II

(Neleģislatīvi akti)

LĒMUMI

KOMISIJAS ĪSTENOŠANAS LĒMUMS (ES) 2019/419

(2019. gada 23. janvāris),

kas pieņemts saskaņā ar Eiropas Parlamenta un Padomes Regulu (ES) 2016/679, par personas datu pietiekamu aizsardzību Japānā atbilstoši Likumam par personas informācijas aizsardzību

(izziņots ar dokumenta numuru C(2019) 304)

(Dokuments attiecas uz EEZ)

EIROPAS KOMISIJA,

ņemot vērā Līgumu par Eiropas Savienības darbību,

ņemot vērā Eiropas Parlamenta un Padomes Regulu (ES) 2016/679 (2016. gada 27. aprīlis) par fizisku personu aizsardzību attiecībā uz personas datu apstrādi un šādu datu brīvu apriti un ar ko atceļ Direktīvu 95/46/EK (Vispārīgā datu aizsardzības regula) ([1]) ("VDAR"), un jo īpaši tās 45. panta 3. punktu,

pēc apspriešanās ar Eiropas Datu aizsardzības uzraudzītāju,

1. IEVADS

(1) Regulā (ES) 2016/679 ir izklāstīti noteikumi par personas datu nosūtīšanu no pārziņiem vai apstrādātājiem Eiropas Savienībā uz trešām valstīm un starptautiskām organizācijām, ciktāl uz šādu nosūtīšanu attiecas regulas darbības joma. Noteikumi par personas datu starptautisku nosūtīšanu ir paredzēti minētās regulas V nodaļā, konkrēti 44.–50. pantā. Personas datu plūsma uz un no valstīm ārpus Eiropas Savienības ir nepieciešama starptautiskās sadarbības un starptautiskās tirdzniecības paplašināšanai, vienlaikus garantējot, ka netiek ietekmēts personas datu aizsardzības līmenis Eiropas Savienībā.

(2) Atbilstoši Regulas (ES) 2016/679 45. panta 3. punktam Komisija pēc aizsardzības līmeņa pietiekamības izvērtēšanas ar īstenošanas aktu var nolemt, ka trešā valsts, trešās valsts teritorija vai viens vai vairāki konkrēti sektori, vai starptautiska organizācija nodrošina pietiekamu aizsardzības līmeni. Šādos apstākļos personas datus uz minēto trešo valsti, teritoriju, sektoru vai starptautisko organizāciju var nosūtīt bez nepieciešamības saņemt jebkādu turpmāku atļauju, kā paredzēts regulas 45. panta 1. punktā un 103. apsvērumā.

(3) Kā norādīts Regulas (ES) 2016/679 45. panta 2. punktā, lēmumu par aizsardzības līmeņa pietiekamību pieņem, pamatojoties uz visaptverošu analīzi par trešās valsts tiesisko kārtību, gan attiecībā uz noteikumiem, kas piemērojami datu importētājiem, gan attiecībā uz ierobežojumiem un garantijām saistībā ar publisko iestāžu piekļuvi personas datiem. Novērtējumā jānosaka, vai attiecīgā trešā valsts garantē aizsardzības līmeni, kas "pēc būtības ir līdzvērtīgs" Eiropas Savienībā nodrošinātajam (Regulas (ES) 2016/679 104. apsvērums). Kā ir precizējusi Eiropas Savienības Tiesa, tas nenozīmē, ka ir vajadzīgs identisks aizsardzības līmenis ([2]). Jo īpaši attiecīgās trešās valsts izmantotie līdzekļi var atšķirties no Eiropas Savienībā izmantotajiem, kamēr vien tie praksē efektīvi nodrošina pietiekamu aizsardzības līmeni ([3]). Tāpēc aizsardzības līmeņa pietiekamības standarts neparedz Savienības

([1]) OV L 119, 4.5.2016., 1. lpp.
([2]) Lieta C-362/14 *Maximillian Schrems | Data Protection Commissioner* ("*Schrems*"), ECLI:EU:C:2015:650, 73. punkts.
([3]) *Schrems*, 74. punkts.

noteikumu precīzu replicēšanu. Pārbaude drīzāk atklāj, vai valsts tiesību sistēma spēj nodrošināt nepieciešamo aizsardzības līmeni, ņemot vērā tiesību uz privātumu būtību un to efektīvu īstenošanu, uzraudzību un izpildi ([4]).

(4) Komisija ir rūpīgi izanalizējusi Japānas tiesību aktus un praksi. Pamatojoties uz 6.–175. apsvērumā izklāstītajiem konstatējumiem, Komisija secina, ka Japāna nodrošina pietiekamu aizsardzības līmeni attiecībā uz personas datiem, ko nosūta organizācijām, uz kurām attiecas Likuma par personas informācijas aizsardzību ([5]) darbības joma un kurām piemēro šajā lēmumā minētos papildu nosacījumus. Šie nosacījumi ir noteikti Papildu noteikumos (I pielikums), ko pieņēmusi Personas informācijas aizsardzības komisija (*PPC*) ([6]), un oficiālajos apliecinājumos, garantijās un saistībās, ko Japānas valdība ir sniegusi Eiropas Komisijai (II pielikums).

(5) Šā lēmuma rezultātā pārzinis vai apstrādātājs Eiropas Ekonomikas zonā (EEZ) ([7]) var nosūtīt datus šādām organizācijām Japānā bez nepieciešamības saņemt jebkādu turpmāku atļauju. Šis lēmums neskar Regulas (ES) 2016/679 tiešu piemērošanu šādām organizācijām, ja ir izpildīti tās 3. panta nosacījumi.

2. NOTEIKUMI, KAS ATTIECAS UZ DATU APSTRĀDI, KURU VEIC UZŅĒMĒJI

2.1. Datu aizsardzības regulējums Japānā

(6) Tiesību sistēmas, kas reglamentē privātumu un datu aizsardzību Japānā, pamatā ir 1946. gadā izsludinātā Konstitūcija.

(7) Konstitūcijas 13. pantā ir noteikts:

"Visus cilvēkus ciena kā personības. Gan tiesību aktos, gan citās valdības lietās viņu tiesībām dzīvot un būt laimīgiem tiek piešķirta visaugstākā vērtība, ciktāl tas netraucē sabiedrības labklājībai."

(8) Pamatojoties uz minēto pantu, Japānas Augstākā tiesa ir precizējusi personu tiesības attiecībā uz personas informācijas aizsardzību. Lēmumā, kas pieņemts 1969. gadā, tā atzina tiesības uz privātumu un datu aizsardzību par konstitucionālām tiesībām ([8]). Proti, Tiesa nosprieda, ka "ikvienai personai ir brīvība aizsargāt savu personas informāciju pret tās izpaušanu trešām personām vai publiskošanu, ja tai nav pamatota iemesla." Turklāt 2008. gada 6. marta lēmumā (*Juki-Net*) ([9]) Augstākā tiesa nosprieda, ka "pilsoņu brīvību privātajā dzīvē aizsargā no valsts varas īstenošanas, un to var interpretēt tādējādi, ka ikvienai personai viena no viņas brīvībām privātajā dzīvē ir brīvība aizsargāt savu personas informāciju pret tās izpaušanu trešām personām vai publiskošanu, ja tam nav pamatota iemesla ([10])."

(9) Japāna 2003. gada 30. maijā ieviesa vairākus likumus datu aizsardzības jomā:

— Likumu par personas informācijas aizsardzību (*APPI*),

— Likumu par administratīvo struktūru rīcībā esošas personas informācijas aizsardzību (*APPIHAO*),

— Likumu par inkorporētu administratīvo aģentūru rīcībā esošas personas informācijas aizsardzību (*APPI-IAA*).

([4]) Sk. Komisijas paziņojumu Eiropas Parlamentam un Padomei "Apmaiņa ar personas datiem un šo datu aizsardzība globalizētā pasaulē", COM(2017) 7, 10.1.2017., 3.1. iedaļa, 6. un 7. lpp.
([5]) Likums par personas informācijas aizsardzību (Likums Nr. 57, 2003. gads).
([6]) Plašāka informācija par *PPC* pieejama saitē: https://www.ppc.go.jp/en/ (kur pieejama arī kontaktinformācija jautājumu un sūdzību iesniegšanai: https://www.ppc.go.jp/en/contactus/access/).
([7]) Šis lēmums attiecas uz EEZ. Līgumā par Eiropas Ekonomikas zonu (EEZ līgums) paredzēta Eiropas Savienības iekšējā tirgus paplašināšana, iekļaujot trīs EEZ valstis: Islandi, Lihtenšteinu un Norvēģiju. EEZ Apvienotā komiteja 2018. gada 6. jūlijā pieņēma Apvienotās komitejas lēmumu (*JCD*), ar ko Regulu (ES) 2016/679 iekļauj EEZ līguma XI pielikumā, un tas stājās spēkā 2018. gada 20. jūlijā. Tādējādi uz regulu attiecas minētais līgums.
([8]) Augstākā tiesa, Virspalātas 1969. gada 24. decembra spriedums, *Keishu*, 23. sēj., Nr. 12, 1625. lpp.
([9]) Augstākā tiesa, 2008. gada 6. marta spriedums, *Minshu*, 62. sēj., Nr. 3, 665. lpp.
([10]) Augstākā tiesa, 2008. gada 6. marta spriedums, *Minshu*, 62. sēj., Nr. 3, 665. lpp.

(10) Abos pēdējos minētajos likumos (grozīti 2016. gadā) ir ietverti konkrēti noteikumi, kas piemērojami personas informācijas aizsardzībai, kuru nodrošina publiskā sektora struktūras. Datu apstrāde, uz ko attiecas minēto likumu piemērošanas joma, nav šajā lēmumā ietvertā konstatējuma par aizsardzības līmeņa pietiekamību priekšmets – šis lēmums attiecas tikai uz personas informācijas aizsardzību, ko nodrošina uzņēmēji, kuri izmanto personas informāciju (*PIHBO*), *APPI* nozīmē.

(11) Pēdējos gados ir veikta *APPI* reforma. Grozītais *APPI* tika izsludināts 2015. gada 9. septembrī un stājās spēkā 2017. gada 30. maijā. Ar grozījumiem tika ieviestas vairākas jaunas garantijas, kā arī nostiprinātas esošās garantijas, tādējādi Japānas datu aizsardzības sistēmu pietuvinot Eiropas sistēmai. Tas ietver, piemēram, īstenojamu individuālu tiesību kopumu vai tādas neatkarīgas uzraudzības iestādes (*PPC*) izveidi, kam uzticēta *APPI* pārraudzība un izpilde.

(12) Papildus *APPI* uz personas informācijas apstrādi, kura ietilpst šā lēmuma darbības jomā, attiecas īstenošanas noteikumi, kas pieņemti, pamatojoties uz *APPI*. To starpā ir grozījumi Ministru kabineta 2016. gada 5. oktobra rīkojumā, ar kuru uzdod izpildīt Likumu par personas informācijas aizsardzību, un *PPC* pieņemtie t.s. Likuma par personas informācijas aizsardzību izpildes noteikumi ([11]). Abi šie noteikumu kopumi ir juridiski saistoši un izpildāmi un stājās spēkā vienlaikus ar grozīto *APPI*.

(13) Turklāt 2016. gada 28. oktobrī Japānas Ministru kabinets (kura sastāvā ir premjerministrs un šo valdību veidojošie ministri) pieņēma "pamatpolitiku", kuras mērķis ir "visaptveroši un integrēti veicināt pasākumus attiecībā uz personas informācijas aizsardzību". Atbilstoši *APPI* 7. pantam pamatpolitiku pieņem kā Ministru kabineta lēmumu, un tajā iekļauj politikas norādījumus par *APPI* izpildi, kas adresēti gan centrālajai valdībai, gan vietējām valdībām.

(14) Nesen Japānas valdība ar Ministru kabineta lēmumu, kas pieņemts 2018. gada 12. jūnijā, grozīja pamatpolitiku. Lai atvieglotu starptautisko datu nosūtīšanu, ar minēto Ministru kabineta lēmumu *PPC* kā kompetentajai iestādei attiecībā uz *APPI* pārvaldību un īstenošanu tiek deleģētas "pilnvaras veikt nepieciešamos pasākumus, lai mazinātu sistēmu un darbību atšķirības starp Japānu un attiecīgo ārvalsti, pamatojoties uz likuma 6. pantu, nolūkā nodrošināt no šādas valsts saņemtas personas informācijas pienācīgu izmantošanu". Ministru kabineta lēmumā ir noteikts, ka tas ietver pilnvaras noteikt pastiprinātus aizsardzības pasākumus, *PPC* pieņemot stingrākus noteikumus, kas papildina un pārsniedz *APPI* un Ministru kabineta rīkojumā paredzētos. Atbilstoši minētajam lēmumam šādi stingrāki noteikumi ir saistoši Japānas uzņēmējiem, kuriem tie ir jāizpilda.

(15) Pamatojoties uz *APPI* 6. pantu un minēto Ministru kabineta lēmumu, *PPC* 2018. gada 15. jūnijā pieņēma Papildu noteikumus saskaņā ar Likumu par personas informācijas aizsardzību no ES nosūtīto personas datu izmantošanai, pamatojoties uz lēmumu par aizsardzības līmeņa pietiekamību ("Papildu noteikumi"), lai pastiprinātu no Eiropas Savienības uz Japānu nosūtītās personas informācijas aizsardzību, pamatojoties uz šo lēmumu par aizsardzības līmeņa pietiekamību. Minētie Papildu noteikumi ir juridiski saistoši Japānas uzņēmējiem, un gan *PPC*, gan tiesām tie ir jāīsteno tāpat kā *APPI* normas, kuras noteikumi papildina ar stingrākiem un/vai sīkāk izstrādātiem noteikumiem ([12]). Tā kā Japānas uzņēmējiem, kuri no Eiropas Savienības saņem un/vai turpmāk apstrādā personas datus, būs juridisks pienākums ievērot papildu noteikumus, viņiem ir jānodrošina (piem., ar tehniskiem līdzekļiem ("marķēšanu") vai organizatoriskiem līdzekļiem (uzglabājot īpašā datubāzē)), ka viņi var identificēt šādus personas datus visā to "aprites ciklā" ([13]). Turpmākajās iedaļās ir analizēts katra Papildu noteikuma saturs kā daļa no to *APPI* pantu novērtējuma, kurus tas papildina.

(16) Atšķirībā no laikposma pirms 2015. gada grozījumiem, kad šis jautājums bija dažādu Japānas ministriju kompetencē konkrētās nozarēs, *APPI* pilnvaro *PPC* pieņemt "pamatnostādnes", "lai nodrošinātu uzņēmēju veicamo darbību pienācīgu un efektīvu īstenošanu" atbilstīgi datu aizsardzības noteikumiem. Ar pamatnostādnēm *PPC* nodrošina minēto noteikumu, jo īpaši *APPI* autoritatīvu interpretāciju. Kā liecina no *PPC* saņemtā informācija,

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

([12]) Sk. Papildu noteikumus (ievaddaļa).

([13]) Tas netiek apšaubīts ar vispārējo prasību saglabāt ierakstus (tikai) noteiktu laikposmu. Pat ja datu izcelsme ir ietverta informācijā, kura saņemošajam *PIHBO* ir jāapstiprina saskaņā ar *APPI* 26. panta 1. punktu, prasība saskaņā ar *APPI* 26. panta 4. punktu kopā ar *PPC* noteikumu 18. pantu attiecas tikai uz konkrētu ieraksta formu (sk. *PPC* noteikumu 16. pantu) un neliedz *PIHBO* nodrošināt datu identifikāciju uz ilgākiem laikposmiem. *PPC* to ir apstiprinājusi, apliecinot, ka: "informācijas par ES datu izcelsmi *PIHBO* ir jāglabā tik ilgi, cik tas nepieciešams, lai ievērotu papildu noteikumus".

minētās pamatnostādnes ir daļa no tiesiskā regulējuma un ir lasāmas kontekstā ar *APPI*, Ministru kabineta rīkojuma, *PPC* noteikumu tekstu un *PPC* sagatavoto jautājumu un atbilžu kopumu ([14]). Tādēļ pamatnostādnes ir "saistošas uzņēmējiem". Ja pamatnostādnēs ir noteikts, ka uzņēmējam "ir" jārīkojas vai tam "nevajadzētu" rīkoties noteiktā veidā, *PPC* uzskatīs, ka neatbilstība attiecīgajiem noteikumiem ir likuma pārkāpums ([15]).

2.2. **Materiālā un personīgā piemērošanas joma**

(17) *APPI* piemērošanas jomu nosaka definētie jēdzieni "personas informācija", "personas dati" un "uzņēmējs, kas izmanto personas informāciju". Tajā pašā laikā *APPI* paredz dažus būtiskus tā piemērošanas jomas izņēmumus, jo īpaši attiecībā uz anonīmi apstrādātiem personas datiem un īpašiem apstrādes veidiem, ko īsteno konkrēti uzņēmēji. Lai arī *APPI* nav lietots jēdziens "apstrāde" (*processing*), tajā ir lietots līdzvērtīgs jēdziens "rīkošanās" (*handling*), kas saskaņā ar informāciju, kura saņemta no *PPC*, aptver "jebkuru darbību saistībā ar personas datiem", tai skaitā ieguvi, ievadi, apkopošanu, organizēšanu, glabāšanu, rediģēšanu/apstrādi, atjaunošanu, dzēšanu, izvadi, izmantošanu, vai personas informācijas sniegšanu.

2.2.1. *Personas informācijas definīcija*

(18) Vispirms, runājot par *APPI* materiālo piemērošanas jomu, *APPI* tiek nošķirta personas informācija no personas datiem, un tikai konkrēti šā likuma noteikumi ir piemērojami attiecībā uz pirmo minēto kategoriju. Saskaņā ar *APPI* 2. panta 1. punktu jēdziens "personas informācija" ietver jebkuru informāciju, kas attiecas uz dzīvu personu un kas ļauj identificēt attiecīgo personu. Pēc definīcijas izšķir divas personas informācijas kategorijas: i) individuālie identifikācijas kodi un ii) cita personas informācija, pēc kuras var identificēt konkrētu personu. Pēdējā minētā kategorija arī ietver informāciju, kas pati par sevi nenodrošina identificēšanu, bet ļauj identificēt konkrētu personu, kad tā tiek "vienkārši salīdzināta" ar citu informāciju. Saskaņā ar *PPC* pamatnostādnēm ([16]) par to, vai informāciju var uzskatīt par viegli salīdzināmu, spriež katrā atsevišķā gadījumā, ņemot vērā uzņēmēja faktisko situāciju ("stāvokli"). Pieņem, ka informācija ir viegli salīdzināma, ja šādu salīdzināšanu veic (vai var veikt) vidusmēra ("parasts") uzņēmējs, izmantojot tam pieejamos līdzekļus. Piemēram, informācija nav "viegli salīdzināma" ar citu informāciju, ja uzņēmējam ir jāpieliek neierastas pūles vai jāiesaistās nelikumīgās darbībās, lai iegūtu salīdzināmo informāciju no viena vai vairākiem citiem uzņēmējiem.

2.2.2. *Personas datu definīcija*

(19) Tikai uz konkrētu veidu personas informāciju var attiecināt jēdzienu "personas dati" saskaņā ar *APPI*. "Personas datus" faktiski definē kā "personas informāciju, kas veido personas informācijas datubāzi", t. i., "kopēju informācijas kopumu", kas ietver personas informāciju, kuru "sistemātiski organizē tā, lai varētu meklēt konkrētu personas informāciju, izmantojot datoru" ([17]) vai kas ar Ministru kabineta rīkojumu noteikta kā "sistemātiski organizēta tā, lai varētu viegli meklēt konkrētu personas informāciju", tomēr "izņemot informāciju, kas ar Ministru kabineta rīkojumu noteikta par tādu, kam ir maza iespējamība kaitēt personas tiesībām un interesēm, ņemot vērā tās izmantošanas metodi" ([18]).

(20) Šis izņēmums ir precizēts Ministru kabineta rīkojuma 3. panta 1. punktā, saskaņā ar kuru jābūt izpildītiem šādiem trim kumulatīviem nosacījumiem: i) kopējam informācijas kopumam jābūt "izveidotam ar nolūku to pārdot lielam skaitam nenoteiktu personu, un tā izveide nav veikta, pārkāpjot kāda likuma vai rīkojuma noteikumus tās pamatā"; ii) kopumam jābūt tādam, ka to "jebkurā laikā var iegādāties liels skaits nenoteiktu personu" un iii) tajā iekļautajiem

([14]) *PPC*, jautājumi un atbildes, 2017. gada 16. februāris (grozījumi izdarīti 2017. gada 30. maijā), pieejami šādā saitē: https://www.ppc.go.jp/files/pdf/kojouhouQA.pdf. Jautājumu un atbilžu kopumā ir aplūkoti vairāki pamatnostādnēs iztirzāti aspekti, sniedzot praktiskus piemērus, piemēram, paskaidrojot, kādi dati uzskatāmi par sensitīviem personas datiem, kā jāinterpretē individuāla piekrišana, datus nosūtīšana trešām personām mākoņdatošanas ietvaros, vai kāds ir uzskaites veikšanas pienākums, kas ir piemērojams datu pārrobežu nosūtīšanā. Jautājumi un atbildes ir pieejamas tikai japāņu valodā.

([15]) Pēc konkrēti uzdota jautājuma *PPC* ir informējusi *EDPB* par to, ka "Japānas tiesas, kad tās piemēro *APPI*/*PPC* noteikumus atsevišķās lietās, kas tām iesniegtas, to sniegtajā interpretācijā pamatojas uz pamatnostādnēm un tādējādi savos spriedumos ir tieši atsaukušās uz *PPC* pamatnostādņu tekstu. Tādēļ arī no šā viedokļa *PPC* pamatnostādnes ir saistošas uzņēmējiem. *PPC* nav zināmi gadījumi, kad tiesa būtu atkāpusies no pamatnostādnēm." Šajā sakarā *PPC* vērsa Komisijas uzmanību uz datu aizsardzības jomā pieņemtu spriedumu, kurā tiesa savu secinājumu izdarīšanā nepārprotami pamatojās uz minētajām pamatnostādnēm (sk. Osakas rajona tiesa, 2006. gada 19. maija lēmums, *Hanrei Jiho*, 1948. sēj., 122. lpp., kurā tiesa nosprieda, ka uzņēmējam ir pienākums īstenot drošības kontroli, pamatojoties uz šādām pamatnostādnēm).

([16]) *PPC* pamatnostādnes (Vispārējo noteikumu izdevums), 6. lpp.

([17]) Tas ietver jebkuru elektroniskās reģistrācijas sistēmu. *PPC* pamatnostādnēs (vispārējais izdevums, 17. lpp.) ir minēti konkrēti piemēri: piem., e-pasta adrešu saraksts, ko glabā e-pasta klientu programmatūrā.

([18]) *APPI* 2. panta 4. un 6. punkts.

personas datiem jābūt tādiem, kas "sniegti to sākotnējam nolūkam, nepievienojot citu informāciju, kas saistīta ar dzīvu personu". Saskaņā ar paskaidrojumiem, kas saņemti no *PPC*, šis ierobežotais izņēmums tika ieviests ar mērķi izslēgt tālruņu grāmatas vai līdzīgus abonentu sarakstus.

(21) Attiecībā uz datiem, kas savākti Japānā, ir svarīgs nošķirums starp "personas informāciju" un "personas dati", jo šāda informācija ne vienmēr var būt daļa no "personas informācijas datubāzes" (piemēram, vienota datu kopa, kas savākta un apstrādāta manuāli), un tāpēc *APPI* noteikumi, kas attiecas tikai uz personas datiem, nebūs piemērojami ([19]).

(22) Turpretī šim nošķirumam nav nozīmes attiecībā uz personas datiem, ko nosūta no Eiropas Savienības uz Japānu, pamatojoties uz lēmumu par aizsardzības līmeņa pietiekamību. Tā kā šādus datus parasti nosūtīs elektroniski (ņemot vērā to, ka digitālajā laikmetā tas ir parastais datu apmaiņas veids, jo īpaši lielos attālumos kā starp ES un Japānu), un tādējādi tie kļūst par daļu no datu saņēmēja elektroniskās reģistrācijas sistēmas, šādi ES dati atbilstoši *APPI* vienmēr būs iekļaujami "personas datu" kategorijā. Izņēmuma gadījumā, kad personas dati no ES tiktu pārsūtīti, izmantojot citus līdzekļus (piem., papīra formā), uz tiem joprojām attieksies *APPI*, ja pēc pārsūtīšanas tie kļūs par daļu no "kopēja informācijas kopuma", kas sistemātiski organizēts tā, lai dotu iespēju viegli meklēt konkrētu informāciju (*APPI* 2. panta 4. punkta ii) apakšpunkts). Saskaņā ar Ministru kabineta rīkojuma 3. panta 2. punktu tas attiecas uz gadījumiem, kad informācija ir izkārtota "saskaņā ar konkrētu noteikumu" un datubāzē ir rīki, piemēram, satura rādītājs vai alfabētiskais rādītājs, kas atvieglo meklēšanu. Tas atbilst "kartotēkas" definīcijai VDAR 2. panta 1. punktā.

2.2.3. *Saglabātu personas datu definīcija*

(23) Konkrēti *APPI* noteikumi, jo īpaši 27.–30. pants, kas attiecas uz individuālām tiesībām, ir piemērojami tikai attiecībā uz konkrētu personas datu kategoriju, proti, "saglabātiem personas datiem". Šādi dati *APPI* 2. panta 7. punktā ir definēti kā personas dati, kas nav dati, kuri i) "ar Ministru kabineta rīkojumu noteikti par tādiem, kas var kaitēt sabiedrības vai citām interesēm, ja tiek darīta zināma to esība vai neesība" vai ii) kurus "paredzēts dzēst laikposmā, kas nepārsniedz vienu gadu un kas noteikts ar Ministru kabineta rīkojumu".

(24) Pirmā no šīm abām kategorijām ir izskaidrota Ministru kabineta rīkojuma 4. pantā un aptver četru veidu izņēmumus ([20]). Šiem izņēmumiem ir līdzīgi mērķi kā tiem, kas uzskaitīti Regulas (ES) 2016/679 23. panta 1. punktā, proti, aizsargāt datu subjektu (*APPI* lietotais termins – "principālu") un citu personu brīvību, valsts drošību, sabiedrības drošību, krimināltiesību izpildi, un citi svarīgi mērķi, kas ir sabiedrības vispārējās interesēs. Turklāt no Ministru kabineta rīkojuma 4. panta 1. punkta i) līdz iv) apakšpunkta formulējuma izriet, ka to piemērošana vienmēr pieņem kā priekšnoteikumu to, ka pastāv konkrēts risks attiecībā uz vienu no aizsargājamajām būtiskajām interesēm ([21]).

(25) Otra kategorija ir sīkāk precizēta Ministru kabineta rīkojuma 5. pantā. Saskaņā ar minēto pantu, to lasot saistībā ar *APPI* 2. panta 7. punktu, jēdziens "saglabāti personas dati" un tādējādi arī individuālās tiesības, kas noteiktas *APPI*, nav attiecināmi uz tiem personas datiem, ko "paredzēts dzēst" sešu mēnešu laikā. *PPC* ir paskaidrojusi, ka šā izņēmuma mērķis ir stimulēt uzņēmējus saglabāt un apstrādāt datus pēc iespējas īsāku laiku. Tomēr tas nozīmētu, ka ES datu subjekti nevar izmantot svarīgas tiesības, un vienīgais iemesls tam ir termiņš, kurā attiecīgajam uzņēmējam ir jāsaglabā to dati.

(26) Lai novērstu šo situāciju, 2. papildu noteikums paredz, ka personas dati, ko nosūta no Eiropas Savienības, "ir izmantojami kā saglabāti personas dati likuma 2. panta 7. punkta nozīmē neatkarīgi no tā, cik ilgā laikā tos paredzēts dzēst". Tādējādi saglabāšanas laikposmam nav ietekmes uz ES datu subjektiem piešķirtajām tiesībām.

([19]) Piemēram, *APPI* 23. pants par nosacījumiem personas datu apmaiņai ar trešām personām.

([20]) Proti, personas dati, i) "attiecībā uz kuriem pastāv iespēja, ka gadījumā, ja tiktu darīta zināma to esība vai neesība, tas kaitētu principāla vai trešās personas dzīvībai, veselībai vai labklājībai"; ii) dati, "attiecībā uz kuriem pastāv iespēja, ka gadījumā, ja tiktu darīta zināma to esība vai neesība, tas veicinātu vai izraisītu nelikumīgu vai nepamatotu darbību"; iii) dati, "attiecībā uz kuriem pastāv iespēja, ka gadījumā, ja tiktu darīta zināma to esība vai neesība, tas kaitētu valsts drošībai, iznīcinātu uzticības attiecības ar ārvalsti vai starptautisku organizāciju vai radītu neizdevīgu stāvokli sarunās ar ārvalsti vai starptautisku organizāciju"; un iv) dati, "attiecībā uz kuriem pastāv iespēja, ka gadījumā, ja tiktu darīta zināma to esība vai neesība, tas traucētu uzturēt sabiedrisko drošību un kārtību, piemēram, novērst, izskaust vai izmeklēt noziegumus."

([21]) Minētajos apstākļos personai nav jāpaziņo. Tas saskan ar VDAR 23. panta 2. punkta h) apakšpunktu, kurā noteikts, ka datu subjekti nav jāinformē par ierobežojumiem, ja "tas var kaitēt ierobežojuma mērķim".

2.2.4. *Anonīmi apstrādātas personas informācijas definīcija*

(27) Prasības, kas piemērojamas anonīmi apstrādātai personas informācijai, kā definēts *APPI* 2. panta 9. punktā, ir noteiktas likuma 4. nodaļas 2. iedaļā ("Tāda uzņēmēja pienākumi, kurš izmanto anonīmi apstrādātu informāciju"). Turpretī šādu informāciju nereglamentē noteikumi, kas izklāstīti *APPI* IV nodaļas 1. iedaļā, kurā ir panti, kas nosaka datu aizsardzības garantijas un tiesības, kuras attiecināmas uz personas datu apstrādi atbilstoši likumam. Tādējādi, lai gan uz "anonīmi apstrādātu personas informāciju" neattiecas standarta datu aizsardzības noteikumi (kas paredzēti IV nodaļas 1. iedaļā un *APPI* 42. pantā), tie tomēr ietilpst *APPI* un konkrēti tā 36.–39. panta piemērošanas jomā.

(28) Saskaņā ar *APPI* 2. panta 9. punktu "anonīmi apstrādāta personas informācija" ir informācija, kas attiecas uz personu un kas ir "iegūta, apstrādājot personas informāciju", izmantojot *APPI* (36. panta 1. punkts) un *PPC* (19. pants) noteikumos paredzētos pasākumus, kā rezultātā ir kļuvis neiespējami identificēt konkrētu personu vai atjaunot personas informāciju.

(29) No minētajiem noteikumiem izriet (kā to apstiprina arī *PPC*), ka personas informācijas "anonimizēšanas" procesam nav jābūt tehniski neatgriezeniskam. Saskaņā ar *APPI* 36. panta 2. punktu uzņēmējiem, kas izmanto "anonīmi apstrādātu personas informāciju," ir tikai jānovērš atkārtota identifikācija, veicot pasākumus, lai aizsargātu "aprakstus utt., un individuālos identifikācijas kodus, kas dzēsti no personas informācijas, kura izmantota anonīmi apstrādātas informācijas iegūšanai, un informāciju, kas attiecas uz izmantoto apstrādes metodi".

(30) Ņemot vērā, ka "anonīmi apstrādāta personas informācija", kā definēts *APPI*, ietver datus, pēc kuriem joprojām ir iespējama atkārtota personas identifikācija, tas var nozīmēt, ka personas dati, ko nosūta no Eiropas Savienības, varētu zaudēt daļu no pieejamās aizsardzības procesā, kas atbilstoši Regulai (ES) 2016/679 tiktu uzskatīts par sava veida "pseidonimizāciju", nevis "anonimizāciju" (tādējādi nemainot to kā personas datu raksturu).

(31) Lai novērstu šo situāciju, Papildu noteikumos ir paredzētas papildu prasības, kas ir attiecināmas tikai uz personas datiem, kurus nosūta no Eiropas Savienības atbilstoši šim lēmumam. Saskaņā ar 5. papildu noteikumu šādu personas informāciju uzskata par "anonīmi apstrādātu personas informāciju" *APPI* nozīmē tikai tad, "ja uzņēmējs, kas izmanto personas informāciju, veic pasākumus, lai personas atkārtotu identifikāciju padarītu neatgriezenisku ikvienam, tostarp dzēšot apstrādes metodi un citu saistītu informāciju". Pēdējā minētā informācija Papildu noteikumos ir noteikta kā informācija, kas attiecas uz aprakstiem un individuāliem identifikācijas kodiem, kuri dzēsti no personas informācijas, kas izmantota "anonīmi apstrādātas personas informācijas" iegūšanai, kā arī informācija, kura attiecas uz apstrādes metodi, kas izmantota, dzēšot šādus aprakstus un individuālos identifikācijas kodus. Proti, saskaņā ar Papildu noteikumiem uzņēmējam, kas iegūst anonīmi apstrādātu personas informāciju, ir jāizņīcina "atslēga", kas ļauj atkārtoti identificēt datus. Tas nozīmē, ka uz personas datiem, kuru izcelsme ir Eiropas Savienībā, *APPI* noteikumi par "anonīmi apstrādātu personas informāciju" attiecas tikai gadījumos, kad tos tāpat uzskatītu par anonīmu informāciju atbilstoši Regulai (ES) 2016/679 ([22]).

2.2.5. *Uzņēmēja, kas izmanto personas informāciju (*PIHBO*), definīcija*

(32) Atbilstoši *APPI* piemērošanas jomai attiecībā uz personām, *APPI* piemēro tikai *PIHBO*. *PIHBO* ir definēts *APPI* 2. panta 5. punktā kā "persona, kas nodrošina personas informācijas datubāzi utt. izmantošanai darījumdarbībā", izņemot valdības aģentūras un administratīvas aģentūras gan centrālā, gan vietējā līmenī.

(33) Saskaņā ar *PPC* pamatnostādnēm "darījumdarbība" ir jebkura "darbība, kas tiek īstenota ar konkrētu mērķi, lai uzturētu sociāli atzītu uzņēmumu neatkarīgi no tā, vai tas tiek darīts peļņas vai bezpeļņas nolūkos". Organizācijas, kam nav juridiskas personas statusa (piemēram, *de facto* apvienības) vai privātpersonas uzskata par *PIHBO*, ja tās nodrošina (izmanto) personas informācijas datubāzi utt. savai darījumdarbībai ([23]). Tāpēc jēdziens "darījumdarbība" atbilstoši *APPI* ir ļoti plašs tādā ziņā, ka tas ietver ne tikai peļņas, bet arī bezpeļņas darbības, ko īsteno visu veidu organizācijas un privātpersonas. Turklāt "izmantošana darījumdarbībā" attiecas arī uz personas informāciju, ko neizmanto uzņēmēja (ārējās) komercattiecībās, bet izmanto iekšēji, piemēram, darbinieku datu apstrādei.

([22]) Sk. Regulu (ES) 2016/679, 26. apsvērumu.
([23]) *PPC* pamatnostādnes (Vispārējo noteikumu izdevums), 18. lpp.

(34) Attiecībā uz *APPI* noteikto aizsardzības pasākumu labuma guvējiem – tie likumā netiek nošķirti, pamatojoties uz personas valstspiederību, dzīvesvietu vai atrašanās vietu. Tas pats attiecas uz personu iespējām prasīt tiesiskās aizsardzības līdzekļus gan no *PPC*, gan no tiesām.

2.2.6. *Jēdzieni "pārzinis" un "apstrādātājs"*

(35) Saskaņā ar *APPI* netiek īpaši nošķirti pārziņiem un apstrādātājiem noteiktie pienākumi. Tas, ka šāda nošķīruma nav, neietekmē aizsardzības līmeni, jo uz visiem *PIHBO* attiecas visi likuma noteikumi. *PIHBO*, kas uztic personas datu apstrādi pilnvarotajam (atbilst apstrādātājam saskaņā ar VDAR), attiecībā uz minētajiem datiem joprojām ir jāpilda *APPI* un Papildu noteikumos ietvertie pienākumi. Turklāt atbilstoši *APPI* 22. pantam "tam ir pienākums nodrošināt nepieciešamo un atbilstošo pilnvarotā pārraudzību". Savukārt pilnvarotajam, kā to ir apliecinājusi *PPC*, ir saistoši visi pienākumi, kas noteikti *APPI* un Papildu noteikumos.

2.2.7. *Izņēmumi attiecībā uz konkrētām nozarēm*

(36) *APPI* 76. pantā ir noteikti konkrēti datu apstrādes veidi, kam nepiemēro likuma IV nodaļu, kurā ietverti galvenie datu aizsardzības noteikumi (pamatprincipi, uzņēmēju pienākumi, individuālās tiesības, *PPC* īstenotā uzraudzība). Apstrādei, kas ietilpst 76. pantā noteiktajos izņēmumos attiecībā uz konkrētām nozarēm, nepiemēro arī *PPC* izpildes pilnvaras atbilstoši *APPI* 43. panta 2. punktam ([24]).

(37) Attiecīgās kategorijas, kurām piemēro *APPI* 76. panta izņēmumus attiecībā uz konkrētām nozarēm, definē, izmantojot dubultu kritēriju, pamatojoties uz tā *PIHBO* veidu, kurš apstrādā personas informāciju, un apstrādes nolūku. Konkrēti šis izņēmums attiecas uz: i) raidsabiedrībām, laikrakstu izdevējiem, komunikāciju aģentūrām vai citām preses organizācijām (tostarp privātpersonām, kuru darījumdarbība ir saistīta ar presi), ciktāl tie apstrādā personas informāciju preses vajadzībām; ii) personām, kuras ir profesionāli nodarbojas ar rakstniecību, ciktāl tas ietver personas informāciju; iii) universitātēm un jebkurām citām organizācijām vai grupām, kuru mērķis ir nodrošināt akadēmiskās studijas, vai jebkurai personai, kas pieder pie šādas organizācijas, ciktāl tās apstrādā personas informāciju akadēmisko studiju mērķiem; iv) reliģiskām struktūrām, ciktāl tās apstrādā personas informāciju reliģiskas darbības mērķiem (tostarp visām saistītajām darbībām), un v) politiskām struktūrām, ciktāl tās apstrādā personas informāciju savas politiskās darbības mērķiem (tostarp visām saistītajām darbībām). Uz personas informācijas apstrādi kādā no nolūkiem, kas uzskaitīti 76. pantā, kuru veic citu veidu *PIHBO*, kā arī personas informācijas apstrādi, ko veic kāds no uzskaitītajiem *PIHBO* citos nolūkos, piemēram, saistībā ar nodarbinātību, joprojām attiecas IV nodaļas noteikumi.

(38) Lai nodrošinātu to personas datu pietiekamu aizsardzības līmeni, kurus nosūta no Eiropas Savienības uzņēmējiem Japānā, šis lēmums būtu jāattiecina tikai uz tās personas informācijas apstrādi, uz kuru attiecas *APPI* IV nodaļa, t. i., apstrādi, ko veic *PIHBO*, ciktāl šādai apstrādes situācijai nepiemēro nevienu no izņēmumiem attiecībā uz konkrētām nozarēm. Lēmuma piemērošanas joma būtu jāsaskaņo ar *APPI* piemērošanas jomu. Saskaņā ar *PPC* sniegto informāciju gadījums, kad kāds *PIHBO*, uz kuru attiecas šis lēmums, veic turpmākas izmaiņas attiecībā uz izmantošanas mērķi (ciktāl tas ir pieļaujams), un uz kuru tad attiektos viens no *APPI* 76. panta izņēmumiem attiecībā uz konkrētām nozarēm, tiktu uzskatīts par starptautisku pārsūtīšanu (ņemot vērā to, ka šādos gadījumos uz personas informācijas apstrādi vairs neattiektos *APPI* IV nodaļa un apstrāde vairs neietilptu tās piemērošanas jomā). Tas pats attiecas uz gadījumu, kad *PIHBO* sniedz personas informāciju subjektam, uz ko attiecas *APPI* 76. pants, izmantošanai vienam no minētajā noteikumā norādītajiem apstrādes mērķiem. Tādējādi attiecībā uz personas datiem, kas pārsūtīti no Eiropas Savienības, tā būtu tālāka nosūtīšana, uz kuru attiecas attiecīgie aizsardzības pasākumi (jo īpaši tie, kas minēti *APPI* 24. pantā un 4. papildu noteikumā). Gadījumos, kad *PIHBO* ir nepieciešama datu subjekta piekrišana ([25]), uzņēmējam būtu jāsniedz subjektam visa nepieciešamā informācija, tai skaitā jānorāda, ka personas informāciju vairs neaizsargātu *APPI*.

([24]) Attiecībā uz citiem uzņēmējiem *PPC*, īstenojot savas izmeklēšanas un izpildes pilnvaras, neierobežo to tiesības uz vārda brīvību, akadēmisko brīvību, reliģisko brīvību un politiskās darbības brīvību (*APPI* 43. panta 1. punkts).

([25]) Atbilstoši *PPC* skaidrojumam *PPC* pamatnostādnēs piekrišana ir interpretēta kā "principāla nodoma apliecinājums, ar ko viņa akceptē, ka viņa personas informāciju var apstrādāt, izmantojot metodi, kuru noradījis personas informācijas apstrādes uzņēmums". *PPC* pamatnostādnēs (Vispārējo noteikumu izdevums, 24. lpp.) ir uzskaitīti piekrišanas paušanas veidi, ko uzskata par "ierastu darījumdarbības praksi Japānā", t. i. mutiska piekrišana, veidlapu vai citu dokumentu atgriešana, piekrišana pa e-pastu, lodziņa atzīmēšana tīmekļa vietnē, uzklikšķināšana mājas lapā, izmantojot pogu "piekrītu", pieskāriens skārienpanelim utt. Visas šīs metodes ir piekrišanas paušanas veidi.

2.3. **Garantijas, tiesības un pienākumi**

2.3.1. *Nolūka ierobežojums*

(39) Personas dati būtu jāapstrādā noteiktā nolūkā, un pēc tam tos var izmantot, ciktāl tas nav pretrunā apstrādes nolūkam. Šis datu aizsardzības princips ir garantēts *APPI* 15. un 16. pantā.

(40) *APPI* paļaujas uz principu, ka uzņēmējam ir jānorāda izmantošanas nolūks "tik skaidri, cik vien iespējams" (15. panta 1. punkts), un tad jāievēro šis nolūks datu apstrādē.

(41) Šajā saistībā *APPI* 15. panta 2. punktā ir paredzēts, ka *PIHBO* nedrīkst mainīt sākotnējo nolūku, "pārsniedzot apmēru, kas atzīts par pamatoti atbilstošu izmantošanas nolūkam pirms tā mainīšanas" un kas interpretēts *PPC* pamatnostādnēs kā atbilstošs tam, ko datu subjekts var objektīvi gaidīt, pamatojoties uz "sociālajām paražām" ([26]).

(42) Turklāt atbilstoši *APPI* 16. panta 1. punktam *PIHBO* ir aizliegts izmantot personas informāciju, pārsniedzot "apmēru, kas ir nepieciešams, lai sasniegtu izmantošanas nolūku", kurš norādīts 15. pantā, pirms tam nesaņemot datu subjekta piekrišanu, ja vien nav piemērojama kāda no 16. panta 3. punktā noteiktajām atkāpēm ([27]).

(43) Attiecībā uz personas informāciju, kas saņemta no cita uzņēmēja, *PIHBO* principā var brīvi noteikt jaunu izmantošanas nolūku ([28]). Lai nodrošinātu, ka gadījumā, kad dati tiek nosūtīti no Eiropas Savienības, to saņēmējam ir saistošs nolūks, kādā dati nosūtīti, 3. papildu noteikums paredz, ka gadījumos, "kad [*PIHBO*] saņem personas datus no ES, pamatojoties uz lēmumu par aizsardzības līmeņa pietiekamību", vai šāds uzņēmējs "saņem no cita [*PIHBO*] personas datus, kas iepriekš nosūtīti no ES, pamatojoties uz lēmumu par aizsardzības līmeņa pietiekamību" (turpmāka apmainīšanās), saņēmējam ir "jānorāda minēto personas datu izmantošanas nolūks atbilstoši tā izmantošanas nolūka apmēram, kādam dati tika sākotnēji vai vēlāk saņemti". Citiem vārdiem sakot, šis noteikums nodrošina, ka nosūtīšanas kontekstā nolūks, kas noteikts atbilstoši Regulai (ES) 2016/679, joprojām nosaka apstrādi un ka nolūka maiņai jebkurā apstrādes ķēdes posmā Japānā ir vajadzīga ES datu subjekta piekrišana. Kaut arī piekrišanas saņemšanai *PIHBO* nepieciešams sazināties ar datu subjektu, gadījumos, kad tas nav iespējams, ir jānodrošina sākotnējā izmantošanas nolūka saglabāšana.

2.3.2. *Apstrādes likumīgums un godprātība*

(44) Papildu aizsardzība, kas minēta 43. apsvērumā, ir vēl jo svarīgāka tāpēc, ka tieši ar nolūka ierobežojuma principu Japānas sistēma arī nodrošina, ka dati tiek apstrādāti likumīgi un godīgi.

(45) Saskaņā ar *APPI*, kad *PIHBO* vāc personas informāciju, tam ir sīki jānorāda personas informācijas izmantošanas nolūks ([29]), kas nekavējoties jāpaziņo datu subjektam (vai jāpaziņo publiski) ([30]). Turklāt *APPI* 17. pants nosaka, ka *PIHBO* nedrīkst iegūt personas informāciju ar viltu vai izmantojot citus neatbilstošus līdzekļus. Attiecībā uz konkrētām datu kategorijām, piemēram, īpaši aizsargājamu personas informāciju, šādu datu iegūšanai ir vajadzīga datu subjekta piekrišana (*APPI* 17. panta 2. punkts).

([26]) *PPC* publicētajos jautājumos un atbildēs ir sniegti vairāki piemēri, lai ilustrētu šo jēdzienu. Situācijas, kad maiņa nepārsniedz pamatoti atbilstošu apmēru, cita starpā ir tādas personas informācijas izmantošana, kura iegūta no preču vai pakalpojumu pircējiem saistībā ar komercdarījumu, lai informētu pircējus par citām saistītām precēm vai pakalpojumiem, kas ir pieejami (piem., fitnesa kluba darbinieks, kurš reģistrē dalībnieku e-pasta adreses, lai viņus informētu par kursiem un programmām). Tajā pašā laikā jautājumos un atbildēs ir arī norādīts tādas situācijas piemērs, kurā nav atļauta izmantošanas nolūka maiņa, proti, kad uzņēmums nosūta informāciju par savām precēm un pakalpojumiem uz e-pasta adresēm, ko tas apkopojis nolūkā brīdināt par krāpšanu vai dalībnieka kartes zādzību.

([27]) Šādi izņēmumi var izrietēt no citiem normatīvajiem aktiem vai attiekties uz situācijām, kad personas informācijas izmantošana ir nepieciešama i) "cilvēka dzīvības, veselības vai īpašuma aizsardzībai"; ii) "lai uzlabotu sabiedrības higiēnu vai veicinātu veselīgu bērnu augšanu" vai iii) "lai sadarbotos ar valdības aģentūrām vai struktūrām vai ar to pārstāvjiem" likumā noteikto to uzdevumu izpildē. Turklāt i) un ii) kategorija ir piemērojama tikai tad, ja ir sarežģīti saņemt datu subjekta piekrišanu, un iii) kategorija ir piemērojama tikai tad, ja pastāv risks, ka datu subjekta piekrišanas saņemšana traucētu šādu uzdevumu izpildei.

([28]) Šajā saistībā, pamatojoties uz *APPI* 23. panta 1. punktu, principā ir vajadzīga personas piekrišana, lai datus izpaustu trešai personai. Tādējādi attiecīgajai personai ir iespēja kaut kādā mērā kontrolēt to, kā cits uzņēmējs izmanto tās datus.

([29]) Saskaņā ar *APPI* 15. panta 1. punktu nolūks jānorāda "tik skaidri, cik vien iespējams".

([30]) *APPI* 18. panta 1. punkts.

(46) Kā paskaidrots 41. un 42. apsvērumā, pēc tam *PIHBO* ir aizliegts apstrādāt personas datus citiem nolūkiem, izņemot, ja datu subjekts piekrīt šādai apstrādei vai ja ir piemērojama kāda no atkāpēm atbilstoši *APPI* 16. panta 3. punktam.

(47) Visbeidzot, attiecībā uz personas informācijas tālāku sniegšanu trešai personai ([31]) – *APPI* 23. panta 1. punkts atļauj šādu nodošanu tikai īpašos gadījumos, parasti ar datu subjekta iepriekšēju piekrišanu ([32]). *APPI* 23. panta 2., 3. un 4. punktā ir paredzēti izņēmumi attiecībā uz prasību saņemt piekrišanu. Tomēr šādi izņēmumi ir piemērojami tikai nesensitīviem datiem, un tiek prasīts, ka uzņēmējam ir iepriekš jāinformē attiecīgās personas par nodomu izpaust viņu personas informāciju trešai personai un par iespēju iebilst pret jebkādu turpmāku informācijas nodošanu ([33]).

(48) Attiecībā uz nosūtīšanu no Eiropas Savienības – personas datiem obligāti jābūt vispirms savāktiem un apstrādātiem ES, ievērojot Regulu (ES) 2016/679. Tas vienmēr ietvers datu vākšanu un apstrādi, arī nosūtīšanai no Eiropas Savienības uz Japānu, pamatojoties uz regulas 6. panta 1. punktā uzskaitītajiem juridiskajiem pamatiem, no vienas puses, un vākšanu konkrētos, skaidros un leģitīmos nolūkos, kā arī aizliegumu veikt datu turpmāku apstrādi, arī tos nosūtot, tādā veidā, kas ir pretrunā regulas 5. panta 1. punkta b) apakšpunktā un 6. panta 4. punktā noteiktajiem nolūkiem, no otras puses.

(49) Saskaņā ar 3. papildu noteikumu pēc nosūtīšanas *PIHBO*, kas saņem datus, ir "jāapstiprina" nosūtīšanas pamatā esošais(-ie) īpašais(-ie) nolūks(-i) (t. i., nolūks, kas norādīts atbilstoši Regulai (ES) 2016/679) un jāveic datu turpmāka apstrāde atbilstoši šādam(-iem) nolūkam(-iem) ([34]). Tas nozīmē, ka ne tikai sākotnējam šādu personas datu saņēmējam Japānā, bet arī katram nākamajam datu saņēmējam (ieskaitot pilnvaroto) ir saistošs(-i) regulā noteiktais(-ie) nolūks(-i).

(50) Turklāt, ja *PIHBO* vēlas mainīt nolūku, kas iepriekš noteikts atbilstoši Regulai (ES) 2016/679, saskaņā ar APPI 16. panta 1. punktu tam principā ir jāsaņem datu subjekta piekrišana. Ja minētā piekrišana nav saņemta, tad, veicot jebkādu datu apstrādi, kas pārsniedz apmēru, kurš ir nepieciešams izmantošanas nolūka sasniegšanai, tiek pārkāpts 16. panta 1. punkts, kura izpilde jānodrošina *PPC* un tiesām.

(51) Tātad, ņemot vērā, ka saskaņā ar Regulu (ES) 2016/679 datu nosūtīšanai ir vajadzīgs juridisks pamats un īpašs nolūks, kas tiek atspoguļoti izmantošanas nolūkā, kuru apstiprina saskaņā ar *APPI*, attiecīgie *APPI* noteikumi apvienojumā ar 3. papildu noteikumu nodrošina Japānā notiekošās ES datu apstrādes pastāvīgu likumīgumu.

2.3.3. *Datu precizitāte un minimizēšana*

(52) Datiem vajadzētu būt precīziem un nepieciešamības gadījumā atjauninātiem. Tiem arī vajadzētu būt adekvātiem, atbilstīgiem, un tiem būtu jāietver tikai tas, kas nepieciešams tiem nolūkiem, kādos tie tiek apstrādāti.

(53) Šie principi Japānas tiesību aktos tiek nodrošināti ar *APPI* 16. panta 1. punktu, kas aizliedz izmantot personas informāciju, pārsniedzot "apmēru, kas ir nepieciešams, lai sasniegtu izmantošanas nolūku". Kā paskaidrojusi *PPC*, tas ne tikai izslēdz datu izmantošanu, kas nav atbilstoša, un pārmērīgu datu izmantošanu (pārsniedzot to, kas ir nepieciešams izmantošanas nolūka sasniegšanai), bet arī ietver aizliegumu izmantot datus, kas nav būtiski izmantošanas nolūka sasniegšanai.

([31]) Lai arī pilnvarotie netiek pieskaitīti pie "trešām personām", 23. panta nolūkos (sk. 5. punktu) šo noteikumu piemēro tikai tiktāl, ciktāl pilnvarotais ar personas datiem rīkojas sava pilnvarojuma robežās ("nepieciešamais tvērums izmantošanas nolūka sasniegšanai"), t. i., darbojas kā datu apstrādātājs.

([32]) Citi (izņēmuma) pamati ir šādi: i) personas informācijas sniegšana, "pamatojoties uz normatīvajiem aktiem"; ii) gadījumi, "kad nepieciešams aizsargāt cilvēka dzīvību, veselību vai labklājību un kad ir sarežģīti saņemt principāla piekrišanu"; iii) gadījumi, "kad īpaši nepieciešams uzlabot sabiedrības higiēnu vai sekmēt bērnu veselības uzlabošanu un kad ir sarežģīti saņemt principāla piekrišanu"; un iv) gadījumi, "kad nepieciešams sadarboties ar centrālās valdības organizāciju vai vietējo valdību, vai ar personu, kurai valdība uzticējusi īstenot normatīvajos aktos noteiktās lietas, un ja pastāv iespēja, ka principāla piekrišanas saņemšana traucētu minēto lietu īstenošanai".

([33]) Sniedzamā informācija jo īpaši ietver personas datu kategorijas, ar ko plānots dalīties ar trešo personu, un nosūtīšanas metodi. Turklāt *PIHBO* ir jāinformē datu subjekts par iespēju iebilst pret nosūtīšanu un par to, kā iesniegt šādu pieprasījumu.

([34]) Saskaņā ar *APPI* 26. panta 1. punkta ii) apakšpunktu *PIHBO*, saņemot personas datus no trešās personas, ir "jāapstiprina" (jāpārbauda) sīka informācija par personas datu nonākšanu trešās personas rīcībā, tostarp šādas datu saņemšanas nolūks. Lai gan 26. pantā nav skaidri noteikts, ka *PIHBO* vēlāk ir jāievēro minētais nolūks, to skaidri nosaka 3. papildu noteikums.

(54) Attiecībā uz pienākumu nodrošināt datu precizitāti un atjaunināšanu *APPI* 19. pantā ir noteikts, ka *PIHBO* "cenšas nodrošināt personas datu precizitāti un atjaunināšanu tādā apmērā, kas nepieciešams izmantošanas nolūka sasniegšanai". Minētais noteikums būtu jālasa saistībā ar *APPI* 16. panta 1. punktu – saskaņā ar skaidrojumiem, kas saņemti no *PPC*, ja *PIHBO* neievēro noteiktos precizitātes standartus, tiks uzskatīts, ka personas informācijas apstrādē netiek sasniegts izmantošanas nolūks, un tādējādi informācijas izmantošana tiks uzskatīta par nelikumīgu saskaņā ar 16. panta 1. punktu.

2.3.4. *Glabāšanas ierobežojums*

(55) Dati principā būtu jāglabā ne ilgāk, kā nepieciešams nolūkiem, kādos attiecīgos personas datus apstrādā.

(56) Saskaņā ar *APPI* 19. pantu *PIHBO* ir "jācenšas (…) nekavējoties dzēst personas datus, kad šāda izmantošana ir kļuvusi lieka". Minēto noteikumu nepieciešams lasīt saistībā ar *APPI* 16. panta 1. punktu, kas aizliedz izmantot personas informāciju, pārsniedzot "apmēru, kas ir nepieciešams, lai sasniegtu izmantošanas nolūku". Tiklīdz izmantošanas nolūks ir sasniegts, personas informācijas apstrādi vairs nevar uzskatīt par nepieciešamu, un tāpēc to nevar turpināt (izņemot, ja *PIHBO* saņem datu subjekta piekrišanu, lai to darītu).

2.3.5. *Datu drošība*

(57) Personas dati būtu jāapstrādā tā, ka tiek nodrošināta to drošība, kas ietver aizsardzību pret neatļautu vai nelikumīgu apstrādi un pret nejaušu nozaudēšanu, iznīcināšanu vai sabojāšanu. Tālab uzņēmējiem būtu jāveic atbilstoši tehniski vai organizatoriski pasākumi, lai aizsargātu personas datus no iespējamiem apdraudējumiem. Šie pasākumi būtu jānovērtē, ņemot vērā faktisko situāciju un saistītās izmaksas.

(58) Šis princips Japānas tiesību aktos ir ieviests ar *APPI* 20. pantu, kas nosaka, ka *PIHBO* "veic nepieciešamos un atbilstošos pasākumus, lai nodrošinātu personas datu drošības kontroli, tostarp novērstu personas datu, ko tas izmanto, noplūšanu, nozaudēšanu vai sabojāšanu". *PPC* pamatnostādnēs ir izskaidroti veicamie pasākumi, tostarp pamatpolitikas noteikšanas metodes, datu izmantošanas noteikumi un dažādas "kontroles darbības" (attiecībā uz organizatorisko drošību, kā arī cilvēku, fizisko un tehnoloģisko drošību) ([35]). Turklāt *PPC* pamatnostādnēs un īpašā paziņojumā (8. pielikums "Veicamo drošības pārvaldības pasākumu saturs"), ko publicējusi *PPC*, ir ietverta sīkāka informācija par pasākumiem saistībā ar drošības incidentiem, kas ietver, piemēram, personas informācijas noplūšanu, *PIHBO* veicamo drošības pārvaldības pasākumu ietvaros ([36]).

(59) Turklāt ikreiz, kad personas informāciju izmanto darbinieki vai apakšuzņēmēji, jānodrošina "nepieciešamā un atbilstošā uzraudzība" saskaņā ar *APPI* 20. un 21. pantu drošības kontroles nolūkos. Visbeidzot, saskaņā ar *APPI* 83. pantu par personas informācijas tīšu nopludināšanu vai zādzību ir paredzēts brīvības atņemšanas sods līdz vienam gadam.

2.3.6. *Pārredzamība*

(60) Datu subjektiem vajadzētu būt informētiem par viņu personas datu apstrādes galvenajām iezīmēm.

(61) *APPI* 18. panta 1. punkts nosaka, ka *PIHBO* informācija par saņemtās personas informācijas izmantošanas nolūku ir jādara zināma datu subjektam, izņemot "gadījumus, kad izmantošanas nolūks ir iepriekš publiski paziņots". Tas pats attiecas uz gadījumu, kad ir atļauts mainīt nolūku (18. panta 3. punkts). Tādējādi tiek nodrošināts datu subjekts ir informēts par to, ka tiek vākti viņa dati. Lai gan *APPI* neparedz vispārēju prasību, ka *PIHBO* ir jāinformē datu subjekts par paredzamajiem personas informācijas saņēmējiem informācijas vākšanas posmā, šāda informēšana ir nepieciešams priekšnosacījums, lai varētu veikt jebkādu turpmāku informācijas nodošanu trešai personai (saņēmējam), pamatojoties uz 23. panta 2. punktu, tātad, ja tas tiek darīts bez datu subjekta iepriekšējas piekrišanas.

([35]) *PPC* pamatnostādnes (Vispārējo noteikumu izdevums), 41. lpp. un 86.–98. lpp.

([36]) Saskaņā ar *PPC* pamatnostādņu 3-3-2. iedaļu, ja notiek šāda noplūde, sabojāšana vai nozaudēšana, PIHBO ir jāveic nepieciešamā izmeklēšana un jo īpaši jānovērtē personas tiesību un interešu pārkāpuma apmērs, kā arī attiecīgās personas informācijas raksturs un apjoms.

(62) Attiecībā uz saglabātiem personas datiem APPI 27. pants nosaka, ka *PIHBO* informē datu subjektu par savu identitāti, izmantošanas nolūku un kārtību atbildes sniegšanai uz pieprasījumu par datu subjekta individuālajām tiesībām atbilstoši *APPI* 28., 29. un 30. pantam.

(63) Tā kā saskaņā ar Papildu noteikumiem personas dati, ko nosūta no Eiropas Savienības, tiks uzskatīti par "saglabātiem personas datiem" neatkarīgi no to glabāšanas ilguma (ja vien nepiemēro izņēmumus), uz tiem vienmēr attiecinās pārredzamības prasības atbilstoši abiem iepriekšminētajiem noteikumiem.

(64) Gan 18. panta prasībām, gan pienākumam informēt par izmantošanas nolūku atbilstoši *APPI* 27. pantam piemēro vienu un to pašu izņēmumu kopumu, kas galvenokārt balstīts uz sabiedrības interešu apsvērumiem un datu subjekta, trešo personu un pārziņa tiesību un interešu aizsardzību ([37]). Saskaņā ar *PPC* pamatnostādnēs sniegto interpretāciju minētie izņēmumi ir piemērojami ļoti īpašās situācijās, piemēram, ja informēšana par izmantošanas nolūku varētu kaitēti leģitīmajiem pasākumiem, ko veic uzņēmējs, lai aizsargātu konkrētas intereses (piemēram, cīņa pret krāpšanu, rūpniecisko spiegošanu, sabotāžu).

2.3.7. *Īpašas datu kategorijas*

(65) Būtu vajadzīgas īpašas garantijas gadījumos, kad tiek apstrādāti "īpašu kategoriju" dati.

(66) "Īpaši aizsargājama personas informācija" ir definēta *APPI* 2. panta 3. punktā. Minētajā noteikumā ir atsauce uz "personas informāciju, kas ietver principāla rasi, pārliecību, sociālo stāvokli, slimības vēsturi, sodāmību, faktus par nozieguma rezultātā nodarītu kaitējumu citu informāciju, kas ar Ministru kabineta rīkojumu noteikta par tādu, kuras izmantošanā jāievēro īpaša rūpība, lai neradītu negodīgu diskrimināciju, kaitējumu vai citas neizdevīgas situācijas principālam". Šīs kategorijas atbilst lielai daļai sensitīvo datu, kas uzskaitīti Regulas (ES) 2016/679 9. un 10. pantā. Jo īpaši "slimības vēsture" atbilst veselības datiem, savukārt "sodāmība un fakti par nozieguma rezultātā nodarītu kaitējumu" pēc būtības atbilst kategorijām, kas minētas Regulas (ES) 2016/679 10. pantā. *APPI* 2. panta 3. punktā minētās kategorijas ir plašāk interpretētas Ministru kabineta rīkojumā un *PPC* pamatnostādnēs. Saskaņā ar *PPC* pamatnostādņu 2.3. iedaļas 8. punktu "slimības vēstures" apakškategorijas, kas sīkāk aprakstītas Ministru kabineta rīkojuma 2. panta ii) un iii) punktā, interpretē kā tādas, kuras ietver ģenētiskos un biometriskos datus. Tāpat arī, lai gan uzskaitījumā nav skaidri ietverti jēdzieni "etniskā izcelsme" un "politiskie uzskati", tajā tomēr ir atsauces uz "rasi" un "pārliecību". Kā paskaidrots *PPC* pamatnostādņu 2.3. iedaļas 1. un 2. punktā, atsauce uz "rasi" ietver arī "etniskās saites vai saikni ar konkrētu pasaules daļu", savukārt ar "pārliecību" saprot gan reliģisko pārliecību, gan politiskos uzskatus.

(67) Kā ir saprotams no šā noteikuma formulējuma, uzskaitījums nav izsmeļošs, jo to var papildināt ar citām datu kategorijām, ciktāl to apstrāde rada "negodīgas diskriminācijas, kaitējumu vai citas neizdevīgas situācijas risku principālam".

(68) Lai gan "sensitīvu" datu jēdziens ir sociāls konstrukts tādā ziņā, ka tas sakņojas konkrētas sabiedrības kultūras un tiesību tradīcijās, morāles apsvērumos, politikas izvēlēs utt., ņemot vērā, cik svarīgi ir nodrošināt atbilstošas garantijas attiecībā uz sensitīviem datiem, kad tos nosūta uzņēmējiem Japānā, Komisija ir panākusi, ka īpašie aizsardzības pasākumi, kas Japānas tiesību aktos ir paredzēti "īpaši aizsargājamai personas informācijai", ir attiecināmi uz visām kategorijām, kas Regulā (ES) 2016/679 atzītas par "sensitīviem datiem". Šajā nolūkā 1. papildu noteikums paredz, ka datus, ko nosūta no Eiropas Savienības un kas attiecas uz personas seksuālo dzīvi, seksuālo orientāciju vai dalību arodbiedrībās, *PIHBO* apstrādā "tāpat kā īpaši aizsargājamu personas informāciju [*APPI*] 2. panta 3. punkta nozīmē".

([37]) Tie ir i) gadījumi, kad pastāv iespēja, ka datu subjekta informēšana par izmantošanas nolūku vai nolūka publiska paziņošana "kaitētu principāla vai trešās personas dzīvībai, veselībai, labklājībai vai citām tiesībām un interesēm" vai "(…) *PIHBO* tiesībām un leģitīmajām interesēm"; ii) gadījumi, kad "ir jāsadarbojas ar centrālās valdības organizāciju vai vietējo valdību" tiesību aktos noteikto to uzdevumu izpildē un ja šāda informēšana vai izpaušana traucētu šādām "lietām"; iii) gadījumi, kad izmantošanas nolūks ir skaidrs, ņemot vērā situāciju, kādā dati iegūti.

(69) Attiecībā uz būtiskajām papildu garantijām, kas piemērojamas īpaši aizsargājamai personas informācijai, saskaņā ar *APPI* 17. panta 2. punktu *PIHBO* nav atļauts iegūt šādus datus bez attiecīgās personas iepriekšējas piekrišanas, ar ierobežotiem izņēmumiem ([38]). Turklāt attiecībā uz šo personas informācijas kategoriju ir izslēgta iespēja izpaust šādu informāciju trešām personām, pamatojoties uz procedūru, kas paredzēta *APPI* 23. panta 2. punktu (kas ļauj nosūtīt datus trešām personām bez attiecīgās personas iepriekšējas piekrišanas).

2.3.8. *Pārskatatbildība*

(70) Saskaņā ar pārskatatbildības principu vienībām, kas apstrādā datus, ir jāievieš atbilstoši tehniskie un organizatoriskie pasākumi, lai tās efektīvi izpildītu savus datu aizsardzības pienākumus, un jāspēj pierādīt šādu izpildi, jo īpaši kompetentajai uzraudzības iestādei.

(71) Kā minēts 34. zemsvītras piezīmē (49. apsvērums), *PIHBO* saskaņā ar *APPI* 26. panta 1. punktu ir jāpārbauda tās trešās personas identitāte, kura tiem sniedz personas datus, un "apstākļi", kādos trešā persona ieguvusi šādus datus (tādu personas datu gadījumā, uz kuriem attiecas šis lēmums, saskaņā ar *APPI* un 3. papildu noteikumu minētie apstākļi ietver faktu, ka datu izcelsme ir Eiropas Savienībā, kā arī datu nosūtīšanas sākotnējo nolūku). Cita starpā šā pasākuma mērķis ir nodrošināt datu apstrādes likumību visā to *PIHBO* ķēdē, kuri izmanto personas datus. Turklāt saskaņā ar *APPI* 26. panta 3. punktu *PIHBO* ir jāreģistrē saņemšanas datums un (obligātā) informācija, kas saņemta no trešās personas atbilstoši 1. punktam, kā arī attiecīgās personas (datu subjekta) vārds, apstrādāto datu kategorijas un – ciktāl piemērojams – fakts, ka datu subjekts ir devis piekrišanu savu personas datu apmaiņai. Kā norādīts *PPC* noteikumu 18. pantā, šī reģistrētā informācija ir jāglabā vismaz vienu līdz trīs gadus atkarībā no apstākļiem. *PPC* savu uzdevumu izpildē var prasīt šādas reģistrētās informācijas iesniegšanu ([39]).

(72) *PIHBO* ir nekavējoties un pienācīgi jāizskata attiecīgo personu sūdzības par viņu personas informācijas apstrādi. Lai veicinātu sūdzību izskatīšanu, *PIHBO* izveido "sistēmu, kas nepieciešama [šā] mērķa sasniegšanai", kas nozīmē, ka tiem būtu jāievieš savā organizācijā atbilstošas procedūras (piemēram, jāsadala pienākumi vai jānorāda kontaktpersona).

(73) Visbeidzot, *APPI* rada satvaru nozaru organizāciju līdzdalībai augsta izpildes līmeņa nodrošināšanā (sk. IV nodaļas 4. iedaļu). Šādu akreditētu personas informācijas aizsardzības organizāciju ([40]) uzdevums ir veicināt personas informācijas aizsardzību, atbalstot uzņēmumus ar savas zinātības starpniecību, kā arī sekmēt garantiju ieviešanu, jo īpaši izskatot personu sūdzības un palīdzot risināt saistītus konfliktus. Šajā nolūkā tās var prasīt, lai iesaistītie *PIHBO* attiecīga gadījumā pieņem nepieciešamos pasākumus ([41]). Turklāt datu aizsardzības pārkāpumu vai citu drošības incidentu gadījumā *PIHBO* principā informē *PPC*, kā arī datu subjektu (vai sabiedrību) un īsteno nepieciešamās darbības, tostarp pasākumus, lai mazinātu jebkādu kaitējumu un novērstu līdzīgu incidentu atkārtošanos ([42]). Lai gan tās ir brīvprātīgas shēmas, *PPC* 2017. gada 10. augustā iekļāva sarakstā 44 organizācijas, vislielākajai no kurām, proti, Japānas Informācijas apstrādes un attīstības centram (*JIPDEC*), vien ir 15 436 iesaistītu

([38]) Izņēmumi ir šādi: i) "gadījumi, kas pamatoti ar normatīvajiem aktiem"; ii) "gadījumi, kad nepieciešams aizsargāt cilvēka dzīvību, veselību vai labklājību un kad ir sarežģīti saņemt principāla piekrišanu"; iii) "gadījumi, kad īpaši nepieciešams uzlabot sabiedrības higiēnu vai sekmēt bērnu veselības uzlabošanu un kad ir sarežģīti saņemt principāla piekrišanu"; iv) "gadījumi, kad nepieciešams sadarboties ar centrālās valdības organizāciju vai vietējo valdību, vai ar personu, kurai valdība uzticējusi īstenot normatīvajos aktos noteiktās lietas, un ja pastāv iespēja, ka principāla piekrišanas saņemšana traucētu minēto lietu īstenošanai"; un v) gadījumi, kad minēto īpaši aizsargājamo personas informāciju publiski izpauž datu subjekts, valdības organizācija, vietējā pašvaldība, persona, kura atbilst kādai no 76. panta 1. punktā norādītajām kategorijām, vai citas personas, kas noteiktas *PPC* noteikumos." Vēl vienā kategorijā ietilpst "citi gadījumi, kas Ministru kabineta rīkojumā atzīti par tādiem, kuri ir līdzvērtīgi katrā iepriekšējā pozīcijā minētajiem gadījumiem", un saskaņā ar pašreizējo Ministru kabineta rīkojumu tā jo īpaši ietver skaidri redzamas personas iezīmes (piem., redzamu veselības stāvokli), ja sensitīvie dati (netīši) iegūti vizuālos novērojumos, filmējot vai fotografējot datu subjektu, piem., ar videonovērošanas kamerām.

([39]) Saskaņā ar *APPI* 40. panta 1. punktu *PPC*, ciktāl tas ir nepieciešams attiecīgo *APPI* noteikumu īstenošanai, var prasīt, lai *PIHBO* iesniedz nepieciešamo informāciju vai materiālus saistībā ar personas informācijas izmantošanu.

([40]) *APPI* cita starpā ir paredzēti noteikumi par šādu organizāciju akreditāciju; sk. *APPI* 47.–50. pantu.

([41]) *APPI* 52. pants.

([42]) *PPC* paziņojums Nr. 1/2017 "Par darbībām, kas veicamas gadījumos, kad ir noticis personas datu aizsardzības pārkāpums vai cits incidents".

uzņēmēju ([43]). Akreditētajās shēmās ir nozaru asociācijas, piemēram, Japānas Vērtspapīru tirgotāju asociācija, Japānas Autoskolu asociācija vai Kāzu rīkotāju asociācija ([44]).

(74) Akreditētās personas informācijas aizsardzības organizācijas iesniedz gada ziņojumus par savu darbību. Saskaņā ar Pārskatu par situāciju *APPI* īstenošanas jomā 2015. finanšu gadā, ko publicējusi *PPC*, akreditētās personas informācijas aizsardzības organizācijas saņēma kopumā 442 sūdzības, pieprasīja 123 paskaidrojumus no uzņēmējiem, kas bija to piekritības jomā, 41 gadījumā pieprasīja dokumentus no minētajiem uzņēmējiem un sniedza 181 norādījumu un 2 ieteikumus ([45]).

2.3.9. *Ierobežojumi attiecībā uz datu tālāku nosūtīšanu*

(75) Aizsardzības līmeni, kāds piešķirts personas datiem, kurus nosūta no Eiropas Savienības uzņēmējiem Japānā, nedrīkst ietekmēt šādu datu tālāka nosūtīšana saņēmējiem trešā valstī ārpus Japānas. Šāda tālāka nosūtīšana, kas no Japānas uzņēmēja skatpunkta ir starptautiska nosūtīšana no Japānas, būtu jāatļauj tikai tad, ja uz nākamo saņēmēju ārpus Japānas attiecina noteikumus, kuri nodrošina aizsardzības līmeni, kas ir līdzīgs Japānas tiesiskajā kārtībā garantētajam.

(76) Pirmais aizsardzības pasākums ir noteikts *APPI* 24. pantā, kas vispārēji aizliedz nosūtīt personas datus trešai personai ārpus Japānas teritorijas bez attiecīgās personas iepriekšējas piekrišanas. Savukārt 4. papildu noteikums nodrošina, ka gadījumā, kad datus nosūta no Eiropas Savienības, šāda piekrišana ir īpaši labi pārdomāta, jo tā paredz, ka attiecīgajai personai "tiek sniegta tā informācija par nosūtīšanas apstākļiem, kura principālam vajadzīga, lai pieņemtu lēmumu par savu piekrišanu". Pamatojoties uz to, datu subjekts tiek informēts par faktu, ka dati tiks nosūtīti uz ārzemēm (ārpus APPI piemērošanas jomas), un par konkrēto galamērķa valsti. Tas ļaus subjektam izvērtēt ar datu nosūtīšanu saistītos draudus privātumam. Tāpat no *APPI* 23. panta var secināt (sk. 47. apsvērumu), ka principālam sniegtajā informācijā būtu jāietver 2. punktā minētie obligātie elementi, proti, trešai personai sniegto personas datu kategorijas un datu izpaušanas metode.

(77) *APPI* 24. pants, to piemērojot apvienojumā ar *PPC* noteikumu 11-2. pantu, paredz vairākus izņēmumus attiecībā uz šo noteikumu, kas balstīts uz piekrišanu. Turklāt atbilstoši 24. pantam atkāpes, kas piemērojamas atbilstoši *APPI* 23. panta 1. punktam, ir piemērojamas arī attiecībā uz datu starptautisko nosūtīšanu ([46]).

(78) Lai nodrošinātu aizsardzības nepārtrauktību gadījumā, kad personas datus nosūta no Eiropas Savienības uz Japānu saskaņā ar šo lēmumu, 4. papildu noteikums paaugstina aizsardzības līmeni šādu datu tālākai nosūtīšanai, ko veic *PIHBO*, saņēmējam trešā valstī. Tas nosaka ierobežojumus un ietvarus starptautiskās nosūtīšanas pamatiem, ko *PIHBO* var izmantot kā alternatīvu piekrišanai. Konkrēti un neskarot *APPI* 23. panta 1. punktā noteiktās atkāpes, personas datus saskaņā ar šo lēmumu var nosūtīt (tālāk) bez piekrišanas tikai divos gadījumos, proti, i) kad datus nosūta uz trešo valsti, kuru *PPC* saskaņā ar *APPI* 24. pantu atzinusi par tādu, kas nodrošina Japānā garantētajam aizsardzības līmenim līdzvērtīgu aizsardzības līmeni ([47]), vai ii) kad *PIHBO* un saņēmējs, kas ir trešā persona, ir kopīgi īstenojuši pasākumus, kas nodrošina tādu pašu aizsardzības līmeni kā *APPI*, to lasot kontekstā ar Papildu noteikumiem, pamatojoties uz līgumu, citu veidu saistošiem nolīgumiem vai saistošiem nolīgumiem uzņēmumu grupā. Otrā kategorija ir instrumenti, ko izmanto atbilstoši Regulai (ES) 2016/679, lai nodrošinātu atbilstošas garantijas (jo īpaši līguma klauzulas un saistošus uzņēmuma noteikumus). Taču pat minētajos gadījumos uz datu nosūtīšana trešai personai attiecas vispārējie noteikumi, kas piemērojami jebkādai datu sniegšanai trešai personai saskaņā ar *APPI* (t. i., prasība par piekrišanas saņemšanu saskaņā ar *APPI* 23. panta 1. punktu vai alternatīvi – informācijas prasība ar iespēju nepiekrist saskaņā ar *APPI* 23. panta 2. punktu. Gadījumos, kad ar datu subjektu

([43]) Saskaņā ar skaitļiem, kas publicēti *JIPDEC PrivacyMark* tīmekļa vietnē un datēti ar 2017. gada 2. oktobri.
([44]) *PPC*, Akreditēto personas informācijas aizsardzības organizāciju saraksts, pieejams interneta vietnē: https://www.ppc.go.jp/personal/nintei/list/ vai https://www.ppc.go.jp/files/pdf/nintei_list.pdf
([45]) *PPC*, Pārskats par situāciju *APPI* īstenošanas jomā 2015. finanšu gadā (2016. gada oktobris), pieejams (tikai japāņu valodā) interneta vietnē: https://www.ppc.go.jp/files/pdf/personal_sekougaiyou_27ppc.pdf
([46]) Sk. 32. zemsvītras piezīmi.
([47]) Saskaņā ar *PPC* noteikumu 11. pantu tas nozīmē, ka ir vajadzīgi ne tikai reāli standarti, kas ir līdzvērtīgi *APPI* un ko efektīvi uzrauga neatkarīga tiesībaizsardzības iestāde, bet arī attiecīgo noteikumu īstenošanas nodrošināšana attiecīgajā trešā valstī.

nevar sazināties, lai tam iesniegtu piekrišanas pieprasījumu vai lai sniegtu nepieciešamo iepriekšējo informāciju saskaņā ar *APPI* 23. panta 2. punktu, datus nedrīkst nosūtīt.

(79) Tāpēc, izņemot gadījumus, kad *PPC* ir konstatējusi, ka attiecīgā trešā valsts nodrošina aizsardzības līmeni, kas ir līdzvērtīgs ar *APPI* garantētajam ([48]), 4. papildu noteikumā paredzētās prasības izslēdz tādu nosūtīšanas instrumentu izmantošanu, kuri nerada saistošas attiecības starp datu nosūtītāju Japānā un datu saņēmēju trešā valstī un kuri negarantē vajadzīgo aizsardzības līmeni. Kā piemēru var minēt *APEC* Pārrobežu privātuma noteikumu (*CBPR*) sistēmu, kurā Japāna ir iesaistītā tautsaimniecība ([49]), jo šajā sistēmā aizsardzība neizriet no vienošanās, kas saista datu nosūtītāju un saņēmēju to divpusējo attiecību kontekstā, un tās līmenis ir acīmredzami zemāks nekā tas, ko garantē *APPI* apvienojumā ar Papildu noteikumiem ([50]).

(80) Visbeidzot, papildu garantija (tālākas) nosūtīšanas gadījumā izriet no *APPI* 20. un 22. panta. Saskaņā ar šiem noteikumiem, ja uzņēmējs trešā valstī (datu saņēmējs) rīkojas *PIHBO* (datu nosūtītāja) vārdā, proti, kā (apakš-)apstrādātājs, tad *PIHBO* ir jānodrošina šāda uzņēmēja uzraudzība attiecībā uz datu apstrādes drošību.

2.3.10. *Individuālās tiesības*

(81) *APPI* tāpat kā ES datu aizsardzības tiesību akti piešķir personām vairākas īstenojamas tiesības. Tas ietver tiesības piekļūt datiem ("izpaušana"), tos labot un dzēst, kā arī tiesības iebilst ("izmantošanas izbeigšana").

(82) Pirmkārt, atbilstoši *APPI* 28. panta 1. un 2. punktam datu subjektam ir tiesības pieprasīt *PIHBO*, lai tas/tie "izpauž glabātus personas datus, pēc kuriem viņu var identificēt", un *PIHBO*, saņemot šādu pieprasījumu, "(…) izpauž glabātus personas datus" datu subjektam. *APPI* 29. pantam (labošanas tiesības) un 30. pantam (izmantošanas izbeigšanas tiesības) ir tāda pati struktūra kā 28. pantam.

(83) Ministru kabineta rīkojuma 9. pantā ir precizēts, ka personas informācijas izpaušana, kā minēts *APPI* 28. panta 2. punktā, notiek rakstiski, ja vien *PIHBO* un datu subjekts nav vienojušies citādi.

(84) Šīm tiesībām piemēro trīs veidu ierobežojumus, kas attiecas uz personas vai trešo personu tiesībām un interesēm ([51]), būtiskiem traucējumiem *PIHBO* darījumdarbībai ([52]), kā arī gadījumiem, kad izpaušana būtu citu normatīvo aktu pārkāpums ([53]). Situācijas, kurās šos ierobežojumus piemēro, ir līdzīgas dažiem no izņēmumiem, kuri piemērojami saskaņā ar Regulas (ES) 2016/679 23. panta 1. punktu, kas ļauj ierobežot personu tiesības tādu

([48]) *PPC* vēl nav pieņēmusi nevienu lēmumu saskaņā ar *APPI* 24. pantu, atzīstot trešo valsti par tādu, kas nodrošina Japānā garantētajam aizsardzības līmenim līdzvērtīgu aizsardzības līmeni. Vienīgais lēmums, kura pieņemšanu tā pašlaik apsver, attiecas uz EEZ. Attiecībā uz citiem iespējamiem lēmumiem nākotnē Komisija cieši uzraudzīs situāciju un vajadzības gadījumā veiks atbilstīgus pasākumus, lai novērstu iespējamo nelabvēlīgo ietekmi uz aizsardzības nepārtrauktību (sk. turpmāk 176., 177., 184. apsvērumu un 3. panta 1. punktu).

([49]) Lai gan tikai divi Japānas uzņēmumi ir sertificēti atbilstoši *APEC CBPR* sistēmai (sk. https://english.jipdec.or.jp/sp/protection_org/cbpr/list.html). Ārpus Japānas vienīgie citi uzņēmēji, kas ir sertificēti atbilstoši šai sistēmai, ir tikai 19 ASV uzņēmumi (sk. https://www.trustarc.com/consumer-resources/trusted-directory/#apec-list).

([50]) Piemēram, nav sensitīvu datu definīcijas un īpašu aizsardzības pasākumu, nav ierobežotas datu glabāšanas pienākuma. Sk. arī 29. panta darba grupas Atzinumu 02/2014 par atsauces materiālu saistībā ar prasībām, kuras piemēro attiecībā uz ES valstu datu aizsardzības iestādēm iesniegtiem saistošajiem uzņēmuma noteikumiem un *APEC CBPR* pārskatatbildības ekspertiem iesniegtiem pārrobežu privātuma noteikumiem, 2014. gada 6. marts.

([51]) Saskaņā ar *PPC* tikai šādas intereses var pamatot "tiesiskas aizsardzības vērtus" ierobežojumus. Šeit katrs gadījums ir jāizvērtē atsevišķi, "ņemot vērā ietekmi uz pamattiesībām uz privātumu, tai skaitā datu aizsardzību, kā tā atzīta Konstitūcijā un judikatūrā." Aizsargātas intereses var būt, piemēram, tirdzniecības vai citi komercnoslēpumi.

([52]) Jēdziens "būtiski traucē uzņēmējam pienācīgi veikt darījumdarbību" ir ilustrēts *PPC* pamatnostādnēs ar vairākiem piemēriem, kas cita starpā ietver atkārtotus un identiskus sarežģītus pieprasījumus, ko iesniedz viena un tā pati persona, ja šādi pieprasījumi ir saistīti ar ievērojamu slogu uzņēmējam, tādējādi ietekmējot tā spēju atbildēt uz citiem pieprasījumiem (*PPC* pamatnostādnes (Vispārējo noteikumu izdevums), 62. lpp.). Vispārīgākā nozīmē *PPC* ir apstiprinājusi, ka šī kategorija ir ierobežota ar izņēmuma gadījumiem, kas pārsniedz vienkāršas neērtības. Konkrēti, *PIHBO* nevar atteikties izpaust datus tikai tādēļ, ka tiek prasīts liels datu apjoms.

([53]) Kā to apstiprinājusi *PPC*, šādiem tiesību aktiem ir jārespektē tiesības uz privātumu, kā tas noteikts Konstitūcijā un tādējādi "ir nepieciešams un saprātīgs ierobežojums."

iemeslu dēļ, kuri saistīti ar "datu subjekta aizsardzību vai citu personu tiesību un brīvību aizsardzību" vai "citiem svarīgiem vispārējo sabiedrības interešu mērķiem". Lai gan to gadījumu kategorija, kuros izpaušana būtu "citu normatīvo aktu" pārkāpums, var šķist plaša, normatīvajos aktos, kas paredz ierobežojumus šajā saistībā, jābūt ievērotām konstitucionālajām tiesībām uz privātumu, un tie var noteikt ierobežojumus tikai tiktāl, ciktāl šo tiesību īstenošana "traucētu sabiedrības labklājībai" ([54]). Šim nolūkam ir nepieciešams līdzsvarot attiecīgās intereses.

(85) Saskaņā ar *APPI* 28. panta 3. punktu, ja prasītie dati nepastāv vai ja attiecīgais *PIHBO* izlemj nepiešķirt piekļuvi glabātajiem datiem, tam ir nekavējoties jāinformē attiecīgā persona.

(86) Otrkārt, atbilstoši *APPI* 29. panta 1. un 2. punktam datu subjektam ir tiesības pieprasīt viņa personas datu labošanu, papildināšanu vai dzēšanu, ja dati ir neprecīzi. Saņemot šādu pieprasījumu, *PIHBO* "veic (…) nepieciešamo izmeklēšanu" un, pamatojoties uz tās rezultātiem, "veic labojumu glabāto datu saturā".

(87) Treškārt, atbilstoši *APPI* 30. panta 1. un 2. punktam datu subjektam ir tiesības pieprasīt *PIHBO*, lai tas pārtrauc izmantot personas informāciju vai dzēš šādu informāciju, ja tā tiek izmantota, pārkāpjot 16. pantu (attiecībā uz nolūka ierobežojumu), vai ir nepienācīgi iegūta, pārkāpjot *APPI* 17. pantu (attiecībā uz iegūšanu ar viltu, izmantojot citus neatbilstošu līdzekļus, vai gadījumā, kad sensitīvi dati iegūti bez piekrišanas). Tāpat saskaņā ar *APPI* 30. panta 3. un 4. punktu personai ir tiesības pieprasīt *PIHBO*, lai tas pārtrauc informācijas sniegšanu trešai personai, ja tādējādi tiek pārkāpti *APPI* 23. panta 1. punkta vai 24. panta noteikumi (attiecībā uz sniegšanu trešām personām, ieskaitot starptautisku datu nosūtīšanu).

(88) Ja šāds pieprasījums ir pamatots, *PIHBO* nekavējoties pārtrauc datu izmantošanu vai to sniegšanu trešai personai, ciktāl tas nepieciešams, lai novērstu pārkāpumu vai – ja uz konkrēto gadījumu attiecas izņēmums (proti, ja izmantošanas pārtraukšana izraisītu īpaši lielas izmaksas) ([55]) – īstenotu nepieciešamos alternatīvos pasākumus nolūkā aizsargāt attiecīgās personas tiesības un intereses.

(89) Atšķirībā no ES tiesību aktiem *APPI* un attiecīgajos pakārtotajos noteikumos nav tiesību normu, kas konkrēti attiektos uz iespēju iebilst pret apstrādi tiešās tirgvedības vajadzībām. Tomēr šāda apstrāde saskaņā ar šo lēmumu notiek iepriekš Eiropas Savienībā savāktu personas datu nosūtīšanas kontekstā. Saskaņā ar Regulas (ES) 2016/679 21. panta 2. punktu datu subjektam vienmēr ir iespēja iebilst pret datu nosūtīšanu to apstrādei tiešās tirgvedības vajadzībām. Turklāt, kā paskaidrots 43. apsvērumā, saskaņā ar 3. papildu noteikumu *PIHBO* dati, ko tas saņēmis atbilstoši lēmumam, ir jāapstrādā tādam pašam nolūkam, kādam tie nosūtīti no Eiropas Savienības, izņemot, ja datu subjekts piekrīt izmantošanas nolūka maiņai. Tāpēc, ja dati nosūtīti jebkādam nolūkam, kas nav tiešā tirgvedība, *PIHBO* Japānā būs aizliegts apstrādāt datus tiešās tirgvedības vajadzībām bez ES datu subjekta piekrišanas.

(90) Visos gadījumos, kas minēti *APPI* 28. un 29. pantā, *PIHBO* ir nekavējoties jāinformē attiecīgā persona par tās pieprasījuma rezultātu un turklāt ir jāpaskaidro katrs (daļējais) atteikums, pamatojoties uz 27.–30. pantā paredzētajiem likumiskajiem izņēmumiem (*APPI* 31. pants).

([54]) Augstākā tiesa ir interpretējusi Konstitūcijas 13. pantu tādējādi, ka tas paredz tiesības uz privātumu (sk. 7. un 8. apsvērumu iepriekš). Lai arī šīs tiesības var ierobežot gadījumos, kad tās "traucē sabiedrības labklājībai", Augstākā tiesa savā 2008. gada 6. marta spriedumā (sk. 8. apsvērumu) skaidri norādīja, ka jebkādi ierobežojumi (kas šajā gadījumā ļauj valsts iestādei vākt un apstrādāt personas datus) ir jālīdzsvaro ar tiesībām uz privātumu, ņemot vērā tādus faktorus kā attiecīgo datu būtība, riski, ko šo datu apstrāde rada privātpersonām, piemērojamie aizsardzības pasākumi un no apstrādes izrietošais labums sabiedrībai. Šī prasība ir ļoti līdzīga līdzsvarošanas veidam, kas, pirms tiek atļauti jebkādi datu aizsardzības tiesību un pasākumu ierobežojumi, ir prasīts ES tiesībās, pamatojoties uz nepieciešamības un proporcionalitātes principiem.

([55]) Plašākus skaidrojumus par šiem izņēmumiem sk. profesora *Katsuya Uga* komentāros par katru no pantiem pārskatītajā Likumā par personas informācijas aizsardzību, 2015. gads, 217. lpp. Piemēram, pieprasījums izraisītu lielas izmaksas gadījumā, kad tikai daži garā sarakstā (piem., izziņu grāmatā) iekļauti vārdi tiek apstrādāti, pārkāpjot nolūka ierobežojuma principu, un izziņu grāmata jau ir pārdošanā, tāpēc attiecīgo kopiju atsaukšana un aizstāšana ar jaunām izmaksātu ļoti dārgi. Tajā pašā piemērā, ja izziņu grāmatas eksemplāri jau ir pārdoti daudziem cilvēkiem un ir neiespējami tos visus atgūt, tad būtu arī "grūti izpildīt izmantošanas pārtraukšanas prasību". Šajos scenārijos nepieciešamā alternatīvā rīcība varētu būt, piemēram, kļūdu labojuma publicēšana vai izplatīšana. Šāda rīcība neizslēdz cita veida (tiesiskās) aizsardzības līdzekļu izmantošanu, piemēram, lai vērstos pret privātuma tiesību aizskārumu, kaitējumu reputācijai (neslavas celšanu), ko izraisījusi publicēšana, vai citu interešu pārkāpumu.

(91) Attiecībā uz nosacījumiem šāda pieprasījuma iesniegšanai *APPI* 32. pants (apvienojumā ar Ministru kabineta rīkojumu) ļauj *PIHBO* noteikt pamatotas procedūras, tostarp attiecībā uz informāciju, kas vajadzīga, lai identificētu glabātos personas datus. Tomēr saskaņā ar šā panta 4. punktu *PIHBO* nedrīkst uzlikt "pārmērīgu slogu principālam". Konkrētos gadījumos *PIHBO* var arī piemērot maksu, kamēr vien tās summa atbilst "apjomam, kas uzskatāms par pamatotu, ņemot vērā faktiskās izmaksas" (*APPI* 33. pants).

(92) Visbeidzot, persona var iebilst pret savas personas informācijas sniegšanu trešai personai atbilstoši *APPI* 23. panta 2. punktam vai atteikt piekrišanu atbilstoši 23. panta 1. punktam (tādējādi novēršot izpaušanu gadījumā, kad nav pieejams neviens cits juridiskais pamats). Tāpat persona var apturēt datu apstrādi, kas tiek veikta citam nolūkam, atsakoties sniegt piekrišanu atbilstoši *APPI* 16. panta 1. punktam.

(93) Atšķirībā no ES tiesību aktiem *APPI* un attiecīgajos pakārtotajos noteikumos nav ietverti vispārēji noteikumi, kas konkrēti attiektos uz lēmumiem, kuri skar datu subjektu un ir balstīti vienīgi uz personas datu automatizētu apstrādi. Tomēr šis jautājums ir aplūkots konkrētos nozaru noteikumos, kas piemērojami Japānā un ir īpaši būtiski attiecībā uz šā veida apstrādi. Tas ietver nozares, kurās uzņēmumi visbiežāk izmanto personas datu automatizētu apstrādi, lai pieņemtu lēmumus, kas skar konkrētas personas (piem., finanšu nozare). Piemēram, Vispārējās pamatnostādnēs par lielo banku uzraudzību, kas pārskatītas 2017. gada jūnijā, ir noteikts pienākums sniegt attiecīgajai personai paskaidrojumus par iemesliem, kādēļ ir noraidīts pieprasījums par aizdevuma līguma noslēgšanu. Minētie noteikumi tādējādi nodrošina aizsardzību tajos (visdrīzāk nedaudzajos) gadījumos, kad automātiskus lēmumus pieņemtu pats datus saņemošais Japānas uzņēmējs (nevis nosūtošais ES datu pārzinis).

(94) Jebkurā gadījumā attiecībā uz personas datiem, kas vākti Eiropas Savienībā, ikvienu lēmumu, pamatojoties uz automatizētu apstrādi, parasti pieņems datu pārzinis Savienībā (kam ir tieša saistība ar attiecīgo datu subjektu), un tam attiecīgi piemēro Regulu (ES) 2016/679 ([56]). Tas ietver nosūtīšanas scenārijus, kuros apstrādi veic ārvalstu (piem., Japānas) uzņēmējs, kas rīkojas kā pārstāvis (apstrādātājs) ES pārziņa vārdā (vai kā apakšapstrādātājs, kas rīkojas ES apstrādātāja vārdā, kurš ir saņēmis datus no ES pārziņa, kas tos savācis), kurš uz šī pamata pieņem lēmumu. Tāpēc tas, ka *APPI* nav īpašu noteikumu par automatizētu lēmumu pieņemšanu, visticamāk, neietekmēs saskaņā ar šo lēmumu nosūtīto personas datu aizsardzības līmeni.

2.4. **Pārraudzība un izpilde**

2.4.1. *Neatkarīga pārraudzība*

(95) Lai nodrošinātu, ka arī praksē tiek garantēts pietiekams datu aizsardzības līmenis, vajadzētu būt izveidotai neatkarīgai uzraudzības iestādei, kurai uzticētas pilnvaras uzraudzīt un nodrošināt datu aizsardzības noteikumu izpildi. Šai iestādei tās uzdevumi būtu jāveic un pilnvaras jāīsteno pilnīgi neatkarīgi un objektīvi.

(96) Japānā par *APPI* uzraudzību un izpildi atbildīgā iestāde ir *PPC*. Tās sastāvā ir priekšsēdētājs un astoņi komisāri, kurus iecēlis premjerministrs ar abu Parlamenta palātu piekrišanu. Priekšsēdētāja un visu komisāru pilnvaru termiņš ir pieci gadi, un ir iespēja viņus iecelt atkārtoti (*APPI* 64. pants). Komisārus var atlaist tikai pamatota iemesla dēļ ierobežotos izņēmuma apstākļos ([57]), un viņi nedrīkst aktīvi iesaistīties politiskās darbībās. Vēl vairāk – saskaņā ar *APPI* pilnas slodzes komisāriem jāatturas no jebkādām citām darbībām, par kurām saņem atlīdzību, vai darījumdarbības. Uz visiem komisāriem attiecas arī iekšējie noteikumi, kas viņiem liedz piedalīties apspriedēs iespējama interešu konflikta gadījumā. *PPC* palīdz sekretariāts, ko vada ģenerālsekretārs un kas izveidots, lai veiktu uzdevumus, kuri uzticēti *PPC* (*APPI* 70. pants). Gan komisāriem, gan visām sekretariāta amatpersonām ir saistoši stingri konfidencialitātes noteikumi (*APPI* 72., 82. pants).

([56]) Turpretī izņēmuma gadījumā, kad Japānas uzņēmējam ir tieša saistība ar datu subjektu no ES, šāda saistība parasti ir rezultāts tam, ka Japānas uzņēmējs ir mērķtiecīgi vērsies pie šīs personas Eiropas Savienībā, piedāvājot tai preces vai pakalpojumus vai vērojot tās uzvedību. Šajā scenārijā uz Japānas uzņēmēju attiecas Regulas (ES) 2016/679 piemērošanas joma (3. panta 2. punkts), un tāpēc tam ir tieši jāievēro ES datu aizsardzības tiesību akti.

([57]) Saskaņā ar *APPI* 65. pantu komisāra atlaišana pret viņa gribu ir iespējama tikai ar kādu no šiem pamatojumiem: i) bankrota procedūras sākšana; ii) notiesāšana par *APPI* vai Datu izmantošanas likuma pārkāpumu; iii) notiesāšana, piespriežot cietumsodu bez piespiedu darba vai vēl bargāku soda mēru; iv) nespēja pildīt pienākumus garīgu vai fizisku traucējumu dēļ vai amatpārkāpuma dēļ.

(97) *PPC* pilnvaras, ko tā īsteno pilnīgi neatkarīgi ([58]), ir paredzētas galvenokārt *APPI* 40., 41. un 42. pantā. Saskaņā ar 40. pantu *PPC* var prasīt *PIHBO*, lai tas ziņo vai iesniedz dokumentus par apstrādes darbībām, un *PPC* var arī veikt gan pārbaudes uz vietas, gan uzskaites un citu dokumentu pārbaudes. Ciktāl tas nepieciešams *APPI* izpildes nodrošināšanai, *PPC* var arī sniegt *PIHBO* norādījumus vai padomus par personas informācijas izmantošanu. *PPC* jau ir izmantojusi šīs pilnvaras saskaņā ar *APPI* 41. pantu, sniedzot norādījumus *Facebook* pēc tam, kad tika atklāti fakti *Facebook* un *Cambridge Analytica* lietā.

(98) Bet vissvarīgākais ir tas, ka *PPC* ir pilnvaras, pamatojoties uz sūdzību vai pēc savas iniciatīvas, individuālos gadījumos izdot ieteikumus un rīkojumus, lai nodrošinātu *APPI* un citu saistošu noteikumu (tostarp Papildu noteikumu) izpildi. Minētās pilnvaras ir noteiktas *APPI* 42. pantā. Lai gan minētā panta 1. un 2. punktā ir paredzēts divposmu mehānisms, kuru izmantojot, *PPC* var izdot rīkojumu (tikai) pēc iepriekšēja ieteikuma, 3. punkts ļauj tieši pieņemt rīkojumu steidzamības gadījumos.

(99) Lai arī ne visi *APPI* IV nodaļas 1. iedaļas noteikumi ir uzskaitīti 42. panta 1. punktā, kas nosaka arī 42. panta 2. punkta piemērošanas jomu, – tas ir skaidrojams ar faktu, ka daži no minētajiem noteikumiem neattiecas uz *PIHBO* ([59]) pienākumiem un ka visus būtiskos aizsardzības pasākumus jau nodrošina citi noteikumi, kuri ir iekļauti minētajā sarakstā. Piemēram, lai gan nav minēts 15. pants (kas paredz, ka *PIHBO* ir jānosaka izmantošanas nolūks un jāapstrādā attiecīgā personas informācija tikai tās apmērā), šīs prasības neievērošana var būt iemesls, lai izdotu ieteikumu, pamatojoties uz to, ka ir pārkāpts 16. panta 1. punkts (kas aizliedz *PIHBO* apstrādāt personas informāciju, pārsniedzot to, kas ir nepieciešams, lai sasniegtu izmantošanas nolūku, izņemot, ja tas saņem datu subjekta piekrišanu) ([60]). Vēl viens noteikums, kas nav iekļauts 42. panta 1. punktā, ir *APPI* 19. pants par datu precizitāti un glabāšanu. Šā noteikuma neievērošanas gadījumā var tikt piemēroti izpildes pasākumi par 16. panta 1. punkta pārkāpumu vai pamatojoties uz 29. panta 2. punkta pārkāpumu, ja attiecīgā persona prasa labot vai dzēst kļūdainus vai pārmērīga apjoma datus un *PIHBO* atsakās izpildīt šo prasību. Attiecībā uz datu subjekta tiesībām saskaņā ar 28. panta 1. punktu, 29. panta 1. punktu un 30. panta 1. punktu pārraudzība, kas jāveic *PPC*, tiek nodrošināta, piešķirot tai izpildes pilnvaras attiecībā uz konkrētajiem *PIHBO* pienākumiem, kuri noteikti minētajos pantos.

(100) Atbilstoši *APPI* 42. panta 1. punktam, ja *PPC* atzīst, ka ir "vajadzība aizsargāt personas tiesības un intereses gadījumos, kad [*PIHBO*] ir pārkāpis" konkrētus *APPI* noteikumus, tā var izdot ieteikumu "izbeigt pārkāpumu vai veikt nepieciešamos pasākumus, lai izlabotu pārkāpumu". Šāds ieteikums nav saistošs, bet paver iespēju izdot saistošu rīkojumu atbilstoši *APPI* 42. panta 2. punktam. Pamatojoties uz šo noteikumu, ja ieteikums netiek izpildīts "bez likumīga pamata" un *PPC* "atzīst, ka pastāv nenovēršams būtisks personas tiesību un interešu pārkāpums", *PPC* var uzdot *PIHBO* rīkoties atbilstoši ieteikumam.

(101) Papildu noteikumos ir sīkāk precizētas un pamatotas *PPC* izpildes pilnvaras. Konkrētāk, gadījumos, kas saistīti ar datiem, kuri nosūtīti no Eiropas Savienības, *PPC* vienmēr uzskatīs *PIHBO* nerīkošanos bez likumīga pamata atbilstoši ieteikumam, kas izdots saskaņā ar *APPI* 42. panta 1. punktu, par nenovēršamu un būtisku personas tiesību un interešu pārkāpumu 42. panta 2. punkta nozīmē un attiecīgi arī par pārkāpumu, kas pamato saistoša rīkojuma izdošanu. Turklāt par ieteikuma neizpildes "likumīgu pamatu" *PPC* atzīst tikai "ārkārtas gadījumu [kas liedz īstenot izpildi], kas ir ārpus [*PIHBO*] kontroles un ko nevar pamatoti prognozēt (piemēram, dabas katastrofas)", vai gadījumus, kad nepieciešamība rīkoties saistībā ar ieteikumu ir zudusi, jo [*PIHBO*] ir īstenojis alternatīvu rīcību, pilnībā novēršot pārkāpumu.

([58]) Sk. *APPI* 62. pantu.

([59]) Piemēram, daži noteikumi attiecas uz *PIHBO* darbībām, kas ir fakultatīvas (*APPI* 32., 33. pants), vai pienākumiem censties sasniegt rezultātu, kuri paši par sevi nav īstenojami (*APPI* 31., 35. pants, 36. panta 6. punkts un 39. pants). Daži noteikumi nav adresēti *PIHBO*, bet ir adresēti citiem dalībniekiem. Kā piemēru var minēt *APPI* 23. panta 4. punktu, 26. panta 2. punktu un 34. pantu) (tomēr *APPI* 26. panta 2. punkta izpildi nodrošina iespēja piemērot krimināLsodus saskaņā ar *APPI* 88. panta i) punktu).

([60]) Turklāt, kā paskaidrots 48. apsvērumā iepriekš, datu nosūtīšanas kontekstā izmantošanas nolūku norāda ES datu nosūtītājs, kam šajā sakarā ir saistošs Regulas (ES) 2016/679 5. panta 1. punkta b) apakšpunktā noteiktais pienākums. Šā pienākuma izpildi nodrošina kompetentā datu aizsardzības iestāde Eiropas Savienībā.

(102) *PPC* rīkojuma neizpildi uzskata par noziedzīgu nodarījumu *APPI* 84. panta nozīmē, un, ja *PIHBO* ir atzīts par vainīgu, tam var piespriest brīvības atņemšanu ar piespiedu darbu uz termiņu līdz sešiem mēnešiem vai naudas sodu līdz 300 000 jenu. Turklāt atbilstoši *APPI* 85. panta i) punktam par nesadarbošanos ar *PPC* vai traucēšanu tās izmeklēšanā var piemērot naudas sodu līdz 300 000 jenu. Šos kriminālsodus piemēro papildus tiem sodiem, ko var piemērot par būtiskiem *APPI* pārkāpumiem (skatīt 108. apvērumu).

2.4.2. *Tiesiskās aizsardzības līdzekļi*

(103) Lai nodrošinātu pietiekamu aizsardzību un jo īpaši individuālo tiesību īstenošanu, datu subjektam vajadzētu būt pieejamiem efektīviem administratīvās un tiesiskās aizsardzības līdzekļiem, tostarp kompensācijai par kaitējumu.

(104) Pirms administratīvās vai tiesiskās aizsardzības līdzekļu izmantošanas vai to izmantošanas vietā persona var nolemt iesniegt pārzinim sūdzību par savu personas datu apstrādi. Pamatojoties uz *APPI* 35. pantu, *PIHBO* cenšas pienācīgi un nekavējoties izskatīt šādas sūdzības un izveidot iekšējās sūdzību izskatīšanas sistēmas, lai sasniegtu šo mērķi. Turklāt saskaņā ar *APPI* 61. panta ii) punktu *PPC* ir atbildīga par "nepieciešamo mediāciju iesniegtas sūdzības gadījumā un sadarbību, ko piedāvā uzņēmējam, kurš izskata sūdzību", un abos gadījumos tas ietver ārvalstnieku iesniegtas sūdzības. Šajā sakarā Japānas likumdevējs ir arī uzticējis centrālajai valdībai pienākumu veikt "nepieciešamās darbības", lai nodrošinātu un veicinātu sūdzību izskatīšanu, ko veic *PIHBO* (9. pants), savukārt vietējām valdībām jāpieliek pūles, lai šādos gadījumos nodrošinātu mediāciju (13. pants). Šajā saistībā personas papildus iespējai iesniegt sūdzību Japānas Valsts patērētāju lietu centrā var arī iesniegt sūdzību kādā no vairāk nekā 1 700 patērētāju tiesību aizsardzības centriem, ko izveidojušas vietējās valdības, pamatojoties uz Patērētāju drošības likumu ([61]). Šādas sūdzības var iesniegt arī par *APPI* pārkāpumiem. Saskaņā ar Patērētāju pamatlikuma ([62]) 19. pantu vietējās valdības cenšas iesaistīties mediācijā attiecībā uz sūdzībām un sniegt iesaistītajām pusēm nepieciešamo zinātību. Šādi strīdu izšķiršanas mehānismi ir diezgan efektīvi – 2015. gadā tika atrisināti vairāk nekā 75 000 sūdzību gadījumu, kas ir 91,2 %.

(105) Ja *PIHBO* pārkāpj *APPI* noteikumus, par to var ierosināt gan civillietu, gan arī krimināllietu un piespriestas sankcijas. Pirmkārt, ja persona uzskata, ka ir pārkāptas viņas tiesības, kā noteikts *APPI* 28., 29. un 30. pantā, viņa var pieprasīt tiesas priekšrakstu, lūdzot, lai tiesa izdod rīkojumu, kas uzliek *PIHBO* pienākumu izpildīt personas prasību atbilstoši vienam no šiem noteikumiem, t. i., izpaust glabātus personas datus (28. pants), labot nepareizus glabātus personas datus (29. pants) vai izbeigt datu nelikumīgu apstrādi vai sniegšanu trešai personai (30. pants). Šādu lietu var ierosināt bez nepieciešamības atsaukties uz Civilkodeksa 709. pantu ([63]) vai uz saistību tiesībām ([64]). Tas jo īpaši nozīmē, ka attiecīgajai personai nav jāpierāda kaitējums.

(106) Otrkārt, gadījumā, kad varbūtējs pārkāpums neattiecas uz individuālām tiesībām atbilstoši 28., 29. un 30. pantam, bet attiecas uz vispārīgiem datu aizsardzības principiem vai *PIHBO* pienākumiem, attiecīgā persona var ierosināt civillietu pret uzņēmēju, pamatojoties uz Japānas Civilkodeksa saistību tiesību noteikumiem, jo īpaši 709. pantu. Lai gan viens no priekšnosacījumiem prasības ierosināšanai saskaņā ar 709. pantu papildus vainai (tīšai rīcībai vai nolaidībai) ir arī pierādījums par kaitējumu, saskaņā ar Civilkodeksa 710. pantu šāds kaitējums var būt gan materiāls, gan nemateriāls. Attiecībā uz kompensācijas apmēru nav noteikti nekādi ierobežojumi.

(107) Attiecībā uz pieejamiem tiesiskās aizsardzības līdzekļiem Japānas Civilkodeksa 709. pantā ir minēta naudas kompensācija. Tomēr Japānas judikatūrā šis pants ir interpretēts arī kā tāds, kas nosaka tiesības prasīt tiesas priekšrakstu ([65]). Tāpēc, ja datu subjekts ceļ prasību atbilstoši Civilkodeksa 709. pantam un apgalvo, ka atbildētājs, pārkāpjot *APPI* noteikumu, ir nodarījis kaitējumu viņa interesēm, prasībā papildus kaitējuma kompensācijai var pieprasīt arī tiesas priekšrakstu, jo īpaši lai apturētu jebkādu nelikumīgu apstrādi.

([61]) 2009. gada 5. jūnija Likums Nr. 50.
([62]) 2012. gada 22. augusta Likums Nr. 60.
([63]) Civilprocesa kodeksa 709. pants ir galvenais pamats civilās tiesvedības uzsākšanai par kaitējumu. Saskaņā ar šo noteikumu "personai, kura ir tīši vai nolaidības dēļ pārkāpusi jebkādas citu personu tiesības vai ar likumu aizsargātas citu personu intereses, ir pienākums kompensēt jebkādu no tā izrietošo kaitējumu".
([64]) Tokijas Augstās tiesas 2015. gada 20. maija spriedums (nav publicēts); Tokijas rajona tiesas 2014. gada 8. septembra spriedums, *Westlaw Japan* 2014WLJPCA09088002. Sk. arī *APPI* 34. panta 1. un 3. punktu.
([65]) Sk. Augstākās tiesas 2002. gada 24. septembra spriedumu (*Hanrei Times*, 1106. sēj., 72. lpp.).

(108) Treškārt, papildus civiltiesiskās (saistību tiesību) aizsardzības līdzekļiem datu subjekts var iesniegt prokuroram vai kriminālpolicijai sūdzību par *APPI* pārkāpumiem, par kuriem var piemērot krimināsodu. *APPI* VII nodaļā ir vairāki noteikumi par sodiem. Vissvarīgākais (84. pants) attiecas uz gadījumiem, kad *PIHBO* neizpilda *PPC* rīkojumus atbilstoši 42. panta 2. un 3. punktam. Ja uzņēmējs neizpilda *PPC* izdotu rīkojumu, *PPC* priekšsēdētājs (kā arī jebkura cita valsts amatpersona) ([66]) var pārsūtīt lietu prokuroram vai kriminālpolicijai, tādējādi uzsākot kriminālprocesu. Sods par *PPC* rīkojuma neizpildi ir brīvības atņemšana līdz sešiem mēnešiem ar piespiedu darbu vai naudas sods līdz 300 000 jenu. Citi *APPI* noteikumi, kas paredz sodus tādu *APPI* pārkāpumu gadījumā, kas skar datu subjektu tiesības un intereses, ir *APPI* 83. pants (attiecībā uz personas informācijas datubāzes "nemanāmu nodrošināšanu vai izmantošanu" "nolūkā gūt (…) nelikumīgu peļņu") un *APPI* 88. panta i) punkts (attiecībā uz gadījumu, kad trešā persona korekti neinformē *PIHBO*, kad tas saņem personas datus saskaņā ar *APPI* 26. panta 1. punktu, jo īpaši nesniedzot sīku informāciju par to, kā trešā persona pati iepriekš ieguvusi šādus datus). Piemērojamie sodi par šādiem *APPI* pārkāpumiem ir attiecīgi brīvības atņemšana ar piespiedu darbu līdz vienam gadam vai naudas sods līdz 500 000 jenu (83. panta gadījumā), vai administratīvs naudas sods līdz 100 000 jenu (88. panta i) punkta gadījumā). Lai arī krimināsoda draudiem vien varētu būt spēcīga atturoša ietekme uz uzņēmuma vadību, kas vada *PIHBO* datu apstrādes operācijas, kā arī uz personām, kuras apstrādā datus, *APPI* 87. pantā ir paskaidrots, ka gadījumā, ja kādas juridiskas personas pārstāvis, darbinieks vai cits darba ņēmējs veicis pārkāpumus saskaņā ar *APPI* 83. līdz 85. pantu, "nodarītāju soda un minētajai juridiskajai personai piemēro naudas sodu, kas noteikts attiecīgajos pantos". Šajā gadījumā gan darbiniekam, gan uzņēmumam var piemērot sodu pat maksimālajā apmērā.

(109) Visbeidzot, personas var arī prasīt tiesiskās aizsardzības līdzekļus saistībā ar *PPC* darbībām vai bezdarbību. Šajā saistībā Japānas tiesību akti paredz vairākas administratīvās un tiesiskās aizsardzības līdzekļu iespējas.

(110) Ja persona nav apmierināta ar *PPC* rīcību, viņa var iesniegt pārsūdzību administratīvā kārtā saskaņā ar Administratīvo sūdzību pārskatīšanas likumu ([67]). Turpretī, ja persona uzskata, ka *PPC* vajadzēja rīkoties, bet tā nav rīkojusies, persona var prasīt, lai *PPC* saskaņā ar minētā likuma 36-3. pantu dod rīkojumu vai sniedz administratīvus norādījumus, ja persona uzskata, ka nav "ticis pieņemts vai piemērots rīkojums vai administratīvi norādījumi, kas nepieciešami, lai izlabotu pārkāpumu".

(111) Attiecībā uz tiesiskās aizsardzības līdzekļiem – saskaņā ar Administratīvo lietu iztiesāšanas likumu persona, kura nav apmierināta ar *PPC* doto administratīvo rīkojumu, var iesniegt *mandamus* prasību ([68]) tiesai, lūdzot, lai tā uzdod *PPC* īstenot turpmāku rīcību ([69]). Konkrētos gadījumos tiesa var arī izdot pagaidu *mandamus* rīkojumu, lai novērstu neatgriezenisku kaitējumu ([70]). Turklāt saskaņā ar minēto Likumu persona var prasīt *PPC* lēmuma atcelšanu ([71]).

(112) Visbeidzot, persona var arī iesniegt prasību pret *PPC* par valsts kompensāciju atbilstoši Valsts tiesiskās aizsardzības līdzekļu likuma 1. panta 1. punktam, ja personai ir nodarīts kaitējums tāpēc, ka *PPC* izdotais rīkojums uzņēmējam ir bijis nelikumīgs vai *PPC* nav īstenojusi savas pilnvaras.

3. JAPĀNAS PUBLISKO IESTĀŽU PIEKĻUVE PERSONAS DATIEM, KO NOSŪTA NO EIROPAS SAVIENĪBAS, UN TO IZMANTOŠANA

(113) Komisija ir arī novērtējusi ierobežojumus un garantijas, tostarp pārraudzības un individuālās tiesiskās aizsardzības mehānismus, kas pieejami atbilstoši Japānas tiesību aktiem saistībā ar tādu personas datu vākšanu un vēlāku izmantošanu, kurus publiskās iestādes nosūta uzņēmējiem Japānā sabiedrības interesēs, jo īpaši krimināltiesību aizsardzības un valsts drošības nolūkos ("valdības piekļuve"). Šajā saistībā Japānas valdība ir iesniegusi Komisijai oficiālus apliecinājumus, garantijas un saistības, kas parakstītas augstākajā ministriju un aģentūru līmenī un ietvertas šā lēmuma II pielikumā.

([66]) Krimināprocesa kodeksa 239. panta 2. punkts.
([67]) Likums Nr. 160, 2014. gads.
([68]) Administratīvo lietu iztiesāšanas likuma 37-2. pants.
([69]) Saskaņā ar Administratīvo lietu iztiesāšanas likuma 3. panta 6. punktu jēdziens "*mandamus* prasība" ir prasība par to, lai tiesa norīko administratīvu aģentūru izdot sākotnēju administratīvu rīkojumu, ko tai vajadzēja izdot (bet ko tā nav izdarījusi).
([70]) Administratīvo lietu iztiesāšanas likuma 37-5. pants.
([71]) Administratīvo lietu iztiesāšanas likuma II nodaļas 1. iedaļa.

3.1. **Vispārējais tiesiskais regulējums**

(114) Valsts varas īstenošanas ietvaros Japānas valdībai, piekļūstot personas datiem, ir pilnībā jāievēro tiesību akti (likumības princips). Šajā saistībā Japānas Konstitūcijā ir ietverti noteikumi, kas nosaka ierobežojumus un satvaru personas datu vākšanai, kuru veic publiskās iestādes. Kā jau minēts attiecībā uz apstrādi, ko veic uzņēmēji, Japānas Augstākā tiesa, pamatojoties uz Konstitūcijas 13. pantu, kas cita starpā aizsargā tiesības uz brīvību, ir atzinusi tiesības uz privātumu un datu aizsardzību ([72]). Viens no būtiskiem šādu tiesību aspektiem ir brīvība neatļaut savas personas informācijas izpaušanu trešai personai bez atļaujas ([73]). Tas ietver tiesības uz efektīvu aizsardzību pret personas datu ļaunprātīgu izmantošanu un (jo īpaši) nelikumīgu piekļuvi tiem. Papildu aizsardzību nodrošina Konstitūcijas 35. pants par visu personu tiesībām sava mājokļa, personas un datu neaizskaramību, kas nozīmē, ka publiskām iestādēm visos "pārmeklēšanas un konfiskācijas" gadījumos ir jāsaņem tiesas orderis, kurš izdots ar "pienācīgu pamatojumu" ([74]). Augstākā tiesa savā 2017. gada 15. marta spriedumā (*GPS* lieta) precizēja, ka šī prasība par orderi ir piemērojama ikreiz, kad valdības aizskar ("iejaucas") privātumā veidā, kas apspiež personas gribu, un veicot "obligātu izmeklēšanu". Tiesnesis var izdot šādu orderi tikai tad, ja ir konkrētas aizdomas par noziegumu, t. i., ja ir iesniegti dokumentēti pierādījumi, uz kuru pamata var uzskatīt, ka persona, pret kuru vērsta izmeklēšana, ir izdarījusi noziedzīgu nodarījumu ([75]). Attiecīgi Japānas iestādēm nav likumīgu pilnvaru vākt personas informāciju piespiedu kārtā situācijās, kad tiesību akta pārkāpums vēl nav noticis ([76]), piemēram, lai novērstu noziegumu vai citus draudus drošībai (kā tas ir gadījumā, kad izmeklēšanu veic, pamatojoties uz valsts drošības apsvērumiem).

(115) Saskaņā ar tiesību atrunas principu jebkurai datu vākšanai, ko veic piespiedu izmeklēšanā, jābūt īpaši atļautai ar likumu (kā atspoguļots, piemēram, Kriminālprocesa kodeksa ("*CCP*") 197. panta 1. punktā, kas attiecas uz obligātu informācijas vākšanu krimināllizmeklēšanas nolūkos). Šī prasība attiecas arī uz piekļuvi elektroniskai informācijai.

(116) Būtiski ir tas, ka Konstitūcijas 21. panta 2. punkts garantē visu saziņas līdzekļu slepenību, un izņēmumi ir atļauti tikai ar tiesību aktiem un sabiedrības interesēs. Ar Telesakaru darījumdarbības likuma 4. pantu, kas nosaka, ka telesakaru operators nedrīkst pārkāpt apstrādāto sakaru slepenību, šī konfidencialitātes prasība tiek īstenota vispārējo tiesību līmenī. Šī prasība ir interpretēta kā aizliegums izpaust sakaru informāciju, izņemot, ja tas notiek ar lietotāju piekrišanu vai pamatojoties uz kādu no Sodu kodeksā skaidri noteiktajiem atbrīvojumiem no krimināl-atbildības ([77]).

(117) Konstitūcija arī garantē tiesības uz piekļuvi tiesām (32. pants) un tiesības iesūdzēt valsti, lai saņemtu tiesiskās aizsardzības līdzekļus gadījumos, kad personai ir nodarīts kaitējums valsts amatpersonas prettiesiskas darbības dēļ (17. pants).

(118) Konkrēti attiecībā uz tiesībām uz datu aizsardzību *APPI* III nodaļas 1., 2. un 3. iedaļā ir noteikti vispārēji principi, kas attiecas uz visām nozarēm, tostarp publisko sektoru. Jo īpaši *APPI* 3. pants paredz, ka visa personas informācija jāizmanto saskaņā ar personas privātuma ievērošanas principu. Kad publiskās iestādes ([78]) ir savākušas ("ieguvušas") personas informāciju, tostarp kā daļu no elektroniskiem ierakstiem, tās izmantošanu reglamentē Likums par

([72]) Sk., piemēram, Augstākās tiesas 2003. gada 12. septembra spriedumu lietā Nr. 1656 (2002 (Ju)). Konkrēti, Augstākā tiesa ir nospriedusi, ka "ikvienai personai ir brīvība aizsargāt savu personas informāciju no tās izpaušanas trešām personām vai publiskošanas, ja tai nav pamatota iemesla".

([73]) Augstākā tiesa, 2008. gada 6. marta spriedums (*Juki-net*).

([74]) "Pienācīgs pamatojums" pastāv tikai tad, ja attiecīgo personu (aizdomās turēto, apsūdzēto) uzskata par izdarījušu noziedzīgu nodarījumu un ja konfiskācija ir vajadzīga krimināllizmeklēšanai. Sk. Augstākās tiesas 1969. gada 18. marta spriedumu lietā Nr. 100 (1968 (*Shi*)).

([75]) Sk. Kriminālprocesa noteikumu 156. panta 1. punktu.

([76]) Tomēr būtu jāatzīmē, ka ar 2017. gada 15. jūnija Likumu par sodiem organizētu noziegumu gadījumos un noziedzīgi iegūtu līdzekļu kontroli tika kriminalizēts jauns nodarījums, proti, gatavošanās teroraktiem un citiem organizētās noziedzības veidiem. Izmeklēšanu var sākt tikai tad, ja, pamatojoties uz pierādījumiem, ir konkrētas aizdomas, ka ir izpildīti visi trīs nosacījumi, kas veido nodarījumu (noziegumā ir iesaistīta organizēta noziedzīga grupa, nozieguma "plānošana" un "gatavošanās īstenot" noziegumu). Sk. arī, piem., Kaitniecisku darbību novēršanas likuma (1952. gada 21. jūlija Likums Nr. 240) 38.–40. pantu.

([77]) Pamatnostādņu par personas informācijas aizsardzību telesakaru nozarē 15. panta 8. punkts.

([78]) Administratīvās struktūras, kā definēts *APPIHAO* 2. panta 1. punktā. Kā liecina no Japānas valdības saņemtā informācija, "administratīvo struktūru" definīcija attiecas uz visām publiskajām iestādēm, izņemot prefektūras policiju. Tajā pašā laikā prefektūras policija darbojas atbilstoši tiesiskajam regulējumam, kuru nosaka ar prefektūru personas informācijas aizsardzības rīkojumiem (sk. *APPI* 11. pantu un pamatpolitiku), kas paredz noteikumus par personas informācijas aizsardzību, kuri ir līdzvērtīgi *APPIHAO*. Sk. II pielikuma I.B. iedaļa. Kā paskaidrojusi *PPC*, saskaņā ar "pamatpolitiku" šie rīkojumi ir jāizpilda, pamatojoties uz *APIHAO* saturu, un *MIC* izdod paziņojumus, lai vietējam valdībām sniegtu nepieciešamās norādes šajā jautājumā. Kā uzsvērusi *PPC*, "[š]o ierobežojumu ietvaros personas informācijas aizsardzības rīkojumu katrā prefektūrā izstrādā, (…) pamatojoties uz pamatpolitiku un paziņojumu saturu."

administratīvo struktūru rīcībā esošās personas informācijas aizsardzību ("*APPIHAO*") ([79]). Principā tas ietver ([80]) arī personas informācijas apstrādi krimināltiesību aizsardzības vai valsts drošības nolūkos. *APPIHAO* cita starpā paredz, ka publiskās iestādes i) var glabāt personas informāciju tikai tādā apmērā, kādā tas ir nepieciešams to pienākumu pildīšanai; ii) neizmanto šādu informāciju negodīgam nolūkam un "nepamatoti" neizpauž to trešai personai; iii) norāda nolūku un to nemaina tādējādi, ka tiek pārsniegts tas, ko var pamatoti uzskatīt par atbilstošu sākotnējam nolūkam (nolūka ierobežojums); iv) principā neizmanto un nesniedz trešai personai glabātu personas informāciju citos nolūkos un, ja to uzskata par nepieciešamu, piemēro trešām personām nolūka vai izmantošanas metodes ierobežojumus; v) cenšas nodrošināt informācijas pareizību (datu kvalitāte); vi) veic nepieciešamos pasākumus pienācīgai informācijas pārvaldībai un nopludināšanas, nozaudēšanas vai sabojāšanas novēršanai (datu drošība), un vii) cenšas pienācīgi un nekavējoties izskatīt visas sūdzības par informācijas apstrādi ([81]).

3.2. **Japānas publisko iestāžu piekļuve datiem un to izmantošana krimināltiesību aizsardzības nolūkos**

(119) Japānas tiesību aktos ir noteikti vairāki ierobežojumi attiecībā uz piekļuvi personas datiem un to izmantošanu krimināltiesību aizsardzības nolūkos, kā arī pārraudzības un tiesiskās aizsardzības mehānismi, kas nodrošina pietiekamas garantijas, lai šos datus varētu efektīvi pasargāt pret nelikumīgu iejaukšanos un ļaunprātīgas izmantošanas risku.

3.2.1. *Juridiskais pamats un piemērojamie ierobežojumi / aizsardzības pasākumi*

(120) Japānas tiesiskajā regulējumā elektroniskās informācijas vākšana krimināltiesību aizsardzības nolūkos ir pieļaujama, pamatojoties uz orderi (piespiedu vākšana) vai brīvprātīgas izpaušanas pieprasījumu.

3.2.1.1. Obligāta izmeklēšana, pamatojoties uz tiesas orderi

(121) Kā norādīts 115. apsvērumā, jebkurai datu vākšanai, ko veic piespiedu izmeklēšanā, jābūt īpaši atļautai ar likumu, un to drīkst veikt tikai, pamatojoties uz tiesas orderi, kurš "izdots ar pienācīgu pamatojumu" (Konstitūcijas 35. pants). Attiecībā uz noziedzīgu nodarījumu izmeklēšanu šī prasība ir atspoguļota Krimināprocesa kodeksa (*CCP*) noteikumos. Saskaņā ar *CCP* 197. panta 1. punktu piespiedu pasākumus "nepiemēro, ja vien šajā kodeksā nav noteikti īpaši noteikumi". Attiecībā uz elektroniskās informācijas vākšanu vienīgie atbilstošie ([82]) juridiskie pamati šajā saistībā ir *CCP* 218. pants (pārmeklēšana un konfiskācija) un *CCP* 222-2. pants, saskaņā ar kuriem piespiedu pasākumus elektronisko sakaru pārtveršanai bez jebkuras puses piekrišanas veic, pamatojoties uz citiem likumiem, proti, Likumu par sarunu noklausīšanos krimināizmeklēšanas nolūkos ("Sarunu noklausīšanās likums"). Abos gadījumos ir piemērojama prasība par orderi.

(122) Konkrēti, atbilstoši *CCP* 218. panta 1. punktam, ja tas nepieciešams nodarījuma izmeklēšanai, prokurors, prokurora palīgs vai krimināpolicijas darbinieks var veikt pārmeklēšanu vai konfiskāciju (tostarp ierakstu pieprasīšanu), pamatojoties uz tiesneša iepriekš izdotu orderi ([83]). Šādā orderī cita starpā norāda aizdomās turētā vai apsūdzētā vārdu, nodarījumu, kurā viņš tiek apsūdzēts ([84]), konfiscējamos elektromagnētiskos ierakstus un "vietu vai priekšmetus", kuri jāpārbauda (*CCP* 219. panta 1. punkts).

([79]) Personas informācija, ko administratīvās struktūras amatpersonas iegūst savu pienākumu pildīšanas gaitā un ko administratīvā struktūra glabā organizatoriskos nolūkos, ietilpst "glabātas personas informācijas" definīcijā *APPIHAO* 2. panta 3. punkta nozīmē, kamēr vien tā ir reģistrēta "administratīvos dokumentos". Šāda informācija ietver elektronisku informāciju, ko vāc un turpmāk apstrādā šādas struktūras, ņemot vērā, ka "administratīvo dokumentu" definīcijā, kas sniegta Likuma par piekļuvi administratīvo struktūru rīcībā esošai informācijai (1999. gada Likums Nr. 42) 2. panta 2. punktā, ietilpst elektromagnētiskie ieraksti.

([80]) Tomēr saskaņā ar Krimināprocesa kodeksa 53-2. pantu *APPIHAO* IV nodaļa neattiecas uz "dokumentiem, kas saistīti ar tiesvedību" un kas saskaņā ar saņemto informāciju ietver elektronisku informāciju, kura iegūta, pamatojoties uz orderi vai prasību par brīvprātīgu sadarbošanos krimināizmeklēšanā. Tāpat attiecībā uz informāciju, ko vāc valsts drošības jomā, personas nevar veiksmīgi atsaukties uz savām tiesībām atbilstoši *APPIHAO*, ja publiskās iestādes vadītājam ir "pamatots iemesls" uzskatīt, ka izpaušana "varētu kaitēt valsts drošībai" (sk. 14. panta iv) punktu). Tomēr publiskām iestādēm ir pienākums piešķirt vismaz daļēju piekļuvi, kad vien tas ir iespējams (15. pants).

([81]) Sk. īpašās atsauces uz *APPIHAO* II pielikumā, II.A. iedaļas 1. punkta b) apakšpunkta 2. punkts.

([82]) Lai gan *CCP* 220. pants atļauj pārmeklēšanu un konfiskāciju "uz vietas" bez ordera, ja prokurors, prokurora palīgs vai krimināpolicijas darbinieks apcietina aizdomās turētu/nozieguma vietā pieķertu noziedzīgā nodarījuma izdarītāju, tas neattiecas uz datu nosūtīšanu un tādējādi nav šā lēmuma tvērumā.

([83]) Saskaņā ar *CCP* 222. panta 1. punktu, to lasot saistībā ar 110. pantu, pārmeklēšanas/konfiskācijas orderis attiecībā uz ierakstiem ir jāuzrāda personai, pret kuru tiek vērsts konkrētais pasākums.

([84]) Sk. arī *CCP* 189. panta 2. punktu, saskaņā ar kuru krimināpolicijas ierēdnis, "kad viņš uzskata, ka ir izdarīts nodarījums", veic izmeklēšanu attiecībā uz noziedzīgā nodarījuma izdarītāju un tā pierādījumiem. Tāpat Krimināprocesa noteikumu 155. panta 1. punkts nosaka, ka rakstiskā ordera pieprasījumā citā starpā norāda "nodarījumu, kurā persona tiek apsūdzēta", un "nozieguma faktu kopsavilkumu".

(123) Attiecībā uz sakaru pārtveršanu ar Sarunu noklausīšanās likuma 3. pantu šādi pasākumi ir atļauti tikai, ievērojot stingras prasības. Konkrēti, publiskajām iestādēm ir jāsaņem iepriekšējs tiesas orderis, ko var izdot tikai konkrētu smagu noziegumu (uzskaitīti likuma pielikumā) izmeklēšanai ([85]) un gadījumos, kad ir "ļoti sarežģīti jebkādos citos veidos noskaidrot nozieguma izdarītāju vai nozieguma izdarīšanas situāciju/apstākļus" ([86]). Saskaņā ar Sarunu noklausīšanās likuma 5. pantu orderi izdod uz noteiktu laikposmu un tiesnesis var noteikt papildu nosacījumus. Turklāt Sarunu noklausīšanās likumā ir noteikta virkne papildu garantiju, piemēram, liecinieku dalības nepieciešamība (12., 20. pants), aizliegums noklausīties konkrētu priviliģētu personu grupu sarunas (piem., ārstu, juristu) (15. pants), pienākums izbeigt sarunu noklausīšanos, ja tā vairs nav pamatota, pat tad, ja orderis joprojām vēl ir spēkā (18. pants), vai vispārīga prasība informēt iesaistīto personu un atļaut piekļuvi sarunu ierakstiem trīsdesmit dienu laikā pēc noklausīšanās izbeigšanas (23., 24. pants).

(124) Visus piespiedu pasākumus uz ordera pamata var veikt tikai kā tādu pārbaudi, "kas ir nepieciešama tās mērķa sasniegšanai", proti, ja izmeklēšanas mērķus nevar sasniegt citādi (*CCP* 197. panta 1. punkts). Lai gan vispārējās tiesībās kritēriji nepieciešamības noteikšanai nav precizēti sīkāk, Japānas Augstākā tiesa ir nospriedusi, ka tiesnesim, kurš izdod orderi, būtu jāveic vispārējs novērtējums, jo īpaši ņemot vērā i) nodarījuma smagumu un to, kā tas izdarīts; ii) materiālu, kas ir konfiscējami kā pierādījumi, vērtību un nozīmīgumu; iii) varbūtību (risku), ka pierādījumi var tikt slēpti vai iznīcināti, un iv) to, kādā mērā konfiskācija var radīt kaitējumu attiecīgajai personai ([87]).

3.2.1.2. Pieprasījums brīvprātīgi izpaust informāciju, pamatojoties uz "pierādījumu vākšanas dokumentu"

(125) Publiskās iestādes savas kompetences robežās var arī vākt elektronisku informāciju, pamatojoties uz pieprasījumiem par brīvprātīgu informācijas izpaušanu. Tas attiecas uz neobligātu sadarbības veidu, ja nav iespējams izpildīt informācijas sniegšanas pieprasījumu ([88]), tādējādi atbrīvojot publiskās iestādes no pienākuma iegūt tiesas orderi.

(126) Ciktāl šāds pieprasījums ir adresēts uzņēmējam un attiecas uz personas informāciju, uzņēmējam ir jāizpilda *APPI* prasības. Saskaņā ar *APPI* 23. panta 1. punktu uzņēmēji var izpaust personas informāciju trešām personām bez attiecīgās personas piekrišanas tikai konkrētos gadījumos, tostarp kad izpaušana ir "balstīta uz normatīvajiem aktiem" ([89]). Krimināltiesību aizsardzības jomā šādu pieprasījumu juridiskais pamats ir noteikts *CCP* 197. panta 2. punktā, saskaņā ar kuru "privātām organizācijām var prasīt, lai tās ziņo par nepieciešamajiem jautājumiem saistībā ar izmeklēšanu". Tā kā šāds pierādījumu vākšanas dokuments ir pieļaujams tikai kā daļa no kriminālizmeklēšanas, lai to izmantotu, ir jābūt konkrētām aizdomām par jau izdarītu noziegumu ([90]). Turklāt, tā kā šādu izmeklēšanu parasti veic prefektūras policija, piemēro Policijas likuma 2. panta 2. punktā noteiktos ierobežojumus ([91]). Saskaņā ar minēto noteikumu policijas darbības ir stingri ierobežotas ar tās uzdevumu un pienākumu izpildi (proti, noziegumu novēršanai, izskaušanai un izmeklēšanai). Turklāt, pildot savus pienākumus, policija rīkojas objektīvi, bez aizspriedumiem un godīgi, un tā nekad nedrīkst ļaunprātīgi izmantot savas pilnvaras tādā veidā, kas kaitē personas tiesībām un brīvībām, kuras garantētas Japānas Konstitūcijā (kuras, kā norādīts, ietver tiesības uz privātumu un datu aizsardzību) ([92]).

(127) Konkrēti attiecībā uz *CCP* 197. panta 2. punktu Valsts policijas aģentūra (*NPA*) kā federālā iestāde, kas cita starpā atbild par visiem jautājumiem, kuri saistīti ar kriminālpoliciju, ir izdevusi norādījumus prefektūras

([85]) Pielikumā ir minēti deviņi noziegumu veidi, piem., noziegumi, kas saistīti ar narkotikām un šaujamieročiem, cilvēku tirdzniecību un organizētu slepkavību. Būtu jāatzīmē, ka šajā izsmeļošajā sarakstā nav iekļauts jaunkriminalizētais nodarījums "gatavošanās teroraktiem un citiem organizētās noziedzības veidiem" (sk. 76. zemsvītras piezīmi).

([86]) Turklāt saskaņā ar Sarunu noklausīšanās likuma 23. pantu izmeklēšanas iestādei ir rakstiski jāinformē par šo faktu persona, kuras sakari ir pārtverti (un tādējādi reģistrēti pārtveršanas uzskaitē).

([87]) Sk. II pielikumu, II.A. iedaļas 1. punkta b) apakšpunkta 1. punkts.

([88]) Kā liecina saņemtā informācija, neviens tiesību akts nenosaka, ka uzņēmējiem, kas nesadarbojas, rodas negatīvas sekas (tostarp sodu piemērošana). Sk. II pielikumu, II.A. iedaļas 2. punkta a) apakšpunkts.

([89]) Saskaņā ar *PPC* pamatnostādnēm (Vispārējo noteikumu izdevums) 23. panta 1. punkta i) apakšpunkts nodrošina pamatu personas informācijas izpaušanai, atbildot gan uz orderi (*CCP* 218. pants), gan uz "pierādījumu vākšanas dokumentu" (*CCP* 197. panta 2. punkts).

([90]) Tas nozīmē, ka pierādījumu vākšanas dokumentu var izmantot tikai informācijas vākšanai atsevišķos gadījumos un to nevar izmantot jebkādai liela apjoma personas datu vākšanai. Sk. II pielikumu, II.A. iedaļas 2. punkta b) apakšpunkta 1. punkts.

([91]) Kā arī prefektūras sabiedriskās drošības komisijas noteikumi; sk. *CCP* 189. panta 1. punktu.

([92]) Sk. arī Policijas likuma 3. pantu, saskaņā ar kuru visiem policijas ierēdņiem ir jānodod zvērests "būt uzticīgiem pienākumam aizsargāt Japānas Konstitūciju un tiesību aktus un nodrošināt to ievērošanu, kā arī pildīt savus pienākumus objektīvi, taisnīgi, godīgi un bez aizspriedumiem".

policijai ([93]) par "rakstiskas pierādījumu gūšanas pienācīgu izmantošanu izmeklēšanas lietās". Saskaņā ar šo paziņojumu pieprasījumi jāiesniedz, izmantojot iepriekš noteiktu veidlapu (veidlapa Nr. 49 jeb tā dēvētais "pierādījumu vākšanas dokuments") ([94]), tiem jābūt saistītiem ar ierakstiem, kas "attiecas uz konkrētu izmeklēšanu", un prasītajai informācijai jābūt "nepieciešamai [minētās] izmeklēšanas vajadzībām". Katrā gadījumā galvenais izmeklētājs "pilnībā izvērtē individuāla[-ā]s pierādījumu gūšanas nepieciešamību, saturu utt.", un viņam ir jāsaņem iekšējs apstiprinājums no augstāka līmeņa amatpersonas.

(128) Turklāt divos spriedumos, kuri pieņemti 1969. un 2008. gadā ([95]), Japānas Augstākā tiesa ir noteikusi ierobežojumus attiecībā uz neobligātajiem pasākumiem, kas skar tiesības uz privātumu ([96]). Tiesa jo īpaši uzskatīja, ka šādiem pasākumiem jābūt "saprātīgiem" un tie nedrīkst pārsniegt "vispārīgi pieļaujamās robežas", proti, tiem jābūt nepieciešamiem izmeklēšanai, kas attiecas uz aizdomās turēto (pierādījumu vākšana), un jābūt īstenotiem, "izmantojot atbilstošas metodes izmeklēšanas mērķa sasniegšanai" ([97]). Minētie spriedumi apliecina, ka tas ietver samērības novērtējumu, ņemot vērā visus lietas apstākļus (piem., to, kādā pakāpē ir notikusi iejaukšanās tiesībās uz privātumu, tai skaitā gaidās uz privātuma ievērošanu, kā arī nozieguma smagumu, noderīgu pierādījumu iegūšanas iespējamību, šādu pierādījumu nozīmīgumu, iespējamos alternatīvos izmeklēšanas veidus u. c.) ([98]).

(129) Papildus šiem valsts varas īstenošanas ierobežojumiem no pašiem uzņēmējiem tiek gaidīts, ka tie pārbaudīs ("apstiprinās") informācijas sniegšanas trešai personai nepieciešamību un "racionalitāti" ([99]). Tas ietver arī jautājumu par to, vai likums neliedz uzņēmējiem sadarboties. Šādas juridisku pienākumu pretrunas var jo īpaši izrietēt no konfidencialitātes pienākumiem, piemēram, Sodu kodeksa 134. panta (par attiecībām starp ārstu, juristu, priesteri utt. un viņu klientiem). Tāpat arī "ikviena telesakaru darījumdarbībā iesaistīta persona, pildot amata pienākumus, ievēro citu personu noslēpumus, kuri tai kļuvuši zināmi saistībā ar telesakariem, kuru apstrādi veic telesakaru operators" (Telesakaru darījumdarbības likuma 4. panta 2. punkts). Par šā pienākuma neizpildi ir paredzēts sods, kas noteikts Telesakaru darījumdarbības likuma 179. pantā, saskaņā ar kuru ikviena persona, kas pārkāpusi pienākumu par telesakaru operatora apstrādāto telesakaru slepenību, tiek atzīta par vainīgu noziedzīgā nodarījumā un sodīta, piespriežot brīvības atņemšanu ar piespiedu darbu līdz diviem gadiem vai naudas sodu, kurš nepārsniedz vienu miljonu jenu ([100]). Lai gan šī prasība nav absolūta un it īpaši pieļauj pasākumus, ar kuriem pārkāpj telesakaru slepenību un kuri uzskatāmi par "attaisnojošām darbībām" Sodu kodeksa 35. panta ([101]) nozīmē, šis izņēmums neattiecas uz atbildi uz publisko iestāžu neobligātajiem pieprasījumiem izpaust elektronisko informāciju saskaņā ar *CCP* 197. panta 2. punktu.

3.2.1.3. Savāktās informācijas turpmāka izmantošana

(130) Uz personas informāciju, ko savākušas Japānas publiskās iestādes, attiecas *APPIHAO* piemērošanas joma. Minētais likums reglamentē "glabātas personas informācijas" izmantošanu (apstrādi) un šajā sakarā nosaka vairākus

([93]) Saskaņā ar Policijas likuma 30. panta 1. punktu un 31. panta 2. punktu, reģionālā policijas biroja (*NPA* vietējās nodaļas) ģenerāldirektors "vada un uzrauga" prefektūras policiju.

([94]) Pierādījumu vākšanas dokumentā ir arī jābūt norādītai personas datu "izmantotāja" kontaktinformācijai ("nodaļas [amata] nosaukumam, personas datu izmantotāja vārdam, biroja tālruņa numuram, paplašinājuma numuram utt.").

([95]) Augstākā tiesa, 1969. gada 24. decembra spriedums (1965(A) 1187); 2008. gada 15. aprīļa spriedums (2007(A) 839).

([96]) Lai gan minētie spriedumi neattiecās uz elektroniskās informācijas vākšanu, Japānas valdība ir precizējusi, ka Augstākās tiesas izstrādāto kritēriju piemērošana tiek paplašināta attiecībā uz jebkuru publisko iestāžu iejaukšanos tiesībās uz privātumu, tai skaitā uz visu veidu "brīvprātīgo izmeklēšanu", un tādējādi kritēriji ir saistoši Japānas iestādēm arī tad, kad tās iesniedz pieprasījumus par informācijas brīvprātīgu izpaušanu. Sk. II pielikumu, II.A. iedaļas 2. punkta b) apakšpunkta 1. punkts.

([97]) Kā liecina saņemtā informācija, šie faktori ir jāuzskata par "saprātīgiem saskaņā ar sabiedrībā pieņemtajām paražām". Sk. II pielikumu, II.A. iedaļas 2. punkta b) apakšpunkta 1. punkts.

([98]) Attiecībā uz līdzīgiem apsvērumiem obligāto izmeklēšanu (noklausīšanās) kontekstā sk. arī Augstākās tiesas 1999. gada 16. decembra spriedumu, 1997 (A) 636.

([99]) Šajā saistībā Japānas iestādes ir norādījušas uz *PPC* pamatnostādnēm (Vispārējo noteikumu izdevumu) un uz 5/14. punktu jautājumos un atbildēs, ko sagatavojusi *PPC* attiecībā uz *APPI* piemērošanu. Kā norādījušas Japānas iestādes, "ņemot vērā, ka uzlabojas personu informētība par to privātuma tiesībām, kā arī pieaugošo darba slodzi, ko rada šādi pieprasījumi, uzņēmēji arvien piesardzīgāk atbild uz šādiem pieprasījumiem". Sk. II pielikumu, II.A. iedaļas 2. punkts, ņemot vērā arī *NPA* 1999. gada paziņojumu. Kā liecina saņemtā informācija, praksē ir bijuši gadījumi, kad uzņēmēji atsakās sadarboties. Piemēram, *LINE* (Japānā populārākā ziņojumapmaiņas lietotne) savā 2017. gada pārredzamības ziņojumā norāda: "Pēc pieprasījumu saņemšanas no izmeklēšanas aģentūrām u. c. iestādēm mēs (…) pārbaudām to atbilstību no likumīguma, lietotāju aizsardzības un citu aspektu viedokļa. Šādā pārbaudē mēs noraidām pieprasījumu, ja pastāv kāda juridiska nepilnība. Ja pieprasījuma apjoms ir pārāk plašs, lai veiktu izmeklēšanu, mēs aicinām izmeklēšanas aģentūru sniegt skaidrojumu. Ja skaidrojumā trūkst pamatojuma, mēs neatbildam uz attiecīgo pieprasījumu." Pieejams interneta vietnē https://linecorp.com/en/security/transparency/top

([100]) Sodi ir brīvības atņemšana uz trīs gadiem ar piespiedu darbu vai naudas sods ne vairāk kā divi miljonu jenu apmērā jebkurai personai, kura "iesaistās telesakaru darījumdarbībā".

([101]) "Attaisnojošas darbības" saskaņā ar Sodu kodeksu ir it īpaši tās telesakaru operatora darbības, ar kurām tas izpilda valsts pasākumus, kam ir juridisks spēks (piespiedu pasākumi), piemēram, kad izmeklēšanas iestādes veic pasākumus, pamatojoties uz tiesneša izdotu orderi. Sk. II pielikuma II.A. iedaļas 2. punkta b) apakšpunkta 2. punkts, ņemot vērā Pamatnostādnes par personas informācijas aizsardzību telesakaru darījumdarbībā.

ierobežojumus un garantijas (sk. 118. apsvērumu) ([102]). Turklāt fakts, ka administratīva struktūra var glabāt personas informāciju tikai tad, ja glabāšana ir nepieciešama, lai īstenotu tās piekritībā esošās lietas, kā to paredz normatīvie akti (*APPIHAO* 3. panta 1. punkts), arī nosaka ierobežojumus – vismaz netieši – informācijas sākotnējai vākšanai.

3.2.2. *Neatkarīga pārraudzība*

(131) Japānā elektroniskās informācijas vākšana krimināltiesību aizsardzības jomā galvenokārt ([103]) ietilpst prefektūras policijas ([104]) pienākumos, kam šajā sakarā piemēro dažādu slāņu pārraudzību.

(132) Pirmkārt, visos gadījumos, kad elektronisko informāciju vāc piespiedu līdzekļiem (veicot pārmeklēšanu un konfiskāciju), policijai ir jāsaņem iepriekšējs tiesas orderis (sk. 121. apsvērumu). Tāpēc minētajos gadījumos datu vākšanu *ex ante* pārbauda tiesnesis, pamatojoties uz stingru "pienācīga pamatojuma" standartu.

(133) Lai gan tiesnesis neveic *ex ante* pārbaudi brīvprātīgās izpaušanas pieprasījumu gadījumā, uzņēmēji, kam adresē šādus pieprasījumus, var iebilst pret tiem, neriskējot, ka tas radīs viņiem negatīvas sekas (ņemot vērā arī jebkuras izpaušanas ietekmi uz privātumu). Turklāt saskaņā ar *CCP* 192. panta 1. punktu policijas darbinieki vienmēr sadarbojas un koordinē savas darbības ar prokuroru (un prefektūras sabiedriskās drošības komisiju) ([105]). Savukārt prokurors var sniegt nepieciešamos vispārējos norādījumus, kuros nosaka godīgas izmeklēšanas standartus, un/vai izdot īpašus rīkojumus attiecībā uz individuālu izmeklēšanu (*CCP* 193. pants). Ja šādus norādījumus un/vai rīkojumus neizpilda, prokuratūra var izvirzīt apsūdzības disciplinārlietas ierosināšanai (*CCP* 194. pants). Tādējādi prefektūras policija darbojas prokurora uzraudzībā.

(134) Otrkārt, saskaņā ar Konstitūcijas 62. pantu katra Japānas Parlamenta palāta var veikt izmeklēšanu attiecībā uz valdību, tostarp par policijas veiktās informācijas vākšanas likumību. Šajā nolūkā tā var pieprasīt liecinieku klātbūtni un liecināšanu un/vai ierakstu uzrādīšanu. Minētās pierādījumu iegūšanas pilnvaras ir plašāk izklāstītas Parlamenta likumā, jo īpaši XII nodaļā. It īpaši Parlamenta likuma 104. pants paredz, ka Ministru kabinetam, publiskajām aģentūrām un citām valdības struktūrām ir jāizpilda Parlamenta vai jebkuras tā komitejas pieprasījumi uzrādīt ziņojumus un ierakstus, kurus nepieciešams izskatīt izmeklēšanas vajadzībām." Atteikšanās izpildīt šo prasību ir pieļaujama tikai tad, ja valdība norāda ticamu iemeslu, ko Parlaments atzīst par pieņemamu, vai ja tiek izdota formāla deklarācija, ka ziņojumu vai ierakstu uzrādīšana "būtiski kaitētu valsts interesēm" ([106]). Turklāt Parlamenta locekļi var uzdot rakstiskus jautājumus Ministru kabinetam (Parlamenta likuma 74., 75. pants), un iepriekš šāda "rakstiska pierādījumu iegūšana" ir veikta arī par personas informācijas izmantošanu valsts pārvaldē ([107]). Parlamenta lomu izpildvaras uzraudzībā nostiprina ziņošanas pienākumi, piemēram, atbilstoši Sarunu noklausīšanās likuma 29. pantam.

(135) Treškārt, arī izpildvaras jomā prefektūras policija ir pakļauta neatkarīgai pārraudzībai. Minētais jo īpaši ietver prefektūru sabiedriskās drošības komisijas, kas izveidotas prefektūru līmenī, lai nodrošinātu policijas demokrātisku pārvaldību un politisko neitralitāti ([108]). Šo komisiju sastāvā ir locekļi, kurus ieceļ prefektūras gubernators ar prefektūras asamblejas piekrišanu (no tādu iedzīvotāju vidus, kuri iepriekšējos piecos gados nav ieņēmuši ierēdņa amatu policijā) un uz noteiktu pilnvaru termiņu (ar iespēju atlaist tikai tad, ja ir pamatos iemesls) ([109]). Kā liecina saņemtā informācija, komisiju locekļiem nav saistoši norādījumi, un tādējādi viņus var uzskatīt par pilnīgi neatkarīgiem ([110]). Kas attiecas uz prefektūru sabiedriskās drošības komisiju uzdevumiem un pilnvarām, tad saskaņā

([102]) Attiecībā uz personu tiesībām sk. 3.1. iedaļu.
([103]) Principā prokurors vai pēc viņa rīkojuma – prokurora palīgs, ja viņš uzskata to par nepieciešamu, var izmeklēt nodarījumu (*CCP* 191. panta 1. punkts).
([104]) Kā liecina saņemtā informācija, Valsts policijas aģentūra neveic individuālu krimināllizmeklēšanu. Sk. II pielikumu II.A. iedaļas 1. punkta a) apakšpunkts.
([105]) Sk. arī *CCP* 246. pantu, saskaņā ar kuru krimināpolicijai ir pienākums nosūtīt lietas materiālus prokuroram, tiklīdz tā ir pabeigusi noziedzīgā nodarījuma izmeklēšanu ("princips par lietas materiālu nosūtīšanu visās lietās").
([106]) Alternatīvi Parlaments var prasīt, lai Īpaši klasificētu noslēpumu pārraudzības un pārskatīšanas padome veic izmeklēšanu par atteikšanos sniegt atbildi. Sk. Parlamenta likuma 104-II. pantu.
([107]) Sk. II pielikumu, II.B. iedaļas 4. punkts.
([108]) Turklāt saskaņā ar Vietējās autonomijas likuma 100. panta noteikumiem vietējai asamblejai ir tiesības izmeklēt prefektūras līmenī izveidoto tiesībaizsardzības iestāžu, tai skaitā prefektūras policijas, darbības.
([109]) Sk. Policijas likuma 39.-41. pantu. Attiecībā uz politisko neitralitāti sk. arī Policijas likuma 42. pantu.
([110]) Sk. II pielikumu, II.B. iedaļas 3. punkts ("neatkarīgo padomju sistēma").

ar 38. panta 3. punktu saistībā ar Policijas likuma 2. pantu un 36. panta 2. punktu tās ir atbildīgas par "personas tiesību un brīvības aizsardzību". Šim nolūkam tās ir pilnvarotas "uzraudzīt" ([111]) visas prefektūras policijas veiktās izmeklēšanas darbības, ieskaitot personas datu vākšanu. Jo īpaši komisijas "vajadzības gadījumā var sniegt sīkus norādījumus prefektūras policijai vai norādījumus īpašā individuālā gadījumā, kad tiek pārbaudīti policijas darbinieku amatpārkāpumi." ([112]) Kad prefektūras policijas priekšnieks ([113]) saņem šādu norādījumu vai pats uzzina par iespējamu amatpārkāpuma gadījumu (tostarp par tiesību akta pārkāpumu vai citu pienākumu neizpildi), viņam ir nekavējoties jāpārbauda konkrētais gadījums un par pārbaudes rezultātu jāziņo prefektūras sabiedriskās drošības komisijai (Policijas likuma 56. panta 3. punkts). Ja minētā komisija to uzskata par nepieciešamu, tā var arī iecelt vienu no saviem locekļiem īstenošanas statusa izvērtēšanai. Šis process turpinās, līdz prefektūras sabiedriskās drošības komisija ir pārliecinājusies, ka attiecīgais incidents ir pienācīgi atrisināts.

(136) Turklāt attiecībā uz *APPIHAO* pareizu piemērošanu kompetentajam ministram vai aģentūras vadītājam (piem., *NPA* ģenerālkomisāram) ir izpildes pilnvaras ar nosacījumu, ka tiek piemērota Iekšlietu un komunikācijas lietu ministrijas (MIC) uzraudzība. Saskaņā ar *APPIHAO* 49. pantu *MIC* "var saņemt ziņojumus par šā likuma piemērošanas statusu" no administratīvo struktūru vadītājiem (ministriem). Minēto pārraudzības funkciju papildina ieguldījums, ko sniedz *MIC* 51 "vispārējās informācijas centrs" (viens centrs katrā prefektūrā visā Japānā), kuri katru gadu izskata tūkstošiem personu sūdzību ([114]) (kas, savukārt, var atklāt iespējamus tiesību aktu pārkāpumus). Ja *MIC* uzskata, ka tas ir nepieciešams minētā likuma izpildes nodrošināšanai, tā var prasīt paskaidrojumu un materiālu iesniegšanu un atzinumu sniegšanu par personas informācijas izmantošanu attiecīgajā administratīvajā struktūrā (*APPIHAO* 50., 51. pants).

3.2.3. *Individuāla tiesiskā aizsardzība*

(137) Papildus *ex officio* pārraudzībai personām ir arī vairākas iespējas saņemt individuālu tiesisko aizsardzību gan ar neatkarīgu iestāžu (piemēram, prefektūras sabiedriskās drošības komisijas vai *PPC*), gan Japānas tiesu starpniecību.

(138) Pirmkārt, attiecībā uz personas informāciju, ko vāc administratīvas struktūras, šīm struktūrām ir pienākums "censties pienācīgi un nekavējoties apstrādāt visas sūdzības", kuras attiecas uz informācijas turpmāku apstrādi (*APPIHAO* 48. pants). Lai gan *APPIHAO* IV nodaļa par individuālām tiesībām nav piemērojama attiecībā uz personas informāciju, kas reģistrēta "dokumentos, kuri attiecas uz tiesas prāvām un konfiscētiem priekšmetiem" (*CCP* 53-2. panta 2. punkts), un tā attiecas uz kriminālizmeklēšanā savāktu personas informāciju, personas var iesniegt sūdzību, atsaucoties uz vispārējiem datu aizsardzības principiem, piemēram, pienākumu glabāt personas informāciju tikai tad, "ja glabāšana ir nepieciešama [tiesībaizsardzības funkciju] izpildei" (*APPIHAO* 3. panta 1. punkts).

(139) Turklāt Policijas likuma 79. pants garantē personām, kam ir bažas par policijas darbinieku "pienākumu izpildi", tiesības iesniegt sūdzību (kompetentajai) neatkarīgajai prefektūras sabiedriskās drošības komisijai. Komisija "godprātīgi" izskata šādas sūdzības saskaņā ar tiesību aktiem un vietējiem rīkojumiem un rakstiski informē sūdzības iesniedzēju par rezultātiem. Pamatojoties uz savām pilnvarām uzraudzīt un vadīt prefektūras policiju attiecībā uz "personāla amatpārkāpumiem" (Policijas likuma 38. panta 3. punkts un 43-2. panta 1. punkts), tā var prasīt, lai prefektūras policija izmeklē faktus, veic atbilstošus pasākumus, pamatojoties uz šīs izmeklēšanas rezultātu, un ziņo par rezultātiem. Ja komisija uzskata, ka policijas veiktā izmeklēšana nav pietiekama, tā var arī sniegt norādījumus par sūdzības izskatīšanu.

(140) Lai veicinātu sūdzību izskatīšanu, *NPA* ir izdevusi "paziņojumu" policijai un prefektūru sabiedriskās drošības komisijām par to, kā pienācīgi izskatīt sūdzības attiecībā uz policijas ierēdņu pienākumu izpildi. Šajā dokumentā *NPA* nosaka Policijas likuma 79. panta interpretācijas un īstenošanas standartus. Tas cita starpā nosaka, ka prefektūras policijai ir jāizveido "sūdzību izskatīšanas sistēma" un "nekavējoties" jāizskata un jāpaziņo visas

([111]) Sk. Policijas likuma 5. panta 3. punktu un 38. panta 3. punktu.
([112]) Sk. Policijas likuma 38. panta 3. punktu un 43-2. panta 1. punktu. Ja prefektūras sabiedriskās drošības komisija "sniedz norādījumu" 43-2. panta 1. punkta nozīmē, tā var uzdot minētās komisijas ieceltai komitejai uzraudzīt norādījuma īstenošanu (2. punkts). Komisija var arī ieteikt disciplinārlietas ierosināšanu vai prefektūras policijas priekšnieka atlaišanu (Policijas likuma 50. panta 2. punkts), kā arī citu policijas ierēdņu atlaišanu (55. panta 4. punkts).
([113]) Tas pats attiecas uz Tokijas Metropoles policijas ģenerālpriekšnieku (sk. Policijas likuma 48. panta 1. punktu).
([114]) Kā liecina saņemtā informācija, 2017. finanšu gadā (no 2017. gada aprīļa līdz 2018. gada martam) "vispārējās informācijas centri" izskatīja kopumā 5 186 personu iesniegtus pieprasījumus.

sūdzības kompetentajai prefektūras sabiedriskās drošības komisijai. Paziņojumā sūdzības ir definētas kā prasījumi novērst "jebkuru konkrētu kaitējumu, kas radies nelikumīgas vai neatbilstošas rīcības rezultātā" ([115]) vai labot situāciju, kad "policists, pildot savus pienākumus, nav veicis kādu nepieciešamu darbību" ([116]), kā arī situāciju, kad ir "iesniegta sūdzība vai izteikta neapmierinātība par to, ka policists neatbilstīgi pildījis savus pienākumus". Tādējādi sūdzības materiālā piemērošanas joma ir plaši definēta, aptverot arī jebkuru sūdzību par datu nelikumīgu vākšanu, un sūdzības iesniedzējam nav jāpierāda, ka tam nodarīts kaitējums policista darbības rezultātā. Svarīgi, ka paziņojumā ir noteikts, ka (cita starpā) sūdzības sagatavošanai ir jāsniedz palīdzība ārvalstniekiem. Izskatot sūdzību, prefektūru sabiedriskās drošības komisijām ir jānodrošina, ka prefektūras policija pārbauda faktus, īsteno pasākumus "atbilstoši pārbaudes rezultātam" un ziņo par rezultātiem. Ja komisija uzskata, ka pārbaude ir bijusi nepietiekama, tā sniedz norādījumu par sūdzības izskatīšanu, kas prefektūras policijai ir jāievēro. Pamatojoties uz saņemtajiem ziņojumiem un veiktajiem pasākumiem, komisija informē attiecīgo personu, citā starpā norādot pasākumus, kas veikti, lai izvērtētu sūdzību. *NPA* paziņojumā uzsver, ka sūdzības būtu jāizskata "godīgi" un ka rezultāts būtu jāpaziņo "termiņā (…), ko uzskata par atbilstošu, ņemot vērā sociālās normas un veselo saprātu".

(141) Otrkārt, ņemot vērā to, ka tiesiskā aizsardzība parasti būs jāprasa citas valsts tiesību sistēmā un svešvalodā, nolūkā atvieglot tiesiskās aizsardzības iespējas ES iedzīvotājiem, kuru personas datus nosūta uzņēmējiem Japānā un tad tiem piekļūst publiskās iestādes, Japānas valdība ir izmantojusi savas pilnvaras izveidot tādu īpašu mehānismu sūdzību izskatīšanai un atrisināšanai šajā jomā, ko pārvalda un uzrauga *PPC*. Minētā mehānisma pamatā ir sadarbošanās pienākums, kas Japānas publiskajām iestādēm noteikts ar *APPI*, un *PPC* īpašā loma attiecībā uz datu starptautisku nosūtīšanu no trešām valstīm atbilstoši *APPI* 6. pantam un pamatpolitikai (kā Japānas valdība noteikusi ar Ministru kabineta rīkojumu). Šis mehānisms sīkāk ir aprakstīts oficiālajā oficiālajos apliecinājumos, garantijās un saistībās, kas saņemtas no Japānas valdības un pievienots šim lēmumam kā II pielikums. Uz mehānismu neattiecas nekādas *locus standi* prasības, un to var izmantot ikviena persona neatkarīgi no tā, vai viņa tiek turēta aizdomās vai apsūdzēta par noziedzīga nodarījuma izdarīšanu.

(142) Saskaņā ar mehānismu, ja personai ir aizdomas, ka viņas personas datus, kas nosūtīti no Eiropas Savienības, ir vākušas vai izmantojušas publiskās iestādes Japānā (tostarp iestādes, kuras atbild par krimināltiesību aizsardzību), pārkāpjot piemērojamos noteikumus, šāda persona var iesniegt sūdzību *PPC* (individuāli vai ar savas datu aizsardzības iestādes Vispārīgās datu aizsardzības regulas (VDAR) 51. panta nozīmē starpniecību). *PPC* ir pienākums izskatīt sūdzību un vispirms informēt par to kompetentās publiskās iestādes, tostarp attiecīgās pārraudzības struktūras. Minētajām iestādēm ir jāsadarbojas ar *PPC*, "cita starpā sniedzot nepieciešamo informāciju un iesniedzot nepieciešamos materiālus, lai *PPC* varētu izvērtēt, vai personas informācijas vākšana un vēlāka izmantošana ir notikusi atbilstoši piemērojamiem noteikumiem" ([117]). Šo pienākumu, kas atvasināts no *APPI* 80. panta (kurā iekļauta prasība Japānas publiskajām iestādēm sadarboties ar *PPC*), piemēro vispārīgi un tādējādi plašāk attiecina uz visām šādu iestāžu veiktām izmeklēšanas darbībām, turklāt šīs iestādes ir apņēmušās šādi sadarboties, kompetento ministriju un aģentūru vadītājiem sniedzot rakstisku apliecinājumu, kā tas atspoguļots II pielikumā.

(143) Ja izvērtējums liecina, ka ir noticis piemērojamo noteikumu pārkāpums, tad "attiecīgo publisko iestāžu sadarbība ar PPC ietver pienākumu novērst pārkāpumu", un personas informācijas nelikumīgas vākšanas gadījumā tas ietver arī šādu datu dzēšanu. Svarīgi ir tas, ka šā pienākuma izpildi uzrauga *PPC*, kas "pirms izvērtējuma noslēgšanas apstiprina, ka pārkāpums ir pilnībā novērsts".

(144) Kad izvērtējums ir noslēgts, *PPC* saprātīgā termiņā informē attiecīgo personu par izvērtējuma rezultātu, attiecīgā gadījumā norādot arī visus veiktos korektīvos pasākumus. Tajā pašā laikā *PPC* arī informē personu par iespēju prasīt, lai kompetentā publiskā iestāde apstiprina rezultātu, un tās iestādes identitāti, kurai būtu jāiesniedz šāds apstiprināšanas pieprasījums. Iespēja saņemt šādu apstiprinājumu, tostarp informāciju par kompetentās iestādes

([115]) Nosacījums par "konkrētu kaitējumu" vienīgi norāda uz to, ka policijas darbība (vai bezdarbība) personīgi skar sūdzības iesniedzēju, bet ne to, ka viņam ir jāpierāda kaitējums.

([116]) Minētajos pienākumos ietilpst tiesību aktu, tai skaitā tiesisko prasību attiecība uz personas datu vākšanu un izmantošanu, ievērošana. Sk. Policijas likuma 2. panta 2. punktu un 3. pantu.

([117]) Veicot izvērtēšanu, *PPC* sadarbojas ar *MIC*, kas, kā paskaidrots 136. apsvērumā, var prasīt paskaidrojumu un materiālu iesniegšanu un atzinumu sniegšanu par personas informācijas izmantošanu attiecīgajā administratīvajā struktūrā (*APPIHAO* 50., 51. pants).

lēmuma pamatā esošajiem apsvērumiem, var būt noderīga attiecīgajai personai jebkādu turpmāku darbību veikšanā, tostarp tiesiskās aizsardzības pieprasīšanas gadījumā. Sīkas informācijas sniegšana par izvērtējuma rezultātu var būt ierobežota, kamēr vien ir pamatoti iemesli uzskatīt, ka šādas informācijas paziņošana varētu apdraudēt notiekošo izmeklēšanu.

(145) Treškārt, ja persona nepiekrīt tiesneša pieņemtajam konfiskācijas lēmumam (orderim) ([118]) attiecībā uz viņas personas datiem vai policijas vai prokuratūras pasākumiem šāda lēmuma izpildei, viņa var iesniegt prasību par šāda lēmuma vai pasākumu atcelšanu vai mainīšanu (*CCP* 429. panta 1. punkts un 430. panta 1., 2. punkts, Sarunu noklausīšanās likuma 26. pants) ([119]). Ja tiesa, kas veic pārskatīšanu, uzskata, ka orderis vai tā izpilde ("konfiskācijas procedūra") ir nelikumīgi, tā apmierina prasību un liek atgriezt konfiscētos priekšmetus ([120]).

(146) Ceturtkārt, ir mazāk tiešs tiesas īstenotas pārskatīšanas veids, proti, ja persona uzskata, ka viņas personas informācijas vākšana kriminālizmeklēšanā ir bijusi nelikumīga, viņa krimināltiesas prāvā var atsaukties uz šo nelikumību. Ja tiesa piekrīt, pierādījumi tiek noraidīti kā nepieņemami.

(147) Visbeidzot, saskaņā ar Valsts tiesiskās aizsardzības līdzekļu likuma 1. panta 1. punktu tiesa var apstiprināt kompensācijas piešķiršanu, ja valsts amatpersona, kura īsteno valsts varu, savu pienākumu izpildē ir nelikumīgi (tīši vai nolaidības pēc) izraisījusi kaitējumu attiecīgajai personai. Saskaņā ar Valsts tiesiskās aizsardzības līdzekļu likuma 4. pantu valsts atbildība par kaitējumu ir balstīta uz Civilkodeksa noteikumiem. Šajā saistībā Civilkodeksa 710. pants paredz, ka atbildība attiecas arī uz citu kaitējumu, kas nav saistīts ar īpašumu, tātad arī uz morālu kaitējumu (piemēram, kaitējumu "garīgu ciešanu" veidā). Tas ietver gadījumus, kad ir notikusi personas privātuma aizskaršana, nelikumīgi uzraugot un/vai vācot personas informāciju (piem., ordera nelikumīga izpilde) ([121]).

(148) Papildus naudas kompensācijai personas konkrētos apstākļos var arī saņemt tiesas priekšrakstu (piem., par publisku iestāžu savākto personas datu dzēšanu), pamatojoties uz savām tiesībām uz privātumu atbilstoši Konstitūcijas 13. pantam ([122]).

(149) Ievērojot visas minētās tiesiskās aizsardzības iespējas, Japānas valdības izveidotais strīdu izšķiršanas mehānisms nosaka, ka persona, kura joprojām nav apmierināta ar procedūras iznākumu, var vērsties pie PPC, "kas informē personu par dažādajām iespējām un precīzu kārtību tiesiskās aizsardzības līdzekļu izmantošanai atbilstoši Japānas normatīvajiem aktiem". Turklāt *PPC* "sniedz personai atbalstu, kas ietver arī konsultācijas un palīdzību jebkādu turpmāku prasību celšanā attiecīgajai administratīvajai vai tiesu iestādei".

(150) Tas ietver procesuālo tiesību izmantošanu atbilstoši Kriminālprocesa kodeksam. Piemēram, "[j]a izvērtēšanā tiek konstatēts, ka attiecīgā persona ir aizdomās turētā persona krimināllietā, *PPC* informē personu par šo faktu" ([123]), kā arī par iespēju atbilstoši *CCP* 259. pantam prasīt, lai prokuratūra viņu informē, kad tā ir nolēmusi nesākt kriminālprocesu. Arī tad, ja izvērtējumā tiek konstatēts, ka ir ierosināta lieta saistībā ar attiecīgās personas informāciju un ka tā ir slēgta, *PPC* informē attiecīgo personu, ka lietas materiālus var izskatīt atbilstoši *CCP* 53. pantam (un Likuma par galīgo krimināllietu uzskaiti 4. pantam). Personas iespēja piekļūt savai lietai ir svarīga, jo tā palīdz

([118]) Tas ietver orderi, ar ko atļauj sarunu noklausīšanos, attiecībā uz kuru Sarunu noklausīšanās likums paredz īpašu paziņošanas prasību (23. pants). Saskaņā ar minēto noteikumu izmeklēšanas iestādei personas, kuru sakari ir pārtverti (un tādējādi reģistrēti pārtveršanas uzskaitē), ir rakstiski jāinformē par šo faktu. Vēl viens piemērs ir *CCP* 100. panta 3. punkts, saskaņā ar kuru tiesa, kad tā ir konfiscējusi pasta pakas vai telegrammas, kas nosūtītas apsūdzētajam vai ko nosūtījis apsūdzētais, informē sūtītāju vai saņēmēju, izņemot, ja pastāv risks, ka šāda paziņošana traucētu tiesvedībai. *CCP* 222. panta 1. punktā ir savstarpēja atsauce uz šo noteikumu attiecībā uz pārmeklēšanu un konfiskāciju, ko veic izmeklēšanas iestāde.

([119]) Lai gan šāds pieprasījums nenozīmē konfiskācijas lēmuma izpildes automātisku apturēšanu, tiesa, kas veic pārskatīšanu, var likt apturēt lēmuma izpildi, līdz tā pieņem lēmumu pēc būtības. Sk. *CCP* 429. panta 2. punktu un 432. pantu saistībā ar 424. pantu.

([120]) Sk. II pielikumu, II.C. iedaļas 1. punkts.

([121]) Sk. II pielikumu, II.C. iedaļas 2. punkts.

([122]) Sk., piem., Tokijas rajona tiesas 1988. gada 24. marta spriedumu (Nr. 2925); Osakas rajona tiesas 2007. gada 26. aprīļa spriedumu (Nr. 2925). Kā noteikusi Osakas rajona tiesa, ir jāizsver vairāki faktori, piemēram, i) attiecīgās personas informācijas veids un saturs; ii) informācijas vākšanas veids; iii) kaitējums, kas radīsies attiecīgajai personai, ja informācija netiks dzēsta, un iv) sabiedrības intereses, tostarp kaitējums, kas radīsies publiskajai iestādei, ja informācija tiks dzēsta.

([123]) Jebkurā gadījumā pēc kriminālprocesa sākšanas prokurors apsūdzētajam dod iespēju iepazīties ar minētajiem pierādījumiem (sk. *CCP* 298. un 299. pantu). Attiecībā uz noziegumos cietušajiem sk. *CCP* 316.–333. pantu.

personai labāk izprast pret viņu vērsto izmeklēšanu un tādējādi sagatavoties iespējamai tiesas prāvai (piem., prasībai par zaudējumu atlīdzināšanu) gadījumā, kad persona uzskata, ka viņas dati ir savākti vai izmantoti nelikumīgi.

3.3. **Japānas publisko iestāžu piekļuve datiem un to izmantošana valsts drošības nolūkos**

(151) Kā norādījušas Japānas iestādes, Japānā nav tiesību aktu, kas atļauj pieprasīt informācijas sniegšanu piespiedu kārtā vai "administratīvu sarunu noklausīšanos" ārpus kriminālizmeklēšanas. Tādējādi, pamatojoties uz valsts drošības apsvērumiem, informāciju var iegūt tikai no informācijas avota, kas ir brīvi pieejams ikvienam, vai ja informācija tiek izpausta brīvprātīgi. Uzņēmējiem, kas saņem pieprasījumu brīvprātīgi sadarboties (izpaužot elektronisku informāciju), nav juridiska pienākuma sniegt šādu informāciju ([124]).

(152) Tāpat saskaņā ar saņemto informāciju tikai četras valdības struktūras ir pilnvarotas vākt Japānas uzņēmēju rīcībā esošu elektronisku informāciju, pamatojoties uz valsts drošības apsvērumiem, un tās ir i) Ministru kabineta Izlūkošanas un izpētes birojs (*CIRO*); ii) Aizsardzības ministrija (*MOD*); iii) policija (Valsts policijas aģentūra (*NPA*) ([125]) un prefektūras policija), un iv) Sabiedriskās drošības izlūkošanas aģentūra (*PSIA*). Tomēr *CIRO* nekad nevāc informāciju tieši no uzņēmējiem, arī ne pārtverot sakarus. Gadījumos, kad birojs saņem informāciju no citām valdības iestādēm, lai sniegtu analīzi Ministru kabinetam, šīm citām iestādēm savukārt ir jāievēro tiesību akti, tai skaitā šajā lēmumā analizētie ierobežojumi un aizsardzības pasākumi. Tādējādi biroja darbībām nav nozīmes datu nosūtīšanas kontekstā.

3.3.1. *Juridiskais pamats un piemērojamie ierobežojumi / aizsardzības pasākumi*

(153) Kā liecina saņemtā informācija, *MOD* vāc (elektronisku) informāciju, pamatojoties uz *MOD* dibināšanas likumu. Atbilstoši tā 3. pantam *MOD* uzdevums ir pārvaldīt un vadīt militāros spēkus un "vadīt ar to saistītās lietas, lai nodrošinātu mieru valstī un tās neatkarību un visas tautas drošību". Likuma 4. panta 4. punkts nosaka, ka *MOD* ir piekritība attiecībā uz "aizsardzību un apsardzi", pašaizsardzības spēku veicamajām darbībām, kā arī militāro spēku izvietošanu, tostarp šo lietu vadīšanai nepieciešamās informācijas vākšanu. *MOD* ir pilnvaras vākt (elektronisku) informāciju no uzņēmējiem tikai tad, ja sadarbība ir brīvprātīga.

(154) Attiecībā uz prefektūras policiju – tās pienākumos un uzdevumos ietilpst "sabiedriskās drošības un kārtības uzturēšana" (35. panta 2. punkts saistībā ar Policijas likuma 2. panta 1. punktu). Šajā piekritības jomā policija var vākt informāciju, bet tikai tad, ja tā tiek sniegta brīvprātīgi, neizmantojot tiesisku spēka. Turklāt policijas darbības ir "stingri ierobežotas" tādā apmērā, kāds ir nepieciešams tās pienākumu pildīšanai. Turklāt tā rīkojas "objektīvi, neatkarīgi, bez aizspriedumiem un godīgi" un nekad ļaunprātīgi neizmanto savas pilnvaras, "kaitējot Japānas Konstitūcijā garantētajām personas tiesībām un brīvībām" (Policijas likuma 2. pants).

(155) Visbeidzot, *PSIA* var veikt izmeklēšanu saskaņā ar Kaitniecisku darbību novēršanas likumu ("*SAPA*") un Likumu par to organizāciju kontroli, kuras veikušas neselektīvas masu slepkavības ("*ACO*"), ja šāda izmeklēšana ir nepieciešama, lai sagatavotos kontroles pasākumu pieņemšanai pret konkrētām organizācijām ([126]). Saskaņā ar abiem minētajiem likumiem pēc *PSIA* ģenerāldirektora pieprasījuma Sabiedriskās drošības izvērtēšanas komisija var izdot konkrētus "rīkojumus" (uzraudzība/aizliegumi *ACO* gadījumā ([127]), likvidācija/aizliegumi *SAPA* gadījumā ([128])), un šajā saistībā *PSIA* var veikt izmeklēšanu ([129]). Saskaņā ar saņemto informāciju šādu izmeklēšanu vienmēr veic brīvprātīgi, kas

([124]) Tāpēc uzņēmēji var brīvi izvēlēties nesadarboties, neriskējot ar to, ka tam būs kādas sankcijas vai citas negatīvas sekas. Sk. II pielikumu, III.A. iedaļas 1. punkts.

([125]) Tomēr, kā liecina saņemtā informācija, NPA galvenais uzdevums ir koordinēt izmeklēšanu, ko veic dažādie prefektūras policijas departamenti, un veikt informācijas apmaiņu ar ārvalstu iestādēm. Pat pildot šo uzdevumu, *NPA* pārrauga Valsts sabiedriskās drošības komisija, kas cita starpā ir atbildīga par personu tiesību un brīvību aizsardzību (Policijas likuma 5. panta 1. punkts).

([126]) Sk. II pielikumu, III.A. iedaļas 1. punkta 3. apakšpunkts. Abu minēto likumu attiecīgā piemērošanas joma ir ierobežota – *SAPA* attiecas uz "kaitējošām teroristu darbībām", savukārt *ACO* attiecas uz "neselektīvām masu slepkavībām" (kas nozīmē "kaitējošas teroristu darbības" *SAPA* izpratnē, "kurās neselektīvi tiek nogalināts liels skaits cilvēku").

([127]) Sk. *ACO* 5. un 8. pantu. Uzraudzības rīkojums ietver arī ziņošanas pienākumu, kas ir saistošs organizācijai, pret kuru tiek vērsts attiecīgais pasākums. Attiecībā uz procesuālajām garantijām, jo īpaši pārredzamības prasībām un Sabiedriskās drošības izvērtēšanas komisijas iepriekšēju atļauju, sk. *ACO* 12., 13. un 15.–27. pantu.

([128]) Sk. *SAPA* 5. un 7. pantu. Attiecībā uz procesuālajām garantijām, jo īpaši pārredzamības prasībām un Sabiedriskās drošības izvērtēšanas komisijas iepriekšēju atļauju, sk. *SAPA* 11.–25. pantu.

([129]) Sk. *SAPA* 27. pantu un *ACO* 29. un 30. pantu.

nozīmē, ka *PSIA* nedrīkst piespiest personas informācijas īpašnieku sniegt šādu informāciju ([130]). Visas kontroles un izmeklēšanas vienmēr veic tikai tādā apjomā, kāds nepieciešams, lai sasniegtu kontroles mērķi, un to nekādos apstākļos neveic, lai "nepamatoti" ierobežotu ar Japānas Konstitūciju garantētās tiesības un brīvības (*SAPA*/*ACO* 3. panta 1. punkts). Turklāt saskaņā ar *SAPA*/*ACO* 3. panta 2. punktu *PSIA* nekādos apstākļos nedrīkst ļaunprātīgi izmantot šādu kontroli vai izmeklēšanu, ko īsteno, lai sagatavotos šādai kontrolei. Ja Sabiedriskās drošības izlūkošanas aģentūras darbinieks ļaunprātīgi izmanto savas pilnvaras, kuras tam nodrošina attiecīgais likums, liekot personai darīt ko tādu, ko tai nav pienākums darīt, vai iejaucoties personas tiesību īstenošanā, attiecīgajam darbiniekam var piemērot krimināsodu atbilstoši *SAPA* 45. pantam vai *ACO* 42. un 43. pantam. Visbeidzot, abi likumi skaidri paredz, ka to noteikumi, tostarp ar tiem piešķirtās pilnvaras, nekādā gadījumā nav interpretējami plaši (*SAPA*/*ACO* 2. pants).

(156) Visos gadījumos, kad valdība piekļūst informācijai, pamatojoties uz valsts drošības apsvērumiem, kā aprakstīts šajā iedaļā, ir piemērojami Japānas Augstākās tiesas noteiktie ierobežojumi attiecībā uz brīvprātīgu izmeklēšanu, kas nozīmē, ka (elektroniskās) informācijas vākšanai jānotiek atbilstoši nepieciešamības un samērīguma principiem ("atbilstoša metode") ([131]). Japānas iestādes ir skaidri apliecinājušas, ka "informācijas vākšana un apstrāde notiek tikai tādā apmērā, kāds nepieciešams kompetentās publiskās iestādes konkrēto uzdevumu veikšanai, kā arī konkrētu draudu gadījumā". Tādējādi "netiek pieļauta persona informācijas masveida un nediferencēta vākšana vai šāda piekļuve tai valsts drošības apsvērumu dēļ" ([132]).

(157) Turklāt pēc tās savākšanas uz jebkuru personas informāciju, ko glabā publiskās iestādes valsts drošības nolūkos, attiecas *APPIHAO* un tajā paredzētie aizsardzības līdzekļi, ciktāl runa ir par šādas informācijas turpmāku glabāšanu, izmantošanu un izpaušanu (sk. 118. apsvērumu).

3.3.2. *Neatkarīga pārraudzība*

(158) Personas informācijas vākšanai valsts drošības nolūkos piemēro vairāklīmeņu pārraudzību, ko īsteno trīs valdības struktūras.

(159) Pirmkārt, Japānas Parlaments ar savu specializēto komiteju starpniecību var izvērtēt izmeklēšanas likumību, pamatojoties uz savām parlamentārās uzraudzības pilnvarām (Konstitūcijas 62. pants, Parlamenta likuma 104. pants; sk. 134. apsvērumu). Šīs pārraudzības funkcijas papildina īpaši pienākumi ziņot par darbībām, kas tiek īstenotas, pamatojoties uz kādu no iepriekš minētajiem juridiskajiem pamatiem ([133]).

(160) Otrkārt, pastāv vairāki pārraudzības mehānismi izpildvaras jomā.

(161) Attiecībā uz *MOD* pārraudzību īsteno Juridiskās atbilstības ģenerālinspektora birojs (*IGO*) ([134]), kas, pamatojoties uz *MOD* dibināšanas likuma 29. pantu, izveidots kā *MOD* birojs aizsardzības ministra (kuram tas ziņo) pārraudzībā, bet ir neatkarīgs no *MOD* operatīvajiem departamentiem. *IGO* uzdevums ir nodrošināt atbilstību normatīvajiem aktiem, kā arī *MOD* amatpersonu pienākumu pienācīgu izpildi. Tā pilnvarās ietilpst tā dēvēto aizsardzības pārbaužu veikšana gan ar regulāriem intervāliem ("regulārās aizsardzības pārbaudes"), gan individuālos gadījumos ("īpašās aizsardzības pārbaudes"), kas līdz šim ir attiecinātas arī uz personas informācijas pienācīgu izmantošanu ([135]). Veicot šādas pārbaudes, *IGO* var iekļūt telpās (birojos) un prasīt, lai tiek sniegti dokumenti vai informācija, tostarp *MOD* ministra vietnieka paskaidrojumi. Pārbaudi noslēdz ar ziņojumu aizsardzības ministram, kurā izklāsta

([130]) Sk. II pielikumu, III.A. iedaļas 1. punkta 3. apakšpunkts.

([131]) Sk. II pielikumu, III.A. iedaļas 2. punkta b) apakšpunkts. "No Augstākās tiesas judikatūras izriet, ka, lai pieprasītu uzņēmēja brīvprātīgu sadarbību, šādam pieprasījumam ir jābūt nepieciešamam izmeklēšanai aizdomu gadījumā par iespējamu noziegumu un jābūt pamatotam izmeklēšanas mērķa sasniegšanas nolūkiem. Lai gan izmeklēšana, ko veic izmeklēšanas iestādes valsts drošības jomā, atšķiras no izmeklēšanas, kuru veic izmeklēšanas iestādes tiesībaizsardzības jomā, gan no izmeklēšanas juridiskā pamata, gan mērķa viedokļa pamatprincipi par "izmeklēšanas nepieciešamību" un "metodes atbilstību" ir līdzīgi piemērojami valsts drošības jomā un ir jāievēro, pienācīgi ņemot vērā katra gadījuma konkrētos apstākļus."

([132]) Sk. II pielikumu, III.A. iedaļas 2. punkta b) apakšpunkts.

([133]) Sk., piem., *SAPA* 36. pantu / *ACO* 31. pantu (attiecībā uz *PSIA*).

([134]) *IGO* vadītājs ir bijušais prokurors. Sk. II pielikumu, III.B. iedaļas 3. punkts.

([135]) Sk. II pielikumu, III.B. iedaļas 3. punkts. Kā liecina iesniegtais piemērs, regulārajā aizsardzības pārbaudē, kas veikta 2016. gadā attiecībā uz "informētību/gatavību tiesību aktu izpildei", cita starpā tika pārbaudīta "situācija personas informācijas aizsardzības jomā" (pārvaldība, glabāšana utt.). Pārbaudes ziņojumā tika konstatēti neatbilstošas datu pārvaldības gadījumi un izteikts aicinājums ieviest uzlabojumus šajā sakarā. *MOD* publicēja ziņojumu savā tīmekļa vietnē.

konstatējumus un pasākumus uzlabojumu veikšanai (kuru īstenošanu, savukārt, var pārbaudīt turpmākās pārbaudēs). Ziņojums savukārt ir pamats aizsardzības ministra rīkojumiem īstenot pasākumus, kas nepieciešami situācijas risināšanai; ministra vietniekam ir uzticēta šādu pasākumu īstenošana, un viņam ir jāziņo par turpmākajiem pasākumiem.

(162) Runājot par prefektūras policiju – pārraudzību nodrošina neatkarīgās prefektūru sabiedriskās drošības komisijas, kā paskaidrots 135. apsvērumā attiecībā uz krimināltiesību aizsardzību.

(163) Visbeidzot, kā norādīts, *PSIA* var veikt izmeklēšanu tikai tādā apmērā, kādā tas ir nepieciešams attiecībā uz aizlieguma, likvidācijas vai uzraudzības rīkojuma pieņemšanu saskaņā ar *SAPA/ACO*, un attiecībā uz šiem rīkojumiem neatkarīgā ([136]) Sabiedriskās drošības izvērtēšanas komisija īsteno *ex ante* pārraudzību. Turklāt regulāras/periodiskas pārbaudes (kurās vispusīgi izvērtē *PSIA* darbības) ([137]) un īpašas iekšējās pārbaudes ([138]) par individuālu departamentu/darbinieku darbībām utt. veic īpaši norīkoti inspektori, un, pamatojoties uz šādām pārbaudēm, var tikt sniegti norādījumi attiecīgo departamentu u. c. vadītājiem korektīvu pasākumu vai uzlabojumu veikšanai.

(164) Šie pārraudzības mehānismi, kurus papildina personām pieejamā iespēja prasīt *PPC* kā neatkarīgas uzraudzības iestādes iejaukšanos (sk. 168. apsvērumu turpmāk), sniedz pietiekamas garantijas pret Japānas iestāžu pilnvaru ļaunprātīgu izmantošanu valsts drošības jomā un pret jebkādu personas informācijas nelikumīgu vākšanu.

3.3.3. *Individuāla tiesiskā aizsardzība*

(165) Kas attiecas uz individuālu tiesisko aizsardzību – attiecībā uz personas informāciju, ko vāc un "glabā" administratīvas struktūras, šīm struktūrām ir pienākums "censties pienācīgi un nekavējoties apstrādāt visas sūdzības", kuras attiecas uz apstrādi (*APPIHAO* 48. pants).

(166) Turklāt – atšķirībā no krimināllizmeklēšanas – personām (tostarp ārvalstniekiem, kuri dzīvo citās valstīs) principā ir tiesības prasīt to informācijas izpaušanu ([139]), labošanu (arī dzēšanu) un izmantošanas/sniegšanas pārtraukšanu atbilstoši *APPIHAO*. Šajā saistībā administratīvās struktūras vadītājs var atteikties izpaust informāciju, "attiecībā uz kuru ir pamatoti iemesli (…) secināt, ka izpaušana varētu radīt kaitējumu valsts drošībai" (*APPIHAO* 14. panta iv) punkts), un viņš var atteikties izpaust informāciju, pat neatklājot šādas informācijas esību (*APPIHAO* 17. pants). Tāpat, lai gan persona var pieprasīt informācijas izmantošanas pārtraukšanu vai dzēšanu atbilstoši *APPIHAO* 36. panta 1. punkta i) apakšpunktam gadījumā, kad administratīvā struktūra ir nelikumīgi ieguvusi informāciju vai to glabā/izmanto, pārsniedzot to, kas ir nepieciešams konkrētā mērķa sasniegšanai, iestāde var noraidīt pieprasījumu, ja tā konstatē, ka izmantošanas pārtraukšana var traucēt pienācīgi īstenot lietas, kas saistītas ar glabātās personas informācijas izmantošanas nolūku, ņemot vērā minēto lietu raksturu (*APPIHAO* 38. pants). Tomēr, ja ir iespējams viegli nošķirt un izslēgt daļas, kam piemēro izņēmumu, administratīvajām struktūrām ir pienākums atļaut vismaz daļēju izpaušanu (sk., piem., *APPIHAO* 15. panta 1. punktu) ([140]).

([136]) Saskaņā ar Likumu par Sabiedriskās drošības izvērtēšanas komisijas izveidi, komisijas priekšsēdētājs un locekļi "savus pienākumus veic neatkarīgi" (3. pants). Viņus ieceļ premjerministrs ar abu Parlamenta palātu piekrišanu, un viņus var atbrīvot tikai pamatota iemesla dēļ (piem., apcietinājums, amata pienākumu pārkāpums, garīgi vai fiziski traucējumi, bankrota procedūras sākšana).

([137]) Sabiedriskās drošības izlūkošanas aģentūras Periodisko pārbaužu reglaments (*PSIA* ģenerāldirektora norādījumi Nr. 4, 1986. gads).

([138]) Sabiedriskās drošības izlūkošanas aģentūras Īpašo pārbaužu reglaments (*PSIA* ģenerāldirektora norādījumi Nr. 11, 2008. gads). Īpašas pārbaudes veic, kad *PSIA* ģenerāldirektors to uzskata par nepieciešamu.

([139]) Tas attiecas uz tiesībām saņemt glabātās personas informācijas kopiju.

([140]) Sk. arī "diskrecionāras izpaušanas" iespēju pat tad, ja "glabātā personas informācijā", ko prasa izpaust, ir ietverta "neizpaužama informācija" (*APPIHAO* 16. pants).

(167) Jebkurā gadījumā administratīvajai struktūrai ir jāpieņem rakstisks lēmums noteiktā termiņā (30 dienās, ko konkrētos apstākļos var pagarināt vēl par 30 dienām). Ja pieprasījums tiek noraidīts vai apmierināts tikai daļēji, vai ja persona citu iemeslu dēļ uzskata administratīvās struktūras darbību par "nelikumīgu vai nepamatotu", persona var prasīt administratīvu pārskatīšanu, pamatojoties uz Administratīvās pārsūdzības likumu ([141]). Šādā gadījumā administratīvās struktūras vadītājs, lemjot par pārsūdzību, apspriežas ar Informācijas izpaušanas un personas informācijas aizsardzības izvērtēšanas padomi (*APPIHAO* 42. un 43. pants), kas ir specializēta neatkarīga padome, kuras locekļus ieceļ premjerministrs ar abu Parlamenta palātu piekrišanu. Kā liecina saņemtā informācija, Izvērtēšanas padome var veikt pārbaudi ([142]) un šajā saistībā prasīt, lai administratīvā struktūra sniedz glabāto personas informāciju, tostarp jebkādu klasificētu saturu, kā arī iesniedz papildu informāciju un dokumentus. Lai gan galīgais ziņojums, ko nosūta sūdzības iesniedzējam un arī administratīvajai struktūrai un ko publisko, nav juridiski saistošs, to gandrīz visos gadījumos ņem vērā turpmākā rīcībā ([143]). Turklāt attiecīgajai personai ir iespēja apstrīdēt pārsūdzības lēmumu tiesā, pamatojoties uz Administratīvo lietu iztiesāšanas likumu. Tādējādi ir iespējama tiesas kontrole pār to, kā tiek piemērots(-ti) izņēmums(-i) attiecībā uz valsts drošību, un arī pār to, vai šāda izņēmuma izmantošana ir bijusi ļaunprātīga vai pamatota.

(168) Lai veicinātu iepriekš minēto tiesību īstenošanu atbilstoši *APPIHAO*, *MIC* ir izveidojusi 51 "vispārējās informācijas centru", kas sniedz apkopotu informāciju par šīm tiesībām, piemērojamām procedūrām prasības iesniegšanai un iespējām izmantot tiesiskās aizsardzības līdzekļus ([144]). Attiecībā uz administratīvajām struktūrām – tām ir pienākums sniegt "informāciju, kas palīdz identificēt glabāto personas informāciju, kura ir turējumā" ([145]), un veikt "citus atbilstošus pasākumus, ņemot vērā tās personas ērtības, kura plāno iesniegt pieprasījumu" (*APPIHAO* 47. panta 1. punkts).

(169) Tāpat kā tas ir attiecībā uz izmeklēšanu krimināltiesību aizsardzības jomā, arī valsts drošības jomā personas var saņemt individuālu tiesisko aizsardzību, tieši sazinoties ar *PPC*. Tādējādi tiek ierosināta īpašā strīdu izšķiršanas procedūra, ko Japānas valdība izveidojusi ES personām, kuru personas dati tiek nosūtīti atbilstoši šim lēmumam (sīkākus skaidrojumus skatīt 141.–144. un 149. apsvērumā).

(170) Turklāt personas var prasīt tiesisko aizsardzību, iesniedzot prasību par zaudējumu atlīdzināšanu atbilstoši Valsts tiesiskās aizsardzības līdzekļu likumam, kas attiecas arī uz morālu kaitējumu un konkrētos gadījumos uz savākto datu dzēšanu (sk. 147. apsvērumu).

4. SECINĀJUMS: PIETIEKAMS TO PERSONAS DATU AIZSARDZĪBAS LĪMENIS, KURUS NOSŪTA NO EIROPAS SAVIENĪBAS UZŅĒMĒJIEM JAPĀNĀ

(171) Komisija uzskata, ka *APPI*, ko papildina I pielikumā ietvertie Papildu noteikumi, kopā ar II pielikumā ietvertajiem oficiālajiem apliecinājumiem, garantijām un saistībām nodrošina no Eiropas Savienības nosūtīto personas datu aizsardzības līmeni, kas pēc būtības ir līdzvērtīgs tam, kādu garantē Regula (ES) 2016/679.

(172) Komisija arī uzskata, ka kopumā pārraudzības mehānismi un tiesiskās aizsardzības iespējas, kas paredzētas Japānas tiesību aktos, ļauj apzināt saņēmēju *PIHBO* pārkāpumus un piemērot praksē attiecīgus sodus, kā arī sniedz datu subjektam tiesisko aizsardzību, ļaujot piekļūt viņa personas datiem un visbeidzot – šādu datu labošanu vai dzēšanu.

([141]) Administratīvo sūdzību pārskatīšanas likums (2014. gada likums Nr. 160), jo īpaši 1. panta 1. punkts.

([142]) Sk. Likuma par Informācijas izpaušanas un personas informācijas aizsardzības izvērtēšanas padomes izveidi (Likums Nr. 60, 2003. gads) 9. pantu.

([143]) Kā liecina saņemtā informācija, 13 gadu laikā kopš 2005. gada (kad stājās spēkā APPIHAO) tikai divos gadījumos no vairāk nekā 2000 gadījumu administratīvā struktūra neņēma vērā ziņojumu, neraugoties uz faktu, ka Izskatīšanas padome vairākos gadījumos iebilda pret administratīviem lēmumiem. Turklāt, kad administratīvā struktūra pieņem lēmumu, kas atšķiras no ziņojumā izklāstītajiem konstatējumiem, tai ir skaidri jānorāda šādas rīcības iemesli. Sk. II pielikumu, III.C. iedaļu, ņemot vērā Administratīvo sūdzību pārskatīšanas likuma 50. panta 1. punkta iv) apakšpunktu.

([144]) Vispārējās informācijas centri – pa vienam katrā prefektūrā – sniedz iedzīvotājiem skaidrojumus par personas informāciju, ko vāc publiskās iestādes (piem., esošās datubāzes), un piemērojamajiem datu aizsardzības noteikumiem (APPIHAO), tai skaitā par to, kā īstenot tiesības uz datu sniegšanu, labošanu vai izmantošanas pārtraukšanu. Vienlaikus centri darbojas kā kontaktpunkti, kur iedzīvotāji var iesniegt jautājumus vai sūdzības. Sk. II pielikumu, II.C. iedaļas 4. punkta a) apakšpunkts.

([145]) Sk. arī *APPIAHO* 10. un 11. pantu par "personas informācijas datņu reģistru", kuros gan ir paredzēti plaši izņēmumi attiecībā uz "personas informācijas datnēm", ko sagatavo vai iegūst krimināllizmeklēšanai vai kas satur jautājumus, kuri saistīti ar drošību un citām svarīgām valsts interesēm (sk. *APPIHAO* 10. panta 2. punkta i) un ii) apakšpunktu).

(173) Visbeidzot, pamatojoties uz pieejamo informāciju par Japānas tiesisko kārtību, tostarp II pielikumā ietvertajiem Japānas valdības apliecinājumiem, garantijām un saistībām, Komisija uzskata, ka jebkāda iejaukšanās to personu pamattiesībās, kuru personas datus Japānas publiskās iestādes sabiedrisko interešu nolūkos un jo īpaši krimināltiesību aizsardzības un valsts drošības nolūkos nosūta no Eiropas Savienības uz Japānu, tiks ierobežota tādā apmērā, kāds ir absolūti nepieciešams attiecīgā leģitīmā mērķa sasniegšanai, un ka pastāv efektīva tiesiskā aizsardzība pret šādu iejaukšanos.

(174) Tāpēc, ņemot vērā šajā lēmumā izdarītos konstatējumus, Komisija uzskata, ka Japāna nodrošina to personas datu pietiekamu aizsardzības līmeni, kurus nosūta no Eiropas Savienības *PIHBO* Japānā, kam piemēro *APPI*, izņemot gadījumus, kad saņēmējs pieder pie vienas no *APPI* 76. panta 1. punktā uzskaitītajām kategorijām un ja visi apstrādes nolūki vai kāda to daļa atbilst kādam no minētajā noteikumā paredzētajiem nolūkiem.

(175) Ņemot vērā iepriekš izklāstīto, Komisija secina, ka ir izpildīts aizsardzības līmeņa pietiekamības standarts, kas noteikts Regulas (ES) 2016/679 45. pantā, to interpretējot atbilstoši Eiropas Savienības Pamattiesību hartai jo īpaši spriedumā *Schrems* lietā ([146]).

5. DATU AIZSARDZĪBAS IESTĀŽU RĪCĪBA UN INFORMĀCIJA KOMISIJAI

(176) Saskaņā ar Eiropas Savienības Tiesas judikatūru ([147]) un kā atzīts Regulas (ES) 2016/679 45. panta 4. punktā, Komisijai pēc lēmuma par aizsardzības līmeņa pietiekamību pieņemšanas būtu pastāvīgi jāuzrauga norises attiecīgajā trešā valstī, lai novērtētu, vai Japāna joprojām nodrošina pēc būtības līdzvērtīgu aizsardzības līmeni. Vajadzība pēc šāda vērtējuma katrā ziņā rodas, ja Komisija saņem informāciju, kura rada šaubas par to.

(177) Tāpēc Komisijai būtu pastāvīgi jāuzrauga situācija attiecībā uz personas datu apstrādes tiesisko regulējumu un faktisko praksi, kas novērtēta šajā lēmumā, tostarp tas, kā Japānas iestādes izpilda II pielikumā ietvertos apliecinājumus, garantijas un saistības. Lai atvieglotu šo procesu, no Japānas iestādēm tiek gaidīts, ka tās informēs Komisiju par būtiskām norisēm saistībā ar šo lēmumu – gan attiecībā uz personas datu apstrādi, ko veic uzņēmēji, gan attiecībā uz ierobežojumiem un garantijām, kuras piemērojamas, kad publiskās iestādes piekļūst personas datiem. Tam vajadzētu ietvert visus lēmumus, kurus *PPC* ir pieņēmusi saskaņā ar *APPI* 24. pantu, atzīstot trešo valsti par tādu, kas nodrošina Japānā garantētajam aizsardzības līmenim līdzvērtīgu aizsardzības līmeni.

(178) Turklāt, lai Komisija varētu efektīvi pildīt savu uzraudzības funkciju, dalībvalstīm būtu jāinformē Komisija par visām būtiskajām darbībām, ko veikušas valstu datu aizsardzības iestādes ("*DPA*"), jo īpaši attiecībā uz ES datu subjektu vaicājumiem un sūdzībām par personas datu nosūtīšanu no Eiropas Savienības uzņēmējiem Japānā. Komisiju vajadzētu informēt arī par visām pazīmēm, kas liecina, ka darbības, kuras veic Japānas publiskās iestādes, kas atbild par noziedzīgu nodarījumu novēršanu, izmeklēšanu, atklāšanu vai kriminālvajāšanu vai par valsts drošību, tostarp jebkādas pārraudzības struktūras, nenodrošina vajadzīgo aizsardzības līmeni.

(179) Dalībvalstīm un to struktūrām ir pienākums veikt nepieciešamos pasākumus, lai izpildītu Savienības iestāžu tiesību aktus, jo tie tiek uzskatīti par likumīgiem un attiecīgi paredz tiesiskās sekas līdz brīdim, kad tiek atcelti, anulēti saskaņā ar prasību atcelt tiesību aktu vai pasludināti par spēkā neesošiem pēc lūguma sniegt prejudiciālu nolēmumu vai iebildes par prettiesiskumu. Tādējādi lēmums par aizsardzības līmeņa pietiekamību, ko Komisija pieņēmusi saskaņā ar Regulas (ES) 2016/679 45. panta 3. punktu, ir saistošs visām dalībvalstu struktūrām, kurām tas adresēts, tostarp to neatkarīgajām uzraudzības iestādēm. Tajā pašā laikā, kā Eiropas Savienības Tiesa paskaidrojusi spriedumā *Schrems* lietā ([148]) un kā atzīts minētās regulas 58. panta 5. punktā, ja *DPA*, tai skaitā pamatojoties uz iesniegtu sūdzību, apšauba Komisijas pieņemtā lēmuma par aizsardzības līmeņa pietiekamību saderība ar personas pamattiesībām uz privātumu un datu aizsardzību, valsts tiesībās ir jābūt paredzētai tiesiskajai aizsardzībai, lai *DPA* šos iebildumus varētu virzītu izskatīšanai valsts tiesā, kas šaubu gadījumā var apturēt tiesvedību un vērsties Eiropas Savienības Tiesā ar lūgumu sniegt prejudiciālu nolēmumu ([149]).

([146]) Skatīt iepriekš 3. zemsvītras piezīmi.
([147]) *Schrems*, 76. punkts.
([148]) *Schrems*, 65. punkts.
([149]) *Schrems*, 65. punkts: "Šajā ziņā valsts likumdevēja ziņā ir paredzēt tiesiskās aizsardzības līdzekļus, kas valsts uzraudzības iestādei ļauj valstu tiesās celt iebildumus, ko tā uzskata par pamatotiem, lai šīs tiesas – ja arī tās piekrīt šīs iestādes šaubām par Komisijas lēmuma spēkā esamību – iesniegtu lūgumu sniegt prejudiciālu nolēmumu šā lēmuma spēkā esamības izvērtēšanas nolūkos."

6. KONSTATĒJUMA PAR AIZSARDZĪBAS LĪMEŅA PIETIEKAMĪBU PERIODISKA PĀRSKATĪŠANA

(180) Piemērojot Regulas (ES) 2016/679 45. panta 3. punktu ([150]) un ņemot vērā faktu, ka ar Japānas tiesību sistēmu nodrošinātais aizsardzības līmenis var mainīties, Komisijai pēc šā lēmuma pieņemšanas būtu periodiski jāpārbauda, vai konstatējumi par Japānas nodrošinātā aizsardzības līmeņa pietiekamību joprojām ir faktiski un juridiski pamatoti.

(181) Tālab šis lēmums būtu pirmo reizi jāpārskata divu gadu laikā pēc tā stāšanās spēkā. Pēc pirmās pārskatīšanas un atkarībā no tās rezultātiem Komisija ciešā sadarbībā ar komiteju, kas izveidota saskaņā ar VDAR 93. panta 1. punktu, pieņems lēmumu par to, vai būtu jāsaglabā divu gadu cikls. Jebkurā gadījumā turpmākās pārskatīšanas būtu jāveic vismaz reizi četros gados ([151]). Pārskatīšanā būtu jāiekļauj visi šā lēmuma darbības aspekti un jo īpaši Papildu noteikumu piemērošana (īpašu uzmanību pievēršot pieejamiem aizsardzības pasākumiem datu tālākas nosūtīšanas gadījumā), noteikumu par piekrišanu piemērošana, ieskaitot piekrišanas atsaukšanu, personas tiesību īstenošanas efektivitāte, kā arī ierobežojumi un garantijas attiecībā uz valdības piekļuvi, tostarp šā lēmuma II pielikumā izklāstītais tiesiskās aizsardzības mehānisms. Tajā būtu arī jāapskata, cik efektīvi tiek pārraudzīti un izpildīti noteikumi, kas piemērojami gan PIHBO, gan krimināltiesību aizsardzības un valsts drošības jomā.

(182) Lai veiktu pārskatīšanu, Komisijai būtu jātiekas ar *PPC* un vajadzības gadījumā arī ar citām Japānas iestādēm, kas atbild par valdības piekļuvi datiem, tostarp ar attiecīgām pārraudzības struktūrām. Būtu jānodrošina iespēja arī Eiropas Datu aizsardzības kolēģijas (EDPB) pārstāvjiem apmeklēt šādas sanāksmes. Kopīgas pārskatīšanas ietvaros Komisijai būtu jāprasa, lai *PPC* sniedz vispusīgu informāciju par visiem aspektiem, kas ir būtiski konstatējumam par aizsardzības lēmuma pietiekamību, tostarp par ierobežojumiem un garantijām attiecībā uz valdības piekļuvi datiem ([152]). Komisijai arī būtu jāprasa paskaidrojumi par jebkuru informāciju, kas ir būtiska šim lēmumam un ko tā saņēmusi, tostarp publiskiem ziņojumiem no Japānas iestādēm vai citām ieinteresētajām personām Japānā, *EDPB*, individuālām *DPA*, pilsoniskās sabiedrības grupām, plašsaziņas līdzekļu ziņojumiem vai jebkuru citu pieejamu informācijas avotu.

(183) Pamatojoties uz kopīgu pārskatīšanu, Komisijai būtu jāsagatavo publisks ziņojums, kas jāiesniedz Eiropas Parlamentam un Padomei.

7. LĒMUMA PAR AIZSARDZĪBAS LĪMEŅA PIETIEKAMĪBU APTURĒŠANA

(184) Ja, pamatojoties uz regulārajām un *ad hoc* pārbaudēm vai jebkādu citu pieejamo informāciju, Komisija secina, ka Japānas tiesiskās kārtības nodrošināto aizsardzības līmeni vairs nevar uzskatīt par tādu, kas ir pēc būtības līdzvērtīgs Eiropas Savienībā nodrošinātajam, tai būtu jāinformē kompetentās Japānas iestādes par to un jāprasa, lai noteiktā, pamatotā termiņā tiek veikti atbilstoši pasākumi. Tas ietver noteikumus, kas piemērojami gan uzņēmējiem, gan Japānas iestādēm, kuras atbild par krimināltiesību aizsardzību vai valsts drošību. Piemēram, šāda procedūra tiktu sākta gadījumos, kad tālāka nosūtīšana, ieskaitot to, kura veikta, pamatojoties uz *PPC* pieņemtajiem lēmumiem saskaņā ar *APPI* 24. pantu par trešās valsts atzīšanu par tādu, kas nodrošina Japānā garantētajam aizsardzības līmenim līdzvērtīgu aizsardzības līmeni, vairs netiks veikta saskaņā ar aizsardzības pasākumiem, kuri nodrošina aizsardzības nepārtrauktību VDAR 44. panta nozīmē.

(185) Ja pēc noteiktā termiņa Japānas kompetentās iestādes nevar apmierinoši pierādīt, ka šā lēmuma pamatā joprojām ir pietiekams aizsardzības līmenis, Komisijai, piemērojot Regulas (ES) 2016/679 45. panta 5. punktu, būtu jāsāk procedūra šā lēmuma daļējai vai pilnīgai apturēšanai vai atcelšanai. Alternatīvi Komisijai būtu jāsāk procedūra šā lēmuma grozīšanai, jo īpaši datu nosūtīšanai piemērojot piemēro papildu nosacījumus vai ierobežojot konstatējuma par aizsardzības līmeņa pietiekamību tvērumu tikai attiecībā uz tādu datu nosūtīšanu, kurai tiek nodrošināta aizsardzības nepārtrauktību VDAR 44. panta nozīmē.

([150]) Saskaņā ar Regulas (ES) 2016/679 45. panta 3. punktu "[ī]stenošanas aktā paredz periodiskas, vismaz reizi četros gados notiekošas pārskatīšanas mehānismu, kurā ņem vērā visas attiecīgās norises trešajā valstī vai starptautiskajā organizācijā".

([151]) Regulas (ES) 2016/679 45. panta 3. punkts paredz, ka periodiska pārskatīšana jāveic vismaz reizi četros gados. Sk. arī *EDPB, Adequacy Referential, WP 254 rev. 01*.

([152]) Sk. arī II pielikumu, IV. iedaļa. "Saistībā ar lēmuma par aizsardzības līmeņa pietiekamību periodisko pārskatīšanu *PPC* un Eiropas Komisija apmainīsies ar informāciju par datu apstrādi atbilstoši konstatējuma par aizsardzības līmeņa pietiekamību nosacījumiem, tostarp tiem, kas izklāstīti šajā apgalvojumā."

(186) Komisijai būtu jāsāk apturēšanas vai atcelšanas procedūra jo īpaši gadījumā, kad ir pazīmes, ka uzņēmēji, kas saņem personas datus atbilstoši šim lēmumam, neievēro I pielikumā ietvertos Papildu noteikumus un/vai ka netiek nenodrošināta to efektīva izpilde, vai ka Japānas iestādes neievēro šā lēmuma II pielikumā ietvertos apliecinājumus, garantijas un saistības.

(187) Komisijai būtu jāapsver šā lēmuma grozīšanas, apturēšanas vai atcelšanas procedūras sākšana arī gadījumā, ja kopīgās pārskatīšanas kontekstā vai citādi Japānas kompetentās iestādes nesniedz informāciju vai paskaidrojumus, kas nepieciešami, lai novērtētu no Eiropas Savienības uz Japānu nosūtīto personas datu aizsardzības līmeni vai atbilstību šim lēmumam. Šajā saistībā Komisijai būtu jāņem vērā tas, kādā apmērā attiecīgo informāciju var iegūt no citiem avotiem.

(188) Pienācīgi pamatotos steidzamības gadījumos, piemēram, ja pastāv būtiska datu subjektu tiesību pārkāpuma risks, Komisijai apsvērt iespēju pieņemt lēmumu par šā lēmuma apturēšanu vai atcelšanu nekavējoties, ievērojot Eiropas Parlamenta un Padomes Regulas (ES) 2016/679 ([153]) 93. panta 3. punktu saistībā ar Regulas (ES) Nr. 182/2011 8. pantu.

8. **NOSLĒGUMA APSVĒRUMI**

(189) Eiropas Datu aizsardzības kolēģija ir publiskojusi savu atzinumu ([154]), un tas tika ņemts vērā, sagatavojot šo lēmumu.

(190) Eiropas Parlaments ir pieņēmis rezolūciju par digitālās tirdzniecības stratēģiju, kurā tas aicina Komisiju noteikt par prioritāti un paātrināt lēmumu pieņemšanu par aizsardzības līmeņa pietiekamību kopā ar tirdzniecības partneriem, ievērojot nosacījumus, kas noteikti Regulā (ES) 2016/679, jo tas ir būtisks mehānisms, kurš aizsargā personas datu nosūtīšanu no Eiropas Savienības ([155]). Arī Eiropas Parlaments ir arī pieņēmis rezolūciju par Japānas nodrošinātās personas datu aizsardzības pietiekamību ([156]).

(191) Šajā lēmumā paredzētie pasākumi atbilst atzinumam, ko sniegusi komiteja, kura izveidota saskaņā ar VDAR 93. panta 1. punktu,

IR PIEŅĒMUSI ŠO LĒMUMU.

1. pants

1. Regulas (ES) 2016/679 45. panta nolūkos Japāna pietiekamā līmenī nodrošina to personas datu aizsardzību, kurus nosūta no Eiropas Savienības uzņēmējiem Japānā, kuri rīkojas ar personas informāciju, ievērojot Likumu par personas informācijas aizsardzību, ko papildina I pielikumā izklāstītie Papildu noteikumi, kopā ar II pielikumā ietvertajiem oficiālajiem apliecinājumiem, garantijām un saistībām.

([153]) Eiropas Parlamenta un Padomes 2011. gada 16. februāra Regula (ES) Nr. 182/2011, ar ko nosaka normas un vispārīgus principus par dalībvalstu kontroles mehānismiem, kuri attiecas uz Komisijas īstenošanas pilnvaru izmantošanu (OV L 55, 28.2.2011., 13. lpp.).

([154]) Atzinums 28/2018 par Eiropas Komisijas Īstenošanas lēmuma projektu par personas datu pietiekamu aizsardzību Japānā, kas pieņemts 2018. gada 5. decembrī.

([155]) Eiropas Parlamenta 2017. gada 12. decembra rezolūcija "Virzība uz digitālās tirdzniecības stratēģiju" (2017/2065(INI)). Sk. jo īpaši 8. punktu ("(…) atgādina, ka personas dati var tikt nosūtīti trešām valstīm, neizmantojot tirdzniecības nolīgumos paredzēto vispārējo kārtību, kad gan tagad, gan turpmāk tiek izpildītas (…) Regulas (ES) 2016/679 V nodaļā paredzētās prasības; atzīst, ka lēmumi par aizsardzības līmeņa pietiekamību, tostarp daļēji un nozarei specifiski lēmumi, ir svarīgs mehānisms, pārsūtot personas datus no ES uz trešo valsti; norāda, ka ES ir pieņēmusi lēmumus par aizsardzības līmeņa pietiekamību tikai ar četriem no tās 20 lielākajiem tirdzniecības partneriem (…)") un 9. punktu ("Aicina Komisiju noteikt lēmumu par aizsardzības līmeņa pietiekamību pieņemšanu par prioritāti un paātrināt to ar nosacījumu, ka trešās valstis, pamatojoties uz valsts tiesību aktiem vai savām starptautiskajām saistībām, nodrošina tādu aizsardzības līmeni, kas "pēc būtības ir līdzvērtīgs" ES garantētajam aizsardzības līmenim (…)").

([156]) Eiropas Parlamenta 2018. gada 13. decembra rezolūcija par Japānas nodrošinātās personas datu aizsardzības pietiekamību (2018/2979 (RSP)).

2. Šis lēmums neattiecas uz personas datiem, ko nosūta saņēmējiem, kuri pieder pie kādas no turpmāk norādītajām kategorijām, ciktāl visi personas datu apstrādes nolūki vai to daļa atbilst kādām no uzskaitītajiem nolūkiem, proti:

a) raidsabiedrībām, laikrakstu izdevējiem, komunikāciju aģentūrām vai citām preses organizācijām (tostarp privātpersonām, kuru darījumdarbība ir saistīta ar presi), ciktāl tie apstrādā personas datus preses vajadzībām;

b) personām, kuras ir profesionāli nodarbojas ar rakstniecību, ciktāl tas ietver personas datus;

c) universitātēm un jebkurām citām organizācijām vai grupām, kuru mērķis ir nodrošināt akadēmiskās studijās, vai jebkurai personai, kas pieder pie šādas organizācijas, ciktāl tās apstrādā personas datus akadēmisko studiju mērķiem;

d) reliģiskām struktūrām, ciktāl tās apstrādā personas datus reliģiskas darbības mērķiem (tostarp visām saistītajām darbībām); un

e) politiskām struktūrām, ciktāl tās apstrādā personas datus savas politiskās darbības mērķiem (tostarp visām saistītajām darbībām).

2. pants

Ikreiz, kad kompetentās iestādes dalībvalstīs nolūkā aizsargāt personas attiecībā uz viņu personas datu apstrādi, īsteno savas pilnvaras atbilstoši Regulas (ES) 2016/679 58. pantam, kā rezultātā tiek apturēta vai galīgi aizliegta datu plūsma kādam konkrētam uzņēmējam Japānā 1. pantā noteiktajā piemērošanas jomā, attiecīgā dalībvalsts nekavējoties informē Komisiju.

3. pants

1. Komisija nepārtraukti pārrauga to, kā tiek piemērots tiesiskais regulējums, kas ir šā lēmuma pamatā, tai skaitā nosacījumi, ar kādiem tiek veikta datu tālāka nosūtīšana, lai izvērtētu, vai Japāna turpina nodrošināt pietiekamu aizsardzības līmeni 1. panta nozīmē.

2. Dalībvalstis un Komisija informē viena otru par gadījumiem, kad Personas informācijas aizsardzības komisija vai jebkura cita Japānas kompetentā iestāde nespēj nodrošināt atbilstību tiesiskajam regulējumam, kas ir šā lēmuma pamatā.

3. Dalībvalstis un Komisija informē viena otru par visām pazīmēm, kas liecina, ka Japānas publisko iestāžu iejaukšanās personu tiesībās uz viņu personas datu aizsardzību pārsniedz absolūti nepieciešamo vai ka nav efektīvas tiesiskās aizsardzības pret šādu iejaukšanos.

4. Divu gadu laikā pēc šā lēmuma paziņošanas dalībvalstīm un pēc tam vismaz reizi četros gados Komisija izvērtē 1. panta 1. punktā ietverto konstatējumu, pamatojoties uz visu pieejamo informāciju, tostarp informāciju, kas saņemta kopā ar attiecīgajām Japānas iestādēm veiktās kopīgās pārskatīšanas ietvaros.

5. Ja Komisija ir konstatējusi pazīmes, ka vairs netiek nodrošināts pietiekams aizsardzības līmenis, Komisija informē Japānas kompetentās iestādes. Vajadzības gadījumā Komisija var lemt par šā lēmuma apturēšanu, grozīšanu vai atcelšanu vai tā piemērošanas jomas ierobežošanu, jo īpaši gadījumos, kad pazīmes liecina, ka:

a) uzņēmēji Japānā, kuri saņēmuši personas datus no Eiropas Savienības atbilstoši šim lēmumam, nenodrošina papildu garantijas, kas izklāstītas šā lēmuma I pielikumā ietvertajos Papildu noteikumos, vai ka pārraudzība un izpilde šajā ziņā ir nepietiekama;

b) Japānas publiskās iestādes nepilda šā lēmuma II pielikumā ietvertos apliecinājumus, garantijas un saistības, tostarp attiecībā uz nosacījumiem un ierobežojumiem to personas datu vākšanai un piekļuvei tiem, kurus atbilstoši šim lēmumam nosūta Japānas publiskās iestādes krimināltiesību aizsardzības vai valsts drošības nolūkos.

Komisija var arī iesniegt šādu pasākumu projektus, ja Japānas valdības nesadarbošanās liedz Komisijai noteikt, vai ir skarts šā lēmuma 1. panta 1. punktā ietvertais konstatējums.

4. pants

Šis lēmums ir adresēts dalībvalstīm.

Briselē, 2019. gada 23. janvārī

Komisijas vārdā –
Komisijas locekle
Věra JOUROVÁ

1. PIELIKUMS

PAPILDU NOTEIKUMI, KAS IZSTRĀDĀTI SASKAŅĀ AR LIKUMU PAR PERSONAS INFORMĀCIJAS AIZSARDZĪBU, NO ES NOSŪTĪTO PERSONAS DATU IZMANTOŠANAI, PAMATOJOTIES UZ LĒMUMU PAR AIZSARDZĪBAS LĪMEŅA PIETIEKAMĪBU

Saturs

[Terminoloģija]

"Likums"	Likums par personas informācijas aizsardzību (Likums Nr. 57, 2003. gads)
"Ministru kabineta rīkojums"	Ministru kabineta rīkojums, ar ko uzdod izpildīt Likumu par personas informācijas aizsardzību (Ministru kabineta rīkojums Nr. 507, 2003. gads)
"Noteikumi"	Likuma par personas informācijas aizsardzību izpildes noteikumi (Personas informācijas aizsardzības komisijas noteikumi Nr. 3, 2016. gads)
"Vispārējo noteikumu pamatnostādnes"	Likuma par personas informācijas aizsardzību pamatnostādnes (Personas informācijas aizsardzības komisijas paziņojums Nr. 65, 2015. gads)
"ES"	Eiropas Savienība, ieskaitot tās dalībvalstis, un, ņemot vērā EEZ līgumu, Islande, Lihtenšteina un Norvēģija
"VDAR"	Eiropas Parlamenta un Padomes Regula par fizisku personu aizsardzību attiecībā uz personas datu apstrādi un šādu datu brīvu apriti un ar ko atceļ Direktīvu 95/46/EK (Vispārīgā datu aizsardzības regula)
"lēmums par aizsardzības līmeņa pietiekamību"	Eiropas Komisijas lēmums par to, ka trešā valsts vai kāda minētās trešās valsts teritorija utt. atbilstoši VDAR 45. pantam nodrošina personas datu pietiekamu aizsardzības līmeni

Lai starp Japānu un ES notiktu savstarpēja un raita personas datu nosūtīšana, Personas informācijas aizsardzības komisija uzskata ES par ārvalsti, kas izveidojusi personas informācijas aizsardzības sistēmu, kuras standarti atzīti par līdzvērtīgiem tiem Japānas standartiem, kas, pamatojoties uz Likuma 24. pantu, izvirzīti personas tiesību un interešu aizsardzībai, un vienlaikus Eiropas Komisija lēma, ka Japāna atbilstoši VDAR 45. pantam nodrošina personas datu pietiekamu aizsardzību.

Ar šo starp Japānu un ES savstarpēja un raita personas datu nodošana notiks tādā veidā, kas nodrošina personas tiesību un interešu augsta līmeņa aizsardzību. Lai nodrošinātu tādas personas informācijas augsta līmeņa aizsardzību, kas no ES saņemta, pamatojoties uz lēmumu par aizsardzības līmeņa pietiekamību, un, ņemot vērā, ka abas sistēmas, lai gan lielā mērā saskaņotas, tomēr dažos aspektos būtiski atšķiras, Personas informācijas aizsardzības komisija ir pieņēmusi minētos papildu noteikumus, pamatojoties uz Likumu par sadarbības īstenošanu u. tml. ar citām valstīm, nolūkā nodrošināt, ka uzņēmējs, kurš izmanto personas informāciju, kas no ES saņemta, pamatojoties uz lēmumu par aizsardzības līmeņa pietiekamību, izmantotu pienācīgi, un pienācīgi un efektīvi īstenot šādos noteikumos ([1]) paredzētos pienākumus.

([1]) Likuma 4. pants, 6. pants, 8. pants, 24. pants, 60. pants un 78. pants un noteikumu 11. pants.

Konkrētāk, Likuma 6. pants sniedz pilnvaras veikt nepieciešamo likumdošanas vai cita veida rīcību, kas nodrošina personas informācijas labāku aizsardzību, un, pieņemot tādus stingrākus noteikumus, kuri papildina un pārsniedz Likuma un Ministru kabineta rīkojuma noteikumus, veidot starptautiski saskaņojamu sistēmu. Tādēļ Personas informācijas aizsardzības komisija kā iestāde, kuras kompetencē ir Likuma vispārējās darbības pārvaldība, atbilstoši Likuma 6. pantam ir pilnvarota ieviest stingrākus noteikumus, izstrādājot šos Papildu noteikumus, kuri nodrošina personas tiesību un interešu augstāka līmeņa aizsardzību saistībā ar tādu personas datu izmantošanu, kas, pamatojoties uz lēmumu par aizsardzības līmeņa pietiekamību, saņemti no ES, ieskaitot "īpaši aizsargājamās personas informācijas" definīciju saskaņā ar Likuma 2. panta 3. punktu un "saglabāto personas datu" definīciju saskaņā ar Likuma 2. panta 7. punktu (arī par attiecīgo glabāšanas ilgumu).

Papildu noteikumi tādējādi ir saistoši uzņēmējam, kurš izmanto personas informāciju un kurš, pamatojoties uz lēmumu par aizsardzības līmeņa pietiekamību, saņem no ES nosūtītus personas datus un kuram tādēļ šie noteikumi ir jāievēro. Tā kā papildu noteikumi ir juridiski saistoši, Personas informācijas aizsardzības komiteja nodrošina visu tiesību un pienākumu izpildi tādā pašā veidā kā Likuma noteikumus, kurus šie noteikumi papildina ar stingrākiem un/vai sīkāk izstrādātiem noteikumiem. Gadījumā, ja tiek pārkāptas tiesības un pienākumi, kuri izriet no Papildu noteikumiem, personas var saņemt tiesisko aizsardzību tādā pašā veidā kā attiecībā uz Likuma noteikumiem, kurus šie noteikumi papildina ar stingrākiem un/vai sīkāk izstrādātiem noteikumiem.

Attiecībā uz Personas informācijas aizsardzības komitejas veikto izpildi – gadījumā, ja uzņēmējs, kurš izmanto personas informāciju, nepilda vienu vai vairākus pienākumus, kas izriet no Papildu noteikumiem, Personas informācijas aizsardzības komisija ir pilnvarota saskaņā ar Likuma 42. pantu pieņemt pasākumus. Attiecībā uz personas informāciju, ko parasti saņem no ES, pamatojoties uz lēmumu par aizsardzības līmeņa pietiekamību, – uzņēmēja, kurš izmanto personas informāciju, nerīkošanās bez likumīga pamata ([2]) atbilstoši Likuma 42. panta 1. punktam saņemtajam ieteikumam tiek uzskatīta par nenovēršamu un būtisku personas tiesību un interešu pārkāpumu Likuma 42. panta 2. punkta nozīmē.

1. Īpaši aizsargājama personas informācija (Likuma 2. panta 3. punkts)

Likuma 2. panta 3. punkts

3. Šajā Likumā "īpaši sargājama personas informācija" ir personas informācija, kas ietver principāla rasi, pārliecību, sociālo stāvokli, slimības vēsturi, sodāmību, faktus par nozieguma rezultātā nodarītu kaitējumu vai citus aprakstus u. tml., kas ar Ministru kabineta rīkojumu noteikti par tādiem, kuras izmantošanā jāievēro īpaša rūpība, lai principālam neradītu negodīgu diskrimināciju, kaitējumu vai citas neizdevīgas situācijas.

Ministru kabineta rīkojuma 2. pants

Tādi apraksti u. tml., kas atbilstoši Likuma 2. panta 3. punktam noteikti ar Ministru kabineta rīkojumu, kuros sniegtas kādas no turpmāk minētajām ziņām (izņemot tās, kuras attiecas uz principāla slimības vēsturi un sodāmību):

i) konstatēti fiziskās attīstības traucējumi, intelektuālās attīstības traucējumi, garīga rakstura traucējumi (arī attīstības traucējumi) vai citādi fizisko vai garīgo funkciju traucējumi, kas minēti Personas informācijas aizsardzības komitejas noteikumos;

ii) principāla medicīniskās apskates vai citas pārbaudes rezultāti (turpmāk "medicīniskā pārbaude"), ko slimību profilakses vai savlaicīgas konstatēšanas nolūkā veicis ārsts vai cita persona, kas pilda ar medicīnu saistītus pienākumus (turpmāk nākamajā apakšpunktā "ārsts u. tml.");

iii) fakts, ka principāla garīgā un fiziskā stāvokļa uzlabošanai ārsts u. tml. sniedzis norādījumus, medicīnisko aprūpi vai zāļu recepti, pamatojoties uz medicīniskās pārbaudes u. tml. rezultātiem, vai sakarā ar slimību, ievainojumu vai citādām garīga un fiziska rakstura izmaiņām;

iv) fakts, ka pret principālu kā aizdomās turamo vai atbildētāju ticis veikts arests, pārmeklēšana, konfiskācija, aizturēšana, kriminālvajāšana vai citas, ar krimināllietu saistītas procedūras;

([2]) Likumīgs pamats ir ārkārtas gadījums, ko uzņēmējs, kurš izmanto personas informāciju, nevar kontrolēt un pamatoti prognozēt (piemēram, dabas katastrofas) vai gadījums, kad nepieciešamība rīkoties saistībā ar ieteikumu, ko atbilstoši Likuma 42. panta 1. punktam sniegusi Personas informācijas aizsardzības komisija, ir zudusi, jo šis uzņēmējs ir īstenojis alternatīvu rīcību, kura pilnībā novērš pārkāpumu.

v) fakts, ka saskaņā ar 3. panta 1. punktu Likumā par nepilngadīgajiem attiecībā uz principālu kā nepilngadīgo noziedznieku vai kā aizdomās turamo par šādu nodarījumu veikta izmeklēšana, novērošanas un aizsardzības pasākums, uzklausīšana un lēmuma pieņemšana, aizsargpasākums vai citādas procedūras, kas saistītas ar nepilngadīgo aizsardzības lietu.

Noteikumu 5. pants

Fizisko un garīgo funkciju traucējumi, kas atbilstoši Rīkojuma 2. panta i) punktam iekļauti Personas informācijas aizsardzības komisijas izstrādātajos noteikumos, ir šādi traucējumi:

i) fiziskās attīstības traucējumi, kas noteikti tabulā, kura pievienota Likumam par personu ar fizisko invaliditāti labklājību (Likums Nr. 283, 1949. gads);

ii) intelektuālās attīstības traucējumi, kas minēti Likumā par personu ar intelektuālās attīstības traucējumiem labklājību (Likums Nr. 37, 1960. gads);

iii) garīga rakstura traucējumi, kas minēti Likumā par garīgo veselību un Likumā par personu ar garīga rakstura traucējumiem labklājību (Likums Nr. 123, 1950. gads) (to skaitā attīstības traucējumi, kas minēti 2. panta 1. punktā Likumā par atbalstu personām ar attīstības traucējumiem, bet ne intelektuālās attīstības traucējumi saskaņā ar Likumu par personu ar intelektuālās attīstības traucējumiem labklājību);

iv) neārstējama slimība vai citādas retas slimības, kuru saskaņā ar Ministru kabineta rīkojumu atbilstoši 4. panta 1. punktam Likumā par vispusīgu atbalstu ikdienā un sociālajā dzīvē personām ar invaliditāti (Likums Nr. 123, 2005. gads) noteiktā smaguma pakāpe ir līdzvērtīga tādu slimību smaguma pakāpei, kuras Veselības, darba un labklājības ministrija noteikusi minētajā punktā.

Ja personas datos, kas no ES saņemti, pamatojoties uz lēmumu par aizsardzības līmeņa pietiekamību, ir tādi dati par fiziskas personas seksuālo dzīvi, seksuālo orientāciju vai dalību arodbiedrībās, kuras atbilstoši VDAR uzskata par īpašām personas datu kategorijām, tad uzņēmējam, kurš izmanto personas informāciju, minētie personas dati jāizmanto tādā pašā veidā kā īpaši sargājama personas informācija Likuma 2. panta 3. punkta nozīmē.

2. Saglabātie personas dati (Likuma 2. panta 7. punkts)

Likuma 2. panta 7. punkts

7. Šajā Likumā "saglabātie personas dati" ir personas dati, kurus uzņēmējs, kurš izmanto personas informāciju, drīkst atklāt, labot, to papildināt vai dzēst, beigt izmantot, izdzēst un beigt sniegt trešai personai un kuri nav nedz dati, kuri ar Ministru kabineta rīkojumu atzīti par tādiem, kas var kaitēt sabiedrības vai citām interesēm, ja tiek darīta zināma to esība vai neesība, nedz dati, kurus paredzēts dzēst laikposmā, kas nepārsniedz vienu gadu un kas noteikts ar Ministru kabineta rīkojumu.

Ministru kabineta rīkojuma 4. pants

Saskaņā ar 2. panta 7. punktu Ministru kabineta rīkojumā noteikti šādi dati:

i) dati, attiecībā uz kuriem pastāv iespēja, ka gadījumā, ja tiktu darīta zināma to esība vai neesība, tas kaitētu principāla vai trešās personas dzīvībai, veselībai vai labklājībai;

ii) dati, attiecībā uz kuriem pastāv iespēja, ka gadījumā, ja tiktu darīta zināma to esība vai neesība, tas veicinātu vai izraisītu nelikumīgu vai nepamatotu darbību;

iii) dati, attiecībā uz kuriem pastāv iespēja, ka gadījumā, ja tiktu darīta zināma to esība vai neesība, tas kaitētu valsts drošībai, iznīcinātu uzticības attiecības ar ārvalsti vai starptautisku organizāciju vai radītu neizdevīgu stāvokli sarunās ar ārvalsti vai starptautisku organizāciju;

iv) dati, attiecībā uz kuriem pastāv iespēja, ka gadījumā, ja tiktu darīta zināma to esība vai neesība, tas traucētu uzturēt sabiedrisko drošību un kārtību, piemēram, novērst, izskaust vai izmeklēt noziegumus.

Ministru kabineta rīkojuma 5. pants

Ministru kabineta rīkojumā saskaņā ar Likuma 2. panta 7. punktu noteiktais laikposms ir seši mēneši.

Personas dati, kas saņemti no ES, pamatojoties uz lēmumu par aizsardzības līmeņa pietiekamību, jāizmanto kā saglabātie personas dati Likuma 2. panta 7. punkta nozīmē neatkarīgi no tā, cik ilgā laikā tos paredzēts dzēst.

Ja Ministru kabineta rīkojuma personas datu definīcijā, proti, "dati, kas var kaitēt sabiedrības vai citām interesēm, ja tiek darīta zināma to esība vai neesība", ietilpst personas dati, kas saņemti no ES, pamatojoties uz lēmumu par aizsardzības līmeņa pietiekamību, tad šādi dati nav jāizmanto kā saglabātie personas dati (skatīt Ministru kabineta rīkojuma 4. pantu; Vispārējo noteikumu pamatnostādnes "2-7. Saglabātie personas dati").

3. Izmantošanas nolūka norādīšana, ierobežojumi izmantošanas nolūka dēļ (Likuma 15. panta 1. punkts, 16. panta 1. punkts un 26. panta 1. un 3. punkts)

Likuma 15. panta 1. punkts

1. Uzņēmums, kurš izmanto personas informāciju, izmantojot personas informāciju, tik skaidri, cik vien iespējams, norāda personas informācijas izmantošanas nolūku (turpmāk "izmantošanas nolūks").

Likuma 16. panta 1. punkts

1. Uzņēmums, kurš izmanto personas informāciju, personas informāciju bez iepriekšējas principāla piekrišanas neizmanto, pārsniedzot apmēru, kas ir nepieciešams, lai sasniegtu izmantošanas nolūku, kurš noteikts atbilstoši iepriekšējam pantam.

Likuma 26. pants (1. un 3. punkts)

1. Kad uzņēmējs, kurš izmanto personas informāciju, no trešās personas saņem personas datus, apstiprina šādas atbilstoši Personas informācijas aizsardzības komisijas noteikumos minētās ziņas: (izlaists);

   i) (izlaists);

   ii) apstākļus, kādos minētā trešā persona bija ieguvusi minētos personas datus.

3. Apstiprinājis ziņas atbilstoši 1. punkta noteikumiem, uzņēmējs, kurš izmanto personas informāciju, atbilstoši Personas informācijas aizsardzības komisijas noteikumiem reģistrē personas datu saņemšanas datumu, ziņas par minēto apstiprinājumu un citas Personas informācijas aizsardzības komisijas noteikumos paredzētās ziņas.

Ja uzņēmēji, kuri izmanto personas informāciju, personas informāciju izmanto, pārsniedzot apmēru, kas ir nepieciešams, lai sasniegtu izmantošanas nolūku, kurš norādīts Likuma 15. panta 1. punktā, tad tie pirms tam saņem attiecīgā principāla piekrišanu (Likuma 16. panta 1. punkts). Ja uzņēmēji, kuri izmanto personas informāciju, saņem personas datus no trešās personas, tad tie saskaņā ar Noteikumiem apstiprina tādas ziņas kā apstākļi, kādos minētā trešā persona saņēmusi minētos personas datus, un minētās ziņas reģistrē (Likuma 26. panta 1. un 3. punkts).

Ja uzņēmējs, kurš izmanto personas informāciju, saņem personas datus no ES, pamatojoties uz lēmumu par aizsardzības līmeņa pietiekamību, tad pie minēto personas datu iegūšanas apstākļiem, kurus apstiprina un reģistrē saskaņā ar 26. panta 1. un 3. punktu, norāda, kādam izmantošanas nolūkam dati no ES saņemti.

Tāpat, ja uzņēmējs, kurš izmanto personas informāciju, no cita uzņēmēja, kurš izmanto personas informāciju, saņem no ES iepriekš nosūtītus personas datus, pamatojoties uz lēmumu par aizsardzības līmeņa pietiekamību, tad pie minēto personas datu iegūšanu apstākļiem, kurus apstiprina un reģistrē saskaņā ar 26. panta 1. un 3. punktu, norāda, kādam izmantošanas nolūkam dati tika saņemti.

Uzņēmējam, kurš izmanto personas informāciju, iepriekš minētajos gadījumos jānorāda minēto personas datu izmantošanas nolūks, kas nepārsniedz izmantošanas nolūka tvērumu, kuram dati tika sākotnēji nosūtīti vai vēlāk saņemti un kurš apstiprināts un reģistrēts atbilstoši 26. panta 1. un 3. punktam, un minētie dati jāizmanto minētajā tvērumā (saskaņā ar Likuma 15. panta 1. punktu un 16. panta 1. punktu).

4. Ierobežojumi sniegt datus trešai personai ārvalstī (Likuma 24. pants, Noteikumu 11-2. pants)

Likuma 24. pants

Izņemot tos gadījumus, kas minēti iepriekšējā panta 1. punkta katrā apakšpunktā, ja uzņēmējs, kurš izmanto personas informāciju, sniedz personas datus trešai personai (izņemot tādu personu, kura izveido Personas informācijas aizsardzības komisijas noteikumos iestrādātajiem standartiem atbilstošu sistēmu, kas vajadzīga nepārtrauktai rīcībai, kura līdzvērtīga tai rīcībai, ko uzņēmējs, kurš izmanto personas informāciju, īsteno attiecībā uz personas datu izmantošanu atbilstoši šīs iedaļas noteikumiem; turpmāk šajā pantā tāpat) ārvalstī (proti, valstī vai reģionā ārpus Japānas teritorijas; turpmāk tāpat) (izņemot ārvalstis, kuras Personas informācijas aizsardzības komisijas noteikumos uzskatītas par ārvalstīm, kuras izveido tādu personas informācijas aizsardzības sistēmu, par kuru atzīts, ka tai personas tiesību un interešu aizsardzībā ir Japānas sistēmas standartiem līdzvērtīgi standarti; turpmāk šajā pantā tāpat) saņemt iepriekšēju principāla piekrišanu par to, ka tas piekrīt datu sniegšanai trešai personai ārvalstī. Šajā gadījumā iepriekšējā panta noteikumus nepiemēro.

Noteikumu 11-2. pants

Standarti, kas saskaņā ar Likuma 24. pantu iestrādāti Personas informācijas aizsardzības komisijas noteikumos, attiecas uz šādiem apakšpunktiem:

i) uzņēmējs, kurš izmanto personas informāciju, un persona, kura saņem personas datus, attiecībā uz personas datiem, kurus izmanto saņemošā persona, ar atbilstošu un samērīgu metodi ir nodrošinājuši pasākumu īstenošanu saskaņā ar Likuma IV nodaļas 1. iedaļas noteikumiem;

ii) personas datus saņemošā persona tikusi atzīta, pamatojoties uz personas informācijas izmantošanas starptautisko sistēmu.

Gadījumos, izņemot no i) līdz iii) apakšpunktam minētos gadījumus, kad uzņēmējs, kurš izmanto personas informāciju, personas datus, kas no ES saņemti, pamatojoties uz lēmumu par aizsardzības līmeņa pietiekamību, sniedz trešai personai ārvalstī, tas atbilstoši Likuma 24. pantam saņem iepriekšēju principāla piekrišanu par to, ka tas piekrīt datu sniegšanai trešai personai ārvalstī pēc tam, kad principālam sniegta lēmumam par piekrišanu vajadzīgā nodošanas apstākļu informācija.

i) Ja trešā persona atrodas valstī, kas Noteikumos uzskatīta par ārvalsti, kura izveido tādu personas informācijas aizsardzības sistēmu, par kuru atzīts, ka tai personas tiesību un interešu aizsardzībā ir Japānas sistēmas standartiem līdzvērtīgi standarti;

ii) ja uzņēmējs, kurš izmanto personas informāciju, un trešā persona, kura saņem personas datus, attiecībā uz trešo personu, kura izmanto personas datus, ir īstenojuši kopīgus pasākumus, kuri ar atbilstošu un samērīgu metodi (proti, līgumu, cita veida saistošu vienošanos vai saistošu kārtību uzņēmumu grupā) nodrošina Likumā, ko skata kopā ar šiem Noteikumiem, noteiktajam aizsardzības līmenim līdzvērtīgu līmeni;

iii) gadījumos, uz kuriem attiecas Likuma 23. panta 1. punkta visi apakšpunkti.

5. Anonīmi apstrādāta informācija (Likuma 2. panta 9. punkts un 36. panta 1. un 2. punkts)

Likuma 2. panta 9. punkts

9. Šajā Likumā "anonīmi apstrādāta informācija" ir personas informācija, ko var iegūt, apstrādājot personas informāciju tādā veidā, ka nav iespējams nedz identificēt konkrētu personu, veicot turpmākajos punktos minēto rīcību saskaņā ar katrā minētajā punktā sniegto personas informācijas iedalījumu, nedz atjaunot personas informāciju:

i) personas informācija, uz ko attiecas 1. punkta i) apakšpunkts.

Minētajā personas informācijā iekļauto aprakstu daļu dzēšana (arī minēto aprakstu daļu u.tml. aizstāšana ar citiem aprakstiem u. tml., kas nenotiek pēc noteiktas metodes, kura ļauj atjaunot minētās aprakstu daļas);

ii) personas informācija, uz ko attiecas 1. punkta i) apakšpunkts.

Visu minētajā personas informācijā iekļauto individuālo identifikācijas kodu dzēšana (arī minēto individuālo identifikācijas kodu aizstāšana ar citiem aprakstiem u. tml., kas nenotiek pēc noteiktas metodes, kura ļauj atjaunot minētos individuālos identifikācijas kodus).

Likuma 36. panta 1. punkts

1. Kad uzņēmējs, kurš izmanto personas informāciju, iegūst anonīmi apstrādātu informāciju (kas nepārsniedz informāciju anonīmi apstrādātas informācijas datubāzē u. tml.; turpmāk tāpat), tas pārstrādā personas informāciju saskaņā ar Personas informācijas aizsardzības komisijas noteikumos iestrādātajiem standartiem, kuri vajadzīgi, lai nebūtu iespējams identificēt konkrētu personu un atjaunot šādas informācijas iegūšanā izmantoto personas informāciju.

Noteikumu 19. pants

Šādi ir Personas informācijas aizsardzības komisijas noteikumos iestrādātie standarti saskaņā ar Likuma 36. panta 1. Punktu:

i) tādu aprakstu u. tml. pilnīga vai daļēja dzēšana, kas ļauj identificēt personas informācijā iekļauto konkrēto personu (arī šādu aprakstu u. tml. aizstāšana ar citiem aprakstiem u. tml., kura nenotiek pēc noteiktas metodes, kura aprakstus u. tml. ļauj atjaunot pilnībā vai daļēji);

ii) visu minētajā personas informācijā iekļauto individuālo identifikācijas kodu dzēšana (arī šādu kodu aizstāšana ar citiem aprakstiem u. tml., kas nenotiek pēc noteiktas metodes, kura ļauj atjaunot individuālos identifikācijas kodus);

iii) tādu kodu dzēšana (tikai tādu kodu dzēšana, kuri savstarpēji saista no daudzām vienībām sastāvošu informāciju, kuru faktiski izmanto uzņēmējs, kurš izmanto personas informāciju), kuri personas informāciju saista ar informāciju, kas iegūta, īstenojot pasākumus attiecībā pret personas informāciju (ieskaitot minēto kodu aizstāšanu ar tādiem citiem kodiem, kuri minēto personas informāciju nevar saistīt ar informāciju, kas iegūta, attiecībā pret minēto personas informāciju īstenojot pasākumus, turklāt to nedarot pēc noteiktas metodes, kura ļauj atjaunot minētos kodus);

iv) idiosinkrātisku aprakstu u. tml. dzēšana (arī tādu aprakstu u. tml. aizstāšana ar citiem aprakstiem u. tml., kura nenotiek pēc noteiktas metodes, kas ļauj atjaunot idiosinkrātiskus aprakstus u. tml.);

v) atbilstošas rīcības īstenošana papildus iepriekšējā apakšpunktā izklāstītajai rīcībai, pamatojoties uz rezultātiem, kas iegūti, ņemot vērā personas informācijas datubāzes elementus u. tml., piemēram, atšķirība starp aprakstiem u.tml. personas informācijā un aprakstiem u.tml. citā personas informācijā, kas iekļauta personas informācijas datubāzē u.tml., kura aptver minēto personas informāciju.

Likuma 36. panta 2. punkts

1. Ieguvis anonīmi apstrādātu informāciju, uzņēmējs, kurš izmanto personas informāciju, saskaņā ar Personas informācijas aizsardzības komisijas noteikumos iestrādātajiem standartiem, kas vajadzīgi, lai novērstu, ka tiek nopludināta informācija, kas saistīta ar minētajiem aprakstiem u.tml. un individuālajiem identifikācijas kodiem, kuri dzēsti no personas informācijas, kas tika izmantota anonīmi apstrādātas informācijas iegūšanai, un informācija, kas saistīta ar atbilstoši iepriekšējā punkta noteikumiem veiktās apstrādes metodi, īsteno šādas informācijas drošības kontroli.

Noteikumu 20. pants

Šādi ir Personas informācijas aizsardzības komisijas noteikumos iestrādātie standarti saskaņā ar Likuma 36. panta 2. Punktu:

i) skaidri definēt personas, kura izmanto informāciju, pilnvaras un atbildību par tiem aprakstiem u. tml. un individuālajiem identifikācijas kodiem, kuri dzēsti no personas informācijas, kura izmantota anonīmi apstrādātas informācijas iegūšanai, un informāciju, kas attiecas uz atbilstoši Likuma 36. panta 1. punktam izmantoto apstrādes metodi (attiecas tikai uz tiem, kuri var atjaunot personas informāciju, izmantojot šādu saistīto informāciju) (turpmāk šajā pantā "apstrādes metode un cita saistīta informācija");

ii) izstrādāt noteikumus par apstrādes metodes un citas saistītās informācijas izmantošanu, pienācīgu apstrādes metodes un citas saistītās informācijas izmantošanu saskaņā ar noteikumiem, izvērtēt izmantošanas situāciju un īstenot vajadzīgo, uz šāda izvērtējuma rezultātiem balstītu rīcību nolūkā panākt uzlabojumus;

iii) īstenot atbilstošu rīcību, kas vajadzīga, lai novērstu, ka persona, kura nav likumīgi pilnvarota izmantot apstrādes metodi un citu saistīto informāciju, izmanto apstrādes metodi un citu saistīto informāciju.

Personas informāciju, kas no ES saņemta, pamatojoties uz lēmumu par aizsardzības līmeņa pietiekamību, uzskata par anonīmi apstrādātu informāciju Likuma 2. panta 9. punkta nozīmē tikai tad, ja uzņēmējs, kurš izmanto personas informāciju, veic pasākumus, lai personas atkārtotu identifikāciju padarītu neatgriezenisku ikvienam, arī dzēšot apstrādes metodi un citu saistītu informāciju (proti, informāciju, kas attiecas uz minētajiem aprakstiem u. tml. un individuālajiem identifikācijas kodiem, kuri dzēsti no personas informācijas, kas izmantota anonīmi apstrādātas informācijas iegūšanai, un informāciju, kas attiecas uz atbilstoši Likuma 36. panta 1. punktam izmantoto apstrādes metodi (attiecas tikai uz tiem, kuri var atjaunot personas informāciju, izmantojot šādu saistīto informāciju)).

2. PIELIKUMS

Viņas Ekselencei Eiropas Komisijas tieslietu, patērētāju un dzimumu līdztiesības komisārei Verai Jourovas kundzei

Jūsu Ekselence!

Es atzinīgi vērtēju konstruktīvās sarunas starp Japānu un Eiropas Komisiju, kuru mērķis bija izveidot regulējumu personas datu savstarpējai nosūtīšanai starp Japānu un ES.

Pamatojoties uz Eiropas Komisijas lūgumu Japānas valdībai, es nosūtu šeit pievienoto dokumentu, kurā sniegts pārskats par Japānas tiesisko regulējumu attiecībā uz piekļuvi informācijai.

Šis dokuments attiecas uz daudzām Japānas valdības ministrijām un aģentūrām, un attiecībā uz dokumenta saturu attiecīgās ministrijas un aģentūras (Ministru kabineta sekretariāts, Valsts policijas aģentūra, Personas informācijas aizsardzības komisija, Iekšlietu un komunikācijas lietu ministrija, Tieslietu ministrija, Sabiedriskās drošības izlūkošanas aģentūra, Aizsardzības ministrija) ir atbildīgas par to attiecīgajā kompetencē esošajām dokumenta daļām. Atbilstošās ministrijas un aģentūras un attiecīgie to pārstāvju paraksti ir atrodami zemāk.

Personas informācijas aizsardzības komisija pieņem visus pieprasījumus saistībā ar šo dokumentu un koordinēs nepieciešamo atbilžu sniegšanu starp ministrijām un aģentūrām.

Ceru, ka šis dokuments būs noderīgs, pieņemot lēmumus Eiropas Komisijā.

Es augsti vērtēju Jūsu līdz šim sniegto ievērojamo ieguldījumu šajā lietā.

Ar cieņu,

Yoko Kamikawa,

tieslietu ministrs

Šo dokumentu ir sagatavojusi Tieslietu ministrija un turpmāk minētās iesaistītās ministrijas un aģentūras.

Koichi Hamano,

Ministru kabineta sekretariāta padomnieks

Schunichi Kuryu,

Valsts policijas aģentūras ģenerālkomisārs

Mari Sonoda,

Personas informācijas aizsardzības komisijas ģenerālsekretārs

Mitsuru Yasuda,

Iekšlietu un komunikācijas lietu ministrijas ministra vietnieks

Seimei Nakagawa,

Sabiedriskās drošības izlūkošanas aģentūras pārstāvis

Kenichi Takahashi,

aizsardzības ministra vietnieks administratīvajos jautājumos

2018. gada 14. septembris

Personas informācijas vākšana un izmantošana, ko Japānas publiskās iestādes veic krimināltiesību aizsardzības un valsts drošības nolūkos

Šajā dokumentā ir sniegts pārskats par to, kāds tiesiskais regulējums paredzēts, lai Japānas publiskās iestādes varētu vākt un izmantot personas (elektronisko) informāciju krimināltiesību aizsardzības un valsts drošības nolūkos (turpmāk – "valdības piekļuve"), jo īpaši attiecībā uz pieejamajiem juridiskajiem pamatiem, piemērojamiem nosacījumiem (ierobežojumiem) un aizsardzības pasākumiem, tostarp neatkarīgu pārraudzību un individuālās tiesiskās aizsardzības iespējām. Šis apliecinājums ir adresēts Eiropas Komisijai, lai paustu apņemšanos un nodrošinātu, ka valdības piekļuve personas informācijai, kas tiek nosūtīta no ES uz Japānu, aprobežosies tikai ar to, kas ir nepieciešams un samērīgs, tā tiks pakļauta neatkarīgai pārraudzībai un attiecīgās personas varēs saņemt tiesisko aizsardzību gadījumā, ja būs pārkāptas viņu pamattiesības uz privātumu un datu aizsardzību. Šis apliecinājums arī paredz izveidot jaunu tiesiskās aizsardzības mehānismu, ko pārvalda Personas informācijas aizsardzības komisija (*PPC*), lai izskatītu ES iedzīvotāju sūdzības par valdības piekļuvi viņu personas datiem, kas nosūtīti no ES uz Japānu.

I. **Vispārējie tiesību principi attiecībā uz valdības piekļuvi**

Valsts varas īstenošanas ietvaros valdībai, piekļūstot personas datiem, ir pilnībā jāievēro tiesību akti (likumības princips). Japānā personas informācija tiek aizsargāta gan privātajā sektorā, gan publiskajā sektorā, izmantojot daudzpakāpju mehānismu.

A. Konstitucionālā sistēma un tiesību atrunas princips

Saskaņā ar Konstitūcijas 13. pantu un judikatūru tiesības uz privātumu ir atzītas kā konstitucionālās tiesības. Šajā saistībā Augstākā tiesa ir nospriedusi, ka ir dabiski, ka privātpersonas nevēlas, lai citi zinātu attiecīgo personas informāciju bez pamatota iemesla, un ka šī paļāvība būtu jāaizsargā ([1]). Turpmāka aizsardzība ir paredzēta Konstitūcijas 21. panta 2. punktā, kas nodrošina sakaru slepenības ievērošanu, un Konstitūcijas 35. pantā, kas garantē tiesības, ka bez ordera nedrīkst veikt personas pārmeklēšanu un konfiskāciju, un tas nozīmē, ka personas informācijas, tostarp piekļuves, obligātai vākšanai vienmēr jābūt balstītai uz tiesas orderi. Šādu orderi var izdot tikai par jau izdarīta nozieguma izmeklēšanu. Tāpēc Japānas tiesiskajā regulējumā informācijas vākšana ar obligātiem līdzekļiem valsts drošības (nevis kriminālizmeklēšanas) nolūkos nav atļauta.

Turklāt saskaņā ar tiesību atrunas principu obligāta informācijas vākšana ir īpaši jāapstiprina ar likumu. Neobligātās/brīvprātīgās informācijas vākšanas gadījumā informāciju iegūst no avota, kam var brīvi piekļūt vai kas ir saņemts, pamatojoties uz brīvprātīgas izpaušanas pieprasījumu, t. i., lūgumu, ko fiziskai vai juridiskai personai, kuras rīcībā ir minētā informācija, nevar noteikt izpildīt kā pienākumu. Tomēr tas ir pieļaujams tikai tiktāl, ciktāl publiskā iestāde ir kompetenta veikt izmeklēšanu, ņemot vērā to, ka katra publiskā iestāde var darboties tikai savas administratīvās jurisdikcijas robežās, kas noteikta tiesību aktos (neatkarīgi no tā, vai tās darbības traucē personu tiesībām un brīvībām). Šis princips attiecas uz iestādes spēju vākt personas informāciju.

B. Īpaši noteikumi par personas informācijas aizsardzību

Likums par personas informācijas aizsardzību (*APPI*) un Likums par administratīvo struktūru rīcībā esošas personas informācijas aizsardzību (*APPIHAO*), kuru pamatā ir konstitucionāli noteikumi un ar kuriem tie ir izstrādāti vēl detalizētāki, garantē tiesības uz personas informāciju gan privātajā, gan valsts sektorā.

APPI 7. pantā ir noteikts, ka *PPC* izstrādā "Pamatpolitiku par personas informācijas aizsardzību" (pamatpolitika). Pamatpolitikā, ko pieņem ar Japānas Ministru kabineta kā Japānas valdības centrālās struktūras (premjerministra un valsts ministru) lēmumu, nosaka personas informācijas aizsardzības virzienu Japānā. Tādējādi *PPC* kā neatkarīga uzraudzības iestāde darbojas kā Japānas personas informācijas aizsardzības sistēmas "komandcentrs".

Ikreiz, kad administratīvās struktūras vāc personas informāciju un neatkarīgi no tā, vai tās to dara ar obligātiem līdzekļiem, principā ([2]) tām ir jāizpilda *APPIHAO* prasības. *APPIHAO* ir vispārēji tiesību akti, ko "administratīvās struktūras" (kā definēts *APPIHAO* 2. panta 1. punktā) piemēro "glabātai personas informācijai" ([3]). Tādējādi tā attiecas arī uz datu apstrādi krimināltiesību aizsardzības un valsts drošības jomā. Starp publiskajām iestādēm, kuras ir pilnvarotas īstenot

([1]) Augstākā tiesa, 2003. gada 12. septembra spriedums (2002 (Ju) Nr.1656).

([2]) Izņēmumus attiecībā uz *APPIHAO* 4. nodaļu sk. turpmāk 16. lpp.

([3]) *APPIHAO* 2. panta 5. punktā "saglabātā personas informācija" ir informācija, kuru administratīvas struktūras darbinieks ir sagatavojis vai ieguvis, pildot darba pienākumus, un kas attiecīgās administratīvajā struktūrā ir tās darbinieku rīcībā izmantošanai organizatoriskos nolūkos.

valdības piekļuvi, visas iestādes, izņemot prefektūras policiju, ir valsts pārvaldes iestādes, uz kurām attiecas "administratīvo struktūru" definīcija. Personas informācijas izmantošanu prefektūras policijā reglamentē prefektūras rīkojumi ([4]), kas paredz noteikumus par personas informācijas, tiesību un pienākumu aizsardzību, kuri ir līdzvērtīgi *APPIHAO*.

II. **Valdības piekļuve krimināltiesību aizsardzības nolūkos**

A. Juridiskie pamati un ierobežojumi

1. Personas informācijas vākšana piespiedu kārtā

a) Juridiskie pamati

Saskaņā ar Konstitūcijas 35. pantu visu personu tiesības uz sava mājokļa, personas un datu neaizskaramību pret ielaušanos, pārmeklēšanu un konfiskāciju netiek skartas, izņemot gadījumos, kad ir izdots tiesas orderis – ar "pienācīgu pamatojumu" un precīzi aprakstot pārmeklējamo vietu un konfiscējamos objektus. Attiecīgi publiskas iestādes kriminālizmeklēšanas ietvaros var vākt elektronisku informāciju vienīgi, pamatojoties uz orderi. Tas attiecas gan uz elektronisko ierakstu vākšanu, kuros ir (personas) informācija, gan uz reāllaikā veiktu sakaru pārtveršanu (t. s. noklausīšanos). Vienīgais izņēmums no šā noteikuma (kas tomēr nav būtisks gadījumā, ja personas informācija tiek elektroniski nosūtīta no ārzemēm) ir Kriminālprocesa kodeksa 220. panta 1. punkts ([5]), saskaņā ar kuru prokurors, viņa palīgs vai kriminālpolicijas darbinieks, arestējot aizdomās turēto/"nozieguma vietā pieķertu noziedzīgā nodarījuma izdarītāju", nepieciešamības gadījumā drīkst veikt pārmeklēšanu un konfiskāciju "uz vietas aresta brīdī".

Kriminālprocesa kodeksa 197. panta 1. punktā noteikts, ka piespiedu izmeklēšanas pasākumus "nepiemēro, ja vien šajā kodeksā nav noteikti īpaši noteikumi". Attiecībā uz elektroniskās informācijas vākšanu piespiedu kārtā atbilstošie juridiskie pamati šajā saistībā ir Kriminālprocesa kodeksa 218. pants (saskaņā ar kuru prokurors, viņa palīgs vai kriminālpolicijas darbinieks drīkst, ja tas nepieciešams nodarījuma izmeklēšanai, veikt pārmeklēšanu, konfiskāciju vai pārbaudi, pamatojoties uz tiesneša izdotu orderi) un Kriminālprocesa kodeksa 222-2. pants (saskaņā ar kuru piespiedu pasākumus elektronisko sakaru pārtveršanai bez jebkuras puses piekrišanas veic, pamatojoties uz citiem likumiem). Pēdējais noteikums atsaucas uz Likumu par noklausīšanos kriminālizmeklēšanas nolūkos (Noklausīšanās likumu), kura 3. panta 1. punktā noteikti nosacījumi, ar kādiem saistībā ar konkrētiem smagiem noziedzīgiem nodarījumiem var noklausīties sakarus, pamatojoties uz tiesneša izdotu noklausīšanās orderi ([6]).

Attiecībā uz policiju izmeklēšanas pilnvaras visos gadījumos ir prefektūras policijai, savukārt Valsts policijas aģentūra (*NPA*) neveic nekādas kriminālizmeklēšanas, pamatojoties uz Kriminālprocesa kodeksu.

b) Ierobežojumi

Elektroniskās informācijas vākšanu piespiedu kārtā ierobežo Konstitūcija un pilnvarojuma akti, kā tie interpretēti tiesu judikatūrā, kas it īpaši sniedz kritērijus, kuri tiesām jāpiemēro ordera izdošanas gadījumā. Turklāt arī *APPIHAO* ir noteikti vairāki ierobežojumi, kas piemērojami gan informācijas vākšanai, gan apstrādei (vietēja mēroga rīkojumos pamatā ir ietverti tie paši kritēriji attiecībā uz prefektūras policiju).

1. Ierobežojumi, kas izriet no Konstitūcijas un pilnvarojuma aktiem

Saskaņā ar Kriminālprocesa kodeksa 197. panta 1. punktu piespiedu pasākumus nepiemēro, ja vien šajā kodeksā nav noteikti īpaši noteikumi. Kriminālprocesa kodeksa 218. pants nosaka, ka konfiskāciju, pamatojoties uz tiesneša izdotu

([4]) Katrai prefektūrai ir pašai savs "prefektūras rīkojums", kas attiecas uz personas informācijas aizsardzību, ko veic prefektūras policija. Šiem prefektūras rīkojumiem nav tulkojumu angļu valodā.

([5]) Kriminālprocesa kodeksa 220. panta 1. punktā noteikts, ka gadījumos, kad prokurors, viņa palīgs vai kriminālpolicijas darbinieks arestē aizdomās turēto, viņš drīkst nepieciešamības gadījumā veikt šādus pasākumus: a) iekļūt citas personas mītnē utml., lai to pārmeklētu aizdomās turētā meklējumos; b) veikt pārmeklēšanu, konfiskāciju vai pārbaudi uz vietas aresta brīdī.

([6]) Konkrēti šis noteikums paredz, ka "prokurors vai tiesu izpildītājs gadījumos, kas ietilpst kādā no turpmāk minētajiem punktiem, ja rodas situācija, kad pastāv pietiekamas aizdomas par to, ka notiks sakari par turpmāku darbību, piem., pierādījumu slēpšanu utt., veikšanu, sagatavošanu, organizēšanu, attiecībā uz noziegumiem, kas minēti katrā konkrētajā punktā (turpmāk otrajā un trešajā punktā saukti "noziegumu virkne"), kā arī sakari par jautājumiem saistībā ar minēto noziegumu (turpmāk šeit saukti "sakari saistībā ar noziegumu"), un gadījumos, kad ir īpaši grūti identificēt likumpārkāpēju vai noskaidrot situāciju/nodarījuma detaļas jebkādiem citiem veidiem, pamatojoties un tiesneša izdotu noklausīšanās orderi attiecībā uz sakaru līdzekļiem, ko precīzi norāda ar tālruņa numuru un citiem numuriem/kodiem, kuri ļauj identificēt izejošā vai ienākošā zvana tālruni, un ko aizdomās turētais izmanto, pamatojoties uz līgumu ar telesakaru nodrošinātāju, utt. (izņemot tos, kurus var uzskatīt par tādiem, kas nerada aizdomas par to izmantošanu "sakaros saistībā ar noziegumu"), vai tiem, attiecībā uz kuriem ir pamats aizdomām par to izmantošanu "sakaros saistībā ar noziegumu", var veikt sakaru saistībā ar noziegumu, kuros izmantoti minētie sakaru līdzekļi, noklausīšanos."

orderi, var veikt tikai tad, "ja tas nepieciešams nodarījuma izmeklēšanai". Lai gan vispārējās tiesībās kritēriji nepieciešamības noteikšanai nav precizēti sīkāk, Augstākā tiesa ir lēmusi ([7]), ka tiesnesim, izvērtējot apstākļus, būtu jāveic vispārējs novērtējums, jo īpaši ņemot vērā šādus elementus:

a) nodarījums smagumu un veids, kā tas izdarīts;

b) materiālu, kas konfiscēti kā pierādījumi, vērtība un nozīmīgums;

c) varbūtība, ka konfiscējamie materiāli tiks slēpti vai iznīcināti;

d) konfiskācijas radīto neērtību apmērs;

e) citi saistīti apstākļi.

Ierobežojumi izriet arī no Konstitūcijas 35. panta, prasot norādīt "pienācīgu pamatojumu". Saskaņā ar "pienācīga pamatojuma" standartu orderus var izdot šādās situācijās: [1] ja ir nepieciešams veikt kriminālizmeklēšanu (sk. Augstākās tiesas 1969. gada 18. marta spriedumu (1968 (*Shi*)Nr.100), minēts iepriekš), [2] pastāv situācija, kurā aizdomās turētais (apsūdzētais) uzskatāms par personu, kas izdarījusi noziedzīgu nodarījumu (Kriminālprocesa kodeksa 156. panta 1. punkts) ([8])[3]. Orderis ķermeņa, lietu, mītnes vai citas vietas saistībā ar personu pārmeklēšanai attiecībā uz personu, kas nav apsūdzētais, būtu jāizdod tikai tad, ja pamatoti var pieņemt, ka konfiscējamie priekšmeti tiešām pastāv (Kriminālprocesa kodeksa 102. panta 2. punkts). Ja tiesnesis uzskata, ka dokumentārie pierādījumi, ko iesniegušas izmeklēšanas iestādes, nav pietiekams pamats turēt kādu aizdomās par noziedzīga nodarījuma izdarīšanu, tiesnesis noraida ordera pieprasījumu. Šajā sakarā būtu jāatzīmē, ka atbilstīgi Likumam par organizētās noziedzības nodarījumu sodīšanu un noziegumu rezultātā gūtu ienākumu kontroli "sagatavošanās darbības nolūkā veikt" plānotu noziedzīgu nodarījumu (piem., naudas līdzekļu sagatavošana teroristu uzbrukuma veikšanai) pašas par sevi ir noziedzīgs nodarījums un par tām var veikt izmeklēšanu piespiedu kārtā, pamatojoties uz orderi.

Visbeidzot, ja orderis attiecas uz ķermeņa, lietu, mītnes vai citas vietas saistībā ar personu pārmeklēšanu attiecībā uz personu, kas nav aizdomās turētais vai apsūdzētais, orderi izdod tikai tad, ja pamatoti var pieņemt, ka konfiscējamie priekšmeti tiešām pastāv (Kriminālprocesa kodeksa 102. panta 2. punkts un 222. panta 1. punkts).

It īpaši attiecībā uz sakaru pārtveršanu kriminālizmeklēšanas nolūkos, pamatojoties uz Noklausīšanās likumu, to var veikt tikai tad, ja ir izpildītas 3. panta 1. punktā noteiktās striktās prasības. Saskaņā ar minēto noteikumu, lai veiktu noklausīšanos, ir nepieciešams tiesas iepriekš izdots orderis, ko savukārt var izdot tikai nedaudzās situācijās ([9]).

2. Ierobežojumi, kas izriet no *APPIHAO*

Attiecībā uz to, kā administratīvas struktūras vāc ([10]) un turpmāk apstrādā (tai skaitā it īpaši saglabā, pārvalda un izmanto) personas informāciju, *APPIHAO* ir noteikti konkrēti šādi ierobežojumi:

a) saskaņā ar *APPIHAO* 3. panta 1. punktu administratīvas struktūras personas informāciju var saglabāt tikai tad, ja glabāšana ir nepieciešama to pienākumu pildīšanai, kuri ir to kompetencē un noteikti normatīvajos aktos. Informācijas saglabāšanas gadījumā tam var prasīt norādīt (iespējami precīzi) personas informācijas izmantošanas mērķi. Saskaņā ar *APPIHAO* 3. panta 2. un 3. punktu administratīvas struktūras personas informāciju saglabā tikai tajā apmērā, kāds nepieciešams norādīto izmantošanas mērķu sasniegšanai, un tās nemaina izmantošanas mērķi tā, ka tas pārsniegtu apmēru, ko var pamatoti uzskatīt par atbilstoši saistītu ar sākotnējo mērķi;

b) saskaņā ar *APPIHAO* 5. pantu administratīvas struktūras vadītājs cenšas nodrošināt, ka personas informāciju saglabā rūpīgi un aktualizētu tās izmantošanas mērķa sasniegšanai nepieciešamajos ietvaros;

c) *APPIHAO* 6. panta 1. punktā noteikts, ka administratīvas struktūras vadītājs veic visus nepieciešamos pasākumus, lai nepieļautu personas informācijas noplūdi, tās nozaudēšanu vai bojāšanu, kā arī atbild par saglabātās personas informācijas pienācīgu pārvaldību;

d) saskaņā ar *APPIHAO* 7. pantu neviens (tai skaitā bijušais) darbinieks neizpauž iegūto personas informāciju citai personai bez pamatota iemesla vai neizmanto šādu informāciju negodīgiem nolūkiem;

([7]) 1969. gada 18. marta spriedums (1968 (*Shi*)Nr. 100).
([8]) Kriminālprocesa noteikumu 156. panta 1. punkts. "Iesniedzot pieprasījumu, kas minēts iepriekšējā panta 1. punktā, prasītājs iesniedz materiālus, pamatojoties uz kuriem būtu uzskatāms, ka aizdomās turētais vai apsūdzētai ir izdarījis noziedzīgu nodarījumu."
([9]) Sk. 6. zemsvītras piezīmi.
([10]) *APPIHAO* 3. panta 1. un 2. punkts ierobežo apmēru personas informācijas saglabāšanai un tādējādi arī vākšanai.

e) turklāt *APPIHAO* 8. panta 1. punktā noteikts, ka administratīvas struktūras vadītājs, ja vien normatīvajos aktos nav noteikts citādi, neizmanto saglabāto personas informāciju un neizsniedz to citai personai mērķiem, kas nav konkrētie izmantošanas mērķi. Lai arī 8. panta 2. punktā ir paredzēti izņēmumi no šā noteikuma konkrētās situācijās, tie ir piemērojami tikai tad, ja šāda informācijas ārkārtas atklāšana nenodarīs "netaisnīgu" kaitējumu datu subjekta vai kādas trešās personas tiesībām un interesēm;

f) Saskaņā ar *APPIHAO* 9. pantu gadījumā, kad saglabātu personas informāciju sniedz citai personai, administratīvas struktūras vadītājs, ja nepieciešams, nosaka izmantošanas mērķa vai metodes ierobežojumus vai citus nepieciešamus ierobežojumus. Tas var arī saņēmējam pieprasīt veikt pasākumus, lai nepieļautu personas informācijas noplūdi un nodrošinātu informācijas pienācīgu pārvaldību;

g) *APPIHAO* 48. pantā ir noteikts, ka administratīvas struktūras vadītājs rūpīgi un ātri cenšas izskatīt visas sūdzības par personas informācijas apstrādi.

2. Personas informācijas vākšana, lūdzot brīvprātīgu sadarbību izmeklēšana brīvprātīgā kārtā)

a) Juridiskais pamats

Papildus tam, ka informāciju iegūst piespiedu kārtā, personas informāciju iegūst vai nu no brīvi pieejama avota, vai pamatojoties uz brīvprātīgu informācijas sniegšanu, ieskaitot gadījumus, kad to dara uzņēmumi, kuru rīcībā ir šāda informācija.

Attiecībā uz pēdējo aspektu Kriminālprocesa kodeksa 197. panta 2. punkts piešķir prokuratūrai un kriminālpolicijai pilnvaras veikt "rakstisku informācijas vākšanu par izmeklēšanas jautājumiem" (t. s. "pierādījumu vākšanas dokuments"). Saskaņā ar Kriminālprocesa kodeksu iztaujājamās personas tiek aicinātas ziņot izmeklēšanas iestādēm. Tomēr nav nekādu iespēju piespiest viņas ziņot, ja publiskās iestādes vai publiskās un/vai privātās organizācijas, kas saņem pieprasījumus, atsakās pakļauties. Ja tās neatbild uz pieprasījumiem, nevar piemērot nekādus krimināsodus vai citus sodus. Ja izmeklēšanas iestādes uzskata, ka pieprasītā informācija ir obligāti nepieciešama, tām šī informācija būs jāiegūst, veicot pārmeklēšanu un konfiskāciju, pamatojoties uz tiesas orderi.

Ņemot vērā to, ka uzlabojas personu informētība par viņu privātuma tiesībām, kā arī pieaugošo darba slodzi, ko rada šādi pieprasījumi, uzņēmēji arvien piesardzīgāk atbild uz šādiem pieprasījumiem ([11]). Pieņemot lēmumu par to, sadarboties vai ne, uzņēmēji it īpaši ņem vērā pieprasītās informācijas būtību, attiecības ar personu, kuras informāciju tas skar, riskus savai reputācijai, tiesāšanās riskus, utt.

b) *Ierobežojumi*

Tāpat kā elektroniskās informācijas vākšanu piespiedu kārtā, arī izmeklēšanu brīvprātīgā kārtā ierobežo Konstitūcija, kā tā interpretēta tiesu judikatūrā, un pilnvarojuma akti. Turklāt uzņēmējiem ar likumu nav ļauts konkrētās situācijās izpaust informāciju. Visbeidzot, *APPIHAO* ir noteikti vairāki ierobežojumi, kas piemērojami gan informācijas vākšanai, gan apstrādei (vietēja mēroga rīkojumos pamatā ir ietverti tie paši kritēriji attiecībā uz prefektūras policiju).

1. Ierobežojumi, kas izriet no Konstitūcijas un pilnvarojuma aktiem

Ņemot vērā Konstitūcijas 13. pantu, Augstāka tiesa divos savos lēmumos – 1969. gada 24. decembrī (1965 (A) Nr.1187) un 2008. gada 15. aprīlī (2007 (A) Nr.839) – ir noteikusi ierobežojumus attiecībā uz izmeklēšanu brīvprātīgā kārtā, ko veic izmeklēšanas iestādes. Lai arī šie lēmumi attiecās uz lietām, kurās personas informāciju (attēlu veidā) vāca, izmantojot fotogrāfijas/filmas, konstatējumi ir svarīgi izmeklēšanai, kas veikta brīvprātīgā (ne piespiedu) kārtā, vispārēji iejaucoties kādas personas privātumā. Tādēļ tos piemēro un tie ir jāievēro attiecībā uz personas informācijas vākšanu izmeklēšanā, kas veikta brīvprātīgā kārtā, ņemot vērā katras lietas konkrētos apstākļus.

Saskaņā ar šiem lēmumiem brīvprātīgā kārtā veiktas izmeklēšanas likumīgums ir atkarīgs no tā, vai ir izpildīti trīs kritēriji, proti:

— "aizdomas par noziedzīgu nodarījumu" (t. i., jābūt izvērtējumam par to, vai ir izdarīts noziedzīgs nodarījums),

— "izmeklēšanas nepieciešamība" (t. i., jābūt izvērtējumam par to, vai pieprasījums nepārsniedz to, kas nepieciešams izmeklēšanas mērķim) un

([11]) Sk. arī paziņojumu, kuru Valsts policijas aģentūra izdevusi 1999. gada 7. decembrī (zemāk 9. punktā) un kurā arī apliecināts iepriekš minētais.

— "metožu atbilstība" (t. i., jābūt izvērtējumam par to, vai brīvprātīgā kārtā veikta izmeklēšana ir "atbilstīga" vai pamatota, lai sasniegtu izmeklēšanas mērķi) ([12]).

Kopumā, ņemot vērā iepriekš minētos trīs kritērijus, brīvprātīgā kārtā veiktas izmeklēšanas likumīgums tiek vērtēts no aspekta, vai to var uzskatīt par pamatotu saskaņā ar sabiedrībā pieņemtajām paražām.

Prasība, ka izmeklēšanai jābūt "nepieciešamai" tieši izriet arī no Kriminālprocesa kodeksa 197. panta, un tā ir apstiprināta instrukcijās, ko prefektūras policijai attiecībā uz "pierādījumu vākšanas dokumenta" izmantošanu izdevusi Valsts policijas aģentūra (*NPA*). *NPA* 1999. gada 7. decembra paziņojumā noteikta virkne procesuālu ierobežojumu, tai skaitā prasība izmantot "pierādījumu vākšanas dokumentus" tikai tad, ja tas nepieciešams izmeklēšanas nolūkiem. Turklāt Kriminālprocesa kodeksa 197. panta 1. punkts attiecas vienīgi uz krimināllizmeklēšanām, un tādēļ to var piemērot tikai gadījumos, kad pastāv konkrētas aizdomas par jau izdarītu noziedzīgu nodarījumu. Toties šis juridiskais pamats nav pieejams personas informācijas vākšanai un izmantošanai situācijās, kad tiesību akta pārkāpums vēl nav noticis.

2. Ierobežojumi attiecībā uz konkrētiem uzņēmējiem

Konkrētās jomās ir piemērojami papildu ierobežojumi, pamatojoties uz citos tiesību aktos noteikto aizsardzību.

Pirmkārt, izmeklēšanas iestādēm, kā arī telesakaru operatoriem, kuru rīcībā ir personas informācija, ir pienākums ievērot sakaru konfidencialitāti, ko garantē Konstitūcijas 21. panta 2. punkts ([13]). Turklāt arī telesakaru operatoriem ir tas pats pienākums saskaņā ar Telesakaru darījumdarbības likuma 4. pantu ([14]). Saskaņā ar "Pamatnostādnēm par personas informācijas aizsardzību telesakaru darījumdarbībā", ko, pamatojoties uz Konstitūciju un Telesakaru darījumdarbības likumu, izdevusi Iekšlietu un komunikācijas lietu ministrija (*MIC*), gadījumos, kad tiek skarta sakaru konfidencialitāte, telesakaru operatoriem nav jāsniedz personas informācija attiecībā uz trešo personu sakaru konfidencialitāti, izņemot gadījumus, kad operatori ir saņēmuši personas piekrišanu vai var paļauties uz vienu no "pamatotajiem iemesliem", kas ļauj atkāpties no Sodu kodeksa. Tas attiecas uz "pamatotām darbībām" (Sodu kodeksa 35. pants), "pašaizsardzību" (Sodu kodeksa 36. pants) un "tiešu briesmu novēršanu" (Sodu kodeksa 37. pants). "Pamatotas darbības" saskaņā ar Sodu kodeksu ir tikai tās telesakaru operatora veiktas darbības, kuras atbilst valsts noteiktajiem pasākumiem piespiedu kārtā, un tas neietver brīvprātīgā kārtā veiktu izmeklēšanu. Tādēļ, ja izmeklēšanas iestādes pieprasa personas informāciju, pamatojoties uz "pierādījumu vākšanas dokumentu" (Kriminālprocesa kodeksa 197. panta 2. punkts), telesakaru operatoram ir aizliegts sniegt datus.

Otrkārt, uzņēmējiem ir pienākums noraidīt pieprasījumus brīvprātīgi sadarboties, ja tiesību akti aizliedz viņiem atklāt personas informāciju. Kā piemēru var minēt gadījumu, kad uzņēmējam ir pienākums ievērot informācijas konfidencialitāti, piem., saskaņā ar Sodu kodeksa 134. pantu ([15]).

3. Ierobežojumi, pamatojoties uz *APPIHAO*

Attiecībā uz to, kā administratīvas struktūras vāc un turpmāk apstrādā personas informāciju, *APPIHAO* ir noteikti ierobežojumi, kā izklāstīts iepriekš II nodaļas A daļas 1. punkta b) apakšpunkta 2. punktā. Līdzvērtīgi ierobežojumi izriet no prefektūras rīkojumiem, ko piemēro prefektūras policijai.

B. Pārraudzība

1. Tiesas pārraudzība

Lai vāktu personas informāciju piespiedu kārtā, ir nepieciešams orderis ([16]), un tādējādi tās nepieciešamību vispirms pārbauda tiesnesis. Gadījumā, ja izmeklēšana ir veikta pretlikumīgi, tiesnesis var izslēgt šādus pierādījumus no krimināllietas turpmākās iztiesāšanas tiesā. Ja izmeklēšana ir veikta pretlikumīgi, persona var pieprasīt šādu pierādījumu izslēgšanu no viņas lietas iztiesāšanas tiesā.

([12]) Vērtējot "metožu atbilstību", nodarījuma smagums un rīcības steidzamība ir būtiski faktori.

([13]) Konstitūcijas 21. panta 2. punktā ir noteikts: "Netiek piemērota cenzūra un netiek pārkāpta jebkādu sakaru konfidencialitāte."

([14]) Telesakaru darījumdarbības likuma 4. pants: "1. Telesakaru operators nedrīkst pārkāpt apstrādāto sakaru konfidencialitāti. 2. Ikviena telesakaru darījumdarbībā iesaistīta persona neatklāj noslēpumus, kas tai kļuvuši zināmi, pildot tās telesakaru operatora pienākumus sakaru nodrošināšanai. Tas pats noteikums ir spēkā, kad operators ir beidzis pildīt savus pienākumus."

([15]) Sodu kodeksa 134. pantā ir noteikts: "1. Ja ārsts, farmaceits, zāļu izplatītājs, vecmāte, prokurors, advokāts, notārs vai jebkura cita persona, kas ir strādājusi kādā no minētajām profesijām, bez pamatota iemesla izpauž citas personas konfidenciālu informāciju, kura ir nonākusi viņas rīcībā minēto profesionālo pienākumu pildīšanas laikā, par to piemēro brīvības atņemšanas sodu ar piespiedu darbu uz laiku līdz sešiem mēnešiem vai naudassodu līdz 100 000 jenām. 2. Tas pats attiecas uz gadījumu, ja persona, kura pildīja vai pilda reliģiozas organizācijas garīgā personāla pienākumus, bez pamatota iemesla izpauž citas personas konfidenciālu informāciju, kas ir nonākusi viņas rīcībā minēto garīgā personāla pienākumu pildīšanas laikā."

([16]) Attiecībā uz izņēmumu no šā noteikuma sk. 5. zemsvītras piezīmi.

2. Pārraudzība, pamatojoties uz *APPIHAO*

Japānā ministram vai katras ministrijas vai aģentūras vadītājam ir pārraudzības un izpildes pilnvaras, pamatojoties uz *APPIHAO*, savukārt Iekšlietu un komunikācijas lietu ministrs var veikt izmeklēšanu par to, kā visas pārējās ministrijas īsteno *APPIHAO*.

Ja Iekšlietu un komunikācijas lietu ministrs – piem., pamatojoties uz izmeklēšanu par *APPIHAO* ([17]) īstenošanas statusu, uz sūdzību izskatīšanu vai uz pieprasījumiem, kas iesniegti kādam no vispārējās informācijas centriem – atzīst, ka tas ir nepieciešams *APPIHAO* mērķu sasniegšanai, viņš var pieprasīt, lai administratīvās struktūras vadītājs iesniedz materiālus un paskaidrojumus par personas informācijas apstrādi konkrētajā administratīvajā struktūrā, pamatojoties uz *APPIHAO* 50. pantu. Ministrs, ja viņš to uzskata par nepieciešamu šā akta mērķa sasniegšanai, var administratīvās struktūras vadītājam sniegt savu atzinumu par personas informācijas vākšanu administratīvajā struktūrā. Turklāt ministrs var, piemēram, pieprasīt pasākumu pārskatīšanu, izmantojot kādu no darbībām, ko viņš var veikt saskaņā ar likuma 50. un 51. pantu, ja pastāv aizdomas, ka likums ticis pārkāpts vai ir veiktas neatbilstošas darbības. Tas palīdz nodrošināt *APPIHAO* vienotu piemērošanu un ievērošanu.

3. Pārraudzība, ko sabiedriskās drošības komisijas īsteno pār policiju

Attiecībā uz policijas pārvaldi, *NPA* ir Valsts sabiedriskās drošības komisijas pārraudzībā, savukārt prefektūras policija atrodas vienas no Prefektūras sabiedrības drošības komisijas pārraudzībā, kas izveidota katrā prefektūrā. Katra no šīm pārraudzības struktūrām nodrošina demokrātisku pārvaldību un policijas vadības politisko neitralitāti.

Valsts sabiedriskās drošības komisija ir atbildīga par jautājumiem, kas ir tās kompetencē saskaņā ar Policijas likumu un citiem likumiem. Tas ietver *NPA* ģenerālkomisāra un vietējo augstākā ranga policijas darbinieku iecelšanu, kā arī visaptverošu rīcībpolitiku izstrādi, kurās noteikti galvenie virzieni vai pasākumi attiecībā uz *NPA* īstenoto pārvaldību.

Prefektūras sabiedriskās drošības komisiju sastāvā ir locekļi, kas pārstāv attiecīgo prefektūru iedzīvotājus, pamatojoties uz Policijas likumu, un tās pārvalda prefektūras policiju kā neatkarīga padomju sistēma. Pamatojoties uz Policijas likuma 39. pantu, locekļus ieceļ prefektūras gubernators ar prefektūras asamblejas piekrišanu. Viņu pilnvaru termiņš ir trīs gadi, un viņus no amata var atbrīvot tikai konkrētu, likumā noteiktu iemeslu dēļ (piemēram, nespēja pildīt pienākumus, pienākumu nepildīšana, amatpārkāpums utt.), tādējādi tiek nodrošināta viņu neatkarība (sk. Policijas likuma 40. un 41. pantu). Turklāt nolūkā garantēt viņu politisko neitralitāti, Policijas likuma 42. pants aizliedz komisijas loceklim vienlaicīgi darboties kādā likumdevējā struktūrā, uzņemties izpildfunkcijas kādā politiskā partijā vai jebkādā citā politiskā organizācijā, vai aktīvi iesaistīties politiskās kustībās. Lai arī katra komisija atrodas attiecīgā prefektūras gubernatora jurisdikcijā, viņam nav nekādu pilnvaru izdot norādījumus attiecībā uz komisijas pienākumu pildīšanu.

Saskaņā ar 38. panta 3. punktu saistībā ar Policijas likuma 2. pantu un 36. panta 2. punktu Prefektūras sabiedriskās drošības komisijas ir atbildīgas par "personas tiesību un brīvības aizsardzību". Šim nolūkam tās no prefektūras policijas vadītājiem saņem ziņojumus par darbībām to kompetencē, tai skaitā regulārās sapulcēs, kas notiek trīs vai četras reizes mēnesī. Komisija sniedz norādījumu par šiem jautājumiem, izstrādājot visaptverošas rīcībpolitikas.

Turklāt, īstenojot savas pārraudzības funkcijas, Prefektūras sabiedriskās drošības komisijas konkrētos gadījumos var izdot norādījumus prefektūras policijai, kad komisijas uzskata to par nepieciešamu saistībā ar prefektūras policijas darbību vai tās darbinieku amatpārkāpumu pārbaudi. Tāpat komisijas var, ja tās uzskata to par nepieciešamu, izraudzīties vienu komisijas locekli, kurš izskata to, kā tiek īstenoti izdotie norādījumi (Policijas likuma 43-2. pants).

([17]) Lai nodrošinātu pārredzamību un sekmētu *MIC* pārraudzības īstenošanu, administratīvās struktūras vadītājam saskaņā ar *APPIHAO* 11. pantu ir pienākums reģistrēt katru elementu, kas noteikts *APPIHAO* 10. panta 1. punktā, piemēram, tās administratīvās struktūras nosaukumu, kura glabās datni, datnes izmantošanas mērķi, personas informācijas vākšanas metodi utt. (t. s. "personas informācijas datņu reģistrs"). Tomēr attiecībā uz personas informācijas datnēm, uz kurām attiecas *APPIHAO* 10. panta 1. punkts, piemēram, datnēm, kuras ir sagatavotas vai iegūtas kā daļa no kriminālizmeklēsanas vai ir saistītas ar valsts drošībai būtiskiem jautājumiem, pastāv atbrīvojums no pienākuma ziņot *MIC* un iekļaut tās publiskajā reģistrā. Tomēr saskaņā ar Publisko reģistru un arhīvu pārvaldības likuma 7. pantu administratīvās struktūras vadītājam vienmēr ir pienākums reģistrēt administratīvo dokumentu klasifikāciju, nosaukumu, glabāšanas laiku un vietu utt. ("administratīvo dokumentu datņu pārvaldības reģistrs"). Abu reģistru satura rādītāju informācija tiek publiskota internetā un ļauj personām pārbaudīt, kāda veida personas informācija ir ietverta datnē un kura administratīvā struktūra glabā šo informāciju.

4. Pārraudzība, ko veic Parlaments

Parlaments var veikt izmeklēšanu saistībā ar publisko iestāžu darbībām un šim nolūkam pieprasīt dokumentu un liecinieku liecību sagatavošanu (Konstitūcijas 62. pants). Šajā sakarā Parlamenta kompetentā komiteja var pārbaudīt to, cik atbilstīgas ir policijas veiktās informācijas vākšanas darbības.

Šīs pilnvaras ir plašāk izklāstītas Parlamenta likumā. Saskaņā ar tā 104. pantu Parlaments var pieprasīt Ministru kabinetam un publiskām iestādēm sagatavot ziņojumus un dokumentāciju, kas nepieciešama parlamentārās izmeklēšanas veikšanai. Turklāt Parlamenta locekļi saskaņā ar Parlamenta likuma 74. pantu var iesniegt "rakstiskus pieprasījumus". Šādi pieprasījumi ir jāapstiprina palātas vadītājam, un principā Ministru kabinetam ir jāsniedz rakstiska atbilde septiņu dienu laikā (ja nav iespējams sniegt atbildi minētajā laikposmā, tam jābūt pamatotam iemeslam un ir jānosaka jauns termiņš, Parlamenta likuma 75. pants). Agrāk Parlamenta rakstiskie pieprasījumi attiecās arī uz to, kā administrācija apstrādā personas informāciju ([18]).

C. Individuāla tiesiskā aizsardzība

Saskaņā ar Japānas Konstitūcijas 32. pantu nevienai personai nevar liegt piekļuvi tiesai. Turklāt Konstitūcijas 17. pants garantē katras personas tiesības iesūdzēt valsti vai publisku iestādi nolūkā izmantot tiesiskās aizsardzības līdzekļus (kā noteikts tiesību aktos) gadījumos, kad personai ir nodarīts kaitējums valsts amatpersonas prettiesiskas darbības dēļ.

1. Tiesiskās aizsardzības līdzekļi pret informācijas vākšanu piespiedu kārtā, pamatojoties uz orderi (Kriminālprocesa kodeksa 430. pants)

Saskaņā ar Kriminālprocesa kodeksa 430. panta 2. punktu persona, kas nav apmierināta ar pasākumiem, kurus policija, pamatojoties uz orderi, ir veikusi saistībā ar priekšmetu konfiskāciju (tai skaitā, ja priekšmeti ietver personas informāciju), var kompetentajai tiesai iesniegt pieprasījumu (t. s. "kvazisūdzību"), prasot šādu pasākumu "atcelšanu vai grozīšanu".

Persona var šādi apstrīdēt pasākumus, negaidot lietas pabeigšanu. Ja tiesa atzīst, ka konfiskācija nebija nepieciešama vai ka pastāv citi iemesli uzskatīt, ka konfiskācija bijusi pretlikumīga, tā var likt šādu pasākumu atcelt vai grozīt.

2. Tiesiskās aizsardzības līdzekļi saskaņā ar Civilprocesa kodeksu un Valsts tiesiskās aizsardzības līdzekļu likumu

Ja persona uzskata, ka ir pārkāptas tās tiesības uz privātumu saskaņā ar Konstitūcijas 13. pantu, persona var celt civilprasību, prasot kriminālizmeklēšanas ietvaros savāktās personas informācijas dzēšanu.

Tāpat persona var celt prasību par kaitējuma atlīdzināšanu, pamatojoties uz Valsts tiesiskās aizsardzības līdzekļu likumu apvienojumā ar Civilprocesa kodeksa attiecīgajiem pantiem, ja persona uzskata, ka viņas tiesības uz privātumu ir pārkāptas un viņai nodarīts kaitējums viņas personas informācijas vākšanas vai viņas novērošanas rezultātā ([19]). Ņemot vērā to, ka "kaitējums", kuru var prasīt atlīdzināt, nav ierobežots ar īpašumam nodarītu kaitējumu (Civilkodeksa 710. pants), tas var ietvert arī "garīgas ciešanas". Atlīdzības par šādu morālu kaitējumu apmēru izvērtēs tiesnesis, pamatojoties uz "brīvu izvērtējumu, ņemot vērā katras lietas dažādos apstākļus" ([20]).

Valsts tiesiskās aizsardzības līdzekļu likuma 1. panta 1. punktā ir noteiktas tiesības uz kompensāciju, ja i) valsts amatpersona, kura īsteno valsts vai publiskas iestādes varu, ii) savu pienākumu izpildē ir iii) tīši vai nolaidības pēc iv) nelikumīgi v) nodarījusi kaitējumu citai personai.

Personai ir jāsniedz prasība tiesā saskaņā ar Civilprocesa kodeksu. Saskaņā ar piemērojamajiem noteikumiem personai tas jādara tiesā, kuras jurisdikcijā atrodas nodarījuma izdarīšanas vieta.

([18]) Sk., piemēram Padomnieku palātas 2009. gada 27. marta rakstisko pieprasījumu Nr. 92. par tās informācijas apstrādi, kas savākta kriminālizmeklēšanas ietvaros, tai skaitā policijas un prokuratūras pieļautiem konfidencialitātes pārkāpumiem.

([19]) Šādas darbības piemērs ir "Lieta par Aizsardzības aģentūras sarakstu" (*Niigata* rajona tiesa, 2006. gada 11. maija lēmums (2002(Wa) Nr.514)). Šajā gadījumā Aizsardzības aģentūras ierēdnis sagatavoja, glabāja un izplatīja to personu sarakstu, kuras bija iesniegušas pieprasījumus izsniegt Aizsardzības aģentūras administratīvos dokumentus. Minētajā sarakstā bija ietverts prasītāja personas informācijas apraksts. Uzstājot uz to, ka viņa privātums, tiesības zināt utml. ir tikušas pārkāptas, prasītājs pieprasīja atbildētājam maksāt kompensāciju par nodarīto kaitējumu saskaņā ar Valsts tiesiskās aizsardzības līdzekļu likuma 1. panta 1. punktu. Tiesa šo prasību daļēji apmierināja, nosakot prasītajam daļēju kompensāciju.

([20]) Augstākā tiesa, 1910. gada 5. aprīļa lēmums (1910(O) Nr.71).

3. Individuāla tiesiskā aizsardzība pret policijas pretlikumīgi/nepienācīgi veiktu izmeklēšanu: sūdzība prefektūras sabiedriskās drošības komisijai (Policijas likuma 79. pants)

Saskaņā ar Policijas likuma 79. pantu ([21]) un kā turpmāk paskaidrots *NPA* vadītāja norādījumos, kas adresēti prefektūras policijai un Prefektūras sabiedriskās drošības komisijām ([22]), personas kompetentajā Prefektūras sabiedriskās drošības komisijā var iesniegt rakstisku sūdzību ([23]) par jebkādu pretlikumīgu vai kļūdainu policijas darbinieka rīcību, tam pildot viņa pienākumus; tas ietver pienākumus attiecībā uz personas informācijas vākšanu un izmantošanu. Komisija "godprātīgi" izskata šādas sūdzības saskaņā ar tiesību aktiem un vietējiem rīkojumiem un rakstiski informē sūdzības iesniedzēju par izmeklēšanas rezultātiem.

Pamatojoties uz savām pārraudzības pilnvarām saskaņā ar Policijas likuma 38. panta 3. punktu, Prefektūras sabiedriskās drošības komisija izdod norādījumus prefektūras policijai izmeklēt faktus, veikt atbilstošus pasākumus, pamatojoties uz pārbaudes rezultātu, un ziņot par rezultātiem komisijai. Ja komisija uzskata par nepieciešamu, tā var arī izdot norādījumus par sūdzības izskatīšanu, piemēram, ja tā uzskata, ka policija izmeklēšanu ir veikusi nepietiekami. Šī īstenošana ir aprakstīta *NPA* paziņojumā, kas adresēts prefektūras policijas vadītajiem.

Sūdzības iesniedzēja rakstiski informē izmeklēšanas rezultātiem, ņemot vērā arī policijas ziņojumus par izmeklēšanu un pēc komisijas pieprasījuma veiktos pasākumus.

4. Individuāla tiesiskā aizsardzība saskaņā ar *APPIHAO* un Kriminālprocesa kodeksu

a) APPIHAO

Saskaņā ar *APPIHAO* 48. pantu administratīvajām struktūrām ir jācenšas pienācīgi un nekavējoties apstrādāt visas sūdzības, kuras attiecas uz personas informācijas apstrādi. Kā rīku konsolidētas informācijas sniegšanai personām (piem., par īstenojamajām tiesībām uz informācijas izpaušanu, labošanu vai dzēšanu saskaņā ar *APPIHAO*) un kontaktpunktu pieprasījumu iesniegšanai *MIC*, pamatojoties uz *APPIHAO* 47. panta 2. punktu, katrā prefektūrā ir izveidojusi vispārējās informācijas centrus informācijas sniegšanai / personas informācijas aizsardzībai. Pieprasījumus var iesniegt arī nerezidenti. Piemēram, *FY*2017 periodā (no 2017. gada aprīlim līdz 2018. gada martam) kopējais gadījumu skaits, kad vispārējās informācijas centri sniedza atbildes uz pieprasījumiem utml., bija 5186.

APPIHAO 12. un 27. pants piešķir personām tiesības pieprasīt saglabātas personas informācijas atklāšanu un labošanu. Turklāt saskaņā ar *APPIHAO* 36. pantu personas var pieprasīt to saglabātās personas informācijas izmantošanas pārtraukšanu vai informācijas dzēšanu gadījumos, kad administratīvā struktūra saglabāto personas informāciju nav ieguvusi likumīgi vai pretlikumīgi turpina glabāt vai izmantot šādu informāciju.

Tomēr attiecībā uz personas informāciju, kas savākta (vai nu pamatojoties uz orderi, vai izmantojot "pierādījumu vākšanas dokumentus") un saglabāta kriminālizmeklēšanas nolūkos ([24]), jāņem vērā, ka šāda informācija principā ietilpst kategorijā "personas informācija, kura ierakstīta dokumentos saistībā ar tiesvedību un konfiscētiem priekšmetiem". Tādējādi šāda personas informācija neietilpst individuālo tiesību piemērošanas jomā, kas noteikta *APPIHAO* 4. nodaļā saskaņā ar Kriminālprocesa kodeksa 53-2. pantu ([25]). Tā vietā uz šādas personas informācijas apstrādi un personas tiesībām tai

([21]) Sk. Policijas likuma 79. pantu (izraksts):
1. Ja personai ir sūdzība par to, kā kāds prefektūras policijas darbinieks pilda savus pienākumus, viņa var iesniegt rakstisku sūdzību Prefektūras sabiedriskās drošības komisijai, izmantojot Rīkojumā par Prefektūras sabiedriskās drošības komisiju noteikto procedūru.
2. Prefektūras sabiedriskās drošības komisija, kas saņēmusi iepriekšējā punktā minēto sūdzību, to godprātīgi izskata saskaņā ar tiesību aktiem un vietējiem rīkojumiem un rakstiski informē sūdzības iesniedzēju par rezultātiem, izņemot šādos gadījumos:
   1) sūdzību var atzīt par tādu, kas celta ar mērķi traucēt prefektūras policijas pienākumi likumīgai izpildei;
   2) nav zināma sūdzības iesniedzēja faktiskā dzīvesvieta;
   3) sūdzību var atzīt par tādu, kas celta kopā ar citiem sūdzības iesniedzējiem, un citi sūdzības iesniedzēji jau ir tikuši informēti par kopīgās sūdzības izskatīšanas rezultātu.

([22]) *NPA* 2001. gada 13. aprīļa Paziņojums par to sūdzību pienācīgu izskatīšanu, kas iesniegtas par policijas darbinieku rīcību, pildot viņu pienākumus, un 1. pielikums "Policijas likuma 79. panta interpretācijas/īstenošanas standarti".

([23]) Saskaņā ar *NPA* paziņojumu (sk. iepriekšējo zemsvītras piezīmi) personām, kurām ir grūtības formulēt rakstisku sūdzību, pienākas palīdzība. Tas jo īpaši ietver ārvalstniekus.

([24]) No otras puses, tie būtu dokumenti, kas netiek klasificēti kā "dokumenti saistībā ar tiesvedību", jo tie paši par sevi nav informācija, kura, pamatojoties uz orderi vai rakstiskiem pieprasījumiem, ir iegūta par izmeklēšanas jautājumiem, bet informācija ir izveidota uz šādu dokumentu pamata. Tas būtu gadījums, kad uz privātu informāciju neattiektos *APPIHAO* 45. panta 1. punkts un tādējādi šāda informācija netiktu izslēgta no *APPIHAO* 2. nodaļas piemērošanas jomas.

([25]) Kriminālprocesa kodeksa 53-2. panta 2. punktā ir noteikts, ka *APPIHAO* 4. nodaļas noteikumus nepiemēro personas informācijai, kura ierakstīta dokumentos saistībā ar tiesvedību un konfiscētiem priekšmetiem.

piekļūt un prasīt tās labošanu attiecas īpaši noteikumi saskaņā ar Kriminālprocesa kodeksu un Likumu par galīgo krimināllietu uzskaiti (sk. zemāk) ([26]). Šo izņēmumu pamato dažādi faktori, piemēram, iesaistīto personu privātuma aizsardzība, izmeklēšanas konfidencialitāte un kriminālās tiesas atbilstoša darbība. Tomēr joprojām ir piemērojami arī *APPIHAO* 2. nodaļas noteikumi, kas reglamentē šādas informācijas apstrādes principus.

b) Kriminālprocesa kodekss

Saskaņā ar Kriminālprocesa kodeksu iespējas piekļūt personas informācijai, kas savākta krimināllizmeklēšanas nolūkos, ir atkarīga gan no procedūras posma, gan no personas statusa izmeklēšanā (aizdomās turētais, apsūdzētais, cietušas, utt.).

Kā izņēmums no Kriminālprocesa kodeksa 47. panta noteikuma, ka dokumentus saistībā ar tiesvedību nevar publiskot pirms tiesvedības sākšanas (jo tas varētu aizskart iesaistīto personu godu un/vai privātumu un traucēt izmeklēšanai/tiesai), jāmin tas, ka noziedzīgā nodarījumā cietušajam principā ir atļauts iepazīties ar šādu informāciju tādā apmērā, kāds tiek uzskatīts par pamatotu, ņemot vērā Kriminālprocesa kodeksa 47. panta noteikuma mērķi ([27]).

Attiecībā uz aizdomās turētajiem – viņi par apstākli, ka attiecībā uz viņiem notiek krimināllizmeklēšana, parasti uzzina nopratināšanas laikā, ko veic kriminālpolicija vai prokurors. Ja prokurors pēc tam nolemj nesākt kriminālvajāšanu, viņš par šo faktu nevilcinoties informē aizdomās turēto pēc tā pieprasījuma (Kriminālprocesa kodeksa 259. pants).

Turklāt pēc kriminālvajāšanas uzsākšanas prokurors apsūdzētajam vai viņa aizstāvim dod iespēju iepriekš iepazīties ar pierādījumiem, pirms lūdz to pārbaudi tiesā (Kriminālprocesa kodeksa 299. pants). Tas ļauj apsūdzētajam pārbaudīt viņa personas informācijai, kas savākta krimināllizmeklēšanas ietvaros.

Visbeidzot, personas informācijas, kas savākta krimināllizmeklēšanas ietvaros, aizsardzība attiecībā uz jebkuru personu – aizdomās turēto, apsūdzēto vai jebkuru citu personu (piem., noziedzīgā nodarījumā cietušo) – ir garantēta ar pienākumu ievērot konfidencialitāti (Likuma par valsts civildienestu 100. pants) un paredzētiem sodiem gadījumā, ja tiks nopludināta konfidenciāla informācija, ko apstrādā, pildot civildienesta pienākumus (Likuma par valsts civildienestu 109. panta xii) punkts).

5. Individuāla tiesiskā aizsardzība pret publisko iestāžu pretlikumīgi/nepienācīgi veiktu izmeklēšanu: sūdzība *PPC*

Saskaņā ar *APPI* 6. pantu valdība sadarbībā ar trešo valstu valdībām veic nepieciešamās darbības, lai izveidotu starptautiski saskaņotu sistēmu attiecībā uz personas informāciju, veicinot sadarbību ar starptautiskām organizācijām un citiem starptautiskiem satvariem. Pamatojoties uz šo noteikumu, Pamatpolitikā personas informācijas aizsardzībai (kas pieņemta ar Ministru kabineta lēmumu) *PPC* kā kompetentajai iestādei attiecībā uz *APPI* vispārējo pārvaldību tiek deleģētas pilnvaras veikt nepieciešamos pasākumus, lai mazinātu sistēmu un darbību atšķirības starp Japānu un attiecīgo ārvalsti nolūkā nodrošināt no šādas valsts saņemtas personas informācijas pienācīgu izmantošanu.

Turklāt, kā noteikts *APPI* 61. panta i) un ii) punktā, *PPC* ir uzdots pienākums formulēt un veicināt pamatpolitiku, kā arī būt par starpnieku gadījumos, kad par uzņēmēju ir iesniegtas sūdzības. Visbeidzot, administratīvajām struktūrām ir jāuztur cieša saziņa un savstarpēja sadarbība (*APPI* 80. pants).

Pamatojoties uz šiem noteikumiem, *PPC* izskata personu iesniegtās sūdzības, ievērojot šādu kārtību:

a) ja personai ir aizdomas, ka viņas personas datus, kas nosūtīti no ES, ir vākušas vai izmantojušas publiskās iestādes Japānā, tostarp iestādes, kuras atbild par darbībām, kas minētas šā apliecinājuma II un III nodaļā, pārkāpjot piemērojamos noteikumus, tai skaitās tos, uz kuriem attiecas šis apliecinājums, šāda persona var iesniegt sūdzību *PPC* (individuāli vai ar savas datu aizsardzības iestādes (DAI) starpniecību);

b) *PPC* izskata sūdzību, izmantojot arī savas pilnvaras saskaņā ar *APPI* 6. pantu, 61. panta ii) punktu un 80. pantu, un par sūdzību informē kompetentās publiskās iestādes, tai skaitā attiecīgās pārraudzības iestādes.

([26]) Saskaņā ar Kriminālprocesa kodeksu un Likumu par galīgo krimināllietu uzskaiti uz piekļuvi konfiscētiem priekšmetiem, kā arī dokumentiem/personas informācijai saistībā ar kriminālās tiesvedību, un to labošanu attiecas unikāla un īpatnēja noteikumu sistēma, kuras mērķis ir aizsargāt iesaistīto personu privātumu, izmeklēšanas konfidencialitāti un kriminālās tiesas atbilstošu darbību utml.

([27]) Konkrēti, kā noteikts Kriminālprocesa kodeksa 316-33. pantā, lai uzlabotu noziedzīgā nodarījumā cietušo aizsardzību, noziedzīgā nodarījumā cietušajam principā ir atļauts iepazīties ar informāciju saistībā ar objektīviem pierādījumiem materiālos, kas nav prokuratūras materiāli, lietās, kurās cietušais ir iesaistīts.

Šīm iestādēm ir pienākums sadarboties ar *PPC* saskaņā ar *APPI* 80. pantu, cita starpā sniedzot nepieciešamo informāciju un iesniedzot nepieciešamos materiālus, lai *PPC* varētu izvērtēt, vai personas informācijas vākšana un turpmāka izmantošana ir notikusi atbilstoši piemērojamiem noteikumiem. Veicot izvērtēšanu, *PPC* sadarbojas ar *MIC*;

c) ja izvērtējums liecina, ka ir noticis piemērojamo noteikumu pārkāpums, tad attiecīgo publisko iestāžu sadarbība ar *PPC* ietver pienākumu novērst pārkāpumu.

Gadījumā, ja saskaņā ar piemērojamiem noteikumiem personas informācijas ir vākta pretlikumīgi, tas ietver savāktās personas informācijas dzēšanu.

Piemērojamo noteikumu pārkāpuma gadījumā *PPC* pirms izvērtējuma noslēgšanas arī apstiprinās, ka pārkāpums ir pilnībā novērsts;

d) kad izvērtējums ir noslēgts, *PPC* saprātīgā termiņā informē attiecīgo personu par izvērtējuma rezultātu, attiecīgā gadījumā norādot arī visus veiktos korektīvos pasākumus. Ar šo paziņojumu *PPC* arī informē personu par iespēju pieprasīt no kompetentās publiskās iestādes rezultāta apstiprinājumu un par iestādi, kurā būtu iesniedzams šāds apstiprināšanas pieprasījums.

Sīkas informācijas sniegšana par izvērtējuma rezultātu var būt ierobežota, kamēr vien ir pamatoti iemesli uzskatīt, ka šādas informācijas paziņošana varētu apdraudēt notiekošo izmeklēšanu.

Ja sūdzība attiecas uz personas datu vākšanu vai izmantošanu krimināltiesību izpildes jomā, *PPC* gadījumā, kad izvērtējumā tiek konstatēts, ka ir ierosināta lieta un ir iesaistīta attiecīgās personas informācija, un ka lieta ir slēgta, informēs attiecīgo personu, ka viņa ar lietas materiāliem var iepazīties atbilstoši Kriminālprocesa kodeksa 53. pantam un Likuma par galīgo kriminālllietu uzskaiti 4. pantam.

Ja izvērtēšanā tiek konstatēts, ka persona ir aizdomās turētais kriminālllietā, *PPC* informē personu par šo faktu un iespēju atbilstoši Kriminālkodeksa 259. pantam iesniegt pieprasījumu;

e) ja persona joprojām nav apmierināta ar procedūras iznākumu, viņa var vērsties pie *PPC*, kas informē personu par dažādajām iespējām un precīzu kārtību tiesiskās aizsardzības līdzekļu izmantošanai atbilstoši Japānas normatīvajiem aktiem. *PPC* sniegs personai atbalstu, kas ietver arī konsultācijas un palīdzību, lai celtu jebkādas turpmākas prasības pret attiecīgo administratīvo vai tiesu iestādi.

III. **Valdības piekļuve valsts drošības nolūkos**

A. Juridiskie pamati un ierobežojumi attiecībā uz personas informācijas vākšanu

1. Juridiskie pamati informācijas vākšanai, ko veic attiecīgā ministrija/aģentūra

Kā norādīts iepriekš, personas informācijas vākšanai valsts drošības nolūkos, ko veic administratīvās struktūras, ir jābūt to administratīvajā jurisdikcijā.

Japānā nav tiesību aktu, kas nodrošinātu informācijas vākšanu piespiedu kārtā tikai valsts drošības nolūkos. Saskaņā ar Konstitūcijas 35. pantu personas informāciju ir iespējams vākt piespiedu kārtā, tikai pamatojoties uz tiesas izsniegtu orderi noziedzīga nodarījuma izmeklēšanai. Tādējādi šādu orderi var izsniegt tikai kriminālizmeklēšanas nolūkos. Tas nozīmē, ka Japānas tiesību sistēmā informācijas vākšana/piekļuve informācijai valsts drošības apsvērumu dēļ, izmantojot piespiedu līdzekļus, nav atļauta. Tā vietā valsts drošības jomā attiecīgās ministrijas vai aģentūras var iegūt informāciju tikai no tiem avotiem, kuriem var brīvi piekļūt, vai saņemt informāciju no uzņēmējiem vai privātpersonām, kuras brīvprātīgi izpauž informāciju. Uzņēmējiem, kas saņem pieprasījumu brīvprātīgi sadarboties, nav juridiska pienākuma sniegt šādu informāciju, un tādējādi tiem nav negatīvas sekas, ja tie atsakās sadarboties.

Valsts drošības jomā atbildība ir vairākiem dažādiem ministriju departamentiem un aģentūrām.

1. Ministru kabineta sekretariāts

Ministru kabineta sekretariāts veic informācijas vākšanu un izpēti attiecībā uz svarīgiem Ministru kabineta politikas virzieniem ([28]), kas noteikti Ministru kabineta likuma ([29]) 12. panta 2. punktā. Tomēr Ministru kabineta sekretariāts nav pilnvarots vākt personas informāciju tieši no uzņēmējiem. Sekretariāts vāc, iekļauj, analizē un novērtē informāciju, kas iegūta no publisko avotu materiāliem, citām publiskām iestādēm u. c.

2. *NPA*/prefektūras policija

Katrā prefektūrā prefektūras policija ir pilnvarota vākt informāciju savas jurisdikcijas ietvaros saskaņā ar Policijas likuma 2. pantu. Var gadīties, ka *NPA* tieši vāc informāciju savas jurisdikcijas ietvaros saskaņā ar Policijas likumu. Tas jo īpaši attiecas uz *NPA* Drošības biroja, kā arī Ārlietu un izlūkošanas dienesta darbību. Saskaņā ar Policijas likuma 24. pantu Drošības birojs atbild par jautājumiem, kas saistīti ar drošības policiju ([30]), un Ārlietu un izlūkošanas dienests atbild par jautājumiem, kas attiecas uz ārvalstniekiem, kā arī uz Japānas valstspiederīgajiem, kuru pamatdarbība ir bāzēta ārvalstīs.

3. Sabiedriskās drošības izlūkošanas aģentūra (*PSIA*)

Kaitniecisku darbību novēršanas likuma (*SAPA*) un Likuma par to organizāciju kontroli, kuras veikušas neselektīvas masu slepkavības (*ACO*), piemērošana ir galvenokārt Sabiedriskās drošības izlūkošanas aģentūras (*PSIA*) pārziņā. Šī ir Tieslietu ministrijas aģentūra.

SAPA un *ACO* nosaka, ka, ievērojot stingrus nosacījumus, administratīvos noteikumus (t. i., pasākumus, ar ko nosaka šādu organizāciju darbības ierobežošanu, to likvidēšanu utt.) var pieņemt pret organizācijām, kas izdarījušas konkrētus smagus nodarījumus ("kaitējošas teroristu darbības" vai "neselektīvas masu slepkavības"), pārkāpjot Konstitūcijā noteiktos "sabiedriskās drošības" vai "sabiedrības pamatsistēmas" principus. "Kaitējošas teroristu darbības" ietilpst *SAPA* darbības jomā (sk. 4. pantu, kas attiecas uz tādām darbībām kā nemieri, kūdīšana uz ārvalstu agresiju, slepkavība ar politisku nodomu utt.), savukārt *ACO* attiecas uz "Neselektīvām masu slepkavībām" (sk. *ACO* 4. pantu). Tikai precīzi identificētas organizācijas, kas rada konkrētus iekšējus vai ārējus draudus sabiedriskajai drošībai, var tikt pakļautas *SAPA* vai *ACO* paredzētajiem noteikumiem.

Šajā nolūkā *SAPA* un *ACO* paredz izmeklēšanas juridiskās pilnvaras. *PSIA* (*PSIO*) ierēdņu pamata izmeklēšanas pilnvaras ir noteiktas *SAPA* 27. pantā un *ACO* 29. pantā. Saskaņā ar šiem noteikumiem *PSIA* veic izmeklēšanu tādā mērā, kādā tā ir nepieciešama, ievērojot iepriekš minētos organizāciju kontroles noteikumus (piemēram, kreisi orientētās radikālās grupas, sekta *Aum Shinrikyo* un konkrēta vietējā grupa, kas ir cieši saistīta ar Ziemeļkoreju, ir iepriekš tikušas minētas kā izmeklēšanas subjekti). Tomēr šī izmeklēšana nevar balstīties uz piespiedu līdzekļiem, un līdz ar to organizācija, kurai ir personas informācija, nevar tikt spiesta sniegt šādu informāciju.

Uz *PSIA* brīvprātīgi atklātās informācijas vākšanu un izmantošanu attiecas attiecīgi aizsardzības pasākumi un ierobežojumi, kas paredzēti tiesību aktos, piemēram, cita starpā, Konstitūcijā garantētā telesakaru slepenība un noteikumi par personas informācijas izmantošanu saskaņā ar *APPIHAO*.

4. Aizsardzības ministrija (*MOD*)

Aizsardzības ministrija (*MOD*) vāc informāciju, pamatojoties uz 3. un 4. pantu Likumā par *MOD* izveidi, ciktāl tas ir vajadzīgs, lai īstenotu tās administratīvajā jurisdikcijā esošās lietas, tostarp attiecībā uz aizsardzību un apsardzi, pašaizsardzības spēku veicamajām darbībām, kā arī pašaizsardzības spēku (sauszemes, jūras un gaisa spēku) izvietošanu. *MOD* var vākt informāciju šim nolūkam, tikai pamatojoties uz brīvprātīgu sadarbību un izmantojot brīvi pieejamus avotus. Tā nevāc informāciju par plašu sabiedrību.

2. Ierobežojumi un aizsardzības pasākumi

a) Likumā noteiktie ierobežojumi

1. Vispārējie ierobežojumi, kuru pamatā ir *APPIHAO*

APPIHAO ir vispārējs tiesību akts, kas attiecas uz personas informācijas vākšanu un izmantošanu, ko veic administratīvās struktūras jebkurā šādu struktūru darbības jomā. Tāpēc II nodaļas A daļas 1. punkta b) apakšpunkta 2. punktā aprakstītie ierobežojumi un aizsardzības pasākumi attiecas arī uz personas informācijas uzkrāšanu, saglabāšanu, izmantošanu utt. valsts drošības jomā.

([28]) Šīs darbības veic Ministru kabineta izlūkošanas un izpētes birojs, pamatojoties uz Ministru kabineta sekretariāta rīkojuma 4. panta noteikumiem.

([29]) Tas ietver "izlūkdatu vākšanu un izpēti par svarīgiem Ministru kabineta politikas virzieniem".

([30]) Drošības policija ir atbildīga par noziedzības kontroles pasākumiem, kas saistīti ar sabiedrisko drošību un valsts interesēm. Tas nozīmē arī noziegumu kontroli un informācijas vākšanu par nelikumīgām darbībām, kas saistītas ar kreisi orientēto ekstrēmistu grupām, labējo ekstrēmistu grupām un kaitējošām darbībām, kas vērstas pret Japānu.

2. Konkrēti ierobežojumi, kas attiecas uz policiju (gan *NPA*, gan prefektūras policiju)

Kā norādīts iepriekš nodaļā par informācijas vākšanu tiesībaizsardzības nolūkos, policija var vākt informāciju tikai savas jurisdikcijas ietvaros, un, to darot, tā saskaņā ar Policijas likuma 2. panta 2. punktu var veikt tikai "stingri ierobežotas" darbības tādā apmērā, kāds ir nepieciešams tās pienākumu pildīšanai, un "objektīvi, neatkarīgi, bez aizspriedumiem un godīgi". Turklāt policijas pilnvaras "nekad nedrīkst tikt ļaunprātīgi izmantotas, kaitējot Japānas Konstitūcijā garantētajām personas tiesībām un brīvībām".

3. *PSIA* piemērojamie konkrētie ierobežojumi

Gan *SAPA* 3. pantā, gan *ACO* 3. pantā ir noteikts, ka izmeklēšanu saskaņā ar šiem tiesību aktiem veic tikai tādā apjomā, kāds nepieciešams, lai sasniegtu izvirzīto mērķi, un to nedrīkst veikt tādā veidā, kas nepamatoti ierobežo pamata cilvēktiesības. Turklāt saskaņā ar *SAPA* 45. pantu un *ACO* 42. pantu, ja *PSIA* ierēdnis ļaunprātīgi izmanto savas pilnvaras, tas ir noziedzīgs nodarījums, kas ir sodāms ar smagākiem kriminālsodiem nekā "vispārīga" varas ļaunprātīga izmantošana citās publiskā sektora jomās.

4. *MOD* piemērojamie konkrētie ierobežojumi

Attiecībā uz *MOD* veiktu informācijas vākšanu/organizēšanu, kā minēts Likuma par *MOD* izveidi 4. pantā, šīs ministrijas veiktās informācijas vākšanas darbības ir ierobežotas tādā apmērā, kāds ir nepieciešams tās pienākumu pildīšanai attiecībā uz 1) aizsardzību un apsardzi, 2) pašaizsardzības spēku veicamajām darbībām, 3) sauszemes, jūras un gaisa spēku organizāciju, personāla skaitu, struktūru, aprīkojumu un izvietošanu.

b) Citi ierobežojumi

Kā paskaidrots iepriekš II nodaļas A daļas 2. punkta b) apakšpunkta 1. punktā par kriminālizmeklēšanu, no Augstākās tiesas judikatūras izriet, ka, lai uzņēmējam adresētu pieprasījumu par brīvprātīgu sadarbību, šādam pieprasījumam jābūt nepieciešamam iespējama nozieguma izmeklēšanai un tam jābūt pamatotam, lai sasniegtu izmeklēšanas mērķi.

Lai gan izmeklēšana, ko veic izmeklēšanas iestādes valsts drošības jomā, atšķiras no izmeklēšanas, kuru veic izmeklēšanas iestādes tiesībaizsardzības jomā, gan no izmeklēšanas juridiskā pamata, gan mērķa viedokļa, pamatprincipi par "izmeklēšanas nepieciešamību" un "metodes atbilstību" ir līdzīgi piemērojami valsts drošības jomā un ir tie jāievēro, pienācīgi ņemot vērā katra gadījuma konkrētos apstākļus.

Iepriekš minēto ierobežojumu apvienojums nodrošina, ka informācijas vākšana un apstrāde notiek tikai tādā apmērā, kāds nepieciešams kompetentās publiskās iestādes konkrēto pienākumu veikšanai, kā arī atkarībā no konkrētajiem draudiem. Tas neattiecas uz personas informācijas masveida un nediferencētu apkopošanu vai piekļuvi tai valsts drošības apsvērumu dēļ.

B. Pārraudzība

1. Pārraudzība, pamatojoties uz *APPIHAO*

Kā paskaidrots iepriekš II nodaļas B daļas 2. punktā, Japānas publiskajā sektorā ministram vai katras ministrijas vai aģentūras vadītājam ir piešķirtas pilnvaras veikt pārraudzību un nodrošināt atbilstību *APPIHAO* viņa/viņas ministrijā vai aģentūrā. Turklāt iekšlietu un komunikācijas lietu ministrs var izmeklēt likuma izpildes statusu, lūgt katram ministram iesniegt materiālus un paskaidrojumus, pamatojoties uz likuma 49. un 50. pantu, sniegt atzinumus katram ministram, pamatojoties uz likuma 51. pantu. Piemēram, viņš/viņa var lūgt pārskatīt pasākumus, veicot darbības saskaņā ar likuma 50. un 51. pantu.

2. Sabiedriskās drošības komisiju veiktā policijas pārraudzība

Kā paskaidrots iepriekšējā nodaļā "II. Informācijas vākšana krimināltiesību aizsardzības nolūkos", neatkarīgas prefektūru sabiedriskās drošības komisijas uzrauga prefektūras policijas darbību.

Valsts policijas aģentūras (*NPA*) uzraudzības funkcijas veic Valsts sabiedriskās drošības komisija. Saskaņā ar Policijas likuma 5. pantu šī komisija ir atbildīga jo īpaši par "personas tiesību un brīvības aizsardzību". Šajā nolūkā tā jo īpaši izstrādā visaptverošu politiku, ar ko paredz regulējumu par lietu pārvaldību, kas noteikta katrā Policijas likuma 5. panta 4. punkta apakšpunktā, un nosaka citus pamatvirzienus vai pasākumus, kas būtu jāizmanto, veicot minētās darbības. Valsts sabiedriskās drošības komisijai (*NPSC*) ir tāda pati neatkarības pakāpe kā prefektūru sabiedriskās drošības komisijām (*PPSC*).

3. Juridiskās atbilstības ģenerālinspektora biroja veikta *MOD* pārraudzība

Juridiskās atbilstības ģenerālinspektora birojs (*IGO*) ir neatkarīgs birojs Aizsardzības ministrijā (*MOD*), ko tieši uzrauga aizsardzības ministrs saskaņā ar Likuma par *MOD* izveidi 29. pantu. *IGO* var veikt pārbaudes par to, kā *MOD* ierēdņi nodrošina atbilstību normatīvajiem aktiem. Šīs pārbaudes sauc par "aizsardzības pārbaudēm".

IGO veic pārbaudes kā neatkarīgs birojs, lai nodrošinātu juridisko atbilstību visā ministrijā, tostarp pašaizsardzības spēkos (*SDF*). Tas pilda savus pienākumus neatkarīgi no *MOD* operatīvajiem departamentiem. Pēc pārbaudes *IGO* nekavējoties ziņo aizsardzības ministram par saviem konstatējumiem un nepieciešamajiem uzlabojošajiem pasākumiem. Pamatojoties uz *IGO* ziņojumu, aizsardzības ministrs var izdot rīkojumus par tādu pasākumu īstenošanu, kas nepieciešami situācijas labošanai. Ministra vietnieks ir atbildīgs par šo pasākumu īstenošanu, un viņam ir jāziņo aizsardzības ministram par šādas īstenošanas statusu.

Aizsardzības pārbaužu rezultāti tagad tiek publiskoti *MOD* tīmekļa vietnē (lai gan tas nav prasīts tiesību aktos), kas ir brīvprātīgs pārredzamības pasākums.

Pastāv trīs aizsardzības pārbaužu kategorijas:

i) regulāras aizsardzības pārbaudes, ko veic periodiski ([31]);

ii) aizsardzības pārbaudes, ko veic, lai pārbaudītu, vai ir efektīvi veikti uzlabojošie pasākumi; un

iii) īpašas aizsardzības pārbaudes, ko veic attiecībā uz īpašiem jautājumiem un kuras norīkojis aizsardzības ministrs.

Saistībā ar šādām pārbaudēm ģenerālinspektors var pieprasīt no attiecīgā biroja ziņojumus, pieprasīt iesniegt dokumentus, iekļūt telpās, lai veiktu pārbaudi, pieprasīt ministra vietniekam sniegt paskaidrojumus utt. Ņemot vērā *IGO* veikto pārbaužu uzdevumu raksturu, šo biroju vada visaugstākā līmeņa juridiskie eksperti (iepriekš superintendents prokurors).

4. *PSIA* pārraudzība

PSIA veic gan regulāras, gan īpašas atsevišķu nodaļu un biroju (Sabiedriskās drošības izlūkošanas birojs, sabiedriskās drošības izlūkošanas iestādes un apakšiestādes utt.) darbību pārbaudes. Regulāras pārbaudes nolūkos par inspektoru(-iem) ir iecelts (-i) ģenerāldirektora palīgs un/vai direktors. Šādas pārbaudes attiecas arī uz personas informācijas pārvaldību.

5. Parlamenta veikta pārraudzība

Attiecībā uz informācijas vākšanu tiesībaizsardzības nolūkos parlaments ar savas kompetentās komitejas starpniecību var pārbaudīt informācijas vākšanas darbību likumību valsts drošības jomā. Parlamenta izmeklēšanas pilnvaru pamatā ir Konstitūcijas 62. pants un Parlamenta likuma 74. un 104. pants.

C. Individuāla tiesiskā aizsardzība

Individuālo tiesisko aizsardzību var īstenot, izmantojot tādas pašas iespējas kā krimināltiesību aizsardzības jomā. Tas ietver arī jauno tiesiskās aizsardzības mehānismu, ko pārvalda un uzrauga *PPC* un kas paredzēts, lai izskatītu un risinātu ES iedzīvotāju iesniegtās sūdzības. Šajā saistībā skatīt attiecīgos II nodaļas C daļas teksta fragmentus.

Turklāt valsts drošības jomā ir pieejami īpaši individuālas tiesiskās aizsardzības līdzekļi.

Uz personas informāciju, ko valsts drošības nolūkos vāc administratīva struktūra, attiecas *APPIHAO* 4. nodaļas noteikumi. Tas ietver tiesības pieprasīt izpaust informāciju (12. pants), labot (tostarp papildināt vai svītrot) glabātu personas informāciju (27. pants), kā arī tiesības pieprasīt pārtraukt personas informācijas izmantošanu gadījumā, ja administratīvā iestāde ir nelikumīgi ieguvusi attiecīgo informāciju (36. pants). Ņemot vērā iepriekš minēto, uz šādu tiesību īstenošanu

([31]) Kā piemēru pārbaudēm, kas saistītas ar jautājumiem, uz kuriem attiecas šis apgalvojums, var minēt 2016. gadā veikto regulāro aizsardzības pārbaudi attiecībā uz "informētību/sagatavošanos juridiskai atbilstībai", jo personas informācijas aizsardzība bija viens no galvenajiem pārbaudes punktiem. Konkrētāk, pārbaude attiecās uz personas informācijas pārvaldības, glabāšanas utt. statusu. Savā ziņojumā *IGO* konstatēja vairākus neatbilstošus aspektus personas informācijas pārvaldībā, kas būtu jāuzlabo, piemēram, nespēja aizsargāt datus, izmantojot paroli. Ziņojums ir pieejams *MOD* tīmekļa vietnē.

valsts drošības jomā attiecas konkrēti ierobežojumi: informācijas izpaušanas, labošanas vai izmantošanas pārtraukšanas pieprasījumi netiks apmierināti gadījumos, kad tie attiecas uz "informāciju, attiecībā uz kuru ir pamatoti iemesli administratīvās struktūras vadītājam secināt, ka izpaušana varētu radīt kaitējumu valsts drošībai, radīt kaitējumu savstarpējas uzticēšanās attiecībām ar citu valsti vai starptautisku organizāciju vai radīt nelabvēlīgu situāciju sarunās ar citu valsti vai starptautisku organizāciju" (14. panta iv) punkts). Līdz ar to šis atbrīvojums neattiecas uz visu brīvprātīgu informācijas vākšanu saistībā ar valsts drošību, jo tam vienmēr nepieciešams konkrēts novērtējums par riskiem, kas saistīti ar informācijas izpaušanu.

Turklāt, ja personas pieprasījums tiek noraidīts, pamatojoties uz to, ka attiecīgo informāciju uzskata par neizpaužamu 14. panta iv) punkta nozīmē, persona var iesniegt administratīvu pārsūdzību šāda lēmuma pārskatīšanai, norādot, piemēram, ka konkrētajā gadījumā nav izpildīti 14. panta iv) punktā minētie nosacījumi. Tādā gadījumā attiecīgās administratīvās struktūras vadītājs pirms lēmuma pieņemšanas apspriežas ar Informācijas izpaušanas un personas informācijas aizsardzības izvērtēšanas padomi. Šī padome pārskatīs apelācijas sūdzību no neatkarīga skatupunkta. Padome ir ļoti specializēta un neatkarīga struktūra, kuras locekļus premjerministrs ar abu parlamenta palātu piekrišanu ieceļ no to cilvēku vidus, kuriem ir izcilas zināšanas ([32]). Padomei ir spēcīgas izmeklēšanas pilnvaras, tostarp iespēja pieprasīt dokumentus un attiecīgās personas informācijas izpaušanu, slepenas apspriedes un *Vaughn* indeksa procedūras piemērošanu ([33]). Pēc tam padome sagatavo rakstisku ziņojumu, ko dara zināmu attiecīgajai personai ([34]). Ziņojumā iekļautie konstatējumi tiek publiskoti. Lai gan ziņojums oficiāli nav juridiski saistošs, attiecīgā administratīvā struktūra izpilda gandrīz visos ziņojumos noteikto ([35]).

Visbeidzot, saskaņā ar Administratīvo lietu iztiesāšanas likuma 3. panta 3. punktu persona var iesniegt prasību tiesā, lūdzot atcelt administratīvās struktūras pieņemto lēmumu neatklāt personas informāciju.

IV. **Periodiska pārskatīšana**

Saistībā ar lēmuma par aizsardzības līmeņa pietiekamību periodisko pārskatīšanu *PPC* un Eiropas Komisija apmainīsies ar informāciju par datu apstrādi atbilstoši konstatējuma par aizsardzības līmeņa pietiekamību nosacījumiem, tostarp tiem, kas izklāstīti šajā apgalvojumā.

([32]) Sk. Likuma par Informācijas izpaušanas un personas informācijas aizsardzības izvērtēšanas padomes izveidi 4. pantu.
([33]) Sk. Likuma par Informācijas izpaušanas un personas informācijas aizsardzības izvērtēšanas padomes izveidi 9. pantu.
([34]) Sk. Likuma par Informācijas izpaušanas un personas informācijas aizsardzības izvērtēšanas padomes izveidi 16. pantu.
([35]) Pēdējo 3 gadu laikā nav bijis neviena precedenta, kad attiecīgā administratīvā struktūra būtu pieņēmusi lēmumu, kas atšķiras no padomes secinājumiem. Skatoties vairāku gadu griezumā, pagātnē ir bijis ļoti maz gadījumu, kad tas ir noticis: tikai divos gadījumos no 2 000 gadījumiem laikposmā no 2005. gada (gads, kurā stājās spēkā *APPIHAO*). Ja administratīvā struktūra nosaka spriedumu/lēmumu, kas atšķiras no padomes secinājumiem, saskaņā ar Administratīvo sūdzību pārskatīšanas likuma 50. panta 1. punkta 4. apakšpunktu, ko piemēro, aizstājot *APPIHAO* 42. panta 2. punktu, tā skaidri norāda šādas rīcības iemeslus.