. Jei toks paaiškinimas nepateikiamas per septynias dienas nuo prašymo pateikimo, galimybė atsisakyti vykdyti prašymą arba liudyti nebesuteikiama.

Jei Nacionalinė Asamblėja nustato neteisėtą ar netinkamą veiklą, ji gali prašyti, kad atitinkama valdžios institucija imtųsi taisomųjų veiksmų, be kita ko, skirtų kompensacijai, taikytų drausmines priemones ir tobulintų savo vidaus procedūras⁽²⁶²⁾. Gavusi tokį prašymą, institucija turi nedelsdama imtis veiksmų ir Nacionalinei Asamblėjai pranešti apie rezultatus. Specialios taisyklės nustatytos dėl ryšius ribojančių priemonių (t. y. ryšių turinio rinkimo) naudojimo pagal RPAĮ parlamentinės priežiūros⁽²⁶³⁾. Ją vykdydama Nacionalinė Asamblėja gali prašyti žvalgybos agentūrų vadovų pateikti ataskaitą apie bet kokią konkrečią ryšius ribojančią priemonę. Be to, ji gali atlikti slapto pokalbių klausymosi įrangos patikrinimus vietoje. Galiausiai Nacionalinės Asamblėjos prašymu žvalgybos agentūros, kurios nacionalinio saugumo tikslais rinko turinio informaciją, ir paslaugų teikėjai, kurie nacionalinio saugumo tikslais atskleidė turinio informaciją, turi pateikti ataskaitą apie tokį atskleidimą.

3.3.3. *Audito ir inspektavimo valdyba*

AIV atlieka tas pačias žvalgybos agentūrų priežiūros funkcijas, kaip ir baudžiamosios teisėsaugos srityje (žr. 2.3.2 skirsnį)⁽²⁶⁴⁾.

3.3.4. *Asmeninės informacijos apsaugos komisija*

Papildomą priežiūrą atliekant duomenų tvarkymą nacionalinio saugumo tikslais, įskaitant duomenų rinkimą, vykdo AIAK. Kaip išsamiau paaiškinta 1.2 skirsnyje, ji prižiūri, kaip laikomasi bendrųjų principų ir pareigų, nustatytų AIAĮ 3 straipsnyje ir 58 straipsnio 4 dalyje, taip pat kaip užtikrinamos asmens teisės, garantuojamos pagal AIAĮ 4 straipsnį. Be to, pagal AIAĮ 7-8 straipsnio 3 ir 4 dalis ir 7-9 straipsnio 5 dalį AIAK priežiūra taip pat apima galimus taisyklių, nustatytų konkrečiais įstatymais, kuriais nustatomi asmeninės informacijos rinkimo apribojimai ir apsaugos priemonės, kaip antai RPAĮ, Kovos su terorizmu įstatymu ir TĮĮ, pažeidimus. Atsižvelgiant į AIAĮ 3 straipsnio 1 dalyje nustatytus reikalavimus dėl teisėto ir teisingo asmeninės informacijos rinkimo, bet koks šių įstatymų pažeidimas reiškia AIAĮ pažeidimą. Taigi AIAK turi įgaliojimus tirti⁽²⁶⁵⁾ teisės aktų, kuriais reglamentuojamas prieigos prie duomenų suteikimas nacionalinio saugumo tikslais, pažeidimus, taip pat AIAĮ duomenų tvarkymo taisyklių pažeidimus, teikti rekomendacijas dėl tobulinimo, taikyti taisomąsias priemones, rekomenduoti drausmines priemones, o nustačiusi galimus teisės pažeidimus gali perduoti atvejus atitinkamoms tyrimo institucijoms⁽²⁶⁶⁾.

3.3.5. *Nacionalinė žmogaus teisių komisija*

NŽTK priežiūra žvalgybos agentūroms taikoma taip pat kaip ir kitoms valdžios institucijoms (žr. 2.3.2 skirsnį).

3.4. **Individualios teisių gynimo priemonės**

3.4.1. *Teisių gynimas kreipiantis į žmogaus teisių apsaugos pareigūną*

Kai asmeninė informacija renkama vykdant kovos su terorizmu veiklą, suteikiama speciali teisių gynimo priemonė kreipiantis į ŽTAP, kurio pareigybę įsteigė Kovos su terorizmu komisija. ŽTAP nagrinėja civilines peticijas, susijusias su žmogaus teisių pažeidimu vykdant kovos su terorizmu veiksmus⁽²⁶⁷⁾. Jis gali rekomenduoti imtis taisomųjų veiksmų, o atitinkama agentūra privalo pranešti pareigūnui apie visas priemones, kurių imtasi šiai rekomendacijai įgyvendinti. Asmenims nebūtina skundą pateikti ŽTAP. Skundą ŽTAP nagrinėja net jei nagrinėjant skundo priimtinumą atitinkamas asmuo negali įrodyti, kad buvo padaryta žala.

⁽²⁵⁹⁾ NŽT įstatymo 18 straipsnis.

⁽²⁶⁰⁾ NŽT įstatymo 15 straipsnio 2 dalis.

⁽²⁶¹⁾ NŽT įstatymo 17 straipsnio 2 dalis. „Valstybės paslaptys“ – tai „faktai, prekės ar žinios, kurie laikomi valstybės paslaptimis, su kuriais leidžiama susipažinti tik ribotam asmenų skaičiui ir kurie negali būti atskleisti jokiai kitai valstybei ar organizacijai, kad būtų išvengta rimtų kliūčių siekiant užtikrinti nacionalinį saugumą (žr. NŽT įstatymo 13 straipsnio 4 dalį).

⁽²⁶²⁾ Valstybės administracijos inspektavimo ir tyrimo įstatymo 16 straipsnio 2 dalis.

⁽²⁶³⁾ RPAĮ 15 straipsnis.

⁽²⁶⁴⁾ Kaip ir Nacionalinės Asamblėjos žvalgybos komiteto atveju, NŽT direktorius atsisakyti pateikti informaciją AIV gali tik tada, kai ji laikoma valstybės paslaptimis, ir jei jos paviešinimas darytų didelį poveikį nacionaliniam saugumui (NŽT įstatymo 13 straipsnio 1 dalis).

⁽²⁶⁵⁾ AIAĮ 63 straipsnis.

⁽²⁶⁶⁾ AIAĮ 61 straipsnio 2 dalis, 65 straipsnio 1 ir 2 dalys ir 64 straipsnio 4 dalis.

⁽²⁶⁷⁾ Kovos su terorizmu įstatymo vykdymo užtikrinimo dekreto 8 straipsnio 1 dalies 2 punktą.

3.4.2. AIAĮ nustatyti teisių gynimo mechanizmai

Pagal AIAĮ asmenys turi teisę susipažinti su nacionalinio saugumo tikslais tvarkoma asmenine informacija, reikalauti ją ištaisyti, ištrinti ir sustabdyti jos tvarkymą⁽²⁶⁸⁾. Prašymai pasinaudoti šiomis teisėmis gali būti teikiami tiesiogiai žvalgybos agentūrai arba netiesiogiai per AIAK. Žvalgybos agentūra gali laikinai neleisti, apriboti arba neleisti naudotis teise tiek ir tol, kol tai būtina siekiant apsaugoti svarbų viešojo intereso tikslą ir kai šie veiksmai yra jam proporcingi (pvz., tiek ir tol, kol teisės suteikimu būtų trukdoma vykstančiam tyrimui arba dėl jo kiltų grėsmė nacionaliniam saugumui), arba kai teisės suteikimas galėtų kelti pavojų trečiosios šalies gyvybei ar fizinei sveikatai. Jei prašymas atmetamas arba apribojamas, asmeniui turi būti nedelsiant pranešta apie priežastis.

Be to, pagal AIAĮ 58 straipsnio 4 dalį (reikalavimas užtikrinti tinkamą individualių skundų nagrinėjimą) ir AIAĮ 4 straipsnio 5 dalį (teisė į tinkamą teisių gynimą patyrus žalą dėl asmeninės informacijos tvarkymo, taikant savalaikę ir sąžiningą procedūrą) asmenys turi teisę į teisių gynimą. Tai, be kita ko, taikoma teisei pranešti apie įtariamą pažeidimą per Korėjos interneto ir saugumo agentūros administruojamą privatumo apsaugos skambučių centrą ir pateikti skundą AIAK⁽²⁶⁹⁾. Šiomis teisių gynimo priemonėmis galima pasinaudoti ir tuo atveju, jei pažeidžiamos taisyklės, nustatytos konkrečiuose įstatymuose, kuriais nustatomi apribojimai ir apsaugos priemonės, susijusios su asmeninės informacijos rinkimu nacionalinio saugumo tikslais, ir AIAĮ. Kaip paaiškinta pranešime Nr. 2021-1, ES asmuo skundą AIAK pateikti gali per savo nacionalinę duomenų apsaugos instituciją. Tokiu atveju, kai tyrimas baigiamas, AIAK informuoja asmenį (įskaitant, kai taikoma, pateikdama informaciją apie taikomus taisomuosius veiksmus) per nacionalinę duomenų apsaugos instituciją. AIAK sprendimai arba neveikimas gali būti apskundžiami Korėjos teismuose pagal Administracinių ginčų įstatymą.

3.4.3. Teisių gynimas Nacionalinėje žmogaus teisių komisijoje

Galimybė ginti asmens teises NŽTK nukentėjus dėl žvalgybos agentūrų veiksmų taikoma taip pat kaip ir nukentėjus dėl kitų valdžios institucijų veiksmų (žr. 2.4.2 skirsnį).

3.4.4. Teisminis teisių gynimas

Kaip ir baudžiamosios teisėsaugos institucijų veiklos atveju, asmenys, nukentėję dėl žvalgybos agentūrų įvykdytų pažeidimų, susijusių su pirmiau minėtais apribojimais ir apsaugos priemonėmis, gali pasinaudoti teisminėmis teisių gynimo priemonėmis.

Pirma, asmenys gali reikalauti žalos atlyginimo pagal Valstybės kompensacijų įstatymą. Pavyzdžiui, vienu atveju kompensacija buvo suteikta už neteisėtą Gynybos paramos vadavietės (Paramos saugumui gynybos vadavietės pirmtakės) vykdomą sekimą⁽²⁷⁰⁾.

Antra, Administracinių ginčų įstatymu asmenims leidžiama užginčyti administracinių agentūrų, įskaitant žvalgybos agentūras, sprendimus ir neveikimą⁽²⁷¹⁾.

Galiausiai pagal Konstitucinio Teismo įstatymą asmenys gali pateikti konstitucinį skundą Konstituciniam Teismui dėl priemonių, kurių ėmėsi žvalgybos agentūros.

⁽²⁶⁸⁾ AIAĮ 3 straipsnio 5 dalis ir 4 straipsnio 1, 3 ir 4 dalys.

⁽²⁶⁹⁾ AIAĮ 62 straipsnis ir 63 straipsnio 2 dalis.

⁽²⁷⁰⁾ 1998 m. liepos 24 d. Aukščiausiojo Teismo sprendimas Nr. 96Da42789.

⁽²⁷¹⁾ Administracinių ginčų įstatymo 3 ir 4 straipsniai.