II

(Muud kui seadusandlikud aktid)

OTSUSED

KOMISJONI RAKENDUSOTSUS (EL) 2019/419,

23. jaanuar 2019,

isikuteabe kaitse seaduse raames Jaapani pakutava isikuandmete kaitse piisavuse kohta vastavalt Euroopa Parlamendi ja nõukogu määrusele (EL) 2016/679

(teatavaks tehtud numbri K(2019) 304 all)

(EMPs kohaldatav tekst)

EUROOPA KOMISJON,

võttes arvesse Euroopa Liidu toimimise lepingut,

võttes arvesse Euroopa Parlamendi ja nõukogu 27. aprilli 2016. aasta määrust (EL) 2016/679 füüsiliste isikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise ning direktiivi 95/46/EÜ kehtetuks tunnistamise kohta (isikuandmete kaitse üldmäärus) ([1]) ja eelkõige selle artikli 45 lõiget 3,

pärast konsulteerimist Euroopa Andmekaitseinspektoriga,

1. SISSEJUHATUS

(1) Määruses (EL) 2016/679 on kehtestatud eeskirjad isikuandmete edastamiseks Euroopa Liidus asuvatelt vastutavatelt või volitatud töötlejatelt kolmandatesse riikidesse ja rahvusvahelistele organisatsioonidele määral, mil see edastamine kuulub määruse kohaldamisalasse. Isikuandmete rahvusvahelise edastamise eeskirjad on sätestatud selle määruse V peatükis, täpsemalt artiklites 44–50. Isikuandmete liikumine Euroopa Liidust väljaspool asuvatesse riikidesse ja neist riikidest on vajalik rahvusvahelise koostöö ja kaubanduse laiendamiseks, samas tagades, et ei alandata Euroopa Liidus isikuandmetele pakutava kaitse taset.

(2) Määruse (EL) 2016/679 artikli 45 lõike 3 alusel võib komisjon võtta rakendusaktiga vastu otsuse, et kolmas riik või kolmanda riigi territoorium või kolmanda riigi üks või mitu kindlaksmääratud sektorit või rahvusvaheline organisatsioon tagab isikuandmete kaitse piisava taseme. Sellisel juhul võib edastada isikuandmeid sellesse kolmandasse riiki või sellele kolmanda riigi territooriumile või sektorile või rahvusvahelisele organisatsioonile ilma täiendava loata, nagu on sätestatud määruse artikli 45 lõikes 1 ja põhjenduses 103.

(3) Nagu on märgitud määruse (EL) 2016/679 artikli 45 lõikes 2, tuleb kaitse piisavuse otsuse vastuvõtmisel tugineda kolmanda riigi õiguskorra põhjalikule analüüsile, mis hõlmab nii andmete importijate suhtes kohaldatavaid eeskirju kui ka isikuandmetele juurdepääsul avaliku sektori asutustele kehtestatud piiranguid ja seotud tagatisi. Hinnanguga tuleb määrata kindlaks, kas kõnealune kolmas riik tagab kaitsetaseme, mis „sisuliselt vastab“ Euroopa Liidus tagatud kaitsetasemele (määruse (EL) 2016/679 põhjendus 104). Nagu Euroopa Liidu Kohus on selgitanud, ei eelda see identset kaitsetaset ([2]). Eelkõige võivad vahendid, mida asjaomane kolmas riik kasutab, erineda nendest, mida Euroopa Liidus rakendatakse, kuivõrd need osutuvad praktikas piisava kaitsetaseme tagamisel tulemuslikuks ([3]). Piisavuse nõue ei eelda seega liidu eeskirjade punkthaaval kordamist. Küsimus on pigem selles, kas ELi-väline

([1]) ELT L 119, 4.5.2016, lk 1.
([2]) Kohtuasi C-362/14, Maximillian Schrems *vs.* Data Protection Commissioner (edaspidi „Schrems“), ECLI:EU:C:2015:650, punkt 73.
([3]) Schrems, punkt 74.

süsteem tervikuna tagab privaatsusõiguste sisu, nende tõhusa rakendamise, järelevalve ja teostamise kaudu nõutava isikuandmete kaitse taseme ([4]).

(4) Komisjon on hoolikalt analüüsinud Jaapani õigust ja tavasid. Komisjon teeb põhjendustes 6–175 esitatud tulemustele tuginedes järelduse, et Jaapan tagab isikuteabe kaitse seaduse ([5]) kohaldamisalasse kuuluvatele organisatsioonidele edastatavate isikuandmete piisava kaitsetaseme, järgides ka käesolevas otsuses osutatud lisatingimusi. Need tingimused on ette nähtud isikuteabe kaitse komisjoni poolt vastu võetud lisaeeskirjades (I lisa) ([6]) ning Jaapani valitsuse poolt Euroopa Komisjonile esitatud ametlikes seisukohtades, kinnitustes ja kohustustes (II lisa).

(5) Käesoleva otsuse kohaselt võib edastada andmeid Euroopa Majanduspiirkonnas (EMP) ([7]) asuvalt vastutavalt või volitatud töötlejalt sellistele organisatsioonidele Jaapanis ilma, et oleks vaja taotleda lisaluba. Otsus ei mõjuta selliste organisatsioonide suhtes määruse (EL) 2016/679 otsest kohaldamist, kui selle artikli 3 tingimused on täidetud.

2. EESKIRJAD, MIDA KOHALDATAKSE ANDMETE TÖÖTLEMISEL ETTEVÕTJATE POOLT

2.1. Jaapani andmekaitseraamistik

(6) Jaapanis privaatsust ja andmekaitset reguleeriv õigussüsteem toetub 1946. aastal välja kuulutatud põhiseadusele.

(7) Põhiseaduse artiklis 13 on sätestatud:

„Kõiki inimesi austatakse kui üksikisikuid. Nende õigus elule, vabadusele ja õnnelikkusele on määral, mil see ei riiva üldsuse heaolu, ülim kaalutlus õigusaktides ja muudes valitsuse toimingutes.“

(8) Selle artikli alusel on Jaapani ülemkohus selgitanud üksikisikute õiguseid seoses isikuteabe kaitsega. 1969. aasta otsuses tunnustas ta õigust privaatsusele ja andmekaitsele kui põhiseaduslikku õigust ([8]). Eelkõige leidis kohus, et „igal isikul on vabadus kaitsta oma isikuteavet kolmandale isikule avaldamise või põhjenduseta avalikustamise eest“. Peale selle leidis ülemkohus 6. märtsi 2008. aasta otsuses ([9]) (Juki-Net), et „kodanike eraelulist vabadust kaitstakse avaliku võimu teostamise eest ning seda saab tõlgendada selliselt, et üksikisiku eraeluline vabadus hõlmab iga isiku vabadust kaitsta oma isikuteavet kolmandale isikule avaldamise või põhjenduseta avalikustamise eest“ ([10]).

(9) 30. mail 2003 kehtestas Jaapan andmekaitse valdkonnas mitu seadust:

— isikuteabe kaitse seadus (*Act on the Protection of Personal Information*, APPI);

— haldusorganite hoitava isikuteabe kaitse seadus (*Act on the Protection of Personal Information Held by Administrative Organs*, APPIHAO);

— haldusametite hoitava isikuteabe kaitse seadus (*Act on the Protection of Personal Information Held by Incorporated Administrative Agencies*, APPI-IAA).

([4]) Vt komisjoni teatis Euroopa Parlamendile ja nõukogule „Isikuandmete vahetamine ja kaitsmine globaliseerunud maailmas“, COM(2017) 7, 10.1.2017, punkt 3.1, lk 6–7.
([5]) Isikuteabe kaitse seadus (seadus nr 57, 2003).
([6]) Lisateave isikuteabe kaitse komisjoni kohta on kättesaadav järgmisel aadressil: https://www.ppc.go.jp/en/ (sealhulgas kontaktandmed päringute ja kaebuste esitamiseks: https://www.ppc.go.jp/en/contactus/access/).
([7]) Käesolev otsus on EMPs kohaldatav. Euroopa Majanduspiirkonna lepingus (edaspidi „EMP leping“) on ette nähtud Euroopa Liidu siseturu laiendamine kolmele EMP liikmesriigile Islandile, Liechtensteinile ja Norrale. Ühiskomitee otsus, millega inkorporeeritakse määrus (EL) 2016/679 EMP lepingu XI lisasse, võeti EMP ühiskomitee poolt vastu 6. juulil 2018 ja see jõustus 20. juulil 2018. Määrus on seega selle lepinguga hõlmatud.
([8]) Ülemkohtu suurkoja 24. detsembri 1969. aasta otsus, Keishu kd 23, nr 12, lk 1625.
([9]) Ülemkohtu 6. märtsi 2008. aasta otsus, Minshu kd 62, nr 3, lk 665.
([10]) Ülemkohtu 6. märtsi 2008. aasta otsus, Minshu kd 62, nr 3, lk 665.

(10) Kaks viimasena nimetatud õigusakti (muudetud 2016. aastal) sisaldavad isikuteabe kaitse suhtes avaliku sektori asutuste kohaldatavaid sätteid. Nende õigusaktide kohaldamisalasse kuuluv andmetöötlus ei ole käesolevas otsuses järeldatud piisavuse objekt; see järeldus piirdub isikuteabe kaitsega „isikuteavet käitlevate ettevõtjate“ poolt APPI tähenduses.

(11) APPIt on viimastel aastatel reformitud. Muudetud APPI kuulutati välja 9. septembril 2015 ja see jõustus 30. mail 2017. Muudetud õigusaktiga kehtestati mitu uut kaitsemeedet ja tugevdati ka kehtivaid kaitsemeetmeid, lähendades seega Jaapani andmekaitsesüsteemi Euroopa süsteemile. See hõlmab näiteks täitmisele pööratavaid individuaalseid õiguseid või sellise sõltumatu järelevalveasutuse (isikuteabe kaitse komisjoni) asutamist, kellele tehakse ülesandeks APPI järelevalve ja täitmise tagamine.

(12) Lisaks APPI-le kohaldatakse käesoleva otsuse kohaldamisalasse kuuluva isikuteabe töötlemise suhtes APPI alusel välja antud rakenduseeskirju. Muu hulgas võib nimetada valitsuse määruse muudatust, et tagada 5. oktoobri 2016. aasta isikuteabe kaitse seaduse täitmine, ja isikuteabe kaitse seaduse täitmise tagamise eeskirju, mille on vastu võtnud isikuteabe kaitse komisjon ([11]). Mõlemad regulatsioonid on õiguslikult siduvad ja täitmisele pööratavad ning jõustusid samal ajal kui muudetud APPI.

(13) Peale selle andis Jaapani valitsus (mis koosneb peaministrist ja tema valitsuse moodustavatest ministritest) 28. oktoobril 2016 välja „aluspoliitika“, et „edendada põhjalikult ja terviklikult isikuteabe kaitse alaseid meetmeid“. Kooskõlas APPI artikliga 7 antakse aluspoliitika välja valitsuse otsusena ning see hõlmab APPI täitmise tagamise poliitilisi suuniseid, mis on suunatud nii keskvalitsusele kui ka kohalikele omavalitsustele.

(14) Jaapani valitsus muutis aluspoliitikat hiljuti 12. juunil 2018 vastu võetud valitsuse otsusega. Eesmärgiga hõlbustada rahvusvahelist andmete edastamist delegeeritakse nimetatud valitsuse otsusega isikuteabe kaitse komisjonile kui ametiasutusele, mis on pädev haldama ja rakendama APPIt, „õigus võtta vajalikke meetmeid, et vähendada süsteemide ja toimingute erinevusi Jaapani ja asjaomase välisriigi vahel seaduse artikli 6 alusel, pidades silmas sellelt riigilt saadud isikuteabe asjakohast käitlemist“. Valitsuse otsuses sätestatakse, et see hõlmab õigust kehtestada ulatuslikum kaitse seeläbi, et isikuteabe kaitse komisjon võtab vastu rangemad eeskirjad, mis täiendavad APPIt ja valitsuse määrust või on neist ulatuslikumad. Otsuse kohaselt on need rangemad eeskirjad Jaapani ettevõtjate jaoks siduvad ja täitmisele pööratavad.

(15) Isikuteabe kaitse komisjon võttis APPI artikli 6 ja nimetatud valitsuse otsuse alusel 15. juunil 2018 vastu „isikuteabe kaitse seaduse kohased lisaeeskirjad kaitse piisavuse otsuse alusel EList edastatud isikuandmete käitlemise kohta“ (edaspidi „lisaeeskirjad“) eesmärgiga täiustada Euroopa Liidust Jaapanisse edastatud isikuteabe kaitset, tuginedes praegusele kaitse piisavuse otsusele. Need lisaeeskirjad on Jaapani ettevõtjate suhtes õiguslikult siduvad ja täitmisele pööratavad nii isikuteabe kaitse komisjoni kui ka kohtute poolt samamoodi nagu APPI sätted, mida eeskirjad täiendavad rangemate ja/või üksikasjalikumate eeskirjadega ([12]). Kuna Euroopa Liidust isikuandmeid saavatele ja/või neid töötlevatele Jaapani ettevõtjatele pannakse õiguslik kohustus lisaeeskirju järgida, peavad nad tagama (nt tehniliselt („sildistades“) või korralduslikult (spetsiaalses andmebaasis talletades)), et nad saavad selliseid isikuandmeid nende olelusringi kestel tuvastada ([13]). Järgmistes punktides on analüüsitud iga lisaeeskirja sisu nende APPI artiklite hindamise osana, mida need täiendavad.

(16) Erinevalt olukorrast enne 2015. aasta muudatust, kui see kuulus konkreetsetes sektorites Jaapani ministeeriumide pädevusse, lubatakse APPIga isikuteabe kaitse komisjonil võtta vastu „suunised“, et andmekaitse-eeskirjade raames „tagada ettevõtja võetavate meetmete nõuetekohane ja tõhus rakendamine“. Isikuteabe kaitse komisjoni suunised toimivad nende eeskirjade autoriteetse tõlgendusena, eriti APPI puhul. Isikuteabe kaitse komisjonilt saadud teabe

([11]) Kättesaadav aadressil: https://www.ppc.go.jp/files/pdf/PPC_rules.pdf

([12]) Vt lisaeeskirjad (sissejuhatav osa).

([13]) Üldnõue, et protokolle tuleb säilitada (üksnes) teatud aja jooksul, ei sea seda kahtluse alla. Kuigi andmete päritolu kuulub sellise teabe hulka, millele isikuteavet saav käitlev ettevõtja peab saama APPI artikli 26 lõike 1 kohaselt kinnituse, puudutab APPI artikli 26 lõike 4 kohane nõue koosmõjus isikuteabe kaitse komisjoni eeskirjade artikliga 18 üksnes teatud liiki protokolli (vt isikuteabe kaitse komisjoni eeskirjade artikkel 16) ega takista isikuteavet käitlevat ettevõtjat tagamast andmete tuvastamise pikema aja jooksul. Seda on kinnitanud ka isikuteabe kaitse komisjon, kes märkis, et „[i]sikuteavet käitlev ettevõtja peab säilitama teavet ELi andmete päritolu kohta niikaua, kui see on lisaeeskirjade järgmiseks vajalik“.

kohaselt moodustavad need suunised õigusraamistiku lahutamatu osa ning neid tuleb tõlgendada koos APPIga, valitsuse määrusega, isikuteabe kaitse komisjoni eeskirjadega ning isikuteabe kaitse komisjoni koostatud küsimuste ja vastustega ([14]). Need on seega „ettevõtjate jaoks siduvad“. Kui suunistes märgitakse, et ettevõtja „peab“ tegutsema või „ei tohiks“ tegutseda konkreetsel viisil, käsitab isikuteabe kaitse komisjon asjaomastele sätetele mittevastavust seaduse rikkumisena ([15]).

2.2. **Materiaalne ja isikuline kohaldamisala**

(17) APPI kohaldamisala on kindlaks määratud isikuteabe, isikuandmete ja isikuteavet käitleva ettevõtja määratletud mõistetega. Samal ajal on APPIga sätestatud mõned olulised välistused selle kohaldamisalast, eelkõige anonüümselt töödeldud isikuandmete ja teatavate ettevõtjate poolse töötlemise konkreetsete liikide puhul. Kuigi APPIs ei kasutata mõistet „töötlemine“, on selles olulisel kohal samaväärne mõiste „käitlemine“, mis isikuteabe kaitse komisjonilt saadud teabe kohaselt hõlmab „igasugust isikuandmetega ümberkäimist“, sealhulgas isikuandmete hankimist, sisestamist, kogumist, korraldamist, säilitamist, toimetamist/töötlemist, uuendamist, kustutamist, väljastamist, kasutamist või esitamist.

2.2.1. *Isikuteabe määratlus*

(18) APPI materiaalse kohaldamisala puhul on APPIs eristatud isikuteavet ja isikuandmeid ning isikuteabe suhtes kohaldatakse seejuures üksnes teatavaid seaduse sätteid. APPI artikli 2 lõike 1 kohaselt kuulub isikuteabe mõiste alla igasugune teave, mis on seotud elava isikuga ja võimaldab seda isikut tuvastada. Määratluses eristatakse kaht liiki isikuteavet: i) isikukoodid ja ii) muu isikuteave, mille järgi saab konkreetse isiku tuvastada. Teise liigi alla kuulub teave, millest ei piisa isiku tuvastamiseks, kuid mida muu teabega „lihtsasti kõrvutades“ on võimalik konkreetne isik tuvastada. Isikuteabe kaitse komisjoni suuniste ([16]) kohaselt hinnatakse seda, kas teavet saab käsitada „lihtsasti kõrvutatavana“, iga juhtumi korral eraldi, võttes arvesse ettevõtja tegelikku olukorda („seisundit“). Seda eeldatakse, kui selline kõrvutamine on (või võib olla) jõukohane keskmisele (ehk tavalisele) ettevõtjale, kasutades talle kättesaadavaid vahendeid. Näiteks ei ole teave muu teabega „lihtsasti kõrvutatav“, kui ettevõtja peab tegema tavatuid jõupingutusi või panema toime ebaseaduslikke tegusid, et saada ühelt või mitmelt ettevõtjalt kõrvutatavat teavet.

2.2.2. *Isikuandmete määratlus*

(19) APPI kohaselt kuulub isikuandmete mõiste alla üksnes teatavat laadi isikuteave. Tegelikult on „isikuandmed“ määratletud kui „isikuteave, mis moodustab isikuteabe andmebaasi“ ehk „ühise teabekogu“, mis sisaldab isikuteavet, mis on „süsteemselt organiseeritud selliselt, et arvutit kasutades saaks otsida konkreetset isikuteavet“ ([17]) või „mille puhul on valitsuse määrusega ette nähtud, et see peab olema süsteemselt organiseeritud selliselt, et oleks võimalik lihtsasti otsida konkreetset isikuteavet“, aga „jättes välja valitsuse määrusega ette nähtud teabe, mille puhul on üksikisiku õiguste ja huvide kahjustamine ebatõenäoline, võttes arvesse selle kasutusmeetodit“ ([18]).

(20) Seda erandit on täpsustatud valitsuse määruse artikli 3 lõikes 1, mille kohaselt peavad olema täidetud kolm järgmist kumulatiivset tingimust: i) ühine teabekogu peab olema „komplekteeritud suurele hulgale määramata isikutele müümiseks ja komplekteerimisega ei ole rikutud seadust ega seadusel alusel antud määrust“, ii) seda peab olema võimalik „osta mis tahes ajal suure arvu määratlemata isikute poolt“ ja iii) selles sisalduvad isikuandmed

([14]) Isikuteabe kaitse komisjon, küsimused ja vastused, 16. veebruar 2017 (muudetud 30. mail 2017), kättesaadav järgmisel aadressil: https://www.ppc.go.jp/files/pdf/kojouhouQA.pdf. Küsimustes ja vastustes kajastatakse mitut suunistes käsitletud teemat, tuues praktilisi näiteid muu hulgas selle kohta, millal on tegemist tundlike isikuandmetega, individuaalse sisu tõlgendamise, pilvandmetöötluse korral kolmandatele isikutele edastamisega või piiriülese edastamise suhtes kohaldatava dokumentide arvestuse pidamise kohustusega. Küsimused ja vastused on kättesaadavad üksnes jaapani keeles.

([15]) Vastusena sellekohasele küsimusele andis isikuteabe kaitse komisjon Euroopa Andmekaitsenõukogule teada, et „Jaapani kohtud tuginevad konkreetsete kohtuasjade lahendamisel APPI / isikuteabe kaitse komisjoni eeskirju tõlgendades suunistele ja on selliselt oma otsustes otse osutanud isikuteabe kaitse komisjoni suuniste sõnastusele. Seepärast on isikuteabe kaitse komisjoni suunised ettevõtjate jaoks siduvad ka sellest aspektist. Isikuteabe kaitse komisjoni teada ei ole kohus kunagi suunistest kõrvale kaldunud.“ Isikuteabe kaitse komisjon juhtis seejuures komisjoni tähelepanu ka andmekaitse valdkonna kohtuotsusele, milles kohus tugines oma järeldustes sõnaselgelt suunistele (vt Osaka ringkonnakohtu 19. mai 2006. aasta otsus, Hanrei Juho, kd 1948, lk 122, milles kohus otsustas, et ettevõtjal on kohustus võtta nende suuniste alusel turvakontrolli meetmeid).

([16]) Isikuteabe kaitse komisjoni suunised (üldeeskirjade väljaanne), lk 6.

([17]) See hõlmab elektroonilist andmete kogumit. Isikuteabe kaitse komisjoni suunistes (üldväljaanne, lk 17) on selle kohta eraldi näited (nagu e-postikliendi tarkvaras salvestatud e-posti aadresside nimekiri).

([18]) APPI artikli 2 lõiked 4 ja 6.

tuleb „esitada nende algsel eesmärgil, lisamata muud elava isikuga seotud teavet“. Isikuteabe kaitse komisjoni selgituste kohaselt kehtestati selline kitsalt määratletud erand selleks, et jätta välja telefoniraamatud ja muud samalaadsed kataloogid.

(21) Jaapanis kogutud andmete puhul on „isikuteabe“ ja „isikuandmete“ eristamine oluline, sest selline teave ei pruugi alati olla osa „isikuteabe andmebaasist“ (näiteks käsitsi kogutud ja töödeldud üksik andmekogum) ning seega ei kohaldata APPI sätteid, mis on seotud üksnes isikuandmetega ([19]).

(22) Ent kaitse piisavuse otsusele tuginedes Euroopa Liidust Jaapanisse imporditud isikuandmete puhul ei ole selline eristamine oluline. Kuna selliseid andmeid edastatakse tavaliselt elektrooniliste vahendite kaudu (arvestades, et digitaalajastul vahetatakse andmeid harilikult sel viisil, eriti kui vahemaad on nii suured nagu ELi ja Jaapani vahel) ja need muutuvad seega importija elektroonilise andmete kogumi osaks, liigitatakse ELi andmed APPI alusel alati „isikuandmeteks“. Erandjuhul, mil isikuandmeid edastataks EList muul viisil (nt paberkandjal), kuuluksid need sellegipoolest APPI kohaldamisalasse, kui need pärast edastamist integreeritakse „ühisesse teabekogusse“, mis on süstemaatiliselt korraldatud selliselt, et konkreetset teavet on lihtne otsida (APPI artikli 2 lõike 4 punkt ii). Valitsuse määruse artikli 3 lõike 2 kohaselt on see nii juhul, kui teave on korraldatud „teatava eeskirja kohaselt“ ja andmebaas sisaldab otsingu hõlbustamiseks selliseid tööriistu nagu sisukord või indeks. See vastab andmete kogumi määratlusele isikuandmete kaitse üldmääruse artikli 2 lõike 1 tähenduses.

2.2.3. *Säilitatavate isikuandmete määratlus*

(23) Teatavaid APPI sätteid, eelkõige artikleid 27–30, mis on seotud individuaalsete õigustega, kohaldatakse üksnes isikuandmete eriliigi, nimelt säilitatavate isikuandmete suhtes. Need on APPI artikli 2 lõikes 7 määratletud kui muud isikuandmed peale andmete, mis on kas i) „valitsuse määruse kohaselt andmed, mis tõenäoliselt kahjustavad avalikke või muid huve, kui tehakse teatavaks nende olemasolu või puudumine“ või ii) „andmed, mis tuleb kustutada valitsuse määrusega ette nähtud kuni üheaastase ajavahemiku jooksul“.

(24) Neist liikidest esimest on selgitatud valitsuse määruse artiklis 4 ja see hõlmab nelja laadi erandeid ([20]). Nende eranditega soovitakse saavutada sarnased eesmärgid nagu on loetletud määruse (EL) 2016/679 artikli 23 lõikes 1, nimelt andmesubjekti (APPI terminoloogia järgi „volitaja“) kaitse ja teiste isikute vabaduse kaitse, riigi julgeolek, avalik julgeolek, kriminaalõiguse täitmise tagamine või muud olulised üldist avalikku huvi pakkuvad eesmärgid. Lisaks tuleneb valitsuse määruse artikli 4 lõike 1 punktide i–iv sõnastusest nende kohaldamisel alati eeldus, et mõne olulise kaitstud huvi puhul esineb konkreetne risk ([21]).

(25) Teist liiki on täpsustatud ka valitsuse määruse artiklis 5. Koostoimes APPI artikli 2 lõikega 7 jäetakse säilitatavate isikuandmete mõiste puhul kohaldamisalast ja seega APPI kohaste individuaalsete õiguste alt välja isikuandmed, „mis tuleb kustutada“ kuue kuu jooksul. Isikuteabe kaitse komisjon on selgitanud, et selle erandi eesmärk on motiveerida ettevõtjaid säilitama ja töötlema andmeid võimalikult lühikese ajavahemiku jooksul. Samas tähendaks see, et ELi andmesubjektid ei saaks kasutada olulisi õiguseid üksnes asjaomase ettevõtja poolt nende andmete säilitamise kestuse tõttu.

(26) Selle olukorra lahendamiseks on lisaeeskirjas 2 nõutud, et Euroopa Liidust edastatavaid isikuandmeid „tuleks käsitada säilitatavate isikuandmetena seaduse artikli 2 lõike 7 tähenduses, olenemata ajavahemikust, mille jooksul need tuleb kustutada“. Seega ei mõjuta säilitamisperiood ELi andmesubjektidele antud õigusi.

([19]) Näiteks APPI artikkel 23 isikuandmete kolmandate isikutega jagamise tingimuste kohta.

([20]) Nimelt isikuandmeid, i) „mille puhul esineb võimalus, et kui asjaomaste isikuandmete olemasolu või puudumine tehakse teatavaks, kahjustaks see volitaja või kolmanda isiku elu, tervist või varalist seisundit“; ii) andmeid, „mille puhul esineb võimalus, et kui asjaomaste isikuandmete olemasolu või puudumine tehakse teatavaks, julgustaks või kallutaks see ebaseaduslikule või ebaõiglasele teole“; iii) andmeid, „mille puhul esineb võimalus, et kui asjaomaste isikuandmete olemasolu või puudumine tehakse teatavaks, vähendaks see riiklikku julgeolekut, hävitaks usaldussuhte välisriigiga või rahvusvahelise organisatsiooniga või tekitaks ebasoodsa olukorra läbirääkimistel välisriigiga või rahvusvahelise organisatsiooniga“; ning iv) andmeid, „mille puhul esineb võimalus, et kui asjaomaste isikuandmete olemasolu või puudumine tehakse teatavaks, takistaks see avaliku turvalisuse ja korra tagamist, näiteks kuriteo ennetamist, peatamist või uurimist“.

([21]) Sellistel juhtudel ei ole üksikisiku teavitamine nõutav. See on kooskõlas isikuandmete kaitse üldmääruse artikli 23 lõike 2 punktiga h, mille kohaselt ei tule andmesubjekte piirangust teavitada, kui see „võib mõjutada piirangu eesmärki“.

2.2.4. *Anonüümselt töödeldava isikuteabe mõiste*

(27) Anonüümselt töödeldava isikuteabe suhtes kohaldatavad nõuded, nagu on määratletud APPI artikli 2 lõikes 9, on sätestatud seaduse IV peatüki 2. jaos (anonüümselt töödeldavat teavet käitleva ettevõtja kohustused). Seevastu ei reguleeri sellist teavet APPI IV peatüki 1. jao sätted, sealhulgas artiklid, millega on sätestatud andmekaitsega seotud kaitsemeetmed ja õigused, mida kohaldatakse selle seaduse alusel isikuandmete töötlemisel. Seega ehkki „anonüümselt töödeldava isikuteabe" suhtes ei kehti „tavapärased" andmekaitse-eeskirjad (mis on sätestatud APPI IV peatüki 1. jaos ja artiklis 42), kuuluvad need APPI ja eelkõige artiklite 36–39 kohaldamisalasse.

(28) Kooskõlas APPI artikli 2 lõikega 9 on „anonüümselt töödeldav isikuteave" üksikisikuga seotud teave, mis on „saadud isikuteabe töötlemisel" kooskõlas APPIs (artikli 36 lõige 1) ette nähtud ja isikuteabe kaitse komisjoni eeskirjades (artikkel 19) täpsustatud meetmetega selliselt, et ei ole võimalik tuvastada konkreetset üksikisikut ega taastada isikuteavet.

(29) Nagu kinnitab ka isikuteabe kaitse komisjon, nähtub nendest sätetest, et isikuteabe „anonüümseks" muutmise protsess ei pea olema tehniliselt pöördumatu. Kooskõlas APPI artikli 36 lõikega 2 peavad ettevõtjad, kes käitlevad „anonüümselt töödeldavat isikuteavet" üksnes ennetama uuesti tuvastamist, võttes meetmeid, millega on tagatud selliste „kirjelduste vms ja isikukoodide, mis kustutatakse anonüümselt töödeldava teabe loomiseks kasutatava isikuteabe seast, ning kasutatud töötlemismeetodi alase teabe" turvalisus.

(30) Kuna APPIs määratletud „anonüümselt töödeldav isikuteave" hõlmab andmeid, mille puhul on isiku uuesti tuvastamine endiselt võimalik, võib see tähendada, et Euroopa Liidust edastatud isikuandmed võivad kaotada osa võimalikust kaitsest protsessis, mida peetakse määruse (EL) 2016/679 alusel pigem „pseudonümiseerimise" kui „anonümiseerimise" vormiks (seega ei muutu nende kui isikuandmete laad).

(31) Selle olukorra lahendamiseks on lisaeeskirjades ette nähtud lisanõuded, mida kohaldatakse üksnes selle otsuse alusel Euroopa Liidust edastatud isikuandmete suhtes. Lisaeeskirjade eeskirja 5 kohaselt käsitatakse sellist isikuteavet APPI tähenduses „anonüümselt töödeldava isikuteabena" üksnes juhul, „kui isikuteavet käitlev ettevõtja võtab meetmeid, mis muudavad isiku uuesti tuvastamise igaühe jaoks võimatuks, sealhulgas kustutades töötlemismeetodi jms teabe". Viimasena nimetatud teave on lisaeeskirjades määratletud kui teave, mis on seotud kirjelduste ja isikukoodidega, mis kustutati isikuteabest, et luua anonüümselt töödeldav isikuteave, samuti teave, mis on seotud töötlemismeetodiga, mida kasutati nende kirjelduste ja isikukoodide kustutamisel. Teisisõnu nõutakse lisaeeskirjadega, et ettevõtja, kes loob anonüümselt töödeldavat isikuteavet, peab hävitama „võtme", mis võimaldab andmeid uuesti isikuga siduda. See tähendab, et Euroopa Liidust pärit isikuandmete puhul kehtivad APPI sätted, millega reguleeritakse „anonüümselt töödeldavat isikuteavet", üksnes juhtudel, mil neid käsitataks samamoodi anonüümse teabena määruse (EL) 2016/679 ([22]) alusel.

2.2.5. *Isikuteavet käitleva ettevõtja määratlus*

(32) Isikulise kohaldamisala poolest kohaldatakse APPI üksnes isikuteavet käitlevate ettevõtjate suhtes. Isikuteavet käitlev ettevõtja on APPI artikli 2 lõikes 5 määratletud kui „isik, kes esitab isikuteabe andmebaasi vms äritegevuses kasutamiseks", välja arvatud valitsus- ja haldusasutused nii kesk- kui ka kohalikul tasandil.

(33) Isikuteabe kaitse komisjoni suuniste kohaselt tähendab „äritegevus" igasugust „tegevust, mille eesmärk on korduvalt ja pidevalt käitada teataval eesmärgil tulunduslikku või mittetulunduslikku sotsiaalselt tunnustatud ettevõtet". Organisatsioone, mis ei ole juriidilised isikud (näiteks *de facto* ühingud), või üksikisikuid käsitatakse isikuteavet käitleva ettevõtjana, kui nad tagavad (kasutavad) isikuteabe andmebaasi jne oma äritegevuses ([23]). Seega on „äritegevuse" mõiste APPI alusel väga lai, kuna see hõlmab igat liiki organisatsioonide ja üksikisikute tulunduslikku ja mittetulunduslikku tegevust. Peale selle hõlmab „äritegevuses kasutamine" ka isikuteavet, mida ei kasutata ettevõtja (välistes) kaubandussuhetes, vaid asutusesiseselt, näiteks töötajate andmete töötlemiseks.

([22]) Vt määruse (EL) 2016/679 põhjendus 26.
([23]) Isikuteabe kaitse komisjoni suunised (üldeeskirjade väljaanne), lk 18.

(34) Mis puutub APPIs sätestatud kaitset saavatesse isikutesse, ei tehta seaduses isikutel vahet nende kodakondsuse, elukoha või asukoha järgi. Sama kehtib üksikisikute võimalusega pöörduda õiguskaitse saamiseks isikuteabe kaitse komisjoni või kohtu poole.

2.2.6. *Vastutava ja volitatud töötleja mõisted*

(35) APPI alusel ei eristata selgelt vastutavatele ja volitatud töötlejatele pandud kohustusi. Selle eristamise puudumine ei mõjuta kaitsetaset, sest kõik isikuteavet käitlevad ettevõtjad peavad täitma kõiki seaduse sätteid. Isikuteavet käitlev ettevõtja, kes usaldab isikuandmete käitlemise usaldusisikule (vastab isikuandmete kaitse üldmääruse kohasele volitatud töötlejale), on endiselt kohustatud usaldatud andmete suhtes täitma talle APPI ja lisaeeskirjadega pandud kohustusi. Lisaks peab ta APPI artikli 22 kohaselt „tegema vajalikku ja asjakohast järelevalvet" usaldusisiku üle. Nagu isikuteabe kaitse komisjon on kinnitanud, on samas ka usaldusisik seotud APPI ja lisaeeskirjade kõigi kohustustega.

2.2.7. *Valdkonnapõhised välistused*

(36) APPI artikliga 76 on teatavat liiki andmetöötlus välistatud seaduse IV peatüki kohaldamisalast, mis sisaldab keskseid andmekaitsesätteid (aluspõhimõtted, ettevõtjate kohustused, individuaalsed õigused, isikuteabe kaitse komisjoni tehtav järelevalve). Artiklis 76 sätestatud valdkonnapõhise välistamisega hõlmatud töötlemine on samuti vabastatud isikuteabe kaitse komisjoni täitmise tagamise volitustest kooskõlas APPI artikli 43 lõikega 2 ([24]).

(37) APPI artiklis 76 sätestatud valdkonnapõhise välistamisel asjaomaste liikide määratlemisel on kasutatud topeltkriteeriumi, mis põhineb isikuteavet käitleva ettevõtja liigil ja töötlemise eesmärgil. Täpsemalt kohaldatakse erandit järgmiste isikute suhtes: i) ringhäälinguasutused, ajalehtede kirjastused, kommunikatsiooniagentuurid või muud pressiorganisatsioonid (sealhulgas üksikisikud, kes tegelevad oma äritegevuses pressitegevusega) määral, mil nad töötlevad ajakirjanduse eesmärgil isikuteavet; ii) isikud, kes tegelevad kutselise kirjutamisega määral, mil see hõlmab isikuteavet; iii) ülikoolid ja muud akadeemilistele õpingutele suunatud organisatsioonid või grupid või sellisesse organisatsiooni kuuluvad isikud määral, mil nad töötlevad akadeemiliste õpingute eesmärgil isikuteavet; iv) usulised organid määral, mil nad töötlevad isikuteavet usulise tegevuse eesmärgil (sealhulgas kõik seotud tegevused); ja (v) poliitilised organid määral, mil nad töötlevad isikuteavet oma poliitilise tegevuse eesmärgil (sealhulgas kõik seotud tegevused). Isikuteabe töötlemine ühel artiklis 76 loetletud eesmärkidest teist liiki isikuteavet käitlevate ettevõtjate poolt, samuti isikuandmete töötlemine teisel eesmärgil mõne loetletud isikuteavet käitleva ettevõtja poolt, näiteks tööhõive kontekstis, on endiselt hõlmatud IV peatüki sätetega.

(38) Selleks et tagada Euroopa Liidust Jaapani ettevõtjatele edastatud isikuandmete piisav kaitsetase, tuleks käesoleva otsusega hõlmata üksnes selline isikuteabe töötlemine, mis kuulub APPI IV peatüki kohaldamisalasse – st isikuteavet käitleva ettevõtja poolt määral, mil töötlemisolukord ei vasta ühele valdkondlikule välistustest. Selle kohaldamisala tuleks seega ühtlustada APPI kohaldamisalaga. Isikuteabe kaitse komisjonilt saadud teabe kohaselt käsitatakse olukorda, kui isikuteavet käitlev ettevõtja, kelle suhtes kohaldatakse käesolevat otsust, hiljem kasutuseesmärki (lubatud ulatuses) muudab ja kelle suhtes seejärel kohaldataks APPI artiklis 76 sätestatud valdkonnapõhise välistamise juhtu, rahvusvahelise edastamisena (arvestades, et sellisel juhul ei oleks isikuandmete töötlemine enam hõlmatud APPI IV peatükiga ja jääks seega kohaldamisalast välja). Sama kehtiks juhul, kui isikuteavet käitlev ettevõtja esitab isikuandmeid APPI artikliga 76 hõlmatud üksusele selles sättes osutatud töötlemise eesmärgil kasutamiseks. Euroopa Liidust edastatavate isikuandmete puhul tähendaks see, et tegemist on edasisaatmisega, mille suhtes kehtivad vastavad kaitsemeetmed (eelkõige need, mis on sätestatud APPI artiklis 24 ja lisaeeskirjas 4). Kui isikuteavet käitleval ettevõtjal on vaja saada andmesubjekti nõusolek ([25]), peaks ettevõtja talle esitama kogu vajaliku teabe, sealhulgas teabe selle kohta, et isikuandmetele ei kehtiks enam APPI kohane kaitse.

([24]) Mis puutub teistesse ettevõtjatesse, siis ei takista isikuteabe kaitse komisjon oma uurimis- ja täitmise tagamise volitusi kasutades kunagi nende õigust väljendusvabadusele, akadeemilisele vabadusele, usuvabadusele ja poliitilise tegevuse vabadusele (APPI artikli 43 lõige 1).

([25]) Nagu isikuteabe kaitse komisjon selgitas, tõlgendatakse nõusolekut isikuteabe kaitse komisjoni suunistes järgmiselt: „volitaja tahteavaldus, millega ta nõustub oma isikuandmete käitlemisega isikuteavet käitleva ettevõtja osutatud meetodil". Isikuteabe kaitse komisjoni suunistes (üldeeskirjade väljaanne, lk 24) on loetletud nõusoleku andmisel „Jaapanis tavapärased äritavad", st suuline nõusolek, vormide või muude dokumentide tagastamine, e-posti teel kokkuleppimine, veebilehel lahtri märgistamine, kodulehel klõpsamine, nõusolekunupu kasutamine, puutepaneeli vajutamine jms. Kõiki nimetatud meetodeid loetakse sõnaselgeks nõusolekuks.

2.3. **Kaitsemeetmed, õigused ja kohustused**

2.3.1. *Eesmärgi piirang*

(39) Isikuandmeid tuleks töödelda konkreetsel eesmärgil ja kasutada seejärel üksnes määral, mil see on kooskõlas töötlemise eesmärgiga. See andmekaitsepõhimõte on tagatud APPI artiklitega 15 ja 16.

(40) APPIs on lähtutud põhimõttest, et ettevõtja peab määratlema kasutamise eesmärgi „nii selgelt kui võimalik“ (artikli 15 lõige 1) ning on seejärel kohustatud andmeid töödeldes seda eesmärki järgima.

(41) Selles suhtes on APPI artikli 15 lõikes 2 sätestatud, et isikuteavet käitlev ettevõtja ei või esialgset eesmärki muuta „rohkem kui ulatuses, mis on tunnistatud võrdlemisi asjakohaseks eelnevalt muudetud kasutuseesmärgi puhul“, tõlgendatuna isikuteabe kaitse komisjoni suunistes selliselt, et see vastab sellele, mida andmesubjekt saab objektiivselt eeldada, tuginedes „tavapärastele ühiskondlikele tavadele“ ([26]).

(42) Peale selle on APPI artikli 16 lõike 1 kohaselt isikuteavet käitlevatel ettevõtjatel keelatud eelnevat andmesubjekti nõusolekut küsimata ületada isikuteabe käitlemisel artiklis 15 määratletud „kasutuseesmärgi saavutamiseks vajalikku ulatust“, välja arvatud juhul, kui kohaldatakse üht artikli 16 lõike 3 eranditest ([27]).

(43) Mis puutub teiselt ettevõtjalt saadud isikuteabesse, siis võib isikuteavet käitlev ettevõtja põhimõtteliselt määrata uue kasutuseesmärgi ([28]). Selleks et tagada, et Euroopa Liidust edastamise korral on see saaja kohustatud järgima eesmärki, milleks andmeid edastati, on lisaeeskirjaga 3 nõutud, et juhtudel, mil „[isikuteavet käitlev ettevõtja] saab kaitse piisavuse otsuse alusel isikuandmeid EList“ või see ettevõtja „saab teiselt [isikuteavet käitlevalt ettevõtjalt] isikuandmeid, mis on varem kaitse piisavuse otsuse alusel edastatud EList“ (jagamiseks edasisaatmine), peab saaja „märkima nimetatud isikuandmete kasutamise eesmärgi selle kasutuseesmärgi ulatuses, milleks andmed esialgselt või hiljem saadi“. Teisisõnu tagab see eeskiri, et edastamise kontekstis määrab määruse (EL) 2016/679 kohaselt kindlaks määratud eesmärk jätkuvalt töötlemise ning selle eesmärgi muutmine töötlemise mis tahes etapis Jaapanis nõuaks ELi andmesubjekti nõusolekut. Isikuteavet käitlev ettevõtja peab selle nõusoleku saamiseks andmesubjektiga ühendust võtma ja kui see ei ole võimalik, tuleb säilitada algne eesmärk.

2.3.2. *Töötlemise õiguspärasus ja õiglus*

(44) Põhjenduses 43 viidatud lisakaitse on seda asjakohasem, et eesmärgi piirangu põhimõtte kaudu tagab Jaapani süsteem ka selle, et isikuandmeid töödeldakse õiguspäraselt ja õiglaselt.

(45) APPIs on sätestatud, et kui isikuteavet käitlev ettevõtja kogub isikuteavet, peab ta märkima isikuteabe kasutamise eesmärgi üksikasjalikult ([29]) ning teavitama kohe andmesubjekti sellest kasutuseesmärgist (või avalikustama selle üldsusele) ([30]). Lisaks on APPI artiklis 17 sätestatud, et isikuteavet käitlev ettevõtja ei hangi isikuandmeid pettuse teel ega muude sobimatute vahendite kaudu. Mis puutub teatavaid andmeliike nagu eritähelepanu nõudev isikuteave, siis tuleb nende omandamiseks saada andmesubjekti nõusolek (APPI artikli 17 lõige 2).

([26]) Isikuteabe kaitse komisjoni välja antud küsimused ja vastused sisaldavad mitut näidet selle mõiste illustreerimiseks. Olukordade, kus muutmine jääb mõistlikesse piiridesse, näidetena on muu hulgas nimetatud sellise isikuteabe kasutamist, mis on saadud kaupade või teenuste ostjatelt kaubandustehingu käigus, et teavitada neid ostjaid muudest asjaomastest pakutavatest kaupadest või teenustest (nt spordiklubi käitaja, kes registreerib liikmete e-posti aadressid, et teavitada treeningutest ja kavadest). Samas on küsimuste ja vastuste all esitatud ka näide sellise olukorra kohta, mille puhul kasutuseesmärgi muutmine ei ole lubatud, nimelt siis, kui äriühing saadab teavet äriühingu kaupade ja teenuste kohta e-posti aadressidele, mille ta on hankinud selleks, et hoiatada pettuse või liikmekaardi varguse eest.

([27]) Need erandid võivad tuleneda muudest õigusnormidest või puudutada olukordi, kus isikuteabe töötlemine on vajalik i) „inimese elu, tervise või vara kaitseks“; ii) selleks et „parandada avalikku hügieeni või edendada laste tervist“; või iii) „valitsuse ametite või organite või nende esindajatega koostöö tegemiseks“ nende seadusjärgsete ülesannete täitmisel. Peale selle kohaldatakse i ja ii punktis nimetatud liike üksnes siis, kui on keeruline saada andmesubjekti nõusolekut, ja iii punktis nimetatud liiki juhul, kui esineb risk, et andmesubjekti nõusoleku hankimine takistaks selliste ülesannete täitmist.

([28]) Seda arvestades nõutakse APPI artikli 23 lõike 1 alusel üksikisiku nõusolekut põhimõtteliselt selleks, et avaldada andmeid kolmandale isikule. Sel viisil saab üksikisik kasutada teatavat kontrolli selle üle, kuidas teine ettevõtja tema andmeid kasutab.

([29]) APPI artikli 15 lõike 1 kohaselt peab see määratlus olema „võimalikult selge“.

([30]) APPI artikli 18 lõige 1.

(46) Seega nagu on selgitatud põhjendustes 41 ja 42, on isikuteavet käitleval ettevõtjal keelatud töödelda isikuandmeid muudel eesmärkidel, välja arvatud juhul, kui andmesubjekt on sellise töötlemisega nõus või kui kohaldatakse mõnda APPI artikli 16 lõike 3 eranditest.

(47) Lisaks mis puutub isikuteabe edasisse edastamisse kolmandale isikule, ([31]) lubatakse APPI artikli 23 lõikega 1 sellist edastamist üksnes erijuhtumitel, mil üldiselt on nõutav andmesubjekti eelnev nõusolek ([32]). APPI artikli 23 lõigetes 2, 3 ja 4 on sätestatud nõusoleku saamise nõude erandid. Samas on sellised erandid kohaldatavad üksnes mittetundlike andmete puhul ning eeldusel, et ettevõtja eelnevalt teavitab asjaomaseid üksikisikuid kavatsusest avaldada nende isikuteavet kolmandale isikule ja võimalusest esitada sellele avaldamisele vastuväiteid ([33]).

(48) Mis puutub Euroopa Liidust edastamisse, siis peavad isikuandmed olema kõigepealt kogutud ja töödeldud ELis kooskõlas määrusega (EL) 2016/679. See tähendab alati ühelt poolt kogumist ja töötlemist, sealhulgas edastamist Euroopa Liidust Jaapanisse, tuginedes ühele määruse artikli 6 lõikes 1 loetletud õiguslikest alustest, ning teiselt poolt kogumist konkreetsel, selgel ja õiguspärasel eesmärgil ning edasise töötlemise keeldu, sealhulgas edastamise kaudu, viisil, mis ei ole määruse artikli 5 lõike 1 punktis b ja artikli 6 lõikes 4 sätestatud eesmärgiga kooskõlas.

(49) Pärast edastamist peab lisaeeskirja 3 kohaselt isikuteavet käitlev ettevõtja, kes saab andmeid, „kinnitama“ edastamise erieesmärki/erieesmärke (st eesmärk, mis on määratletud kooskõlas määrusega (EL) 2016/679) ning töötlema neid andmeid edaspidi kooskõlas selle eesmärgiga või nende eesmärkidega ([34]). See tähendab, et määruse alusel kindlaks määratud eesmärki või eesmärke peab lisaks isikuandmete esialgsele saajale Jaapanis järgima ka nende andmete edasine saaja, sh usaldusisik.

(50) Pealegi kui isikuteavet käitlev ettevõtja sooviks seda eesmärki muuta, nagu on varem määratletud määruses (EL) 2016/679, peaks ta kooskõlas APPI artikli 16 lõikega 1 saama põhimõtteliselt andmesubjekti nõusoleku. Ilma selle nõusolekuta oleks kasutuseesmärgi saavutamiseks vajalikust ulatuslikum andmete töötlemine artikli 16 lõike 1 rikkumine ja seega isikuteabe kaitse komisjoni ja kohtute poolt täitmisele pööratav.

(51) Seega arvestades, et määruse (EL) 2016/679 alusel on edastamiseks vaja kehtivat õiguslikku alust ja konkreetset eesmärki ning need vastavad APPI kohasele „kinnitatud“ kasutuseesmärgile, tagavad APPI ja lisaeeskirja 3 asjaomased sätted ELi andmete Jaapanis töötlemise jätkuva õiguspärasuse.

2.3.3. *Andmete täpsus ja minimeerimine*

(52) Andmed peavad olema õiged ja vajaduse korral ka ajakohastatud. Need peavad olema ka piisavad, asjakohased ja mitte ülemäärased seoses eesmärgiga, mille tarvis neid töödeldakse.

(53) Need põhimõtted tagatakse Jaapani õiguses APPI artikli 16 lõikega 1, mille kohaselt on keelatud isikuteabe käitlemisel ületada „kasutuseesmärgi saavutamiseks vajalikku ulatust“. Nagu isikuteabe kaitse komisjon on selgitanud, siis see mitte üksnes ei välista ebapiisavate andmete kasutamist ja andmete ülemäärast kasutamist (suuremas ulatuses, kui kasutuseesmärgi saavutamiseks vaja), vaid hõlmab ka selliste andmete käitlemise keeldu, mis ei ole kasutuseesmärgi saavutamiseks asjakohased.

([31]) Kuigi usaldusisikud jäetakse artikli 23 (vt lõige 5) kohaldamisel mõiste „kolmas isik“ alt välja, kohaldatakse seda erandit üksnes niivõrd, kui usaldusisik käitleb isikuandmeid talle usaldatud pädevuse piires („ületamata kasutuseesmärgi saavutamiseks vajalikku ulatust“), st tegutseb volitatud töötlejana.

([32]) Muud (erandlikud) põhjendused on: i) isikuteabe esitamine „õigusnormide alusel“; ii) juhtumid, „mil esineb vajadus kaitsta isiku elu, tervist või varalist seisundit ning on keeruline saada volitaja nõusolekut“; iii) juhtumid, „mil esineb erivajadus parandada avalikku hügieeni või edendada laste tervist ning on keeruline saada volitaja nõusolekut“; ning iv) juhtumid, „mil on vaja teha koostööd seoses keskvalitsuse organisatsiooni või kohaliku omavalitsusega või isikuga, kellele nad on andnud ülesande tegeleda õigusnormides ette nähtud küsimustega, ning on võimalus, et volitaja nõusoleku saamine takistaks nimetatud küsimustega tegelemist“.

([33]) Esitatav teave hõlmab eelkõige kolmanda isikuga jagatavate isikuandmete liike ja edastamise meetodit. Peale selle peab isikuteavet käitlev ettevõtja teavitama andmesubjekti võimalusest esitada edastamisele vastuväide ning sellest, kuidas esitada vastav taotlus.

([34]) APPI artikli 26 lõike 1 punkti ii alusel peab isikuteavet käitlev ettevõtja kolmandalt isikult isikuandmete saamise korral „kinnitama“ (kontrollima) „kolmandalt isikult isikuandmete saamise üksikasju“, sealhulgas selle saamise eesmärki. Ehkki artiklis 26 ei määratleta selgelt, et isikuteavet käitlev ettevõtja peab seda eesmärki järgima, on see sõnaselgelt nõutav lisaeeskirjaga 3.

(54) Mis puutub kohustusse tagada andmete õigsus ja ajakohasus, siis on APPI artikliga 19 nõutud, et isikuteavet käitlev ettevõtja „üritaks tagada isikuandmete õigsus ja ajakohus kasutuseesmärgi saavutamiseks vajalikus ulatuses“. Seda sätet tuleks tõlgendada koos APPI artikli 16 lõikega 1: kui isikuteavet käitlev ettevõtja ei järgi täpsuse suhtes ette nähtud nõudeid, siis isikuteabe kaitse komisjonilt saadud selgituste kohaselt ei loeta isikuteabe töötlemist kasutuseesmärki saavutatuks ning seega muutub selle käitlemine artikli 16 lõike 1 alusel ebaseaduslikuks.

2.3.4. *Säilitamise piirang*

(55) Andmeid ei tohiks põhimõtteliselt säilitada kauem kui see on vajalik isikuandmete töötlemise eesmärgi täitmiseks.

(56) APPI artikli 19 kohaselt peavad isikuteavet käitlevad ettevõtjad „püüdma […] kustutada isikuandmed viivitamata, kui nende kasutamine on muutunud ebavajalikuks“. Seda sätet tuleb tõlgendada koostoimes APPI artikli 16 lõikega 1, millega keelatakse isikuteabe käitlemisel ületada „kasutuseesmärgi saavutamiseks vajalikku ulatust“. Kui kasutuseesmärk on saavutatud, ei saa isikuteabe töötlemist enam vajalikuks pidada ning seega ei saa see jätkuda (välja arvatud juhul, kui isikuteavet käitlev ettevõtja saab selleks andmesubjekti nõusoleku).

2.3.5. *Andmete turvalisus*

(57) Isikuandmeid tuleks töödelda viisil, mis tagab nende turvalisuse, sealhulgas kaitse loata või ebaseadusliku töötlemise ning juhusliku kaotsimineku, hävimise või kahju eest. Sel eesmärgil peaks ettevõtjad võtma asjakohaseid tehnilisi ja korralduslikke meetmeid, et kaitsta isikuandmeid võimalike ohtude eest. Neid meetmeid tuleks hinnata, võttes arvesse tehnika taset ja seonduvaid kulusid.

(58) Seda põhimõtet rakendatakse Jaapani õiguses APPI artikliga 20, milles on sätestatud, et isikuteavet käitlev ettevõtja „peab võtma vajalikke ja asjakohaseid meetmeid isikuandmete turvakontrolliks, sealhulgas tema käideldavate isikuandmete lekke, kaotsimineku või kahju ärahoidmiseks“. Isikuteabe kaitse komisjoni suunistes selgitatakse võetavaid meetmeid, sealhulgas aluspoliitika, andmete käitlemise eeskirjade ja mitmesuguste „kontrollmeetmete“ kehtestamise meetodeid (organisatsioonilise ohutuse ning inimeste, füüsilise ja tehnoloogilise turvalisuse vallas) ([35]). Lisaks on isikuteabe kaitse komisjoni avaldatud suunistes ja spetsiaalses teates (lisa 8 võetavate ohutusjuhtimise meetmete sisu kohta) ette nähtud täiendavad üksikasjad meetmete kohta, mis on seotud turvaintsidentidega (nt isikuteabe leke) isikuteavet käitlevate ettevõtjate võetavate turvalisuse juhtimise meetmete osana ([36]).

(59) Peale selle tuleb alati, kui isikuteavet käitlevad töötajad või alltöövõtjad, tagada turvakontrolli eesmärgil „vajalik ja asjakohane järelevalve“ APPI artiklite 20 ja 21 alusel. Samuti on isikuteabe tahtliku lekitamise või varguse eest APPI artikliga 83 karistusena ette nähtud kuni üheaastane vangistus.

2.3.6. *Läbipaistvus*

(60) Andmesubjekte tuleks teavitada nende isikuandmete töötlemise põhiomadustest.

(61) APPI artikli 18 lõikega 1 nõutakse, et isikuteavet käitlevad ettevõtjad teevad andmesubjektile kättesaadavaks teabe saadud isikuteabe kasutamise eesmärgi kohta, välja arvatud „juhtudel, mil kasutuseesmärk on eelnevalt üldsusele avalikustatud“. Sama kohustus kehtib eesmärgi lubatava muutmise korral (artikli 18 lõige 3). Sellega tagatakse ühtlasi, et andmesubjektile antakse tema andmete kogumise asjaolust teada. Ehkki APPIga ei nõuta üldiselt, et isikuteavet käitlev ettevõtja teavitaks kogumise etapis andmesubjekti isikuteabe eeldatavatest saajatest, on selline teavitamine eeltingimus, et hiljem teavet ükskõik millisel viisil edastada kolmandale isikule (saajale) artikli 23 lõike 2 alusel, st juhul, kui selleks ei olnud andmesubjekti eelnevat nõusolekut.

([35]) Isikuteabe kaitse komisjoni suunised (üldeeskirjade väljaanne), lk 41 ja 86–98.

([36]) Isikuteabe kaitse komisjoni suuniste punkti 3.3.2 kohaselt peab isikuteavet käitlev ettevõtja sellise lekke, kahju või kaotsimineku korral korraldama vajaliku uurimise ning hindama eelkõige üksikisiku õiguste ja huvide rikkumise ulatust ning asjaomase isikuteabe laadi ja mahtu.

(62) Mis puutub „säilitatavatesse isikuandmetesse“, siis on APPI artiklis 27 sätestatud, et isikuteavet käitlev ettevõtja teavitab andmesubjekti oma identiteedist (kontaktandmed), kasutuseesmärgist ja andmesubjekti individuaalseid õiguseid puudutavale taotlusele vastamise korrast APPI artiklite 28, 29 ja 30 alusel.

(63) Kuna lisaeeskirjade alusel käsitatakse Euroopa Liidust edastatud isikuandmeid „säilitatavate isikuandemetena“ nende säilitamisperioodist sõltumata (välja arvatud juhul, kui need on hõlmatud eranditega), kehtivad nende suhtes mõlema ülalnimetatud sätte alusel alati läbipaistvusnõuded.

(64) Nii artikli 18 nõuete puhul kui ka kohustuse puhul teavitada kasutuseesmärgist APPI artikli 27 alusel kehtivad samad erandid, mis põhinevad peamiselt avaliku huvi kaalutlustel ning andmesubjekti, kolmandate isikute ja vastutava töötleja õiguste ja huvide kaitsel ([37]). Isikuteabe kaitse komisjoni suunistes esitatud tõlgenduse kohaselt kohaldatakse neid erandeid väga konkreetsetes olukordades, näiteks juhul, kui kasutuseesmärki puudutav teave võib seada ohtu ettevõtja poolt teatavate huvide kaitsmiseks võetavad õiguspärased meetmed (näiteks pettusevastane võitlus, tööstusspionaaž, sabotaaž).

2.3.7. *Isikuandmete eriliigid*

(65) „Eriliiki“ andmete töötlemisel tuleks kohaldada konkreetseid kaitsemeetmeid.

(66) „Eritähelepanu nõudev isikuteave“ on määratletud APPI artikli 2 lõikes 3. See säte viitab „isikuteabele, mis hõlmab volitaja rassi, usutunnistust, sotsiaalset seisundit, haiguslugusid, karistusregistri andmeid, asjaolu, et ta on olnud kuriteos kannatanu, või muid kirjeldusi jne, mis on valitsuse määrusega ette nähtud kui kirjeldused, mille käitlemine nõuab erihoolt, et ära hoida volitaja ebaõiglane diskrimineerimine, tema kahjustamine või muud tema jaoks ebasoodsad asjaolud“. Need liigid vastavad suurel määral määruse (EL) 2016/679 artiklites 9 ja 10 esitatud tundlike andmete loetelule. Eelkõige vastab termin „haiguslood“ terviseandmetele ning väljend „karistusregistri andmeid ja asjaolu, et ta on olnud kuriteos kannatanu“ on sisuliselt sama nagu määruse (EL) 2016/679 artiklis 10 viidatud liigid. APPI artikli 2 lõikes 3 viidatud liike on täiendavalt tõlgendatud valitsuse määruses ja isikuteabe kaitse komisjoni suunistes. Isikuteabe kaitse komisjoni suuniste jao 2.3 punkti 8 kohaselt tõlgendatakse valitsuse määruse artikli 2 punktides ii ja iii täpsustatud „haiguslugusid“ geneetilisi ja biomeetrilisi andmeid hõlmavana. Samuti ehkki loetelu ei sisalda termineid „etniline päritolu“ või „poliitilised vaated“, sisaldab see viiteid „rassile“ ja „usutunnistusele“. Nagu on selgitatud isikuteabe kaitse komisjoni suuniste jao 2.3 punktides 1 ja 2, hõlmab viide „rassile“ „etnilisi sidemeid või sidemeid teatava maailmajaoga“ ning terminit „usutunnistus“ mõistetakse nii usulisi kui ka poliitilisi vaateid hõlmavana.

(67) Nagu on selge sätte sõnastusest, ei ole see ammendav loetelu ning sellele võib lisada muid andmete liike määral, mil nende töötlemine tekitab „volitaja ebaõiglase diskrimineerimise, tema kahjustamise või muude tema jaoks ebasoodsate asjaolude“ ohu.

(68) Ehkki „tundlike“ andmete mõiste on iseenesest sotsiaalne mõiste, sest see põhineb asjaomase ühiskonna kultuurilistel ja õiguslikel tavadel, moraalsetel kaalutlustel, poliitilistel valikutel jne, võttes arvesse tundlikele andmetele piisavate kaitsemeetmete tagamise tähtsust, kui neid andmeid edastatakse Jaapanis asuvatele ettevõtjatele, on komisjon leidnud, et Jaapani õiguse alusel „eritähelepanu nõudvale isikuteabele“ tagatud erikaitse laieneb kõikidele määruse (EL) 2016/679 kohastele „tundlikele andmetele“. Sel eesmärgil on lisaeeskirjaga 1 ette nähtud, et Euroopa Liidust edastatud andmed, mis puudutavad üksikisiku seksuaalelu, seksuaalset sättumust või ametiühingutes osalust, töötleb isikuteavet käitlev ettevõtja „samal viisil nagu eritähelepanu nõudvat isikuteavet [APPI] artikli 2 lõike 3 tähenduses“.

([37]) Need on i) juhtumid, mille puhul esineb võimalus, et andmesubjekti teavitamine kasutuseesmärgist või kasutuseesmärgi avalikustamine „kahjustaks volitaja või kolmanda isiku elu, tervist, varalist seisundit või muid õiguseid ja huve“ või „[…] isikuteavet käitleva ettevõtja õiguseid või õigustatud huve“; ii) juhtumid, mil „on vaja teha koostööd seoses keskvalitsuse organisatsiooni või kohaliku omavalitsusega“ nende seadusest tulenevate ülesannete täitmisel ning kui see teavitamine või avaldamine takistaks nende „küsimustega“ tegelemist; iii) juhtumid, mille puhul on kasutuseesmärk selge, tuginedes olukorrale, kus andmed on saadud.

(69) Mis puutub täiendavatesse sisulistesse kaitsemeetmetesse, mida kohaldatakse eritähelepanu nõudva isikuteabe suhtes, ei ole kooskõlas APPI artikli 17 lõikega 2 isikuteavet käitlevate ettevõtjatel lubatud omandada seda liiki andmeid ilma asjaomase isiku eelneva nõusolekuta, v.a üksikud erandid ([38]). Peale selle on välistatud seda liiki isikuteabe avaldamine kolmandale isikule APPI artikli 23 lõikes 2 sätestatud menetluse (andmete kolmandatele isikutele ilma asjaomase isiku eelneva nõusolekuta edastamise lubamine) alusel.

2.3.8. *Vastutus*

(70) Vastutuse põhimõtte kohaselt peavad andmeid töötlevad üksused kehtestama asjakohased tehnilised ja korralduslikud meetmed, et täita tõhusalt oma andmekaitse kohustusi ja suuta tõendada sellist vastavust, eriti pädevale järelevalveasutusele.

(71) Nagu on märgitud joonealune märkuses 34 (põhjendus 49), peavad isikuteavet käitlevad ettevõtjad APPI artikli 26 lõike 1 alusel kontrollima neile isikuandmeid esitava kolmanda isiku identiteeti ja „asjaolusid", mille alusel kolmas isik on need andmed omandanud (käesoleva otsusega hõlmatud isikuandmete korral hõlmavad need asjaolud kooskõlas APPI ja lisaeeskirjaga 3 asjaolu, et andmed on pärit Euroopa Liidust, samuti andmete algset edastamise eesmärki). Muu hulgas on selle meetme eesmärk tagada andmetöötluse õiguspärasus kogu isikuteavet käitlevate ettevõtjate isikuandmete töötlemise ahelas. Peale selle on APPI artikli 26 lõikes 3 nõutud, et isikuteavet käitlevad ettevõtjad peaksid registrit, milles kajastatakse saamise kuupäev ja kolmandalt isikult lõike 1 alusel saadud (kohustuslik) teave, samuti asjaomase üksikisiku (andmesubjekti) nimi, töödeldavate andmete liigid ja vajaduse korral asjaolu, et andmesubjekt on andnud nõusoleku oma isikuandmete jagamiseks. Nagu on märgitud isikuteabe kaitse komisjoni eeskirjade artiklis 18, tuleb neid registreid hoida olenevalt asjaoludest alles vähemalt üks kuni kolm aastat. Isikuteabe kaitse komisjon võib oma ülesannete täitmisel nõuda selliste registrite esitamist ([39]).

(72) Isikuteavet käitlevad ettevõtjad peavad kiiresti ja asjakohaselt lahendama asjaomaste isikute kaebused nende isikuteabe töötlemise kohta. Kaebuste lahendamise hõlbustamiseks kehtestavad nad „[selle] eesmärgi saavutamiseks vajaliku süsteemi", mis tähendab, et nad peavad kehtestama asjakohased menetlused oma organisatsioonis (näiteks määrama vastutusalad või nägema ette kontaktisiku).

(73) Lisaks luuakse APPIga raamistik, mille alusel saavad valdkondlikud organisatsioonid osaleda kõrge vastavustaseme tagamisel (vt IV peatüki 4. jagu). Selliste spetsiaalsete isikuteabe kaitse organisatsioonide ([40]) roll on tugevdada isikuteabe kaitset, toetades selleks ettevõtjaid oma ekspertteadmistega, aga ka aidata rakendada kaitsemeetmeid, eelkõige lahendades üksikisikute kaebuseid ja aidates lahendada seotud konflikte. Nad võivad sel eesmärgil nõuda, et isikuteavet käitlevad ettevõtjad võtavad vajaduse korral vajalikke meetmeid ([41]). Peale selle teavitavad isikuteavet käitlevad ettevõtjad andmetega seotud rikkumiste või muude turvaintsidentide korral isikuteabe kaitse komisjoni ja andmesubjekti (või üldsust) ning võtavad vajalikke meetmeid, sealhulgas meetmeid, et vähendada kahju ja ära hoida sarnaste intsidentide kordumine ([42]). Ehkki need on vabatahtlikud skeemid, loetles isikuteabe kaitse komisjon 10. augustil 2017. aastal 44 organisatsiooni, millest suurim on Jaapani infotöötlus- ja -arenduskeskus (JIPDEC),

([38]) Erandid on järgmised: i) „õigusnormidel põhinevad juhtumid"; ii) „juhtumid, mil esineb vajadus kaitsta isiku elu, tervist või varalist seisundit ning on keeruline saada volitaja nõusolekut"; iii) „juhtumid, mil esineb erivajadus parandada avalikku hügieeni või edendada laste tervist ning keeruline saada volitaja nõusolekut"; iv) „juhtumid, mil esineb vajadus teha koostööd seoses keskvalitsuse organisatsiooniga või kohaliku omavalitsusega või isikuga, kellele nad on andnud ülesande tegeleda õigusnormides ette nähtud küsimustega, ning on võimalus, et volitaja nõusoleku saamine takistaks nimetatud küsimustega tegelemist". ning v) juhtumid, mil nimetatud eritähelepanu nõudva isikuteabe avaldab üldsusele andmesubjekt, valitsusasutus, kohalik omavalitsus, artikli 76 lõike 1 kohasesse kategooriasse kuuluv isik või muu isikuteabe kaitse komisjoni eeskirjades ette nähtud isik. Lisakategooria hõlmab „muid juhtumeid, mis on valitsuse määruse kohaselt samaväärsed juhtumitega, mis on sätestatud igas eelnevas punktis" ning hõlmab kehtiva valitsuse määruse alusel eelkõige isiku selgesti nähtavaid omadusi (nt nähtav tervislik seisund), kui tundlikud andmed on saadud (tahtmatult) andmesubjekti visuaalse vaatluse, filmimise või pildistamise teel, näiteks videovalve kaamerate abil.

([39]) APPI artikli 40 lõike 1 alusel võib isikuteabe kaitse komisjon APPI asjakohaste sätete rakendamiseks vajalikul määral nõuda, et isikuteavet käitlev ettevõtja esitaks vajaliku teabe või materjali seoses isikuteabe käitlemisega.

([40]) APPIs on muu hulgas sätestatud selliste organisatsioonide akrediteerimise eeskirjad; vt APPI artiklid 47–50.

([41]) APPI artikkel 52.

([42]) Isikuteabe kaitse komisjoni teatis nr 1/2017 „Meetmete kohta, mida tuleb võtta sellistel juhtudel nagu isikuandmetega seotud rikkumine või muud intsidendid".

millel ainuüksi on 15 436 osalevat ettevõtjat ([43]). Akrediteeritud skeemide seas võib nimetada valdkondlikke ühinguid, nagu Jaapani väärtpaberimaaklerite ühing, Jaapani sõidukoolide ühing või abielusõlmijate ühing ([44]).

(74) Akrediteeritud isikuteabe kaitse organisatsioonid esitavad oma tegevuse kohta aastaaruandeid. Kooskõlas isikuteabe kaitse komisjoni avaldatud dokumendiga „APPI rakendamise seisu ülevaade 2015. eelarveaastal" said akrediteeritud isikuteabe kaitse organisatsioonid kokku 442 kaebust, nõudsid oma pädevuse alla kuuluvatelt ettevõtjatelt selgitusi 123 korral, nõudsid nendelt ettevõtjatelt dokumente 41 korral, andsid 181 juhist ja esitasid kaks soovitust ([45]).

2.3.9. *Andmete edasisaatmise piirangud*

(75) Euroopa Liidust Jaapanis asuvatele ettevõtjatele edastatavatele isikuandmetele pakutavat kaitsetaset ei tohi vähendada selliste andmete edasisaatmine kolmandasse riiki Jaapanist väljaspool. Selline „edasisaatmine", mis tähendab Jaapani ettevõtja seisukohast rahvusvahelist edastamist Jaapanist, tuleks lubada üksnes juhul, kui järgmine saaja väljapool Jaapanit järgib ise eeskirju, mis tagavad sarnase kaitse, nagu on tagatud Jaapani õiguskorraga.

(76) Esmane kaitse on ette nähtud APPI artikliga 24, mis üldiselt keelab isikuandmete edastamise kolmandale isikule väljaspool Jaapani territooriumit ilma asjaomase isiku eelneva nõusolekuta. Lisaeeskirjaga 4 tagatakse, et andmete edastamisel Euroopa Liidust on see nõusolek eriti teadlik, sest see nõuab, et asjaomastele üksikisikutele „antakse teavet asjaolude kohta, mis puudutavad edastamist ja mille alusel saab volitaja teha otsuse oma nõusoleku kohta". Sellest lähtudes teavitatakse andmesubjekti asjaolust, et andmed edastatakse välisriiki (mis ei kuulu APPI kohaldamisalasse), ja nimetatakse konkreetne sihtriik. See võimaldab isikul hinnata edastamisega seotud riski eraelu puutumatusele. Nagu saab järeldada APPI artiklist 23 (vt põhjendus 47), peaks volitajale esitatav teave hõlmama kõnealuse artikli lõike 2 kohaseid kohustuslikke andmeid, nimelt kolmandale isikule edastatud isikuandmete liike ja avaldamise meetodit.

(77) APPI artiklis 24, mida kohaldatakse koos isikuteabe kaitse komisjoni eeskirjade artikliga 11-2, on sätestatud sellele nõusolekupõhisele eeskirjale mitu erandit. Peale selle kohaldatakse artikli 24 alusel samu erandeid, mis on kohaldatavad APPI artikli 23 lõike 1 alusel, ka rahvusvahelise andmete edastamise suhtes ([46]).

(78) Et tagada selle otsuse alusel jätkuv kaitse Euroopa Liidust Jaapanisse edastatavate isikuandmete korral, tugevdatakse lisaeeskirjaga 4 kaitset selliste andmete edasisaatmisel isikuteavet käitlevate ettevõtjate poolt kolmandas riigis asuvale saajale. Kaitset tugevdatakse seeläbi, et piiritletakse ja raamistatakse rahvusvahelise edastamise alused, mida isikuteavet käitlev ettevõtja võib nõusoleku asemel kasutada. Täpsemalt ja ilma et see piiraks APPI artikli 23 lõikes 1 sätestatud erandite kohaldamist, tähendab see seda, et selle otsuse alusel edastatavaid isikuandmeid võib ilma nõusolekuta (edasi) saata üksnes kahel juhul: i) kui andmed saadetakse kolmandasse riiki, mida isikuteabe kaitse komisjon on APPI artikli 24 alusel tunnustanud kui riiki, mis tagab Jaapani tagatava kaitsetasemega samaväärse kaitsetaseme ([47]); või ii) kui isikuteavet käitlev ettevõtja või kolmandast isikust saaja on koos rakendanud meetmeid, mis tagavad APPIga (koostoimes lisaeeskirjadega) samaväärse kaitsetaseme kas lepingu, muude siduvate kokkulepete või ettevõtjate kontsernis sõlmitud siduvate kokkulepete kaudu. Teine kategooria vastab instrumentidele, mida kasutatakse määruse (EL) 2016/679 alusel asjakohaste kaitsemeetmete tagamiseks (eelkõige lepingu tüüptingimused ja siduvad kontsernisisesed eeskirjad). Nagu isikuteabe kaitse komisjon on kinnitanud, kohaldatakse ka sellistel juhtudel kolmandale isikule edastamise suhtes APPI raames isikuandmete jagamisel kehtivaid üldeeskirju

([43]) JIPDECi PrivacyMarki veebisaidil avaldatud näitajate kohaselt, 2. oktoober 2017.
([44]) Isikuteabe kaitse komisjoni akrediteeritud isikuteabe kaitse organisatsioonide loetelu, kättesaadav internetis aadressil: https://www.ppc.go.jp/personal/nintei/list/ või https://www.ppc.go.jp/files/pdf/nintei_list.pdf
([45]) Isikuteabe kaitse komisjon, APPI rakendamise seisu ülevaade 2015. eelarveaastal (oktoober 2016), kättesaadav (üksnes jaapani keeles) internetis aadressil: https://www.ppc.go.jp/files/pdf/personal_sekougaiyou_27ppc.pdf
([46]) Vt joonealune märkus 32.
([47]) Isikuteabe kaitse komisjoni eeskirjade artikli 11 kohaselt eeldab see nii seda, et APPIga samaväärsete sisuliste nõuete üle teeb tõhusat järelevalvet sõltumatu õiguskaitseasutus, kui ka seda, et kolmandas riigis on tagatud asjaomaste eeskirjade rakendamine.

(st artikli 23 lõike 1 kohase nõusoleku saamise nõue või alternatiivina APPI artikli 23 lõike 2 kohase loobumisklausli kasutamise võimalus). Kui andmesubjekt ei ole nõusoleku küsimiseks või APPI artikli 23 lõike 2 kohaselt nõutava eelteabe esitamiseks kättesaadav, ei ole edastamine lubatud.

(79) Seega välja arvatud juhtudel, mil isikuteabe kaitse komisjon on leidnud, et kõnealune kolmas riik tagab APPI garanteeritava kaitsetasemega samaväärse kaitsetaseme ([48]), välistatakse lisaeeskirjas 4 sätestatud nõuetega selliste edastamisinstrumentide kasutamine, millega ei looda siduvat suhet Jaapani andmeeksportija ja kolmanda riigi andmeimportija vahel ning mis ei taga nõutavat kaitsetaset. Sellega on tegu näiteks APECi piiriüleste privaatsuseeskirjade (CBPR) süsteemi puhul, mille osalisriik Jaapan on ([49]), sest selle süsteemi alusel ei tulene kaitse eksportija ja importija suhtes siduvast kokkuleppest nende kahepoolse suhte kontekstis ning see tagab selgelt madalama taseme, kui on garanteeritud APPIt ja lisaeeskirju koos kohaldades ([50]).

(80) Lisaks tuleneb täiendav kaitsemeede (edasi)saatmise korral APPI artiklitest 20 ja 22. Nendes on sätestatud, et kui kolmanda riigi ettevõtja (andmete importija) tegutseb isikuteavet käitleva ettevõtja (andmete eksportija) nimel, peab isikuteavet käitlev ettevõtja tagama kolmanda riigi ettevõtja üle järelevalve seoses andmetöötluse turvalisusega.

2.3.10. *Üksikisiku õigused*

(81) Nagu ELi andmekaitseõiguses, antakse APPIga üksikisikutele mitu täitmisele pööratavat õigust. See hõlmab juurdepääsuõigust („avaldamine“), andmete parandamise ja kustutamise õigust ning õigust esitada vastuväiteid („kasutamise lõpetamine“).

(82) Esiteks on andmesubjektil kooskõlas APPI artikli 28 lõigetega 1 ja 2 õigus taotleda isikuteavet käitlevalt ettevõtjalt „selliste säilitatavate isikuandmete avaldamist, millega saab teda tuvastada“ ning sellise taotluse saamisel peab isikuteavet käitlev ettevõtja „[…] avaldama säilitatavad isikuandmed“ andmesubjektile. Artiklitel 29 (parandamisõigus) ja 30 (kasutamise lõpetamise taotlemise õigus) on sama struktuur nagu artiklil 28.

(83) Valitsuse määruse artiklis 9 sätestatakse, et isikuteabe avaldamine, nagu on viidatud APPI artikli 28 lõikes 2, toimub kirjalikult, välja arvatud juhul, kui isikuteavet käitlev ettevõtja ja andmesubjekt on teisiti kokku leppinud.

(84) Nende õiguste suhtes kohaldatakse kolme liiki piiranguid, mis on seotud üksikisiku enda või kolmandate isikute õiguste ja huvidega ([51]), isikuteavet käitleva ettevõtja äritegevuse raske riivamisega ([52]) ning juhtumitega, mille puhul avaldamine rikuks muid õigusnorme ([53]). Olukorrad, kus neid piiranguid kohaldatakse, on sarnased määruse (EL) 2016/679 artikli 23 lõike 1 alusel kohaldatavate eranditega, mis võimaldavad piirata üksikisikute õiguseid

([48]) Seni ei ole isikuteabe kaitse komisjon veel APPI artikli 24 alusel vastu võtnud otsuseid, millega tunnistataks kolmanda riigi tagatav kaitsetase Jaapani tagatava kaitsetasemega samaväärseks. Praegu on arutamisel ainult ühe otsuse vastuvõtmine ja see otsus puudutab EMPd. Võimalike muude tulevikus vastu võetavate otsustega seoses jälgib komisjon tähelepanelikult olukorda ja võtab vajaduse korral asjakohaseid meetmeid, millega reageerida võimalikele kaitse jätkumist ohustavatele mõjudele (vt põhjendused 176, 177, 184 ja artikli 3 lõige 1).

([49]) Ehkki APECi CBPRi süsteemi alusel on sertifitseeritud üksnes kaks Jaapani äriühingut (vt https://english.jipdec.or.jp/sp/protection_org/cbpr/list.html). Väljaspool Jaapanit olevatest ettevõtetest on selle süsteemi alusel sertifitseeritud üksnes loetud arv (23) USA äriühinguid (vt https://www.trustarc.com/consumer-resources/trusted-directory/#apec-list).

([50]) Näiteks puudub tundlike andmete määratlus ja erikaitse ning andmete säilitamise piiramise kohustus. Vt ka artikli 29 töörühma arvamus 02/2014, milles käsitletakse ELi liikmesriikide andmekaitseasutustele esitatud siduvate kontsernisiseste eeskirjade ja APECi piiriüleste privaatsuseeskirjade järgimise kinnitamise eest vastutavatele ametitele esitatud piiriüleste privaatsuseeskirjade nõudeid, 6. märts 2014.

([51]) Isikuteabe kaitse komisjoni kohaselt võivad piirangud olla õigustatud üksnes selliste huvide korral, mis „väärivad seaduslikku kaitset“. Seda tuleb hinnata igal üksikjuhul eraldi, „võttes arvesse kuivõrd riivatakse põhiõigust eraelu puutumatusele, kaasa arvatud andmekaitsele, nagu on tunnustatud põhiseaduses ja kohtupretsedentides.“ Kaitstud huvid võivad hõlmata näiteks äri- või muid kaubanduslikke saladusi.

([52]) Mõistet „takistab tõsiselt ettevõtja äritegevuse nõuetekohast elluviimist“ on illustreeritud isikuteabe kaitse komisjoni suunistes mitme näitega, milleks on muu hulgas korduvad ja identsed keerulised taotlused, mille esitab sama isik, kui need taotlused tekitavad ettevõtjale märkimisväärse koormuse, mis vähendab tema suutlikkust teistele taotlustele vastata (isikuteabe kaitse komisjoni suunised (üldeeskirjade väljaanne), lk 62). Üldisemalt on isikuteabe kaitse komisjon kinnitanud, et see kategooria piirdub erandlike juhtumitega, mille puhul pole tegemist pelgalt ebamugavustega. Eelkõige ei saa isikuteavet käitlev ettevõtja avaldamisest keelduda vaid seetõttu, et on küsitud suurt hulka andmeid.

([53]) Nagu isikuteabe kaitse komisjon on kinnitanud, tuleb sellistes seadustes austada põhiseadusega tagatud õigust eraelu puutumatusele ja seega peab neis „kajastuma piirangu vajalikkus ja kohasus.“

põhjustel, mis on seotud „andmesubjekti kaitsega või teiste isikute õiguste ja vabaduste kaitsega“ või „muude üldist avalikku huvi pakkuvate oluliste eesmärkidega“. Ehkki selliste juhtude kategooria, mille puhul avaldamine rikuks „muid õigusnorme“, võib näida lai, peavad sellega seotud piiranguid sätestavad õigusnormid olema vastavuses põhiseadusliku õigusega privaatsusele ning nendega võidakse kehtestada piiranguid üksnes määral, mil selle õiguse kasutamine „riivaks üldsuse heaolu“ ([54]). See nõuab asjaomaste huvide tasakaalustamist.

(85) APPI artikli 28 lõikes 3 on sätestatud, et kui nõutavaid andmeid ei eksisteeri või asjaomane isikuteavet käitlev ettevõtja otsustab mitte anda juurdepääsu säilitatavatele andmetele, tuleb üksikisikut viivitamata teavitada.

(86) Teiseks on APPI artikli 29 lõigete 1 ja 2 alusel andmesubjektil õigus taotleda oma säilitatavate isikuandmete parandamist, täiendamist või kustutamist juhul, kui andmed on ebatäpsed. Sellise taotluse saamisel viib isikuteavet käitlev ettevõtja „[…] läbi vajaliku uurimise“ ning teeb selle uurimise tulemuste alusel „säilitatavate andmete sisus parandusi jne“.

(87) Kolmandaks on APPI artikli 30 lõigete 1 ja 2 alusel andmesubjektil õigus taotleda, et isikuteavet käitlev ettevõtja lõpetaks isikuteabe käitlemise või kustutaks selle teabe, kui seda käideldakse artiklit 16 (eesmärgi piirangu kohta) rikkudes või see on saadud mittenõuetekohaselt APPI artiklit 17 (pettuse teel omandamise, muude mittenõuetekohaste vahendite või nõusolekuta tundlike andmete edastamise kohta) rikkudes. Samamoodi on isikul APPI artikli 30 lõigete 3 ja 4 alusel õigus nõuda, et isikuteavet käitlev ettevõtja lõpetab teabe edastamise kolmandale isikule, kui see rikub APPI artikli 23 lõiget 1 või artiklit 24 (kolmandale isikule andmete edastamise, sealhulgas rahvusvahelise edastamise kohta).

(88) Kui taotlus on põhjendatud, lõpetab isikuteavet käitlev ettevõtja viivitamata andmete kasutamise või kolmandale isikule esitamise määral, mil see on vajalik rikkumise kõrvaldamiseks, või kui see juhtum on hõlmatud erandiga (eelkõige juhul, kui kasutamise peatamine põhjustaks eriti suuri kulusid), ([55]) rakendab ta vajalikke alternatiivseid meetmeid, et kaitsta asjaomase üksikisiku õiguseid ja huve.

(89) Erinevalt liidu õigusest ei sisalda APPI ja asjaomased eeskirjad õiguslikke erisätteid otseturunduseesmärgil töötlemise vaidlustamise võimaluse kohta. Siiski toimub selline töötlemine käesoleva otsuse raames alati eelnevalt Euroopa Liidus kogutud isikuandmete edastamise kontekstis. Määruse (EL) 2016/679 artikli 21 lõike 2 alusel on andmesubjektil alati võimalus esitada vastuväide andmete edastamisele nende otseturunduse eesmärgil töötlemiseks. Nagu on selgitatud põhjenduses 43, peab isikuteavet käitlev ettevõtja lisaeeskirja 3 alusel töötlema otsuse alusel saadud andmeid samal eesmärgil, milleks andmed on Euroopa Liidust edastatud, välja arvatud juhul, kui andmesubjekt nõustub kasutuseesmärgi muutmisega. Seega kui andmed on edastatud muul eesmärgil kui otseturundus, ei lubata isikuteavet käitleval ettevõtjal Jaapanis töödelda andmeid otseturunduse eesmärgil, kui selleks ei ole ELi andmesubjekti nõusolekut.

(90) Kõikidel APPI artiklites 28 ja 29 viidatud juhtudel peab isikuteavet käitlev ettevõtja teavitama üksikisikut tema taotluse tulemusest viivitamata ning selgitama võimalikku (osalist) keeldumist artiklites 27–30 (APPI artikkel 31) sätestatud seadusjärgsete erandite alusel.

([54]) Põhiseaduse artiklit 13 on ülemkohus tõlgendanud selliselt, et see tagab õiguse privaatsusele (vt põhjendused 7 ja 8). Kuigi seda õigust võib piirata juhtudel, kui see „kahjustab üldsuse heaolu“, selgitas ülemkohus 6. märtsi 2008. aasta otsuses (vt põhjendus 8), et igasugune piirang (või kõnealusel juhul avaliku sektori asutusel isikuandmete kogumise ja töötlemise lubamine) peab olema tasakaalustatud õigusega eraelu puutumatusele, võttes arvesse selliseid tegureid nagu asjaomaste andmete laad, nende andmete töötlemisest üksikisikutele tulenevad riskid, kohaldatavad kaitsemeetmed ja töötlemisest tulenevad avalikud hüved. See on väga sarnane andmekaitseõiguste ja kaitsemeetmete piiramise lubamisel ELi õiguses ette nähtud tasakaalustamisele, mis põhineb vajalikkuse ja proportsionaalsuse põhimõtetel.

([55]) Neid erandite kohta on lisaselgitusi esitatud väljaandes: professor Katsuya Uga, Article by Article Commentary of the revised Act on the Protection of Personal Information, 2015, lk 217. „Suuri kulusid“ tekitava taotluse näide on juhtum, kui üksnes mõnda mahukas nimekirjas (nt kataloogis) olevat nime töödeldakse eesmärgi piirangu põhimõtet rikkudes ja kataloog on juba müügil ning selle eksemplaride turult tagasivõtmine ja nende uutega asendamine oleks väga kulukas. Sama näite puhul on juhul, kui kataloogi eksemplare on müüdud juba paljudele inimestele ning on võimatu neid kõiki kokku koguda, väga „keeruline nende kasutamine lõpetada“. Nende stsenaariumide puhul võivad „vajalikud alternatiivsed meetmed“ tähendada näiteks parandusteate avaldamist või levitamist. See tegevus ei välista muid (õigus)kaitse vorme nii privaatsusõiguste rikkumise, avaldamisega tekitatud mainekahju (laimu) või muude huvide rikkumise puhul.

(91) Seoses taotluse esitamise tingimustega võimaldab APPI artikkel 32 (koos valitsuse määrusega) isikuteavet käitleval ettevõtjal määrata kindlaks mõistlik menetlus, sealhulgas seoses teabega, mida on vaja säilitatavate isikuandmete kindlakstegemiseks. Kõnealuse artikli lõike 4 kohaselt ei tohi isikuteavet käitlevad ettevõtjad siiski kehtestada „volitajale ülemäärast koormust". Teatavatel juhtudel võivad isikuteavet käitlevad ettevõtjad kehtestada ka tasusid, eeldusel et nende summa jääb „vahemikku, mida peetakse tegelikke kulusid arvesse võttes mõistlikuks" (APPI artikkel 33).

(92) Lisaks võib üksikisik esitada vastuväite oma isikuteabe kolmandale isikule esitamisele APPI artikli 23 lõike 2 alusel või keelduda andmast nõusolekut artikli 23 lõike 1 alusel (seega hoides ära avaldamist juhul, kui ükski muu õiguslik alus ei ole kättesaadav). Samamoodi võib üksikisik peatada isikuandmete töötlemise muul eesmärgil, keeldudes andmast nõusolekut APPI artikli 16 lõike 1 alusel.

(93) Erinevalt ELi õigusest ei sisalda APPI ja asjaomased eeskirjad üldsätteid selliste otsuste kohta, mis mõjutavad andmesubjekti ja põhinevad isikuandmete automatiseeritud töötlemisel. Seda küsimust on siiski reguleeritud teatavate Jaapanis kohaldatavate valdkondlike eeskirjadega, mis on seda liiki töötlemise jaoks eriti olulised. See hõlmab sektoreid, kus äriühingud kõige suurema tõenäosusega tuginevad isikuandmete automatiseeritud töötlemisele, et teha üksikisikuid mõjutavaid otsuseid (nt finantssektor). Näiteks dokumendiga „Suuremate pankade põhjalikud järelevalvesuunised" (muudetud juunis 2017) nõutakse, et asjaomasele üksikisikule esitatakse konkreetsed selgitused põhjuste kohta, miks tema laenulepingu sõlmimise taotlus on tagasi lükatud. Nimetatud eeskirjad tagavad seega kaitse nendel tõenäoliselt üsna piiratud arvul juhtudel, kui automatiseeritud otsused on teeb Jaapani „importiv" ettevõtja ise (ja mitte „eksportiv" ELi vastutav töötleja).

(94) Igal juhul teeb Euroopa Liidus kogutud isikuandmete puhul kõik automatiseeritud töötlemisel põhinevad otsused tavaliselt liidu vastutav töötleja (kellel on otsene suhe asjaomase andmesubjektiga) ja nende suhtes kohaldatakse seega määrust (EL) 2016/679 ([56]). See kehtib ka edastamisolukordades, mille puhul töötleja on välisriigi (nt Jaapani) ettevõtja, kes esindab ELi vastutavat töötlejat (volitatud töötlejana) (või ELi volitatud töötleja nimel tegutseva alamtöötlejana, kes on saanud andmed need kogunud ELi vastutavalt töötlejalt) ja teeb selle põhjal otsuse. Seepärast tõenäoliselt ei mõjuta automatiseeritud otsuste tegemise konkreetsete eeskirjade puudumine APPIs käesoleva otsuse alusel edastatud isikuandmete kaitsetaset.

2.4. **Järelevalve ja täitmise tagamine**

2.4.1. *Sõltumatu järelevalve*

(95) Et tagada andmekaitse piisav tase ka praktikas, peaks olema loodud sõltumatu järelevalveasutus, millele on antud volitused jälgida andmekaitse-eeskirjadele vastavust ja tagada nende täitmine. See asutus peaks tegutsema oma ülesandeid täites ja volitusi kasutades täiesti sõltumatult ja erapooletult.

(96) Jaapanis teeb APPI üle järelevalvet ja tagab APPI täitmise isikuteabe kaitse komisjon. See koosneb esimehest ja kaheksast liikmest, kelle on nimetanud peaminister parlamendi (*Diet*) mõlema koja nõusolekul. Esimehe ja iga liikme ametiaeg on viis aastat uuesti ametisse nimetamise võimalusega (APPI artikkel 64). Liikmed võib ametist vabastada üksnes põhjendatud juhul piiratud arvul erandlikel asjaoludel ([57]) ja nad ei või aktiivselt osaleda poliitilises tegevuses. APPI kohaselt peavad täistööajaga volinikud lisaks hoiduma mis tahes muust tasustatavast tegevusest või äritegevusest. Samuti kohaldatakse kõikide volinike suhtes sise-eeskirju, millega neil keelatakse võimaliku huvide konflikti korral aruteludes osaleda. Isikuteabe kaitse komisjoni abistab sekretariaat, mida juhib peasekretär ja mis on asutatud isikuteabe kaitse komisjonile antud ülesannete täitmise eesmärgil (APPI artikkel 70). Nii komisjoni liikmed kui ka kõik sekretariaadi ametnikud peavad järgima rangeid salajasuse eeskirju (APPI artiklid 72 ja 82).

([56]) Seevastu erandjuhul, mil Jaapani ettevõtjal on otsene suhe ELi andmesubjektiga, tuleneb see tavaliselt sellest, et ta on ise pöördunud Euroopa Liidus asuva üksikisiku poole, pakkudes talle kaupu ja teenuseid või jälgides tema käitumist. Selle stsenaariumi puhul kuulub Jaapani ettevõtja ise määruse (EL) 2016/679 (artikli 3 lõike 2) kohaldamisalasse ja peab seega järgima otse ELi andmekaitseõigust.

([57]) APPI artikli 65 kohaselt on vastava liikme ametist vabastamine võimalik üksnes ühel järgmistest põhjustest: i) pankrotimenetluse algatamine; ii) süüdimõistmine APPI või numbrite kasutamise seaduse rikkumise eest; iii) töökohustuseta vanglakaristuse või veelgi rangema karistuse määramine; iv) suutmatus täita ülesandeid tingituna vaimsest või füüsilisest häirest või väärkäitumisest.

(97) Täiesti sõltumatult tegutseva ([58]) isikuteabe kaitse komisjoni volitused on sätestatud peamiselt APPI artiklites 40, 41 ja 42. Artikli 40 kohaselt võib isikuteabe kaitse komisjon nõuda isikuteavet käitlevatelt ettevõtjatelt töötlemistoimingute kohta teabe või dokumentide esitamist ning teha samas ka nii kohapealseid kontrolle kui ka raamatupidamise ja muude dokumentide kontrolli. APPI täitmise tagamiseks vajalikul määral võib isikuteabe kaitse komisjon anda isikuteavet käitlevatele ettevõtjatele ka suuniseid või nõuandeid isikuteabe käitlemise kohta. Isikuteabe kaitse komisjon on seda õigust juba APPI artikli 41 kohaselt kasutanud ja esitanud Cambridge Analytica paljastuste järel Facebookile suunised.

(98) Veelgi olulisem on see, et isikuteabe kaitse komisjonil on õigus – tegutsedes kaebuse alusel või omal algatusel – anda soovitusi ja korraldusi, et tagada APPI ja muude siduvate eeskirjade (sealhulgas lisaeeskirjade) täitmine eri juhtumite korral. Need õigused on sätestatud APPI artiklis 42. Ehkki selle artikli lõigetes 1 ja 2 on sätestatud kaheetapiline mehhanism, mille alusel isikuteabe kaitse komisjon võib välja anda määruse (üksnes) siis, kui sellele on eelnenud soovitus, on lõike 3 kohaselt lubatud kiireloomulistel juhtudel võtta korraldus vastu kohe.

(99) Ehkki kõik APPI IV peatüki 1. jao sätted ei ole artikli 42 lõikes 1 loetletud – mis määrab kindlaks ka artikli 42 lõike 2 kohaldamisala – võib seda selgitada asjaoluga, et teatavad sätted neist ei puuduta isikuteavet käitlevate ettevõtjate kohustusi ([59]) ning et kõiki vajalikke kaitsemeetmeid juba pakutakse teiste sätetega, mida ei ole selles loetelus. Näiteks ehkki artiklit 15 (millega nõutakse, et isikuteavet käitlev ettevõtja kehtestab kasutuseesmärgi ja töötleb isikuteavet üksnes selle ulatuses) ei mainita, võib selle nõude järgimata jätmine olla aluseks soovitusele, mis põhineb artikli 16 lõike 1 rikkumisel (millega keelatakse isikuteavet käitleval ettevõtjal isikuteabe töötlemine suuremas ulatuses, kui on vajalik kasutuseesmärgi saavutamiseks, välja arvatud juhul, kui ta saab andmesubjekti nõusoleku) ([60]). Teine säte, mida ei ole artikli 42 lõikes 1 loetletud, on APPI artikkel 19 (andmete täpsuse ja säilitamise kohta). Kui seda sätet ei järgita, saab tagada selle sätte täitmise kas artikli 16 lõike 1 rikkumisena või artikli 29 lõike 2 rikkumisele tuginedes, kui asjaomane isik palub vigased või ülemäärased andmed parandada või kustutada ning isikuteavet käitlev ettevõtja keeldub seda taotlust rahuldamast. Mis puutub andmesubjekti õigustesse kooskõlas artikli 28 lõikega 1, artikli 29 lõikega 1 ja artikli 30 lõikega 1, tagatakse isikuteabe kaitse komisjoni tehtav järelevalve, andes talle täitmise tagamise volitused seoses isikuteavet käitleva ettevõtja vastavate kohustustega.

(100) APPI artikli 42 lõike 1 alusel võib isikuteabe kaitse komisjon, kui ta tuvastab, et esineb „vajadus kaitsta üksikisiku õiguseid ja huve juhtudel, mil [isikuteavet käitlev ettevõtja] on rikkunud“ konkreetseid APPI sätteid, anda soovituse „peatada rikkumine või võtta muid vajalikke meetmeid rikkumise parandamiseks“. See soovitus ei ole siduv, vaid võimaldab APPI artikli 42 lõike 2 alusel välja anda siduva määruse. Kui soovitus ei põhine „õiguspärastel alustel“ ja isikuteabe kaitse komisjon „tunnistab, et üksikisiku õiguste ja huvide tõsine rikkumine on vältimatu“, võib ta lasta isikuteavet käitleval ettevõtjal võtta meetmeid kooskõlas soovitusega.

(101) Lisaeeskirjades on isikuteabe kaitse komisjoni täitmise tagamise volitusi täpsustatud ja tugevdatud. Täpsemalt juhtudel, mis hõlmavad Euroopa Liidust imporditud andmeid, käsitab isikuteabe kaitse komisjon juhtumit, mil isikuteavet käitlev ettevõtja ei ole võtnud meetmeid kooskõlas soovitusega, mis on antud APPIga vastavalt artikli 42 lõikega 1 ilma õiguspärase aluseta, alati vahetult rikkumisega, mille laadiks on üksikisiku õiguste ja huvide raske rikkumine artikli 42 lõike 2 tähenduses, ning seega rikkumisena, mis tagab siduva korralduse väljaandmise. Peale selle aktsepteerib isikuteabe kaitse komisjon soovituse mittejärgimise „õiguspärase alusena“ üksnes „erakorralist laadi sündmust [mis takistab vastavust] väljaspool [isikuteavet käitleva ettevõtja] kontrolli, mida ei saa mõistlikult ette näha (näiteks loodusõnnetused)“ või juhtudel, mil soovitustest tulenev vajadus meetmete võtmiseks „on kadunud, sest [isikuteavet käitlev ettevõtja] on võtnud alternatiivseid meetmeid, mis kõrvaldavad täielikult rikkumise“.

([58]) Vt APPI artikkel 62.

([59]) Näiteks teatavad sätted puudutavad isikuteavet käitleva ettevõtja tegevust, mis on vabatahtlik (APPI artiklid 32 ja 33), või „suurimate jõupingutuste“ tegemise kohustused, mis ei ole iseenesest täitmisele pööratavad (APPI artikkel 31, artikkel 35, artikli 36 lõige 6 ja artikkel 39). Teatavad sätted ei ole mõeldud isikuteavet käitlevale ettevõtjale, vaid teistele osalistele. See on nii näiteks APPI artikli 23 lõike 4, artikli 26 lõike 2 ja artikli 34 korral (seevastu tagatakse APPI artikli 26 lõike 2 täitmine APPI artikli 88 punkti i kohaste kriminaalkaristuste võimalusega).

([60]) Pealegi nagu on selgitatud põhjenduses 48, määrab edastamise korral „kasutuseesmärgi“ kindlaks ELi andmete eksportija, kes peab selles suhtes järgima määruse (EL) 2016/679 artikli 5 lõike 1 punkti b kohaseid kohustusi. See kohustus on täitmisele pööratav pädeva andmekaitseasutuse poolt Euroopa Liidus.

(102) Isikuteabe kaitse komisjoni määrusele mittevastavust käsitatakse APPI artikli 84 alusel kuriteona ning süüdi tunnistatud isikuteavet käitlevat ettevõtjat võidakse karistada kuni kuulekuulise vangistusega, mis sisaldab töökohustust, või kuni 300 000 jeeni suuruse rahatrahviga. Peale selle on APPI artikli 85 punkti i kohaselt isikuteabe kaitse komisjoniga koostööga mittetegemine või tema uurimise takistamine karistatav trahviga kuni 300 000 jeeni. Kõnealuseid kriminaalkaristusi kohaldatakse APPI oluliste rikkumiste eest määratavate võimalike karistuste kõrval (vt põhjendus 108).

2.4.2. *Õiguskaitse*

(103) Piisava kaitse tagamiseks ja eelkõige üksikisiku õiguste täitmise tagamiseks tuleks andmesubjektile tagada tõhus haldus- ja õiguskaitse, sealhulgas kahju hüvitamine.

(104) Enne haldus- või õiguskaitse kasutamist või selle asemel võib üksikisik otsustada esitada kaebuse oma isikuandmete töötlemise kohta vastutavale töötlejale otse. APPI artikli 35 alusel püüavad isikuteavet käitlevad ettevõtjad lahendada selliseid kaebused „asjakohaselt ja kiiresti“ ning kehtestavad sisemised kaebuste lahendamise süsteemid selle eesmärgi saavutamiseks. Lisaks on isikuteabe kaitse komisjon APPI artikli 61 punkti ii kohaselt vastutav „esitatud kaebuse puhul vajaliku vahendamise ja kaebusega tegelevale ettevõtjale pakutava koostöö eest“, mis mõlemal juhul kehtib ka välismaalaste esitatud kaebuste puhul. Sellega seoses on Jaapani seadusandja teinud keskvalitsusele ülesandeks võtta „vajalikke meetmeid“, et võimaldada ja hõlbustada isikuteavet käitlevate ettevõtjate kaebuste lahendamist (artikkel 9), samal ajal kui kohalikud omavalitsused püüavad tagada nendel juhtudel lepituse (artikkel 13). Sellel otstarbel võivad üksikisikud lisaks võimalusele esitada kaebus Jaapani riiklikule tarbijaküsimuste keskusele, esitada kaebuse rohkem kui 1 700 tarbijakeskuses, mille kohalikud omavalitsused on tarbijaohutuse seaduse ([61]) alusel rajanud. Need kaebused võib esitada ka APPI rikkumise korral. Põhitarbijaõiguste seaduse ([62]) artikli 19 alusel püüavad kohalikud omavalitsused asuda kaebuste lahendamiseks lepitusmenetlusse ja pakkuda pooltele vajalikke ekspertteadmisi. Need vaidluste lahendamise mehhanismid on osutunud üsna tõhusaks – vaidluste lahendamise määr oli 2015. aastal rohkem kui 75 000 kaebuse juures 91,2 %.

(105) Kui isikuteavet käitlev ettevõtja rikub APPI sätteid, võib see anda aluse tsiviilhagile, samuti kriminaalmenetlusele ja sanktsioonidele. Esiteks kui üksikisik leiab, et tema APPI artiklite 28, 29 ja 30 kohaseid õiguseid on rikutud, võib ta taotleda esialgset õiguskaitset, paludes kohtul välja anda isikuteavet käitlevale ettevõtjale määrus rahuldada tema taotlus neist ühe sätte alusel, st avaldada säilitatavaid isikuandmeid (artikkel 28), parandada säilitatavaid isikuandmeid, mis on valed (artikkel 29), või peatada ebaseaduslik töötlemine või andmete kolmandale isikule edastamine (artikkel 30). Sellise hagi võib esitada ilma vajaduseta tugineda tsiviilseadustiku ([63]) artiklile 709 või muule kahju õigusvastase tekitamise õiguse sättele ([64]). Eelkõige tähendab see seda, et üksikisikul ei ole vaja kahju tõestada.

(106) Teiseks juhul, kui väidetav rikkumine ei ole seotud individuaalsete õigustega artiklite 28, 29 ja 30 alusel, vaid isikuteavet käitleva ettevõtja üldiste andmekaitsepõhimõtetega, võib asjaomane isik esitada tsiviilhagi ettevõtja vastu, tuginedes Jaapani tsiviilseadustiku kahju õigusvastase tekitamise sätetele ja eelkõige artiklile 709. Ehkki artikli 709 kohase kohtuasja puhul on lisaks süüle (tahtlus või hooletus) nõutav kahju tõendamine, võib tsiviilseadusitku artikli 710 kohaselt olla see kahju nii materiaalne kui ka mittemateriaalne. Hüvitise suurust ei ole piiratud.

(107) Mis puutub kättesaadavatesse õiguskaitsevahenditesse, siis viitab Jaapani tsiviilseadustiku artikkel 709 rahalisele hüvitisele. Samas on Jaapani kohtupraktikas tõlgendatud seda artiklit selliselt, et sellest tuleneb kohtumääruse saamise õigus ([65]). Seega kui andmesubjekt esitab tsiviilseadustiku artikli 709 alusel hagi ning väidab, et tema õiguseid või huve on rikutud sellega, et kostja on rikkunud APPI sätet, võib see nõue/hagi lisaks kahjutasu nõudele sisaldada esialgse õiguskaitse taotlust, mille eesmärk on eelkõige ebaseadusliku töötlemise peatamine.

([61]) Seadus nr 50, 5. juuni 2009.
([62]) Seadus nr 60, 22. august 2012.
([63]) Tsiviilseadustiku artikkel 709 on peamine alus kahju hüvitamise tsiviilhagile. Selle sätte kohaselt „peab isik, kes on tahtlikult või hooletusest rikkunud teiste isikute mis tahes õigust või teiste isikute seaduslikult kaitstud huvi, hüvitama selle tagajärjel tekkinud kahjud“.
([64]) Tokyo kõrge kohtu 20. mai 2015. aasta otsus (ei ole avaldatud); Tokyo kõrge kohtu 8. septembri 2014. aasta otsus, Westlaw Japan 2014WLJPCA09088002. Vt ka APPI artikli 34 lõiked 1 ja 3.
([65]) Vt ülemkohtu 24. septembri 2002. aasta otsus (Hanrei Times, kd 1106, lk 72).

(108) Kolmandaks võib andmesubjekt lisaks tsiviilõiguslikele (kahju õigusvastase tekitamisega seotud) õiguskaitsevahenditele esitada kaebuse prokurörile või kohtupolitsei ametnikule, kui tegemist on APPI rikkumistega, mis võivad kaasa tuua kriminaalkaristused. APPI VII peatükk sisaldab mitut karistussätet. Kõige olulisem (artikkel 84) on seotud sellega, et isikuteavet käitlev ettevõtja ei järgi isikuteabe kaitse komisjoni määruseid vastavalt artikli 42 lõigetele 2 ja 3. Kui ettevõtja ei täida isikuteabe kaitse komisjoni välja antud korraldust, võib isikuteabe kaitse komisjoni esimees (samuti muu valitsusametnik) ([66]) edastada juhtumi prokurörile või kohtupolitsei ametnikule ning sel viisil algatada kriminaalmenetluse algatamise. Karistus isikuteabe kaitse komisjoni korralduse rikkumise eest on kuni kuuekuuline töökohustusega vangistus või kuni 300 000 jeeni suurune rahatrahv. Muud APPI sätted, millega on sätestatud andmesubjektide õiguseid ja huve mõjutavad sanktsioonid APPI rikkumise korral, on näiteks APPI artikkel 83 (seoses isikuteabe andmebaasi „salaja esitamise või kasutamisega“ selleks, et saada […] ebaseaduslikku kasu“) ja APPI artikli 88 punkt i (seoses sellega, et kolmas isik ei teavita õigesti isikuteavet käitlevat ettevõtjat, kui see ettevõtja saab isikuandmeid kooskõlas APPI artikli 26 lõikega 1, eelkõige seoses eelnevalt kolmanda isiku poolt selliste andmete omandamise üksikasjadega). APPI selliste rikkumiste eest kohaldatavad karistused on vastavalt kuni üheaastane vangistus koos tööga või kuni 500 000 jeeni suurune trahv (artikli 83 korral) või kuni 100 000 jeeni suurune haldustrahv (artikli 88 punkti i korral). Kuigi kriminaalkaristuse võimalus juba tõenäoliselt avaldab tugevat heidutavat mõju nii isikuteavet käitleva ettevõtja töötlemistoiminguid suunavale juhtkonnale kui ka andmeid käitlevatele üksikisikutele, on APPI artiklis 87 täpsustatud, et kui juriidilise isiku esindaja, alluv või muu töötaja on pannud toime APPI artiklite 83–85 kohase rikkumise, siis „karistatakse rikkujat ja kõnealusele juriidilisele isikule määratakse kõnealustes artiklites ette nähtud trahv“. Sellisel juhul saab maksimaalse karistuse määrata nii töötajale kui ka ettevõtjale.

(109) Lisaks võivad üksikisikud taotleda kaitset ka isikuteabe kaitse komisjoni tegevuse või tegevusetuse eest. Selleks nähakse Jaapani õiguses ette mitmed haldus- ja õiguskaitse võimalused.

(110) Kui üksikisik ei ole rahul isikuteabe kaitse komisjoni toimingutega, võib ta esitada halduskaebuse halduskaebuste läbivaatamise seaduse ([67]) alusel. Seevastu juhul, kui üksikisik leiab, et isikuteabe kaitse komisjon oleks pidanud tegutsema, aga ei teinud seda, võib üksikisik taotleda isikuteabe kaitse komisjonilt kooskõlas selle seaduse artikliga 36-3, et kehtestataks säte või esitataks haldussuunised, kui ta leiab, et „rikkumise kõrvaldamiseks vajalikku sätet või haldussuunist ei oleks antud või kehtestatud“.

(111) Mis puutub õiguskaitsesse, siis halduskohtumenetluse seaduse alusel võib isik, kes ei ole rahul isikuteabe kaitse komisjoni kehtestatud haldussättega, esitada *mandamus* kohtuasja, ([68]) milles palutakse kohtul anda välja määrus, et isikuteabe kaitse komisjon võtab lisameetmeid ([69]). Teatavatel juhtudel võib kohus välja anda ka esialgse *mandamus* määruse, et ära hoida pöördumatut kahju ([70]). Peale selle võib üksikisik sama seaduse alusel taotleda isikuteabe kaitse komisjoni otsuse kehtetuks tunnistamist ([71]).

(112) Lisaks võib üksikisik esitada hagi ka selleks, et saada riigilt hüvitist isikuteabe kaitse komisjoni vastu riigivastutuse seaduse artikli 1 lõike 1 alusel, kui ta on kannatanud kahju tingituna asjaolust, et isikuteabe kaitse komisjoni poolt ettevõtjale antud määrus on ebaseaduslik või isikuteabe kaitse komisjon ei ole kasutanud oma volitusi.

3. EUROOPA LIIDUST JAAPANIS ASUVATELE AVALIKU SEKTORI ASUTUSTELE EDASTATUD ISIKUANDMETELE JUURDEPÄÄS JA NENDE KASUTAMINE

(113) Komisjon on hinnanud ka piiranguid ja kaitsemeetmeid, sealhulgas Jaapani õiguses kättesaadavaid järelevalve- ja individuaalse kaitse mehhanisme seoses selliste isikuandmete kogumise ja järgneva edastamisega, mida edastatakse Jaapanis asuvatele ettevõtjatele avaliku sektori asutuste poolt avalikus huvis, eelkõige kriminaalõiguse täitmise tagamise ja riikliku julgeoleku eesmärgil (edaspidi „valitsuse juurdepääs“). Seoses sellega on Jaapani valitsus esitanud komisjonile ametlikud seisukohad, kinnitused ja kohustused, mis on allkirjastatud kõrgeimal ministrite ja ametite tasandil ning on esitatud käesoleva otsuse II lisas.

([66]) Kriminaalmenetluse seadustiku artikli 239 lõige 2.
([67]) 2014. aasta seadus nr 160.
([68]) Halduskohtumenetluse seaduse artikkel 37-2.
([69]) Halduskohtumenetluse seaduse artikli 3 lõike 6 kohaselt viitab termin „*mandamus* hagi“ hagile, millega taotletakse kohtu määrust haldusasutuse suhtes, et kehtestada esialgne halduskorraldus, mille ta „oleks“ pidanud kehtestama, aga jättis kehtestamata.
([70]) Halduskohtumenetluse seaduse artikkel 37-5.
([71]) Halduskohtumenetluse seaduse II peatükk, 1. jagu.

3.1. **Üldine õigusraamistik**

(114) Avaliku sektori volituste kasutamisega peab valitsuse juurdepääs toimuma täielikult õiguspäraselt (õiguspärasuse põhimõte). Seoses sellega sisaldab Jaapani põhiseadus sätteid, mis piiravad ja raamistavad isikuandmete kogumise avaliku sektori asutuste poolt. Nagu juba ettevõtjate poolt töötlemise kohta märgitud, on Jaapani ülemkohus, tuginedes põhiseaduse artiklile 13, mis muu hulga kaitseb õigust vabadusele, tunnustanud õigust privaatsusele ja andmekaitsele ([72]). Selle õiguse üks oluline aspekt on vabadus mitte lasta avaldada oma isikuteavet kolmandale isikule ilma loata ([73]). Sellest tuleneb õigus isikuandmete tõhusale kaitsele kuritarvitamise ja (eelkõige) ebaseadusliku juurdepääsu eest. Lisakaitse on tagatud põhiseaduse artikliga 35, milles on sätestatud kõikide isikute õigus kaitsta oma kodu, dokumente ja vara, ning nõutud, et avaliku sektori asutused taotleksid kõikidel „läbiotsimise ja arestimise“ juhtudel „piisava põhjuse“ ([74]) alusel kohtumääruse. Oma 15. märtsi 2017. aasta otsuses (GPSi juhtum) on ülemkohus selgitanud, et kõnealuse määruse nõue kehtib alati, kui valitsus tungib („siseneb“) isiklikku ruumi viisil, mille käigus eiratakse üksikisiku tahet ja seega toimub „sunduslik uurimine“. Kohtunik võib anda välja sellise määruse üksnes konkreetsele kuriteokahtlusele tuginedes, st kui esitatakse dokumentaalsed tõendid, mille põhjal uurimisega mõjutatud isikut saab käsitada kuriteo toime pannuna ([75]). Järelikult ei ole Jaapani ametiasutustel õiguslikku alust koguda isikuteavet sunduslike vahenditega olukordades, kus seaduse rikkumine ei ole veel toimunud, ([76]) näiteks selleks, et ära hoida kuritegu või muu turvalisuse ohu korral (nt uurimised riigi julgeoleku kaalutlustel).

(115) Seadusreservatsiooni põhimõtte kohaselt peab sunnimeetmete abil toimuva uurimise raames toimuv andmete kogumine olema alati konkreetselt seadusega lubatud (vt näiteks kriminaalmenetluse seadustiku artikli 197 lõige 1 kriminaaluurimise eesmärgil teabe sunduslike vahendite abil kogumise kohta). Seda nõuet kohaldatakse elektroonilisele teabele juurdepääsu suhtes.

(116) Oluline on see, et põhiseaduse artikli 21 lõikega 2 on tagatud kõikide teabevahendite salajasus ning piirangud on lubatud üksnes avalikes huvides vastuvõetavate õigusaktidega. Telekommunikatsiooniseaduse artikliga 4, mille kohaselt on telekommunikatsioonisettevõtja kohustatud hoidma sõnumisaladust, rakendatakse see konfidentsiaalsusnõue riigi seaduse tasandil. Seda on tõlgendatud kui kommunikatsiooniteabe avaldamise keelamist, välja arvatud juhul, kui selleks on kasutajate nõusolek või kui see põhineb kriminaalvastutuse sõnaselgetel eranditel karistusseadustiku ([77]) alusel.

(117) Põhiseadusega on tagatud ka õiguskaitse kättesaadavus (artikkel 32) ning õigus kaevata riik kohtusse kaitse saamiseks juhul, kui üksikisik on kannatanud kahju riigiametniku ebaseadusliku teo tõttu (artikkel 17).

(118) Mis puutub konkreetselt andmekaitse õigusse, siis on APPI III peatüki 1., 2. ja 3. jaos sätestatud üldpõhimõtted, mis hõlmavad kõiki sektoreid, sealhulgas avalikku sektorit. Eelkõige APPI artiklis 3 on sätestatud, et igasugust isikuteavet tuleb käidelda kooskõlas üksikisiku isikuõiguste austamise põhimõttega. Kui isikuteave, sealhulgas elektrooniliste dokumentide osana, on kogutud („omandatud“) avaliku sektorite asutuste ([78]) poolt, siis reguleerib selle

([72]) Vt näiteks ülemkohtu 12. septembri 2003. aasta otsus, kohtuasi nr 1656 (2002 (Ju)). Eelkõige on ülemkohus leidnud, et „igal isikul on vabadus kaitsta oma isikuteavet kolmandale isikule avaldamise või põhjenduseta avalikustamise eest“.

([73]) Ülemkohtu 6. märtsi 2008. aasta otsus (Juki-net).

([74]) „Piisav põhjus“ eksisteerib üksnes juhul, kui asjaomast isikut (kahtlustatav, süüdistatav) käsitatakse õigusrikkumise toimepanijana ning läbiotsimine ja arestimine on vajalik kriminaaluurimise jaoks. Vt ülemkohtu 18. märtsi 1969. aasta otsus, kohtuasi nr 100 (1968 (Shi)).

([75]) Vt kriminaalmenetluse eeskirjade artikli 156 lõige 1.

([76]) Samas tuleks märkida, et organiseeritud kuritegevuse ja kuritegevuse teel saadud tulu korral karistamise 15. juuni 2017. aasta seadusega on ette nähtud uus õigusrikkumise liik, millega kriminaliseeritakse terrorismiaktide ettevalmistamine ja teatavad muud organiseeritud kuritegevuse vormid. Uurimise võib algatada üksnes juhul, kui olemas on konkreetne kahtlus, mis põhineb tõenditel, et täidetud on kõik kolm vajalikku tingimust, mis moodustavad õigusrikkumise (osalemine organiseeritud kuritegelikus rühmituses, kuriteo „kavandamine“ ja „toimepanemise ettevalmistamine“). Vt ka nt õõnestustegevuse ärahoidmise seaduse artiklid 38–40 (21. juuli 1952. aasta seadus nr 240).

([77]) Telekommunikatsioonisektoris isikuteabe kaitse suuniste artikli 15 lõige 8.

([78]) Haldusorganid on määratletud APPIHAO artikli 2 lõikes 1. Jaapani valitsuselt saadud teabe kohaselt kuuluvad kõik avaliku sektori asutused peale prefektuuri politseiameti „haldusorganite“ määratluse alla. Samal ajal tegutseb prefektuuri politseiamet õigusraamistikus, mis on sätestatud prefektuuri isikuteabe kaitse määrustega (vt APPI artikkel 11 ja aluspoliitika), milles on ette nähtud APPIHAOga samaväärsed isikuteabe kaitse sätted. Vt II lisa jagu I.B. Nagu isikuteabe kaitse komisjon selgitas, tuleb „aluspoliitika“ kohaselt nende määruste kehtestamisel tugineda APPIHAO-le ning siseasjade ja teabevahetuse ministeerium avaldab teatisi, et anda kohalikkele omavalitsustele selles küsimuses vajalikke juhendeid. Nagu isikuteabe kaitse komisjon rõhutas, „[o]n vaja neid piiranguid silmas pidades igas perfektuuris kehtestada isikuteabe kaitse määrus […], mis põhineb aluspoliitikal ja teatiste sisul.“

käitlemist haldusorganite hoitava isikuteabe kaitse seadus (APPIHAO) ([79]). Põhimõtteliselt ([80]) kuulub selle alla ka isikuteabe töötlemine kriminaalõiguse täitmise tagamise või riikliku julgeoleku eesmärgil. Muu hulgas on APPIHAOs sätestatud, et avaliku sektori asutused: i) võivad säilitada isikuteavet üksnes määral, mil see on vajalik nende ülesannete täitmiseks; ii) ei kasuta seda teavet „ebaõiglasel" eesmärgil ega avalda seda kolmandale isikule ilma põhjenduseta; iii) määratlevad eesmärgi ning ei muuda seda eesmärki rohkem kui nii, nagu võib põhjendatult pidada esialgse eesmärgi puhul asjakohaseks (eesmärgi piiramine); iv) põhimõtteliselt ei kasuta ega esita kolmandale isikule säilitatud isikuteavet muudel eesmärkidel ning, kui nad peavad seda vajalikuks, kehtestavad piirangud kolmandate isikute poolt kasutamise eesmärgile või meetodile; v) üritavad tagada teabe õigsuse (andmete kvaliteedi); vi) võtavad vajalikke meetmeid nõuetekohaseks teabehalduseks või selleks, et ära hoida leket, kadumist või kahju (andmete turvalisus); ning vii) üritavad nõuetekohaselt ja kiiresti töödelda kõiki teabe töötlemise kohta esitatud kaebusi ([81]).

3.2. **Jaapani avaliku sektori asutuste juurdepääs ja nende poolt andmete kasutamine kriminaalõiguse täitmise tagamise eesmärgil**

(119) Jaapani õigus sisaldab mitmeid piiranguid isikuandmetele juurdepääsule ja isikuandmete kasutamisele kriminaalõiguse täitmise tagamise eesmärgil ning ka järelevalve- ja õiguskaitsemehhanisme, mis piisaval määral tagavad nende andmete tõhusa kaitse ebaseadusliku riive ja kuritarvitamise riski eest.

3.2.1. *Õiguslik alus ja kohaldatavad piirangud/kaitsemeetmed*

(120) Jaapani õigusraamistikus on elektroonilise teabe kogumine kriminaalõiguse täitmise tagamise eesmärkidel lubatud määruse (sunduslike vahendite abil kogumine) või vabatahtliku avaldamise taotluse alusel.

3.2.1.1. Kohtumäärusel põhinev sunduslik uurimine

(121) Nagu on märgitud põhjenduses 115, peab igasugune andmete kogumine sundkorras uurimise osana olema seaduses konkreetselt lubatud ning seda võib teha üksnes kohtumääruse alusel, mis on „väljastatud piisavuse põhjusel" (põhiseaduse artikkel 35). Seoses kuritegude uurimisega kajastatakse seda nõuet kriminaalmenetluse seadustiku sätetes. Kooskõlas CCP artikli 197 lõikega 1 „kohaldatakse sunduslikke meetmeid üksnes juhul, kui selle seadustikuga on kehtestatud erisätted". Mis puutub elektroonilise teabe kogumisse, siis ainus seotud ([82]) õiguslik alus on CCP artikkel 218 (läbiotsimine ja arestimine) ja CCP artikkel 222-2, mille kohaselt kohaldatakse sunduslikke meetmeid elektroonilise teabevahetuse pealtkuulamiseks kummagi poole nõusolekuta muude seaduste, nimelt kriminaaluurimise eesmärgil telefonikõne pealtkuulamise seaduse (edaspidi „telefonikõne pealtkuulamise seadus") alusel. Mõlemal juhul kehtib nõue välja anda määrus.

(122) Täpsemalt võib öelda, et kooskõlas CCP artikli 218 lõikega 1 võib prokurör, prokuröri abi või kohtupolitsei ametnik, kui see on õigusrikkumise uurimise jaoks vajalik, korraldada kohtu eelnevalt väljaantud määruse alusel läbiotsimise või arestimise (sealhulgas dokumentide väljanõudmiseks) ([83]). Muu hulgas sisaldab see määrus kahtlustatava või süüdistatava nime, süüks pandavat õigusrikkumist, ([84]) arestitavaid elektromagnetilisi andmekandjaid ja kontrollitavaid „kohti või esemeid" (CCP artikli 219 lõige 1).

([79]) Isikuteave, mille on saanud haldusorgani ametnikud oma ülesannete täitmise käigus ning mida hoiab asjaomane haldusorgan organisatsiooniliseks kasutamiseks, kuulub „säilitatud isikuteabe" määratluse alla APPIHAO artikli 2 lõike 3 tähenduses, kuivõrd see on haldusdokumentides protokollitud. See hõlmab elektroonilist teavet, mida need asutused koguvad ja seejärel täiendavalt töötlevad, arvestades, et haldusorganite hoitavale teabele juurdepääsu seaduse [1999. aasta seadus nr 42] artikli 2 lõikes 2 esitatud „haldusdokumentide" määratlus hõlmab elektromagnetilisi dokumente.

([80]) Samas on kooskõlas kriminaalmenetluse seadustiku (Code of Criminal Procedure, edaspidi „CCP") artikliga 53-2 APPIHAO IV peatükk jäetud välja „kohtuprotsessidega seotud dokumentide" puhul, mille hulka saadud teabe kohaselt kuulub ka elektrooniline teave, mis on saadud kriminaaluurimise osana vabatahtliku koostöö määruse või taotluse alusel. Samamoodi ei saa üksikisikud riigi julgeoleku valdkonnas kogutud teabe korral oma õiguseid APPIHAO alusel edukalt kasutada, kui avaliku sektori asutuse juhil on „põhjendatud alus" arvata, et avaldamine „tõenäoliselt kahjustab riigi julgeolekut" (vt artikli 14 punkt iv). Seda arvestades nõutakse avaliku sektori asutuse alati, kui see on võimalik, vähemalt osalist avaldamist (artikkel 15).

([81]) APPIHAO viiteid vt: II lisa jagu II.A.1, punkt b, alapunkt 2.

([82]) Ehkki CCP artikliga 220 lubatakse läbiotsimist ja arestimist „kohapeal" ilma määruseta, kui prokurör, prokuröri abi või kohtupolitsei ametnik peab kinni kahtlusaluse / avaliku õigusrikkuja, ei ole see edastamise kontekstis ja seega käesoleva otsuse eesmärgil asjakohane.

([83]) Kooskõlas artikli 222 lõikega 1 koostoimes CCP artikliga 110 tuleb isikule, kes sellele meetmele peab alluma, näidata läbiotsimis-/arestimismäärust.

([84]) Vt ka CCP artikli 189 lõige 2, mille kohaselt peab kohtupolitsei ametnik uurima õigusrikkujat ja tõendeid, „kui ta leiab, et õigusrikkumine on toime pandud." Samamoodi on kriminaalmenetluse eeskirjade artikli 155 lõikes 1 nõutud, et määruse kirjalik taotlus sisaldaks muu hulgas „süüks pandavat õigusrikkumist" ja „kuriteo asjaolude kokkuvõtet".

(123) Mis puutub telefonikõne pealtkuulamisse, siis on telefonikõne pealtkuulamise seaduse artikli 3 kohaselt sellised meetmed lubatud üksnes rangete nõuete alusel. Eelkõige peavad avaliku sektori asutused hankima eelneva kohtumääruse, mille võib välja anda üksnes konkreetsete raskete kuritegude uurimiseks (loetletud seaduse lisas) ([85]) ning juhul, kui on „erakordselt raske teha kindlaks kurjategijat või selgitada toimepanemise olukorda/üksikasju mingil muul viisil“ ([86]). Telefonikõne pealtkuulamise seaduse artiklis 5 on ette nähtud, et väljaantav määrus on ajaliselt piiratud ja kohtunik võib kehtestada lisatingimusi. Lisaks on telefonikõne pealtkuulamise seaduses sätestatud mitmed lisagarantiid, näiteks tunnistajate osalemise nõue (artiklid 12 ja 20), pealtkuulamise keeld privilegeeritud rühmade (nt arstid, juristid) puhul (artikkel 15), kohustus pealkuulamine lõpetada, kui pealkuulamine ei ole enam põhjendatud (ka enne määruse aegumist) (artikkel 18), samuti üldnõude, et asjaomast isikut tuleb teavitada ja anda talle andmetele juurdepääs 30 päeva jooksul alates pealkuulamise lõpetamisest (artiklid 23 ja 24).

(124) Määruse alusel võetavate sunduslike meetmete puhul võib läbi viia üksnes sellist kontrolli, „mis on vajalik selle eesmärgi saavutamiseks“ – see tähendab, kui uurimise eesmärke ei saa muul viisil saavutada (CCP artikli 197 lõige 1). Ehkki vajaduse kindlaksmääramise kriteeriumeid ei ole seadusandlusega täpsemalt määratletud, on Jaapani ülemkohus teinud otsuse, et määrust välja andev kohtunik peaks andma üldise hinnangu, võttes arvesse eelkõige i) õigusrikkumise tõsidust ja selle toimepaneku viisi; ii) tõendina arestitavate materjalide väärtust ja olulisust; iii) (sellise riski) tõenäosust, et tõendeid võidakse varjata või need võidakse hävitada; ning iv) ulatust, milles arestimine võib põhjustada asjaomasele isikule kahju ([87]).

3.2.1.2. Vabatahtliku avaldamise taotlus, mis põhineb „päringuvormil“

(125) Avaliku sektori asutused võivad oma pädevuse piires samuti koguda elektroonilist teavet, tuginedes vabatahtliku avaldamise taotlustele. See viitab mittesunduslikule koostöövormile, mille puhul ei saa taotluse täitmiseks kohustada, ([88]) vabastades seega avaliku sektori asutused kohtumääruse taotlemise kohustusest.

(126) Määral, mil see taotlus on suunatud ettevõtjale ja puudutab isikuteavet, peab ettevõtja järgima APPI nõudeid. APPI artikli 23 lõike 1 kohaselt võivad ettevõtjad avaldada isikuteavet kolmandatele isikutele asjaomase isiku nõusolekuta üksnes teatavatel juhtudel, sealhulgas juhul, kui avaldamine „põhineb õigusnormidel“ ([89]). Kriminaalõiguse täitmise tagamise valdkonnas on selliste taotluste õiguslik alus sätestatud CCP artikli 197 lõikes 2, mille kohaselt „võidakse eraõiguslikel organisatsioonidel lasta teada anda vajalikest küsimustest seoses uurimisega“. Kuna selline „päringuvorm“ on lubatud üksnes kriminaaluurimise osana, eeldab see alati juba toime pandud kuriteo konkreetset kahtlust ([90]). Kuna sellist uurimist korraldab tavaliselt prefektuuri politseiamet, kehtivad lisaks politseiseaduse ([91]) artikli 2 lõike 2 kohased piirangud. Selle sätte kohaselt on politsei tegevus „rangelt piiratud“ nende ülesannete ja kohustuste täitmisega (see tähendab kuritegude ennetamise, peatamise ja uurimisega). Lisaks tegutseb politsei oma ülesandeid täites erapooletult, eelarvamustevabalt ja õiglaselt ning ei või kunagi kuritarvitada oma volitusi „selliselt, et see riivab Jaapani põhiseadusega tagatud üksikisiku õigusi ja vabadusi“ (sealhulgas, nagu märgitud, õigust privaatsusele ja andmekaitsele) ([92]).

(127) Riiklik politseiamet kui föderaalne ametiasutus, mis vastutab muu hulgas kõikide kriminaalpolitseiga seotud küsimuste eest, on eelkõige CCP artikli 197 lõikest 2 lähtuvalt prefektuuride politseiametitele välja andnud

([85]) Lisas on viidatud üheksat liiki kuritegudele, nt kuritegudele, mis on seotud narkootikumide ja relvadega, inimkaubandusega ja organiseeritud mõrvaga. Tuleb märkida, et äsja kehtestatud õigusrikkumist, milleks on „terrorismiaktide ettevalmistamine ja muu organiseeritud kuritegevus“ (vt joonealune märkus 76) piirangute loetelus ei ole.

([86]) Peale selle peab telefonikõne pealtkuulamise seaduse artikli 23 kohaselt uurimisasutus üksikisikut, kelle teabevahetust on pealt kuulatud (ning seega kellega pealtkuulamise salvestis on seotud), sellest asjaolust kirjalikult teavitama.

([87]) Vt II lisa jagu II.A.1, punkt b, alapunkt 1.

([88]) Saadud teabe kohaselt ei tulene koostööd mittetegevale ettevõtjatele ühestki seadusest negatiivseid tagajärgi (sealhulgas karistusi). Vt II lisa jagu II.A.2, punkt a.

([89]) Isikuteabe kaitse komisjoni suuniste (üldeeskirjade väljaanne) artikli 23 lõike 1 punktis i on ette nähtud isikuteabe avaldamise alus nii määrusele (CCP artikkel 218) kui ka päringuvormile (CCP artikli 197 lõige 2) vastates.

([90]) See tähendab, et „päringuvormi“ võib kasutada üksnes konkreetsete juhtumite asjus teabe kogumiseks, mitte suuremahuliseks isikuandmete kogumiseks. Vt ka II lisa jagu I.A.2, punkt b, alapunkt 1.

([91]) Samuti avaliku turvalisuse prefektuurikomisjoni määrused, vt CCP artikli 189 lõige 1.

([92]) Vt ka politseiseaduse artikkel 3, mille kohaselt on kõikide politseiametnike ametivanne „täita kohustust kaitsta ja järgida Jaapani põhiseadust ja seaduseid ning täita oma kohustusi erapooletult, õiglaselt, ausalt ja eelarvamustevabalt“.

suunised ([93]) „uurimistel kirjalike päringute nõuetekohase kasutamise kohta“. Selle teate kohaselt tuleb taotlused esitada eelnevalt kindlaks määratud vormis („vorm nr 49“ ehk nn „päringuvorm“), ([94]) mis puudutab „konkreetse uurimise“ protokolle, ning nõutav teave peab olema „[selle] uurimise jaoks vajalik“. Iga juhtumi korral peab peauurija „täielikult kontrollima konkreetse päringu vajadust, sisu jne“ ning saama kõrge tasandi ametnikult asutusesisese heakskiidu.

(128) Peale selle on Jaapani ülemkohtu kahes otsuses aastatest 1969 ja 2008 ([95]) ette nähtud õigust privaatsusele riivavate mittesunduslike meetmete piirangud ([96]). Eelkõige leidis kohus, et need meetmed peavad olema „mõistlikud“ ja jääma „üldiselt lubatud piiridesse“, see tähendab, et need peavad olema vajalikud kahtlusaluse uurimise jaoks (tõendite kogumiseks) ning neid tuleb kasutada „uurimise eesmärgi saavutamiseks asjakohaste meetodite abil“ ([97]). Kohtuotsused näitavad, et see tähendab proportsionaalsuse kontrollimist, võttes arvesse kõiki juhtumi asjaolusid (näiteks privaatsuse õiguse riivamise tase, sealhulgas privaatsuse eeldust, kuriteo tõsidust, kasulike tõendite saamise tõenäosust, selle tõendi olulisust, võimalikke muid uurimise vahendeid jne) ([98]).

(129) Lisaks neile piirangutele avaliku sektori asutuse tegevuses peavad ettevõtjad ise kontrollima („kinnitama“) kolmandale isikule teabe avaldamise vajadust ja „põhjendatust“ ([99]). See hõlmab küsimust, kas seadus takistab neid koostööd tegemast. Sellised vastuolulised õiguslikud kohustused võivad eelkõige tuleneda konfidentsiaalsuse kohustustest, näiteks karistusseadustiku artiklist 134 (arsti, juristi, preestri jne ja tema kliendi vahelise suhte kohta). Samuti „peab iga isik, kes töötab telekommunikatsioonivaldkonnas, hoidma oma töökohustusi täites teiste isikute saladusi, mis on saanud teatavaks telekommunikatsioonivahendi ettevõtja käideldava teabevahetuse käigus“ (telekommunikatsiooniseaduse artikli 4 lõige 2). Seda kohustust toetab telekommunikatsiooniseaduse artiklis 179 sätestatud sanktsioon, mille kohaselt on iga isik, kes on rikkunud telekommunikatsioonivahendi ettevõtja käideldavas teabevahetuses sõnumisaladust, süüdi kuriteos ning teda karistatakse kuni kaheaastase vangistusega, mis sisaldab töökohustust, või kuni ühe miljoni jeeni suuruse trahviga ([100]). Ehkki see nõue ei ole absoluutne ning lubab eelkõige meetmeid, mis rikuvad sõnumisaladust, kui see on „põhjendatud tegevus“ karistusseadustiku artikli 35 tähenduses, ei hõlma see erand avaliku sektori asutuste vastuseid mittesunduslikele taotlustele elektroonilise teabe avaldamiseks CCP artikli 197 lõike 2 ([101]) kohaselt.

3.2.1.3. Kogutud teabe edasine kasutamine

(130) Isikuteave, mida Jaapani avaliku sektori asutused koguvad, kuulub APPIHAO kohaldamisalasse. See seadus reguleerib „säilitatava isikuteabe“ käitlemist (töötlemist) ning kehtestab praegu mitu piirangut ja kaitsemeedet

([93]) Politseiseaduse artikli 30 lõike 1 ja artikli 31 lõike 2 kohaselt on prefektuuri politseiameti „juhendamine ja järelevalve“ piirkondlike politseijaoskondade (riikliku politseiameti kohalikud teenindused) peadirektori ülesanne.

([94]) Päringuvormis tuleb märkida ka „käitleja“ kontaktandmed („jaoskonna [ametikoha] nimi, käitleja nimi, ametiasutuse telefon, töötaja otsetelefon jne).

([95]) Ülemkohtu 24. detsembri 1969. aasta otsus (1965(A) 1187); 15. aprilli 2008. aasta otsus (2007(A) 839).

([96]) Ehkki need kohtuotsused ei puudutanud elektroonilise teabe kogumist, on Jaapani valitsus selgitanud, et ülemkohtu väljatöötatud kriteeriume tuleb kohaldada alati, kui avaliku sektori asutused riivavad eraelu puutumatuse õigust, sh kõikide „vabatahtlike uurimiste“ puhul, ning seega on Jaapani ametiasutused kohustatud neid kriteeriume ka vabatahtlike teabetaotluste tegemise korral järgima. Vt II lisa jagu II.A.2, punkt b, alapunkt 1.

([97]) Saadud teabe kohaselt tuleb neid tegureid käsitada „kooskõlas sotsiaalselt tunnustatud lepetega põhjendatuna“. Vt II lisa jagu II.A.2, punkt b, alapunkt 1.

([98]) Sunduslike uurimiste (telefonikõne pealtkuulamine) kontekstis on sama teemat lahatud ülemkohtu 16. detsembri 1999. aasta otsuses (1997(A) 636).

([99]) Seoses sellega on Jaapani ametiasutused osutanud isikuteabe kaitse komisjoni suunistele (üldeeskirja väljaanne) ning isikuteabe kaitse komisjoni poolt APPI kohaldamiseks koostatud küsimuste ja vastuste dokumendi punktile 5/14. Nagu väidavad Jaapani ametiasutused, siis „võttes arvesse üksikisikute kasvavat teadlikkust seoses nende privaatsusõigustega, samuti selliste taotlustega tekitatud töökoormust, on ettevõtjad sellistele taotlustele vastates aina ettevaatlikumad“. Vt II lisa, jagu II.A.2, samuti seoses riikliku politseiameti 1999. aasta teatisega. Saadud teabe kohaselt on need olnud tõepoolest juhtumid, mil ettevõtjad on koostööst keeldunud. Näiteks LINE (Jaapani kõige populaarsem sõnumite saatmise rakendus) märgib oma 2017. aasta läbipaistvusaruandes järgmist: „Olles saanud mitmeid taotluseid uurimisasutustelt jne, […] kontrollime me asjakohasust õiguspärasuse, kasutaja kaitse jne seisukohast. Sellel kontrollimisel keeldume taotlusele vastamast, kui esineb mõni õiguslik puudus. Kui nõude ulatus on uurimise eesmärki arvestades liiga lai, palume uurimisasutuselt selgitust. Kui selgitus põhjendust ei sisalda, siis me ei vasta sellele taotlusele.“ Kättesaadav internetis aadressil: https://linecorp.com/en/security/transparency/top

([100]) Karistuseks on kolmeaastane töökohustusega vangistus või kuni kahe miljoni jeeni suurune trahv igale isikule, kes „töötab telekommunikatsioonivaldkonnas“.

([101]) Karistusseadustiku alusel on „põhjendatud teod“ eelkõige need telekommunikatsioonifirma teod, millega ta täidab riigi meetmeid, millel on õigusjõud (sunduslikud meetmed), näiteks kui uurimisasutused võtavad meetmeid kohtuniku välja antud määruse alusel. Vt II lisa jagu II.A.2, punkt b, alapunkt 2, viidates isikuteabe kaitse suunistele telekommunikatsioonivaldkonnas.

(vt põhjendus 118) ([102]). Pealegi asjaolu, et haldusorgan võib säilitada isikuteavet „üksnes juhul, kui säilitamine on vajalik tema õigusnormidega sätestatud pädevusse kuuluvate küsimuste lahendamiseks“ (APPIHAO artikli 3 lõige 1), kehtestab piirangud – vähemalt kaudselt – ka esialgsele kogumisele.

3.2.2. *Sõltumatu järelevalve*

(131) Jaapanis on elektroonilise teabe kogumine kriminaalõiguse täitmise tagamise valdkonnas usaldatud eelkõige ([103]) prefektuuri politseiametile ([104]), kelle suhtes kohaldatakse selles osas mitmetasandilist järelevalvet.

(132) Esiteks kõikidel juhtudel, mil elektroonilist teavet kogutakse sunduslike vahendite abil (läbiotsimine ja arestimine), peab politsei saama eelneva kohtumääruse (vt põhjendus 121). Seepärast peab kohtunik nendel juhtudel teabe kogumist eelnevalt kontrollima, tuginedes rangele „piisava põhjuse“ nõudele.

(133) Kuna vabatahtliku teabe avaldamise taotluste korral puudub kohtuniku eelnev kontroll, võivad ettevõtjad, kellele sellised taotlused esitatakse, esitada neile vastuväite, riskimata negatiivsete tagajärgedega (ning nad peavad võtma arvesse igasuguse avaldamise mõju privaatsusele). Peale selle teevad politseiametnikud CCP artikli 192 lõike 1 kohaselt alati koostööd ja kooskõlastavad oma tegevuse prokuröriga (ja avaliku turvalisuse prefektuurikomisjoniga) ([105]). Prokurör võib omakorda anda vajalikke üldjuhiseid, et kehtestada õiglase uurimise reeglid ja/või anda üksikuurimise raames konkreetseid korraldusi (CCP artikkel 193). Kui neid juhiseid ja/või korraldusi ei järgita, võib prokuratuur esitada süüdistuse distsiplinaarmenetluses (CCP artikkel 194). Seega tegutseb prefektuuri politseiamet prokuröri järelevalve all.

(134) Seega võib põhiseaduse artikli 62 kohaselt Jaapani parlamendi kumbki koda viia läbi uurimise seoses valitsusega, sealhulgas seoses politsei teabekogumise õiguspärasusega. Sel eesmärgil võib ta nõuda tunnistajate kohalolekut ja ütlusi ja/või protokollide koostamist. Neid uurimisvolitusi on täiendavalt kirjeldatud parlamendiseaduses ja eelkõige selle XII peatükis. Konkreetselt on parlamendiseaduse artiklis 104 sätestatud, et valitsus, riigi ametiasutused ja muud valitsuse osad „peavad täitma parlamendi ja tema komisjonide taotluseid esitada uurimise jaoks vajalikke aruandeid ja protokolle“. Täitmisest keeldumine on lubatud üksnes juhul, kui valitsus esitab rahuldava põhjenduse, mida parlament aktsepteerib, või kui väljastatakse ametlik deklaratsioon, et aruannete või protokollide esitamine „kahjustab tõsiselt riigi huvi“ ([106]). Lisaks võivad parlamendiliikmed esitada valitsusele kirjalikke küsimusi (parlamendiseaduse artiklid 74 ja 75) ning varem on sellised „kirjalikud päringud“ puudutanud ka valitsuse poolt isikuteabe käitlemist ([107]). Parlamendi rolli täitevvõimu järelevalvel toetavad aruandekohustused, näiteks telefonikõne pealtkuulamise seaduse artikli 29 alusel.

(135) Kolmandaks peab ka prefektuuri politseiameti kui täidesaatva haru üle toimuma sõltumatu järelevalve. See hõlmab eelkõige avaliku turvalisuse prefektuurikomisjone, mis on asutatud prefektuuride tasandil, et tagada politsei demokraatlik juhtimine ja poliitiline neutraalsus ([108]). Nendesse komisjonidesse kuuluvad prefektuuri kuberneri poolt prefektuuri täiskogu nõusolekul nimetatud liikmed (kes on valitud selliste kodanike seast, kes ei ole ega ole olnud viiel eelneval aastal avalikus teenistuses), kelle ametisolek on kindlustatud (st kes eelkõige vabastatakse ametist üksnes põhjendatud juhul) ([109]). Kooskõlas saadud teabega ei anta neile juhiseid ja seetõttu saab neid pidada täiesti sõltumatuks ([110]). Avaliku turvalisuse prefektuurikomisjonidele antud ülesannetest ja volitustest

([102]) Asjaomaste üksikisikute õiguste kohta vt punkt 3.1.
([103]) Põhimõtteliselt võib prokurör – või prokuröri abi prokuröri korraldusel – uurida õigusrikkumist, kui ta peab seda vajalikuks (CCP artikli 191 lõige 1).
([104]) Saadud teabe alusel ei vii riigi politseiamet läbi eraldi kriminaaluurimist. Vt II lisa jagu II.A.1, punkt a.
([105]) Vt ka CCP artikkel 246, mille kohaselt on kohtupolitsei kohustatud saatma juhtumi toimiku prokurörile kohe, kui ta on kuriteo uurimise läbi viinud („saatmise põhimõte kõikides juhtumites“).
([106]) Alternatiivina võib parlament lasta saladuseks tunnistatud teabe järelevalve ja läbivaatamise nõukogul vastamisest keeldumist uurida. Vt parlamendiseaduse artikkel 104-II.
([107]) Vt II lisa jagu II.B.4.
([108]) Lisaks on kohaliku autonoomia seaduse artikli 100 kohaselt kohalik kogu pädev uurima prefektuuri tasandil loodud täitevasutuste, sealhulgas prefektuuri politseiameti tegevust.
([109]) Vt politseiseaduse artiklid 39–41. Politsei neutraalsuse kohta vt ka politseiseaduse artikkel 42.
([110]) Vt II lisa jagu II.B.3 („sõltumatu nõukogu süsteem“).

tuleneb, et nad vastutavad politseiseaduse artikli 38 lõike 3 kohaselt ja koostoimes artikliga 2 ja artikli 36 lõikega 2 „üksikisiku õiguste ja vabaduse kaitse“ eest. Selleks on neile antud õigus teha prefektuuri politseiameti uurimistegevuse üle „järelevalvet“, ([111]) sh isikuandmete kogumise suhtes. Eelkõige võivad komisjonid „juhendada prefektuuri politseiametit üksikasjalikult või konkreetsetel üksikjuhtumitel politseitöötajate väärkäitumise kontrollimisel, kui see on vajalik“ ([112]). Kui prefektuuri politseiameti juht ([113]) saab sellise korralduse või temani jõuab teave võimalikust väärkäitumisest (sealhulgas seaduste rikkumisest või muust hooletusest ametiülesannete täitmisel) muul moel, peab ta asja kohe kontrollima ja teatama kontrolli tulemusest avaliku turvalisuse prefektuurikomisjonile (politseiseaduse artikli 56 lõige 3). Kui see komisjon peab seda vajalikuks, võib ta nimetada ka ühe oma liikmetest rakendamise seisundit läbi vaatama. Protsess jätkub seni, kuni avaliku turvalisuse prefektuurikomisjon on teinud kindlaks, et juhtum on nõuetekohaselt lahendatud.

(136) Lisaks on APPIHAO nõuetekohaseks kohaldamiseks antud pädevale ministrile või ameti juhile (nt riikliku politseiameti peadirektorile) täitmise tagamise volitused ja järelevalve on usaldatud siseasjade ja teabevahetuse ministeeriumile. APPIHAO artikli 49 kohaselt võib siseasjade ja teabevahetuse ministeerium „koguda aruandeid selle seaduse täitmise seisundi kohta“ haldusorganite juhtidelt (minister). Seda järelevalvefunktsiooni toetavad ka siseasjade ja teabevahetuse ministeeriumi 51 „koondteabekeskust“ (üks igas prefektuuris üle Jaapani), mis käitlevad igal aastal tuhaneid üksikisikute päringuid ([114]) (mis omakorda võib paljastada võimalikke seaduse rikkumisi). Kui siseasjade ja teabevahetuse ministeerium peab seda vajalikuks, et tagada seaduse täitmine, võib ta lasta esitada selgitusi ja materjale ning avaldada arvamusi seoses asjaomase haldusorgani poolt isikuteabe käitlemisega (APPIHAO artiklid 50 ja 51).

3.2.3. *Üksikisiku õiguskaitse*

(137) Lisaks *ex officio* järelevalvele on üksikisikutel mitu võimalust saada ka üksikisiku õiguskaitset nii sõltumatute ametiasutuste (nagu avaliku turvalisuse prefektuurikomisjonid või isikuteabe kaitse komisjon) kui ka Jaapani kohtute kaudu.

(138) Esiteks on haldusorganite kogutud isikuteabe puhul neil organitel kohustus edasisel töötlemisel „teha jõupingutusi, et vaadata kaebused läbi nõuetekohaselt ja kiiresti“ (APPIHAO artikkel 48). Ehkki APPIHAO IV peatükki individuaalsete õiguste kohta ei kohaldata sellise isikuteabe puhul, mis sisaldub „dokumentides, mis on seotud kohtuprotsesside ja arestitud esemetega“ (CCP artikli 53–2 lõige 2) – mis hõlmab kriminaaluurimise osana kogutud isikuteavet –, võivad üksikisikud esitada kaebuse, et tugineda üldistele andmekaitse põhimõtetele, nagu kohustus säilitada isikuteavet „üksnes juhul, kui säilitamine on vajalik [õiguskaitsefunktsioonide] täitmiseks“ (APPIHAO artikli 3 lõige 1).

(139) Lisaks garanteeritakse politseiseaduse artikliga 79 üksikisikutele, kes ei ole rahul politseiametnike „tööülesannete täitmisega“, õigus esitada kaebus (pädevale) sõltumatule avaliku turvalisuse prefektuurikomisjonile. Komisjon tegeleb selliste kaebustega „usaldusväärselt“ kooskõlas seaduste ja kohalike määrustega ning teavitab kaebuse esitajat tulemustest kirjalikult. Tuginedes komisjoni pädevusele teha prefektuuri politseiameti üle järelevalvet ja anda „töötajate väärkäitumise“ korral „juhiseid“ (politseiseaduse artikli 38 lõige 3, artikli 43–2 lõige 1), võib ta nõuda, et prefektuuri politseiamet uuriks asjaolusid, võtaks selle uurimise tulemusest lähtudes meetmeid ja annaks tulemustest teada. Kui komisjon leiab, et politsei läbi viidud uurimine ei ole olnud piisav, võib ta anda ka juhiseid kaebuse menetlemise kohta.

(140) Selleks et hõlbustada kaebuste menetlemist, on riiklik politseiamet välja andnud „teatise“ politseile ja avaliku turvalisuse prefektuurikomisjonidele politseiametnike töökohustuste täitmise suhtes esitatud kaebuste nõuetekohase menetlemise kohta. Selles dokumendis sätestab riiklik politseiamet politseiseaduse artikli 79 tõlgendamise ja

([111]) Vt politseiseaduse artikli 5 lõige 3 ja artikli 38 lõige 3.

([112]) Vt politseiseaduse artikli 38 lõige 3, artikli 43-2 lõige 1. Juhul kui ta „teeb korralduse“ artikli 43-2 lõike 1 tähenduses, võib avaliku turvalisuse prefektuurikomisjon lasta komisjonil nimetada komitee, kes jälgib selle rakendamist (lõige 2). Samuti võib komisjon soovitada prefektuuri politseiameti juhi (politseiseaduse artikli 50 lõige 2) ja teiste politseiametnike (artikli 55 lõige 4) suhtes distsiplinaarmeetme või ametist vabastamise kasutamist.

([113]) Sama õigus on Tokio politsei puhul politseiameti ülemal (vt politseiseaduse artikli 48 lõige 1).

([114]) Saadud teabe kohaselt tegelesid „koondteabekeskused“ 2017. eelarveaastal (2017. aasta aprillist 2018. aasta märtsini) kokku 5 186 üksikisikute päringuga.

rakendamise reeglid. Muu hulgas nõutakse selles, et prefektuuri politseiamet looks „kaebuste menetlemise süsteemi“ ning menetleks kõiki pädevale avaliku turvalisuse prefektuurikomisjonile esitatud kaebuseid „kiiresti“ ja samas teataks neist. Teatises on kaebused määratletud nõuetena, millega taotletakse „ebaseadusliku või sobimatu käitumisega konkreetsel juhul tekitatud ebasoodsa olukorra“ ([115]) või „politseiniku poolt ametiülesannete täitmisel vajaliku meetme võtmata jätmise“ ([116]) parandamist, samuti igasuguse „etteheitena/rahulolematusena seoses viisiga, kuidas politseinik oma tööülesandeid täitis“. Kaebuse sisulise kohaldamisala määratlus on seega lai, hõlmates igasuguseid andmete ebaseadusliku kogumise juhtumeid, ja kaebuse esitaja ei pea tõendama, et politseiniku tegevuse tulemusel on tekkinud kahju. Oluline on see, et teatises on ette nähtud, et kaebuse koostamisel abistatakse (muu hulgas ka) välismaalasi. Kaebuse esitamise järel peavad avaliku turvalisuse prefektuurikomisjonid tagama, et prefektuuri politseiamet kontrollib fakte, rakendab meetmeid „kooskõlas kontrollimise tulemusega“ ja annab tulemustest teada. Kui komisjon leiab, et kontrollimine on ebapiisav, annab ta kaebuse menetlemiseks juhise, mida prefektuuri politseiamet peab järgima. Saadud aruannetele ja võetud meetmetele tuginedes teavitab komisjon üksikisikut, märkides muu hulgas meetmed, mida on võetud kaebuse lahendamiseks. Riikliku politseiameti teatises rõhutatakse, et kaebuseid tuleks menetleda „siiralt“ ning tulemusest tuleks teatada „sellise aja jooksul, […] mida peetakse sotsiaalseid norme ja mõistlikkust arvestades asjakohaseks“.

(141) Teiseks arvestades, et õiguskaitset tuleb loogiliselt taotleda välisriigis välisriigi süsteemi alusel ja võõrkeeles, siis selleks, et hõlbustada õiguskaitse saamist ELi üksikisikute jaoks, kelle isikuandmed on edastatud Jaapanis asuvatele ettevõtjatele ja kelle isikuandmetele on seejärel avaliku sektori asutused juurde pääsenud, on Jaapani valitsus kasutanud oma volitusi luua konkreetne mehhanism, mida haldab ja mille üle teeb järelevalvet isikuteabe kaitse komisjon, selles valdkonnas kaebuste menetlemiseks ja lahendamiseks. See mehhanism tugineb Jaapani avaliku sektori asutustele APPI alusel pandud koostöökohustusele ja isikuteabe kaitse komisjoni erirollile seoses kolmandatest riikidest rahvusvahelise andmete edastamisega APPI artikli 6 ja aluspoliitika alusel (mille on kehtestanud Jaapani valitsus valitsuse määrusega). Selle mehhanismi üksikasjad on esitatud Jaapani valitsuselt saadud ametlikes seisukohtades, kinnitustes ja kohustustes, mis lisatud käesolevale otsusele II lisana. Mehhanismi suhtes ei kohaldata põhjendatud huvi nõuet ja seda võivad taotleda kõik isikud olenemata sellest, kas isikut ennast kahtlustatakse või süüdistatakse kuriteos või mitte.

(142) Selle mehhanismiga on ette nähtud, et isik, kes kahtlustab, et Jaapani avaliku sektori asutus (sealhulgas kriminaalõiguse täitmise tagamise eest vastutav asutus) on kogunud või kasutanud tema Euroopa Liidust edastatud andmeid ja seejuures rikkunud kohaldatavaid eeskirju, võib esitada kaebuse isikuteabe kaitse komisjonile (isiklikult või oma andmekaitseasutuse kaudu isikuandmete kaitse üldmääruse artikli 51 tähenduses). Isikuteabe kaitse komisjonil on kohustus menetleda kaebust ja teavitada sellest esimese sammuna pädevaid avaliku sektori asutusi, sealhulgas asjaomaseid järelevalveasutusi. Need ametiasutused peavad tegema isikuteabe kaitse komisjoniga koostööd, „sealhulgas esitades vajalikku teavet ja asjakohaseid materjale, mille alusel isikuteabe kaitse komisjon saaks hinnata, kas isikuteabe kogumine või järgnev kasutamine on toimunud kooskõlas kohaldatavate eeskirjadega“ ([117]). APPI artiklist 80 (millega nõutakse Jaapani avaliku sektori asutustelt isikuteabe kaitse komisjoniga koostöö tegemist) tulenev kõnealune kohustus on üldkohaldatav, laienedes seega kõnealuste avaliku sektori asutuste igasugustele uurimistoimingutele, kusjuures need asutused on sellise koostöö tahet kinnitanud asjaomaste ministeeriumide ja ametite juhtide kirjalike avaldustega, nagu on osutatud II lisas.

(143) Kui hinnang näitab, et kohaldatavaid eeskirju on rikutud, „hõlmab asjaomaste avaliku sektori asutuste koostöö isikuteabe kaitse komisjoniga ka kohustust rikkumine kõrvaldada“, mis isikuteabe ebaseadusliku kogumise korral hõlmab ka nende andmete kustutamist. Oluline on see, et kohustust täidetakse isikuteabe kaitse komisjoni järelevalve all, kes „kinnitab enne hindamise lõpuleviimist, et rikkumine on täielikult kõrvaldatud“.

(144) Kui hindamine on lõpetatud, teavitab isikuteabe kaitse komisjon üksikisikut mõistliku aja jooksul hindamise tulemustest, sealhulgas võetud parandusmeetmetest (vajaduse korral). Samal ajal teavitab isikuteabe kaitse komisjon üksikisikut võimalusest küsida pädevalt avaliku sektori asutuselt tulemuse kinnitust ja sellest, millise ametiasutuse poole tuleb tulemuse kinnituse saamiseks pöörduda. Sellise kinnituse, sealhulgas pädeva asutuse otsuse põhjenduste

([115]) „Ebasoodsa asjaolu“ tingimus osutab üksnes sellele, et kaebuse esitaja peab olema politsei tegevusest (või tegevusetusest) isiklikult puudutatud, ega eelda isikult kahju tekkimise tõendamist.

([116]) Need kohustused hõlmavad seaduskuulekust, sh isikuandmete kogumise ja kasutamise õiguslike nõuete järgimist. Vt politseiseaduse artikli 2 lõige 2, artikkel 3.

([117]) Nimetatud hindamisel teeb isikuteabe kaitse komisjon koostööd siseasjade ja teabevahetuse ministeeriumiga, kes võib, nagu selgitatud põhjenduses 136, lasta esitada selgitusi ja materjale ning avaldada arvamusi seoses asjaomase haldusorgani poolt isikuteabe käitlemisega (APPIHAO artiklid 50 ja 51).

saamise võimalus võib aidata üksikisikul astuda edasisi samme, sealhulgas taotleda õiguskaitset. Hindamise tulemuse kohta ei tule esitada kõiki üksikasju, kui on põhjendatud alus arvata, et sellise teabe edastamine seab tõenäoliselt ohtu käimasoleva uurimise.

(145) Kolmandaks, üksikisik, kes ei ole nõus tema isikuandmete saamiseks kohtuniku tehtud arestimisotsusega (määrusega) ([118]) või politsei või prokuratuuri meetmetega selle otsuse täitmisel, võib ta esitada taotluse, et otsus või need meetmed tühistataks või neid muudetaks (CCP artikli 429 lõige 1, artikli 430 lõiked 1 ja 2, telefonikõne pealtkuulamise seaduse artikkel 26) ([119]). Juhul kui asja läbi vaatav kohus leiab, et määrus ise või selle täitmine („arestimismenetlus“) on ebaseaduslik, rahuldab ta taotluse ja annab korralduse arestitud esemed tagastada ([120]).

(146) Neljandaks võib kaudsema kohtuliku kontrolli vormis üksikisik, kes leiab, et tema isikuteabe kogumine kriminaaluurimise osana tema kriminaalprotsessis oli ebaseaduslik, tugineda sellele ebaseaduslikkusele. Kui kohus nõustub, toob see kaasa tõendite välistamise nende vastuvõetamatuse tõttu.

(147) Viimasena tuleks märkida, et riigivastutuse seaduse artikli 1 lõike 1 alusel võib kohus määrata hüvitise, kui riigi ametiisik, kes täidab riigi avalikke volitusi, on oma ametikohustusi täites ebaseaduslikult ja süüliselt (tahtlikult või hooletusest) tekitanud asjaomasele isikule kahju. Riigivastutuse seaduse artikli 4 kohaselt põhineb riigi vastutus kahju eest tsiviilseadustiku sätetel. Selle kohta on tsiviilseadustiku artiklis 710 sätestatud, et vastutus hõlmab ka muud kahju kui varale tekitatud kahju, hõlmates seega moraalset kahju (näiteks „psüühiliste kannatuste“ vormis). Näiteks võib tuua juhud, mil üksikisiku privaatsust on tema isikuteabe ebaseadusliku järelevalve ja/või kogumisega rikutud (nt määruse ebaseaduslik täitmine) ([121]).

(148) Lisaks rahalisele hüvitisele võivad üksikisikud saada teatavatel juhtudel ka esialgset õiguskaitset (nt avaliku sektori asutuste kogutud isikuandmete kustutamine), tuginedes oma privaatsusõigustele põhiseaduse artikli 13 ([122]) alusel.

(149) Kõikide nende õiguskaitsevõimaluste osas tagab Jaapani valitsuse loodud vaidluste lahendamise mehhanism, et üksikisik, kes ei ole endiselt rahul menetluse tulemusega, võib pöörduda isikuteabe kaitse komisjoni poole, „kes teavitab üksikisikut Jaapani õigusnormide alusel õiguskaitse saamise eri võimalustest ja üksikasjalikest menetlustest“. Lisaks isikuteabe kaitse komisjon „toetab üksikisikut, sealhulgas asjaomase haldus- või kohtuorgani poole pöördumisel nõu ja abi pakkumisega“.

(150) See hõlmab kriminaalmenetluse seadustiku kohaste menetlusõiguste kasutamist. Näiteks „kui hindamisel selgub, et üksikisik on kriminaalõiguslikus asjas kahtlustatav, teavitab isikuteabe kaitse komisjon üksikisikut sellest asjaolust“ ([123]), samuti CCP artikli 259 kohasest võimalusest lasta prokuratuuri teavitada, kui ta on otsustanud kriminaalmenetlust mitte algatada. Kui hindamisel selgub, et on algatatud üksikisiku isikuteabega seotud uurimine ja see uurimine on lõpetatud, teavitab isikuteabe kaitse komisjon üksikisikut, et uurimistoimikuga saab tutvuda kooskõlas CCP artikliga 53 (ja lõplike kriminaaltoimikute seaduse artikliga 4). Oma toimikule juurdepääsu saamine on oluline,

([118]) Kaasa arvatud telefonikõne pealtkuulamise määrust, mille puhul on telefonikõne pealtkuulamise seaduses sätestatud konkreetne teavitamise nõue (artikkel 23). Selle sätte kohaselt peab uurimisasutus üksikisikut, kelle teabevahetust on pealt kuulatud (ning seega kellega pealtkuulamise salvestis on seotud), sellest asjaolust kirjalikult teavitama. Teine näide on CCP artikli 100 lõige 3, mille kohaselt peab kohus, kui ta on arestinud süüdistatavale või süüdistatava saadetud postisaadetise või telegrammi, teavitama saatjat või saajat, välja arvatud juhul, kui on oht, et see teatamine takistab kohtumenetlust. CCP artikli 222 lõige 1 sisaldab ristviidet sellele sättele uurimisasutuse läbi viidud läbiotsimisteks või arestimisteks.

([119]) Ehkki selline taotlus ei too automaatselt kaasa arestimisotsuse täitmise peatamist, võib asja läbi vaatav kohus anda korralduse peatamiseks, kuni ta on teinud sisulise otsuse. Vt CCP artikli 429 lõiget 2 ja artiklit 432 koostoimes artikliga 424.

([120]) Vt II lisa jagu II.C.1.

([121]) Vt II lisa jagu II.C.2.

([122]) Vt nt Tokyo ringkonnakohtu 24. märtsi 1988. aasta otsus (nr 2925); Osaka ringkonnakohtu 26. aprilli 2007. aasta otsus (nr 2925). Osaka ringkonnakohtu väitel peavad mitmed tegurid olema tasakaalus, näiteks: i) asjaomase isikuteabe laad ja sisu; ii) selle kogumise viis; iii) üksikisikule tekitatav kahju, kui teavet ei kustutata; ning iv) avalik huvi, sealhulgas avaliku sektori asutusele tekitatav kahju, kui teave kustutatakse.

([123]) Igal juhul peab prokuratuur pärast kriminaalmenetluse algatamist andma süüdistatavale võimaluse nende tõenditega tutvuda (vt CCP artiklid 298–299). Seoses kuriteoohvritega vt CCP artiklid 316–333.

sest see aitab üksikisikul paremini mõista tema suhtes läbi viidud uurimist ning seega valmistada ette lõplik hagi (nt kahjutasude nõudeks), juhul kui ta leiab, et tema andmeid koguti või kasutati ebaseaduslikult.

3.3. **Teabele juurdepääs ja teabe kasutamine Jaapani avaliku sektori asutuste poolt riikliku julgeoleku eesmärgil**

(151) Jaapani ametiasutuste kinnitusel ei ole Jaapanis seadust, mis lubaks sunduslikke teabetaotlusi või „halduslikku telefonikõne pealtkuulamist" muidu kui kriminaaluurimiste puhul. Seega võib riigi julgeoleku kaalutlustel saada teavet üksnes teabeallikast, millele on igaühel vaba juurdepääs, või vabatahtliku teabe avaldamise kaudu. Ettevõtjad, kes saavad taotluse vabatahtlikuks koostööks (elektroonilise teabe avaldamise vormis), ei ole seaduse järgi kohustatud sellist teavet esitama ([124]).

(152) Lisaks on saadud teabe kohaselt ainult neljal valitsusasutusel õigus koguda Jaapani ettevõtjate hoitavat elektroonilist teavet riigi julgeoleku kaalutlustel, nimelt: i) valitsuse luure- ja uurimisametil (CIRO); ii) kaitseministeeriumil (MOD); iii) politseil (nii riiklikul politseiametil ([125]) kui ka prefektuuri politseiametil); ja iv) riigi julgeoleku luureagentuuril (PSIA). Samas ei kogu CIRO kunagi teavet otse ettevõtjatelt, sealhulgas teabevahetuse pealtkuulamise teel. Kui teistest valitsusasutuselt saadakse valitsuse jaoks analüüsi koostamiseks teavet, peavad kõnealused teised ametiasutused omakorda järgima seadust, sealhulgas käesolevas otsuses analüüsitud piiranguid ja kaitsemeetmeid. Tema tegevus ei ole seega andmete edastamise kontekstis oluline.

3.3.1. *Õiguslik alus ja kohaldatavad piirangud/kaitsemeetmed*

(153) Saadud teabe alusel kogub kaitseministeerium (elektroonilist) teavet kaitseministeeriumi asutamise seaduse alusel. Kooskõlas selle artikliga 3 on kaitseministeeriumi ülesanne juhtida ja opereerida sõjaväge ning „teha sellega seotud toiminguid, et tagada riigis rahu ja riigi sõltumatus ning rahva ohutus". Artikli 4 lõikes 4 on sätestatud, et kaitseministeeriumil on pädevus „kaitse ja valve", omakaitsejõudude tegevuse ja sõjaväe kasutamise üle, sealhulgas sellise tegevuse jaoks vajaliku teabe kogumiseks. Tal on õigus koguda ettevõtjatelt (elektroonilist) teavet üksnes nende vabatahtliku koostöö raames.

(154) Prefektuuri politseiameti kohustused ja ülesanded hõlmavad „avaliku turvalisuse ja korra säilitamist" (politseiseaduse artikli 35 lõige 2 koostoimes artikli 2 lõikega 1). Politsei võib oma pädevusalas koguda teavet, aga üksnes vabatahtlikult ja ilma seaduse sunnita. Peale selle peab politsei tegevus „piirduma rangelt" tema ülesannete täitmiseks vajalikuga. Samuti peab ta tegutsema „erapooletult, sõltumatult, eelarvamustevabalt ja õiglaselt" ja ei või kunagi kuritarvitada oma volitusi „selliselt, et see riivab Jaapani põhiseadusega tagatud üksikisiku õigusi ja vabadusi" (vt politseiseaduse artikkel 2).

(155) PSIA võib oma uurimisi läbi viia õõnestustegevuse ärahoidmise seaduse (*Subversive Activities Prevention Act*, edaspidi „SAPA") ning valimatult massimõrvu toimepannud organisatsioonide kontrolli seaduse (*Act on the Control of Organisations Which Have Committed Acts of Indiscriminate Mass Murder*, edaspidi „ACO") alusel, kui sellised uurimised on vajalikud kontrollimeetmete võtmiseks teatavate organisatsioonide suhtes ([126]). Mõlema seaduse alusel võib avaliku julgeoleku kontrolli komisjon PSIA direktori taotlusel välja anda teatavaid „korraldusi" (järelevalve/keelud ACO korral ([127]), peatamised/keelud SAPA ([128]) korral) ning PSIA võib selle raames läbi viia uurimisi ([129]). Kooskõlas saadud teabega viiakse need uurimised alati läbi vabatahtlikult, mis tähendab, et PSIA ei või sundida

([124]) Seepärast võivad ettevõtjad otsustada vabalt koostööst keelduda, riskimata sanktsioonide või muude negatiivsete tagajärgedega. Vt II lisa jagu III.A.1.

([125]) Samas on kooskõlas saadud teabega riikliku politseiameti peamine roll koordineerida eri prefektuuride politseiametite osakondade uurimisi ja vahetada teavet välisriigi ametiasutustega. Ka selles rollis teeb riikliku politseiameti üle järelevalvet riiklik avaliku turvalisuse komisjon, mis vastutab muu hulgas üksikisikute õiguste ja vabaduste kaitse eest (politseiseaduse artikli 5 lõige 1).

([126]) Vt II lisa jagu III.A.1, punkt 3. Nende kahe seaduse vastav kohaldamisala on piiratud, sest SAPAs on viidatud „terroristlikule õõnestustegevusele" ning ACOs „valimatult massimõrva toimepanekut" (mis tähendab SAPA alusel „terroristlikku õõnestustegevust", „mille kaudu suur hulk inimesi mõrvatakse valimatult").

([127]) Vt ACO artiklid 5 ja 8. Järelevalvekorraldus hõlmab ka aruandekohustust meetmest mõjutatud organisatsiooni jaoks. Menetluslike kaitsemeetmete kohta, eelkõige läbipaistvusnõuete ja avaliku julgeoleku kontrolli komisjoni antud eelneva loa kohta vt ACO artiklid 12, 13, 15–27.

([128]) Vt SAPA artiklid 5 ja 7. Menetluslike kaitsemeetmete kohta, eelkõige läbipaistvusnõuete ja avaliku julgeoleku kontrolli komisjoni antud eelneva loa kohta vt SAPA artiklid 11–25.

([129]) VT SAPA artikkel 27 ja ACO artiklid 29 ja 30.

isikuteabe omanikku sellist teavet esitama ([130]). Iga kord viiakse kontroll ja uurimine läbi üksnes kontrolli eesmärgi saavutamiseks vähimal vajalikul vähimal määral ning neid ei viida ühelgi juhul läbi selleks, et piirata „põhjendamatult“ õiguseid ja vabadusi, mis on tagatud Jaapani põhiseadusega (SAPA/ACO artikli 3 lõige 1). Peale selle ei või SAPA/ACO artikli 3 lõike 2 alusel PSIA mingil juhul kuritarvitada sellist kontrolli ega viia läbi uurimisi sellise kontrolli ettevalmistamiseks. Kui riigi julgeoleku luureametnik on talle asjaomase seadusega antud volitusi kuritarvitades sundinud isikut tegema midagi, mida isik ei pea tegema, või takistanud isiku õiguste kasutamist, võidakse tema suhtes kohaldada kriminaalkaristusi SAPA artikli 45 või ACO artikli 42 alusel. Lisaks on mõlemas seaduses sõnaselgelt ette nähtud, et nende sätteid, sealhulgas nendega antud volitusi ei „või mingil juhul laiemalt tõlgendada“ (SAPA/ACO artikkel 2).

(156) Kõikidel juhtudel, mil valitsusel on riigi julgeoleku kaalutlustel andmetele juurdepääs ja mida on kirjeldatud selles punktis, kohaldatakse vabatahtlike uurimiste suhtes Jaapani ülemkohtu poolt ette nähtud piiranguid, mis tähendab, et (elektroonilise) teabe kogumine peab vastama vajalikkuse ja proportsionaalsuse põhimõtetele („asjakohane meetod“) ([131]). Jaapani ametiasutused on sõnaselgelt kinnitanud, et „teabe kogumine ja töötlemine toimub üksnes ulatuses, mis on vajalik pädeva avaliku sektori asutuse konkreetsete ülesannete täitmiseks, samuti konkreetsetest ohtudest lähtudes“. Seetõttu „on välja jäetud riikliku julgeoleku huvides isikuteabe massiline ja valimatu kogumine või sellele juurdepääs“ ([132]).

(157) Samuti kuulub kogutud isikuteave, mida säilitavad avaliku sektori asutused riikliku julgeoleku eesmärgil, APPIHAO kohaldamisalasse ning seega kohaldatakse selle suhtes APPIHAO kohaseid kaitsemeetmeid, mis puutub nende järgnevasse hoidmisse, kasutamisse ja avaldamisse (vt põhjendus 118).

3.3.2. *Sõltumatu järelevalve*

(158) Isikuteabe kogumisel riikliku julgeoleku eesmärgil toimub mitmetasandiline järelevalve valitsuse kolme haru poolt.

(159) Esiteks võib Jaapani parlamendi oma erikomisjonide kaudu kontrollida uurimiste õiguspärasust, tuginedes oma parlamentaarsetele uurimisvolitustele (põhiseaduse artikkel 62, parlamendiseaduse artikkel 104; vt põhjendus 134). Seda järelevalvefunktsiooni toetavad konkreetsed aruandekohustused ülalnimetatud õiguslikul alusel elluviidava tegevuse kohta ([133]).

(160) Teiseks on täidesaatvas harus mitu järelevalvemehhanismi.

(161) Kaitseministeeriumi järelevalvet teeb õigusliku vastavuse peainspektsioon (IGO) ([134]) – kaitseministeeriumi asutamise seaduse artikli 29 alusel asutatud amet, mis kuulub kaitseministeeriumi järelevalve alla (ja annab kaitseministeeriumile oma tegevusest aru), kuid on kaitseministeeriumi operatsioonilistest osakondadest sõltumatu. Õigusliku vastavuse peainspektsiooni ülesanne on tagada vastavus õigusnormidele, samuti kaitseministeeriumi ametnike kohustuste nõuetekohane täitmine. Ta on muu hulgas volitatud tegema nn kaitsekontrolle nii korrapäraselt („korralised kaitsekontrollid“) kui ka üksikjuhtudel („erakorralised kaitsekontrollid“), mis on varem hõlmanud ka isikuteabe nõuetekohast käitlemist ([135]). Selliste kontrollide kontekstis võib IGO siseneda tegevuskohtadesse (kontoritesse) ja nõuda dokumentide või teabe esitamist, sealhulgas selgitusi kaitseministeeriumi aseministri asetäitjalt.

([130]) Vt II lisa jagu III.A.1, punkt 3.

([131]) Vt II lisa jagu III.A.2, punkt b. „Ülemkohtu praktikast järeldub, et ettevõtjale vabatahtliku koostöö taotluse esitamiseks peab selline taotlus olema kuriteokahtluse uurimise jaoks vajalik ja uurimise eesmärgi saavutamise seisukohast mõistlik. Ehkki uurimisasutuste läbi viidud uurimised riigi julgeoleku valdkonnas erinevad uurimistest, mille viivad läbi uurimisasutused õiguskaitse valdkonnas, seoses nii nende õigusliku aluse kui ka eesmärgiga, siis „uurimise jaoks vajalikkuse“ ja „meetodi asjakohasuse“ keskseid põhimõtteid kohaldatakse samamoodi riigi julgeoleku valdkonnas ning neid tuleb järgida, võttes asjakohaselt arvesse iga juhtumi konkreetseid asjaolusid“.

([132]) Vt II lisa jagu III.A.2, punkt b.

([133]) Vt nt SAPA artikkel 36 või ACO artikkel 31 (PSIA puhul).

([134]) Inspektsiooni juht on endine prokurör. Vt II lisa jagu III.B.3.

([135]) Vt II lisa jagu III.B.3. Esitatud näite kohaselt hõlmas 2016. aasta korraline kaitsekontroll „Õiguslikust vastavusest teadlikkuse ja selleks valmisoleku“ väljaselgitamiseks muu hulgas „isikuteabe kaitse seisundit“ (haldamine, hoidmine jne). Tulenev aruanne sisaldas ka näiteid mittenõuetekohase andmehalduse kohta ning selles nõuti sellega seotud parandusi. Kaitseministeerium avaldas aruande oma veebisaidil.

Kontroll viiakse lõpule kaitseministrile esitatava aruandega, milles esitatakse järeldused ja parendusmeetmed (mille rakendamist võib kontrollida edasiste kontrollide käigus). Aruanne alusel annab kaitseminister omakorda juhiseid olukorra lahendamiseks vajalike meetmete rakendamiseks; aseministri asetäitja ülesanne on neid meetmeid ellu viia ja järelmeetmetest aru anda.

(162) Mis puutub prefektuuri politseiametisse, siis on järelevalve tagatud sõltumatute avaliku turvalisuse prefektuurikomisjonide kaudu, nagu on selgitatud põhjenduses 135 kriminaalõiguse täitmise tagamise kohta.

(163) Lisaks, nagu on märgitud, võib PSIA viia läbi uurimisi üksnes määral, mil see on vajalik, et võtta vastu SAPA/ACO kohaseid keelu, peatamis- või järelevalvekorraldusi, ning nende korralduste puhul teeb eelnevat järelevalvet sõltumatu ([136]) avaliku julgeoleku kontrolli komisjon. Lisaks teevad spetsiaalselt nimetatud inspektorid eri osakondade/ametite jne korralisi/perioodilisi kontrolle (mille käigus vaadatakse põhjalikult PSIA tegevust) ([137]) ja erakorralisi sisekontrolle ([138]), mille järel võidakse anda juhiseid asjaomaste osakondade juhtidele jne parandus- või parendusmeetmete võtmiseks.

(164) Need järelevalvemehhanismid, mida tugevdab üksikisikute võimalus algatada isikuteabe kaitse komisjoni kui sõltumatu järelevalveasutuse sekkumine (vt punkt 168), näevad ette piisavad garantiid selle vastu, et Jaapani ametiasutused võivad kuritarvitada oma volitusi riigi julgeoleku valdkonnas, ning elektroonilise teabe ebaseadusliku kogumise vastu.

3.3.3. *Üksikisiku õiguskaitse*

(165) Mis puutub üksikisikute õiguskaitsesse, siis on haldusorganite kogutava ja seega ka „säilitatava“ isikuteabe puhul nendel organitel kohustus sellisel töötlemisel „teha jõupingutusi, et vaadata kaebusi läbi nõuetekohaselt ja kiiresti“ (APPIHAO artikkel 48).

(166) Pealegi erinevalt kriminaaluurimistest on üksikisikutel (sealhulgas välisriigis elavatel välisriigi kodanikel) põhimõtteliselt õigus andmete avaldamisele ([139]), parandamisele (sealhulgas kustutamisele) ning kasutamise/esitamise peatamisele APPIHAO alusel. Seda arvestades võib haldusorgani juht keelduda avaldamast andmeid seoses teabega, „mille puhul on põhjendatud alus […] otsustada, et avaldamine tõenäoliselt kahjustab riigi julgeolekut“ (APPIHAO artikli 14 punkt iv) ning ta võib seda teha isegi sellise teabe olemasolu paljastamata (APPIHAO artikkel 17). Samamoodi kehtib säte, et ehkki üksikisik võib taotleda andmete kasutamise peatamist või andmete kustutamist kooskõlas APPIHAO artikli 36 lõike 1 punktiga i juhul, kui haldusorgan on saanud teabe ebaseaduslikult või säilitab/kasutab seda ulatuslikumal määral kui konkreetse eesmärgi saavutamiseks vaja, võib ametiasutus keelduda taotlusest, kui ta leiab, et kasutamise peatamine „võib tõenäoliselt takistada säilitatud isikuteabe kasutamise eesmärki puutuvate toimingute nõuetekohast täitmist tingituna nimetatud toimingute laadist“ (APPIHAO artikkel 38). Samas kui on võimalik lihtsasti eraldada ja välistada need osad, mille suhtes see erand kehtib, peavad haldusorganid võimaldama vähemalt osalist avaldamist (vt APPIHAO artikli 15 lõige 1) ([140]).

([136]) Avaliku julgeoleku kontrolli komisjoni asutamise seadusega on ette nähtud, et komisjoni esimees ja liikmed „täidavad ülesandeid sõltumatult“ (artikkel 3). Nad nimetab parlamendi mõlema koja nõusolekul ametisse peaminister ja nende ametist vabastamine peab olema „põhjendatud“ (näiteks vangistus, väärkäitumine, vaimne või füüsiline tervisehäire, pankrotimenetluse algatamine).

([137]) Riigi julgeoleku luureagentuuri perioodilise kontrolli määrus (PSIA peadirektori korraldus nr 4, 1986).

([138]) Riigi julgeoleku luureagentuuri erikontrolli määrus (PSIA peadirektori korraldus nr 11, 2008). Erikontrolle tehakse, kui PSIA peadirektor peab seda vajalikuks.

([139]) See viitab õigusele saada koopia „säilitatavast isikuteabest“.

([140]) Vt ka „kaalutlusõigusel põhineva avaldamise“ võimalus isegi juhul, kui „teabe mitteavaldamine“ kuulub „säilitatava isikuteabe“ alla, mille avaldamist taotletakse (APPIHAO artikkel 16).

(167) Igal juhul peab haldusorgan tegema kirjaliku otsuse teatava ajavahemiku jooksul (30 päeva, mida saab teatavatel tingimustel pikendada veel 30 päeva). Kui taotlus lükatakse tagasi, rahuldatakse üksnes osaliselt või üksikisik leiab, et haldusorgani käitumine oli muul põhjusel „ebaseaduslik või ebaõiglane“, võib ta taotleda halduslikku läbivaatamist halduskaebuste läbivaatamise seaduse alusel ([141]). Sel juhul peab kaebust lahendava haldusorgani juht konsulteerima teabe avaldamise ja isikuteabe kaitse läbivaatamise nõukoguga (APPIHAO artiklid 42 ja 43), mis on sõltumatu erinõukogu, mille liikmed nimetab ametisse peaminister parlamendi mõlema koja nõusolekul. Läbivaatamisnõukogu võib kooskõlas saadud teabega viia läbi kontrollimise ([142]) ning lasta selle konkreetse taotlusega haldusorganil esitada säilitatavat isikuteavet, sealhulgas võimalikku salastatud sisu, samuti lisateavet ja -dokumente. Ehkki kaebuse esitajale ja haldusorganile saadetav ja avalikustatav lõpparuanne ei ole õiguslikult siduv, siis peaaegu kõikidel juhtudel seda järgitakse ([143]). Peale selle on üksikisikul võimalus vaidlustada edasikaebeotsus kohtus, tuginedes halduskohtumenetluse seadusele. See võimaldab teha riigi julgeoleku erandi(te) kasutamise õiguslikku kontrolli, sealhulgas kontrollida, kas seda erandit on kuritarvitatud või kas see on endiselt põhjendatud.

(168) Selleks et aidata kaasa ülalnimetatud õiguste kasutamisele APPIHAO alusel, on siseasjade ja teabevahetuse ministeerium loonud 51 „koondteabekeskust“, mis annavad konsolideeritud teavet nende õiguste, taotluse esitamiseks kohaldatava menetluse ja võimalike õiguskaitsevõimaluste kohta ([144]). Mis puutub haldusorganitesse, siis peavad nad esitama „teavet, mis aitab täpsustada säilitatavat isikuteavet“ ([145]) ning võtma „muid piisavaid meetmeid, võttes arvesse selle isiku mugavust, kes kavatseb taotluse esitada“ (APPIHAO artikli 47 lõige 1).

(169) Nagu kriminaalõiguse täitmise tagamise valdkonnas läbi viidud uurimiste korral, võivad ka riigi julgeoleku valdkonnas üksikisikud saada võimaluse õiguskaitseks, võttes otse ühendust isikuteabe kaitse komisjoniga. Seeläbi algatatakse spetsiaalne vaidluste lahendamise menetlus, mille Jaapani valitsus on loonud ELi kodanikele, kelle isikuandmeid edastatakse käesoleva otsuse alusel (vt üksikasjalikud selgitused põhjendustest 141–144 ja 149).

(170) Lisaks võivad üksikisikud taotleda õiguskaitset kahju hüvitamise hagiga riigivastutuse seaduse alusel, mis hõlmab ka moraalset kahju ja teatavatel tingimustel kogutud andmete kustutamist (vt põhjendus 147).

4. JÄRELDUS: EUROOPA LIIDUST JAAPANIS ASUVATELE ETTEVÕTJATELE EDASTATUD ISIKUANDMETE PIISAV KAITSETASE

(171) Komisjon leiab, et APPI, mida täiendavad I lisas esitatud lisaeeskirjad, koos II lisas esitatud ametlike seisukohtade, kinnituste ja kohustustega tagavad Euroopa Liidust edastavate isikuandmete kaitsetaseme, mis on põhimõtteliselt samaväärne määruse (EL) 2016/679 kohaselt tagatud kaitsetasemega.

(172) Lisaks leiab komisjon, et Jaapani õiguses ettenähtud järelevalvemehhanismid ja õiguskaitse võimalused võimaldavad praktikas tuvastada isikuteavet käitlevate ettevõtjate rikkumisi ja nende eest karistada ning pakuvad andmesubjektile õiguskaitsevahendeid temaga seotud isikuandmetele juurdepääsu saamiseks ning vajaduse korral nende parandamiseks või kustutamiseks.

([141]) Halduskaebuste läbivaatamise seadus (2014. aasta seadus nr 160), eelkõige artikli 1 lõige 1.

([142]) Vt teabe avaldamise ja isikuteabe kaitse läbivaatamise nõukogu asutamise seaduse artikkel 9 (2003. aasta seadus nr 60).

([143]) Saadud teabe kohaselt ei ole haldusorgan alates 2005. aastast (kui APPIHAO jõustus) 13 aasta jooksul ja kokku rohkem kui 2000 juhtumi arvestuses aruannet järginud üksnes kahel korral, hoolimata asjaolust, et läbivaatamisnõukogu on haldusotsuseid mitmel korral vaidlustatud. Lisaks peab haldusorgan juhul, kui ta võtab vastu otsuse, millega ta kaldub aruandes esitatud järeldustest kõrvale, seda selgelt põhjendama. Vt II lisa jagu III.C, viidates halduskaebuste läbivaatamise seaduse artikli 50 lõike 1 punktile iv.

([144]) Koondteabekeskused – üks igas prefektuuris – jagavad kodanikele selgitusi nii avaliku sektori asutuste (nt olemasolevates andmebaasides) kogutud isikuteabe kui ka kohaldatavate andmekaitse-eeskirjade (APPIHAO) kohta, sealhulgas selle kohta, kuidas kasutada andmete avaldamise, parandamise või kasutamise peatamise õigust. Ühtlasi toimivad keskused kodanike päringute/kaebuste korral kontaktpunktina. Vt II lisa jagu II.C.4, punkt a.

([145]) Vt ka APPIAHO artiklid 10 ja 11, mis käsitlevad „isikuteabe toimikute registrit“, mis sisaldavad samas laiaulatuslikke erandeid, mis puutub isikuteabe toimikutesse“, mis koostatakse või saadakse kriminaaluurimise eesmärgil või mis sisaldavad küsimusi, mis puudutavad julgeolekut ja muid riigi olulisi huve (APPIHAO artikli 10 lõike 2 punktid i ja ii).

(173) Lisaks leiab komisjon Jaapani õigussüsteemi kohta kättesaadava teabe, sealhulgas II lisas esitatud Jaapani valitsuse seisukohtade, kinnituste ja kohustuste põhjal, et selliste üksikisikute põhiõiguste riivamine Jaapani avaliku sektori asutuste poolt avaliku julgeoleku eesmärgil ning eriti kriminaalõiguse täitmise tagamise ja riikliku julgeoleku eesmärgil, kelle isikuandmeid edastatakse Euroopa Liidust Jaapanisse, piirdub asjaomase seadusliku eesmärgi saavutamiseks rangelt vajalikuga ning tagatud on tõhus õiguskaitse selliste riivete vastu.

(174) Seega arvestades käesoleva otsuse järeldusi, leiab komisjon, et Jaapan tagab Euroopa Liidust Jaapanis asuvatele isikuteavet käitlevatele ettevõtjatele, kelle suhtes kehtib APPI, edastatavate isikuandmete piisava kaitsetaseme, välja arvatud juhtudel, kui saaja kuulu ühte APPI artikli 76 lõikes 1 loetletud kategooriatest ning kõik töötlemise eesmärgid või osad neist vastavad ühele selles sättes ette nähtud eesmärkidest.

(175) Selle põhjal järeldab komisjon, et määruse (EL) 2016/679 artikli 45 kohane piisavuse nõue, tõlgendatuna Euroopa Liidu põhiõiguste hartat ja eelkõige Schremsi kohtuotsust ([146]) arvesse võttes, on täidetud.

5. ANDMEKAITSEASUTUSTE TEGEVUS JA KOMISJONI TEAVITAMINE

(176) Euroopa Kohtu kohtupraktika kohaselt ([147]) ja nagu on tunnustatud määruse (EL) 2016/679 artikli 45 lõikes 4, peaks komisjon pidevalt jälgima asjaomaseid muutuseid kolmandas riigis pärast kaitse piisavuse otsuse vastuvõtmist, et hinnata, kas Jaapan tagab endiselt sisuliselt samaväärse kaitsetaseme. Niisugune kontrollimine on igal juhul nõutav, kui komisjonile laekunud teave tekitab kõnealuse küsimuse suhtes põhjendatud kahtluse.

(177) Seepärast peaks komisjon pidevalt jälgima käesolevas otsuses hinnatud olukorda nii isikuandmete töötlemise õigusraamistiku kui ka tegelike tavade osas, sealhulgas seda, kas Jaapani ametiasutused järgivad II lisas esitatud seisukohti, kinnitusi ja kohustusi. Selle protsessi hõlbustamiseks peaksid Jaapani ametiasutused teavitama komisjoni käesoleva otsuse jaoks olulistest muudatustest nii isikuandmete ettevõtjate poolsel töötlemisel kui ka isikuandmetele juurdepääsul avaliku sektori asutustele kehtestatud piirangute ja seotud tagatistega. See peaks hõlmama kõiki isikuteabe kaitse komisjoni poolt APPI artikli 24 alusel vastu võetud otsuseid, millega tunnistatakse kolmanda riigi tagatav kaitsetase Jaapani tagatava kaitsetasemega samaväärseks.

(178) Pealegi selleks, et komisjonil oleks võimalik tõhusalt täita oma järelevalvefunktsiooni, peaksid liikmesriigid teavitama komisjoni kõikidest asjakohastest meetmetest, mida riigi andmekaitseasutused võtavad, eelkõige seoses ELi andmesubjektide päringute või kaebustega, mis puudutavad isikuandmete edastamist Euroopa Liidust Jaapanis asuvatele ettevõtjatele. Komisjoni tuleks teavitada ka võimalikest märkidest, et kuritegude ennetamise, uurimise, avastamise või nende eest süüdimõistmise või riigi julgeoleku eest vastutavate Jaapani avaliku sektori asutuste tegevus, samuti järelevalveasutuste tegevus ei taga nõutavat kaitsetaset.

(179) Liikmesriigid ja nende organid peavad võtma liidu institutsioonide aktid järgimiseks vajalikud meetmed, kuna eeldatakse nende õiguspärasust ja need tekitavad seega õiguslikke tagajärgi seni, kuni neid ei ole tagasi võetud, tühistamishagi menetlemise tulemusena tühistatud ega eelotsusemenetluse tulemusel või õigusvastasuse väite alusel kehtetuks tunnistatud. Seega on määruse (EL) 2016/679 artikli 45 lõike 3 alusel komisjoni vastu võetud kaitse piisavuse otsus siduv kõikide otsuse adressaadiks olevate liikmesriikide organitele, sealhulgas sõltumatutele järelevalveasutustele. Nagu Euroopa Kohus on selgitanud Schremsi kohtuotsuses ([148]) ja on tunnustatud määruse artikli 58 lõikes 5, peab samas olema liikmesriigi õigusega juhuks, kui andmekaitseasutus kahtleb (sh laekunud kaebuse põhjal) komisjoni piisavusotsuse kooskõlas üksikisiku põhiõigustega eraelu puutumatusele ja andmekaitsele, ette nähtud õiguskaitsevahend, mis võimaldab tal edastada need vastuväited siseriiklikule kohtule, kes kahtluste korral peab menetluse peatama ja esitama Euroopa Kohtule eelotsusetaotluse ([149]).

([146]) Vt joonealune märkus 3.
([147]) Schremsi kohtuotsus, punkt 76.
([148]) Schremsi kohtuotsus, punkt 65.
([149]) Schremsi kohtuotsus, punkt 65: „Sellega seoses on liikmesriigi seadusandja kohustatud ette nägema õiguskaitsevahendid, mis võimaldavad järelevalveasutusel esitada siseriiklikes kohtutes väiteid, mida ta peab põhjendatuks, selleks et kohtud juhul, kui neil on komisjoni otsuse kehtivuse suhtes samasugused kahtlused, esitaksid eelotsusetaotluse kõnealuse otsuse kehtivuse analüüsimiseks“.

6. KAITSE PIISAVUSE OTSUSE KORRAPÄRANE LÄBIVAATAMINE

(180) Kohaldades määruse (EL) 2016/679 artikli 45 lõiget 3 ([150]) ja pidades silmas asjaolu, et Jaapani õiguskorrast tulenev kaitsetase võib muutuda, kontrollib komisjon pärast käesoleva otsuse vastuvõtmist korrapäraselt, kas järeldused Jaapani tagatava kaitse piisava taseme kohta on endiselt faktiliselt ja õiguslikult põhjendatud.

(181) Sel eesmärgil tuleks otsus esimest korda läbi vaadata kaks aastat pärast selle jõustumist. Pärast esimest läbivaatamist otsustab komisjon olenevalt tehtud järeldustest ja tihedas koostöös isikuandmete kaitse üldmääruse artikli 93 lõike 1 alusel asutatud komiteega, kas jätkata läbivaatamist iga kahe aasta tagant. Igal juhul peaksid edasised läbivaatamised toimuma vähemalt iga nelja aasta tagant ([151]). Läbivaatamine peaks hõlmama käesoleva otsuse toimimise kõiki aspekte ning eelkõige lisaeeskirjade kohaldamist (pöörates eritähelepanu edasisaatmisel tagatavale kaitsele), nõusolekueeskirjade kohaldamist, sealhulgas loobumise korral, üksikisiku õiguste kasutamise tulemuslikkust, samuti valitsuse juurdepääsu suhtes kehtestatud piiranguid ja kaitsemeetmeid, sealhulgas käesoleva otsuse II lisas sätestatud õiguskaitsemehhanismi. Samuti peaks see hõlmama järelevalve ja täitmise tagamise tulemuslikkust nii isikuteavet käitlevate ettevõtjate suhtes kohaldatavate kui ka kriminaalõiguse täitmise tagamise ja riigi julgeoleku valdkonna eeskirjade puhul.

(182) Läbivaatamise tegemiseks peaks komisjon kohtuma isikuteabe kaitse komisjoniga ning, kui see on asjakohane, siis teiste Jaapani ametiasutustega, kes vastutavad valitsuse juurdepääsu eest, sealhulgas asjaomaste järelevalveasutustega. Sellel kohtumisel peaks olema lubatud osaleda ka Euroopa Andmekaitsenõukogu liikmete esindajatel. Ühise läbivaatamise raamistikus peaks komisjon laskma isikuteabe kaitse komisjonil esitada põhjalikku teavet piisavuse jaoks oluliste aspektide, sealhulgas valitsuse juurdepääsu suhtes kehtestatud piirangute ja kaitsemeetmete kohta ([152]). Komisjon peaks küsima ka selgitusi igasuguse teabe kohta, mis on käesoleva otsuse puhul oluline ja mida ta on saanud, sealhulgas Jaapani ametiasutuste või muude sidusrühmade, Euroopa Andmekaitsenõukogu, eri andmekaitseasutuste, kodanikuühiskonna rühmade avalike aruannete, meediakajastuste või muude kättesaadavate teabeallikate kohta.

(183) Ühise läbivaatamise alusel peab komisjon koostama avaliku aruande, mis esitatakse Euroopa Parlamendile ja nõukogule.

7. KAITSE PIISAVUSE OTSUSE KEHTIVUSE PEATAMINE

(184) Kui komisjon teeb korrapäraste ja erikontrollide või muu kättesaadava teabe alusel järelduse, et Jaapani õigussüsteemi tagatavat kaitsetaset ei saa enam pidada Euroopa Liidu kaitsetasemega olulisel määral samaväärseks, peab ta teavitama sellest Jaapani pädevaid asutusi ning nõudma, et kindlaksmääratud mõistliku tähtaja jooksul võetakse asjakohaseid meetmeid. See hõlmab eeskirju, mida kohaldatakse nii ettevõtjate kui ka nende Jaapani avaliku sektori asutuste suhtes, kes vastutavad kriminaalõiguse täitmise tagamise või riigi julgeoleku eest. Näiteks algatataks selline menetlus juhtudel, kui (edasi)saatmisel, sh selliste isikuteabe kaitse komisjoni poolt APPI artikli 24 alusel vastu võetud otsuste alusel, millega tunnistatakse kolmanda riigi tagatav kaitsetase Jaapani tagatava kaitsetasemega samaväärseks, ei kasutata enam kaitse jätkumist tagavaid kaitsemeetmeid isikuandmete kaitse üldmääruse artikli 44 tähenduses.

(185) Kui Jaapani pädevad asutused ei ole kindlaksmääratud ajavahemiku jooksul rahuldavalt tõendanud, et käesolev otsus põhineb endiselt piisaval kaitsetasemel, peab komisjon, kohaldades määruse (EL) 2016/679 artikli 45 lõiget 5 algatama menetluse käesoleva otsuse osaliseks või täielikuks peatamiseks või kehtetuks tunnistamiseks. Alternatiivina peaks komisjon algatama menetluse käesoleva otsuse muutmiseks, et eelkõige kehtestada andmete edastamise lisatingimused või piirata kaitse piisavuse otsuse kohaldamisala selliselt, et selle alla kuuluks üksnes andmeedastus, mille puhul on tagatud kaitse jätkumine isikuandmete kaitse üldmääruse artikli 44 tähenduses.

([150]) Määruse (EL) 2016/679 artikli 45 lõikes 3 on sätestatud, et „[r]akendusaktis nähakse ette korrapärase, vähemalt iga nelja aasta tagant toimuva läbivaatamise mehhanism, milles võetakse arvesse kõiki asjaomaseid suundumusi kolmandas riigis või rahvusvahelises organisatsioonis".

([151]) Määruse (EL) 2016/679 artikli 45 lõikes 3 on sätestatud, et korrapärane läbivaatamine peaks toimuma vähemalt nelja aasta tagant. Vt ka Euroopa Andmekaitsenõukogu, piisavuse viitedokument, WP 254 rev. 01.

([152]) Vt ka II lisa jagu IV. „Kaitse piisavuse otsuse korrapärase läbivaatamise raames vahetavad isikuteabe kaitse komisjon ja Euroopa Komisjon teavet andmete töötlemise kohta kaitse piisavuse otsuse tingimuste alusel, sealhulgas käesolevas ülevaates sätestatud tingimuste alusel".

(186) Eelkõige peaks komisjon peaks algatama peatamis- või kehtetuks tunnistamise menetluse siis, kui esineb märke selle kohta, et käesoleva otsuse alusel isikuandmeid saavad ettevõtjad ei täida I lisas esitatud lisaeeskirju ja/või nende lisaeeskirjade täitmine ei ole tulemuslikult tagatud või Jaapani ametiasutused ei järgi käesoleva otsuse II lisas esitatud seisukohti, kinnitusi ja kohustusi.

(187) Komisjon peab kaaluma ka menetluse algatamist käesoleva otsuse muutmiseks, peatamiseks või kehtetuks tunnistamiseks, kui ühist läbivaatamist või muid asjaolusid silmas pidades ei esita Jaapani pädevad asutused teavet või selgitusi, mida on vaja Euroopa Liidust Jaapanisse edastatud isikuandmetele võimaldatava kaitsetaseme hindamiseks või käesoleva otsuse täitmiseks. Sellega seoses peab komisjon võtma arvesse võimalusi saada asjakohast teavet muudest allikatest.

(188) Komisjon peaks kaaluma käesoleva otsuse peatamiseks või kehtetuks tunnistamiseks kooskõlas määruse (EL) 2016/679 artikli 93 lõikega 3 ja koostoimes Euroopa Parlamendi ja nõukogu määruse (EL) nr 182/2011 ([153]) artikliga 8 viivitamata kohaldatava otsuse vastuvõtmist üksnes nõuetekohaselt põhjendatud kiireloomulistel juhtudel, näiteks andmesubjekti õiguste raske rikkumise ohu korral.

8. **LÕPPMÄRKUSED**

(189) Euroopa Andmekaitsenõukogu avaldas arvamuse ([154]), mida on käesoleva otsuse koostamisel arvesse võetud.

(190) Euroopa Parlament on vastu võtnud resolutsiooni digitaalkaubanduse strateegia loomise kohta, kutsudes komisjoni üles seadma kaitse piisavuse otsuste vastuvõtmine prioriteediks ja seda kiirendama oluliste kaubanduspartnerite puhul kooskõlas määruses (EL) 2016/679 sätestatud tingimustega, kui olulise mehhanismi Euroopa Liidust isikuandmete edastamise kaitsmiseks ([155]). Euroopa Parlament on ka vastu võtnud resolutsiooni Jaapani pakutava isikuandmete kaitse piisavuse kohta ([156]).

(191) Käesoleva otsusega sätestatud meetmed on kooskõlas isikuandmete kaitse üldmääruse artikli 93 lõike 1 alusel loodud komitee arvamusega.

ON VASTU VÕTNUD KÄESOLEVA OTSUSE:

Artikkel 1

1. Määruse (EL) 2016/679 artikli 45 kohaldamiseks tagab Jaapan Euroopa Liidust Jaapanis tegutsevatele isikuteavet käitlevatele ettevõtjatele edastatavate isikuandmete piisava kaitsetaseme isikuteabe kaitse seaduse alusel, mida täiendavad I lisas sätestatud lisaeeskirjad ning II lisas esitatud ametlikud seisukohad, kinnitused ja kohustused.

([153]) Euroopa Parlamendi ja nõukogu 16. veebruari 2011. aasta määrus (EL) nr 182/2011, millega kehtestatakse eeskirjad ja üldpõhimõtted, mis käsitlevad liikmesriikide läbiviidava kontrolli mehhanisme, mida kohaldatakse komisjoni rakendamisvolituste teostamise suhtes (ELT L 55, 28.2.2011, lk 13).

([154]) Arvamus 28/2018 Euroopa Komisjoni rakendusotsuse (Jaapani pakutava isikuandmete kaitse piisavuse kohta) eelnõu kohta, vastu võetud 5. detsembril 2018.

([155]) Euroopa Parlamendi 12. detsembri 2017. aasta resolutsioon „Digitaalkaubanduse strateegia loomine“ (2017/2065(INI)). Vt eelkõige punkt 8 („… tuletab meelde, et isikuandmeid võib edastada kolmandatele riikidele, kasutamata üldisi kohustusi kaubanduslepingutes, kui on täidetud – nii praegu kui ka tulevikus – määruse (EL) 2016/679 […] V peatükis sätestatud nõuded; tunnistab, et kaitse piisavuse otsused, sealhulgas osalised ja sektoripõhised otsused, on põhimehhanismid isikuandmete edastamise kaitsmiseks nende edastamise korral ELilt kolmandale riigile; märgib, et EL on võtnud vastu kaitse piisavuse otsused oma 20 suurimast kaubanduspartnerist ainult nelja puhul; ning punkt 9 („kutsub komisjoni üles seadma kaitse piisavuse otsuste vastuvõtmine prioriteediks ja seda kiirendama, tingimusel et kolmandad riigid tagavad oma siseriikliku õiguse või rahvusvaheliste kohustuste alusel kaitsetaseme, mis on ELis tagatud kaitsega „sisuliselt samaväärne“).

([156]) Euroopa Parlamendi 13. detsembri 2018. aasta resolutsioon „Jaapani pakutava isikuandmete kaitse piisavus“ (2018/2979(RSP)).

2. Käesolev otsus ei hõlma isikuandmeid, mida edastatakse saajatele, kes kuuluvad ühte järgmistest kategooriatest, kuivõrd kõik või osad isikuandmete töötlemise eesmärgid vastavad ühele loetletud eesmärkidest, nimelt:

a) ringhäälinguasutused, ajalehtede kirjastused, kommunikatsiooniagentuurid või muud pressiorganisatsioonid (sealhulgas üksikisikud, kes tegelevad oma äritegevuses pressitegevusega) määral, mil nad töötlevad ajakirjanduse eesmärgil isikuandmeid;

b) isikud, kes tegelevad kutselise kirjutamisega määral, mil see hõlmab isikuandmeid;

c) ülikoolid ja muud akadeemilistele õpingutele suunatud organisatsioonid või grupid või sellisesse organisatsiooni või gruppi kuuluvad isikud määral, mil nad töötlevad akadeemiliste õpingute eesmärgil isikuandmeid;

d) usulised organid määral, mil nad töötlevad isikuandmeid usulise tegevuse eesmärgil (sealhulgas kõik seotud tegevused); ning

e) poliitilised organid määral, mil nad töötlevad isikuandmeid oma poliitilise tegevuse eesmärgil (sealhulgas kõik seotud tegevused).

Artikkel 2

Kui liikmesriikide pädevad asutused kasutavad isikute kaitsmiseks seoses nende isikuandmete töötlemisega oma volitusi, mis tulenevad määruse (EL) 2016/679 artiklist 58, mis toob kaasa Jaapanis asuvale konkreetsele ettevõtjale suunduva andmevoo peatamise või lõpliku keelu artiklis 1 sätestatud kohaldamisalas, teavitab asjaomane liikmesriik komisjoni viivitamata.

Artikkel 3

1. Komisjon jälgib pidevalt seda, kuidas kohaldatakse käesoleva otsuse aluseks olevat õigusraamistikku, sealhulgas andmete edasisaatmisel kohaldatavaid tingimusi, et hinnata, kas Jaapan tagab jätkuvalt piisava kaitsetaseme artikli 1 tähenduses.

2. Liikmesriigid ja komisjon teavitavad üksteist juhtudest, mil isikuteabe kaitse komisjon või muu Jaapani pädev asutus ei ole suutnud tagada vastavust käesoleva otsuse aluseks olevale õigusraamistikule.

3. Liikmesriigid ja komisjon teavitavad üksteist kõikidest märkidest, et Jaapani avaliku sektori asutuste poolsed üksikisikute isikuandmete kaitse õiguse riived ületavad rangelt vajalikku ja/või selliste riivete vastu puudub tõhus õiguskaitse.

4. Komisjon hindab kahe aasta jooksul alates käesoleva otsuse liikmesriikidele teatavakstegemisest ning edaspidi vähemalt iga nelja aasta tagant artikli 1 lõikes 1 sätestatud järeldust kogu olemasoleva teabe, sealhulgas koos asjaomaste Jaapani ametiasutustega tehtud ühise läbivaatamise käigus saadud teabe alusel.

5. Kui komisjonil on andmeid, et piisav kaitsetase ei ole enam tagatud, teavitab komisjon Jaapani pädevaid asutusi. Ta võib vajaduse korral otsustada käesoleva otsuse peatada, seda muuta või selle kehtetuks tunnistada või piirata selle kohaldamisala, eelkõige, kui esineb märke, et:

a) Jaapani ettevõtjad, kes on saanud käesoleva otsuse alusel Euroopa Liidust isikuandmeid, ei järgi käesoleva otsuse I lisas esitatud lisaeeskirjades sätestatud täiendavaid kaitsemeetmeid, või sellega seotud järelevalve ja täitmise tagamine on ebapiisav;

b) Jaapani avaliku sektori asutused ei järgi käesoleva otsuse II lisas esitatud seisukohti, kinnitusi ja kohustusi, sealhulgas seoses tingimuste ja piirangutega, mis kehtivad käesoleva otsuse alusel edastatud isikuandmete kogumisele ja neile juurdepääsule Jaapani avaliku sektori asutuste poolt kriminaalõiguse täitmise tagamise või riikliku julgeoleku eesmärgil.

Komisjon võib esitada need esialgsed meetmed ka juhul, kui Jaapani valitsuse koostöö puudumine takistab komisjoni tegema kindlaks, kas käesoleva otsuse artikli 1 lõikes 1 tehtud järeldus on mõjutatud.

Artikkel 4

Käesolev otsus on adresseeritud liikmesriikidele.

Brüssel, 23. jaanuar 2019

Komisjoni nimel
komisjoni liige
Věra JOUROVÁ

1. LISA

ISIKUTEABE KAITSE SEADUSE KOHASED LISAEESKIRJAD, MILLES KÄSITLETAKSE KAITSE PIISAVUSE OTSUSE ALUSEL ELIST EDASTATUD ISIKUANDMETE KÄITLEMIST

Sisukord

[Mõisted]

Seadus	Isikuteabe kaitse seadus (2003. aasta seadus nr 57)
Valitsuse määrus	Valitsuse määrus isikuteabe kaitse seaduse (valitsuse 2003. aasta määrus nr 507) rakendamise kohta
Eeskirjad	Isikuteabe kaitse seaduse rakenduseeskirjad (isikuteabe kaitse komisjoni 2016. aasta eeskiri nr 3)
Üldsuunised	Suunised isikuteabe kaitse seaduse kohta (üldeeskirjade köide) (isikuteabe kaitse komisjoni 2015. aasta teade nr 65)
EL	Euroopa Liit ja selle liikmesriigid ning EMP lepingut silmas pidades ka Island, Liechtenstein ja Norra
Isikuandmete kaitse üldmäärus	Euroopa Parlamendi ja nõukogu määrus füüsiliste isikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise ning direktiivi 95/46/EÜ kehtetuks tunnistamise kohta (isikuandmete kaitse üldmäärus)
Kaitse piisavuse otsus	Euroopa Komisjoni otsus selle kohta, et kolmas riik, kolmanda riigi territoorium vms tagab isikuandmete kaitse piisava taseme vastavalt isikuandmete kaitse üldmääruse artiklile 45

Selleks et isikuandmete edastamine Jaapani ja ELi vahel kulgeks mõlemalt poolt sujuvalt, tunnustas isikuteabe kaitse komisjon ELi sellise isikuteabe kaitse süsteemiga välisriigina, kus kooskõlas seaduse artikliga 24 kehtivad Jaapaniga samaväärsed üksikisiku õiguste ja huvide kaitse nõuded, ning Euroopa Komisjon otsustas samal ajal, et Jaapan tagab isikuandmete kaitse piisava taseme kooskõlas isikuandmete kaitse üldmääruse artikliga 45.

Seega toimub isikuandmete edastamine Jaapani ja ELi vahel mõlemalt poolt sujuvalt ning viisil, millega tagatakse üksikisiku õiguste ja huvide kõrgetasemelise kaitse. Selleks et tagada kaitse piisavuse otsuse alusel ELilt saadud isikuteabe kõrgetasemeline kaitse ning võttes arvesse, et vaatamata kummagi süsteemi suurele sarnasusele leidub nende vahel ka olulisi erinevusi, on isikuteabe kaitse komisjon vastu võtnud käesolevad lisaeeskirjad, mis põhinevad teiste riikide valitsustega tehtavat koostööd jms käsitleva seaduse sätetel, et tagada EList kaitse piisavuse otsuse alusel saadud isikuteabe nõuetekohane käitlemine isikuteavet käitlevate ettevõtjate poolt ning asjakohastes eeskirjades sätestatud kohustuste nõuetekohane ja tõhus rakendamine ([1]).

([1]) Seaduse artiklid 4, 6, 8, 24, 60 ja 78 ning eeskirjade artikkel 11.

Eelkõige on seaduse artiklis 6 sätestatud õigus võtta seadusandlikke ja muid meetmeid isikuteabe kaitse tugevdamiseks ning luua rahvusvaheliselt kokkusobiv isikuteabe käitlemise süsteem, kehtestades seaduse ja valitsuse määruste täiendamiseks neist rangemad eeskirjad. Seepärast on isikuteabe kaitse komisjonil kui seaduse üldise haldamise eest vastutaval asutusel vastavalt seaduse artiklile 6 õigus kehtestada rangemad õigusnormid, sõnastades käesolevad lisaeeskirjad, millega nähakse ette kõrgematasemeline üksikisiku õiguste ja huvide kaitse EList kaitse piisavuse otsuse alusel saadud isikuandmete käitlemisel, sealhulgas seaduse artikli 2 lõike 3 kohase eritähelepanu nõudva isikuteabe ja seaduse artikli 2 lõike 7 kohaste säilitatavate isikuandmete ja nende säilitustähtaja kindlaksmääramisel.

Seda arvesse võttes on lisaeeskirjad siduvad ja kohustuslikud isikuteavet käitlevale ettevõtjale, kes saab EList kaitse piisavuse otsuse alusel isikuandmeid. Kuna kõnealused õigused ja kohustused on õiguslikult siduvad, tagab isikuteabe kaitse komisjon nende täitmise võrdselt seaduse sätetega, mida nad täiendavad rangemate ja/või üksikasjalikumate eeskirjadega. Lisaeeskirjadest tulenevate õiguste ja kohustuste rikkumise võivad üksikisikud kohtusse kaevata samamoodi nagu nende seaduse sätete puhul, mida need täiendavad rangemate ja/või üksikasjalikumate õigusnormidega.

Juhul kui isikuteavet käitlev ettevõtja ei täida üht või mitut lisaeeskirjadest tulenevat kohustust, on isikuteabe kaitse komisjonil nende täitmise tagamiseks õigus võtta meetmeid vastavalt seaduse artiklile 42. Mis puudutab kaitse piisavuse otsuse alusel EList saadud isikuteavet üldiselt, siis juhul, kui isikuteavet käitlev ettevõtja ilma mõjuva põhjuseta ei võta meetmeid vastavalt seaduse artikli 42 lõike 1 kohaselt esitatud soovitusele, ([2]) käsitatakse seda seaduse artikli 42 lõikes 2 määratletud üksikisiku võõrandamatute õiguste ja huvide raske rikkumisena.

1) Eritähelepanu nõudev isikuteave (seaduse artikli 2 lõige 3)

Seaduse artikli 2 lõige 3

3) Seaduses sätestatud „eritähelepanu nõudev isikuteave“ on määratletud kui isikuteave, mis hõlmab volitaja rassi, usutunnistust, sotsiaalset seisundit, haiguslugu, karistusregistri andmeid ja asjaolu, et ta on olnud kuriteos kannatanu, ning muid kirjeldusi jne, mis valitsuse määruse kohaselt on kirjeldused, mille käitlemine nõuab eritähelepanu, et ära hoida volitaja ebaõiglane diskrimineerimine või kahjustamine või tema sattumine muusse ebasoodsasse olukorda.

Valitsuse määruse artikkel 2

Seaduse artikli 2 lõike 3 alusel antud valitsuse määruses sätestatud kirjeldused jms on kirjeldused, mis sisaldavad järgmist (kuid ei sisalda volitaja tervisekaardi ja karistusregistri andmeid):

i) füüsilise, intellekti- või vaimse puude (sealhulgas arengupuude) või muu isikuteabe kaitse komisjoni eeskirjades sätestatud tegutsemist takistava füüsilise ja vaimse puude olemasolu;

ii) arsti või muu tervishoiutöötaja (edaspidi „arst“) poolt volitaja haiguste ennetamiseks ja varaseks avastamiseks määratud tervisekontrolli või muu arstliku läbivaatuse (edaspidi „arstlik läbivaatus“) tulemused;

iii) asjaolu, et arst on volitajale arstliku läbivaatamise vms tulemuste põhjal või haiguse, vigastuse või muu vaimse või füüsilise muutuse tõttu andnud soovitusi vaimse või füüsilise seisundi parandamiseks või osutanud arstiabi või kirjutanud välja retsepti;

iv) asjaolu, et volitaja suhtes on kriminaalmenetluse raames kahtlustatava või süüdistatavana kohaldatud vahistamist, läbiotsimist, kinnipidamist või varade arestimist või tehtud muid toiminguid või talle on esitatud süüdistus;

([2]) Mõjuva põhjusena mõistetakse erakorralist sündmust, mida isikuteavet käitlev ettevõtja ei saa mõjutada ja mida ei ole mõistlikult võimalik ette näha (näiteks loodusõnnetused), või kui seaduse artikli 42 lõike 1 alusel isikuteabe kaitse komisjoni antud soovituse kohaste meetmete võtmise vajadus on kadunud, sest isikuteavet käitlev ettevõtja on võtnud muid meetmeid, mis on rikkumise täielikult heastanud.

v) asjaolu, et volitaja kui alaealiste kaitse seaduse artikli 3 lõikes 1 nimetatud alaealise kurjategija või kuriteos kahtlustatava suhtes on läbi viidud uurimine, ta on võetud jälgimise ja kaitse alla, ta on üle kuulatud või tema suhtes on alaealiste kaitse juhtumi raames langetatud otsus, võetud kaitsemeetmed või tehtud muid toiminguid.

Eeskirjade artikkel 5

Määruse artikli 2 punkti i kohased isikuteabe kaitse komisjoni eeskirjades sätestatud tegutsemist takistavad füüsilised ja vaimsed puuded on järgmised:

i) füüsilised puuded, mis on sätestatud füüsilise puudega inimeste heaolu seaduse (1949. aasta seadus nr 283) liite tabelis;

ii) intellektipuuded, millele on osutatud intellektipuudega inimeste heaolu seaduses (1960. aasta seadus nr 37);

iii) vaimne puue, millele on osutatud vaimse puudega inimeste vaimse tervise ja heaolu seaduses (1950. aasta seadus nr 123) (kaasa arvatud puuetega inimeste toetamise seaduse artikli 2 lõikes 1 nimetatud arengupuuded, kuid välja arvatud intellektipuudega inimeste heaolu seaduses nimetatud intellektipuuded);

iv) haigus, mille puhul ei ole ravimeetodeid kindlaks määratud, ja muud erihaigused, mille raskusaste on vastavalt puuetega inimeste igapäevase ja sotsiaalse elu üldist toetamist käsitleva seaduse (2005. aasta seadus nr 123) artikli 4 lõikel 1 põhinevale valitsuse määrusele samaväärne osutatud lõikel põhinevas tervishoiu, tööjõu ja sotsiaalministri määruses osutatud raskusastmega.

Kui kaitse piisavuse otsuse alusel EList saadud isikuandmed sisaldavad isikuandmete kaitse üldmääruses isikuandmete eriliikidena määratletud andmeid füüsilise isiku seksuaalelu, seksuaalse sättumuse ja ametiühingu liikmesuse kohta, peavad isikuteavet käitlevad ettevõtjad neid isikuandmeid käitlema samal viisil kui seaduse artikli 2 lõike 3 tähenduses eritähelepanu nõudvat isikuteavet.

2) Säilitatavad isikuandmed (seaduse artikli 2 lõige 7)

Seaduse artikli 2 lõige 7

7) „Säilitatavad isikuandmed“ on seaduses määratletud kui isikuandmed, mille sisu isikuteavet käitleval ettevõtjal on õigus avalikustada, parandada, täiendada ja kustutada, mille kasutamise ta võib lõpetada, mille ta võib kustutada ja mille edastamise kolmandatele isikutele ta võib lõpetada, kuid nende andmete hulka ei kuulu sellised valitsuse määruses sätestatud andmed, mille olemasolu või puudumise avalikustamine tõenäoliselt kahjustab avalikke või muid huve, ega ka need valitsuse määruses sätestatud andmed, mis kustutatakse ühe aasta jooksul.

Valitsuse määruse artikkel 4

Valitsuse määruse artikli 2 lõikes 7 sätestatud andmed on järgmised:

i) andmed, mille olemasolu või puudumise teatavaks tegemine võib kahjustada volitaja või kolmanda isiku elu, tervist või varalist seisundit;

ii) isikuandmed, mille olemasolu või puudumise teatavaks tegemine võib julgustada või kallutada ebaseaduslikule või ebaõiglasele teole;

iii) isikuandmed, mille olemasolu või puudumise teatavaks tegemine võib õõnestada riiklikku julgeolekut, hävitada usaldussuhte välisriigi või rahvusvahelise organisatsiooniga või kahjustada läbirääkimisi välisriigi või rahvusvahelise organisatsiooniga;

iv) isikuandmed, mille olemasolu või puudumise teatavaks tegemine võib takistada avaliku turvalisuse ja korra tagamist, näiteks kuriteo ennetamist, peatamist või uurimist.

Valitsuse määruse artikkel 5

Seaduse artikli 2 lõike 7 kohase valitsuse määrusega ettenähtud tähtaeg on kuus kuud.

Kaitse piisavuse otsuse alusel EList saadud isikuandmeid tuleb käsitada säilitatavate isikuandmetena seaduse artikli 2 lõike 7 tähenduses, olenemata tähtajast, mille jooksul need tuleb kustutada.

Neid kaitse piisavuse otsuse alusel EList saadud isikuandmed, mis kuuluvad selliste valitsuse määruses sätestatud isikuandmete hulka, mille olemasolu või puudumise teatavaks tegemine tõenäoliselt kahjustab avalikke või muid huve, ei tule käidelda säilitatavate isikuandmetena (vt valitsuse määruse artikkel 4 ja üldsuuniste punkti 2 alapunkt 7, milles käsitletakse säilitatavaid isikuandmeid.

3) Kasutuseesmärgi kindlaksmääramine, kasutuseesmärgist tulenevad piirangud (seaduse artikli 15 lõige 1, artikli 16 lõige 1 ning artikli 26, lõiked 1 ja 3)

Seaduse artikli 15 lõige 1

1) Isikuteavet käitlev ettevõtja sõnastab isikuteavet käideldes võimalikult selgelt isikuteabe kasutamise otstarbe (edaspidi „kasutusotstarve“).

Seaduse artikli 16 lõige 1

1) Isikuteavet käitlev ettevõtja ei tohi isikuteabe käitlemisel ilma volitaja eelneva nõusolekuta ületada eelmise artikli kohaselt kindlaksmääratud kasutuseesmärgi saavutamiseks vajalikku ulatust.

Seaduse artikli 26 lõiked 1 ja 3

1) Isikuteavet käitlev ettevõtja kontrollib kolmandalt isikult isikuandmete saamisel järgmisi isikuteabe kaitse komisjoni eeskirjades sätestatud asjaolusid: (välja jäetud)

   i) (välja jäetud)

   ii) asjaolud, mille raames nimetatud kolmas isik on need isikuandmed saanud;

3) Isikuteavet käitlev ettevõtja registreerib pärast lõikes 1 nimetatud asjaolude kontrollimist isikuandmete saamise kuupäeva vastavalt isikuteabe kaitse komisjoni eeskirjadele, kontrollimise sisu ja muud isikuteabe kaitse komisjoni eeskirjadega ettenähtud asjaolud.

Kui isikuteavet käitlevad ettevõtjad ületavad isikuteabe käitlemisel seaduse artikli 15 lõike 1 alusel kindlaksmääratud kasutueesmärgi saavutamiseks vajalikku ulatust, peavad nad saama asjaomase volitaja eelneva nõusoleku (seaduse artikli 16 lõige 1). Kolmandalt isikult isikuandmete saamisel kontrollivad isikuteavet käitlevad ettevõtjad kooskõlas eeskirjadega muu hulgas asjaolusid, mille raames nimetatud kolmas isik on need isikuandmed saanud, ning registreerib need asjaolud (seaduse artikli 26 lõiked 1 ja 3).

Isikuteavet käitlev ettevõtja, kes saab kaitse piisavuse otsuse alusel EList isikuandmeid, kontrollib nende saamise asjaolusid ja registreerib need, sealhulgas nende isikuandmete kasutusotstarbe, vastavalt artikli 26 lõigetele 1 ja 3.

Kui isikuteavet käitlev ettevõtja saab varem kaitse piisavuse otsuse alusel EList saadud isikuandmeid teiselt isikuteavet käitlevalt ettevõtjalt, kontrollib ka tema nende isikuandmete saamise asjaolusid ja registreerib need, sealhulgas nende isikuandmete kasutusotstarbe, vastavalt artikli 26 lõigetele 1 ja 3.

Eespool nimetatud juhtudel määrab isikuteavet käitlev ettevõtja nende isikuandmete kasutusotstarbe kindlaks selliselt, et see ei oleks laiem kui see kasutusotstarve, milleks isikuandmed algselt või hiljem saadi ja mis on kontrollitud ja registreeritud vastavalt artikli 26 lõigetele 1 ja 3, ning kasutab neid isikuandmeid ainult nimetatud ulatuses (kooskõlas seaduse artikli 15 lõikega 1 ja artikli 16 lõikega 1).

4) Isikuteabe välisriigis olevale kolmandale isikule edastamise piirangud (seaduse artikkel 24; eeskirjade artikli 11 punkt 2.

Seaduse artikkel 24

Isikuteavet käitlev ettevõtja peab juhul (välja arvatud eelmises artikli lõikes 1 sätestatud juhud), kui isikuandmeid edastatakse kolmandale isikule (v.a isikule, kes on loonud isikuteabe kaitse komisjoni eeskirjadele vastava süsteemi, mille raames on toimingud pidevalt samaväärsed selle isikuteavet käitleva ettevõtja toimingutega isikuteabe käesoleva jao kohase käitlemise käigus; käesolevas artiklis edaspidi sama), kes asub välisriigis (s.t riigis või piirkonnas, mis ei ole Jaapani territoorium; edaspidi sama) (välja arvatud sellise isikuteabe kaitse komisjoni eeskirjade nõuetele vastava isikuteabe kaitse süsteemiga välisriigid, mida tunnustatakse riigina, kus kehtivad Jaapaniga samaväärsed üksikisiku õiguste ja huvide kaitse nõuded; edaspidi käesolevas artiklis sama) saama volitaja eelneva nõusoleku tema andmete edastamiseks välisriigi kolmandale isikule. Sellisel juhul ei kohaldata eelmist artiklit.

Eeskirjade punkti 11 alapunkt 2

Seaduse artikli 24 kohaselt isikuteabe kaitse komisjoni eeskirjadega ettenähtud nõuded peavad liigituma mõne järgmise punkti alla:

i) isikuteavet käitlev ettevõtja ja isikuandmeid saav isik on veendunud, et meetodid, mida isikuandmeid saav isik nende andmete käitlemiseks kasutab, on kooskõlas seaduse IV peatüki 1. jaos sätestatud eesmärgiga isikuandmete käitlemiseks asjakohased ja mõistlikud;

ii) isikuandmeid saav isik on rahvusvahelise isikuteabe käitlemise raamistiku kohase tunnustuse saanud isik.

Kui isikuteavet käitlev ettevõtja, kes edastab välisriigi kolmandale isikule isikuandmeid, mille ta on kaitse piisavuse otsuse alusel saanud EList, peab volitaja andmete edastamiseks välisriigi kolmandale isikule saama volitaja eelneva nõusoleku vastavalt seaduse artiklile 24, olles volitajale eelnevalt teinud teatavaks sellised edastamise asjaolud, mille alusel too saab anda oma nõusoleku, välja arvatud järgmised punktide i–iii kohased juhtumid:

i) kui kolmas isik asub sellises isikuteabe kaitse komisjoni eeskirjade nõuetele vastava isikuteabe kaitse süsteemiga välisriigis, mida tunnustatakse riigina, kus kehtivad Jaapaniga samaväärsed üksikisiku õiguste ja huvide kaitse nõuded;

ii) kui isikuteavet käitlev ettevõtja ja isikuandmeid saav kolmas isik tagavad isikuandmete kolmanda isiku poolse käitlemise puhul ühiselt samaväärse kaitsetaseme, mis vastab seadusele koostoimes käesolevate eeskirjadega, kasutades mõnda asjakohast ja mõistlikku meetodit – lepingut, muud siduvat kokkulepet või ettevõtjate grupi sisest siduvat kokkulepet;

iii) seaduse artikli 23 lõike 1 kõigi punktide kohastel juhtudel.

5) Anonüümselt töödeldav teave (seaduse artikli 2 lõige 9 ning artikli 36 lõiked 1 ja 2)

Seaduse artikli 2 lõige 9

9) „Anonüümselt töödeldav teave“ on seaduses määratletud kui isikuteabe töötlemisel üksikisiku kohta saadud teave, mille alusel ei ole võimalik teha kindlaks üksikisiku isikusamasust üheski järgmistes punktis kirjeldatud viisil, kui isikuteave on jaotatud neis punktides kirjeldatud viisil, ja mille alusel ei ole võimalik isikuteavet taastada.

i) Lõike 1 punkti i kohane isikuteave.

Nimetatud isikuteabes sisalduvate kirjelduste vms osaline kustutamine (sealhulgas kirjelduses vms selle osa asendamine muu kirjeldusega vms, kasutades juhuslikkusel põhinevat meetodit, mida ei saa kasutada nimetatud kirjelduste vms osa taastamiseks).

ii) Lõike 1 punkti ii kohane isikuteave.

Nimetatud isikuteabes sisalduvate identifitseerimiskoodide kustutamine (sealhulgas nende koodide asendamine muu kirjeldusega vms, kasutades juhuslikkusel põhinevat meetodit, mida ei saa kasutada nimetatud identifitseerimiskoodide taastamiseks).

Seaduse artikli 36 lõige 1

1) Teabe muutmisel anonüümselt töödeldavaks teabeks (pidades silmas ainult anonüümselt töödeldava teabe andmebaase jms, edaspidi sama) töötleb isikuteavet käitlev ettevõtja isikuteavet vastavalt isikuteabe kaitse komisjoni eeskirjades sätestatud nõuetele, et teha võimatuks üksikisiku isikusamasuse kindlakstegemine ja anonüümseks muudetud isikuteabe taastamine.

Eeskirjade artikkel 19

Seaduse artikli 36 lõike 1 kohaselt isikuteabe kaitse komisjoni eeskirjadega ettenähtud nõuded peavad liigituma mõne järgmise punkti alla:

i) üksikisiku isikusamasuse kindlakstegemist võimaldavate kirjelduste jms osaline või täielik kustutamine (sealhulgas kirjelduse vms mingi osa asendamine muu kirjeldusega vms, kasutades juhuslikkusel põhinevat meetodit, mida ei saa kasutada nimetatud kirjelduste vms osaliseks või täielikuks taastamiseks);

ii) isikuteabes sisalduvate identifitseerimiskoodide kustutamine (sealhulgas nende koodide asendamine muu kirjeldusega vms, kasutades juhuslikkusel põhinevat meetodit, mida ei saa kasutada nimetatud identifitseerimiskoodide taastamiseks);

iii) isikuteavet ja isikuteabe teatava töötlemise teel saadud teavet ühendavate koodide kustutamine (pidades silmas ainult koode, mis ühendavad omavahel ühe ja sama isikuteavet käitleva ettevõtja käideldavat eri teavet), sealhulgas nende koodide asendamine muude koodidega, mille abil ei saa omavahel seostada isikuteavet ja isikuteabe teatava töötlemise teel saadud teavet, kasutades juhuslikkusel põhinevat meetodit, mida ei saa kasutada nimetatud koodide taastamiseks;

iv) idiosünkraatiliste kirjelduste jms kustutamine (sealhulgas kirjelduste jms asendamine muude kirjeldustega jms, kasutades juhuslikkusel põhinevat meetodit, mida ei saa kasutada idiosünkraatiliste kirjelduste jms taastamiseks;

v) lisaks eelmistes punktides nimetatud toimingutele asjakohaste meetmete võtmine nende tunnuste alusel, mis selgitatakse välja isikuteabe andmebaasi läbivaatamise teel, näiteks isikuteabes olevate kirjelduste ning nimetatud isikuteavet hõlmavas andmebaasis vms sisalduvas muus isikuteabes olevate kirjelduste erinevused.

Seaduse artikli 36 lõige 2

2) Kui isikuteavet käitlev ettevõtja on loonud anonüümselt töödeldavat teavet, peab ta vastavalt isikuteabe kaitse komisjoni poolt vastu võetud lisaeeskirjadega ette nähtud nõuetele, mis on vajalikud selleks, et vältida sellise teabe lekkimist, mis on seotud kirjelduste jms, samuti isikukoodidega, mis kustutati isikuteabest, et luua anonüümselt töödeldav isikuteave, ning samuti sellise teabe lekkimist, mis on seotud eelmise lõike kohase töötlemismeetodiga, võtma meetmeid sellise teabe turvalisuse kontrollimiseks.

Eeskirjade artikkel 20

Seaduse artikli 36 lõikes 2 sätestatud isikuteabe kaitse komisjoni poolt vastu võetud lisaeeskirjadega ette nähtud nõuded on järgmised:

i) määrata täpselt kindlaks sellise isiku volitused ja vastutus, kes käitleb teavet, mis on seotud kirjelduste jms, samuti isikukoodidega, mis kustutati isikuteabest, et luua anonüümselt töödeldav isikuteave, ning teavet, mis on seotud artikli 36 lõike 1 kohase töötlemismeetodiga (piirdudes sellega, millega on võimalik sellise seotud teabe abil isikut tuvastada) (edaspidi „töötlemismeetod ja muu seotud teave“);

ii) kehtestada töötlemismeetodi jms teabe käitlemise eeskirjad ja menetlused, käidelda nõuetekohaselt töötlemismeetodi jms teavet kooskõlas eeskirjade ja menetlustega, hinnata teabe käitlemise olukorda ja võtta hinnangust lähtuvalt vajalikud meetmed olukorra parandamiseks;

iii) võtta vajalikud ja asjakohased meetmed, et isikul, kellel ei ole seadusest tulenevat volitust töötlemismeetodi jms teabe käitlemiseks, ei tekiks võimalust käidelda teavet, mis on seotud töötlemismeetod jms teabega.

Euroopa Liidult kaitse piisavuse otsuse alusel saadud isikuteavet käsitletakse seaduse artikli 2 lõike 9 tähenduses anonüümsena üksnes siis, kui isikuteavet käitlev ettevõtja võtab meetmeid, mis muudavad isiku uuesti tuvastamise igaühe jaoks võimatuks, sealhulgas kustutades töötlemismeetodi jms teabe (st teabe, mis on seotud kirjelduste jms, samuti isikukoodidega, mis kustutati isikuteabest, et luua anonüümselt töödeldav isikuteave, ning teabe, mis on seotud seaduse artikli 36 lõike 1 kohase töötlemismeetodiga (piirdudes sellega, millega on võimalik sellise teabe abil isikut uuesti tuvastada).

LISA 2

Euroopa Komisjoni õigus- ja tarbijaküsimuste ning soolise võrdõiguslikkuse volinik Věra Jourová

Lugupeetud Věra Jourová

Mul on hea meel, et Jaapani ja Euroopa Komisjoni vahel toimuvad konstruktiivsed arutelud, mille eesmärk on luua raamistik isikuandmete vastastikuseks edastamiseks Jaapani ja ELi vahel.

Vastuseks Euroopa Komisjoni poolt Jaapani valitsusele esitatud palvele, on käesolevale kirjale lisatud ülevaade õigusraamistikust, mis käsitleb Jaapani valitsuse juurdepääsu teabele.

Ülevaade hõlmab mitut Jaapani valitsuse ministeeriumi ja ametit ning selles käsitletakse asjaomaseid ministeeriume ja ameteid (valitsuse sekretariaat, riiklik politseiamet, isikuteabe kaitse komisjon, siseasjade ja teabevahetuse ministeerium, justiitsministeerium, riigi julgeoleku luureagentuur, kaitseministeerium), kes sõltuvalt dokumendi sisust, vastutavad oma pädevuse piires nende käitlemise eest. Allpool on loetletud asjaomased ministeeriumid ja ametid ning esitatud vastavad allkirjad.

Kõikide kõnealuse dokumendiga seotud küsimustega võib pöörduda isikuteabe kaitse komisjoni, kes koordineerib vastuste saamist asjaomastelt ministeeriumidelt ja asutustelt.

Loodan, et esitatud dokument on abiks otsuste tegemisel Euroopa Komisjonis.

Hindan kõrgelt Teie suurt panust selles protsessis.

Lugupidamisega

Yoko Kamikawa

Justiitsminister

Dokumendi on koostanud justiitsministeerium koos järgmiste ministeeriumide ja ametitega.

Koichi Hamano

valitsuse sekretariaadi nõunik

Schunichi Kuryu

riigi politseiameti peadirektor

Mari Sonoda

isikuteabe kaitse komisjoni peasekretär

Mitsuru Yasuda

siseasjade ja teabevahetuse aseminister

Seimei Nakagawa

riigi julgeoleku luureagentuur

Kenichi Takahashi

kaitseministri asetäitja

14. september 2018

Isikuteabe kogumine ja kasutamine Jaapani avaliku sektori asutuste poolt kriminaalõiguse täitmise tagamise ja riikliku julgeoleku eesmärkidel

Järgnevas dokumendis on esitatud ülevaade õigusraamistikust, millest Jaapani avaliku sektori asutused peavad lähtuma (elektroonilise) isikuteabe kogumisel ja kasutamisel kriminaalõiguse täitmise tagamise ja riikliku julgeoleku eesmärkidel (edaspidi „valitsuse juurdepääs"), eelkõige on kirjeldatud kehtivat õiguslikku alust, kohaldatavaid tingimusi (piirangud) ja kaitsemeetmeteid, sealhulgas sõltumatu järelevalve teostamist ja individuaalseid õiguskaitsevõimalusi. Ülevaade on adresseeritud Euroopa Komisjonile eesmärgiga väljendada oma pühendumust ja kinnitada, et valitsuse juurdepääs EList Jaapanisse edastatud isikuteabele piirdub sellega, mis on vajalik ja proportsionaalne, ning juurdepääsu üle teostatakse sõltumatut järelevalvet ja asjaomastele isikutele on tagatud õiguskaitse, kui nende põhiõigust eraelu puutumatusele ja andmekaitsele on mis tahes moel rikutud. Ülevaates puudutatakse ka isikuteabe kaitse komisjoni hallatava uue õiguskaitsemehhanismi loomist, et käsitleda ELi üksikisikute kaebusi seoses valitsuse juurdepääsuga EList Jaapanisse edastatud isikuandmetele.

I. **Valitsuse juurdepääsu suhtes kohaldatavad õiguse üldpõhimõtted**

Kuna tegemist on avaliku sektori volituste kasutamisega, peab valitsuse juurdepääs toimuma täielikult õiguspäraselt (õiguspärasuse põhimõte). Jaapanis kaitstakse isikuteavet mitmekihilise mehhanismi abil nii erasektoris kui ka avalikus sektoris.

A. Põhiseaduslik raamistik ja seadusreservatsiooni põhimõte

Põhiseaduse artiklis 13 ja kohtupraktikas tunnustatakse õigust eraelu puutumatusele kui põhiseaduslikku õigust. Sellega seoses on ülemkohus seisukohal, et on loomulik, kui üksikisik ei soovi oma isikuteabe avaldamist kolmandatele isikutele ilma mõjuva põhjuseta ning seda ootust tuleks kaitsta ([1]). Täiendavad kaitsemeetmed on sätestatud põhiseaduse artikli 21 lõikes 2, millega tagatakse sõnumisaladuse austamine, ja põhiseaduse artiklis 35, millega tagatakse õigus, et läbiotsimine ja vara arestimine ei tohi toimuda ilma kohtumääruseta, mis tähendab, et isikuteabe kogumine sunduslike vahendite abil ja juurdepääsu võimaldamine sellele, peab alati põhinema kohtumäärusel. Sellise kohtumääruse võib välja anda ainult juba toime pandud kuriteo uurimiseks. Seega ei ole Jaapani õigusraamistiku kohaselt lubatud koguda sunduslike vahendite abil teavet, mis on vajalik mitte kriminaaluurimise, vaid riikliku julgeoleku seisukohast.

Lisaks peab teabe kogumine sunduslike vahendite abil olema seadusreservatsiooni põhimõtte kohaselt konkreetselt seadusega lubatud. Kui tegemist on andmete mittesundusliku/vabatahtliku kogumisega, siis on teave saadud allikast, mis on vabalt kättesaadav, või vabatahtliku avaldamise taotluse alusel, st taotluse alusel, mida ei saa teavet valdava füüsilise või juriidilise isiku suhtes täitmisele pöörata. See on siiski lubatud üksnes juhul, kui avaliku sektori asutus on pädev uurimist läbi viima, arvestades, et iga avaliku sektori asutus saab tegutseda üksnes talle seadusega ettenähtud halduspädevuse piires (olenemata sellest, kas tema tegevus riivab üksikisikute õigusi ja vabadusi või mitte). See põhimõte kehtib ka asutuse suutlikkuse kohta koguda isikuteavet.

B. Isikuteabe kaitse erieeskirjad

Nii era- kui ka avalikus sektoris on isikuteabega seotud õigused tagatud isikuteabe kaitse seadusega (edaspidi „APPI") ja haldusorganite käsutuses oleva isikuteabe kaitse seadusega (edaspidi „APPIHAO"), mis põhinevad põhiseaduse sätetel ja täiendavad neid.

APPI artiklis 7 on sätestatud, et isikuteabe kaitse komisjon sõnastab isikuteabe kaitse aluspoliitika (edaspidi „aluspoliitika"). Lähtudes Jaapani valitsuskabineti, kui Jaapani keskse valitsusorgani (peaministri ja ministrite) otsusega vastu võetud aluspoliitikast, on kehtestatud suunised isikuteabe kaitse tagamiseks Jaapanis. Sel viisil toimib isikuteabe kaitse komisjon kui sõltumatu järelevalveasutus Jaapani isikuteabe kaitse süsteemi juhtimiskeskusena.

Kui haldusorganid koguvad isikuteavet, siis olenemata sellest, kas nad teevad seda sunduslike vahendite abil või mitte, peavad nad põhimõtteliselt ([2]) täitma APPIHAOs sätestatud nõudeid. APPIHAO on üldseadus, mida haldusorganid kohaldavad säilitatud isikuteabe ([3]) suhtes (nagu on määratletud APPIHAO artikli 2 lõikes 1). Seepärast hõlmab osutatud seadus

([1]) Ülemkohtu 12. septembri 2003. aasta otsus (2002 (Ju) No.1656).
([2]) APPIHAO 4. peatükiga seotud erandite kohta vt lk 16.
([3]) APPIHAO artikli 2 lõike 5 kohaselt on „säilitatud " selline isikuteave, mille on koostanud või mille on saanud haldusorgani töötaja oma tööülesannete täitmise käigus, ning mis on kõnealuse haldusorgani valduses, et töötajad saaksid seda asutuse siseselt kasutada.

ka kriminaalõiguse rakendamise ja riikliku julgeoleku tagamisega seotud andmetöötlust. Valitsusele ettenähtud juurdepääsu isikuteabele saavad kasutada kõik avaliku sektori asutused (välja arvatud prefektuuride politseiametid), mis kuuluvad haldusorgani määratluse alla. Prefektuuride politseiametid lähtuvad isikuteabe käitlemisel prefektuuri määrustest ([4]), milles sätestatakse isikuteabe kaitse põhimõtted, õigused ja kohustused, mis on samaväärsed APPIHAOs sätestatutega.

II. **Valitsuse juurdepääs isikuteabele kriminaalõiguse täitmise tagamise eesmärgil**

A) Õiguslik alus ja piirangud

1) Isikuteabe kogumine sunduslike vahendite abil

a) *Õiguslik alus*

Põhiseaduse artikli 35 kohaselt on igal isikul õigus eeldada, et tema kodu, dokumendid ja vara on kaitstud valdusesse sisenemise, selle läbiotsimise ja vara arestimise vastu ning seda õigust tohib piirata ainult piisavalt põhjendatud juhul väljastatud kohtumäärusega, milles on konkreetselt nimetatud läbiotsimise koht ja arestitav vara. Sellest tulenevalt võivad avaliku sektori asutused koguda kriminaaluurimise kontekstis elektroonilisi andmeid sunduslike vahenditega ainult kohtumääruse alusel. See kehtib nii (isiku)teavet sisaldavate elektrooniliste andmete kogumise kohta, kui ka reaalajas sidevahendite jälgimisel (nt telefonikõnede pealtkuulamine) saadud teabe kohta. Selle eeskirja ainus erand (mis ei puuduta isikuteabe elektroonilist edastamist välismaalt) on kriminaalmenetluse seadustiku ([5]) artikli 220 lõige 1, mille kohaselt võib prokurör, prokuröri abi või kohtupolitsei ametnik kahtlustatava või jõhkra õigusrikkuja vahistamisel, teostada vajaduse korral läbiotsimist ja vara arestimist isiku vahi alla võtmise paigas.

Vastavalt kriminaalmenetluse seadustiku artikli 197 lõikele 1 kohaldatakse uurimisel sunnimeetmeid üksnes juhul, kui see on ette nähtud seadustiku erisätetega. Sunduslike vahendite abil elektroonilise teabe kogumise õiguslik alus on kriminaalmenetluse seadustiku artikli 218 lõige 1 (mille kohaselt võib prokurör, prokuröri abi või kohtupolitsei ametnik, kui see on vajalik õigusrikkumise uurimiseks, teostada läbiotsimist, vara arestimist või kontrollimist kohtuniku väljastatud kohtumääruse alusel) ja artikli 222 lõige 2 (mille kohaselt peab elektroonilise side pealtkuulamine sunduslike vahendite abil ilma kummagi poole nõusolekuta toimuma muu seaduse alusel). Viimati nimetatud sätte puhul viidatakse kriminaaluurimise eesmärgil telefonikõne pealtkuulamise seadusele (edaspidi „telefonikõne pealtkuulamise seadus“), mille artikli 3 lõikes 1 on sätestatud tingimuste kohaselt võib teatavate raskete kuritegudega seotud telefonikõnesid pealt kuulata kohtuniku antud pealtkuulamismääruse alusel ([6]).

Uurimispädevus on kõikide juhtumite puhul prefektuuri politseiametil ning riiklik politseiamet kriminaalmenetluse seadustiku kohaseid kriminaaluurimisi ei teosta.

b) *Piirangud*

Vastavalt kohtupraktika tõlgendusele tuleb elektroonilise teabe kogumisel sunduslike vahendite abil võtta arvesse piiranguid, mis tulenevad põhiseadusest ja õigusaktist, millega antakse volitus, ning milles on eelkõige sätestatud kriteeriumid, millest kohtud peavad lähtuma kohtumääruse väljaandmisel. Lisaks on APPIHAOs sätestatud arvukalt piiranguid, mida kohaldatakse nii teabe kogumise kui ka töötlemise suhtes (kohalike määrustega on prefektuuri politseiameti suhtes kehtestatud sisuliselt samad kriteeriumid.).

1) Piirangud, mis tulenevad põhiseadusest ja õigusaktist, millega volitus antakse.

Kooskõlas kriminaalmenetluse seadustiku artikli 197 lõikega 1 kohaldatakse sunnivõimalusi üksnes juhul, kui seadustikuga on kehtestatud erisätted. Kriminaalmenetluse seadustiku artikli 218 lõikes 1 on sätestatud, et kohtuniku välja antud määruse alusel võib vara arestida vms ainult juhul, kui see on vajalik õigusrikkumise uurimiseks. Kuigi vajalikkuse

([4]) Igal prefektuuril on oma prefektuuri määrus, mida prefektuuri politseiamet kohaldab isikuteabe kaitse suhtes. Kõnealuseid prefektuuri määrusi ei ole inglise keelde tõlgitud.

([5]) Kriminaalmenetluse seadustiku artikli 220 lõikes 1 on sätestatud, et prokurör, prokuröri abi või kohtupolitsei ametnik võib kahtlustatava vahistamisel võtta vajaduse korral järgmisi meetmeid: a) siseneda teise isiku eluruumi vms kahtlustatava isiku otsimiseks; b) teostada läbiotsimist, vara arestimist või kontrollimist isiku vahi alla võtmise paigas.

([6]) Täpsemalt on selle sättega ette nähtud, et sellisel juhul ja olukorras, kui on piisav kahtlus, et suhtlus puudutab edasise tegevuse kokkuleppimist ja ettevalmistamist, vandenõu, näiteks tõendite eemaldamist jms, juhiseid ja seoseid mõne eelneva kuriteoga (edaspidi teise ja kolmanda kuriteo puhul „kuritegude seeria“), samuti teavet kõnealuse kuriteoga seotud üksikasjade kohta (edaspidi käesolevas lõikes „kuriteoga seotud teave“), ning juhul, kui kurjategijat või kuriteo toimepanemise olukorda/üksikasju on mis tahes muul viisil väga keeruline kindlaks teha, siis võib prokurör või kohtupolitsei ametnik kuriteoga seotud suhtlust pealt kuulata, kui see toimub kohtuniku poolt väljastatud pealtkuulamismääruse kohaselt, ning seda tehakse sidevahendis, mille kohta on pealkuulamismääruses esitatud telefoninumber ja muud numbrid/koodid, et tuvastada helistaja ja kõne vastuvõtja, ning mida kahtlustatav kasutab telekommunikatsioonifirmaga sõlmitud lepingu alusel (välja arvatud sidevahendid, mille võib kõrvale jätta, kuna puudub kahtlus, et neid kasutatakse kuriteoga seotud teabe edastamiseks) või sidevahendis, mille puhul on alust kahtlustada, et seda kasutatakse kuriteoga seotud teabe edastamisel.

hindamise kriteeriume ei ole seaduses täiendavalt täpsustatud, on ülemkohus ([7]) otsustanud, et kohtumääruse vajaduse hindamisel peaks kohtunik lähtuma üldhinnangust ja võtma arvesse eelkõige järgmisi asjaolusid:

a) õigusrikkumise raskus ja toimepanemise viis;

b) konfiskeeritud asitõendite kui tõendusmaterjali väärtus ja tähtsus;

c) konfiskeeritud asitõendite varjamise või hävitamise tõenäosus;

d) vara arestimisega kaasneva ebasoodsa olukorra ulatus;

e) muud asjaomased tingimused.

Piirangud tulenevad ka põhiseaduse artikli 35 nõudest osutada piisavale põhjusele. Vastavalt piisava põhjuse põhimõttele võib kohtumääruse välja anda, kui [1] on vaja viia läbi kriminaaluurimine (vt ülemkohtu eespool nimetatud 18. märtsi 1969. aasta otsus (1968 (Shi) nr 100)), [2] on olukord, kus kahtlustatavat (süüdistatavat) käsitatakse õigusrikkumise toimepanijana (kriminaalmenetluse eeskirjade artikli 156 lõige 1) ([8]). [3] Kohtumäärus, millega lubatakse otsida läbi isikuid, vara, eluruume ja muud valdusi ning isikuid, kes ei ole süüdistatavad, tuleks välja anda ainult siis, kui on alust arvata, et on olemas vara, mida tuleks arestida (kriminaalmenetluse seadustiku artikli 102 lõige 2). Kui kohtunik leiab, et lähtudes uurimisasutuse esitatud dokumentaalsetest tõenditest puudub piisav alus kuritegu kahtlustada, lõpetab ta määruse taotluse. Sellega seoses tuleb märkida, et kooskõlas seadusega, milles käsitletakse karistamist organiseeritud kuritegevuse ja kuritegelikul teel saadud tulu korral, on kavandatud kuritegu ettevalmistav tegevus (nt rahaliste vahendite kogumine terrorismi kuriteo toimepanemiseks) samuti kuritegu ja selle suhtes võidakse algatada kohtumäärusel põhinev sunduslik uurimine.

Kui kohtumäärus on seotud isikuga, kes ei ole kahtlustatav või süüdistatav, tema vara, elukoha või muu valdusega, antakse kohtumäärus välja ainult siis, kui on võimalik põhjendatult eeldada, et vara, mida tahetakse arestida, on olemas (kriminaalmenetluse seadustiku artikli 102 lõige 2 ja artikli 222 lõige 1).

Telefonikõnede pealtkuulamise seaduse kohaselt võib telefonikõnesid kriminaaluurimise eesmärgil pealt kuulata üksnes siis, kui on täidetud artikli 3 lõikes 1 sätestatud ranged nõuded. Selle sätte kohaselt peab pealtkuulamine toimuma alati kohtumääruse alusel, mida võib anda vaid piiratud juhtudel ([9]).

2) Piirangud, mis tulenevad APPIHAOst.

Seoses isikuteabe kogumise ([10]) ja edasise käitlemisega (sealhulgas isikuteabe säilitamine, haldamine ja kasutamine) haldusorganite poolt, on APPIHAOs sätestatud eelkõige järgmised piirangud:

a) APPIHAO artikli 3 lõike 1 kohaselt võivad haldusorganid säilitada isikuteavet ainult juhul, kui säilitamine on vajalik nende pädevusse kuuluvate ülesannete täitmiseks, nagu on ette nähtud õigus- ja haldusnormidega. Peale selle peavad nad (nii täpselt kui võimalik) kindlaks määrama isikuteabe kasutamise eesmärgi. Vastavalt APPIHAO artikli 3 lõigetele 2 ja 3 ei säilita haldusorganid isikuteavet, mis läheb kaugemale sellest, mis on vajalik sel viisil kindlaksmääratud kasutuseesmärgi saavutamiseks, ega muuda kasutuseesmärki rohkem, kui saab mõistlikult asjakohaseks pidada esialgse eesmärgi seisukohast.

b) APPIHAO artiklis 5 on sätestatud, et haldusorgani juht püüab saavutada, et säilitatud isikuteave on täpne ja ajakohastatud kasutuseesmärgi saavutamiseks vajalikus ulatuses.

c) Vastavalt APPIHAO artikli 6 lõikele 1 võtab haldusorgani juht vajalikud meetmed, et ennetada teabe lekkimist, kaotsiminekut või kahjustumist ning tagada säilitatud isikuteabe nõuetekohane haldamine.

d) APPIHAO artikli 7 kohaselt ei tohi töötaja (sh endine töötaja) omandatud isikuteavet avaldada põhjendamatult teisele isikule või kasutada sellist teavet ebaõigel eesmärgil.

([7]) 18. märtsi 1969. aasta otsus (1968 (Shi) nr 100).

([8]) Kriminaalmenetluse eeskirjade artikli 156 lõikes 1 on sätestatud: „Eelmise artikli lõikes 1 sätestatud taotluse puhul esitab taotleja materjalid, mille alusel tuleks kahtlustatavat või süüdistatavat pidada õigusrikkumise toimepanijaks."

([9]) Vt joonealune märkus 6.

([10]) APPIHAO artikli 3 lõigetes 1 ja 2 on sätestatud piirangud isikuteabe säilitamise ulatuse ja seega ka isikuteabe kogumise suhtes.

e) Lisaks on APPIHAO artikli 8 lõikes 1 sätestatud, et kui õigusnormidega ei ole ette nähtud teisiti, ei või haldusorgani juht kasutada säilitatud isikuteavet või anda seda teisele isikule muul eesmärgil, kui ettenähtud kasutuseks. Kuigi artikli 8 lõikega 2 on ette nähtud, et teatud olukordades saab sellest reeglist teha erandi, kohaldatakse seda üksnes siis, kui erakorraline avalikustamine ei põhjusta tõenäoliselt ebaõiglast kahju andmesubjekti või kolmanda isiku õigustele ja huvidele.

f) Kui säilitatud isikuteavet antakse teisele isikule, määrab haldusorgani juht vastavalt APPIHAO artiklile 9 vajaduse korral piirangud eesmärgi või kasutusviisi suhtes või muud vajalikud piirangud; ta võib ka nõuda, et vastuvõttev isik võtaks meetmed, mis on vajalikud teabe lekkimise vältimiseks ja teabe nõuetekohaseks haldamiseks.

g) APPIHAO artiklis 48 on sätestatud, et haldusorgani juht püüab saavutada, et kõik kaebused, mis on seotud isikuteabe nõuetekohase ja kiire käitlemisega, saaksid läbi vaadatud.

2) Isikuteabe kogumine vabatahtliku koostöö taotluste kaudu (vabatahtlik uurimine)

a) *Õiguslik alus*

Lisaks sunduslikele vahenditele saadakse isikuteavet kas vabalt juurdepääsetavast allikast või kui seda vabatahtlikult avalikustatakse, sealhulgas sellist teavet valdavate ettevõtjate poolt.

Viimati nimetatu puhul on kriminaalmenetluse seadustiku artikli 197 lõikega 2 antud prokurörile ja kohtupolitsei ametnikule volitus kirjalike uurimisalaste järelepärimiste esitamiseks (nn järelepärimised). Kriminaalmenetluse seadustiku kohaselt nõutakse, et järelepärimisi teinud isikud annaksid sellest uurimisasutustele teada. Siiski ei ole võimalik neid teatama sundida, kui avaliku sektori asutused või avalikud ja/või eraorganisatsioonid, kes järelepärimise said, keelduvad teatamisest. Kui nad ei esita järelepärimiste kohta aruannet, ei saa kohaldada ei kriminaal- ega muud karistust. Kui uurimisasutused leiavad, et nõutav teave on hädavajalik, peavad nad hankima teavet kohtumääruse alusel toimuva läbiotsimise ja vara arestimise kaudu.

Võttes arvesse üksikisikute kasvavat teadlikkust seoses nende privaatsusõigustega, samuti selliste taotlustega tekitatud töökoormust, on ettevõtjad sellistele taotlustele vastates aina ettevaatlikumad ([11]). Selleks et otsustada, kas teha koostööd, võtavad ettevõtjad eelkõige arvesse nõutava teabe laadi, suhet isikuga, keda teave puudutab, ohtu mainele, kohtuvaidlustega seotud riske jne.

b) *Piirangud*

Mis puudutab sunduslikku elektroonilise teabe kogumist, siis piirab vabatahtlikku uurimist põhiseadus, nagu seda on tõlgendatud kohtupraktikas, ja volitusi andev seadus. Lisaks ei ole ettevõtjatel seaduse järgi lubatud teatavates olukordades teavet avaldada. Ka APPIHAO näeb ette hulga piiranguid, mis kehtivad nii teabe kogumise kui ka selle käitlemise suhtes (samas kui kohalikud määrused kordavad sisuliselt samu kriteeriume prefektuuride politseiametite jaoks).

1) Põhiseadusest ja volitusi andvast seadusest tulenevad piirangud

Võttes arvesse põhiseaduse artikli 13 eesmärke, kehtestas ülemkohus kahes otsuses – 24. detsembri 1969. aasta otsuses (1965 (A) No.1187) ja 15. aprilli 2008. aasta otsuses (2007 (A) No.839) – uurimisorganite läbiviidavatele vabatahtlikele uurimistele piirangud. Kuigi need otsused käsitlesid juhtumeid, kus isikuteavet (fotosid) koguti pildistamise/filmimise teel, on järeldused asjakohased ka vabatahtlike (mittekohustuslike) uurimiste puhul, mis riivavad isiku eraelu puutumatust üldiselt. Seetõttu tuleb neid otsuseid kohaldada ja järgida ka isikuteabe kogumisel vabatahtlike uurimiste käigus, võttes arvesse iga juhtumi konkreetseid asjaolusid.

Nende otsuste kohaselt sõltub vabatahtliku uurimise õiguspärasus sellest, kas on täidetud kolm kriteeriumi:

— „kuriteo kahtlus“ (st tuleb hinnata, kas on toime pandud kuritegu),

— „uurimise vajalikkus“ (st tuleb hinnata, kas taotlus jääb uurimise jaoks vajaliku piiresse), ning

([11]) Vt ka riikliku politseiameti teatis 7. detsembril 1999 (allpool punktis 9), milles on kinnitatud sama.

— „meetodite asjakohasus“ (st tuleb hinnata, kas vabatahtlik uurimine on uurimise eesmärgi saavutamiseks „asjakohane“ või mõistlik) ([12]).

Arvestades eespool nimetatud kolme kriteeriumi, hinnatakse vabatahtliku uurimise õiguspärasust üldiselt sellest vaatenurgast, kas seda võib ühiskondlikult aktsepteeritavate tavade kohaselt pidada mõistlikuks.

Nõue, et uurimine peab olema „vajalik“, tuleneb ühtlasi otseselt kriminaalmenetluse seadustiku artiklist 197 ja seda on kinnitatud ka korraldustes, mida riiklik politseiamet (NPA) on andnud prefektuuride politseiametitele „päringuvormide“ kasutamise kohta. NPA 7. detsembri 1999. aasta teatises on ette nähtud mitu menetluslikku piirangut, sealhulgas nõue kasutada „päringuvorme“ ainult juhul, kui see on vajalik uurimiseks. Lisaks piirdub kriminaalmenetluse seadustiku artikli 197 lõige 1 kriminaaluurimisega ja seega saab seda kohaldada ainult juhul, kui on olemas konkreetne kahtlustus juba toime pandud kuriteos. Õigusliku alusena ei saa sellele aga tugineda isikuteabe kogumiseks ja kasutamiseks juhtudel, kui õigusrikkumist ei ole veel toime pandud.

2) Teatavate ettevõtjate suhtes kehtivad piirangud

Teatavates valdkondades kohaldatakse täiendavaid piiranguid, mis põhinevad muudes õigusaktides sätestatud kaitsemeetmetel.

Esiteks on uurimisorganitel ja isikuteavet omavatel telekommunikatsiooniettevõtjatel kohustus austada sõnumisaladust, mis on tagatud põhiseaduse artikli 21 lõikega 2 ([13]). Telekommunikatsiooniettevõtjatel on sama kohustus ka telekommunikatsiooniseaduse artikli 4 alusel ([14]). Vastavalt „Telekommunikatsioonivaldkonna isikuandmete kaitse juhendile“, mille sise- ja kommunikatsiooniministeerium (MIC) andis välja põhiseaduse ja telekommunikatsiooniseaduse alusel, ei tohi telekommunikatsiooniettevõtjad juhul, kui on tegemist sõnumisaladusega, avaldada sõnumisaladuse alla kuuluvat isikuteavet kolmandatele isikutele, välja arvatud juhul, kui nad on saanud selleks isiku nõusoleku või kui nad saavad tugineda ühele „õigustatud alustest“, mille korral võib karistusseadustikku mitte järgida. Viimased on „õigustatud teod“ (karistusseadustiku artikkel 35), „hädakaitse“ (karistusseadustiku artikkel 36) ja „hädaseisund“ (karistusseadustiku artikkel 37). „Õigustatud teod“ on karistusseadustiku järgi ainult sellised telekommunikatsiooniettevõtja teod, millega ta täidab riigi kohustuslikke meetmeid, ning see välistab vabatahtliku uurimise. Seega kui uurimisasutused nõuavad „päringuvormile“ tuginedes isikuteavet (kriminaalmenetluse seadustiku artikli 197 lõige 2), on telekommunikatsiooniettevõtjal keelatud andmeid avaldada.

Teiseks on ettevõtjad kohustatud vabatahtliku koostöö taotlused tagasi lükkama, kui neil on seadusega keelatud isikuteavet avaldada. Siia kuuluvad näiteks juhtumid, kus ettevõtjal on kohustus austada teabe konfidentsiaalsust, näiteks karistusseadustiku artikli 134 kohaselt ([15]).

3) APPIHAO-l põhinevad piirangud

Isikuteabe kogumise ja edasise käitlemise suhtes haldusorganite poolt on APPIHAOs ette nähtud piirangud, nagu on selgitatud II jao A osa punkti 1 alapunkti b lõikes 2. Samaväärsed piirangud tulenevad ka prefektuuride määrustest, mis kehtivad prefektuuride politseiametite suhtes.

B) Järelevalve

1) Kohtulik järelevalve

Isikuteabe kogumine sunduslike vahenditega peab põhinema kohtu määrusel ([16]) ning seega peab kohtunik selle eelnevalt läbi vaatama. Kui uurimine on olnud ebaseaduslik, võib kohtunik kriminaalasja kohtuliku arutamise käigus need tõendid kõrvale jätta. Isik võib taotleda, et tõendid tema kriminaalmenetluses kõrvale jäetaks, väites, et uurimine oli ebaseaduslik.

([12]) Kuriteo raskusaste ja asja kiireloomulisus on „meetodite asjakohasuse“ hindamisel kohased tegurid.

([13]) Põhiseaduse artikli 21 lõikes 2 on sätestatud: „Igasugune tsensuur on keelatud ja sõnumisaladuse rikkumine, olenemata sidevahendist, on samuti keelatud.“

([14]) Telekommunikatsiooniseaduse artiklis 4 on sätestatud: „1) Telekommunikatsiooniettevõtja käideldavate sõnumite saladust ei rikuta. 2) Isikul, kes tegutseb telekommunikatsiooniäris, on keelatud avaldada talle töö käigus teatavaks saanud saladusi, mis on seotud telekommunikatsiooniettevõtja käideldavate sõnumitega. Sama kehtib ka siis, kui ta on ametist lahkunud.“

([15]) Karistusseadustiku artiklis 134 on sätestatud: „1) Kui arst, farmatseut, proviisor, ämmaemand, advokaat, kaitsja, notar või mõni muu isik, kes varem on tegutsenud sellisel kutsealal, avaldab ilma seadusliku aluseta teise isiku kohta konfidentsiaalse teabe, mis on talle teatavaks saanud sellel kutsealal tegutsedes, karistatakse teda kuni 6 kuu pikkuse vangistusega koos töötamisega või kuni 100 000 jeeni suuruse trahviga. 2) Sama kehtib juhul, kui isik, kes tegutseb või on varem tegutsenud religioossel tegevusalal, avaldab ilma seadusliku aluseta teise isiku kohta konfidentsiaalse teabe, mis on talle teatavaks saanud sellel kutsealal tegutsedes.“

([16]) Erandit sellest reeglist on kirjeldatud joonealuses märkuses 5.

2) APPIHAO-l põhinev järelevalve

Jaapanis on ministril või iga ministeeriumi või ameti juhil APPIHAO alusel järelevalve ja õiguskaitse tagamise volitus, samas kui sise- ja kommunikatsiooniminister võib uurida APPIHAO nõuete täitmist kõikides teistes ministeeriumides.

Kui sise- ja kommunikatsiooniminister peab seda vajalikuks, et saavutada APPIHAO eesmärgid – lähtudes näiteks APPIHAO täitmise seisu käsitlenud uurimisest ([17]), kaebuste menetlemisest või mõnele tema koondteabekeskusele saadetud päringust –, võib ta paluda haldusorgani juhil esitada APPIHAO artikli 50 alusel materjalid ja selgitused isikuteabe käitlemise kohta asjaomases haldusorganis. Minister võib adresseerida haldusorgani juhile arvamusi isikuteabe töötlemise kohta haldusorganis, kui ta leiab, et see on nimetatud seaduse eesmärgi saavutamiseks vajalik. Lisaks võib minister paluda meetmed läbi vaadata, tegutsedes nimetatud seaduse artiklite 50 ja 51 alusel, kui kahtlustatakse seaduse rikkumist või sobimatut tegutsemist. See aitab tagada APPIHAO ühetaolise kohaldamise ja järgimise.

3) Avaliku turvalisuse komisjonide järelevalve politsei üle

NPA üle teostab järelevalvet riiklik avaliku turvalisuse komisjon, samas kui iga prefektuuri politseiameti üle teostab järelevalvet selle prefektuuri avaliku turvalisuse komisjon. Kõik need järelevalveorganid kindlustavad politseiameti demokraatliku juhtimise ja poliitilise neutraalsuse.

Riiklik avaliku turvalisuse komisjon vastutab politseiseaduse ja muude seaduste kohaselt tema pädevusse kuuluvate küsimuste eest. Nende küsimuste hulka kuulub NPA ülemvoliniku ja kohalike kõrgemate politseiametnike ametisse nimetamine ning tervikliku poliitika väljatöötamine, milles nähakse ette NPA juhtimise põhisuunised või -meetmed.

Prefektuuride avaliku turvalisuse komisjonid koosnevad politseiseaduse alusel selle prefektuuri elanikkonda esindavatest liikmetest ja juhivad prefektuuri politseiametit sõltumatu nõukoguna. Liikmed määrab prefektuuri kuberner prefektuuri assamblee nõusolekul, lähtudes politseiseaduse artiklist 39. Nende ametiaeg on kolm aastat ja neid võib nende tahte vastaselt ametist vabastada ainult seaduses loetletud erijuhtudel (näiteks suutmatus täita oma kohustusi, kohustuste rikkumine, väärkäitumine jne), mis tagab nende sõltumatuse (vt politseiseaduse artiklid 40 ja 41). Et tagada komisjoniliikmete poliitilist neutraalsust, on neil politseiseaduse artikli 42 alusel keelatud olla samal ajal seadusandliku organi liige, olla erakonna või mõne muu poliitilise organi juhtkonna liige või osaleda aktiivselt poliitilises liikumises. Kuigi iga komisjon kuulub vastava prefektuuri kuberneri jurisdiktsiooni alla, ei tähenda see, et kuberneril oleks volitus anda komisjonile juhiseid tema ülesannete täitmise kohta.

Politseiseaduse artikli 38 lõike 3 kohaselt koostoimes selle artikliga 2 ja artikli 36 lõikega 2 vastutavad prefektuuride avaliku turvalisuse komisjonid „üksikisiku õiguste ja vabaduse kaitse“ eest. Selleks esitavad prefektuuride politseiametite ülemad neile aruandeid nende pädevusse kuuluva tegevuse kohta, sealhulgas korrapärastel nõupidamistel, mis toimuvad kolm või neli korda kuus. Komisjon annab neis küsimustes juhtnööre tervikliku poliitika kehtestamise kaudu.

Lisaks sellele võivad prefektuuride avaliku turvalisuse komisjonid oma järelevalvefunktsiooni täites anda prefektuuri politseiametile suuniseid konkreetsetes üksikjuhtumites, kui nad peavad seda prefektuuri politseiameti tegevuse või politseiametnike väärkäitumise uurimise käigus vajalikuks. Samuti võib komisjon, kui ta seda vajalikuks peab, määrata komisjoniliikme, kes kontrollib antud suunise rakendamise seisu (politseiseaduse artikkel 43-2).

([17]) Et tagada läbipaistvust ja hõlbustada MIC-poolset järelevalvet, peab haldusorgani juht vastavalt APPIHAO artiklile 11 dokumenteerima kõik APPIHAO artikli 10 lõikes 1 nõutud andmed, nagu selle haldusorgani nime, kelle käes toimik on hoiul, toimiku kasutamise eesmärk, isikuandmete kogumise meetodi jne (nn „Isikuteabe toimikute register“). Isikuteabe toimikud, mis kuuluvad APPIHAO artikli 10 lõike 2 kohaldamisalasse, näiteks toimikud, mis on koostatud või saadud kriminaaluurimise osana või seotud riigi julgeolekut puudutavate küsimustega, on siiski vabastatud nõudest teatada neist MIC-le ja lisada nad avalikku registrisse. Avalike registrite ja arhiivide haldamise seaduse artikli 7 alusel peab haldusorgani juht siiski alati registreerima haldusdokumentide salastatuse kategooria, pealkirja, säilitamisaja, säilitamiskoha jms („Haldusdokumentide haldamise register“). Mõlema registri indeksandmed avaldatakse internetis ja see võimaldab inimestel kontrollida, missugust isikuteavet toimik sisaldab ja milline haldusorgan seda teavet säilitab.

4) Parlamendipoolne järelevalve

Parlament võib uurida riigiasutuste tegevust ning nõuda sel eesmärgil dokumentide esitamist ja tunnistajate ütlusi (põhiseaduse artikkel 62). Sellega seoses võib parlamendi pädev komisjon uurida politsei korraldatud teabekogumise asjakohasust.

Neid volitusi on täpsustatud parlamendiseaduses. Nimetatud seaduse artikli 104 kohaselt võib parlament nõuda, et valitsus ja riigiasutused esitaksid aruandeid ja dokumente, mida ta vajab oma uurimise jaoks. Peale selle võivad parlamendiliikmed esitada kirjalikke järelepärimisi vastavalt parlamendiseaduse artiklile 74. Järelepärimised peab heaks kiitma parlamendikoja eesistuja ning valitsus peab neile põhimõtteliselt vastama kirjalikult seitsme päeva jooksul (kui selle aja jooksul ei ole võimalik vastata, tuleb seda põhjendada ja määrata uus tähtaeg – parlamendiseaduse artikkel 75). Minevikus on parlamendi kirjalikes järelepärimistes käsitletud ka isikuteabe käitlemist valitsuses ([18]).

C) Üksikisiku õiguskaitse

Vastavalt Jaapani põhiseaduse artiklile 32 ei keelata ühelegi isikule õigust kohtusse pöörduda. Lisaks tagab põhiseaduse artikkel 17 igale isikule õiguse kaevata riik või avaliku sektori asutus kohtusse, et saada seaduse alusel hüvitist, kui ta on ametiisiku ebaseadusliku tegevuse tõttu kahju kannatanud.

1) Edasikaebeõigus sundusliku teabekogumise korral kohtu määruse alusel (kriminaalmenetluse seadustiku artikkel 430)

Kriminaalmenetluse seadustiku artikli 430 lõikes 2 on sätestatud, et isik, kes ei ole rahul meetmetega, mida politseiametnik on võtnud seoses esemete arestimisega (kaasa arvatud juhul, kui need sisaldavad isikuteavet) kohtu määruse alusel, võib esitada pädevale kohtule taotluse (nn „kvaasikaebuse“) selliste meetmete tühistamiseks või muutmiseks.

Sellise vaidlustuse võib esitada, ilma et isik peaks ootama kohtumenetluse lõppu. Kui kohus leiab, et arestimine ei olnud vajalik või et on muid põhjusi, miks arestimist tuleb pidada ebaseaduslikuks, võib ta nõuda selliste meetmete tühistamist või muutmist.

2) Edasikaebeõigus tsiviilkohtumenetluse seadustiku ja riigivastutuse seaduse alusel

Kui isik leiab, et tema põhiseaduse artikli 13 kohast õigust eraelu puutumatusele on rikutud, võib ta esitada tsiviilhagi, milles nõuab kriminaaluurimise käigus kogutud isikuteabe kustutamist.

Lisaks võib isik riigivastutuse seaduse alusel koostoimes tsiviilseadustiku asjakohaste artiklitega esitada kahju hüvitamise hagi, kui ta leiab, et tema õigust eraelu puutumatusele on rikutud ja ta on oma isikuteabe kogumise või jälgimise tulemusena kahju kannatanud ([19]). Kuna hüvitisnõude aluseks olev „kahju“ ei piirdu üksnes varakahjuga (tsiviilseadustiku artikkel 710), võib see hõlmata ka „hingelist valu“. Sellise moraalse kahju hüvitamise määra hindab kohtunik „vaba hindamise vormis, kaaludes igal üksikjuhul selle kõiki erinevaid tegureid“ ([20]).

Riigivastutuse seaduse artikli 1 lõikega 1 on ette nähtud õigus saada hüvitist, kui i) ametiisik, kes teostab riigivõimu või avaliku asutuse võimu, on ii) oma tööülesandeid täites iii) tahtlikult või hooletusest iv) ebaseaduslikult v) tekitanud kahju teisele isikule.

Isik peab hagi esitama tsiviilkohtumenetluse seadustiku alusel. Kohaldatavate normide kohaselt võib ta teha seda selles kohtus, mille tööpiirkonnas asub koht, kus õigusvastane kahju tekitati.

([18]) Vt nt ülemkoja 27. märtsi 2009. aasta kirjalikku järelepärimist nr 92, mis käsitleb kriminaaluurimiste käigus kogutud teabe käitlemist, sealhulgas politsei- ja prokuratuuripoolseid konfidentsiaalsuskohustuste rikkumisi.

([19]) Sellise tegevuse näide on nn „Kaitseagentuuri nimekirja juhtum“ (Niigata ringkonnakohus, 11. mai 2006. aasta otsus (2002(Wa) No.514)). Selles juhtumis oli kaitseagentuuri ametnik koostanud nimekirja isikutest, kes olid esitanud kaitseagentuurile haldusdokumentidega tutvumise taotluse, pidas seda nimekirja ja levitas seda. Nimekirjas oli kirjeldatud hageja isikuteavet. Väites, et tema eraelu puutumatust ja õigust teada on rikutud, nõudis hageja, et kostja maksaks talle tekitatud kahju eest riigivastutuse seaduse artikli 1 lõike 1 alusel hüvitist. Kohus rahuldas selle taotluse osaliselt, mõistes hageja kasuks välja osalise hüvitise.

([20]) Ülemkohus, 5. aprilli 1910. aasta otsus (1910(O) No.71).

3) Üksikisiku õiguskaitse politsei ebaseaduslike/nõuetevastaste uurimiste korral: kaebus prefektuuri avaliku turvalisuse komisjonile (politseiseaduse artikkel 79)

Vastavalt politseiseaduse artiklile 79, ([21]) mida on täiendavalt selgitatud NPA juhi korralduses prefektuuride politseiametitele ja prefektuuride avaliku turvalisuse komisjonidele, ([22]) võivad isikud esitada pädevale prefektuuri avaliku turvalisuse komisjonile kirjaliku kaebuse ([23]) selle kohta, et politseiametnik on oma ametiülesannete täitmisel käitunud ebaseaduslikult või sobimatult; see hõlmab ka ametiülesandeid, mis on seotud isikuandmete kogumise ja kasutamisega. Komisjon tegeleb selliste kaebustega tões ja vaimus vastavalt seadustele ja kohalikele määrustele ning teeb oma uurimise tulemused kaebajale kirjalikult teatavaks.

Lähtudes oma järelevalvevolitustest, mis tulenevad politseiseaduse artikli 38 lõikest 3, annab prefektuuri avaliku turvalisuse komisjon prefektuuri politseiametile korralduse uurida asjaolusid, rakendada vajalikud meetmed vastavalt uurimise tulemustele ja anda tulemustest komisjonile aru. Kui komisjon seda vajalikuks peab, võib ta anda ka korralduse kaebuse menetlemise kohta, näiteks juhul, kui ta leiab, et politsei teostatud uurimine ei ole olnud piisav. Seda rakendamist kirjeldatakse NPA teatises prefektuuride politseiametite juhtidele.

Uurimise tulemused tehakse kaebuse esitajale teatavaks, võttes arvesse ka politseilt uurimise ja komisjoni nõudmisel võetud meetmete kohta saadud aruandeid.

4) Üksikisiku õiguskaitse APPIHAO ja kriminaalmenetluse seadustiku alusel

a) *APPIHAO*

APPIHAO artikli 48 alusel peavad haldusorganid püüdma menetleda kõiki isikuteabe käitlemist puudutavaid kaebusi korrakohaselt ja kiiresti. Vahendina, mille kaudu anda isikutele konsolideeritud teavet (nt APPIHAOst tuleneva õiguse kohta teavet avaldada, andmeid parandada ja kasutus peatada), ja päringute esitamise kontaktpunktina on MIC APPIHAO artikli 47 lõike 2 alusel loonud igas prefektuuris teabe avaldamise ja isikuteabe kaitse koondteabekeskused. Seal võivad päringuid teha ka mitteresidendid. Näiteks 2017. majandusaastal (aprill 2017 kuni märts 2018) vastasid koondteabekeskused päringutele 5186 korral.

APPIHAO artiklid 12 ja 27 annavad isikutele õiguse taotleda, et säilitatav isikuteave neile avaldataks ja et seda parandataks. Peale selle võivad isikud APPIHAO artikli 36 alusel taotleda, et neile kuuluva säilitatava isikuteabe kasutamine peataks või et see teave kustutataks, kui haldusorgan ei ole säilitatud isikuteavet saanud õiguspäraselt või kui ta säilitab või kasutab sellist teavet seadusevastaselt.

Isikuteave, mis on kogutud (kas kohtu määruse alusel või „päringuvormide“ abil) ja mida säilitatakse kriminaaluurimise jaoks, ([24]) kuulub üldjuhul siiski kategooriasse „kohtumenetlusega seotud dokumentides ja arestitud esemetes salvestatud “. Selline isikuteave jääb seega kriminaalmenetluse seadustiku artikli 53-2 alusel APPIHAO 4. peatükis sätestatud üksikisiku õiguste kohaldamisalast välja ([25]). Sellise isikuteabe töötlemise suhtes ning isiku õiguse suhtes selle teabega tutvuda ja seda

([21]) Politseiseaduse artikkel 79 (väljavõte):
1. Igaüks, kellel on kaebus prefektuuri politsei ametiülesannete täitmise kohta, võib esitada riikliku avaliku turvalisuse komisjoni määruses ette nähtud korra kohaselt kirjaliku kaebuse prefektuuri avaliku turvalisuse komisjonile.
2. Prefektuuri avaliku turvalisuse komisjon, kes on saanud eelmises lõikes sätestatud kaebuse, käsitleb seda tões ja vaimus vastavalt seadustele ja kohalikele määrustele ning teeb oma uurimise tulemused kaebajale kirjalikult teatavaks, välja arvatud järgmistel juhtudel:
   1) leitakse, et kaebus on esitatud selleks, et takistada prefektuuri politseid tema seadusest tulenevate kohustuste täitmisel;
   2) kaebuse esitaja praegune elukoht ei ole teada;
   3) leitakse, et kaebus on esitatud ühiselt koos teiste kaebajatega ja teistele kaebajatele on ühiskaebuse tulemusest juba teatatud.

([22]) NPA, teatis kaebuste nõuetekohase käsitlemise kohta politseiametnike poolt ametiülesannete täitmisel, 13. aprill 2001, selle lisa 1 „Politseiseaduse artikli 79 tõlgendamise/rakendamise reeglid“.

([23]) NPA teatise (vt eelmine joonealune märkus) kohaselt peavad isikud, kellel on raskusi kaebuse kirjalikul vormistamisel, saama abi. Siia hulka kuuluvad sõnaselgelt ka välismaalased.

([24]) Teisest küljest leidub aga dokumente, mida ei liigitata „kohtumenetlusega seotud dokumentideks“, kuna need ei ole iseenesest teave, mis on saadud kohtu määruse või uurimismenetluse käigus tehtud kirjalike päringute tulemusena, vaid need on loodud selliste dokumentide alusel. Sellisel juhul ei kuulu eraelulised andmed APPIHAO artikli 45 lõike 1 kohaldamisalasse ega ole seega APPIHAO 4. peatüki kohaldamisalast välja jäetud.

([25]) Kriminaalmenetluse seadustiku artikli 53-2 lõikes 2 on sätestatud, et APPIHAO 4. peatüki sätteid ei kohaldata isikuteabe suhtes, mis on salvestatud kohtumenetlusega seotud dokumentides ja arestitud esemetes.

parandada kohaldatakse selle asemel kriminaalmenetluse seadustiku ja lõplike kriminaaltoimikute seaduse erinorme (vt allpool) ([26]). Sellist väljajätmist õigustavad mitmesugused tegurid, nagu asjaomaste isikute eraelu kaitse, uurimiste salastatus ja kriminaalmenetluse nõuetekohane läbiviimine. Sellegipoolest kohaldatakse sellise teabe suhtes APPIHAO 2. peatükki, mis reguleerib sellise teabe käitlemise põhimõtteid.

b) *Kriminaalmenetluse seadustik*

Kriminaalmenetluse seadustiku kohaselt sõltub võimalus tutvuda kriminaaluurimise jaoks kogutud isikuteabega nii menetluse etapist kui ka isiku rollist uurimises (kahtlustatav, süüdistatav, ohver jne).

Erandina kriminaalmenetluse seadustiku artiklis 47 sätestatud nõudest, et kohtumenetlusega seotud dokumente ei tehta enne kohtumenetluse algust avalikuks (kuna see võib riivata asjaomaste isikute au ja/või rikkuda nende eraelu puutumatust ja takistada uurimist/kohtulikku arutamist), on kuriteoohvril põhimõtteliselt lubatud sellise teabega tutvuda, niivõrd kui seda peetakse mõistlikuks, võttes arvesse kriminaalmenetluse seadustiku artikli 47 sätte eesmärki ([27]).

Kahtlusalused saavad üldjuhul teada asjaolust, et nende suhtes on algatatud kriminaaluurimine, siis, kui kohtupolitsei või riigiprokurör neid üle kuulab. Kui prokurör seejärel otsustab süüdistuse esitamata jätta, teatab ta sellest kahtlustatavale tolle taotluse korral kohe (kriminaalmenetluse seadustiku artikkel 259).

Peale selle annab prokurör pärast süüdistuse esitamist süüdistatavale või tema kaitsjale võimaluse tutvuda tõenditega, enne kui ta palub kohtul tõendid läbi vaadata (kriminaalmenetluse seadustiku artikkel 299). See võimaldab süüdistataval kontrollida oma isikuteavet, mis on kriminaaluurimise käigus kogutud.

Lõpetuseks on kriminaaluurimise käigus kogutud isikuteabe kaitse, olgu tegemist kahtlustatava, süüdistatava või mõne muu isikuga (nt kuriteoohver), tagatud konfidentsiaalsuskohustusega (riikliku avaliku teenistuse seaduse artikkel 100) ja karistustega, mis on ette nähtud juhul, kui avaliku teenistuse ametiülesannete täitmise käigus käideldud konfidentsiaalne teave lekitatakse (riikliku avaliku teenistuse seaduse artikli 109 punkt xii).

5) Üksikisiku õiguskaitse ametivõimude ebaseaduslike/nõuetevastaste uurimiste korral: kaebus isikuteabe kaitse komisjonile

APPI artikli 6 kohaselt võtab valitsus koostöös kolmandate riikide valitsustega vajalikke meetmeid, et luua isikuteabe valdkonnas rahvusvaheliselt kooskõlaline süsteem, soodustades koostööd rahvusvaheliste organisatsioonide ja muude rahvusvaheliste raamistikega. Selle sätte põhjal on isikuteabe kaitse aluspoliitikaga (mis on vastu võetud valitsuskabineti otsusega) isikuandmete kaitse komisjonile kui APPI üldise haldamise alal pädevale asutusele delegeeritud volitus võtta vajalikke meetmeid, et ületada lõhe Jaapani ja asjaomase välisriigi süsteemide ja tegutsemisviiside vahel, selleks et tagada sellelt riigilt saadud isikuandmete kohane käitlemine.

Nagu on sätestatud APPI artikli 61 punktides i ja ii, on isikuteabe kaitse komisjonile lisaks tehtud ülesandeks aluspoliitika sõnastamine ja tutvustamine, samuti ettevõtjate vastu esitatud kaebuste puhul vahendamine. Samuti peavad haldusorganid üksteisega tihedalt suhtlema ja koostööd tegema (APPI artikkel 80).

Nimetatud sätete alusel menetleb isikuteabe kaitse komisjon üksikisikute esitatud kaebusi järgmiselt:

a) Isik, kes kahtlustab, et Jaapani avaliku sektori asutus, sealhulgas käesoleva „ülevaate“ II ja III peatükis osutatud tegevuse eest vastutav asutus, on kogunud või kasutanud tema EList edastatud andmeid ja seejuures rikkunud kohaldatavaid eeskirju, sealhulgas neid, mida on käsitletud käesolevas „ülevaates“, võib esitada isikuteabe kaitse komisjonile kaebuse (isiklikult või oma andmekaitseasutuse kaudu).

b) Isikuteabe kaitse komisjon menetleb kaebust, milleks ta muu hulgas kasutab talle APPI artikli 6, artikli 61 punkti ii ja artikli 80 kohaselt antud volitusi, ning teavitab kaebusest pädevaid avaliku sektori asutusi, sealhulgas asjaomaseid järelevalveasutusi.

([26]) Kriminaalmenetluse seadustiku ja lõplike kriminaaltoimikute seaduse alusel kehtib arestitud esemetele juurdepääsu ja paranduste tegemise ning kriminaalmenetlustega seotud dokumentide/isikuteabe suhtes unikaalne ja omalaadne reeglistik, mille eesmärk on kaitsta asjaomaste isikute eraelu puutumatust, uurimiste saladust, kriminaalmenetluse nõuetekohast läbiviimist jmt.

([27]) Täpsemalt on kuriteoohvril põhimõtteliselt lubatud tutvuda objektiivsete tõenditega seotud teabega, mis käsitleb süüdistuse esitamata jätmist juhtumites, milles kriminaalmenetluse seadustiku artikli 316-33 jj alusel on vajalik ohvri osalemine, selleks et muuta kuriteoohvrite kaitse rahuldavamaks.

Need ametiasutused peavad tegema isikuteabe kaitse komisjoniga artikli 80 kohaselt koostööd, sealhulgas esitades vajalikku teavet ja asjakohaseid materjale, mille alusel isikuteabe kaitse komisjon saaks hinnata, kas isikuteabe kogumine või järgnev kasutamine on toimunud kooskõlas kohaldatavate eeskirjadega. Isikuteabe kaitse komisjon teeb hindamisel koostööd siseasjade ja teabevahetuse ministeeriumiga.

c) Kui hinnang näitab, et kohaldatavaid eeskirju on rikutud, hõlmab asjaomaste avaliku sektori asutuste koostöö isikuteabe kaitse komisjoniga ka kohustust rikkumine kõrvaldada.

Kui isikuteave koguti kohaldatavate eeskirjade järgi ebaseaduslikult, tuleb kogutud isikuteabe kustutada.

Kohaldatavate eeskirjade rikkumise korral teeb isikuteabe kaitse komisjoni enne hindamise lõpuleviimist kindaks, et rikkumine oleks täielikult kõrvaldatud.

d) Kui hindamine on lõpetatud, teavitab isikuteabe kaitse komisjon üksikisikut mõistliku aja jooksul hindamise tulemustest, sealhulgas võetud parandusmeetmetest (vajaduse korral). Ühtlasi teavitab isikuteabe kaitse komisjon üksikisikut võimalusest küsida pädevalt avaliku sektori asutuselt tulemuse kinnitust ja sellest, millise ametiasutuse poole sellise kinnituse saamiseks pöörduda.

Hindamise tulemuse kohta ei tule esitada kõiki üksikasju, kui on põhjendatud alus arvata, et sellise teabe edastamine seab tõenäoliselt ohtu käimasoleva uurimise.

Kui kaebus puudutab isikuandmete kogumist või kasutamist kriminaalõiguse täitmise tagamise valdkonnas, siis juhul kui hindamisel selgub, et algatatud on üksikisiku isikuteabega seotud uurimine ja see uurimine on lõpetatud, teavitab isikuteabe kaitse komisjon üksikisikut, et uurimistoimikuga saab tutvuda kooskõlas kriminaalmenetluse seadustiku artikliga 53 ja lõplike kriminaaltoimikute seaduse artikliga 4.

Kui hindamisel selgub, et isik on kriminaalasjas kahtlustatav, teavitab isikuteabe kaitse komisjon isikut sellest asjaolust ja võimalusest esitada kriminaalmenetluse seadustiku artikli 259 kohane taotlus.

e) Kui üksikisik ei ole kõnealuse menetluse tulemusega endiselt rahul, võib ta pöörduda isikuteabe kaitse komisjoni, kes teavitab üksikisikut Jaapani õigusnormide alusel õiguskaitse saamise eri võimalustest ja üksikasjalikest menetlustest. Isikuteabe kaitse komisjon toetab üksikisikut, sealhulgas asjaomase haldus- või kohtuorgani poole pöördumisel nõu ja abi pakkumisega.

III. **Valitsuse juurdepääs riikliku julgeoleku eesmärgil**

A. Isikuteabe kogumise õiguslik alus ja piirangud

1) Asjaomase ministeeriumi/asutuse poolt teabe kogumise õiguslik alus

Nagu eespool märgitud, ei tohi haldusorganid riikliku julgeoleku eesmärgil isikuteavet kogudes ületada oma halduspädevust.

Jaapanis ei ole seadust, mis võimaldaks teabe kogumist sunduslike vahenditega, et seda kasutada üksnes riikliku julgeoleku eesmärgil. Põhiseaduse artikli 35 kohaselt on isikuteavet võimalik sunniviisiliselt koguda üksnes õiguserikkumise uurimiseks kohtu antud määruse alusel. Seega võib sellist määrust välja anda üksnes kriminaaluurimise eesmärgil. See tähendab, et Jaapani õigussüsteemis ei anna riiklik julgeolek alust teabe kogumiseks ega teabele juurdepääsuks sunduslike vahenditega. Selle asemel saavad asjaomased ministeeriumid või ametid riikliku julgeoleku valdkonnas hankida teavet üksnes vabalt kättesaadavatest allikatest või sellistelt ettevõtjatelt või üksikisikutelt, kes teavet vabatahtlikult avaldavad. Vabatahtliku koostöö taotluse saanud ettevõtjad ei ole õiguslikult kohustatud sellist teavet andma ja seetõttu ei ole koostööst keeldumisel neile negatiivseid tagajärgi.

Vastutust riikliku julgeoleku valdkonna eest jagavad eri ministeeriumide osakonnad ja ametid.

1) Valitsuse sekretariaat

Valitsuse sekretariaat kogub teavet ja tegeleb uurimistööga valitsuse jaoks olulistes poliitikavaldkondades, ([28]) mis on sätestatud valitsuse seaduse artiklis 12-2 ([29]). Siiski ei ole valitsuse sekretariaadil õigust koguda isikuteavet otse ettevõtjatelt. Ta kogub, kaasab, analüüsib ja hindab teavet, mis on saadud vabalt kättesaadavatest allikatest, teistest avaliku sektori asutustest jne.

2) Riiklik politseiamet / prefektuuri politseiamet

Igas prefektuuris on prefektuuri politseiametil õigus teavet koguda üksnes oma pädevuse piires kooskõlas politseiseaduse artikliga 2. Võib juhtuda, et riiklik politseiamet kogub politseiseaduse alusel oma pädevuse piires teavet otse. See puudutab eelkõige riikliku politseiameti julgeolekubüroo ning välisasjade ja luureosakonna tegevust. Politseiseaduse artikli 24 kohaselt kuuluvad julgeolekupolitseiga ([30]) seotud küsimused julgeolekubüroo vastutusalasse ning välisriikide kodanikega ja välisriikides tegevuskohti omavate Jaapani kodanikega seotud küsimused kuuluvad välisasjade ja luureosakonna vastutusalasse.

3) Riigi julgeoleku luureagentuur (PSIA)

Õõnestustegevuse ärahoidmise seaduse (*Subversive Activities Prevention Act*, edaspidi „SAPA“) ja valimatult massimõrvu toimepannud organisatsioonide kontrolli seaduse (*Act on the Control of Organisations Which Have Committed Acts of Indiscriminate Mass Murder*, edaspidi „ACO“) kohaldamine kuulub peamiselt riigi julgeoleku luureagentuuri (*Public Security Intelligence Agency* (edaspidi „PSIA“)) pädevusse. See on justiitsministeeriumi agentuur.

SAPA ja ACOga on ette nähtud, et halduskorraldusi (st meetmeid, millega nõutakse selliste organisatsioonide tegevuse piiramist, nende laialisaatmist jne) võib rangetel tingimustel teha selliste organisatsioonide suhtes, kes panevad toime teatavaid raskeid tegusid („terroristlik õõnestustegevus“ või „valimatult toimepandud massimõrv“), millega nad rikuvad põhiseaduse kohast „avalikku julgeolekut“ või „ühiskonna alussüsteemi“. „Terroristlik õõnestustegevus“ on reguleeritud SAPAga (vt artiklit 4, milles on nimetatud selline tegevus nagu ülestõus, välismaise agressiooni õhutamine, poliitmõrvad jne), ACO aga reguleerib valimatult toimepandud massimõrvasid (vt ACO artikkel 4). SAPA või ACO kohaseid korraldusi saab teha üksnes selliste üheselt kindlaksmääratud organisatsioonide suhtes, kellest lähtub avalikule julgeolekule konkreetne sise- või välisoht.

Selleks on SAPAs ja ACOs sätestatud uurimise õiguslikud alused. PSIA (PSIO) ametnike peamised uurimisvolitused on sätestatud SAPA artiklis 27 ja ACO artiklis 29. Nende sätete raames toimuv PSIA uurimistegevus ei ületa seda, mis on vajalik organisatsioonide eespool nimetatud kontrolli korralduste andmiseks (näiteks on varem uuritud vasakradikaalide rühmitusi, *Aum Shinrikyo* sekti ja üht kohalikku rühmitust, millel olid tihedad sidemed Põhja-Koreaga). Siiski ei saa nendes uurimistes kasutada sunduslikke vahendeid ja seega ei saa isikuteavet valdavatelt organisatsioonilt sellist teavet välja nõuda.

PSIA-le vabatahtlikult avalikustatud teabe kogumise ja kasutamise suhtes kehtivad vastavad seadusega sätestatud kaitsemeetmed ja piirangud, sealhulgas põhiseadusega tagatav sõnumisaladus ja APPIHAO raames isikuteabe nõuetekohase käitlemise eeskirjad.

4) Kaitseministeerium

Kaitseministeeriumi jaoks on teabe kogumisel ette nähtud, et kaitseministeerium kogub teavet kaitseministeeriumi asutamise seaduse artiklite 3 ja 4 alusel, kuivõrd see on vajalik tema halduspädevuse teostamiseks, sealhulgas kaitse ja valve osas, omakaitsejõudude sekkumise ning maaväe, mereväe ja õhuväe alla kuuluvate omakaitsejõudude kasutamise puhul. Kaitseministeerium saab nimetatud eesmärgil teavet koguda üksnes vabatahtliku koostöö raames ja vabalt kättesaadavatest allikatest. Ta ei kogu teavet üldsuse kohta.

2) Piirangud ja kaitsemeetmed

a) *Seadusest tulenevad piirangud*

1) APPIHAO kohased üldised piirangud

APPIHAO on üldseadus, millega reguleeritakse haldusorganite tegevusvaldkonnas nende poolt isikuteabe kogumist ja käitlemist. Seetõttu kohaldatakse jao II.A.1 punkti b alapunktis 2 kirjeldatud piiranguid ja kaitsemeetmeid ka riikliku julgeoleku valdkonnas isikuteabe säilitamise, salvestamise, kasutamise jms suhtes.

([28]) Valitsuse sekretariaadi korralduse määruse artikli 4 kohaselt on see valitsuse luure- ja uurimisameti ülesanne.
([29]) See sisaldab „valitsuse oluliste poliitikasuundade kohta teabe kogumist ja seotud uurimistööd“.
([30]) Julgeolekupolitsei vastutab avaliku julgeoleku ja riigi huvide valdkonnas kuritegevuse piiramiseks elluviidava tegevuse eest. See hõlmab kuritegevuse piiramist ja teabe kogumist sellise ebaseadusliku tegevuse kohta, mis on seotud vasak- ja paremäärmuslike rühmituste ning Jaapani vastu suunatud tegevusega.

2) Politsei (nii riikliku politseiameti kui ka prefektuuri politseiameti) suhtes kohaldatavad eripiirangud

Nagu eespool teabe õiguskaitse eesmärgil kogumist käsitlevas jaotises täpsustatud, võib politsei koguda teavet üksnes oma pädevuse piires ja ta peab seejuures politseiseaduse artikli 2 lõike 2 kohaselt „rangelt piirduma“ oma ülesannete täitmisega ja seda „erapooletult, sõltumatult, eelarvamustevabalt ja õiglaselt“. Lisaks ei tohi ta oma volitusi „kunagi selliselt kuritarvitada, et see riivab Jaapani põhiseadusega tagatud üksikisiku õigusi ja vabadusi“.

3) PSIA suhtes kohaldatavad eripiirangud

Nii SAPA artiklis 3 kui ka ACO artiklis 3 on sätestatud, et nende õigusaktide alusel teostatavad uurimised viiakse läbi ainult sel määral, mis on vajalik taotletava eesmärgi saavutamiseks, ning neid ei teostata viisil, mis põhjendamatult piirab põhilisi inimõigusi. Kui PSIA ametnik kuritarvitab oma volitusi, on see vastavalt SAPA artiklile 45 ja ACO artiklile 42 kuritegu, mille eest on ette nähtud karmimad kriminaalkaristused kui „üldise“ volituste kuritarvitamise eest avaliku sektori muudes valdkondades.

4) Kaitseministeeriumi suhtes kohaldatavad eripiirangud

Seoses teabe kogumisega kaitseministeeriumi poolt, nagu on osutatud kaitseministeeriumi asutamise seaduse artiklis 4, on see piiratud teabe kogumisega, mis on „vajalik“ tema kohustuste täitmiseks seoses 1) kaitse ja valvega, 2) meetmetega, mida peavad võtma kaitsejõud, 3) maa-, mere- ja õhukaitsejõudude korralduse, isikkoosseisu, struktuuri, varustuse ja kasutusega.

b) *Muud piirangud*

Nagu selgitatud eespool jao II.A.2 punkti b alapunktis 1 seoses kriminaaluurimistega, järeldub ülemkohtu praktikast, et ettevõtjale vabatahtliku koostöö taotluse esitamiseks peab selline taotlus olema kuriteokahtluse uurimise jaoks vajalik ja uurimise eesmärgi saavutamise seisukohast mõistlik.

Ehkki uurimisasutuste läbi viidud uurimised riigi julgeoleku valdkonnas erinevad uurimistest, mille viivad läbi uurimisasutused õiguskaitse valdkonnas, nii nende õigusliku aluse kui ka eesmärgi poolest, siis „uurimise jaoks vajalikkuse“ ja „meetodi asjakohasuse“ keskseid põhimõtteid kohaldatakse samamoodi riigi julgeoleku valdkonnas ning neid tuleb järgida, võttes asjakohaselt arvesse iga juhtumi konkreetseid asjaolusid.

Eespool esitatud piirangute kombinatsioon tagab, et teabe kogumine ja töötlemine toimub üksnes ulatuses, mis on vajalik pädeva avaliku sektori asutuse konkreetsete ülesannete täitmiseks, samuti konkreetsetest ohtudest lähtudes. Välja on jäetud riikliku julgeoleku huvides isikuteabe massiline ja valimatu kogumine või sellele juurdepääs.

B. Järelevalve

1) APPIHAO-l põhinev järelevalve

Nagu selgitatud eespool jaos II.B.2, on Jaapani avalikus sektoris ministril või iga ministeeriumi või ameti juhil õigus teha oma ministeeriumis või ametis järelevalvet ja tagada seal APPIHAO nõuete järgimine. Lisaks võib siseasjade ja teabevahetuse minister uurida seaduse täitmise seisu, paluda igal ministril esitada seaduse artikli 49 ja 50 alusel materjalid ja selgitused ning esitada igale ministrile seaduse artikli 51 alusel arvamusi. Näiteks võib ta taotleda meetmete läbivaatamist vastavalt seaduse artiklitele 50 ja 51.

2) Avaliku turvalisuse komisjonide järelevalve politsei üle

Nagu selgitatud eespool jaos „II. Teabe kogumine kriminaalõiguse täitmise tagamise eesmärgil“, teevad prefektuuride politseiametite tegevuse üle järelevalvet sõltumatud avaliku turvalisuse prefektuurikomisjonid.

Riikliku politseiameti (NPA) üle teeb järelevalvet riiklik avaliku turvalisuse komisjon. Vastavalt politseiseaduse artiklile 5 vastutab kõnealune komisjon eelkõige „üksikisiku õiguste ja vabaduse kaitse“ eest. Selleks kehtestab ta eelkõige tervikliku poliitika, millega nähakse ette politseiseaduse artikli 5 lõike 4 punktide kohaste küsimuste käsitlemise kord, ja kehtestab muud põhisuunad või meetmed, millele tuleks asjaomaste tegevuste puhul tugineda. Riiklik avaliku turvalisuse komisjon (NPSC) on sama sõltumatu kui avaliku turvalisuse prefektuurikomisjonid (PPSCd).

3) Õigusliku vastavuse peainspektsiooni järelevalve kaitseministeeriumi üle

Õigusliku vastavuse peainspektsioon (IGO) on kaitseministeeriumi sõltumatu amet, mis on kaitseministri otsese järelevalve all vastavalt kaitseministeeriumi asutamise seaduse artiklile 29. IGO võib kontrollida seda, kuidas ministeeriumi ametnikud täidavad õigusnorme. Neid kontrolle nimetatakse „kaitsekontrollideks".

IGO teostab kontrolli sõltumatult, et tagada õigusnormide täitmine kogu ministeeriumis, sealhulgas kaitsejõududes. Ta täidab oma ülesandeid sõltumatult kaitseministeeriumi operatsioonilistest osakondadest. Pärast kontrolli esitab IGO oma järeldused koos vajalike parandusmeetmetega viivitamata otse kaitseministrile. IGO aruande põhjal võib kaitseminister anda määrusi olukorra parandamiseks vajalike meetmete võtmiseks. Aseministri asetäitja vastutab nende meetmete rakendamise eest ja peab kaitseministrile rakendamise seisu kohta aru andma.

Vabatahtliku läbipaistvusmeetmena avalikustatakse kaitsekontrollide tulemused nüüdsest kaitseministeeriumi veebisaidil (kuigi see ei ole seadusega ette nähtud).

On olemas kolme liiki kaitsekontrolle:

i) korrapärased kaitsekontrollid, mida teostatakse perioodiliselt ([31]);

ii) kontrolli eesmärgil tehtavad kaitsekontrollid, mille raames kontrollitakse, kas parendusmeetmeid on tulemuslikult võetud, ning

iii) spetsiaalsed kaitsekontrollid, mida tehakse kaitseministri nõudel konkreetsetes küsimustes.

Selliste kontrollide puhul võib IGO nõuda asjaomaselt büroolt aruandeid, dokumentide esitamist, siseneda kohapealse kontrolli tegemiseks tegevuskohtadesse, nõuda aseministri asetäitjalt selgitusi jne. Võttes arvesse IGO kontrolliülesannete laadi, juhivad seda väga kõrgel tasemel õiguseksperdid (endine kõrgem prokurör).

4) PSIA järelevalve

PSIA teostab nii korrapäraseid kui ka erikontrolle oma üksikute büroode ja ametite (riigi julgeoleku luureagentuur, riigi julgeoleku luureasutused ja allasutused jne) tegevuse üle. Korrapärase kontrolli eesmärgil määratakse inspektori(te)ks peadirektori asetäitja ja/või direktor. Sellised kontrollid hõlmavad ka isikuteabe haldamist.

5) Parlamendipoolne järelevalve

Õiguskaitse eesmärgil teabe kogumisel võib parlament oma pädeva komitee kaudu uurida teabe kogumise seaduslikkust riikliku julgeoleku valdkonnas. Parlamendi uurimisvolitused põhinevad põhiseaduse artiklil 62 ja parlamendiseaduse artiklitel 74 ja 104.

C. Üksikisiku õiguskaitse

Üksikisiku õiguskaitsevahendid on samad nagu kriminaalõiguse kohaldamise valdkonnas. See hõlmab ka uut ELi üksikisikute esitatud kaebuste käsitlemise ja lahendamise õiguskaitsemehhanismi, mida haldab ja mille üle teeb järelevalvet isikuteabe kaitse komisjon. Rohkem teavet selle kohta on esitatud jao II.C asjakohastes lõikudes.

Lisaks sellele on riikliku julgeoleku valdkonnas üksikisikule ette nähtud eriõiguskaitsevahendid.

Riikliku julgeoleku huvides haldusorgani kogutud isikuteabe suhtes kohaldatakse APPIHAO 4. peatüki sätteid. See hõlmab õigust nõuda teabe avalikustamist (artikkel 12), isiku kohta säilitatud isikuteabe parandamist (sealhulgas teabe lisamine või kustutamine) (artikkel 27) ning õigust nõuda isikuteabe kasutamise peatamist, kui haldusorgan on asjaomase teabe saanud ebaseaduslikult (artikkel 36). Riikliku julgeoleku valdkonnas on nimetatud õiguste kasutamise suhtes kehtestatud teatavad

([31]) Käesoleva ülevaatega hõlmatud küsimustes tehtud kontroll oli näiteks 2016. aasta korrapärane kaitsekontroll „õiguslikust vastavusest teadlikkuse ja selleks valmisoleku" väljaselgitamiseks, kuna isikuteabe kaitse oli üks kontrolli kesksetest punktidest. Täpsemalt hõlmas kontroll isikuteabe haldamist, säilitamist jms. Oma aruandes tõi IGO esile mitu isikuteabe haldamise sobimatut aspekti, mida tuleks parandada, nt andmete salasõnaga kaitsmata jätmine. Aruanne on kättesaadav kaitseministeeriumi veebisaidil.

piirangud: avalikustamise, parandamise või peatamise taotlust ei rahuldata, kui see käsitleb „teavet, mille puhul on haldusorgani juhil mõistlik alus arvata, et avalikustamine võib kahjustada riiklikku julgeolekut, kahjustada vastastikusel usaldusel põhinevaid suhteid teise riigi või rahvusvahelise organisatsiooniga või halvendada positsiooni teise riigi või rahvusvahelise organisatsiooniga peetavatel läbirääkimistel“ (artikli 14 punkt iv). Seega ei kuulu igasugune riikliku julgeolekuga seotud teabe vabatahtlik kogumine selle erandi alla, kuna erandiga on ette nähtud, et teabe avalikustamisega kaasnevaid riske tuleb alati konkreetselt hinnata.

Kui isiku taotlus lükatakse tagasi põhjusel, et asjaomast teavet loetakse artikli 14 punkti iv tähenduses mitteavalikustatavaks, võib isik esitada vaide sellise otsuse läbivaatamiseks, väites näiteks, et artikli 14 punktis iv sätestatud tingimused ei ole asjaomasel juhul täidetud. Sel juhul konsulteerib asjaomase haldusorgani juht enne otsuse tegemist teabe avalikustamise ja isikuteabe kaitse läbivaatamise nõukoguga. Nõukogu vaatab sõltumatust seisukohast lähtudes vaide läbi. Nõukogu on väga spetsialiseerunud ja sõltumatu organ, mille liikmed nimetab väljapaistvate erialateadmistega isikute hulgast ametisse peaminister parlamendi mõlema koja heakskiidul ([32]). Nõukogul on suured uurimisvolitused, sealhulgas õigus nõuda dokumente ja avalikustada asjaomast isikuteavet, pidada kinnist arutelu ning kohaldada Vaughni indeksi menetlust ([33]). Seejärel koostab nõukogu kirjaliku aruande, mis esitatakse asjaomasele isikule ([34]). Aruandes esitatud järeldused avalikustatakse. Kuigi aruanne ei ole formaalselt võttes õiguslikult siduv, on asjaomased haldusorganid peaaegu alati kõiki aruandeid järginud ([35]).

Lõpuks võib üksikisik vastavalt halduskohtumenetluse seaduse artikli 3 lõikele 3 pöörduda kohtusse, et tühistada haldusorgani tehtud otsus jätta isikuteave avalikustamata.

IV. **Korrapärane läbivaatamine**

Kaitse piisavuse otsuse korrapärase läbivaatamise raames vahetavad isikuteabe kaitse komisjon ja Euroopa Komisjon teavet andmete töötlemise kohta kaitse piisavuse otsuses sätestatud tingimustel, sealhulgas käesolevas ülevaates sätestatud tingimustel.

([32]) Vt teabe avalikustamise ja isikuteabe kaitse läbivaatamise nõukogu asutamise seaduse artikkel 4.
([33]) Vt teabe avalikustamise ja isikuteabe kaitse läbivaatamise nõukogu asutamise seaduse artikkel 9.
([34]) Vt teabe avalikustamise ja isikuteabe kaitse läbivaatamise nõukogu asutamise seaduse artikkel 16.
([35]) Viimase kolme aasta jooksul ei ole asjaomane haldusorgan võtnud vastu nõukogu järeldustest erinevat otsust. Veelgi varasematel aastatel on seda juhtunud äärmiselt harva: vaid kahel korral kokku 2 000 juhtumist alates 2005. aastast (aasta, mil jõustus APPIHAO). Kui haldusorgan teeb otsuse, mis erineb nõukogu järeldustest, märgib ta selgelt selle põhjused vastavalt halduskaebuse läbivaatamise seaduse artikli 50 lõike 1 punktile 4, nagu seda kohaldatakse kooskõlas APPIHAO artikli 42 lõike 2 asendamisega.