II

(Neleģislatīvi akti)

LĒMUMI

KOMISIJAS ĪSTENOŠANAS LĒMUMS (ES) 2022/254

(2021. gada 17. decembris),

kas saskaņā ar Eiropas Parlamenta un Padomes Regulu (ES) 2016/679 pieņemts par personas datu pietiekamu aizsardzību Korejas Republikā atbilstīgi Likumam par personas informācijas aizsardzību

(izziņots ar dokumenta numuru C(2021) 9316)

(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]), un jo īpaši tās 45. panta 3. punktu,

tā kā:

1. IEVADS

(1) Ar Regulu (ES) 2016/679 ir paredzēti noteikumi, saskaņā ar kuriem Savienībā esoši pārziņi vai apstrādātāji var nosūtīt personas datus trešām valstīm un starptautiskām organizācijām, ciktāl šāda nosūtīšana ietilpst regulas piemērošanas jomā. Noteikumi par datu starptautisko nosūtīšanu ir izklāstīti minētās regulas V nodaļā (44.–50. pants). Lai gan personas datu plūsma uz valstīm ārpus Eiropas Savienības un no tām ir būtiska pārrobežu tirdzniecības un starptautiskās sadarbības paplašināšanas nodrošināšanai, datu nosūtīšana uz trešām valstīm nedrīkst samazināt Savienībā nodrošināto personas datu aizsardzības līmeni ([2]).

(2) Atbilstīgi Regulas (ES) 2016/679 45. panta 3. punktam Komisija ar īstenošanas aktu var nolemt, ka trešā valsts, trešās valsts teritorija vai viens vai vairāki konkrēti sektori, vai starptautiska organizācija nodrošina pietiekamu aizsardzības līmeni. Saskaņā ar šo nosacījumu personas datus var nosūtīt uz trešo valsti bez nepieciešamības saņemt jebkādu turpmāku atļauju, kā paredzēts Regulas (ES) 2016/679 45. panta 1. punktā un 103. apsvērumā.

(3) Kā norādīts Regulas (ES) 2016/679 45. panta 2. punktā, lēmums par aizsardzības līmeņa pietiekamību jāpieņem, pamatojoties uz visaptverošu trešās valsts tiesību sistēmas analīzi, gan attiecībā uz noteikumiem, kas piemērojami datu saņēmējiem, gan attiecībā uz ierobežojumiem un garantijām saistībā ar publisko iestāžu piekļuvi personas datiem. Komisijai novērtējumā jānosaka, vai attiecīgā trešā valsts garantē aizsardzības līmeni, kurš "pēc būtības ir līdzvērtīgs" Eiropas Savienībā nodrošinātajam (Regulas (ES) 2016/679 104. apsvērums). Vai tas tā ir, ir jāvērtē, ņemot vērā Savienības tiesību aktus, jo īpaši Regulu (ES) 2016/679, kā arī Eiropas Savienības Tiesas judikatūru ([3]).

([1]) OV L 119, 4.5.2016., 1. lpp.
([2]) Sk. Regulas (ES) 2016/679 101. apsvērumu.
([3]) Sk. spriedumu jaunākajā lietā C-311/18 *Facebook Ireland* un *Schrems* (*Schrems II*), ECLI:EU:C:2020:559.

(4) Kā ir precizējusi Eiropas Savienības Tiesa, tas nenozīmē, ka ir jākonstatē identisks aizsardzības līmenis ([4]). Konkrēti, attiecīgās trešās valsts izmantotie līdzekļi personas datu aizsardzībai var atšķirties no Savienībā izmantotajiem, ja vien tie praksē efektīvi nodrošina pietiekamu aizsardzības līmeni ([5]). Tāpēc aizsardzības līmeņa pietiekamības standarts neparedz Savienības noteikumu precīzu replicēšanu. Drīzāk ir jāpārbauda, vai attiecīgās valsts tiesību sistēma spēj nodrošināt nepieciešamo aizsardzības līmeni, ņemot vērā tiesību uz privātumu būtību un to efektīvu īstenošanu, uzraudzību un izpildi ([6]). Šajā saistībā norādījumi sniegti arī Eiropas Datu aizsardzības kolēģijas Pietiekamības atsaucēs, kuru mērķis ir sīkāk precizēt šo standartu ([7]).

(5) Komisija ir rūpīgi izanalizējusi Korejas tiesību aktus un praksi. Pamatojoties uz konstatējumiem, kas izklāstīti 8.–208. apsvērumā, Komisija secina, ka Korejas Republika nodrošina pietiekamu aizsardzības līmeni personas datiem, kurus pārzinis vai apstrādātājs Savienībā ([8]) nosūtījis vienībām (piemēram, fiziskām vai juridiskām personām, organizācijām, publiskām iestādēm) Korejā, uz kurām attiecas Likums par personas informācijas aizsardzību (2011. gada 29. marta Likums Nr. 10465, kurš pēdējo reizi grozīts ar 2020. gada 4. februāra Likumu Nr. 16930). Tas ietver gan pārziņus, gan apstrādātājus (dēvēti par "ārpakalpojumu sniedzējiem" ([9])) Regulas (ES) 2016/679 nozīmē. Konstatējums par pietiekamību neattiecas uz personas datu apstrādi, kuru reliģiskas organizācijas veic misionāru darbību vajadzībām, politisko partiju veiktu personas datu apstrādi kandidātu nominēšanai vai personas kredītinformācijas apstrādi saskaņā ar Kredītinformācijas likumu, ko veic pārziņi, kuri pakļauti Finanšu pakalpojumu komisijas uzraudzībai.

(6) Šajā secinājumā ir ņemtas vērā papildu garantijas, kas izklāstītas Paziņojumā Nr. 2021-5 (I pielikums), un Korejas valdības oficiālie apliecinājumi, garantijas un saistības pret Komisiju (II pielikums).

(7) Saskaņā ar šo lēmumu nav nepieciešams saņemt jebkādu turpmāku atļauju datu nosūtīšanai pārziņiem un apstrādātājiem Korejas Republikā. Tas neietekmē Regulas (ES) 2016/679 tiešu piemērošanu šādām vienībām, ja ir izpildīti minētās regulas 3. pantā paredzētie nosacījumi attiecībā uz tās teritoriālo darbības jomu.

2. PERSONAS DATU APSTRĀDEI PIEMĒROJAMIE NOTEIKUMI

2.1. Datu aizsardzības regulējums Korejas Republikā

(8) Tiesību sistēma, kas reglamentē privātumu un datu aizsardzību Korejā, balstās uz 1948. gada 17. jūlijā izsludināto Konstitūciju. Lai gan Konstitūcijā nav skaidri noteiktas tiesības uz personas datu aizsardzību, tomēr tās ir atzītas par pamattiesībām, kas izriet no konstitucionālajām tiesībām uz cilvēka cieņu un tiekšanos pēc laimes (10. pants), privāto dzīvi (17. pants) un saziņas privātumu (18. pants). To ir apstiprinājusi gan Augstākā tiesa ([10]), gan Konstitucionālā tiesa ([11]). Pamattiesību un brīvību (tostarp tiesību uz privātumu) ierobežojumus tiesību aktos var paredzēt tikai tad, ja tie nepieciešami valsts drošības vai sabiedriskās kārtības un drošības uzturēšanai un tie neietekmē attiecīgo tiesību vai brīvības būtību (37. panta 2. punkts).

([4]) Lieta C-362/14 *Maximillian Schrems/Data Protection Commissioner* (*Schrems*), ECLI:EU:C:2015:650, 73. punkts.
([5]) Spriedums lietā *Schrems*, 74. punkts.
([6]) 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.
([7]) Eiropas Datu aizsardzības kolēģija, Pietiekamības atsauces, WP 254 rev. 01, pieejamas tīmekļa vietnē: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=614108.
([8]) 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. Tāpēc šajā lēmumā atsauces uz ES un ES dalībvalstīm ir jāsaprot arī kā atsauces uz EEZ valstīm.
([9]) Sk. šā lēmuma 2.2.3. iedaļu.
([10]) Sk., piemēram, Augstākās tiesas 2015. gada 15. oktobra Lēmumu Nr. 2014Da77970 (kopsavilkums angļu valodā pieejams tīmekļa vietnē https://www.privacy.go.kr/eng/enforcement_01.do saitē *Lawmaker's disclosure of teachers' trade union members case*) un tajā citēto judikatūru, tai skaitā 2014. gada 24. jūlija Lēmumu Nr. 2012Da49933.
([11]) Sk. jo īpaši Konstitucionālās tiesas 2005. gada 26. maija Lēmumu Nr. 99Hun-ma513 (kopsavilkums angļu valodā pieejams tīmekļa vietnē http://www.koreanlii.or.kr/w/index.php/99Hun-Ma513?ckattempt=2) un 2015. gada 23. decembra Lēmumu Nr. 2014JHun-ma449 2013 Hun-Ba68 (konsolidēts) (kopsavilkums angļu valodā pieejams tīmekļa vietnē https://www.privacy.go.kr/eng/enforcement_01.do saitē *Change of resident registration number case*).

(9) Lai gan Konstitūcijā vairākās vietās ir minētas Korejas valstspiederīgo tiesības, Konstitucionālā tiesa ir nolēmusi, ka pamattiesības attiecas arī uz ārvalstniekiem ([12]). Tiesa jo īpaši norādīja, ka cilvēka cieņas un vērtības aizsardzība, kā arī tiesības meklēt laimi ir jebkura cilvēka, ne tikai valstspiederīgā, tiesības ([13]). Turklāt saskaņā ar Korejas valdības oficiālajiem apliecinājumiem ([14]) ir vispāratzīts, ka Konstitūcijas 12.–22. pants (kas ietver tiesības uz privātumu) nosaka cilvēka pamattiesības ([15]). Lai gan līdz šim nav iedibināta judikatūra, kas īpaši attiektos uz ārvalstnieku tiesībām uz privātumu, tās pamatojums cilvēka cieņas aizsardzībā un laimes meklējumos pamato šo secinājumu ([16]).

(10) Turklāt Koreja ir pieņēmusi vairākus tiesību aktus datu aizsardzības jomā, kas paredz garantijas visām personām neatkarīgi no to valstspiederības ([17]). Šajā lēmumā minētie attiecīgie tiesību akti ir šādi:

— Likums par personas informācijas aizsardzību (*Personal Information Protection Act – "PIPA"*),

— Likums par kredītinformācijas izmantošanu un aizsardzību ([18]),

— Saziņas privātuma aizsardzības likums.

(11) *PIPA* nodrošina datu aizsardzības vispārējo tiesisko regulējumu Korejas Republikā. To papildina Izpildes dekrēts (Prezidenta 2011. gada 29. septembra dekrēts Nr. 23169, kurā jaunākie grozījumi izdarīti ar Prezidenta 2020. gada 4. augusta dekrētu Nr. 30892) ("PIPA Izpildes dekrēts"), kas tāpat kā *PIPA* ir juridiski saistošs un izpildāms.

(12) Turklāt Personas informācijas aizsardzības komisijas ("*PIPC*") pieņemtajos "Paziņojumos" ir sniegti papildu noteikumi par *PIPA* interpretāciju un piemērošanu. Pamatojoties uz *PIPA* 5. pantu (Valsts pienākumi) un 14. pantu (Starptautiskā sadarbība), *PIPC* pieņēma 2020. gada 1. septembra Paziņojumu Nr. 2021-5 (kurā grozījumi izdarīti ar 2021. gada 21. janvāra Paziņojumu Nr. 2021-1 un 2021. gada 16. novembra Paziņojumu Nr. 2021-5, "Paziņojums Nr. 2021-5") par atsevišķu *PIPA* noteikumu interpretāciju, piemērošanu un izpildi. Šajā paziņojumā ir sniegti skaidrojumi, kas attiecas uz personas datu jebkādu apstrādi saskaņā ar *PIPA*, kā arī papildu garantijas personas datiem, kas nosūtīti uz Koreju, pamatojoties uz šo lēmumu. Paziņojums ir juridiski saistošs personas informācijas pārziņiem, un to var piemērot gan *PIPC*, gan tiesas ([19]). Paziņojumā izklāstīto noteikumu pārkāpums nozīmē *PIPA* attiecīgo noteikumu pārkāpumu, kurus tie papildina. Tāpēc papildu garantiju saturs tiek analizēts kā daļa no attiecīgo *PIPA* pantu novērtējuma. Visbeidzot, papildu norādījumi par *PIPA* un tā Izpildes dekrētu, kas sniedz informāciju par *PIPC* īstenojamo datu aizsardzības noteikumu piemērošanu un izpildi, ir sniegti *PIPA* rokasgrāmatā un pamatnostādnēs, ko pieņēmusi *PIPC* ([20]).

([12]) Konstitucionālās tiesas 1994. gada 29. decembra Lēmums Nr. 93 Hun-MA120.

([13]) Konstitucionālās tiesas 2001. gada 29. novembra Lēmums Nr. 99HeonMa494.

([14]) Skatīt II pielikuma 1.1. iedaļu.

([15]) Sk. arī Likuma par personas informācijas aizsardzību 1. pantu, kurā ir skaidra atsauce uz "personu brīvībām un tiesībām". Konkrētāk, tajā noteikts, ka šāda likuma mērķis ir "nodrošināt personas informācijas apstrādi un aizsardzību, lai aizsargātu personu brīvību un tiesības, kā arī lai turpinātu respektēt cilvēku cieņu un vērtību". Tāpat Likuma par personas informācijas aizsardzību 5. panta 1. punktā noteikts, ka valsts pienākums ir "izstrādāt politiku, lai novērstu kaitīgas sekas, ko rada personas informācijas vākšana bez nolūka, ļaunprātīga un nepareiza izmantošana, nediskrēta novērošana un izsekošana utt., kā arī lai veicinātu cilvēka cieņas un personas privātuma respektēšanu".

([16]) Turklāt Konstitūcijas 6. panta 2. punktā noteikts, ka ārvalstnieku statuss tiek garantēts saskaņā ar starptautiskajām tiesībām un līgumiem. Koreja ir parakstījusi vairākus starptautiskus nolīgumus, kas garantē tiesības uz privātumu, piemēram, Starptautisko paktu par pilsoniskajām un politiskajām tiesībām (17. pants), Konvenciju par personu ar invaliditāti tiesībām (22. pants) un Konvenciju par bērna tiesībām (16. pants).

([17]) Tas ietver noteikumus, kas attiecas uz personas datu aizsardzību, bet nav piemērojami situācijā, kad personas dati tiek vākti Savienībā un nosūtīti uz Koreju saskaņā ar Regulu (ES) 2016/679, piemēram, Likumā par atrašanās vietas informācijas aizsardzību, izmantošanu utt.

([18]) Šā likuma mērķis ir sekmēt stabilu kredītinformācijas darījumdarbību, veicinot kredītinformācijas efektīvu izmantošanu un sistemātisku pārvaldību, kā arī aizsargāt privātumu no kredītinformācijas ļaunprātīgas un nepareizas izmantošanas (likuma 1. pants).

([19]) Piemēram, Korejas tiesas ir pieņēmušas nolēmumus par atbilstību normatīvajiem Paziņojumiem vairākās lietās, tostarp saucot Korejas pārziņus pie atbildības par Paziņojuma pārkāpumiem (sk., piemēram, Augstākās tiesas 2018. gada 25. oktobra Lēmumu Nr. 2018Da219406, kurā tiesa lika pārzinim izmaksāt personām kompensāciju par ciestajiem zaudējumiem, kurus radīja "Paziņojuma par personas informācijas drošības pasākumu standartu" pārkāpums; sk. arī Augstākās tiesas 2018. gada 25. oktobra Lēmumu Nr. 2018Da219352; Augstākās tiesas 2016. gada 16. maija Lēmumu Nr. 2011Da24555; Seulas apgabala centrālās tiesas 2016. gada 13. oktobra Lēmumu Nr. 2014Gahap511956; Seulas apgabala centrālās tiesas 2010. gada 26. janvāra Lēmumu Nr. 2009Gahap43176).

([20]) *PIPA* 12. panta 1. punkts.

(13) Turklāt Likumā par kredītinformācijas izmantošanu un aizsardzību (*Act on the Use and Protection of Credit Information* – "*CIA*") ir paredzēti īpaši noteikumi, kas attiecas gan uz "parastiem" komerciālajiem operatoriem, gan specializētām finanšu sektora vienībām, kad tās apstrādā personas kredītinformāciju, proti, informāciju, kas nepieciešama, lai noteiktu finanšu darījumu vai komercdarījumu pušu kredītspēju. Tas jo īpaši attiecas uz vārdu un uzvārdu, kontaktinformāciju, finanšu darījumiem, kredītreitingu, apdrošināšanas statusu vai aizdevuma atlikumu, ja šāda informācija tiek izmantota, lai noteiktu personas kredītspēju ([21]). Savukārt, ja šāda informācija tiek izmantota citiem nolūkiem (piemēram, cilvēkresursu jomā), *PIPA* piemēro pilnībā. Atbilstību konkrētiem *CIA* noteikumiem par datu aizsardzību daļēji uzrauga *PIPC* (attiecībā uz komerciālām organizācijām, sk. *CIA* 45. panta 3. punktu) un daļēji – Finanšu pakalpojumu komisija ([22]) (attiecībā uz finanšu sektoru, ieskaitot kredītreitinga aģentūras, bankas, apdrošināšanas uzņēmumus, kopieguldījumu krājbankas, specializētas kredītiestādes, ieguldījumu pakalpojumu uzņēmumus, vērtspapīru uzņēmumus, krājaizdevu sabiedrības utt., sk. *CIA* 45. panta 1. punktu kopā ar *CIA* Izpildes dekrēta 36. panta 2. punktu un Likuma par Finanšu pakalpojumu komisiju 38. pantu). Šajā ziņā šā lēmuma darbības joma attiecas tikai uz komerciālajiem operatoriem, kuriem piemērojama *PIPC* īstenota pārraudzība ([23]). Šajā kontekstā piemērojamie īpašie *CIA* noteikumi (ja nav īpašu noteikumu, piemēro vispārīgos *PIPA* noteikumus) ir aprakstīti 2.3.11. iedaļā.

2.2. ***PIPA* materiālā un personīgā piemērošanas joma**

(14) Personas datu aizsardzību reglamentē *PIPA* (6. pants), ja vien citos likumos nav īpaši noteikts citādi. Tā materiālo un personīgo piemērošanas jomu nosaka definētie jēdzieni "personas informācija", "apstrāde" un "personas informācijas pārzinis".

2.2.1. *Personas datu definīcija*

(15) *PIPA* 2. panta 1. punktā personas informācija ir definēta kā informācija, kas attiecas uz dzīvu personu un kas identificē personu tieši, piemēram, pēc tās vārda, uzvārda, iedzīvotāju reģistrācijas numura vai attēla, vai netieši, proti, ja informāciju, pēc kuras nevar identificēt konkrētu personu, var viegli apvienot ar citu informāciju. Tas, vai informāciju var "viegli" apvienot, ir atkarīgs no tā, vai šāda kombinēšana jeb apvienošana ir saprātīgi iespējama, ņemot vērā iespēju iegūt citu informāciju, kā arī laiku, izmaksas un tehnoloģijas, kas nepieciešami personas identificēšanai.

(16) Turklāt pseidonimizēta informācija – t. i., informācija, pēc kuras nevar identificēt konkrētu personu, neizmantojot vai neapvienojot to ar papildu informāciju, lai atjaunotu tās sākotnējo stāvokli, – saskaņā ar *PIPA* tiek uzskatīta par personas datiem (*PIPA* 2. panta 1. punkta c) apakšpunkts). Savukārt informācija, kas ir pilnībā "anonimizēta", ir izslēgta no *PIPA* piemērošanas jomas (*PIPA* 58-2. pants). Tas attiecas uz informāciju, pēc kuras nevar identificēt konkrētu personu, pat ja to apvieno ar citu informāciju, ņemot vērā laiku, izmaksas un tehnoloģiju, kas pamatoti nepieciešami identificēšanai.

(17) Tas atbilst Regulas (ES) 2016/679 materiālajai piemērošanas jomai un tās jēdzieniem "personas dati", "pseidonimizācija" ([24]) un "anonimizēta informācija" ([25]).

([21]) *CIA* 2. panta 1. punkts

([22]) Finanšu pakalpojumu komisija ir Korejas finanšu sektora uzraudzības iestāde, kas arī īsteno *CIA*.

([23]) Ja tas nākotnē mainīsies, piemēram, ar *PIPC* jurisdikcijas paplašināšanu attiecinot to uz visu personas kredītinformācijas apstrādi saskaņā ar *CIA*, varētu apsvērt iespēju grozīt lēmumu par aizsardzības līmeņa pietiekamību, lai tas attiektos arī uz vienībām, kas pašlaik ir Finanšu pakalpojumu komisijas pārraudzībā.

([24]) *PIPA* par "pseidonimizētu apstrādi" uzskatīta apstrāde ar tādām metodēm kā personas datu daļēja dzēšana vai to daļēja vai pilnīga aizstāšana tā, ka bez papildu informācijas nav iespējams atpazīt konkrētu personu (*PIPA* 2. panta 1-2. punkts). Tas atbilst Regulas (ES) 2016/679 4. panta 5. punktā ietvertajai pseidonimizācijas definīcijai: "personas datu apstrāde, ko veic tādā veidā, lai personas datus vairs nav iespējams saistīt ar konkrētu datu subjektu bez papildu informācijas izmantošanas, ar noteikumu, ka šāda papildu informācija tiek turēta atsevišķi un tai piemēro tehniskus un organizatoriskus pasākumus, lai nodrošinātu, ka personas dati netiek saistīti ar identificētu vai identificējamu fizisku personu."

([25]) Konkrēti, Regulas (ES) 2016/679 26. apsvērumā precizēts, ka regula neattiecas uz anonimizētu jeb anonīmu informāciju, t. i., informāciju, kura neattiecas uz identificētu vai identificējamu fizisku personu. Tas savukārt ir atkarīgs no visiem līdzekļiem, kurus pārzinis vai cita persona varētu saprātīgi izmantot, lai tieši vai netieši identificētu fizisku personu. Lai pārliecinātos, vai šādus līdzekļus varētu saprātīgi izmantot, būtu jāņem vērā visi objektīvie faktori, piemēram, identificēšanai nepieciešamās izmaksas un laiks, ņemot vērā apstrādes laikā pieejamo tehnoloģiju un tehnoloģiju attīstību."

2.2.2. *Apstrādes definīcija*

(18) "Apstrādes" jēdziens *PIPA* ir plaši definēts kā tāds, kas ietver "personas informācijas vākšanu, ģenerēšanu, savienošanu, sasaistīšanu, reģistrēšanu, glabāšanu, saglabāšanu, apstrādi ar pievienoto vērtību, rediģēšanu, izgūšanu, izvadi, labošanu, atgūšanu, izmantošanu, sniegšanu un atklāšanu, iznīcināšanu un citas līdzīgas darbības" ([26]). Lai gan daži *PIPA* noteikumi attiecas tikai uz konkrētiem apstrādes veidiem, piemēram, "izmantošana", "sniegšana" vai "vākšana" ([27]), jēdziens "izmantošana" tiek interpretēts kā tāds, kas ietver jebkuru apstrādes veidu, izņemot "vākšanu" vai "sniegšanu" (trešai personai). Tādējādi šī plašā "izmantošanas" jēdziena interpretācija nodrošina, ka nav nepilnību aizsardzībā attiecībā uz konkrētām apstrādes darbībām. Tādējādi apstrādes jēdziens atbilst tam pašam jēdzienam kā Regulā (ES) 2016/679.

2.2.3. *Personas informācijas pārzinis un "ārpakalpojumu sniedzējs"*

(19) *PIPA* attiecas uz "personas informācijas pārziņiem" ("pārzinis"). Līdzīgi kā Regulā (ES) 2016/679 tas attiecas uz jebkuru publisko iestādi, juridisku personu, organizāciju vai fizisku personu, kas tieši vai netieši apstrādā personas datus, lai savas darbības ietvaros pārvaldītu personas datu datnes ([28]). Šajā saistībā "personas informācijas datne" ir jebkurš "sistemātiski sakārtots vai sistemātiski organizēts personas informācijas kopums vai kopumi, pamatojoties uz konkrētu noteikumu, lai personas informācijai būtu viegli piekļūt" (*PIPA* 2. panta 4. punkts) ([29]). Iekšēji pārzinim ir pienākums apmācīt personas, kas iesaistītas apstrādē tā vadībā, piemēram, uzņēmuma amatpersonas vai darbiniekus, un veikt pienācīgu kontroli un uzraudzību (*PIPA* 28. panta 1. punkts).

(20) Konkrēti pienākumi attiecas uz gadījumiem, kad pārzinis ("ārpakalpojumu saņēmējs") nodod personas datu apstrādi trešai personai ("ārpakalpojumu sniedzējs"). Konkrētāk, ārpakalpojumu izmantošana ir jāreglamentē ar juridiski saistošu vienošanos (parasti – līgumu) ([30]), kurā ir noteikts ārpakalpojumā nodotā darba apjoms, apstrādes nolūks, piemērojamie tehniskie un pārvaldības aizsardzības pasākumi, pārziņa īstenota uzraudzība, atbildība (piemēram, kompensācija par līgumsaistību neizpildes rezultātā nodarīto kaitējumu), kā arī ierobežojumi attiecībā uz jebkādu apakšapstrādi ([31]) (*PIPA* 26. panta 1. un 2. punkts kopā ar Izpildes dekrēta 28. panta 1. punktu) ([32]).

(21) Turklāt pārzinim ir jāpublicē un pastāvīgi jāatjaunina informācija par ārpakalpojumā nodoto darbu un ārpakalpojumu sniedzēja identitāti vai, ciktāl ārpakalpojumā nodotā apstrāde attiecas uz tiešās tirgvedības darbībām, tieši jāpaziņo attiecīgā informācija fiziskām personām (*PIPA* 26. panta 2. un 3. punkts kopā ar Izpildes dekrēta 28. panta 2.–5. punktu) ([33]).

(22) Turklāt saskaņā ar *PIPA* 26. panta 4. punktu un Izpildes dekrēta 28. panta 6. punktu pārzinim ir pienākums "izglītot" ārpakalpojumu sniedzēju par nepieciešamajiem drošības pasākumiem un uzraudzīt, cita starpā veicot pārbaudes, vai tas pilda visus pārziņa pienākumus saskaņā ar *PIPA* ([34]), kā arī saskaņā ar ārpakalpojuma līgumu. Ja ārpakalpojumu sniedzējs rada kaitējumu *PIPA* pārkāpuma dēļ, tā darbība vai bezdarbība atbildības nolūkos tiks attiecināta uz pārzini tāpat kā darbinieka gadījumā (*PIPA* 26. panta 6. punkts).

([26]) *PIPA* 2. panta 2. punkts.
([27]) Piemēram, *PIPA* 15.–19. pants attiecas tikai uz personas informācijas vākšanu, izmantošanu un sniegšanu.
([28]) *PIPA* 2. panta 5. punkts. Publiskās iestādes *PIPA* nozīmē ir visas centrālās pārvaldes iestādes vai aģentūras un ar tām saistītās struktūras, pašvaldības, skolas un valsts uzņēmumi ar pašvaldības finansējumu, Nacionālās asamblejas administratīvās struktūras un tiesu iestādes (tostarp Konstitucionālā tiesa) (*PIPA* 2. panta 6. punkts kopā ar *PIPA* Izpildes dekrēta 2. pantu).
([29]) Tas atbilst Regulas (ES) 2016/679 materiālajai piemērošanas jomai. Saskaņā ar Regulas (ES) 2016/679 2. panta 1. punktu šo regulu piemēro "personas datu apstrādei, kas pilnībā vai daļēji veikta ar automatizētiem līdzekļiem, un tādu personas datu apstrādei, kuri veido daļu no kartotēkas vai ir paredzēti, lai veidotu daļu no kartotēkas, ja apstrādi neveic ar automatizētiem līdzekļiem." Regulas (ES) 2016/679 4. panta 6. punktā "kartotēka" ir definēta kā "jebkurš strukturēts personas datu kopums, kas ir pieejams saskaņā ar konkrētiem kritērijiem". Saskaņā ar to 15. apsvērumā paskaidrots, ka fizisku personu aizsardzībai būtu jāattiecas "gan uz personas datu apstrādi ar automatizētiem līdzekļiem, gan uz datu manuālu apstrādi, ja personas dati ir ietverti vai tos paredzēts ietvert kartotēkā. Šīs regulas darbības jomai nebūtu jāaptver datnes vai datņu kopumi, kā arī to ievadlapas, kuras nav sakārtotas atbilstīgi konkrētiem kritērijiem."
([30]) Sk. *PIPA* rokasgrāmatas III nodaļas 2. iedaļu par 26. pantu (203.–212. lpp.), kurā paskaidrots, ka *PIPA* 26. panta 1. punkts attiecas uz saistošiem vienošanās dokumentiem, piemēram, līgumiem vai līdzīgiem dokumentiem.
([31]) Saskaņā ar *PIPA* 26. panta 5. punktu apstrādātājam ir aizliegts izmantot jebkādu personas informāciju ārpus ārpakalpojumā nodotā darba apjoma vai sniegt personas informāciju trešai personai. Par šīs prasības neievērošanu var piemērot kriminālsodu saskaņā ar *PIPA* 71. panta 2. punktu.
([32]) Par šīs prasības neievērošanu var piemērot naudas sodu (sk. *PIPA* 75. panta 4. punkta 4. apakšpunktu).
([33]) Par šīs prasības neievērošanu var piemērot naudas sodu (sk. *PIPA* 75. panta 2. punkta 1. apakšpunktu un 4. panta 5. punktu).
([34]) Sk. arī *PIPA* 26. panta 7. punktu, saskaņā ar kuru 15.–25., 27.–31., 33.–38. un 50. pants *mutatis mutandis* attiecas uz apstrādātāju.

(23) Lai gan *PIPA* tādēļ nav izmantoti dažādi jēdzieni attiecībā uz "pārziņiem" un "apstrādātājiem", ārpakalpojumu noteikumos būtībā ir paredzēti pēc būtības līdzvērtīgi pienākumi un garantijas kā tie, kas regulē attiecības starp pārziņiem un apstrādātājiem saskaņā ar Regulu (ES) 2016/679.

2.2.4. *Īpaši noteikumi informācijas un komunikācijas pakalpojumu sniedzējiem*

(24) Lai gan *PIPA* attiecas uz personas datu apstrādi, ko veic jebkurš pārzinis, daži nosacījumi ietver īpašus noteikumus (kā *lex specialis*) par "lietotāju" personas datu apstrādi, ko veic "informācijas un komunikācijas pakalpojumu sniedzēji" ([35]). Jēdziens "lietotāji" attiecas uz personām, kas izmanto informācijas un komunikācijas pakalpojumus (Likuma par informācijas un komunikācijas tīkla izmantošanas veicināšanu un datu aizsardzību ("Tīkla likums") 2. panta 1. punkta 4. apakšpunkts). Tas nozīmē, ka persona vai nu tieši izmanto Korejas telesakaru operatora sniegtos telesakaru pakalpojumus, vai arī izmanto informācijas pakalpojumus ([36]), ko komerciālā nolūkā (t. i., peļņas gūšanas nolūkā) sniedz vienība, kas savukārt izmanto Korejā licencēta/reģistrēta telesakaru operatora pakalpojumus ([37]). Abos gadījumos īpašie *PIPA* noteikumi ir saistoši vienībai, kas piedāvā tiešsaistes pakalpojumu tieši personai (t. i., lietotājam).

(25) Turpretim konstatējums par pietiekamību attiecas tikai uz aizsardzības līmeni, kas tiek nodrošināts personas datiem, kurus Savienībā esošs pārzinis/apstrādātājs pārsūta vienībai trešā valstī (šajā gadījumā – Korejas Republikā). Pēdējā scenārija gadījumā fiziskām personām Savienībā parasti būs tieša saistība tikai ar Savienībā esošu "datu nosūtītāju", nevis ar Korejas informācijas un komunikācijas pakalpojumu sniedzēju ([38]). Tāpēc *PIPA* īpašie noteikumi attiecībā uz informācijas un komunikācijas pakalpojumu lietotāju personas datiem saskaņā ar šo lēmumu pārsūtītajiem personas datiem tiks piemēroti tikai ierobežotos gadījumos.

2.2.5. *Izņēmumi no atsevišķiem PIPA noteikumiem*

(26) *PIPA* 58. panta 1. punkts izslēdz *PIPA* daļas (t. i., 15.–57. panta) piemērošanu attiecībā uz četrām datu apstrādes kategorijām ([39]). Konkrēti, nepiemēro *PIPA* daļas, kas attiecas uz īpašiem apstrādes pamatojumiem, konkrētiem datu aizsardzības pienākumiem, sīki izstrādātiem noteikumiem par individuālo tiesību īstenošanu, kā arī noteikumiem, kas reglamentē strīdu izšķiršanu, ko veic Personas informācijas strīdu starpniecības komiteja. Citi *PIPA* pamatnoteikumi joprojām ir piemērojami, konkrēti, vispārīgie noteikumi par datu aizsardzības principiem (*PIPA* 3. pants), tai skaitā, piemēram, likumīguma, nolūka precizēšanas un nolūka ierobežojuma, datu minimizēšanas, datu precizitātes un drošības principi, un individuālās tiesības (attiecībā uz piekļuvi, labošanu, dzēšanu un izmantošanas apturēšanu sk. *PIPA* 4. pantu). Turklāt *PIPA* 58. panta 4. punkts attiecībā uz šīm apstrādes darbībām uzliek konkrētus pienākumus, proti, attiecībā uz datu minimizēšanu, datu ierobežotu saglabāšanu, drošības pasākumiem un sūdzību izskatīšanu ([40]). Tādējādi fiziskas personas joprojām var iesniegt sūdzību *PIPC*, ja šie principi un pienākumi netiek ievēroti, un *PIPC* ir pilnvarota veikt izpildes pasākumus, ja tie netiek ievēroti.

([35]) Sk. konkrēti *PIPA* 18. panta 2. punktu un VI nodaļu.

([36]) Informācijas pakalpojumi ietver gan informācijas sniegšanu, gan starpniecības pakalpojumus informācijas sniegšanai.

([37]) Sk. Tīkla likuma 2. panta 1. punkta 3. apakšpunktu (kopā ar 2. panta 1. punkta 2. un 4. apakšpunktu) un Telesakaru darījumdarbības likuma 2. panta 6. un 8. punktu.

([38]) Ciktāl Korejas informācijas un komunikācijas pakalpojumu sniedzējiem būtu tieša saistība ar personām ES (piedāvājot tiešsaistes pakalpojumus), tas varētu izraisīt Regulas (ES) 2016/679 tiešu piemērošanu saskaņā ar tās 3. panta 2. punkta a) apakšpunktu.

([39]) Turklāt *PIPA* 58. panta 2. punktā noteikts, ka 15. pants, 22. pants, 27. panta 1.–2. punkts, 34. un 37. pants neattiecas uz personas informāciju, ko apstrādā, izmantojot vizuālās datu apstrādes ierīces, kuras uzstādītas un darbojas atklātās vietās. Tā kā šis noteikums attiecas uz videonovērošanas izmantošanu Korejā, t. i., personas informācijas tiešu vākšanu no personām Korejā, tas nav būtisks šā lēmuma nolūka izpratnē, jo tas attiecas uz personas datu nosūtīšanu no pārziņiem/apstrādātājiem ES uz vienībām Korejā. Turklāt saskaņā ar *PIPA* 58. panta 3. punktu 15. pants (personas informācijas vākšana un izmantošana), 30. pants (pienākums ieviest publisku privātuma politiku) un 31. pants (pienākums iecelt privātuma amatpersonu) neattiecas uz personas informāciju, kas tiek apstrādāta, lai darbotos sadraudzības grupās vai apvienībās (piemēram, interešu klubos). Tā kā šādas grupas tiek uzskatītas par personiska rakstura grupām, kas nav saistītas ar profesionālu vai komerciālu darbību, nav nepieciešams īpašs juridiskais pamats (piemēram, attiecīgo personu piekrišana), lai šajā saistībā vāktu un izmantotu to informāciju. Tomēr visi pārējie *PIPA* noteikumi (piemēram, datu minimizēšana, nolūka ierobežojums, apstrādes likumīgums, drošība un individuālās tiesības) paliek spēkā. Turklāt izņēmums neattiektos uz tādu personas informācijas apstrādi, kas pārsniedz sociālās grupas izveides nolūku.

([40]) Konkrētāk, *PIPA* 58. panta 4. punktā ir noteikts pienākums apstrādāt personas informāciju minimālā apjomā, kas nepieciešams, lai sasniegtu paredzēto nolūku, apstrādāt to minimāli ilgu laiku un veikt nepieciešamos pasākumus šādas personas informācijas drošai pārvaldībai un pienācīgai apstrādei. Tie ietver tehniskus pārvaldības un fiziskus aizsardzības pasākumus, kā arī pasākumus, kas paredzēti, lai nodrošinātu individuālu sūdzību pienācīgu izskatīšanu.

(27) Pirmkārt, daļējais atbrīvojums attiecas uz personas datiem, kas savākti saskaņā ar Statistikas likumu, lai tos apstrādātu publiskās iestādes. Saskaņā ar skaidrojumiem, kas saņemti no Korejas valdības, šajā saistībā apstrādātie personas dati parasti attiecas uz Korejas valstspiederīgajiem un tikai izņēmuma kārtā var ietvert informāciju par ārvalstniekiem, proti, statistiku par ieceļošanu un izceļošanu no valsts teritorijas vai par ārvalstu ieguldījumiem. Tomēr pat šādās situācijās šādi dati parasti netiek nosūtīti no Savienībā esošiem pārziņiem/apstrādātājiem, bet drīzāk tos vāc tieši Korejas publiskās iestādes ([41]). Turklāt līdzīgi tam, kas norādīts Regulas (ES) 2016/679 162. apsvērumā, uz datu apstrādi saskaņā ar Statistikas likumu attiecas vairāki nosacījumi un garantijas. Jo īpaši Statistikas likumā paredzēti konkrēti pienākumi, piemēram, nodrošināt precizitāti, konsekvenci un objektivitāti; garantēt personu konfidencialitāti; aizsargāt informāciju par respondentiem, kas atbild uz statistikas pieprasījumiem, tai skaitā, lai novērstu šādas informācijas izmantošanu citiem nolūkiem, kas nav statistikas apkopošana, un attiecināt uz darbiniekiem konfidencialitātes prasības ([42]). Publiskām iestādēm, kuras apstrādā datus, cita starpā ir jāievēro datu minimizēšanas, datu izmantošanas mērķa ierobežojuma un drošības principi (*PIPA* 3. pants un 58. panta 4. punkts) un jāļauj personām īstenot savas tiesības (tiesības uz piekļuvi datiem, to labošanu, dzēšanu un piekļuves apturēšanu, sk. *PIPA* 4. pantu). Visbeidzot, dati ir jāapstrādā anonimizētā vai pseidonimizētā formā, ja tas ļauj īstenot apstrādes nolūku (*PIPA* 3. panta 7. punkts).

(28) Otrkārt, *PIPA* 58. panta 1. punkts attiecas uz personas datiem, kas savākti vai pieprasīti ar valsts drošību saistītas informācijas analīzei. Šā daļējā atbrīvojuma darbības joma un sekas ir sīkāk aprakstītas 149. apsvērumā.

(29) Treškārt, daļējs atbrīvojums attiecas uz personas datiem, kas tiek apstrādāti uz laiku, ja tas ir steidzami nepieciešams sabiedrības drošumam un sabiedriskajai drošībai, tai skaitā sabiedrības veselībai. *PIPC* šo kategoriju interpretē stingri, un saskaņā ar saņemto informāciju tā nekad nav izmantota. To piemēro tikai ārkārtas situācijās, kad nepieciešama steidzama rīcība, piemēram, lai izsekotu infekcijas ierosinātājus vai lai glābtu un palīdzētu dabas katastrofu upuriem ([43]). Pat šajās situācijās daļējais atbrīvojums attiecas tikai uz personas datu apstrādi uz ierobežotu laiku ar nolūku veikt minētās darbības. Vēl retāki ir gadījumi, kad atbrīvojums varētu attiekties uz tādu datu nosūtīšanu, uz kuriem attiecas šis lēmums, ņemot vērā nelielo varbūtību, ka personas dati, kas no Savienības nosūtīti Korejas operatoriem, būtu tāda veida dati, kuru turpmāka apstrāde varētu būt "steidzami nepieciešama" šādu ārkārtas situāciju gadījumā.

(30) Visbeidzot, daļējs atbrīvojums attiecas uz personas datiem, ko vāc vai izmanto prese, reliģiskās organizācijas (misionāru darbību nolūkā) vai politiskās partijas (kandidātu izvirzīšanai). Atbrīvojums attiecas tikai uz gadījumiem, kad personas datus apstrādā prese, reliģiskās organizācijas vai politiskās partijas šiem konkrētajiem nolūkiem (t. i., žurnālistikas darbībām, misionāru darbam un politisko kandidātu izvirzīšanai). Ja šīs vienības personas datus apstrādā citiem nolūkiem, piemēram, cilvēkresursu pārvaldībai vai iekšējai administrācijai, *PIPA* ir piemērojams pilnā apmērā.

(31) Attiecībā uz preses veikto personas datu apstrādi žurnālistikas darbībām līdzsvaru starp vārda brīvību un citām tiesībām (tostarp tiesībām uz privātumu) nodrošina Likums par šķīrējtiesu un tiesiskās aizsardzības līdzekļiem u. c. saistībā ar preses reportāžu radīto kaitējumu ("Preses likums") ([44]). Konkrēti, Preses likuma 5. pantā noteikts, ka prese (t. i., jebkura raidorganizācija, laikraksts, periodiskais izdevums vai tiešsaistes laikraksts), jebkurš interneta ziņu dienests vai jebkura interneta multimediju raidorganizācija nedrīkst aizskart personu privātumu. Ja privātuma pārkāpums tomēr ir noticis, tas nekavējoties jānovērš saskaņā ar likumā noteiktajām īpašajām procedūrām. Šajā ziņā likums personām, kurām ir nodarīts kaitējums preses ziņojuma dēļ, piešķir vairākas tiesības, piemēram,

([41]) Šajā sakarā Statistikas likuma 33. pantā publiskajām iestādēm ir paredzēts pienākums aizsargāt informāciju par respondentiem, kas atbild uz statistikas pieprasījumiem, tai skaitā nepieļaut, ka šāda informācija tiek izmantota citiem nolūkiem, nevis statistikas apkopošanai.

([42]) Statistikas likuma 2. panta 2.–3. punkts, 30. panta 2. punkts, 33. un 34. pants.

([43]) *PIPA* rokasgrāmatas iedaļa par 58. pantu.

([44]) Piemēram, Preses likuma 4. pantā noteikts, ka preses ziņojumiem jābūt objektīviem un taisnīgiem, sabiedrības interesēs, jārespektē cilvēka cieņa un vērtība un ka tie nedrīkst nedz ietekmēt citas personas, nedz pārkāpt viņu tiesības, sabiedrības morāli vai sociālo ētiku.

panākt nepatiesa paziņojuma labojuma publicēšanu, panākt labojumu ar pretēju apgalvojumu vai papildu ziņojumu (ja preses ziņojums attiecas uz apgalvojumiem par noziegumiem, par kuriem persona vēlāk tiek attaisnota) ([45]). Personu sūdzības preses izdevumi var risināt tieši (ar ombuda starpniecību) ([46]), samierināšanas tiesas vai šķīrējtiesas ceļā (specializētā Preses šķīrējtiesas komisijā) ([47]) vai tiesā. Personas var saņemt kompensāciju arī tad, ja preses nelikumīgas darbības (tīši vai aiz neuzmanības) dēļ tām nodarīts finansiāls kaitējums, aizskartas personības tiesības vai radītas citas emocionālas ciešanas ([48]). Prese saskaņā ar likumu ir atbrīvota no atbildības, ciktāl preses ziņojums, kas pārkāpj personas tiesības, nav pretrunā ar sociālajām vērtībām un tiek publicēts vai nu ar attiecīgās personas piekrišanu, vai sabiedrības interesēs (un ir pietiekams pamats uzskatīt, ka ziņojums atbilst patiesībai) ([49]).

(32) Tādējādi uz preses veikto personas datu apstrādi žurnālistikas darbībām attiecas īpašas garantijas, kas izriet no Preses likuma, taču nav šādu papildu garantiju, kas regulētu izņēmumu piemērošanu attiecībā uz reliģisko organizāciju un politisko partiju veiktajām apstrādes darbībām tādā veidā, kas ir salīdzināms ar Regulas (ES) 2016/679 85., 89. un 91. pantu. Tāpēc Komisija uzskata, ka ir lietderīgi reliģiskās organizācijas, ciktāl tās apstrādā personas datus savām misionāru darbībām, un politiskās partijas, ciktāl tās apstrādā personas datus saistībā ar kandidātu izvirzīšanu, izslēgt no šā lēmuma piemērošanas jomas.

2.3. **Garantijas, tiesības un pienākumi**

2.3.1. *Apstrādes likumīgums un godprātība*

(33) Personas dati ir jāapstrādā likumīgi un godprātīgi.

(34) Šis princips ir noteikts *PIPA* 3. panta 1. un 2. punktā, un to pastiprina *PIPA* 59. pants, kas aizliedz personas datu apstrādi "ar krāpšanu, nepienācīgiem vai netaisnīgiem līdzekļiem", "bez likumīgas pilnvaras" vai "pārsniedzot atbilstīgas pilnvaras" ([50]). Šie likumīgās apstrādes vispārējie principi ir izklāstīti *PIPA* 15.–19. pantā, kurā noteikti dažādi apstrādes juridiskie pamati (datu vākšana, izmantošana un sniegšana trešām personām), tostarp apstākļi, kādos tā var būt saistīta ar nolūka maiņu (*PIPA* 18. pants).

([45]) Preses likuma 15.–17. pants.

([46]) Katram preses vai mediju avotam ir jābūt savam ombudam, lai novērstu un labotu jebkādu iespējamo preses radīto kaitējumu (piemēram, iesakot labot nepatiesus vai citu personu reputāciju graujošus preses ziņojumus); sk. Preses likuma 6. pantu.

([47]) Komisijas sastāvā ir no 40 līdz 90 šķīrējtiesas komisāriem, kurus ieceļ kultūras, sporta un tūrisma ministrs, izraugoties starp personām, kas kvalificētas kā tiesneši, zvērināti advokāti, personām, kas vismaz 10 gadus nodarbojas ar ziņu vākšanu vai izziņošanu, vai citām ar preses nozari saistītām personām. Šķīrējtiesas komisāri vienlaikus nevar būt valsts amatpersonas, politisko partiju biedri vai žurnālisti. Saskaņā ar Preses likuma 8. pantu šķīrējtiesas komisāri savus pienākumus veic neatkarīgi un saistībā ar šiem pienākumiem viņiem nedrīkst dot nekādus norādījumus vai instrukcijas. Turklāt ir ieviesti īpaši noteikumi, lai novērstu interešu konfliktus, piemēram, liedzot atsevišķiem komisāriem izskatīt lietas, kurās iesaistīts viņu laulātais vai radinieki (Preses likuma 10. pants). Komisija var izskatīt strīdus samierināšanas tiesas vai šķīrējtiesas ceļā, kā arī var sniegt ieteikumus pārkāpumu novēršanai (Preses likuma 5. pants).

([48]) Preses likuma 30. pants.

([49]) Preses likuma 5. pants.

([50]) *PIPA* 59. pants aizliedz jebkurai personai, "kas apstrādā vai jebkad ir apstrādājusi personas informāciju", "iegūt personas informāciju vai piekrišanu personas informācijas apstrādei ar krāpšanu, nepienācīgiem vai netaisnīgiem līdzekļiem", "izpaust darījumdarbības gaitā iegūto personas informāciju vai bez pilnvarojuma nodot tos trešās personas lietošanai" vai "bojāt, iznīcināt, pārveidot, viltot vai izpaust citu personu personas informāciju bez likumīgas pilnvaras vai pārsniedzot atbilstīgas pilnvaras". Par šā aizlieguma pārkāpšanu var piemērot krimināLsodus (skatīt *PIPA* 71. panta 5. un 6. punktu un 72. panta 2. punktu). Turklāt *PIPA* 70. panta 2. punkts ļauj piemērot kriminālsodu par tādas personas informācijas iegūšanu, ko trešās personas apstrādā ar krāpšanu vai citiem netaisnīgiem līdzekļiem vai metodēm, vai par tās sniegšanu trešai personai peļņas gūšanas vai negodīgos nolūkos, kā arī par šādas rīcības atbalstīšanu vai organizēšanu.

(35) Saskaņā ar *PIPA* 15. panta 1. punktu pārzinis var vākt personas datus (saskaņā ar datu vākšanas nolūku), pamatojoties tikai uz ierobežotu skaitu juridisko pamatojumu. Tie ir šādi: 1) datu subjekta piekrišana ([51]) (1. punkts); 2) nepieciešamība noslēgt un izpildīt līgumu ar datu subjektu (4. punkts); 3) īpašs likumā noteikts pilnvarojums vai nepieciešamība izpildīt juridisku pienākumu (2. punkts); publiskās iestādes nepieciešamība ([52]) veikt tās jurisdikcijā esošos uzdevumus, kā noteikts tiesību aktos; 4) acīm redzama nepieciešamība datu subjekta vai trešās personas dzīvības, veselības vai īpašuma aizsardzībai pret nenovēršamu apdraudējumu (tikai tad, ja datu subjekts nespēj paust savu gribu vai nav iespējams saņemt iepriekšēju piekrišanu) (5. punkts); 5) nepieciešamība īstenot pārziņa "pamatotas intereses", ja tās ir "acīm redzami svarīgākas" par datu subjekta interesēm (un tikai tad, ja apstrādei ir "būtiska saikne" ar leģitīmajām interesēm un tā nepārsniedz to, kas ir saprātīga) (6. punkts) ([53]). Šie apstrādes pamatojumi pēc būtības ir līdzvērtīgi Regulas (ES) 2016/679 6. pantā noteiktajiem pamatojumiem, tai skaitā pamatojums "pamatotas intereses", kas ir līdzvērtīgs Regulas (ES) 2016/679 6. panta 1. punkta f) apakšpunktā noteiktajam pamatojumam "leģitīmas intereses".

(36) Kad personas dati ir savākti, tos var izmantot vākšanas nolūka ietvaros (*PIPA* 15. panta 1. punkts) vai ar vākšanas nolūku "pamatoti saistītā apjomā", ņemot vērā iespējamo datu subjektam radīto nelabvēlīgo situāciju un ar nosacījumu, ka ir pieņemti nepieciešamie drošības pasākumi (piemēram, šifrēšana) (*PIPA* 15. panta 3. punkts). Lai noteiktu, vai izmantošanas nolūks ir "pamatoti saistīts" ar sākotnējo vākšanas nolūku, Izpildes dekrētā ir noteikti konkrēti kritēriji, kas ir līdzīgi Regulas (ES) 2016/679 6. panta 4. punktā noteiktajiem. Konkrēti, tam jābūt būtiski saistītam ar sākotnējo nolūku; papildu izmantošanai jābūt paredzamai (piemēram, ņemot vērā apstākļus, kādos informācija tika vākta); un, ja iespējams, datiem jābūt pseidonimizētiem ([54]). Konkrētie kritēriji, ko šajā novērtējumā izmanto pārzinis, iepriekš jāizklāsta privātuma politikā ([55]). Turklāt privātuma amatpersonai (sk. 94. apsvērumu) ir īpaši jāpārbauda, vai turpmākā izmantošana notiek saskaņā ar šiem parametriem.

([51]) Piekrišana ir jādod brīvi, apzināti, konkrēti un jāizsaka vienā no vairākiem likumā noteiktajiem veidiem. Jebkurā gadījumā piekrišanu nedrīkst iegūt ar krāpšanu, nepienācīgiem vai citādi netaisnīgiem līdzekļiem (*PIPA* 59. panta 1. punkts). Pirmkārt, saskaņā ar *PIPA* 4. panta 2. punktu datu subjektiem ir tiesības "piekrist vai nepiekrist" un "izvēlēties piekrišanas apmēru", un viņi par to būtu jāinformē (*PIPA* 15. panta 2. punkts, 16. panta 2. un 3. punkts, 17. panta 2. punkts un 18. panta 3. punkts). *PIPA* 22. panta 5. punktā ir ietverts papildu aizsargpasākums, aizliedzot pārzinim liegt preču piegādi vai pakalpojumu sniegšanu, ja tas varētu apdraudēt personas brīvu izvēli dot piekrišanu. Tas ietver situācijas, kad tikai noteikta veida apstrādei ir nepieciešama piekrišana (savukārt pārējiem apstrādes veidiem pamatā ir līgums), un tas attiecas arī uz tādu personas datu turpmāku apstrādi, kas savākti saistībā ar preču piegādi vai pakalpojumu sniegšanu. Otrkārt, saskaņā ar *PIPA* 15. panta 2. punktu, 17. panta 2. un 3. punktu un 18. panta 3. punktu, pieprasot piekrišanu, pārzinim ir jāsniedz datu subjektam informācija par attiecīgajiem personas datiem (piemēram, ka tie ir sensitīvi dati, sk. *PIPA* Izpildes dekrēta 17. panta 2. punkta 2.a) apakšpunktu), apstrādes nolūku, saglabāšanas laikposmu un datu saņēmēju. Jebkuru šādu pieprasījumu iesniedz "skaidri atpazīstamā veidā", kas atšķir jautājumus, kuriem nepieciešama piekrišana, no citiem jautājumiem (*PIPA* 22. panta 1.–4. punkts). Treškārt, *PIPA* Izpildes dekrēta 17. panta 1. punkta 1-6. apakšpunktā ir noteiktas konkrētas metodes, ar kādām pārzinim ir jāsaņem piekrišana, piemēram, rakstveida piekrišana ar datu subjekta parakstu vai piekrišana, nosūtot (atbildes) e-pastu. Lai gan *PIPA* konkrēti nepiešķir personām vispārējas tiesības atsaukt piekrišanu, personām tomēr ir tiesības apturēt ar viņām saistīto datu apstrādi, kuru īstenošanas rezultātā datu apstrādi pārtrauc un datus dzēš (sk. 78. apsvērumu par tiesībām uz apturēšanu).

([52]) Saskaņā ar informāciju, kas saņemta no *PIPC*, publiskās iestādes var atsaukties uz šo pamatojumu tikai tad, ja personas informācijas apstrāde ir nenovēršama, t. i., iestādei nav iespējams vai ir pārmērīgi sarežģīti veikt savas funkcijas bez datu apstrādes.

([53]) *PIPA* 39-3. pants uzliek īpašus (stingrākus) pienākumus informācijas un komunikācijas pakalpojumu sniedzējiem attiecībā uz lietotāju personas informācijas vākšanu un izmantošanu. Jo īpaši tas paredz, ka pakalpojumu sniedzējam ir jāsaņem lietotāja piekrišana pēc tam, kad ir sniegta informācija par personas informācijas vākšanas/izmantošanas nolūku, par apkopojamās personas informācijas kategorijām un laikposmu, kurā informācija tiks apstrādāta (*PIPA* 39-3. panta 1. punkts). Tas pats attiecas uz gadījumiem, kad mainās kāds no šiem aspektiem. Par informācijas vākšanu bez piekrišanas saņemšanas draud krimināls ods (*PIPA* 71. panta 4-5. punkts). Izņēmuma kārtā informācijas un komunikācijas pakalpojumu sniedzēji var vākt vai izmantot lietotāju personas informāciju bez iepriekšējas piekrišanas saņemšanas. Tas attiecas uz šādiem gadījumiem: 1) kad ekonomisku un tehnoloģisku iemeslu dēļ ir acīm redzami grūti iegūt parastu piekrišanu attiecībā uz personas informāciju, kas vajadzīga, lai izpildītu līgumu, kurš reglamentē informācijas un komunikācijas pakalpojumu sniegšanu (piemēram, ja līguma izpildes procesā neizbēgami tiek radīti personas dati, piemēram, norēķinu informācija, piekļuves reģistri un maksājumu ieraksti); 2) ja tas nepieciešams, lai nokārtotu maksājumus pēc informācijas un komunikācijas pakalpojumu sniegšanas; vai 3) ja to atļauj citi tiesību akti (piemēram, Likuma par patērētāju aizsardzību elektroniskajā komercijā 21. panta 1. punkta 6. apakšpunktā noteikts, ka uzņēmēji var vākt personas informāciju par nepilngadīgas personas likumiskajiem aizbildņiem, lai pārliecinātos, vai nepilngadīgās personas vārdā ir saņemta derīga piekrišana) (*PIPA* 39-3. panta 2. punkts). Jebkurā gadījumā informācijas un komunikācijas pakalpojumu sniedzēji nedrīkst atteikties sniegt pakalpojumus tikai tāpēc, ka lietotājs nesniedz vairāk personas informācijas nekā minimāli nepieciešamo (t. i., informācija, kas nepieciešama attiecīgā pakalpojuma būtisku elementu izpildei), sk. *PIPA* 39-3. panta 3. punktu.

([54]) Sk. *PIPA* Izpildes dekrēta 14-2. pantu.

([55]) *PIPA* Izpildes dekrēta 14-2. panta 2. punkts.

(37) Līdzīgi (bet nedaudz stingrāki) noteikumi attiecas uz datu sniegšanu trešām personām. Saskaņā ar *PIPA* 17. panta 1. punktu personas datu sniegšana trešai personai ir atļauta, pamatojoties uz piekrišanu ([56]), vai, ņemot vērā informācijas vākšanas nolūku, ja informācija ir vākta, pamatojoties uz kādu no *PIPA* 15. panta 1. punkta 2., 3. un 5. apakšpunktā minētajiem juridiskajiem pamatojumiem. Tas konkrēti izslēdz jebkādu informācijas izpaušanu, pamatojoties uz pārziņa "pamatotām interesēm". Papildus tam saskaņā ar *PIPA* 17. panta 4. punktu ir atļauta informācijas sniegšana trešām personām ar vākšanas nolūku "pamatoti saistītā apjomā", ņemot vērā arī iespējamo datu subjektam radīto nelabvēlīgo situāciju un ar nosacījumu, ka ir pieņemti nepieciešamie drošības pasākumi (piemēram, šifrēšana). Jāņem vērā tie paši faktori, kas aprakstīti 36. apsvērumā, lai novērtētu, vai noteikums ietilpst apjomā, kas ir pamatoti saistīts ar vākšanas nolūku, un jāpiemēro tās pašas garantijas (t. i., attiecībā uz pārredzamību, izmantojot privātuma politiku un privātuma amatpersonas iesaistīšanu).

(38) Ja Korejas datu pārzinis saņem no Savienības personas datus, tas tiek uzskatīts par "vākšanu" *PIPA* 15. panta nozīmē. Paziņojumā Nr. 2021-5 (šā lēmuma I pielikuma I iedaļa) ir paskaidrots, ka nolūks, kādam attiecīgā ES vienība ir nosūtījusi datus, ir Korejas datu pārziņa datu vākšanas nolūks. Līdz ar to Korejas datu pārziņiem, kas saņem personas datus no Savienības, principā ir jāapstrādā šāda informācija saskaņā ar *PIPA* 17. pantu, ievērojot nosūtīšanas nolūku.

(39) Īpaši ierobežojumi attiecas uz gadījumiem, kad pārzinis vēlas izmantot personas datus vai sniegt tos trešai personai citam nolūkam, kas atšķiras no datu vākšanas nolūka ([57]). Saskaņā ar *PIPA* 18. panta 2. punktu privāts pārzinis var izņēmuma kārtā ([58]) izmantot personas datus vai sniegt tos trešai personai citam nolūkam: 1) pamatojoties uz datu subjekta papildu (t. i., atsevišķu) piekrišanu; 2) ja to paredz īpaši tiesību akti; vai 3) ja tas ir acīm redzami nepieciešams datu subjekta vai trešās personas dzīvības, veselības vai īpašuma aizsardzībai pret nenovēršamu apdraudējumu (tikai tad, ja datu subjekts nespēj paust savu gribu un nav iespējams saņemt iepriekšēju piekrišanu) ([59]).

(40) Publiskās iestādes noteiktās situācijās var arī izmantot personas datus vai sniegt tos trešai personai citam nolūkam. Tas attiecas arī uz gadījumiem, kad pretējā gadījumā publiskajām iestādēm būtu neiespējami pildīt savus likumā noteiktos pienākumus, kā to paredz tiesību akti, ja ir saņemta *PIPC* atļauja. Turklāt publiskās iestādes var sniegt personas datus citai iestādei vai tiesai, ja tas ir nepieciešams noziegumu izmeklēšanai un kriminālvajāšanai vai apsūdzības izvirzīšanai; lai tiesa varētu veikt savas funkcijas, kas saistītas ar notiekošo tiesvedību; vai krimināls oda izpildei, vai rīkojuma par aprūpi vai aizgādības izpildei ([60]). Tās var arī sniegt personas datus ārvalstu valdībai vai starptautiskai organizācijai, lai izpildītu juridisku pienākumu, kas izriet no līguma vai starptautiskas konvencijas, un šādā gadījumā tām arī ir jāievēro pārrobežu datu nosūtīšanas prasības (sk. 90. apsvērumu).

(41) Tādējādi Korejas tiesiskajā regulējumā apstrādes likumīguma un godprātības principi ir īstenoti pēc būtības līdzvērtīgi Regulai (ES) 2016/679, atļaujot veikt apstrādi tikai ar likumīgu un skaidri noteiktu pamatojumu. Turklāt visos minētajos gadījumos apstrāde ir atļauta tikai tad, ja nav iespējams "negodīgi aizskart" datu subjekta vai trešās personas intereses, kas prasa interešu līdzsvarošanu. Turklāt *PIPA* 18. panta 5. punktā ir paredzētas papildu garantijas, ja pārzinis sniedz personas datus trešai personai, un tie var ietvert prasību ierobežot izmantošanas nolūku un metodi vai ieviest īpašus drošības pasākumus. Savukārt trešai pusei ir jāīsteno pieprasītie pasākumi.

([56]) Par *PIPA* 17. panta 1. punkta 1. apakšpunkta pārkāpumiem var piemērot kriminālsodus (*PIPA* 71. panta 1. punkts).

([57]) "Paredzētais nolūks" ir nolūks, kādam informācija tika vākta. Piemēram, ja informācija tiek vākta, pamatojoties uz attiecīgās personas piekrišanu, paredzētais nolūks ir nolūks, kas tiek paziņots personai saskaņā ar *PIPA* 15. panta 2. punktu.

([58]) Sk. *PIPA* 18. panta 1. punktu. Par *PIPA* 18. panta 1. un 2. punkta pārkāpumiem var piemērot kriminālsodus (*PIPA* 71. panta 2. punkts).

([59]) Informācijas un komunikācijas pakalpojumu sniedzēji var izmantot personas informāciju vai sniegt to trešai personai citam nolūkam, kas atšķiras no sākotnējā nolūka, tikai *PIPA* 18. panta 2. punkta 1. un 2. apakšpunktā izklāstīto pamatojumu dēļ (t. i., ja ir saņemta papildu piekrišana vai ja tiesību aktos ir paredzēti īpaši noteikumi). Sk. *PIPA* 18. panta 2. punktu.

([60]) Izņemot gadījumus, kad apstrāde ir nepieciešama noziegumu izmeklēšanai, apsūdzības izvirzīšanai un kriminālvajāšanai, publiskajām iestādēm, kas izmanto personas informāciju vai sniedz to trešai personai citam nolūkam, kas atšķiras no vākšanas nolūka (piemēram, ja tas ir īpaši atļauts ar likumu vai nepieciešams līguma izpildei), ir jāpublicē apstrādes juridiskie pamatojumi, nolūks un apjoms savā tīmekļa vietnē vai Oficiālajā Vēstnesī un jāveic uzskaite (*PIPA* 18. panta 4. punkts kopā ar PIPA Izpildes dekrēta 15. pantu).

(42) Visbeidzot, *PIPA* 28-2. pants atļauj (turpmāku) pseidonimizētas informācijas apstrādi bez attiecīgās personas piekrišanas statistikas, zinātniskās pētniecības ([61]) un arhivēšanas nolūkos sabiedrības interesēs, ievērojot īpašas garantijas. Līdzīgi kā Regulā (ES) 2016/679 ([62]) *PIPA* tādējādi atvieglo personas datu (turpmāku) apstrādi šādos nolūkos saskaņā ar regulējumu, kas paredz atbilstošas garantijas, lai aizsargātu personu tiesības. Tā vietā, lai paļautos uz pseidonimizāciju kā iespējamo aizsardzības līdzekli, *PIPA* to nosaka kā priekšnosacījumu, lai veiktu noteiktas apstrādes darbības statistikas, zinātniskās pētniecības un arhivēšanas nolūkos sabiedrības interesēs (piemēram, lai varētu apstrādāt datus bez piekrišanas vai apvienot dažādas datu kopas).

(43) Turklāt *PIPA* noteiktas vairākas īpašas garantijas, konkrēti attiecībā uz nepieciešamajiem tehniskajiem un organizatoriskajiem pasākumiem, uzskaiti, datu kopīgas lietošanas ierobežojumiem un iespējamo atkārtotas identificēšanas risku novēršanu. 44.–48. apsvērumā aprakstīto dažādo garantiju apvienojums nodrošina, ka personas datu apstrādei šajā saistībā piemēro pēc būtības līdzvērtīgu aizsardzību salīdzinājumā ar aizsardzību, kas būtu nepieciešama saskaņā ar Regulu (ES) 2016/679.

(44) Pirmkārt, un pats svarīgākais ir tas, ka *PIPA* 28-5. panta 1. punkts aizliedz apstrādāt pseidonimizētu informāciju konkrētas personas identificēšanas nolūkā. Ja, apstrādājot pseidonimizētu informāciju, tomēr tiktu iegūta informācija, ar ko varētu identificēt personu, pārzinim nekavējoties jāaptur apstrāde un šāda informācija jāiznīcina (*PIPA* 28-5. panta 2. punkts). Par šo noteikumu neievērošanu var tikt piemērots administratīvs naudas sods, un tas ir uzskatāms par noziedzīgu nodarījumu ([63]). Tas nozīmē, ka pat tajās situācijās, kad būtu *praktiski* iespējams atkārtoti identificēt personu, šāda atkārtota identificēšana ir *juridiski* aizliegta.

(45) Otrkārt, veicot (turpmāku) pseidonimizētas informācijas apstrādi šādos nolūkos, pārzinim ir jāievieš īpaši tehniski, pārvaldības un fiziski pasākumi, lai nodrošinātu informācijas drošību (tostarp atsevišķi jāglabā un jāpārvalda informācija, kas nepieciešama, lai atjaunotu pseidonimizēto informāciju tās sākotnējā stāvoklī) ([64]). Turklāt ir jāreģistrē apstrādātā pseidonimizētā informācija, tās apstrādes nolūks, izmantošanas vēsture un visi trešās personas saņēmēji (*PIPA* Izpildes dekrēta 29-5. panta 2. punkts).

(46) Treškārt un visbeidzot, *PIPA* paredz īpašas garantijas, lai novērstu trešo personu veiktu personu identificēšanu gadījumos, kad informācija tiek kopīgota. Konkrēti, sniedzot pseidonimizētu informāciju trešai personai statistikas, zinātniskās pētniecības vai arhivēšanas nolūkos sabiedrības interesēs, pārziņi nedrīkst iekļaut informāciju, ko varētu izmantot, lai identificētu konkrētu personu (*PIPA* 28-2. panta 2. punkts) ([65]).

(47) Konkrētāk, lai gan *PIPA* ļauj apvienot pseidonimizētu informāciju (ko apstrādā dažādi pārziņi) statistikas, zinātniskās pētniecības vai arhivēšanas nolūkos sabiedrības interesēs, tas patur šīs pilnvaras specializētām iestādēm, kas aprīkotas ar īpašām drošības iekārtām (*PIPA* 28-3. panta 1. punkts) ([66]). Iesniedzot pieteikumu par pseidonimizētu datu apvienošanu, pārzinim cita starpā jāiesniedz dokumentācija par apvienojamiem datiem, apvienošanas

([61]) *PIPA* 2. panta 8. punktā zinātniskā pētniecība ir definēta kā "pētniecība, kurā izmanto zinātniskas metodes, piemēram, tehnoloģiju attīstība un demonstrējumi, fundamentālie pētījumi, lietišķie pētījumi un privāti finansēti pētījumi". Šīs kategorijas atbilst Regulas (ES) 2016/679 159. apsvērumā noteiktajām kategorijām.

([62]) Sk. Regulas (ES) 2016/679 5. panta 1. punkta b) apakšpunktu, 89. panta 1. un 2. punktu, kā arī 50. un 157. apsvērumu.

([63]) Sk. *PIPA* 28-6. panta 1. punktu, 71. panta 4-3. punktu un 75. panta 2. punkta 4-4. apakšpunktu.

([64]) *PIPA* 28-4. pants un *PIPA* Izpildes dekrēta 29-5. pants. Par šā pienākuma neievērošanu var piemērot administratīvus sodus un krimināsodus (sk. *PIPA* 73. panta 1. punktu un 75. panta 2. punkta 6. apakšpunktu).

([65]) Par šo prasību pārkāpumiem var piemērot krimināsodus (*PIPA* 71. panta 2. punkts). *PIPC* nekavējoties sāka piemērot šos jaunos noteikumus, piemēram, tās 2021. gada 28. aprīļa lēmumā, ar kuru tā piemēroja naudas sodu un korektīvos pasākumus uzņēmumam, kas līdztekus citiem *PIPA* pārkāpumiem neievēroja *PIPA* 28-2. panta 2. punkta prasību, sk. https://www.pipc.go.kr/np/cop/bbs/selectBoardArticle.do?bbsId=BS074&mCode=C020010000&nttId=7298&fbclid=IwAR3SKcMQi6G5pR9k4I7j6GNXtc8aBVDOwcURevvvzQtYI7AS40UKYXoOXo8

([66]) Lai pieteikuma iesniedzējs tiktu apstiprināts par šādu specializētu iestādi ("datu apvienošanas ekspertu aģentūru"), Personas informācijas aizsardzības komisijā ir jāiesniedz pieteikums kopā ar apliecinošiem dokumentiem, kuros cita starpā ir sīki izklāstītas iekārtas un aprīkojums, kas paredzēti drošai pseidonimizētu datu apvienošanai, un apliecinājums, ka pieteikuma iesniedzējs nodarbina vismaz trīs pilna laika darbiniekus ar kvalifikāciju vai pieredzi personas datu aizsardzības jomā (*PIPA* Izpildes dekrēta 29-2. panta 1.–2. punkts). Sīki izstrādātas prasības, piemēram, attiecībā uz personāla kvalifikāciju, pieejamajām iekārtām, drošības pasākumiem, iekšējo politiku un procedūrām, kā arī finansiālās prasības ir izklāstītas *PIPC* Paziņojumā Nr. 2020-09 par pseidonimizētas informācijas apvienošanu un publiskošanu (I pielikums). *PIPC* (pēc uzklausīšanas) var atsaukt datu apvienošanas ekspertu aģentūras apstiprinājumu noteiktu iemeslu dēļ, piemēram, ja aģentūra vairs neatbilst apstiprinājumam nepieciešamajiem drošības standartiem vai ja saistībā ar datu apvienošanu ir noticis datu aizsardzības pārkāpums (*PIPA* Izpildes dekrēta 29-2. panta 5.–6. punkts). *PIPC* ir jāpublicē ikviens datu apvienošanas ekspertu aģentūras apstiprinājums (vai apstiprinājuma atsaukšana) (*PIPA* Izpildes dekrēta 29-2. panta 7. punkts).

nolūku, kā arī ierosinātajiem drošības pasākumiem apvienoto datu apstrādei ([67]). Lai varētu veikt apvienošanu, pārzinim ir jānosūta apvienojamie dati specializētajai iestādei un jāiesniedz "apvienošanas atslēga" (t. i., informācija, kas izmantota pseidonimizācijai) Korejas Interneta un drošības aģentūrai ([68]). Aģentūra ģenerē "apvienošanas atslēgas sasaistes datus" (kas ļauj sasaistīt dažādu pieteikuma iesniedzēju apvienošanas atslēgas, lai panāktu datu kopu apvienošanu) un sniedz tos specializētajai iestādei ([69]).

(48) Pārzinis, kas pieprasa datu apvienošanu, var analizēt apvienoto informāciju specializētās iestādes telpās, vietā, kurā tiek piemēroti īpaši tehniski, fiziski un administratīvi drošības pasākumi (*PIPA* Izpildes dekrēta 29-3. pants). Pārziņi, kas sniedz datu kopu šādai apvienošanai, var nodot apvienotos datus ārpus specializētās iestādes tikai pēc apvienoto datu turpmākas pseidonimizācijas vai anonimizācijas un ar šīs iestādes apstiprinājumu (*PIPA* 28-3. panta 2. punkts) ([70]). Apsverot, vai piešķirt šādu apstiprinājumu, iestāde izvērtēs saikni starp apvienotajiem datiem un apstrādes nolūku un to, vai šādu datu izmantošanai ir izstrādāts īpašs drošības plāns ([71]). Apvienotās informācijas eksportēšana ārpus iestādes nebūs atļauta, ja informācija ietver datus, kas ļautu identificēt personu ([72]). Visbeidzot, specializētās iestādes veikto pseidonimizēto datu apvienošanu un publiskošanu uzrauga *PIPC* (*PIPA* Izpildes dekrēta 29-4. panta 3. punkts).

2.3.2. *Īpašu kategoriju personas datu apstrāde*

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

(50) *PIPA* ietver īpašus noteikumus attiecībā uz gadījumiem, kad tiek apstrādāti sensitīvi dati ([73]), kas ir definēti kā personas dati, kuri atklāj informāciju par personas ideoloģiju, pārliecību, iestāšanos vai izstāšanos no arodbiedrības vai politiskās partijas, politiskajiem uzskatiem, veselību un seksuālo dzīvi, kā arī cita personas informācija, kas var "ievērojami" apdraudēt datu subjekta privātumu un kas ar Prezidenta dekrētu ([74]) ir noteikta kā sensitīva informācija. Saskaņā ar *PIPC* sniegtajiem skaidrojumiem seksuālā dzīve tiek interpretēta arī kā personas seksuālā orientācija ([75]). Turklāt Izpildes dekrēta 18. pantā sensitīvo datu klāsts ir papildināts ar citām kategorijām, konkrēti, ar DNS informāciju, kas iegūta, veicot ģenētisko testēšanu, un sodāmības reģistrā iekļautajiem datiem. Ar nesenajiem grozījumiem *PIPA* Izpildes dekrētā ir vēl vairāk paplašināts sensitīvo datu jēdziens, iekļaujot tajā arī personas datus, kas atklāj rasi vai etnisko izcelsmi un biometrisko informāciju ([76]). Pēc minētā grozījuma sensitīvu datu jēdziens saskaņā ar *PIPA* pēc būtības ir līdzvērtīgs Regulas (ES) 2016/679 9. pantā minētajam.

(51) Saskaņā ar *PIPA* 23. panta 1. punktu un līdzīgi, kā noteikts Regulas (ES) 2016/679 9. panta 1. punktā, sensitīvu datu apstrāde parasti ir aizliegta, ja vien nepiemēro kādu no uzskaitītajiem izņēmumiem ([77]). Šie ierobežojumi attiecas tikai uz gadījumiem, kad pārzinis informē datu subjektu saskaņā ar *PIPA* 15. un 17. pantu un saņem atsevišķu piekrišanu (t. i., atsevišķi no piekrišanas citu personas datu apstrādei) vai kad apstrādi prasa vai atļauj likums. Publiskās iestādes var apstrādāt arī biometrisko informāciju, DNS informāciju, kas iegūta, veicot ģenētisko

([67]) Paziņojuma Nr. 2020-09 par pseidonimizētas informācijas apvienošanu un publiskošanu 8. panta 1.–2. punkts.
([68]) Paziņojuma Nr. 2020-09 par pseidonimizētas informācijas apvienošanu un publiskošanu 2. panta 3. un 6. punkts un 9. panta 1. punkts.
([69]) Paziņojuma Nr. 2020-09 par pseidonimizētas informācijas apvienošanu un publiskošanu 2. panta 4. punkts un 9. panta 2.–3. punkts. Pēc datu apvienošanas specializētajai iestādei nekavējoties jāiznīcina apvienošanas atslēgas sasaistes dati (Paziņojuma 9. panta 4. punkts).
([70]) Par datu kopu apvienošanas prasību pārkāpumiem var piemērot krimināsodus (*PIPA* 71. panta 4-2. punkts). Sk. arī *PIPA* Izpildes dekrēta 29-2. panta 4. punktu.
([71]) Apvienoto datu publiskošanas apstiprināšanas procedūra ir izklāstīta Paziņojuma Nr. 2020-9 par pseidonimizētas informācijas apvienošanu un publiskošanu 11. pantā. Konkrēti, specializētajai iestādei ir jāizveido "publiskošanas pārskatīšanas komiteja", kuras sastāvā ir locekļi ar plašām zināšanām un pieredzi datu aizsardzības jomā.
([72]) *PIPA* Izpildes dekrēta 29-2. panta 4. punkts un Paziņojuma Nr. 2020-9 11. pants.
([73]) Nepieciešamību nodrošināt īpašu aizsardzību sensitīvu datu, piemēram, datu par veselību vai seksuālo uzvedību, apstrādei ir atzinusi arī Korejas Konstitucionālā tiesa, sk. Konstitucionālās tiesas 2007. gada 31. maija Lēmumu Nr. *HunMa* 1139.
([74]) *PIPA* 23. panta 1. punkts.
([75]) Sk. arī *PIPA* rokasgrāmatas III nodaļas 2. iedaļu par 23. pantu (157.–164. lpp.).
([76]) Proti, personas informācija, kas iegūta, specifiski tehniski apstrādājot datus, kuri attiecas uz personas fiziskajām, fizioloģiskajām vai uzvedības īpašībām, lai unikāli identificētu šo personu.
([77]) Par šo prasību neievērošanu var piemērot sodus saskaņā ar *PIPA* 71. panta 3. punktu.

testēšanu, personas informāciju, kas atklāj rasi vai etnisko izcelsmi, un sodāmības reģistrā iekļautos datus, pamatojoties uz vienīgi šīm iestādēm pieejamajiem apsvērumiem (piemēram, ja tas nepieciešams noziegumu izmeklēšanai vai ja tas nepieciešams tiesai, lai turpinātu lietas izskatīšanu) ([78]). Tādējādi sensitīvu datu apstrādei pieejamie juridiskie pamati ir ierobežotāki nekā cita veida personas datu apstrādei, un Korejas tiesību aktos tie ir vēl ierobežojošāki nekā Regulas (ES) 2016/679 9. panta 2. punktā noteiktie.

(52) Turklāt *PIPA* 23. panta 2. punktā, par kura neievērošanu var tikt piemēroti sodi ([79]), ir uzsvērts, ka, apstrādājot sensitīvus datus, ir īpaši svarīgi nodrošināt pienācīgu drošību, lai tos "nevarētu pazaudēt, nozagt, izpaust, viltot, pārveidot vai bojāt". Lai gan tā ir vispārīga prasība saskaņā ar *PIPA* 29. pantu, 3. panta 4. punktā ir skaidri noteikts, ka drošības līmenis ir jāpielāgo apstrādājamo personas datu veidam, kas nozīmē, ka ir jāņem vērā īpašie riski, kas saistīti ar sensitīvu datu apstrādi. Turklāt datu apstrāde vienmēr jāveic "tā, lai līdz minimumam samazinātu iespēju pārkāpt" datu subjekta privātumu, un, ja iespējams, "anonīmi" (*PIPA* 3. panta 6. un 7. punkts). Šīs prasības ir īpaši svarīgas, ja apstrāde attiecas uz sensitīviem datiem.

2.3.3. *Nolūka ierobežojums*

(53) Personas dati būtu jāvāc konkrētam nolūkam un tādā veidā, kas nav pretrunā ar apstrādes nolūku.

(54) Šo principu īsteno saskaņā ar *PIPA* 3. panta 1. un 2. punktu, kurā noteikts, ka pārzinis "precizē un skaidri norāda" apstrādes nolūku, apstrādā personas datus piemērotā veidā, kas vajadzīgs šim nolūkam, un neizmanto tos ārpus šā nolūka. Nolūka ierobežojuma vispārējais princips ir apstiprināts arī 15. panta 1. punktā, 18. panta 1. punktā, 19. pantā un – attiecībā uz apstrādātājiem (tā dēvētajiem "ārpakalpojumu sniedzējiem") – *PIPA* 26. panta 1. punkta 1. apakšpunktā un 5. un 7. punktā. Konkrēti, personas datus principā drīkst izmantot un sniegt trešām personām tikai tā nolūka ietvaros, kādam tie tika vākti (15. panta 1. punkts un 17. panta 1. punkta 2. apakšpunkts). Apstrāde saderīgā nolūkā, t. i., "ar sākotnējo vākšanas nolūku pamatoti saistītā apjomā", var notikt tikai tad, ja tā negatīvi neietekmē attiecīgos datu subjektus un ja ir pieņemti nepieciešamie drošības pasākumi (piemēram, šifrēšana) (*PIPA* 15. panta 3. punkts un 17. panta 4. punkts). Lai noteiktu, vai turpmāka apstrāde atbilst saderīgam nolūkam, *PIPA* Izpildes dekrētā ir uzskaitīti konkrēti kritēriji, kas ir līdzīgi Regulas (ES) 2016/679 6. panta 4. punktā noteiktajiem kritērijiem, sk. 36. apsvērumu.

(55) Kā paskaidrots 38. apsvērumā, datu vākšanas nolūks gadījumā, kad Korejā esoši pārziņi saņem personas datus no Savienības, atbilst datu nosūtīšanas nolūkam. Pārzinim ir atļauts mainīt nolūku tikai izņēmuma kārtā, īpašos (uzskaitītos) gadījumos (*PIPA* 18. panta 2. punkta 1-3. apakšpunkts, sk. arī 39. apsvērumu). Ciktāl nolūka maiņa ir atļauta saskaņā ar tiesību aktiem, šādos tiesību aktos savukārt ir jāievēro pamattiesības uz privātumu un datu aizsardzību, kā arī Korejas Konstitūcijā noteiktie nepieciešamības un samērīguma principi. Turklāt *PIPA* 18. panta 2. un 5. punktā ir paredzētas papildu garantijas, jo īpaši prasība, ka šāda nolūka maiņa nedrīkst "negodīgi aizskart datu subjekta intereses", tādējādi vienmēr ir nepieciešams līdzsvarot intereses. Tas nodrošina aizsardzības līmeni, kas pēc būtības ir līdzvērtīgs aizsardzības līmenim, kurš noteikts Regulas (ES) 2016/679 5. panta 1. punkta b) apakšpunktā un 6. pantā saistībā ar 50. apsvērumu.

2.3.4. *Datu precizitāte un minimizēšana*

(56) Personas datiem vajadzētu būt precīziem un vajadzības gadījumā atjauninātiem. Tiem arī vajadzētu būt adekvātiem un atbilstīgiem, kā arī vajadzētu ietvert tikai to, kas nepieciešams tiem nolūkiem, kādiem tie tiek apstrādāti.

([78]) *PIPA* Izpildes dekrēta 18. pantā noteikts, ka tajā uzskaitītās datu kategorijas ir izslēgtas no Likuma 23. panta 1. punkta noteikumu piemērošanas jomas, ja tās apstrādā publiska iestāde saskaņā ar *PIPA* 18. panta 2. punkta 5.–9. apakšpunktu.

([79]) Sk. *PIPA* 73. panta 1. punktu un 75. panta 2. punkta 6. apakšpunktu.

(57) Precizitātes princips ir atzīts arī *PIPA* 3. panta 3. punktā, kurā noteikts, ka personas datiem jābūt "precīziem, pilnīgiem un atjauninātiem, ciktāl tas ir nepieciešams saistībā ar nolūkiem", kādiem dati tiek apstrādāti. Datu minimizēšana ir obligāta saskaņā ar *PIPA* 3. panta 1. un 6. punktu un 16. panta 1. punktu, kur noteikts, ka pārzinis vāc personas datus (tikai) "minimāli nepieciešamajā apjomā" paredzētajam nolūkam un ka tam šajā saistībā ir jāuzņemas pierādīšanas pienākums. Ja vākšanas nolūku ir iespējams īstenot, apstrādājot informāciju anonimizētā veidā, pārziņiem būtu jācenšas to darīt (*PIPA* 3. panta 7. punkts).

2.3.5. *Glabāšanas ierobežojums*

(58) Personas dati principā būtu jāglabā ne ilgāk, kā nepieciešams nolūkiem, kādos attiecīgos personas datus apstrādā.

(59) Glabāšanas ierobežojuma princips ir līdzīgi noteikts arī *PIPA* 21. panta 1. punktā ([80]), saskaņā ar kuru pārzinim ir pienākums "iznīcināt" ([81]) personas datus nekavējoties pēc apstrādes nolūka īstenošanas vai pēc saglabāšanas laikposma beigām (atkarībā no tā, kas notiek agrāk), ja vien turpmāka saglabāšana nav paredzēta likumā ([82]). Pēdējā gadījumā attiecīgie personas dati "tiek glabāti un pārvaldīti atsevišķi no citas informācijas par personu" (*PIPA* 21. panta 3. punkts).

(60) *PIPA* 21. panta 1. punktu nepiemēro, ja pseidonimizētus datus apstrādā statistikas, zinātniskās pētniecības vai arhivēšanas nolūkos sabiedrības interesēs ([83]). Lai arī šajā gadījumā nodrošinātu ierobežotas datu saglabāšanas principu, Paziņojumā Nr. 2021-5 noteikts, ka pārziņiem ir pienākums anonimizēt informāciju saskaņā ar PIPA 58-2. pantu, ja dati nav iznīcināti pēc tam, kad ir īstenots konkrētais apstrādes nolūks ([84]).

2.3.6. *Datu drošība*

(61) 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 tehniskie vai organizatoriskie pasākumi, lai aizsargātu personas datus no iespējamiem apdraudējumiem. Šie pasākumi būtu jāizvērtē, ņemot vērā jaunākos sasniegumus, saistītās izmaksas un apstrādes raksturu, apjomu, kontekstu un nolūkus, kā arī riskus attiecībā uz fizisku personu tiesībām.

(62) Līdzīgs drošības princips ir noteikts *PIPA* 3. panta 4. punktā, saskaņā ar kuru pārziņiem ir pienākums "droši pārvaldīt personas informāciju atbilstīgi personas informācijas apstrādes metodēm, veidiem utt., ņemot vērā datu subjektu tiesību pārkāpuma iespējamību un attiecīgo risku nopietnību". Turklāt pārzinis "apstrādā personas informāciju tā, lai līdz minimumam samazinātu iespēju pārkāpt datu subjekta privātumu", un šajā saistībā cenšas apstrādāt personas informāciju anonīmi vai, ja iespējams, pseidonimizētā veidā (*PIPA* 3. panta 6. un 7. punkts).

(63) Šīs vispārīgās prasības ir sīkāk izstrādātas *PIPA* 29. pantā, saskaņā ar kuru katrs pārzinis "veic tādus tehniskus, pārvaldības un fiziskus pasākumus, piemēram, izstrādā iekšējo pārvaldības plānu, saglabā pieteikšanās datus u. c., kas nepieciešami to drošībai, kā noteikts Prezidenta dekrētā, lai personas informāciju nevarētu pazaudēt, nozagt,

([80]) 8. pants (kopā ar Izpildes dekrēta 8-2. pantu), 11. pants (kopā ar Izpildes dekrēta 12. panta 2. punktu).

([81]) Par personas informācijas iznīcināšanas metodēm sk. *PIPA* Izpildes dekrēta 16. pantu. *PIPA* 21. panta 2. punktā precizēts, ka tas ietver "nepieciešamos pasākumus, lai bloķētu atgūšanu un atjaunošanu".

([82]) Par šo prasību neievērošanu var piemērot kriminālsodu (*PIPA* 73. panta 1.–2. punkts). *PIPA* 39-6. pantā ir noteikta papildu prasība informācijas un komunikācijas pakalpojumu sniedzējiem dzēst to lietotāju personas informāciju, kuri nav izmantojuši piedāvātos informācijas un komunikācijas pakalpojumus vismaz vienu gadu (ja vien tiesību aktos vai pēc personas pieprasījuma nav paredzēta turpmāka saglabāšana). Personas ir jāinformē par plānoto informācijas dzēšanu 30 dienas pirms viena gada termiņa beigām (*PIPA* 39-6. panta 2. punkts un *PIPA* Izpildes dekrēta 48-5. panta 3. punkts). Ja turpmāku saglabāšanu pieprasa tiesību akti, saglabātie dati ir jāglabā atsevišķi no citas lietotāju informācijas, un tos drīkst izmantot vai izpaust tikai saskaņā ar šiem tiesību aktiem (*PIPA* Izpildes dekrēta 48-5. panta 1.–2. punkts).

([83]) *PIPA* 28-7. pants.

([84]) Paziņojuma Nr. 2021-5 (I pielikums) 4. iedaļa.

izpaust, viltot, pārveidot vai sabojāt." *PIPA* Izpildes dekrēta 30. panta 1. punktā šie pasākumi ir precizēti, norādot uz 1) personas datu drošas apstrādes iekšējā pārvaldības plāna izstrādi un īstenošanu, 2) piekļuves kontroli un ierobežojumiem, 3) šifrēšanas tehnoloģiju ieviešanu, lai droši glabātu un nosūtītu personas datus, 4) pieteikšanās datiem, 5) drošības programmām un 6) fiziskiem pasākumiem, piemēram, drošu glabāšanas vai slēgšanas sistēmu ([85]).

(64) Turklāt datu aizsardzības pārkāpuma gadījumā tiek piemēroti konkrēti pienākumi (*PIPA* 34. pants kopā ar *PIPA* Izpildes dekrēta 39. un 40. pantu) ([86]). Konkrēti, pārzinim ir pienākums nekavējoties paziņot cietušajiem datu subjektiem sīkāku informāciju par pārkāpumu ([87]), tai skaitā informāciju par pārziņa veiktajiem (obligātajiem) pretpasākumiem un to, ko datu subjekti var darīt, lai mazinātu kaitējuma risku (*PIPA* 34. panta 1. un 2. punkts) ([88]). Ja datu aizsardzības pārkāpums attiecas uz vismaz 1 000 datu subjektiem, pārzinis par datu aizsardzības pārkāpumu un veiktajiem pretpasākumiem nekavējoties ziņo arī *PIPC* un Korejas Interneta un drošības aģentūrai, kas var sniegt tehnisko palīdzību (*PIPA* 34. panta 3. punkts kopā ar *PIPA* Izpildes dekrēta 39. pantu). Pārziņi ir atbildīgi par kaitējumu, kas radies datu aizsardzības pārkāpumu rezultātā, saskaņā ar Civillikuma noteikumiem par civiltiesisko atbildību (sk. arī 2.5. iedaļu par tiesisko aizsardzību) ([89]).

(65) Pildot savus drošības pienākumus, pārzinim ir jāsaņem palīdzība no privātuma amatpersonas, kuras uzdevumos cita starpā ietilpst iekšējās kontroles sistēmas izveide, lai "novērstu personas informācijas izpaušanu, ļaunprātīgu izmantošanu un nepareizu izmantošanu" (*PIPA* 31. panta 2. punkta 4. apakšpunkts). Turklāt pārzinim ir pienākums veikt "pienācīgu kontroli un uzraudzību" attiecībā uz tiem saviem darbiniekiem, kas apstrādā personas datus, tai skaitā attiecībā uz to drošu pārvaldību; tas ietver darbinieku nepieciešamo apmācību ("izglītību") (*PIPA* 28. panta 1. un 2. punkts). Visbeidzot, apakšapstrādes gadījumā pārzinim ir jānosaka prasības "ārpakalpojumu sniedzējam", cita starpā attiecībā uz personas datu drošu pārvaldību ("tehniskie un pārvaldības aizsardzības pasākumi"), un jāuzrauga, kā tās tiek īstenotas, veicot pārbaudes (*PIPA* 26. panta 1. un 4. punkts kopā ar *PIPA* Izpildes dekrēta 28. panta 1. punkta 3. un 4. apakšpunktu un 6. punktu).

2.3.7. *Pārredzamība*

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

([85]) Attiecībā uz personas datu apstrādi, ko veic informācijas un komunikācijas pakalpojumu sniedzēji, *PIPA* 39-5. pantā skaidri noteikts, ka to personu skaits, kas apstrādā lietotāju personas informāciju, ir ierobežots līdz minimumam. Turklāt informācijas un komunikācijas pakalpojumu sniedzēji nodrošina, ka lietotāju personas informācija netiek publiskota, izmantojot informācijas un komunikācijas tīklu (*PIPA* 39-10. panta 1. punkts). Pēc *PIPC* pieprasījuma atklātā informācija ir jādzēš vai jābloķē (*PIPA* 39-10. panta 2. punkts). Vispārīgāk runājot, informācijas un komunikācijas pakalpojumu sniedzējiem (un trešām personām, kas saņem lietotāju personas datus) ir jāievēro papildu drošības pienākumi, kas noteikti *PIPA* Izpildes dekrēta 48-2. pantā, piemēram, jāizstrādā un jāīsteno iekšējais pārvaldības plāns attiecībā uz drošības pasākumiem, piekļuves kontroles nodrošināšanas pasākumiem, šifrēšanu, ļaunprātīgu programmu atklāšanas programmatūras izmantošanu utt.

([86]) Turklāt pastāv vispārējs aizliegums bojāt, iznīcināt, pārveidot, viltot vai nopludināt personas informāciju bez likumīgas pilnvaras (sk. *PIPA* 59. panta 3. punktu).

([87]) Prasība informēt personu nav piemērojama, ciktāl datu aizsardzības pārkāpums attiecas uz pseidonimizētu informāciju, ko apstrādā statistikas, zinātniskās pētniecības vai arhivēšanas nolūkos sabiedrības interesēs (*PIPA* 28-7. pants, kas paredz atbrīvojumu no *PIPA* 34. panta 1. punkta un 39-4. panta). Lai nodrošinātu individuālu paziņošanu, attiecīgajam pārzinim būtu jāidentificē personas no pseidonimizētās datu kopas, kas ir skaidri aizliegts saskaņā ar *PIPA* 28-5. pantu. Tomēr vispārējā prasība par datu aizsardzības pārkāpumu paziņošanu (*PIPC*) joprojām ir spēkā.

([88]) Paziņošanas prasības, tostarp tās termiņi un iespēja paziņot "pa posmiem", ir sīkāk precizētas *PIPA* Izpildes dekrēta 40. pantā. Stingrāki noteikumi attiecas uz informācijas un komunikācijas pakalpojumu sniedzējiem, kuriem ir pienākums 24 stundu laikā pēc tam, kad tie uzzinājuši, ka personas informācija ir nozaudēta, nozagta vai nopludināta, par to paziņot datu subjektam un *PIPC* (*PIPA* 39-4. panta 1. punkts). Šajā paziņojumā jāietver sīkāka informācija par nopludināto personas informāciju, brīdi, kad tas noticis, par pasākumiem, ko lietotājs var veikt, par pakalpojumu sniedzēja veiktajiem atbildes pasākumiem un tās struktūrvienības kontaktinformācija, kurai lietotājs var uzdot jautājumus (*PIPA* 39-4. panta 1. punkta 1.–5. apakšpunkts). Attaisnojoša iemesla dēļ, piemēram, ja trūkst lietotāja kontaktinformācijas, var izmantot citus paziņošanas līdzekļus, piemēram, publiskojot informāciju tīmekļa vietnē (*PIPA* 39-4. panta 1. punkts kopā ar *PIPA* Izpildes dekrēta 48-4. panta 4. punktu un turpmākajiem punktiem). Šādā gadījumā *PIPC* ir jāinformē par iemesliem (*PIPA* 34-4. panta 3. punkts).

([89]) Sk., piemēram, Augstākās tiesas 2012. gada 26. decembra Lēmumus Nr. 2011Da59834, 2011Da59858 un 2011Da59841. Kopsavilkums angļu valodā ir pieejams tīmekļa vietnē: http://library.scourt.go.kr/SCLIB_data/decision/9-69%202012.12.26.2011Da59834.htm.

(67) Korejas sistēmā tas tiek nodrošināts dažādos veidos. Papildus tiesībām uz informāciju saskaņā ar *PIPA* 4. panta 1. punktu (vispārīgi) un 20. panta 1. punktu (attiecībā uz personas datiem, kas iegūti no trešām personām), kā arī tiesībām piekļūt datiem saskaņā ar *PIPA* 35. pantu *PIPA* ietver vispārēju pārredzamības prasību attiecībā uz apstrādes nolūku (*PIPA* 3. panta 1. punkts) un īpašas pārredzamības prasības gadījumos, kad apstrāde pamatojas uz piekrišanu (*PIPA* 15. panta 2. punkts, 17. panta 2. punkts un 18. panta 3. punkts) ([90]). Turklāt saskaņā ar *PIPA* 20. panta 2. punktu dažiem pārziņiem – tiem, kuru veiktā apstrāde pārsniedz noteiktas robežvērtības ([91]), – ir pienākums paziņot datu subjektam, kura personas datus tie ir saņēmuši no trešās personas, par informācijas avotu, apstrādes nolūku un datu subjekta tiesībām pieprasīt apstrādes apturēšanu, ja vien šāds paziņojums nav neiespējams kontaktinformācijas trūkuma dēļ. Izņēmumi attiecas uz noteiktām personas datu datnēm, kas ir publisko iestāžu rīcībā, jo īpaši datnēm ar datiem, kas tiek apstrādāti valsts drošības, citu īpaši svarīgu ("būtisku") valsts interešu vai krimināltiesību aizsardzības nolūkos, vai ja paziņošana var kaitēt citas personas dzīvībai vai veselībai vai negodīgi kaitēt citas personas mantiskajām un citām interesēm, tomēr tikai tad, ja attiecīgās valsts vai privātās intereses ir "acīm redzami svarīgākas" nekā attiecīgo datu subjektu tiesības (*PIPA* 20. panta 4. punkts). Šim nolūkam ir nepieciešams līdzsvarot intereses.

(68) Turklāt *PIPA* 3. panta 5. punktā noteikts, ka pārziņiem jāpublisko sava privātuma politika (un citi ar personas datu apstrādi saistīti jautājumi). Šī prasība ir sīkāk precizēta *PIPA* 30. pantā un *PIPA* Izpildes dekrēta 31. pantā. Saskaņā ar šiem noteikumiem publiskajā privātuma politikā cita starpā jāietver 1) apstrādāto personas datu veidi, 2) apstrādes nolūks, 3) saglabāšanas laikposms, 4) tas, vai personas dati tiek sniegti trešai personai ([92]), 5) jebkāda apakšapstrāde, 6) informācija par datu subjekta tiesībām un to, kā tās īstenot, un 7) kontaktinformācija (tostarp privātuma amatpersonas vai par datu aizsardzības noteikumu ievērošanu un sūdzību izskatīšanu atbildīgās iekšējās struktūrvienības nosaukums). Privātuma politikai jābūt publiski pieejamai tā, lai datu subjekti "varētu to viegli atpazīt" (*PIPA* 30. panta 2. punkts) ([93]), un tā ir pastāvīgi jāatjaunina (*PIPA* Izpildes dekrēta 31. panta 2. punkts).

(69) Uz publiskajām iestādēm attiecas papildu pienākums reģistrēt *PIPC* konkrēti šādu informāciju: 1) publiskās iestādes nosaukums, 2) personas datu datņu apstrādes pamatojums un nolūki, 3) dati par reģistrētajiem personas datiem, 4) apstrādes metode, 5) saglabāšanas laikposms, 6) to datu subjektu skaits, kuru personas dati tiek glabāti, 7) struktūrvienība, kas apstrādā datu subjektu pieprasījumus, un 8) personas datu saņēmēji, ja dati tiek sniegti regulāri vai atkārtoti (*PIPA* 32. panta 1. punkts) ([94]). *PIPC* publisko reģistrētās personas datu datnes, un publiskajām iestādēm uz tām ir jāatsaucas arī savā privātuma politikā (*PIPA* 30. panta 1. punkts un 32. panta 4. punkts).

(70) Lai uzlabotu pārredzamību tiem datu subjektiem Savienībā, kuru personas dati, pamatojoties uz šo lēmumu, tiek nosūtīti Korejai, Paziņojuma Nr. 2021-5 (I pielikums) 3. iedaļas i) un ii) punktā ir noteiktas papildu pārredzamības prasības. Pirmkārt, saņemot personas datus no Savienības, pamatojoties uz šo lēmumu, Korejā esošiem pārziņiem bez nepamatotas kavēšanās (un jebkurā gadījumā ne vēlāk kā vienu mēnesi pēc nosūtīšanas) jāpaziņo attiecīgajiem datu subjektiem to vienību nosaukums un kontaktinformācija, kuras nosūta un saņem informāciju, nosūtītie

([90]) Konkrēti, ja personas informācija tiek apstrādāta ar personas piekrišanu, pārzinim ir jāinformē persona par apstrādes nolūku, jāsniedz sīkākas ziņas par apstrādājamo informāciju, informācijas saņēmēju, personas informācijas glabāšanas un izmantošanas laikposmu, kā arī par personas tiesībām atteikt piekrišanu (un par jebkādu nelabvēlīgu situāciju, kas var rasties tā rezultātā).

([91]) Saskaņā ar *PIPA* Izpildes dekrēta 15-2. panta 1. punktu tas attiecas uz pārziņiem, kas apstrādā sensitīvu informāciju par vismaz 50 000 datu subjektu vai "parastu" personas informāciju par vismaz 1 miljonu datu subjektu. *PIPA* Izpildes dekrēta 15-2. panta 2. punktā ir noteiktas paziņošanas metodes un termiņi, bet 15-2. panta 3. punktā – prasība veikt noteiktu uzskaiti. Turklāt īpaši noteikumi attiecas uz noteiktu kategoriju informācijas un komunikācijas pakalpojumu sniedzējiem (tiem, kas iepriekšējā gadā guvuši pārdošanas ieņēmumus vismaz 10 miljardu vonu apmērā, vai tiem, kas dienā vidēji glabā/pārvalda vismaz viena miljona lietotāju personas datus trīs mēnešu laikā pirms iepriekšējā gada beigām), kuriem regulāri jāinformē lietotāji par viņu personas informācijas izmantošanas vēsturi, ja vien tas nav neiespējami kontaktinformācijas trūkuma dēļ (*PIPA* 39-8. pants un *PIPA* Izpildes dekrēta 48-6. pants).

([92]) Saskaņā ar informāciju, kas saņemta no Korejas valdības, tas nozīmē pienākumu individuāli uzskaitīt saņēmēju(-us) publiskajā privātuma politikā.

([93]) Papildu kārtība ir izklāstīta *PIPA* Izpildes dekrēta 31. panta 3. punktā.

([94]) Reģistrācijas prasība neattiecas uz noteikta veida personas informācijas datnēm, piemēram, datnēm, kurās reģistrēti ar valsts drošību, diplomātisko noslēpumu, kriminālizmeklēšanu, kriminālvajāšanu, sodīšanu, nodokļu jomas noziegumu izmeklēšanu saistīti jautājumi, vai datnēm, kas attiecas tikai uz iekšējo darba izpildi (*PIPA* 32. panta 2. punkts).

personas dati (vai personas datu kategorijas), Korejā esoša pārziņa veiktās vākšanas nolūks, saglabāšanas laikposms un saskaņā ar *PIPA* pieejamās tiesības. Otrkārt, sniedzot trešām personām personas datus, kas saņemti no Savienības, pamatojoties uz šo lēmumu, datu subjekti cita starpā ir jāinformē par saņēmēju, sniedzamajiem personas datiem vai personas datu kategorijām, valsti, kurai dati tiek sniegti (attiecīgā gadījumā), kā arī par tiesībām, kas pieejamas saskaņā ar *PIPA* ([95]). Tādējādi Paziņojums nodrošina, ka ES fiziskās personas joprojām ir informētas par konkrētiem pārziņiem, kas apstrādā viņu informāciju, un var izmantot savas tiesības attiecībā uz attiecīgajām vienībām.

(71) Paziņojuma 3. iedaļas iii) punkts (I pielikums) pieļauj dažus ierobežotus un kvalificētus izņēmumus no šiem papildu pārredzamības pienākumiem, kas pēc būtības ir līdzvērtīgi Regulā (ES) 2016/679 paredzētajiem. Konkrēti, paziņošana datu subjektiem Savienībā nav nepieciešama 1) ja un tik ilgi, kamēr ir nepieciešams ierobežot paziņošanu noteiktu sabiedrības interešu apsvērumu dēļ (piemēram, ja informācija tiek apstrādāta valsts drošības vai notiekošas kriminālizmeklēšanas nolūkos), ciktāl šie sabiedrības interešu mērķi ir acīm redzami svarīgāki par datu subjekta tiesībām; 2) ja informācija jau ir datu subjekta rīcībā; 3) ja un tik ilgi, kamēr paziņošana var apdraudēt fiziskas personas vai citas personas dzīvību vai veselību vai negodīgi aizskart citas personas mantiskās intereses, ja šīs tiesības vai intereses ir acīm redzami svarīgākas par datu subjekta tiesībām; vai 4) trūkst kontaktinformācijas par attiecīgajām personām vai to informēšanai būtu jāpieliek nesamērīgas pūles. Nosakot, vai ir vai nav iespējams sazināties ar datu subjektu vai arī tas ir saistīts ar pārmērīgām pūlēm, ņem vērā iespēju sadarboties ar Savienībā esošu datu nosūtītāju.

(72) Tādēļ 67.–71. apsvērumā ietvertie noteikumi nodrošina pēc būtības līdzvērtīgu aizsardzības līmeni attiecībā uz pārredzamību kā Regulā (ES) 2016/679 paredzētais.

2.3.8. *Individuālās tiesības*

(73) Datu subjektiem vajadzētu būt noteiktām tiesībām, kas ir īstenojamas attiecībā uz pārzini vai apstrādātāju, jo īpaši tiesībām piekļūt datiem, tiesībām uz datu labošanu, tiesībām iebilst pret apstrādi un tiesībām uz datu dzēšanu. Tajā pašā laikā uz šādām tiesībām var attiecināt ierobežojumus, ciktāl šie ierobežojumi ir nepieciešami un samērīgi, lai aizsargātu svarīgus vispārējo sabiedrības interešu mērķus.

(74) Saskaņā ar *PIPA* 3. panta 5. punktu pārzinis garantē datu subjekta tiesības, kas uzskaitītas *PIPA* 4. pantā un sīkāk noteiktas *PIPA* 35.–37., 39. un 39-2. pantā.

(75) Pirmkārt, personām ir tiesības uz informāciju un piekļuvi tai. Ja pārzinis ir vācis personas datus no trešās personas – kā tas vienmēr būs gadījumos, kad dati tiek nosūtīti no Savienības –, datu subjektiem parasti ir tiesības saņemt informāciju par 1) savākto personas datu "avotu" (t. i., nosūtītāju), 2) apstrādes nolūku un 3) datu subjekta tiesībām pieprasīt apstrādes apturēšanu (*PIPA* 20. panta 1. punkts). Piemēro ierobežotus izņēmumus, proti, ja šāda paziņošana var kaitēt citas personas dzīvībai vai veselībai vai "negodīgi kaitē citas personas mantiskajām un citām interesēm", bet tikai tad, ja šīs trešās personas intereses ir "nepārprotami svarīgākas" par datu subjekta tiesībām (*PIPA* 20. panta 4. punkta 2. apakšpunkts).

(76) Turklāt *PIPA* 35. panta 1. un 3. punkts kopā ar *PIPA* Izpildes dekrēta 41. panta 4. punktu paredz datu subjektiem tiesības piekļūt savai personas informācijai ([96]). Piekļuves tiesības ietver apstiprinājumu par apstrādi, informāciju par apstrādāto datu veidu, apstrādes nolūku, saglabāšanas laikposmu, kā arī par jebkādu izpaušanu trešai personai

([95]) Paziņojuma Nr. 2021-5 3. iedaļas ii) punkts (I pielikums).

([96]) Saskaņā ar *PIPA* 35. panta 3. punktu un *PIPA* Izpildes dekrēta 42. panta 2. punktu pārzinis var atlikt piekļuvi "nopietna iemesla dēļ" (t. i., pamatota iemesla dēļ, piemēram, ja nepieciešams vairāk laika, lai novērtētu, vai ir iespējams nodrošināt piekļuvi), taču par šādu pamatojumu 10 dienu laikā jāinformē datu subjekts un jāsniedz informācija par šā lēmuma pārsūdzēšanas iespējām; tiklīdz atlikšanas iemesls vairs nepastāv, piekļuve ir jānodrošina.

un apstrādātās personas informācijas kopijas izsniegšanu (*PIPA* 4. panta 3. punkts kopā ar *PIPA* Izpildes dekrēta 41. panta 1. punktu) ([97]). Piekļuvi var ierobežot (daļēja piekļuve) ([98]) vai liegt tikai tad, ja to paredz tiesību akti ([99]), ja tas varētu radīt kaitējumu trešās personas dzīvībai vai veselībai vai nepamatoti aizskart citas personas mantiskās un citas intereses (*PIPA* 35. panta 4. punkts) ([100]). Tas nozīmē, ka ir jāpanāk līdzsvars starp konstitucionāli aizsargātajām personas tiesībām un brīvībām, no vienas puses, un citu personu tiesībām un brīvībām, no otras puses. Ja piekļuve ir ierobežota vai liegta, pārzinim ir jāinformē datu subjekts par tā iemesliem un par lēmuma pārsūdzēšanas iespējām (*PIPA* Izpildes dekrēta 41. panta 5. punkts, 42. panta 2. punkts).

(77) Otrkārt, datu subjektiem ir tiesības uz savu personas datu labošanu vai dzēšanu ([101]), "ja vien citos likumos nav īpaši noteikts citādi" (*PIPA* 36. panta 1. un 2. punkts) ([102]). Saņemot pieprasījumu, pārzinim nekavējoties jāizmeklē jautājums, jāveic nepieciešamie pasākumi ([103]) un 10 dienu laikā par to jāinformē datu subjekts; ja pieprasījumu nevar apmierināt, šī paziņošanas prasība attiecas uz atteikuma iemesliem un pārsūdzēšanas iespējām (sk. *PIPA* 36. panta 4. punktu kopā ar *PIPA* Izpildes dekrēta 43. panta 3. punktu) ([104]).

(78) Visbeidzot, datu subjektiem ir tiesības nekavējoties apturēt savu personas datu apstrādi ([105]), ja vien nav piemērojams kāds no uzskaitītajiem izņēmumiem (*PIPA* 37. panta 1. un 2. punkts) ([106]). Pārzinis var noraidīt pieprasījumu, 1) ja tas ir īpaši atļauts ar tiesību aktiem vai ir nepieciešams ("neizbēgams") juridisko pienākumu izpildei, 2) ja apturēšana varētu radīt kaitējumu trešās personas dzīvībai vai veselībai vai nepamatoti aizskart citas personas mantiskās un citas intereses, 3) ja publiskajai iestādei nebūtu iespējams veikt tiesību aktos noteiktās funkcijas, neapstrādājot informāciju, vai 4) ja datu subjekts nepārprotami nepārtrauc pamatlīgumu ar pārzini, lai gan bez šādas datu apstrādes līgumu būtu neiespējami izpildīt. Šādā gadījumā pārzinim nekavējoties jāinformē datu subjekts par atteikuma iemesliem un par pārsūdzēšanas iespējām (*PIPA* 37. panta 2. punkts kopā ar *PIPA* Izpildes dekrēta 44. panta 2. punktu). Saskaņā ar *PIPA* 37. panta 4. punktu pārzinim, izpildot apturēšanas pieprasījumu, ir nekavējoties "jāveic nepieciešamie pasākumi, tostarp attiecīgās personas informācijas iznīcināšana" ([107]).

(79) Tiesības apturēt datu sniegšanu attiecas arī uz gadījumiem, kad personas dati tiek izmantoti tiešās tirgvedības nolūkos, t. i., lai reklamētu preces vai pakalpojumus vai aicinātu tos iegādāties. Turklāt šādai turpmākai apstrādei parasti ir nepieciešama īpaša (papildu) datu subjekta piekrišana (sk. *PIPA* 15. panta 1. punkta 1. apakšpunktu, 17. panta 2. punkta 1. apakšpunktu) ([108]). Pieprasot šādu piekrišanu, pārzinim "skaidri atpazīstamā veidā" ir īpaši

([97]) Piekļuvi publiskās iestādes apstrādātai personas informācijai var saņemt tieši no iestādes vai netieši, iesniedzot pieprasījumu *PIPC*, kas nekavējoties pārsūta pieprasījumu (*PIPA* 35. panta 2. punkts un *PIPA* Izpildes dekrēta 41. panta 3. punkts).

([98]) Saskaņā ar *PIPA* Izpildes dekrēta 42. panta 1. punktu pārzinim ir pienākums piešķirt daļēju piekļuvi, ja atteikuma pamatojums neattiecas vismaz uz daļu informācijas.

([99]) Šādam tiesību aktam savukārt jāievēro pamattiesības uz privātumu un datu aizsardzību, kā arī Korejas Konstitūcijā nostiprinātie nepieciešamības un samērīguma principi.

([100]) Turklāt publiskās iestādes var atteikt piekļuvi, ja tas radītu nopietnas grūtības veikt noteiktas funkcijas, tostarp veikt revīzijas vai uzlikt, iekasēt vai atmaksāt nodokļus (*PIPA* 35. panta 4. punkts).

([101]) Šādā gadījumā pārzinim ir jāveic pasākumi, kas novērš personas informācijas atgūšanu (sk. *PIPA* 36. panta 3. punktu).

([102]) Šādiem likumiem ir jāatbilst Konstitūcijas prasībām, ka pamattiesības var ierobežot tikai tad, ja tas ir nepieciešams valsts drošībai vai likumības un kārtības uzturēšanai sabiedrības labklājības labad, un tie nedrīkst skart brīvības vai tiesību būtību (Konstitūcijas 37. panta 2. punkts).

([103]) *PIPA* Izpildes dekrēta 43. panta 2. punktā ir paredzēta īpaša procedūra gadījumā, ja pārzinis apstrādā personas informācijas datnes, ko sniedzis cits pārzinis.

([104]) Ja netiek veikti nepieciešamie pasākumi, lai labotu vai dzēstu personas informāciju, un šī informācija pastāvīgi tiek izmantota vai sniegta trešai personai, var tikt piemēroti kriminālsodi (*PIPA* 73. panta 2. punkts).

([105]) Saskaņā ar *PIPA* Izpildes dekrēta 44. panta 2. punktu pārzinis 10 dienu laikā pēc pieprasījuma saņemšanas informē datu subjektu par to, ka tas ir pienācīgi apturējis apstrādi.

([106]) Attiecībā uz publiskajām iestādēm tiesības uz apstrādes apturēšanu var izmantot saistībā ar reģistrētās personas informācijas datnēs iekļauto informāciju (*PIPA* 37. pants kopā ar 32. pantu). Šāda reģistrācija nav nepieciešama dažās situācijās, piemēram, ja personas informācijas datnes attiecas uz valsts drošību, kriminālizmeklēšanu, diplomātiskajām attiecībām utt. (*PIPA* 32. panta 2. punkts).

([107]) Ja apstrāde netiek apturēta, var tikt piemēroti kriminālsodi (*PIPA* 73. panta 3. punkts).

([108]) Strīdu starpniecības komiteja (sk. 133. apsvērumu) ir risinājusi vairākas lietas, kurās personas ir sūdzējušās par viņu datu izmantošanu tiešās tirgvedības nolūkos bez piekrišanas, kā rezultātā izmaksātas kompensācijas un attiecīgie pārziņi dzēsuši personas datus (sk., piemēram, Strīdu starpniecības komitejas lēmumus 20R10-024(2020.11.18), 20R08-015(2020.8.28), 20R07-031 (2020.9.1)).

jāinformē datu subjekts par datu plānoto izmantošanu tiešās tirgvedības nolūkos, t. i., par to, ka ar viņu var sazināties, lai reklamētu preces vai pakalpojumus vai aicinātu tos iegādāties (*PIPA* 22. panta 2. un 4. punkts kopā ar *PIPA* Izpildes dekrēta 17. panta 2. punkta 1. apakšpunktu).

(80) Lai atvieglotu individuālo tiesību īstenošanu, pārzinim ir jāizstrādā īpašas procedūras un publiski par tām jāpaziņo (*PIPA* 38. panta 4. punkts) ([109]). Tas ietver procedūras, kā celt iebildumus pret pieprasījuma noraidījumu (*PIPA* 38. panta 5. punkts). Pārzinim ir jānodrošina, lai tiesību īstenošanas procedūra būtu "datu subjektam labvēlīga" un nebūtu sarežģītāka par personas datu vākšanas procedūru; tas ietver arī pienākumu sniegt informāciju par procedūru savā tīmekļa vietnē (*PIPA* Izpildes dekrēta 41. panta 2. punkts, 43. panta 1. punkts un 44. panta 1. punkts) ([110]). Personas var pilnvarot pārstāvi iesniegt šādu pieprasījumu (*PIPA* 38. panta 1. punkts kopā ar *PIPA* Izpildes dekrēta 45. pantu). Lai gan pārzinim ir tiesības noteikt maksu (un, ja tiek pieprasīts nosūtīt personas datu kopijas pa pastu, arī pasta izdevumus), summa ir jānosaka to "faktisko izdevumu robežās, kas nepieciešami [pieprasījuma] apstrādei"; maksu (un pasta izdevumus) nedrīkst noteikt, ja pārzinis ir iesniedzis pieprasījumu (*PIPA* 38. panta 3. punkts kopā ar *PIPA* Izpildes dekrēta 47. pantu).

(81) *PIPA* un tā Izpildes dekrētā nav ietverti vispārīgi noteikumi, kas konkrēti attiektos uz lēmumiem, kuri skar datu subjektu un ir balstīti vienīgi uz personas datu automatizētu apstrādi. Tomēr attiecībā uz personas datiem, kas vākti Savienībā, ikvienu lēmumu, pamatojoties uz automatizētu apstrādi, parasti pieņems Savienībā esošs pārzinis (kam ir tieša saistība ar attiecīgo datu subjektu), un tam attiecīgi piemēro Regulu (ES) 2016/679 ([111]). Tas ietver nosūtīšanas scenārijus, kuros apstrādi veic ārvalstu (piem., Korejas) uzņēmējs, kas rīkojas kā pārstāvis (apstrādātājs) Savienībā esoša pārziņa vārdā (vai kā apakšapstrādātājs, kas rīkojas Savienībā esoša apstrādātāja vārdā, kurš ir saņēmis datus no Savienībā esoša pārziņa, kas tos savācis), kurš uz šā pamata pieņem lēmumu. Tāpēc tas, ka *PIPA* nav īpašu noteikumu par automatizētu lēmumu pieņemšanu, visticamāk, neietekmēs saskaņā ar šo lēmumu nosūtīto personas datu aizsardzības līmeni.

(82) Izņēmuma kārtā noteikumus par pārredzamību pēc pieprasījuma (20. pants) un individuālajām tiesībām (35.–37. pants), kā arī individuālo paziņošanas prasību informācijas un komunikācijas pakalpojumu sniedzējiem (*PIPA* 39-8. pants) nepiemēro attiecībā uz pseidonimizētu informāciju, ja to apstrādā statistikas, zinātniskās pētniecības vai arhivēšanas nolūkos sabiedrības interesēs (*PIPA* 28-7. pants) ([112]). Saskaņā ar Regulas (ES) 2016/679 11. panta 2. punktu (kopā ar 57. apsvērumu) to pamato fakts, ka, lai nodrošinātu pārredzamību vai piešķirtu individuālās tiesības, pārzinim būtu jākonstatē, vai jebkādi dati (un, ja jā, tad kādi) ir saistīti ar personu, kura iesniegusi pieprasījumu, un saskaņā ar *PIPA* tas ir aizliegts (*PIPA* 28-5. panta 1. punkts). Turklāt, ja šāda atkārtota datu identifikācija ietver visas (pseidonimizētās) datu kopas pseidonimizācijas pārtraukšanu, tā visu citu iesaistīto personu informāciju pakļautu paaugstinātam riskam. Regula (ES) 2016/679 attiecas uz situācijām, kad atkārtota identificēšana ir praktiski neiespējama, savukārt *PIPA* izmanto stingrāku pieeju, skaidri aizliedzot atkārtotu identificēšanu visās situācijās, kad tiek apstrādāta pseidonimizēta informācija.

(83) Tādēļ Korejas sistēmā, kā aprakstīts 74.–82. apsvērumā, ir noteikumi par datu subjektu tiesībām, kas nodrošina aizsardzības līmeni, kurš pēc būtības ir līdzvērtīgs Regulā (ES) 2016/679 noteiktajam.

([109]) Sk. arī *PIPA* 30. panta 1. punkta 5. apakšpunktu par privātuma politiku, kurā cita starpā ir informācija par personai pieejamajām tiesībām un to izmantošanas iespējām.

([110]) Sk. arī *PIPA* 39-7. panta 2. punktu attiecībā uz informācijas un komunikācijas pakalpojumu sniedzējiem.

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

([112]) Sk. arī Paziņojumu Nr. 2021-5, kurā apstiprināts, ka *PIPA* 3. iedaļa (tostarp 28-7. pants) ir piemērojama tikai tad, ja pseidonimizētu informāciju apstrādā zinātniskās pētniecības, statistikas vai arhivēšanas nolūkos sabiedrības interesēs (sk. šā lēmuma I pielikuma 4. iedaļu).

2.3.9. *Tālāka nosūtīšana*

(84) Aizsardzības līmeni, kāds piešķirts personas datiem, kurus no Savienības nosūta pārziņiem Korejas Republikā, nedrīkst samazināt šādu datu tālāka nosūtīšana saņēmējiem trešā valstī.

(85) Šāda "tālāka nosūtīšana" no Korejā esoša pārziņa viedokļa ir starptautiska nosūtīšana no Korejas Republikas. Šajā ziņā *PIPA* nošķirta apstrādes nodošana ārpakalpojumu sniedzējam (t. i., apstrādātājam) un personas datu sniegšana trešām personām ([113]).

(86) Pirmkārt, ja personas datu apstrāde tiek nodota ārpakalpojumu sniedzējam, kas atrodas trešā valstī, Korejā esošam pārzinim ir jānodrošina atbilstība *PIPA* noteikumiem par ārpakalpojumiem (*PIPA* 26. pants). Tas ietver juridiski saistoša instrumenta ieviešanu, kas cita starpā ierobežo ārpakalpojumu sniedzēja veikto apstrādi tikai ārpakalpojumā nodotā darba nolūkam, nosaka tehniskos un pārvaldības aizsardzības pasākumus un ierobežo apakšapstrādi (sk. *PIPA* 26. panta 1. punktu); un informācijas publicēšanu par ārpakalpojumā nodoto darbu. Turklāt pārzinim ir pienākums "izglītot" ārpakalpojumu sniedzēju par nepieciešamajiem drošības pasākumiem un uzraudzīt, cita starpā veicot pārbaudes, visu pārziņa pienākumu izpildi saskaņā ar *PIPA* ([114]), kā arī ārpakalpojuma līgumu.

(87) Ja ārpakalpojumu sniedzējs rada kaitējumu, apstrādājot personas datus, pārkāpjot *PIPA*, atbildības nolūkos tas tiks attiecināts uz pārzini, kā tas būtu pārziņa darbinieku gadījumā (*PIPA* 26. panta 6. punkts). Tāpēc Korejā esošais pārzinis joprojām ir atbildīgs par personas datiem, kas ir nodoti ārpakalpojumu sniedzējam, un tam ir jānodrošina, lai ārvalstu apstrādātājs apstrādā informāciju saskaņā ar *PIPA*. Ja ārpakalpojumu sniedzējs apstrādā informāciju, pārkāpjot *PIPA*, Korejā esošo pārzini var saukt pie atbildības par to, ka tas nav izpildījis savu pienākumu nodrošināt *PIPA* ievērošanu, piemēram, uzraugot ārpakalpojumu sniedzēju. Ārpakalpojuma līgumā iekļautās garantijas un Korejā esoša pārziņa atbildība par ārpakalpojumu sniedzēja darbībām nodrošina aizsardzības nepārtrauktību, ja personas datu apstrāde tiek nodota ārpakalpojumu sniedzējam ārpus Korejas.

(88) Otrkārt, Korejā esoši pārziņi var sniegt personas datus trešai personai, kas atrodas ārpus Korejas. Lai gan *PIPA* ir ietverti vairāki juridiskie pamatojumi, kas ļauj sniegt datus trešām personām kopumā, ja trešā persona atrodas ārpus Korejas, pārzinim principā ([115]) ir jāsaņem datu subjekta piekrišana ([116]) pēc tam, kad datu subjektam ir sniegta informācija par 1) personas datu veidu, 2) personas datu saņēmēju, 3) nosūtīšanas nolūku tādā nozīmē, kāds ir saņēmēja apstrādes nolūks, 4) saņēmēja veiktās apstrādes saglabāšanas laikposmu, kā arī 5) datu subjekta iespējām atteikt piekrišanu (*PIPA* 17. panta 2. un 3. punkts). Paziņojuma Nr. 2021-5 iedaļā par pārredzamību (sk. 70. apsvērumu) ir prasība informēt personas par trešo valsti, kurai tiks sniegti viņu dati. Tādējādi datu subjekti Savienībā var pieņemt pilnībā apzinātu lēmumu par to, vai piekrist vai nepiekrist datu sniegšanai ārvalstīs. Turklāt pārzinis nedrīkst noslēgt līgumu ar trešo personu, kas ir saņēmēja, pārkāpjot *PIPA*, kas nozīmē, ka līgumā nedrīkst būt ietvertas saistības, kuras būtu pretrunā ar *PIPA* noteiktajām prasībām pārzinim ([117]).

([113]) Īpaši noteikumi attiecas uz informācijas un komunikācijas pakalpojumu sniedzējiem. Saskaņā ar *PIPA* 39-12. pantu informācijas un komunikācijas pakalpojumu sniedzējiem principā ir jāsaņem lietotāja piekrišana jebkurai personas informācijas nosūtīšanai uz ārvalstīm. Ja personas informācija tiek nosūtīta kā daļa no apstrādes darbību nodošanas ārpakalpojumu sniedzējam, tai skaitā glabāšanai, piekrišana nav nepieciešama, ja attiecīgās personas ir iepriekš tieši vai ar publiska paziņojuma starpniecību tādā veidā, kas nodrošina vieglu piekļuvi, informētas par 1) nosūtāmās informācijas datiem, 2) valsti, uz kuru informācija tiks nosūtīta (kā arī par nosūtīšanas datumu un metodi), 3) saņēmēja nosaukumu un 4) saņēmēja īstenotas izmantošanas un saglabāšanas nolūku (*PIPA* 39-12. panta 3. punkts). Turklāt šajā gadījumā tiks piemērotas vispārīgās prasības attiecībā uz ārpakalpojumiem. Katrai nosūtīšanai ir jāievieš īpašas garantijas attiecībā uz drošību, sūdzību un strīdu izskatīšanu, kā arī citi lietotāju informācijas aizsardzībai nepieciešamie pasākumi (*PIPA* Izpildes dekrēta 48-10. pants).

([114]) Sk. arī *PIPA* 26. panta 7. punktu, saskaņā ar kuru 15.–25., 27.–31., 33.–38. un 50. pants *mutatis mutandis* attiecas uz apstrādātāju.

([115]) Ja informācijas un komunikācijas pakalpojumu sniedzēji sniedz lietotāju personas informāciju trešām personām, vienmēr ir nepieciešama lietotāja piekrišana (*PIPA* 39-12. panta 2. punkts).

([116]) Kā detalizētāk paskaidrots 51. apsvērumā, lai piekrišana būtu spēkā esoša, tā ir jādod brīvi, apzināti, konkrēti.

([117]) Sk. arī *PIPA* 39-12. panta 1. punktu attiecībā uz informācijas un komunikācijas pakalpojumu sniedzējiem.

(89) Bez personas piekrišanas personas datus var sniegt trešai personai (ārvalstīs), ja izpaušanas nolūks joprojām ir "pamatoti saistīts" ar sākotnējo vākšanas nolūku (*PIPA* 17. panta 4. punkts, sk. 36. apsvērumu). Tomēr, pieņemot lēmumu par to, vai izpaust (vai neizpaust) personas datus "saistītam" nolūkam, pārzinim ir jāņem vērā, vai izpaušana nerada personai nelabvēlīgu situāciju un vai ir veikti nepieciešamie drošības pasākumi (piemēram, šifrēšana). Ņemot vērā to, ka trešā valsts, uz kuru nosūta personas datus, var nepiedāvāt tādu aizsardzību, kas ir līdzīga *PIPA* paredzētajai, Paziņojuma Nr. 2021-5 2. iedaļā ir atzīts, ka šāda nelabvēlīga situācija var rasties un to var novērst tikai tad, ja Korejā esošs pārzinis un ārvalstu saņēmējs ar juridiski saistošu instrumentu (piemēram, līgumu) nodrošina *PIPA* līdzvērtīgu aizsardzības līmeni, tai skaitā attiecībā uz datu subjektu tiesībām.

(90) Īpaši noteikumi attiecas uz datu izpaušanu "ārpus nolūka", t. i., datu sniegšanu trešai personai jaunam (nesaistītam) nolūkam, kas var notikt tikai tad, ja ir kāds no *PIPA* 18. panta 2. punktā minētajiem pamatojumiem, kā aprakstīts 39. apsvērumā. Tomēr pat saskaņā ar šiem nosacījumiem datu sniegšana trešām personām ir izslēgta, ja tā varētu "negodīgi aizskart" datu subjekta vai trešās personas intereses, tāpēc ir nepieciešams līdzsvarot intereses. Turklāt saskaņā ar *PIPA* 18. panta 5. punktu pārzinim ir jāpiemēro papildu garantijas, kas var ietvert pieprasījumu trešai personai ierobežot apstrādes nolūku un metodi vai ieviest īpašus drošības pasākumus. Arī šajā gadījumā, ņemot vērā to, ka trešā valsts, uz kuru nosūta personas datus, var nepiedāvāt tādu aizsardzību, kas ir līdzīga *PIPA* paredzētajai, Paziņojuma Nr. 2021-5 2. iedaļā ir atzīts, ka var rasties personas vai trešās personas interešu "negodīgs aizskārums" un to var novērst tikai tad, ja Korejā esošs pārzinis un ārvalstu saņēmējs ar juridiski saistošu instrumentu (piemēram, līgumu) nodrošina *PIPA* līdzvērtīgu aizsardzības līmeni, tai skaitā attiecībā uz datu subjektu tiesībām.

(91) Tādēļ 86.–90. apsvēruma noteikumi nodrošina aizsardzības nepārtrauktību, kad personas dati no Korejas Republikas tiek nosūtīti tālāk (ārpakalpojumu sniedzējam vai trešai personai) tādā veidā, kas pēc būtības ir līdzvērtīgs Regulā (ES) 2016/679 paredzētajai aizsardzībai.

2.3.10. *Pārskatatbildība*

(92) 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, konkrēti – kompetentajai uzraudzības iestādei.

(93) Saskaņā ar *PIPA* 3. panta 6. un 8. punktu pārzinim ir jāapstrādā personas dati "tā, lai līdz minimumam samazinātu iespēju pārkāpt" datu subjekta privātumu, un jācenšas iegūt datu subjekta uzticību, ievērojot un pildot *PIPA* un citos saistītajos likumos noteiktos pienākumus un atbildību. Tas ietver iekšējā pārvaldības plāna izstrādi (*PIPA* 29. pants), kā arī atbilstošu personāla apmācību un uzraudzību (*PIPA* 28. pants).

(94) Lai nodrošinātu pārskatatbildību, *PIPA* 31. pants kopā ar *PIPA* Izpildes dekrēta 32. pantu paredz pārziņiem pienākumu iecelt privātuma amatpersonu, kas "visaptveroši uzņemas atbildību par personas informācijas apstrādi". Konkrēti, šādai privātuma amatpersonai ir uzdots veikt šādas funkcijas: 1) izveidot un īstenot personas datu aizsardzības plānu un izstrādāt privātuma politiku, 2) veikt regulārus apsekojumus par personas datu apstrādes stāvokli un praksi, lai novērstu trūkumus, 3) izskatīt sūdzības un atlīdzināt zaudējumus, 4) izveidot iekšējās kontroles sistēmu, lai novērstu personas datu izpaušanu, ļaunprātīgu vai nepareizu izmantošanu, 5) sagatavot un īstenot izglītības programmu, 6) aizsargāt, kontrolēt un pārvaldīt personas datu datnes un 7) iznīcināt personas datus pēc apstrādes nolūka īstenošanas vai saglabāšanas laikposma beigām. Veicot šos pienākumus, privātuma amatpersona var pārbaudīt personas datu apstrādes statusu un ar to saistītās sistēmas un pieprasīt informāciju par tām (*PIPA* 31. panta 3. punkts). Ja privātuma amatpersona uzzina par *PIPA* vai citu attiecīgo datu aizsardzības likumu pārkāpumiem, tā nekavējoties veic korektīvus pasākumus un vajadzības gadījumā ziņo par tiem pārziņa vadībai ("vadītājam") (*PIPA* 31. panta 4. punkts). Saskaņā ar *PIPA* 31. panta 5. punktu privātuma amatpersona nedrīkst ciest no nepamatotas nelabvēlīgas situācijas šo funkciju veikšanas dēļ.

(95) Turklāt pārziņiem proaktīvi jācenšas veikt ietekmes uz privātumu novērtējumu gadījumos, kad personas datu datņu darbība rada privātuma risku (*PIPA* 33. panta 8. punkts). Pamatojoties uz *PIPA* 33. panta 1. un 2. punktu un *PIPA* Izpildes dekrēta 35., 36. un 38. pantu, tādi faktori kā apstrādāto datu veids un raksturs (jo īpaši tas, vai tā ir sensitīva informācija), to apjoms, saglabāšanas laikposms un datu aizsardzības pārkāpumu iespējamība būs būtiski, lai novērtētu riska pakāpi datu subjektu tiesībām. Ietekmes uz privātumu novērtējuma mērķis ir nodrošināt, ka tiek analizēti privātuma riska faktori, kā arī jebkādi drošības vai citi pretpasākumi, un norādīt jautājumus, kas jāuzlabo (sk. *PIPA* 33. panta 1. punktu kopā ar *PIPA* Izpildes dekrēta 38. pantu).

(96) Publiskajām iestādēm ir pienākums veikt ietekmes novērtējumu, apstrādājot noteiktas personas datu datnes, kas rada lielāku risku iespējamiem privātuma pārkāpumiem (*PIPA* 33. panta 1. punkts). Saskaņā ar *PIPA* Izpildes dekrēta 35. pantu tas cita starpā attiecas uz datnēm, kas ietver sensitīvu informāciju par vismaz 50 000 datu subjektu, datnēm, kas tiks saskaņotas ar citām datnēm un tā rezultātā ietver informāciju par vismaz 500 000 datu subjektu, vai datnēm, kas ietver informāciju par vismaz vienu miljonu datu subjektu. Publiskās iestādes veiktā ietekmes novērtējuma rezultāti ir jāpaziņo *PIPC* (*PIPA* 33. panta 1. punkts), kas var sniegt savu atzinumu (*PIPA* 33. panta 3. punkts).

(97) Visbeidzot, *PIPA* 13. pantā noteikts, ka *PIPC* izstrādā politiku, kas vajadzīga, lai veicinātu un atbalstītu pārziņu "pašregulējošas datu aizsardzības darbības", cita starpā izmantojot izglītību par datu aizsardzību, veicinot un atbalstot datu aizsardzībā iesaistītās organizācijas un palīdzot pārziņiem izstrādāt un īstenot pašregulācijas noteikumus. Turklāt tā ievieš un veicina *ePRIVACY Mark* sistēmu. Šajā ziņā *PIPA* 32-2. pants kopā ar *PIPA* Izpildes dekrēta 34-2.–34-8. pantu paredz iespēju apliecināt, ka pārziņa personas datu apstrādes un aizsardzības sistēma (-as) atbilst *PIPA* prasībām. Saskaņā ar šiem noteikumiem sertifikāciju ([118]) var piešķirt (uz 3 gadiem), ja pārzinis atbilst *PIPC* noteiktajiem sertifikācijas kritērijiem, tostarp ir izveidojis pārvaldības, tehniskos un fiziskos aizsardzības pasākumus personas datu aizsardzībai ([119]). *PIPC* vismaz reizi gadā ir jāpārbauda pārziņa sistēmas, kas attiecas uz sertifikāciju, lai uzturētu to efektivitāti, un tas var novest pie sertifikācijas atsaukšanas (*PIPA* 32. panta 4. punkts kopā ar *PIPA* Izpildes dekrēta 34-5. pantu; tā dēvētā "turpmākā pārvaldība").

(98) Tādējādi Korejas regulējums īsteno pārskatatbildības principu tādā veidā, kas nodrošina aizsardzības līmeni, kurš pēc būtības ir līdzvērtīgs Regulā (ES) 2016/679 noteiktajam aizsardzības līmenim, tai skaitā paredzot dažādus mehānismus, lai nodrošinātu un pierādītu atbilstību *PIPA* prasībām.

2.3.11. *Īpaši noteikumi par personas kredītinformācijas apstrādi*

(99) Kā aprakstīts 13. apsvērumā, *CIA* paredz īpašus noteikumus par personas kredītinformācijas apstrādi, ko veic komerciālie operatori. Tāpēc, apstrādājot personas kredītinformāciju, komerciālajiem operatoriem ir jāievēro *PIPA* vispārīgās prasības, ja vien *CIA* nav ietverti konkrētāki noteikumi. Tas, piemēram, attiecas uz gadījumiem, kad tie apstrādā ar kredītkarti vai bankas kontu saistītu informāciju saistībā ar komercdarījumu ar fizisku personu. Kā nozaru tiesību akts, kas attiecas uz kredītinformācijas (gan personas datu, gan citu datu) apstrādi, *CIA* ne tikai nosaka īpašas datu aizsardzības garantijas (piemēram, attiecībā uz pārredzamību un drošību), bet arī vispārīgāk reglamentē īpašus apstākļus, kādos var apstrādāt personas kredītinformāciju. Tas jo īpaši ir atspoguļots detalizētajās prasībās par datu izmantošanu, sniegšanu trešām personām un šādu datu saglabāšanu.

(100) Tāpat kā *PIPA*, arī *CIA* atspoguļo likumīguma un samērīguma principu. Pirmkārt, kā vispārīga prasība *CIA* 15. panta 1. punktā ir noteikts, ka personas kredītinformāciju drīkst vākt tikai ar saprātīgiem un taisnīgiem līdzekļiem un vismazākajā apjomā, kas nepieciešams, lai kalpotu konkrētam nolūkam saskaņā ar *PIPA* 3. panta 1.–2. punktu. Otrkārt, *CIA* īpaši reglamentē personas kredītinformācijas apstrādes likumīgumu, ierobežojot tās vākšanu, izmantošanu un sniegšanu trešai personai un kopumā saistot šīs apstrādes darbības ar prasību par attiecīgās personas piekrišanu.

([118]) Turklāt, ja pārzinis plāno atsaukties uz sertifikāciju vai reklamēt to savā darījumdarbībā, tas var izmantot *PIPC* izveidoto personas informācijas aizsardzības zīmi. Sk. *PIPA* Izpildes dekrēta 34-7. pantu.

([119]) Kopš 2018. gada novembra ir izstrādāta "Personas informācijas un informācijas drošības pārvaldības sistēma" (*ISMS-P*), kas apliecina, ka pārziņi izmanto visaptverošu pārvaldības sistēmu.

(101) Personas kredītinformāciju var vākt, pamatojoties uz vienu no *PIPA* noteiktajiem pamatojumiem vai īpašiem *CIA* noteiktajiem pamatojumiem. Ņemot vērā to, ka Regulas (ES) 2016/679 45. pants paredz personas datu nosūtīšanu, ko veic pārzinis vai apstrādātājs Savienībā, bet neattiecas uz datu tiešu vākšanu (piemēram, no personas vai tīmekļa vietnes), ko veic pārzinis Korejā, attiecībā uz šo lēmumu ir būtiska tikai piekrišana un saskaņā ar *PIPA* pieejamie pamatojumi. Šie pamatojumi jo īpaši ietver scenārijus, kad nosūtīšana ir nepieciešama, lai izpildītu līgumu ar personu, vai Korejā esoša pārziņa leģitīmo interešu labad (*PIPA* 15. panta 1. punkta 4. un 6. apakšpunkts) ([120]).

(102) Pēc tam, kad personas kredītinformācija ir apkopota, to var izmantot 1) sākotnējam nolūkam, kādam to (tieši) ir sniegusi persona ([121]); 2) nolūkam, kas ir saderīgs ar sākotnējo vākšanas nolūku ([122]); 3) lai noteiktu, vai nodibināt vai uzturēt personas pieprasītās komercattiecības ([123]); 4) statistikas, pētniecības un arhivēšanas nolūkos sabiedrības interesēs ([124]), ja informācija ir pseidonimizēta ([125]); 5) ja ir saņemta papildu piekrišana vai 6) saskaņā ar tiesību aktiem.

(103) Ja komerciālais operators plāno izpaust personas kredītinformāciju trešai personai, tam ir jāsaņem personas piekrišana ([126]) pēc tam, kad viņš ir informējis personu par datu saņēmēju, saņēmēja nolūku attiecībā uz datu apstrādi, sniedzamo datu sīku informāciju, saņēmēja īstenotas datu glabāšanas laikposmu un tiesībām atteikt piekrišanu (*CIA* 32. panta 1. punkts un *CIA* Izpildes dekrēta 28. panta 2. punkts) ([127]). Šī piekrišanas prasība nav piemērojama īpašās situācijās, proti, ja tiek izpausta personas kredītinformācija ([128]): 1) ārpakalpojumu sniedzējam ārpakalpojuma nolūkos ([129]); 2) trešai personai uzņēmuma nodošanas, sadalīšanas vai apvienošanās gadījumā; 3) statistikas, pētniecības un arhivēšanas nolūkos sabiedrības interesēs, ja informācija ir pseidonimizēta; 4) nolūkam, kas ir saderīgs ar sākotnējo vākšanas nolūku; 5) trešai personai, kas izmanto informāciju, lai piedzītu fiziskas personas parādu ([130]); 6) lai izpildītu tiesas rīkojumu; 7) prokuroram / kriminālpolicijas ierēdnim ārkārtas

([120]) *CIA* ir paredzēti arī citi datu vākšanas juridiskie pamati, t. i., ja to pieprasa tiesību akti, ja publiskā iestāde informāciju publisko saskaņā ar tiesību aktiem par informācijas brīvību vai ja informācija ir pieejama sociālajā tīklā. Lai komerciālais operators varētu atsaukties uz pēdējo pamatojumu, tam ir jāspēj pierādīt, ka datu vākšana atbilst datu subjekta piekrišanas darbības jomai, pamatojoties uz saprātīgu ("objektīvu") interpretāciju un ņemot vērā datu raksturu, mērķi un nolūku padarīt tos pieejamus sociālajā tīklā un to, vai vākšanas nolūks ir "ļoti nozīmīgs" šim mērķim utt. (*CIA* Izpildes dekrēta 13. pants). Tomēr, kā paskaidrots 101. apsvērumā, šie pamatojumi principā nebūs būtiski nosūtīšanas scenārijā.

([121]) Piemēram, ja kredītinformācija tiek ģenerēta/nodrošināta saistībā ar komercdarījumu ar personu. Tomēr uz šo pamatojumu nevar atsaukties, lai izmantotu personas kredītinformāciju tiešās tirgvedības nolūkos (sk. *CIA* 33. panta 1. punkta 3. apakšpunktu).

([122]) Lai noteiktu, vai izmantošanas nolūks ir saderīgs ar sākotnējo vākšanas nolūku, jāņem vērā šādi faktori: 1) saikne ("atbilstība") starp abiem nolūkiem; 2) informācijas vākšanas veids; 3) izmantošanas ietekme uz personu un 4) tas, vai ir īstenoti atbilstoši drošības pasākumi, piemēram, pseidonimizācija (sk. *CIA* 32. panta 6. punkta 9-4. apakšpunktu).

([123]) Piemēram, pārzinim var būt jāņem vērā personas kredītinformācija, ko tas ir saņēmis no personas, lai izlemtu, vai pagarināt aizdevuma termiņu šai personai.

([124]) *CIA* 33. pants kopā ar *CIA* 32. panta 6. punkta 9-2., 9-4. un 10. apakšpunktu.

([125]) Pseidonimizācija ir definēta *CIA* 2. panta 15. punktā kā personas kredītinformācijas apstrāde tādā veidā, ka personas pēc šīs informācijas vairs nav identificējamas, izņemot apvienojumā ar papildu informāciju. Lai gan *CIA* ietver īpašas garantijas pseidonimizētas informācijas apstrādei statistikas, pētniecības un arhivēšanas nolūkos sabiedrības interesēs (*CIA* 40-2. pants), šie noteikumi neattiecas uz komerciālām organizācijām. Tā vietā uz tām joprojām attiecas īpašās *PIPA* III iedaļas prasības, kā aprakstīts (42)–48. apsvērumā. Turklāt ar *CIA* 40-3. pantu pseidonimizētas kredītinformācijas apstrāde, ja tā notiek statistikas, zinātniskās pētniecības vai arhivēšanas nolūkos sabiedrības interesēs, ir atbrīvota no pārredzamības un individuālo tiesību prasībām, kas ir līdzīgas *PIPA* 28-7. pantā paredzētajiem izņēmumiem un uz ko attiecas *PIPA* III iedaļas garantijas, kā sīkāk aprakstīts 42.–48. apsvērumā.

([126]) Tas neattiecas uz gadījumiem, kad informācija tiek sniegta trešai personai, lai uzturētu precīzu un atjauninātu personas kredītinformāciju, ja vien informācijas sniegšana atbilst sākotnējam apstrādes nolūkam (*CIA* 32. panta 1. punkts). Tas var notikt, piemēram, ja kredītreitingu aģentūrai tiek sniegta atjaunināta informācija, lai nodrošinātu, ka tās ieraksti ir precīzi.

([127]) Ja iepriekš minētās informācijas sniegšana nav praktiski iespējama, var pietikt ar to, ka persona tiek nosūtīta pie trešās personas, kas ir saņēmēja, lai saņemtu nepieciešamo informāciju.

([128]) Ņemot vērā to, ka *CIA* īpaši neregulē personas kredītinformācijas izpaušanu ārvalstīs, šādai izpaušanai ir jāatbilst garantijām, kas noteiktas Paziņojuma Nr. 2021-5 2. iedaļā attiecībā uz tālāku nosūtīšanu.

([129]) Personas kredītinformācijas apstrādes ārpakalpojumu izmantošana var notikt tikai uz rakstiska līguma pamata un saskaņā ar *PIPA* 26. panta 1.–3. un 5. punkta prasībām, kā aprakstīts 20. apsvērumā (*CIA* 17. pants un *CIA* Izpildes dekrēta 14. pants). Ārpakalpojumu sniedzējs nedrīkst izmantot informāciju, kas pārsniedz ārpakalpojumu sniegšanas pienākumu darbības jomu, un ārpakalpojumu uzņēmumam ir jāievieš īpašas drošības prasības (piemēram, šifrēšana) un jāizglīto ārpakalpojumu sniedzējs par to, kā novērst kredītinformācijas nozaudēšanu, zādzību, izpaušanu, pārveidošanu vai kompromitēšanu.

([130]) Sk. arī *CIA* Izpildes dekrēta 28. panta 10. punkta 1., 2. un 6. apakšpunktu.

situācijā, kad ir apdraudēta personas dzīvība vai ir paredzams, ka tai tiks nodarīti miesas bojājumi, un nav laika izdot tiesas orderi ([131]); 8) kompetentajām nodokļu iestādēm, lai ievērotu nodokļu jomas tiesību aktus; vai 9) saskaņā ar citiem tiesību aktiem. Ja datu izpaušana notiek, pamatojoties uz kādu no šiem iemesliem, par to iepriekš jāpaziņo datu subjektam (*CIA* 32. panta 7. punkts).

(104) *CIA* arī īpaši reglamentē personas kredītinformācijas apstrādes ilgumu, pamatojoties uz vienu no šiem pamatojumiem, lai to izmantotu vai sniegtu trešai personai pēc tam, kad ir beigušās komercattiecības ar personu ([132]). Var saglabāt tikai to informāciju, kas bija nepieciešama šo attiecību nodibināšanai vai uzturēšanai, ievērojot papildu garantijas (tā jāglabā atsevišķi no kredītinformācijas, kas attiecas uz personām, ar kurām tiek uzturētas komercattiecības, jāaizsargā ar īpašiem drošības pasākumiem, un tai jābūt pieejamai tikai pilnvarotām personām) ([133]). Visi pārējie dati ir jādzēš (*CIA* Izpildes dekrēta 17-2. panta 1. punkta 2. apakšpunkts). Lai noteiktu, kuri dati bija nepieciešami komercattiecībām, jāņem vērā dažādi faktori, tostarp tas, vai attiecības būtu bijis iespējams nodibināt bez šiem datiem un vai tie ir tieši saistīti ar personai piegādātajām precēm vai sniegtajiem pakalpojumiem (*CIA* Izpildes dekrēta 17-2. panta 2. punkts).

(105) Pat gadījumos, kad personas kredītinformāciju principā var glabāt arī pēc komercattiecību beigām, tā ir jādzēš trīs mēnešu laikā pēc turpmākā apstrādes nolūka īstenošanas ([134]) vai jebkurā gadījumā pēc pieciem gadiem (*CIA* 20-2. pants). Ierobežotā skaitā gadījumu personas kredītinformāciju var glabāt ilgāk nekā piecus gadus, jo īpaši, ja tas ir nepieciešams, lai izpildītu juridisko pienākumu; ja tas ir nepieciešams vitālo interešu nodrošināšanai attiecībā uz personas dzīvību, veselību un īpašumu; pseidonimizētas informācijas arhivēšanai (kas tika izmantota zinātniskās pētniecības, statistikas vai arhivēšanas nolūkos sabiedrības interesēs); vai apdrošināšanas nolūkos (jo īpaši apdrošināšanas maksājumiem vai apdrošināšanas krāpšanas novēršanai) ([135]). Šādos izņēmuma gadījumos piemēro īpašas garantijas (piemēram, personas informēšana par datu turpmāku izmantošanu, saglabātās informācijas nošķiršana no informācijas, kas attiecas uz personām, ar kurām joprojām pastāv komercattiecības, piekļuves tiesību ierobežošana, sk. *CIA* Izpildes dekrēta 17-2. panta 1.–2. punktu).

(106) *CIA* arī sīkāk nosaka precizitātes un datu kvalitātes principus, pieprasot, lai personas kredītinformācija tiktu "reģistrēta, grozīta un pārvaldīta", lai tā būtu precīza un atjaunināta (*CIA* 18. panta 1. punkts un *CIA* Izpildes dekrēta 15. panta 3. punkts) ([136]). Sniedzot kredītinformāciju noteiktām citām vienībām (piemēram, kredītreitingu aģentūrām), komerciālajiem operatoriem ir arī īpašs pienākums pārbaudīt informācijas precizitāti, lai nodrošinātu, ka saņēmējs reģistrē un pārvalda tikai precīzu informāciju (*CIA* Izpildes dekrēta 15. panta 1. punkts kopā ar *CIA* 18. panta 1. punktu). Vispārīgāk runājot, *CIA* nosaka, ka ir jāveic uzskaite par personas kredītinformācijas vākšanu, izmantošanu, izpaušanu trešām personām un iznīcināšanu (*CIA* 20. panta 2. punkts) ([137]).

(107) Turklāt uz personas kredītinformācijas apstrādi attiecas īpašas prasības saistībā ar datu drošību. *CIA* jo īpaši paredzēta prasība īstenot tehnoloģiskus, fiziskus un organizatoriskus pasākumus, lai novērstu nelikumīgu piekļuvi datorsistēmām, kā arī apstrādāto datu pārveidošanu, iznīcināšanu vai jebkādu citu apdraudējumu (piemēram, izmantojot piekļuves kontroli, sk. *CIA* 19. pantu un *CIA* Izpildes dekrēta 16. pantu). Turklāt, apmainoties ar personas kredītinformāciju ar trešo personu, jānoslēdz līgums, kurā noteikti īpaši drošības pasākumi (*CIA* 19. panta 2. punkts). Ja notiek personas kredītinformācijas aizsardzības pārkāpums, jāveic pasākumi, lai mazinātu jebkādu kaitējumu, un nekavējoties jāinformē attiecīgās personas (*CIA* 39-4. panta 1.–2. punkts). Turklāt ir jāinformē *PIPC* par personām sniegto paziņojumu un īstenotajiem pasākumiem (*CIA* 39-4. panta 4. punkts).

([131]) Šādā gadījumā ir nekavējoties jāpieprasa orderis. Ja 36 stundu laikā rīkojums netiek izdots, saņemtie dati ir nekavējoties jādzēš (*CIA* 32. panta 6. punkta 6. apakšpunkts).

([132]) Piemēram, tāpēc, ka līgumsaistības ir izpildītas, viena no pusēm ir izmantojusi savas tiesības izbeigt līgumu utt. (sk. *CIA* Izpildes dekrēta 17-2. panta 5. punktu).

([133]) *CIA* 20- 2. panta 1. punkts un *CIA* Izpildes dekrēta 17- 2. panta 1. punkta 1. apakšpunkts.

([134]) Šajā laikposmā tiek ņemts vērā, ka dzēšana bieži vien nav iespējama uzreiz, bet parasti ir jāveic konkrēti pasākumi (piemēram, dzēšamo datu nošķiršana no citiem datiem un dzēšana, neietekmējot informācijas sistēmu stabilitāti), kuru īstenošanai nepieciešams zināms laiks.

([135]) *CIA* 20-2. panta 2. punkts.

([136]) *CIA* 18. panta 2. punktā un *CIA* Izpildes dekrēta 15. panta 4. punktā ir paredzēti konkrētāki noteikumi attiecībā uz šo prasību par uzskaiti, piemēram, attiecībā uz uzskaiti, kas var kaitēt personai, piemēram, informāciju par noziedzīgu nodarījumu un bankrotu.

([137]) Attiecībā uz citiem pārskatatbildības mehānismiem *CIA* nosaka, ka dažām organizācijām (piemēram, kooperatīviem un valsts uzņēmumiem, sk. *CIA* Izpildes dekrēta 21. panta 2. punktu) ir jāieceļ "kredītinformācijas administrators/aizbildnis", kas ir atbildīgs par *CIA* ievērošanas uzraudzību un pilda *PIPA* noteiktos "privātuma amatpersonas" pienākumus (*CIA* 20. panta 3. un 4. punkts).

(108) *CIA* arī uzliek īpašus pārredzamības pienākumus, kas jāpilda, saņemot piekrišanu personas kredītinformācijas izmantošanai vai sniegšanai (*CIA* 32. panta 4. punkts, *CIA* 34-2. pants un *CIA* Izpildes dekrēta 30-3. pants) un, vispārīgāk, pirms informācijas sniegšanas trešai personai (*CIA* 32. panta 7. punkts) ([138]). Turklāt personām ir tiesības pēc pieprasījuma saņemt informāciju par savas kredītinformācijas izmantošanu un sniegšanu trešām personām trīs gadu laikā pirms pieprasījuma iesniegšanas (cita starpā par šādas izmantošanas/sniegšanas nolūku un datumu) ([139]).

(109) Saskaņā ar *CIA* fiziskām personām ir arī tiesības piekļūt savai personas kredītinformācijai (*CIA* 38. panta 1. punkts) un saņemt neprecīzu datu labojumus (*CIA* 38. panta 2.–3. punkts) ([140]). Turklāt papildus vispārējām tiesībām uz dzēšanu saskaņā ar *PIPA* (sk. 77. apsvērumu) *CIA* paredz īpašas tiesības dzēst personas kredītinformāciju, kas ir saglabāta ilgāk par 104. apsvērumā minētajiem saglabāšanas laikposmiem, t. i., piecus gadus (attiecībā uz personas kredītinformāciju, kas bija nepieciešama komercattiecību nodibināšanai vai uzturēšanai) vai trīs mēnešus (attiecībā uz cita veida personas kredītinformāciju) ([141]). Dzēšanas pieprasījumu izņēmuma kārtā var noraidīt, ja turpmāka saglabāšana ir nepieciešama 105. apsvērumā aprakstītajos apstākļos. Ja persona pieprasa dzēšanu, bet ir piemērojams kāds no izņēmumiem, attiecīgajai kredītinformācijai jāpiemēro īpašas garantijas (*CIA* 38-3. panta 3. punkts un *CIA* Izpildes dekrēta 33-3. pants). Piemēram, informācija ir jāglabā atsevišķi no citas informācijas, tai drīkst piekļūt tikai pilnvarota persona, un uz to jāattiecina īpaši drošības pasākumi.

(110) Papildus 109. apsvērumā minētajām tiesībām *CIA* garantē personām tiesības pieprasīt pārzinim pārtraukt sazināšanos ar tām tiešās tirgvedības nolūkos (Likuma 37. panta 2. punkts) un tiesības uz datu pārnesamību. Attiecībā uz pēdējo minēto *CIA* ļauj personām pieprasīt, lai viņu personas kredītinformācija tiktu nosūtīta viņām pašām vai noteiktām trešām personām (piemēram, finanšu iestādēm un kredītreitingu aģentūrām). Personas kredītinformācijai jābūt apstrādātai un nosūtītai trešai personai tādā formātā, ko var apstrādāt ar informācijas apstrādes ierīci (piemēram, datoru).

(111) *CIA* ietver īpašus noteikumus salīdzinājumā ar *PIPA*, tāpēc Komisija uzskata, ka arī šie noteikumi nodrošina aizsardzības līmeni, kurš pēc būtības ir līdzvērtīgs Regulā (ES) 2016/679 noteiktajam.

2.4. **Pārraudzība un izpilde**

(112) 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.

2.4.1. *Neatkarīga pārraudzība*

(113) Korejas Republikā par *PIPA* uzraudzību un izpildi atbildīgā neatkarīgā iestāde ir *PIPC*. *PIPC* sastāvā ir priekšsēdētājs, priekšsēdētāja vietnieks un septiņi komisāri. Priekšsēdētāju un priekšsēdētāja vietnieku pēc premjerministra ieteikuma ieceļ prezidents. Divus no komisāriem ieceļ prezidents, pamatojoties uz priekšsēdētāja ieteikumiem, un piecus – pamatojoties uz Nacionālās asamblejas ieteikumiem (divus no tiem pēc tās politiskās partijas

([138]) Tas ietver vispārēju paziņošanas prasību (*CIA* 32. panta 7. punkts) un īpašu pārredzamības pienākumu, ja informācija, pēc kuras var noteikt personas kredītspēju, tiek sniegta noteiktām vienībām, piemēram, kredītreitingu aģentūrām un kredītinformācijas vākšanas aģentūrām (*CIA* 35-3. pants un *CIA* Izpildes dekrēta 30-3. pants), vai ja komercdarījuma attiecības tiek atteiktas vai izbeigtas, pamatojoties uz personas kredītinformāciju, kas saņemta no trešās personas (*CIA* 36. pants un *CIA* Izpildes dekrēta 31. pants).

([139]) *CIA* 35. pants. Dažām komerciālām organizācijām, piemēram, kooperatīviem un valsts uzņēmumiem (*CIA* Izpildes dekrēta 21. panta 2. punkts), piemēro papildu pārredzamības prasības, piemēram, publiskot noteiktu informāciju (*CIA* 31. pants) un informēt personas par iespējamiem nelabvēlīgiem kredītreitinga rādītājiem, ja tās iesaistās finanšu darījumos, kas rada kredītrisku (*CIA* 35-2. pants).

([140]) Attiecībā uz piekļuves un labošanas tiesību nosacījumiem un izņēmumiem piemēro *PIPA* noteikumus (aprakstīti 76.–77. apsvērumā). Turklāt *CIA* 38. panta 4.–8. punktā un *CIA* Izpildes dekrēta 33. pantā ir noteikta papildu kārtība. Konkrēti, komerciālajam operatoram, kas ir izlabojis vai izdzēsis neprecīzu kredītinformāciju, par to ir jāinformē attiecīgā persona. Turklāt ir jāinformē jebkura trešā persona, kurai šī informācija tika izpausta iepriekšējo sešu mēnešu laikā, un par to jāinformē attiecīgā persona. Ja persona nav apmierināta ar to, kā tika apstrādāts labojuma pieprasījums, tā var iesniegt pieprasījumu *PIPC*, kas pārbauda pārziņa rīcību un var noteikt korektīvus pasākumus.

([141]) *CIA* 38-3. pants.

ieteikuma, kurai pieder prezidents, un trīs pēc citu politisko partiju ieteikumiem (*PIPA* 7-2. panta 2. punkts), kas palīdz mazināt politisko partiju lobēšanas ietekmi uz iecelšanas procesu) ([142]). Šī procedūra atbilst prasībām, kādas Savienībā piemēro datu aizsardzības iestāžu locekļu iecelšanai (Regulas (ES) 2016/679 53. panta 1. pants). Turklāt visiem komisāriem ir jāatturas no jebkādas ar peļņas gūšanu saistītas darījumdarbības, politiskās darbības un amatu ieņemšanas valsts pārvaldē vai Nacionālajā asamblejā (*PIPA* 7-6. pants un 7-7. panta 1. punkta 3. apakšpunkts) ([143]). Uz visiem komisāriem attiecas īpaši noteikumi, kas liedz viņiem piedalīties apspriedēs iespējama interešu konflikta gadījumā (*PIPA* 7-11. pants). *PIPC* palīdz sekretariāts (7-13. pants), un tā var izveidot apakškomisijas (trīs komisāru sastāvā) nelielu pārkāpumu un atkārtotu lietu izskatīšanai (*PIPA* 7-12. pants).

(114) Katru *PIPC* locekli ieceļ uz trim gadiem, un viņu var iecelt amatā atkārtoti vienu reizi (*PIPA* 7-4. panta 1. punkts). Komisārus var atbrīvot no amata tikai īpašos apstākļos, proti, ja viņi vairs nespēj pildīt savus pienākumus ilgstošas garīgas vai fiziskas invaliditātes dēļ, rīkojas, pārkāpjot tiesību aktus, vai pieļauj kādu no situācijām, kas uzskatāma par pamatu atstādināšanai no amata ([144]) (*PIPA* 7-5. pants). Tas viņiem nodrošina institucionālo aizsardzību funkciju pildīšanai.

(115) Vispārīgāk runājot, *PIPA* 7. panta 1. punktā ir skaidri garantēta *PIPC* neatkarība, un *PIPA* 7-5. panta 2. punktā noteikts, ka komisāri savus pienākumus veic neatkarīgi, saskaņā ar tiesību aktiem un savu sirdsapziņu ([145]). Aprakstītās institucionālās un procesuālās garantijas, tostarp attiecībā uz tās locekļu iecelšanu un atbrīvošanu no amata, nodrošina, ka *PIPC* darbojas pilnīgi neatkarīgi, bez ārējas ietekmes vai norādījumiem. Turklāt *PIPC* kā centrāla administratīva aģentūra ik gadu pati sagatavo sava budžeta priekšlikumu (kuru finanšu ministrija pārskata kā daļu no kopējā valsts budžeta pirms apstiprināšanas Nacionālajā asamblejā) un ir atbildīga par sava personāla vadību. *PIPC* pašreizējais budžets ir aptuveni 35 miljoni EUR un tajā strādā 154 darbinieki (tostarp 40 darbinieki, kuri specializējušies informācijas un komunikācijas tehnoloģijās, 32 darbinieki, kuri koncentrējas uz izmeklēšanām, un 40 juridiskie eksperti).

(116) *PIPC* uzdevumi un pilnvaras galvenokārt ir noteiktas *PIPA* 7-8. un 7-9. pantā, kā arī 61.–66. pantā ([146]). Jo īpaši *PIPC* uzdevumos ietilpst konsultāciju sniegšana par tiesību aktiem un noteikumiem, kas saistīti ar datu aizsardzību, datu aizsardzības politikas un pamatnostādņu izstrāde, individuālo tiesību pārkāpumu izmeklēšana, sūdzību izskatīšana un starpniecība strīdu izšķiršanā, *PIPA* ievērošanas nodrošināšana, izglītošana datu aizsardzības jomā un tās popularizēšana, kā arī apmaiņa un sadarbība ar trešo valstu datu aizsardzības iestādēm ([147]).

(117) Pamatojoties uz *PIPA* 68. pantu un *PIPA* Izpildes dekrēta 62. pantu, daži *PIPC* uzdevumi ir deleģēti Korejas Interneta un drošības aģentūrai, proti: 1) izglītība un sabiedriskās attiecības, 2) speciālistu apmācība un kritēriju izstrāde ietekmes uz privātuma novērtējumiem, 3) pieprasījumu izskatīšana par tā dēvētās ietekmes uz privātumu novērtējuma iestādes iecelšanu, 4) pieprasījumu izskatīšana par netiešu piekļuvi publisko iestāžu rīcībā esošajiem

([142]) Par *PIPC* komisāriem var iecelt tikai personas, kas atbilst noteiktiem kritērijiem: augstākos valsts ierēdņus, kas atbild par personas informācijas lietām; bijušos tiesnešus, prokurorus vai advokātus, kas praktizējuši vismaz 10 gadus; bijušos vadītājus ar pieredzi datu aizsardzības jomā, kuri strādājuši publiskajā iestādē vai organizācijā ilgāk nekā trīs gadus vai kurus ieteikusi šāda iestāde vai organizācija; un bijušos asociētos profesorus ar profesionālām zināšanām datu aizsardzības jomā, kas vismaz piecus gadus nostrādājuši akadēmiskā iestādē (*PIPA* 7-2. pants).

([143]) Sk. arī *PIPA* Izpildes dekrēta 4-2. pantu.

([144]) Sk. *PIPA* 7-7. pantu, saskaņā ar kuru par *PIPC* locekļiem nevar kļūt personas, kas nav Korejas valstspiederīgie, un politisko partiju biedri. Tas pats attiecas uz personām, kurām ir piemēroti noteikta veida kriminālsodi un kuras pēdējo piecu gadu laikā ir atstādinātas no amata disciplinārā kārtā utt. (*PIPA* 7-7. pants kopā ar Likuma par valsts amatpersonām 33. pantu).

([145]) Lai gan *PIPA* 7. panta 2. punktā ir atsauce uz premjerministra vispārējām pilnvarām saskaņā ar Likuma par valdības organizāciju 18. pantu apturēt vai atcelt – ar prezidenta piekrišanu – jebkuru nelikumīgu vai netaisnīgu centrālās administratīvās aģentūras rīkojumu, šādas pilnvaras nav piešķirtas attiecībā uz *PIPC* izmeklēšanas vai izpildes pilnvarām (sk. *PIPA* 7. panta 2. punkta 1. un 2. apakšpunktu). Saskaņā ar paskaidrojumiem, kas saņemti no Korejas valdības, Likuma par valdības organizāciju 18. pantā ir paredzēts nodrošināt premjerministram iespēju rīkoties ārkārtas apstākļos, piemēram, rīkojoties kā starpniekam domstarpībās starp dažādām valsts aģentūrām. Tomēr kopš šā noteikuma pieņemšanas 1963. gadā premjerministrs nekad nav izmantojis šīs pilnvaras.

([146]) Vajadzības gadījumā, lai veiktu uzdevumus saskaņā ar *PIPA* 7.-9. panta 1. punktu, *PIPC* var lūgt attiecīgo valsts amatpersonu, datu aizsardzības ekspertu, pilsonisko organizāciju un attiecīgo uzņēmēju atzinumus. Turklāt *PIPC* var pieprasīt attiecīgus materiālus, sniegt ieteikumus uzlabojumiem un pārbaudīt, vai tie tiek īstenoti (*PIPA* 7-9. panta 2.–5. punkts).

([147]) Sk. arī *PIPA* 9. pantu (trīs gadu ģenerālplāns personas informācijas aizsardzībai), *PIPA* 12. pantu (personas informācijas aizsardzības standarta pamatnostādnes), *PIPA* 13. pantu (pašregulācijas veicināšanas un atbalsta politika).

personas datiem (*PIPA* 35. panta 2. punkts) un 5) materiālu pieprasīšana un pārbaužu veikšana saistībā ar sūdzībām, kas saņemtas, izmantojot tā dēvēto Privātuma jautājumu zvanu centru. Saistībā ar sūdzību izskatīšanu, izmantojot Privātuma jautājumu zvanu centru, Korejas Interneta un drošības aģentūra pārsūta lietu *PIPC* vai prokuratūrai, ja tā konstatē, ka ir noticis tiesību akta pārkāpums. Iespēja iesniegt sūdzību Privātuma jautājumu zvanu centram neliedz personām iesniegt sūdzību tieši *PIPC* vai vērsties *PIPC*, ja tās uzskata, ka Korejas Interneta un drošības aģentūra nav apmierinoši izskatījusi viņu sūdzību.

2.4.2. *Izpildes panākšana, ieskaitot sankcijas*

(118) Lai nodrošinātu *PIPA* ievērošanu, likumdevējs ir piešķīris *PIPC* gan izmeklēšanas, gan izpildes pilnvaras, sākot no ieteikumiem līdz administratīviem naudas sodiem. Šīs pilnvaras tiek papildinātas ar krimināsodu režīmu.

(119) Attiecībā uz izmeklēšanas pilnvarām, ja ir aizdomas par *PIPA* pārkāpumu vai ir saņemts ziņojums par šādu pārkāpumu, vai ja tas ir nepieciešams, lai aizsargātu datu subjektu tiesības pārkāpumu gadījumā, *PIPC* var veikt pārbaudes uz vietas un pieprasīt no personas datu pārziņiem visus attiecīgos materiālus (piemēram, rakstus un dokumentus) (*PIPA* 63. pants kopā ar *PIPA* Izpildes dekrēta 60. pantu) ([148]).

(120) Attiecībā uz izpildi saskaņā ar *PIPA* 61. panta 2. punktu *PIPC* var sniegt konsultācijas datu pārziņiem par to, kā uzlabot personas datu aizsardzības līmeni konkrētās apstrādes darbībās. Datu pārziņiem ir godprātīgi jācenšas īstenot šādus ieteikumus un jāinformē *PIPC* par rezultātiem. Turklāt, ja ir pamatots iemesls uzskatīt, ka ir noticis *PIPA* pārkāpums, un bezdarbība var radīt grūti novēršamu kaitējumu, *PIPC* var noteikt korektīvus pasākumus (*PIPA* 64. panta 1. punkts) ([149]). Paziņojuma Nr. 2021-5 (I pielikums) 5. iedaļā ir saistošā veidā paskaidrots, ka šie nosacījumi ir izpildīti attiecībā uz jebkura *PIPA* noteikuma pārkāpumu, kas aizsargā personu tiesības uz privātumu saistībā ar personas informāciju ([150]). Pasākumi, ko ir pilnvarota veikt *PIPC*, ietver rīkojumu pārtraukt pārkāpumu izraisījušo rīcību, uz laiku apturēt datu apstrādi vai veikt citus nepieciešamos pasākumus. Par korektīvo pasākumu neievērošanu var piemērot sankcijas, uzliekot naudas sodu, kura maksimālais apmērs ir 50 miljoni vonu (*PIPA* 75. panta 2. punkta 13. apakšpunkts).

(121) Attiecībā uz noteiktām publiskajām iestādēm (piemēram, Nacionālo asambleju, centrālajām administratīvajām aģentūrām, pašvaldību iestādēm un tiesām) *PIPA* 64. panta 4. punktā noteikts, ka *PIPC* var "ieteikt" jebkuru no 120. apsvērumā minētajiem korektīvajiem pasākumiem un ka šīm iestādēm šāds ieteikums ir jāizpilda, ja vien nepastāv ārkārtas apstākļi. Saskaņā ar Paziņojuma Nr. 2021-5 5. iedaļu tas attiecas uz faktiskajiem vai juridiskajiem ārkārtas apstākļiem, par kuriem *PIPC*, sniedzot ieteikumu, nebija informēta. Attiecīgā publiskā iestāde var atsaukties uz šādiem ārkārtas apstākļiem tikai tad, ja tā skaidri pierāda, ka pārkāpums nav noticis, un *PIPC* konstatē, ka tā tas patiešām ir. Pretējā gadījumā publiskajai iestādei ir jāseko *PIPC* ieteikumam un "jāveic korektīvs pasākums, tostarp nekavējoties jāpārtrauc darbība, un jākompensē kaitējums izņēmuma gadījumā, ja nelikumīga darbība tomēr ir notikusi".

(122) *PIPC* var arī lūgt citām administratīvajām aģentūrām ar konkrētām pilnvarām saskaņā ar nozaru tiesību aktiem (piemēram, veselības, izglītības jomā) atsevišķi vai kopā ar *PIPC* veikt izmeklēšanu par (iespējamiem) privātuma pārkāpumiem, ko izdarījuši pārziņi, kuri darbojas attiecīgajā nozarē aģentūru jurisdikcijā, un noteikt korektīvos pasākumus (*PIPA* 63. panta 4.–5. punkts). Aprakstītajā gadījumā *PIPC* nosaka izmeklēšanas pamatojumu, mērķi un jomu ([151]). Savukārt attiecīgajai administratīvajai aģentūrai jāiesniedz *PIPC* pārbaudes plāns un jāinformē *PIPC* par pārbaudes rezultātiem. *PIPC* var ieteikt konkrētus korektīvos pasākumus, un attiecīgajai aģentūrai jācenšas tos īstenot. Šāds pieprasījums jebkurā gadījumā neierobežo *PIPC* kompetenci veikt savu izmeklēšanu vai piemērot sankcijas.

([148]) Turklāt *PIPC* var iekļūt pārziņa telpās, lai pārbaudītu darījumdarbības statusu, uzskaiti, dokumentus u. c. (*PIPA* 63. panta 2. punkts). Sk. arī *CIA* 45-3. pantu un *CIA* Izpildes dekrēta 36-4. pantu attiecībā uz *PIPC* pilnvarām saskaņā ar šo likumu.

([149]) Sk. arī *CIA* 45-4. pantu attiecībā uz *PIPC* pilnvarām saskaņā ar *CIA*.

([150]) Paziņojuma 5. iedaļā noteikts, ka "būtisks pamats uzskatīt, ka ir noticis pārkāpums attiecībā uz personas informāciju un ka bezdarbība var radīt grūti novēršamu kaitējumu *PIPA* 64. panta 1. un 2. punkta izpratnē, attiecas uz jebkuru tiesību aktos ietverto principu, tiesību un pienākumu pārkāpumu, lai aizsargātu personas tiesības uz personas informāciju". Tas pats attiecas uz *PIPC* pilnvarām saskaņā ar *CIA* 45-4. pantu.

([151]) *PIPA* Izpildes dekrēta 60. pants.

(123) Papildus savām korektīvajām pilnvarām *PIPC* var uzlikt administratīvos naudas sodus no 10 līdz 50 miljoniem vonu apmērā par dažādu *PIPA* prasību pārkāpumiem (*PIPA* 75. pants) ([152]). Cita starpā tas ietver apstrādes likumīguma prasību neievērošanu, nepieciešamo drošības pasākumu neveikšanu, nepaziņošanu datu subjektiem datu aizsardzības pārkāpuma gadījumā, apakšapstrādes prasību neievērošanu, privātuma politikas neizstrādāšanu un nepubliskošanu, privātuma amatpersonas neiecelšanu vai bezdarbību, saņemot no datu subjekta pieprasījumu, ko tas iesniedzis, īstenojot savas individuālās tiesības, kā arī dažus procesuālus pārkāpumus (nesadarbošanos izmeklēšanas laikā). Ja viens pārzinis pārkāpis vairākus *PIPA* noteikumus, par katru pārkāpumu var uzlikt naudassodu, un naudassoda apmēra noteikšanā ņem vērā cietušo personu skaitu.

(124) Turklāt, ja ir pamatotas aizdomas par *PIPA* vai citu "ar datu aizsardzību saistītu likumu" pārkāpumu, *PIPC* var iesniegt kriminālsūdzību kompetentajai izmeklēšanas iestādei (piemēram, prokuroram, sk. *PIPA* 65. panta 1. punktu). Turklāt *PIPC* var ieteikt pārzinim uzsākt disciplinārlietu pret atbildīgo personu (tostarp atbildīgo vadītāju, sk. *PIPA* 65. panta 2. punktu). Saņemot šādu ieteikumu, pārzinim tas ir jāpilda ([153]) un rakstiski jāpaziņo *PIPC* par rezultātu (*PIPA* 65. pants kopā ar *PIPA* Izpildes dekrēta 58. pantu).

(125) Attiecībā uz ieteikumiem saskaņā ar 61. pantu, korektīvajiem pasākumiem saskaņā ar 64. pantu, apsūdzību vai ieteikumu par disciplinārlietu saskaņā ar 65. pantu un administratīvo naudas sodu uzlikšanu saskaņā ar *PIPA* 75. pantu *PIPC* var publiskot faktus, t. i., informāciju par pārkāpumu, tiesību aktu pārkāpēju vienību un paredzēto (-os) pasākumu(-us), publicējot to savā tīmekļa vietnē vai vispārējā valsts mēroga dienas laikrakstā (*PIPA* 66. pants kopā ar *PIPA* Izpildes dekrēta 61. panta 1. punktu) ([154]).

(126) Visbeidzot, *PIPA* (kā arī citos "ar datu aizsardzību saistītos likumos") noteikto datu aizsardzības prasību ievērošanu atbalsta krimināsodu režīms. Šajā saistībā *PIPA* 70.–73. pantā ir ietverti noteikumi par sankcijām, kuru rezultātā var piemērot vai nu naudas sodu (no 20 līdz 100 miljoniem vonu apmērā), vai ieslodzījumu (maksimālais sods svārstās no 2 līdz 10 gadiem). Attiecīgie pārkāpumi cita starpā ietver personas datu izmantošanu vai šādu datu sniegšanu trešai personai bez nepieciešamās piekrišanas, sensitīvas informācijas apstrādi, kas ir pretrunā *PIPA* 23. panta 1. punktā noteiktajam aizliegumam, piemērojamo drošības prasību neievērošanu, kā rezultātā personas dati tiek pazaudēti, nozagti, izpausti, viltoti, pārveidoti vai bojāti, nepieciešamo pasākumu neveikšanu, lai labotu, dzēstu vai apturētu personas datu sniegšanu, vai personas datu nelikumīgu nosūtīšanu uz trešo valsti ([155]). Saskaņā ar *PIPA* 74. pantu katrā no šiem gadījumiem atbildīgs ir pārziņa darbinieks, aģents vai pārstāvis, kā arī pats pārzinis ([156]).

(127) Papildus *PIPA* paredzētajiem krimināsodiem personas datu nepareiza izmantošana arī var būt noziedzīgs nodarījums saskaņā ar Krimināllikumu. Tas konkrēti attiecas uz vēstuļu, dokumentu vai elektronisko ierakstu slepenības pārkāpšanu (316. pants), dienesta noslēpuma informācijas izpaušanu (317. pants), krāpšanu, izmantojot datorus (347-2. pants), kā arī piesavināšanos un uzticības ļaunprātīgu izmantošanu (355. pants).

(128) Tāpēc Korejas sistēma apvieno dažādus sankciju veidus – no korektīviem pasākumiem un administratīviem naudas sodiem līdz krimināsodiem, kam, visticamāk, būs īpaši spēcīga preventīva ietekme uz pārziņiem un personām, kas apstrādā datus. Uzreiz pēc izveides 2020. gadā *PIPC* sāka izmantot savas pilnvaras. *PIPC* 2021. gada ziņojums parāda, ka *PIPC* jau izdeva vairākus ieteikumus un korektīvus rīkojumus un uzlika administratīvos

([152]) Turklāt, ja pārziņa izmantotās personas informācijas apstrādes un aizsardzības sistēmas ir sertificētas kā atbilstīgas *PIPA*, bet faktiski nav izpildīti sertifikācijas kritēriji saskaņā ar *PIPA* Izpildes dekrēta 34-2. panta 1. punktu, vai ja ir konstatēts nopietns ar "[personas] informācijas aizsardzību saistītu tiesību aktu" pārkāpums, *PIPC* var atsaukt sertifikāciju (*PIPA* 32.-2. panta 3. un 5. punkts). Par šādu atsaukšanu *PIPC* paziņo pārzinim un publiski par to paziņo vai publicē to savā tīmekļa vietnē vai Oficiālajā Vēstnesī (*PIPA* Izpildes dekrēta 34-4. pants). Par *CIA* pārkāpumiem ir paredzēti arī administratīvie naudas sodi (*CIA* 52. pants) un krimināsodi (*CIA* 50. pants).

([153]) Saskaņā ar *PIPA* Izpildes dekrēta 58. panta 2. punktu, ja īpašu apstākļu dēļ ieteikuma ievērošana ir "neiespējama", pārzinim ir jāiesniedz *PIPC* argumentēts pamatojums.

([154]) Pieņemot lēmumu par to, vai publiskot šādu informāciju, *PIPC* ņem vērā pārkāpuma būtību un smagumu, tā ilgumu un biežumu, kā arī tā sekas (kaitējuma apmēru). Attiecīgajai vienībai sniedz iepriekšēju paziņojumu un iespēju aizstāvēties. Sk. *PIPA* Izpildes dekrēta 61. panta 2. un 3. punktu.

([155]) Sk. 71. panta 2. punktu kopā ar *PIPA* 18. panta 1. punktu (tādu *PIPA* 17. panta 3. punkta nosacījumu neievērošana, uz kuriem attiecas 18. panta 1. punkts). Sk. arī 75. panta 2. punkta 1. apakšpunktu kopā ar *PIPA* 17. panta 2. punktu (nepieciešamās informācijas nesniegšana attiecīgajai personai saskaņā ar *PIPA* 17. panta 2. punktu, uz kuru attiecas 17. panta 3. punkts).

([156]) Turklāt *PIPA* 74-2. pants ļauj konfiscēt jebkādu pārkāpuma rezultātā iegūto naudu, preces vai citu peļņu vai, ja konfiskācija nav iespējama, "iekasēt" nelikumīgi iegūto labumu.

sodus gan publiskajam sektoram (aptuveni 34 publiskajām iestādēm), gan privātiem operatoriem (aptuveni 140 uzņēmumiem) ([157]). Daži pieminēšanas vērti gadījumi: piemēram, 2020. gada decembrī *PIPC* piemēroja naudas sodu 6,7 miljardu vonu apmērā kādam uzņēmumam par dažādu *PIPA* noteikumu pārkāpšanu (tai skaitā drošības prasību, prasību par piekrišanu informācijas sniegšanai trešām personām un pārredzamības prasību) ([158]) un 2021. gada aprīlī – naudas sodu 103,3 miljonu vonu apmērā kādam mākslīgā intelekta tehnoloģiju uzņēmumam (cita starpā par noteikumu pārkāpumiem saistībā ar apstrādes likumīgumu, jo īpaši piekrišanu, un pseidonimizētas informācijas apstrādi ([159]). 2021. gada augustā *PIPC* noslēdza vēl vienu izmeklēšanu par triju uzņēmumu darbībām, kuras rezultātā tika noteikti korektīvie pasākumi un uzlikti naudas sodi līdz pat 6,47 miljardu vonu apmērā (cita starpā par personu neinformēšanu par personas datu izpaušanu trešām personām, ieskaitot nodošanu trešām valstīm) ([160]). Turklāt jau pirms nesenās reformas Dienvidkoreja bija guvusi ievērojamus panākumus izpildes nodrošināšanā, atbildīgajām iestādēm izmantojot pilnu izpildes pasākumu klāstu, tostarp administratīvos naudas sodus, korektīvos pasākumus un "nosaukšanu un kopīgošanu" attiecībā uz dažādiem pārziņiem, tai skaitā sakaru pakalpojumu sniedzējiem (Korejas Komunikācijas komisija), kā arī komerciālajiem operatoriem, finanšu iestādēm, publiskajām iestādēm, universitātēm un slimnīcām (Iekšlietu un drošības ministrija) ([161]). Pamatojoties uz to, Komisija secina, ka Korejas sistēma nodrošina datu aizsardzības noteikumu efektīvu izpildi praksē, tādējādi garantējot aizsardzības līmeni, kurš pēc būtības ir līdzvērtīgs Regulā (ES) 2016/679 noteiktajam.

2.5. **Tiesiskā aizsardzība**

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

(130) Korejas sistēma nodrošina personām dažādus mehānismus, lai efektīvi īstenotu savas tiesības un panāktu (tiesisko) aizsardzību.

(131) Personas, kuras uzskata, ka ir pārkāptas viņu datu aizsardzības tiesības vai intereses, vispirms var vērsties pie attiecīgā pārziņa. Saskaņā ar *PIPA* 30. panta 1. punkta 5. apakšpunktu pārziņa privātuma politikā cita starpā iekļauj informāciju par datu subjektu tiesībām un to īstenošanas iespējām. Turklāt tā ietver kontaktinformāciju (piemēram, privātuma amatpersonas vārdu, uzvārdu vai par datu aizsardzību atbildīgās struktūrvienības nosaukumu un tālruņa numuru) sūdzību iesniegšanai. Pārziņa organizācijā privātuma amatpersona ir atbildīga par sūdzību izskatīšanu, korektīvo pasākumu pieņemšanu privātuma pārkāpuma gadījumā un zaudējumu atlīdzināšanu (*PIPA* 31. panta 2. punkta 3. apakšpunkts un 4. punkts). Tas ir svarīgi, piemēram, datu aizsardzības pārkāpuma gadījumā, jo pārzinim cita starpā ir jāinformē datu subjekts par kontaktpunktu(-iem), kur ziņot par jebkādu kaitējumu (*PIPA* 34. panta 1. punkta 5. apakšpunkts).

(132) Turklāt *PIPA* piedāvā vairākus tiesiskās aizsardzības līdzekļus fiziskām personām pret pārziņiem. Pirmkārt, ikviena persona, kas uzskata, ka pārzinis ir pārkāpis tās datu aizsardzības tiesības vai intereses, var ziņot par šādu pārkāpumu *PIPC* un/vai vienai no specializētajām iestādēm, ko *PIPC* ir izraudzījusies sūdzību pieņemšanai un izskatīšanai; tas attiecas arī uz Korejas Interneta un drošības aģentūru, kas šim nolūkam pārvalda personas informācijas zvanu centru (tā dēvēto "Privātuma jautājumu zvanu centru") (*PIPA* 62. panta 1. un 2. punkts kopā ar *PIPA* Izpildes dekrēta 59. pantu). Privātuma jautājumu zvanu centrs izmeklē un konstatē pārkāpumus,

([157]) Sk. *PIPC* 2021. gada ziņojumu, 50.–55. lpp. (pieejams tikai korejiešu valodā): https://www.pipc.go.kr/np/cop/bbs/selectBoardArticle.do?bbsId=BS074&mCode=C020010000&nttId=7511#LINK

([158]) Sk. (pieejams tikai korejiešu valodā) https://www.pipc.go.kr/np/cop/bbs/selectBoardArticle.do?bbsId=BS074&mCode=C020010000&nttId=6954#LINK.

([159]) Sk. (pieejams tikai korejiešu valodā) https://www.pipc.go.kr/np/cop/bbs/selectBoardArticle.do?bbsId=BS074&mCode=C020010000&nttId=7298&fbclid=IwAR3SKcMQi6G5pR9k4I7j6GNXtc8aBVDOwcURevvvzQtYI7AS40UKYXoOXo8.

([160]) Sk. (pieejams tikai korejiešu valodā): https://www.pipc.go.kr/np/cop/bbs/selectBoardArticle.do?bbsId=BS074&mCode=C020010000&nttId=7497#LINK.

([161]) Sk., piemēram, 2020. gada pārskatu (pieejams tikai korejiešu valodā): https://www.pipc.go.kr/np/cop/bbs/selectBoardList.do?bbsId=BS079&mCode=D070020000 un piemērus angļu valodā: https://www.privacy.go.kr/eng/enforcement_02.do.

sniedz konsultācijas par personas datu apstrādi (*PIPA* 62. panta 3. punkts) un var ziņot par pārkāpumiem *PIPC* (bet pats nevar īstenot izpildes pasākumus). Privātuma jautājumu zvanu centrs saņem lielu skaitu sūdzību/pieprasījumu (piemēram, 177 457 2020. gadā, 159 255 2019. gadā un 164 497 2018. gadā) ([162]). Saskaņā ar *PIPC* sniegto informāciju pati *PIPC* saņēma aptuveni 1 000 sūdzību laikposmā no 2020. gada augusta līdz 2021. gada augustam. Reaģējot uz sūdzību, *PIPC* var sniegt padomu par uzlabojumiem, veikt korektīvus pasākumus, iesniegt "apsūdzību" kompetentajai izmeklēšanas iestādei (tai skaitā prokuroram) vai sniegt padomu par disciplinārlietu (sk. *PIPA* 61., 64. un 65. pantu). *PIPC* lēmumus (piemēram, atteikumu izskatīt sūdzību vai sūdzības noraidījumu pēc būtības) var apstrīdēt saskaņā ar Administratīvo lietu iztiesāšanas likumu ([163]).

(133) Otrkārt, saskaņā ar *PIPA* 40.–50. pantu un *PIPA* Izpildes dekrēta 48-14.–57. pantu datu subjekti var iesniegt prasības tā dēvētajā "Strīdu starpniecības komitejā", ko veido *PIPC* priekšsēdētāja iecelti pārstāvji no *PIPC* augstākā izpilddienesta locekļu vidus un personas, kas ieceltas, pamatojoties uz viņu pieredzi datu aizsardzības jomā, no noteiktām atbilstīgām grupām (sk. *PIPA* 40. panta 2., 3. un 7. punktu, *PIPA* Izpildes dekrēta 48-14. pantu) ([164]). Iespēja izmantot starpniecību Strīdu starpniecības komitejā piedāvā alternatīvu iespēju izmantot tiesiskās aizsardzības līdzekļus, bet neierobežo personas tiesības vērsties *PIPC* vai tiesā. Lai izskatītu lietu, Komiteja var pieprasīt strīdā iesaistītajām pusēm iesniegt nepieciešamos materiālus un/vai uzaicināt attiecīgos lieciniekus uz Komitejas sēdi (*PIPA* 45. pants). Kad jautājums ir noskaidrots, Komiteja sagatavo starpniecības lēmuma projektu ([165]), par kuru jāvienojas Komitejas locekļu vairākumam. Starpniecības lēmuma projekts var ietvert pārkāpuma pārtraukšanu, nepieciešamos tiesiskās aizsardzības līdzekļus (tostarp restitūciju vai kompensāciju), kā arī jebkādus pasākumus, kas nepieciešami, lai novērstu tāda paša vai līdzīga(-u) pārkāpuma(-u) atkārtošanos (*PIPA* 47. panta 1. punkts). Ja abas puses piekrīt starpniecības lēmumam, tam ir tāds pats spēks kā izlīgumam tiesā (*PIPA* 47. panta 5. punkts). Nevienai no pusēm nav liegts uzsākt tiesvedību tiesā, kamēr notiek starpniecība, un šādā gadījumā starpniecība tiek apturēta (sk. *PIPA* 48. panta 2. punktu) ([166]). *PIPC* publicētie ikgadējie skaitļi liecina, ka personas regulāri izmanto Strīdu starpniecības komitejas procedūru, kurai bieži ir veiksmīgs iznākums. Piemēram, 2020. gadā komiteja izskatīja 126 lietas, no kurām 89 tika atrisinātas komitejā (77 lietās puses jau bija vienojušās vēl pirms starpniecības procedūras beigām, un 12 lietās puses pieņēma starpniecības priekšlikumu), līdz ar to starpniecības koeficients bija 70,6 % ([167]). Līdzīgi 2019. gadā komiteja izskatīja 139 lietas, no kurām 92 tika atrisinātas, un starpniecības koeficients bija 62,2 %.

(134) Turklāt, ja vismaz 50 personām ir nodarīts kaitējums vai to datu aizsardzības tiesības ir pārkāptas identiskā vai līdzīgā veidā pēc viena un tā paša (veida) incidenta ([168]), datu subjekts vai datu aizsardzības organizācija šāda kolektīva vārdā var pieteikties kolektīvai strīdu starpniecībai; citi datu subjekti var pieteikties, lai pievienotos šādai starpniecībai, par ko publiski paziņos Strīdu starpniecības komiteja (*PIPA* 49. panta 1.–3. punkts kopā ar *PIPA* Izpildes dekrēta 52.–54. pantu) ([169]). Strīdu starpniecības komiteja var izvēlēties vismaz vienu personu, kas

([162]) Sk. *PIPC* 2021. gada ziņojumu, 174. lpp. 2020. gadā šādas sūdzības attiecās, piemēram, uz datu vākšanu bez piekrišanas, neatbilstību pārredzamības pienākumiem, apstrādātāju veiktiem *PIPA* pārkāpumiem, nepietiekamiem drošības pasākumiem un neatbildēšanu uz datu subjektu pieprasījumiem un vispārīgiem jautājumiem.

([163]) Konkrēti, personas var pārsūdzēt administratīvās aģentūras publisko pilnvaru īstenošanu vai atteikumu to īstenot (Administratīvo lietu iztiesāšanas likuma 2. panta 1. punkta 1. apakšpunkts, 3. panta 1. punkts). Detalizētāka informācija par procesuālajiem aspektiem, tostarp pieņemamības prasībām, ir sniegta 181. apsvērumā.

([164]) Visiem locekļiem ir noteikts pilnvaru termiņš, un viņus var atlaist tikai pamatota iemesla dēļ (sk. *PIPA* 40. panta 5. punktu un 41. pantu). Turklāt *PIPA* 42. pantā ir ietvertas garantijas, lai aizsargātu pret interešu konfliktiem.

([165]) Sk. *PIPA* 44. pantu. Turklāt tā var ierosināt izlīguma projektu un ieteikt izlīgumu bez starpniecības (sk. *PIPA* 46. pantu).

([166]) Turklāt Komiteja var noraidīt starpniecību, ja tā uzskata, ka starpniecība nav piemērota, ņemot vērā strīda būtību, vai tāpēc, ka starpniecības pieteikums ir iesniegts negodīgā nolūkā (*PIPA* 48. pants).

([167]) Sk. *PIPC* 2021. gada ziņojumu, 179.–180. lpp. Minētās lietas cita starpā attiecās uz pārkāpumiem saistībā ar prasību saņemt piekrišanu datu vākšanai, nolūka ierobežojuma principu un datu subjektu tiesībām.

([168]) Sk. *PIPA* 49. panta 1. punktu, kurā noteikts, ka datu subjektiem jābūt nodarītam kaitējumam vai tiesību pārkāpumam "identiskā vai līdzīgā veidā", un *PIPA* Izpildes dekrēta 52. panta 2. punktu, kurā noteikts, ka "galvenie incidenta jautājumi ir faktiski vai juridiski kopīgi".

([169]) Turklāt pat personas, kas nav iesaistītās puses, var gūt labumu no kolektīvās strīda starpniecības lēmuma, ko pieņēmis pārzinis, jo Strīdu starpniecības komiteja var ieteikt pārzinim sagatavot un iesniegt kompensācijas plānu, kas (arī) attiecas uz tām (*PIPA* 49. panta 5. punkts).

vispiemērotāk pārstāv kopējās intereses kā pārstāvības puse (*PIPA* 49. panta 4. punkts). Ja pārzinis noraida kolektīvo strīda starpniecību vai nepieņem starpniecības lēmumu, noteiktas organizācijas ([170]) var iesniegt kolektīvo prasību tiesā, lai novērstu pārkāpumu (*PIPA* 51.–57. pants).

(135) Treškārt, tāda privātuma pārkāpuma gadījumā, kas personai nodara "kaitējumu", datu subjektam ir tiesības uz atbilstošu tiesisko aizsardzību "ātrā un taisnīgā procedūrā" (*PIPA* 4. panta 5. punkts kopā ar 39. pantu) ([171]). Pārzinis var sevi attaisnot, pierādot vainas ("ļauna nodoma" vai nolaidības) neesamību. Ja datu subjektam nodarīts kaitējums viņa personas datu nozaudēšanas, zādzības, izpaušanas, viltošanas, pārveidošanas vai bojāšanas rezultātā, tiesa, ņemot vērā vairākus faktorus, var noteikt kompensāciju līdz pat trīskāršam faktiskā kaitējuma apmēram (*PIPA* 39. panta 3. un 4. punkts). Alternatīvi datu subjekts var pieprasīt "saprātīgu kompensāciju", kas nepārsniedz 3 miljonus vonu (*PIPA* 39-2. panta 1. un 2. punkts). Turklāt saskaņā ar Civillikumu kompensāciju var pieprasīt no jebkuras personas, "kas ar prettiesisku darbību, tīši vai neuzmanības dēļ radījusi zaudējumus vai nodarījusi miesas bojājumus citai personai" ([172]), vai no personas, "kas aizskārusi citu personu, tās brīvību vai reputāciju vai radījusi citai personai garīgas ciešanas" ([173]). Šādu civiltiesisko atbildību par kaitējumu, kas izriet no datu aizsardzības noteikumu pārkāpuma, ir apstiprinājusi Augstākā tiesa ([174]). Ja kaitējumu radījusi publiskās iestādes prettiesiska darbība, kompensācijas pieprasījumu var iesniegt arī saskaņā ar Valsts kompensāciju likumu ([175]). Prasību saskaņā ar Valsts kompensāciju likumu var iesniegt specializētajā "Kompensāciju padomē" vai tieši Korejas tiesās ([176]). Valsts atbildība sedz arī nemateriālo kaitējumu (piemēram, garīgās ciešanas) ([177]). Ja cietušais ir ārvalstnieks, Valsts kompensāciju likumu piemēro tik ilgi, kamēr viņa izcelsmes valsts vienlīdz nodrošina valsts kompensāciju Korejas valstspiederīgajiem ([178]).

(136) Ceturtkārt, Augstākā tiesa ir atzinusi, ka personām ir tiesības pieprasīt tiesiskās aizsardzības līdzekļus, ja ir pārkāptas viņu konstitucionālās tiesības, tostarp tiesības uz personas datu aizsardzību ([179]). Šajā saistībā tiesa var, piemēram, likt pārziņiem apturēt vai pārtraukt jebkādu prettiesisku darbību. Turklāt datu aizsardzības tiesības, tostarp *PIPA* aizsargātās tiesības, var īstenot, iesniedzot civilprasību. Šo privātuma konstitucionālās aizsardzības horizontālo piemērošanu attiecībām starp fiziskām personām ir atzinusi Augstākā tiesa ([180]).

([170]) Proti, noteikta lieluma patērētāju grupas vai bezpeļņas NVO, kuru izvirzītais nolūks ir datu aizsardzība (lai gan attiecībā uz pēdējo ir papildu prasība, ka vismaz 100 datu subjekti, kas saskārušies ar tādu pašu (tāda paša veida) pārkāpumu, ir iesnieguši pieprasījumu kolektīvās prasības iesniegšanai tiesā). Sk. *PIPA* 51. pantu.

([171]) *CIA* 43.–43-3. pantā ir noteikta arī atbildība par tāda kaitējuma kompensēšanu, kas radies minētā likuma pārkāpumu rezultātā.

([172]) Civillikuma 751. panta 1. punkts.

([173]) Civillikuma 750. pants.

([174]) Sk., piemēram, Augstākās tiesas 2018. gada 30. maija Lēmumu Nr. 2015Da251539, 251546, 251553, 251560, 251577. Turklāt Augstākā tiesa apstiprināja, ka par datu aizsardzības pārkāpumiem var piespriest kaitējuma kompensāciju saskaņā ar Civillikumu, sk. Augstākās tiesas 2012. gada 26. decembra Lēmumu Nr. 2011Da59834, 59858, 59841 (kopsavilkums angļu valodā pieejams tīmekļa vietnē http://library.scourt.go.kr/SCLIB_data/decision/9-69%202012.12.26.2011Da59834.htm). Šajā lietā Augstākā tiesa paskaidroja, ka, lai novērtētu, vai personai ir radītas emocionālas ciešanas, kas kvalificējamas kā kompensējams kaitējums, jāņem vērā vairāki faktori, piemēram, noplūdušās informācijas veids un raksturojums, personas identificējamība pārkāpuma dēļ, iespēja trešām personām piekļūt datiem, personas informācijas izplatīšanas apjoms un tas, vai tas izraisīja individuālo tiesību papildu pārkāpumus un kā personas informācija tika pārvaldīta un aizsargāta utt.

([175]) Pamatojoties uz Valsts kompensāciju likumu, personas var pieprasīt kompensāciju par kaitējumu, ko nodarījušas valsts amatpersonas, pildot savus oficiālos pienākumus, pārkāpjot likumu (likuma 2. panta 1. punkts).

([176]) Valsts kompensāciju likuma 9. un 12. pants. Ar likumu izveidotas apgabala padomes (tās vada attiecīgās prokuratūras prokurora vietnieks), Centrālā padome (tās priekšsēdētājs ir tieslietu ministra vietnieks) un Īpašā padome (tā atbild par kompensācijas pieprasījumiem par militārpersonu vai militārpersonu civilo darbinieku nodarīto kaitējumu, tās priekšsēdētājs ir valsts aizsardzības ministra vietnieks). Kompensācijas pieprasījumus principā izskata apgabala padomes, kurām noteiktos apstākļos ir jānosūta lietas Centrālajai/Īpašajai padomei, piemēram, ja kompensācija pārsniedz noteiktu summu vai ja persona iesniedz pieteikumu atkārtotai izskatīšanai. Visu padomju sastāvā ir tieslietu ministra iecelti locekļi (piemēram, Tieslietu ministrijas amatpersonas, tiesu izpildītāji, juristi un personas ar kompetenci valsts kompensāciju jomā), un uz tiem attiecas īpaši noteikumi par interešu konfliktu (sk. Valsts kompensāciju likuma Izpildes dekrēta 7. pantu).

([177]) Sk. Valsts kompensāciju likuma 8. pantu (kas attiecas uz Civillikumu), kā arī Civillikuma 751. pantu.

([178]) Valsts kompensāciju likuma 7. pants.

([179]) Augstākās tiesas 1996. gada 12. aprīļa Lēmums Nr. 93Da40614 un 2011. gada 2. septembra Lēmums Nr. 2008Da42430 (kopsavilkums angļu valodā pieejams tīmekļa vietnē https://www.scourt.go.kr/eng/supreme/decisions/NewDecisionsView.work?seq=696&pageIndex=1&mode=6&searchWord=).

([180]) Sk., piemēram, Augstākās tiesas 2011. gada 2. septembra Lēmumu Nr. 2008Da42430 (kopsavilkums angļu valodā pieejams tīmekļa vietnē https://www.scourt.go.kr/eng/supreme/decisions/NewDecisionsView.work?seq=696&pageIndex=1&mode=6&searchWord=).

(137) Visbeidzot, saskaņā ar Kriminālprocesa likumu (223. pants) personas var iesniegt krimināls ūdzību prokuroram vai kriminālpolicijas ierēdnim ([181]).

(138) Tādējādi Korejas sistēma piedāvā dažādus veidus, kā saņemt tiesisko aizsardzību, sākot no viegli pieejamiem un lētiem risinājumiem (piemēram, sazinoties ar Privātuma jautājumu zvanu centru vai izmantojot (kolektīvo) starpniecību) līdz administratīviem (*PIPC*) un tiesu iestāžu līdzekļiem, tostarp ar iespēju saņemt kompensāciju par kaitējumu.

3. **KOREJAS REPUBLIKAS PUBLISKO IESTĀŽU PIEKĻUVE PERSONAS DATIEM, KO NOSŪTA NO EIROPAS SAVIENĪBAS, UN ŠĀDU DATU IZMANTOŠANA**

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

(140) Novērtējot, vai nosacījumi, ar kādiem valdības piekļuve datiem, kas saskaņā ar šo lēmumu nosūtīti uz Koreju, atbilst "līdzvērtības pēc būtības" pārbaudei saskaņā ar Regulas (ES) 2016/679 45. panta 1. punktu, kā to interpretējusi Eiropas Savienības Tiesa, ņemot vērā Pamattiesību hartu, Komisija jo īpaši ņēma vērā turpmāk minētos kritērijus.

(141) Pirmkārt, jebkuriem ierobežojumiem, kas skar tiesības uz personas datu aizsardzību, ir jābūt paredzētiem tiesību aktos, un juridiskajam pamatam, kurš pieļauj šādu tiesību ierobežojumu, pašam jānosaka attiecīgo tiesību īstenošanas ierobežojuma darbības joma ([182]).

(142) Otrkārt, lai nodrošinātu atbilstību samērīguma prasībai, saskaņā ar kuru atkāpes no personas datu aizsardzības un to ierobežojumi piemērojami tikai tiktāl, ciktāl tas ir absolūti nepieciešams (noteikti vajadzīgs) demokrātiskā sabiedrībā, lai sasniegtu konkrētus vispārējas nozīmes mērķus, kas ir līdzvērtīgi Savienībā atzītajiem, attiecīgās trešās valsts tiesību aktos, kas pieļauj ierobežojumu, jāparedz skaidri un precīzi noteikumi, kas reglamentē attiecīgo pasākumu darbības jomu un piemērošanu, un jānosaka minimāli aizsardzības pasākumi, lai personām, kuru dati ir nosūtīti, būtu pietiekamas garantijas efektīvai viņu personas datu aizsardzībai pret ļaunprātīgas izmantošanas risku ([183]). Tiesību aktos jo īpaši jānorāda, kādos apstākļos un ar kādiem nosacījumiem var īstenot pasākumu, kas nodrošina šādu datu apstrādi ([184]), kā arī piemērot šādu prasību izpildei neatkarīgu pārraudzību ([185]).

(143) Treškārt, tiesību aktiem un to prasībām jābūt juridiski saistošiem saskaņā ar valsts tiesību aktiem. Tas vispirms attiecas uz attiecīgās trešās valsts iestādēm, bet šīm juridiskajām prasībām jābūt arī īstenojamām piespiedu kārtā tiesas ceļā pret šīm iestādēm ([186]). Datu subjektiem jo īpaši jābūt iespējai celt prasību neatkarīgā un objektīvā tiesā, lai gūtu piekļuvi saviem personas datiem vai panāktu šādu datu labošanu vai dzēšanu ([187]).

3.1. **Vispārējais tiesiskais regulējums**

(144) Ierobežojumi un garantijas, kas piemērojami personas datu vākšanai un vēlākai izmantošanai, ko veic Korejas publiskās iestādes, izriet no visaptveroša konstitucionālā regulējuma, īpašiem tiesību aktiem, kuri regulē to darbību krimināltiesību aizsardzības un valsts drošības jomā, kā arī noteikumiem, kas konkrēti attiecas uz personas datu apstrādi.

([181]) Kā paskaidrots 127. apsvērumā, datu nepareiza izmantošana ir uzskatāma par noziedzīgu nodarījumu saskaņā ar Krimināllikumu.
([182]) Sk. spriedumu lietā *Schrems II*, 174.–175. punkts, un minēto judikatūru. Attiecībā uz dalībvalstu publisko iestāžu piekļuvi sk. arī spriedumu lietā C-623/17 *Privacy International*, ECLI:EU:C:2020:790, 65. punkts, un apvienotajās lietās C-511/18, C-512/18 un C-520/18, *La Quadrature du Net* un citi, ECLI:EU:C:2020:791, 175. punkts.
([183]) Sk. spriedumu lietā Schrems II, 176. un 181. punkts, kā arī minēto judikatūru. Attiecībā uz dalībvalstu publisko iestāžu piekļuvi sk. arī spriedumu lietā *Privacy International*, 68. punkts, un *La Quadrature du Net* un citi, 132. punkts.
([184]) Sk. spriedumu lietā *Schrems II*, 176. punkts. Attiecībā uz dalībvalstu publisko iestāžu piekļuvi sk. arī spriedumu lietā *Privacy International*, 68. punkts, un *La Quadrature du Net* un citi, 132. punkts.
([185]) Sk. spriedumu lietā *Schrems II*, 179. punkts.
([186]) Sk. spriedumu lietā *Schrems II*, 181. un 182. punkts.
([187]) Sk. spriedumu lietā *Schrems I*, 95. punkts, un spriedumu lietā *Schrems II*, 194. punkts. Šajā sakarā EST ir īpaši uzsvērusi, ka Pamattiesību hartas 47. panta ievērošana, garantējot tiesības uz efektīvu tiesisko aizsardzību neatkarīgā un objektīvā tiesā, "atbilst arī Eiropas Savienībā prasītajam aizsardzības līmenim, kura ievērošana Komisijai ir jākonstatē, pirms tā pieņem lēmumu par atbilstību [aizsardzības līmeņa pietiekamību] saskaņā ar Regulas (ES) 2016/679 45. panta 1. punktu" (spriedums lietā *Schrems II*, 186. punkts).

(145) Pirmkārt, Korejas publisko iestāžu piekļuvi personas datiem reglamentē vispārējie likumības, nepieciešamības un samērīguma principi, kas izriet no Korejas Konstitūcijas ([188]). Jo īpaši pamattiesības un pamatbrīvības (tostarp tiesības uz privātumu un tiesības uz korespondences privātumu) ([189]) var ierobežot tikai ar tiesību aktiem un tikai tad, ja tas ir nepieciešams valsts drošībai vai likumības un kārtības uzturēšanai un sabiedrības labklājības labad. Šādi ierobežojumi nedrīkst ietekmēt attiecīgo tiesību vai brīvību būtību. Jo īpaši attiecībā uz kratīšanu un konfiskāciju Konstitūcijā ir paredzēts, ka tās var veikt tikai saskaņā ar tiesību aktiem, pamatojoties uz tiesneša izdotu orderi un ievērojot noteikto kārtību ([190]). Visbeidzot, personas var atsaukties uz savām tiesībām un brīvībām Konstitucionālajā tiesā, ja tās uzskata, ka publiskās iestādes tās ir pārkāpušas, kad tās īstenojušas savas pilnvaras ([191]). Līdzīgi arī personām, kurām nodarīts kaitējums valsts amatpersonas veiktas prettiesiskas darbības dēļ oficiālo pienākumu izpildes laikā, ir tiesības pieprasīt taisnīgu kompensāciju ([192]).

(146) Otrkārt, kā sīkāk aprakstīts 3.2.1. un 3.3.1. iedaļā, 145. apsvērumā minētie vispārējie principi ir atspoguļoti arī īpašajos tiesību aktos, kas regulē tiesībaizsardzības un valsts drošības iestāžu pilnvaras. Piemēram, attiecībā uz kriminālizmeklēšanu Kriminālprocesa likums (*Criminal Procedure Act* – "*CPA*") paredz, ka obligātos pasākumus var veikt tikai tad, ja tas ir skaidri noteikts *CPA*, un tikai tādā vismazākajā apmērā, kāds ir nepieciešams, lai sasniegtu izmeklēšanas mērķi ([193]). Līdzīgi arī Saziņas privātuma aizsardzības likuma (*Communications Privacy Protection Act* – "*CPPA*") 3. pantā ir aizliegts piekļūt privātai saziņai, izņemot gadījumus, kad tas tiek darīts, pamatojoties uz tiesību aktiem un ievērojot tajos noteiktos ierobežojumus un garantijas. Valsts drošības jomā Likums par Valsts izlūkdienestu (*National Intelligence Service – NIS*, "*NIS* likums") paredz, ka jebkurai piekļuvei saziņas vai atrašanās vietas informācijai jāatbilst tiesību aktiem un par ļaunprātīgu varas izmantošanu un likumpārkāpumiem piemēro krimināsodus ([194]).

(147) Treškārt, uz personas datu apstrādi, ko veic publiskās iestādes, tostarp tiesībaizsardzības un valsts drošības nolūkos, attiecas datu aizsardzības noteikumi saskaņā ar *PIPA* ([195]). *PIPA* 5. panta 1. punktā kā vispārējs princips ir noteikts, ka publiskajām iestādēm ir jāizstrādā politika, ko izmanto, lai nepieļautu "personas informācijas ļaunprātīgu un nepareizu izmantošanu, nediskrētu novērošanu un izsekošanu utt. un lai veicinātu cilvēka cieņas un personas privātuma respektēšanu". Turklāt ikvienam pārzinim ir jāapstrādā personas dati tādā veidā, kas samazina iespēju pārkāpt datu subjekta privātumu (*PIPA* 3. panta 6. punkts).

(148) Visas *PIPA* prasības, kas sīki aprakstītas 2. iedaļā, attiecas uz personas datu apstrādi tiesībaizsardzības nolūkos. Tās ietver pamatprincipus (piem., likumīgums un godprātība, nolūka ierobežojums, precizitāte, datu minimizēšana, glabāšanas ierobežojums, drošība un pārredzamība), pienākumus (piem., attiecībā uz datu aizsardzības pārkāpumu paziņošanu un sensitīviem datiem) un tiesības (iegūt piekļuvi, pieprasīt labošanu, dzēšanu un izmantošanas apturēšanu).

(149) Lai gan uz personas datu apstrādi, ko veic valsts drošības nolūkos, saskaņā ar *PIPA* attiecas ierobežotāks noteikumu kopumus, piemēro arī pamatprincipus, kā arī noteikumus par pārraudzību, izpildi un tiesisko aizsardzību ([196]). Konkrētāk, *PIPA* 3. un 4. pantā ir noteikti vispārējie datu aizsardzības principi (likumīgums un godprātība, nolūka ierobežojums, precizitāte, datu minimizēšana, drošība un pārredzamība) un individuālās tiesības (tiesības saņemt informāciju, piekļuves tiesības un tiesības pieprasīt datu labošanu, dzēšanu un izmantošanas apturēšanu) ([197]). Turklāt *PIPA* 4. panta 5. punktā ir noteikts, ka personām ātrā un taisnīgā procedūrā ir tiesības saņemt atbilstošu tiesisko aizsardzību par jebkuru kaitējumu, kas radies no to personas datu apstrādes.

([188]) Sk. II pielikuma 1.1. iedaļu.
([189]) Konstitūcijas 37. panta 2. punkts.
([190]) Konstitūcijas 16. pants un 12. panta 3. punkts. Turklāt Konstitūcijas 12. panta 3. punktā ir noteikti izņēmuma apstākļi, kādos kratīšana vai konfiskācija var tikt veikta bez ordera (tomēr joprojām ir nepieciešams *ex post* orderis), t. i., pārkāpuma izdarīšanas brīdī vai par noziegumiem, par kuriem var piespriest brīvības atņemšanu vismaz uz trim gadiem, ja pastāv risks, ka pierādījumi tiks iznīcināti vai aizdomās turētais pazudīs.
([191]) Konstitucionālās tiesas likuma 68. panta 1. punkts.
([192]) Konstitūcijas 29. panta 1. punkts.
([193]) *CPA* 199. panta 1. punkts. Vispārīgāk runājot, publiskajām iestādēm, īstenojot savas pilnvaras saskaņā ar *CPA*, ir jāievēro aizdomās turamā un citu attiecīgo personu pamattiesības (*CPA* 198. panta 2. punkts).
([194]) NIS likuma 14. pants.
([195]) Sk. II pielikuma 1.2. iedaļu.
([196]) *PIPA* 58. panta 1. punkta 2. apakšpunkts. Sk. arī Paziņojuma Nr. 2021-5 6. iedaļu (I pielikums). Šis atbrīvojums no atsevišķiem *PIPA* noteikumiem attiecas tikai tad, ja personas datus apstrādā "valsts drošības nolūkos". Kad valsts drošības situācija, kura pamato datu apstrādi, ir beigusies, atbrīvojumu vairs nevar izmantot un piemēro visas *PIPA* prasības.
([197]) Šādas tiesības var ierobežot tikai tad, ja tas ir paredzēts tiesību aktos, tikai tādā apmērā un tik ilgi, cik tas ir nepieciešams un samērīgi, lai aizsargātu svarīgu sabiedrības interešu mērķi, vai ja tiesību piešķiršana varētu radīt kaitējumu trešās personas dzīvībai vai veselībai vai nepamatoti aizskart trešās personas mantiskās un citas intereses. Sk. Paziņojuma Nr. 2021-5 6. iedaļu.

Tas ir papildināts ar konkrētākiem pienākumiem, proti, apstrādāt personas datus tikai tādā apjomā, kāds nepieciešams, lai sasniegtu paredzēto nolūku, un minimālajā laikposmā, ieviest nepieciešamos pasākumus, lai nodrošinātu drošu datu pārvaldību un pienācīgu apstrādi (piem., tehniski, pārvaldības un fiziski aizsardzības pasākumi), kā arī ieviest pasākumus individuālu sūdzību atbilstīgai izskatīšanai ([198]). Visbeidzot, Korejas Konstitūcijā (sk. 145. apsvērumu) paredzētie vispārējie likumības, nepieciešamības un samērīguma principi attiecas arī uz personas datu apstrādi valsts drošības nolūkos.

(150) Šos vispārējos ierobežojumus un garantijas personas var apstrīdēt neatkarīgās pārraudzības struktūrās (piem., *PIPC* un/vai Valsts cilvēktiesību komisijā, sk. 177.–178. apsvērumu) un tiesās (sk. 179.–183. apsvērumu), lai iegūtu tiesisko aizsardzību.

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

(151) Korejas Republikas tiesību aktos ir noteikti vairāki ierobežojumi attiecībā uz piekļuvi personas datiem un to izmantošanu krimināltiesību aizsardzības nolūkos, kā arī ir paredzēti pārraudzības un tiesiskās aizsardzības mehānismi, kas atbilst šā lēmuma 141.–143. apsvērumā minētajām prasībām. Nosacījumi, saskaņā ar kuriem var notikt šāda piekļuve, un garantijas, kas piemērojamas šo pilnvaru izmantošanai, ir sīki novērtēti turpmākajās iedaļās.

3.2.1. *Juridiskais pamats, ierobežojumi un garantijas*

(152) Korejā esošu pārziņu apstrādātos personas datus, kas saskaņā ar šo lēmumu tiktu nosūtīti no Savienības ([199]), Korejas iestādes var vākt krimināltiesību aizsardzības nolūkā saistībā ar kratīšanu vai konfiskāciju (pamatojoties uz *CPA*), piekļūstot saziņas informācijai (pamatojoties uz *CPPA*) vai iegūstot abonenta datus pēc tam, kad iesniegts pieprasījums par brīvprātīgu informācijas izpaušanu (pamatojoties uz Telesakaru darījumdarbības likumu (*Telecommunications Business Act – "TBA"*)) ([200]).

3.2.1.1. Kratīšana un konfiskācija

(153) *CPA* ir paredzēts, ka kratīšanu vai konfiskāciju var veikt tikai tad, ja persona tiek turēta aizdomās par noziegumu, tas ir nepieciešams izmeklēšanai un ir konstatēta saistība starp izmeklēšanu un personu, kurai veicama kratīšana, vai priekšmetu, kas pārbaudāms vai konfiscējams ([201]). Turklāt kratīšanu vai konfiskāciju (kā obligātu pasākumu) drīkst atļaut/veikt tikai vismazākajā nepieciešamajā apmērā ([202]). Ja kratīšana attiecas uz datora disku vai citu datu nesēju, tad būtībā tiks konfiscēti tikai nepieciešamie dati (kopēti vai izdrukāti), nevis viss datu nesējs ([203]). To var konfiscēt tikai tad, ja tiek uzskatīts, ka ir būtiski neiespējami atsevišķi izdrukāt vai kopēt nepieciešamos datus, vai ja tiek uzskatīts, ka ir būtiski nepraktiski citādi sasniegt kratīšanas mērķi ([204]). Tādēļ *CPA* ir paredzēti skaidri un precīzi noteikumi par šo pasākumu darbības jomu un piemērošanu, tādējādi nodrošinot, ka iejaukšanās personu tiesībās kratīšanas vai konfiskācijas gadījumā būs ierobežota līdz tādai, kas ir nepieciešama konkrētai krimināllizmeklēšanai un samērīga ar noteikto mērķi.

([198]) *PIPA* 58. panta 4. punkts.

([199]) Sk. II pielikuma 2.1. iedaļu. Korejas valdības oficiālajā apliecinājumā (II pielikuma 2.1. iedaļa) arī ir norādīta iespēja vākt finanšu darījumu informāciju nolūkā novērst nelikumīgi iegūtu līdzekļu legalizāciju un terorisma finansēšanu, pamatojoties uz Likumu par konkrētu finanšu darījumu informācijas paziņošanu un izmantošanu (*Act on Reporting and Using Specified Financial Transaction Information – "ARUSFTI"*). Tomēr *ARUSFTI* informācijas izpaušanas pienākumi ir noteikti tikai tiem pārziņiem, kuri apstrādā personas kredītinformāciju saskaņā ar *CIA* un uz kuriem attiecas Finanšu pakalpojumu komitejas (*FSC*) pārraudzība (sk. 13. apsvērumu). Tā kā šādu pārziņu veiktā personas kredītinformācijas apstrāde nav ietverta šā lēmuma darbības jomā, šajā novērtējumā *ARUSFTI* netiek ņemts vērā.

([200]) *CPPA* 3. pantā kā iespējamais juridiskais pamats saziņas datu vākšanai ir minēts arī Militārās tiesas likums. Tomēr minētais likums reglamentē informācijas vākšanu par militārpersonām un uz civilpersonām var attiekties tikai ierobežotā skaitā gadījumu (piem., lietu militārajā tiesā var ierosināt, ja militārpersonas un civilpersonas izdara noziegumu kopā vai ja persona izdara noziegumu pret militārpersonu, sk. Militārās tiesas likuma 2. pantu). Jebkurā gadījumā tajā ir paredzēti vispārīgi noteikumi, kas reglamentē kratīšanu un konfiskāciju un kas ir līdzīgi *CPA* paredzētajiem (sk., piem., Militārās tiesas likuma 146.–149. pantu un 153.–156. pantu), un tajā ir paredzēts, piem., ka pasta sūtījumus var savākt tikai tad, ja tas ir nepieciešams izmeklēšanai un pamatojoties uz Militārās tiesas orderi. Tiktāl, ciktāl elektroniskā saziņa var tikt vākta, pamatojoties uz minēto likumu, piemēro *CPPA* ierobežojumus un garantijas. Sk. II pielikuma 2.2.2. iedaļu un 50. zemsvītras piezīmi.

([201]) *CPA* 215. panta 1. un 2. punkts. Sk. arī *CPA* 106. panta 1. punktu, 107. pantu un 109. pantu, kas paredz, ka tiesas var veikt kratīšanu un konfiskāciju, ja attiecīgie priekšmeti vai personas tiek uzskatīti par saistītiem ar konkrēto lietu. Sk. II pielikuma 2.2.1.2. iedaļu.

([202]) *CPA* 199. panta 1. punkts.

([203]) *CPA* 106. panta 3. punkts.

([204]) *CPA* 106. panta 3. punkts.

(154) Procesuālo garantiju ziņā *CPA* ir noteikts, ka no tiesas ir jāsaņem orderis, lai varētu veikt kratīšanu vai konfiskāciju ([205]). Kratīšana vai konfiskācija bez ordera ir atļauta tikai izņēmuma gadījumos, proti, steidzamos apstākļos ([206]), uz vietas aizdomās turētā aizturēšanas vai apcietināšanas brīdī ([207]) vai arī gadījumos, kad aizdomās turētais vai trešā persona (attiecībā uz personas datiem – attiecīgā persona) izmet vai brīvprātīgi uzrāda priekšmetu ([208]). Par nelikumīgu kratīšanu un konfiskāciju piemēro krimināLsodus ([209]), un visus pierādījumus, kas iegūti, pārkāpjot *CPA*, uzskata par nepieņemamiem ([210]). Visbeidzot, attiecīgās personas vienmēr ir nekavējoties jāinformē par kratīšanu vai konfiskāciju (tostarp viņu datu konfiskāciju) ([211]), kas savukārt atvieglos personas materiālo tiesību īstenošanu un tiesības uz tiesisku aizsardzību (sk. jo īpaši iespēju apstrīdēt konfiskācijas ordera izpildi, sk. 180. apsvērumu).

3.2.1.2. Piekļuve saziņas informācijai

(155) Pamatojoties uz *CPPA*, Korejas krimināltiesību aizsardzības iestādes var veikt divu veidu pasākumus ([212]): no vienas puses, "saziņas apstiprinājuma datu" vākšanu ([213]), kas ietver telesakaru datumu, to sākuma un beigu laiku, veikto un saņemto zvanu skaitu, kā arī otras puses abonenta numuru, izmantošanas biežumu, žurnāldatnes par telesakaru pakalpojumu izmantošanu un atrašanās vietas informāciju (piem., no pārraides torņiem, kuros uztver signālus); un, no otras puses, "saziņu ierobežojošus pasākumus", kas ietver gan tradicionālā pasta satura vākšanu, gan telesakaru satura tiešu pārtveršanu ([214]).

(156) Saziņas apstiprinājuma datiem var piekļūt tikai tad, ja ir jāveic krimināLizmeklēšana vai jāizpilda sods ([215]), pamatojoties uz tiesas izdotu orderi ([216]). Šajā saistībā *CPPA* ir prasīts sniegt detalizētu informāciju gan ordera pieprasījuma pieteikumā (piem., par pieprasījuma iemesliem, saistību ar mērķobjektu/abonentu un nepieciešamajiem datiem), gan orderī (piem., par pasākuma mērķobjektu, uzdevumu un darbības jomu) ([217]). Datu vākšanu bez ordera var veikt tikai tad, ja steidzamības dēļ no tiesas nav iespējams saņemt atļauju, bet šādā gadījumā orderis ir

([205]) *CPA* 215. panta 1. un 2. punkts, *CPA* 113. pants. Iesniedzot pieteikumu ordera saņemšanai, attiecīgajā iestādē jāiesniedz materiāli, kas pierāda, ka ir pamats aizdomām tam, ka persona ir izdarījusi noziegumu, ka ir nepieciešama kratīšana, pārbaude vai konfiskācija un ka attiecīgie konfiscējamie priekšmeti eksistē (Kriminālprocesuālo noteikumu 108. panta 1. punkts). Orderī cita starpā jānorāda aizdomās turamās personas vārds un uzvārds un nodarījums; pārmeklējamā vieta, persona vai priekšmeti vai konfiscējamie priekšmeti; izdošanas datums un spēkā esības laikposms (114. panta 1. punkts kopā ar *CPA* 219. pantu). Sk. II pielikuma 2.2.1.2. iedaļu.

([206]) Proti, ja orderi nav iespējams saņemt nodarījuma izdarīšanas vietā pastāvošās steidzamības dēļ (*CPA* 216. panta 3. punkts), bet šajā gadījumā joprojām ir nekavējoties jāsaņem orderis vēlāk (*CPA* 216. panta 3. punkts).

([207]) *CPA* 216. panta 1. un 2. punkts.

([208]) *CPA* 218. pants. Turklāt, kā skaidrots II pielikuma 2.2.1.2. iedaļā, brīvprātīgi uzrādītie priekšmeti tiek atzīti par pierādījumiem tiesvedībā tikai tad, ja nav pamatotu šaubu par uzrādīšanas brīvprātīgumu, kas prokuroram jāpierāda.

([209]) Krimināllikuma 321. pants.

([210]) *CPA* 308-2. pants. Turklāt persona (un tās advokāts) var atrasties klāt, kad tiek izpildīts kratīšanas vai konfiskācijas orderis, un tādējādi var arī izvirzīt iebildumu laikā, kad tiek izpildīts orderis (*CPA* 121. un 219. pants).

([211]) *CPA* 121. un 122. pants (attiecībā uz kratīšanu) un *CPA* 219. pants kopā ar *CPA* 106. panta 4. punktu (attiecībā uz konfiskāciju).

([212]) Sk. arī II pielikuma 2.2.2.1. iedaļu. Šādus pasākumus var veikt ar telesakaru operatoru piespiedu palīdzību, piešķirot šiem operatoriem rakstisku atļauju, kura saņemta no tiesas (*CPPA* 9. panta 2. punkts) un kura operatoriem ir jāglabā (*CPPA* 15-2. pants un *CPPA* Izpildes dekrēta 12. pants). Telesakaru pakalpojumu sniedzēji var atteikties sadarboties, ja informācija par mērķpersonu, kā norādīts tiesas rakstiskajā atļaujā (piem., personas tālruņa numurs), ir nepareiza, un jebkuros apstākļos tiem ir aizliegts atklāt telesakaros izmantotās paroles (*CPPA* 9. panta 4. punkts).

([213]) *CPPA* 2. panta 11. punkts.

([214]) Sk. *CPPA* 2. panta 6. punktu, kas attiecas uz "cenzūru" (pasta atvēršana bez attiecīgās personas piekrišanas vai zināšanu iegūšana par tā saturu, tā ierakstīšana vai aizturēšana, izmantojot citus līdzekļus), un *CPPA* 2. panta 7. punktu, kas attiecas uz "sarunu noklausīšanos" (telesakaru satura iegūšana vai ierakstīšana, noklausoties vai kopīgi nolasot sakaru skaņas, vārdus, simbolus vai attēlus, izmantojot elektroniskās un mehāniskās ierīces bez attiecīgās personas piekrišanas, vai iejaucoties to pārraidē un uztveršanā).

([215]) *CPPA* 13. panta 1. punkts. Sk. arī II pielikuma 2.2.2.3. iedaļu. Turklāt reāllaika atrašanās vietas izsekošanas datus un saziņas apstiprinājuma datus, kas attiecas uz konkrētu bāzes staciju, var vākt tikai smagu noziegumu izmeklēšanai vai gadījumos, kad citādi būtu grūti novērst nozieguma izdarīšanu vai vākt pierādījumus (*CPPA* 13. panta 2. punkts). Tas atspoguļo vajadzību paredzēt papildu garantijas, jo īpaši attiecībā uz pasākumiem, kas skar privātumu, saskaņā ar samērīguma principu.

([216]) *CPPA* 13. un 6. pants.

([217]) Sk. *CPPA* 13. panta 3. un 9. punktu kopā ar 6. panta 4. un 6. punktu.

jāsaņem un jānodod telesakaru pakalpojumu sniedzējam uzreiz pēc datu pieprasīšanas ([218]). Ja tiesa atsakās piešķirt šo atļauju, savāktā informācija ir jāiznīcina ([219]).

(157) Saistībā ar papildu garantijām attiecībā uz saziņas apstiprinājuma datu vākšanu *CPPA* ir noteiktas īpašas uzskaites veikšanas un pārredzamības prasības ([220]). Konkrētāk, gan krimināltiesību aizsardzības iestādēm ([221]), gan telesakaru pakalpojumu sniedzējiem ([222]) ir jāveic pieprasījumu un izpaustās informācijas uzskaite. Turklāt krimināltiesību aizsardzības īstenošanas laikā būtībā ir jāpaziņo personām par to, ka tiek vākti to saziņas apstiprinājuma dati ([223]). Šo paziņošanu var atlikt tikai izņēmuma apstākļos, pamatojoties uz kompetentās apgabala prokuratūras direktora atļauju ([224]). Šādu atļauju var izsniegt tikai tad, ja paziņojums varētu: 1) apdraudēt valsts drošību, sabiedrisko drošību un kārtību, 2) izraisīt nāvi vai miesas bojājumus, 3) kavēt taisnīgu tiesvedību (piem., izraisīt pierādījumu iznīcināšanu vai apdraudējumu lieciniekiem) vai 4) apmelot aizdomās turētos, cietušos vai citas personas, kas saistītas ar lietu, vai aizskart to privātumu. Šajos gadījumos paziņojums jāsniedz 30 dienu laikā, tiklīdz atlikšanas pamatojums(-i) vairs nepastāv ([225]). Pēc paziņojuma saņemšanas personām ir tiesības saņemt informāciju par to datu vākšanas iemesliem ([226]).

(158) Attiecībā uz saziņu ierobežojošiem pasākumiem piemēro stingrākus noteikumus, un pasākumus var izmantot tikai tad, ja ir pamatots iemesls aizdomām, ka tiek plānoti, tiek izdarīti vai ir izdarīti noteikti smagi noziegumi, kuri konkrēti uzskaitīti *CPPA* ([227]). Turklāt saziņu ierobežojošus pasākumus var veikt tikai kā galēju pasākumu un gadījumos, kad citādi ir grūti novērst nozieguma izdarīšanu, aizturēt noziedznieku vai vākt pierādījumus ([228]). Tie ir nekavējoties jāpārtrauc, tiklīdz tie vairs nav nepieciešami, lai nodrošinātu, ka saziņas privātuma pārkāpumi ir pēc iespējas mazāki ([229]). Informācija, kas ir nelikumīgi iegūta, izmantojot saziņu ierobežojošus pasākumus, netiek pieņemta kā pierādījums tiesā vai disciplinārlietās ([230]).

(159) Procesuālo garantiju ziņā *CPPA* ir noteikts, ka ir jāsaņem tiesas orderis, lai varētu veikt saziņu ierobežojošus pasākumus ([231]). Turklāt *CPPA* ir prasīts, lai ordera pieprasījuma pieteikumā un pašā orderī būtu iekļauta detalizēta informācija ([232]), tostarp pieprasījuma pamatojums, kā arī vācamā saziņa (kam jābūt izmeklēšanā aizdomās turētās personas saziņai) ([233]). Šādus pasākumus bez ordera var veikt tikai nenovēršamu organizētās noziedzības draudu gadījumā vai tad, ja draud cits smags noziegums, kas var tieši izraisīt nāvi vai smagus miesas bojājumus,

([218]) *CPPA* 13. panta 2. punkts.
([219]) *CPPA* 13. panta 3. punkts.
([220]) Sk. II pielikuma 2.2.2.3. iedaļu.
([221]) *CPPA* 13. panta 5. un 6. punkts.
([222]) *CPPA* 13. panta 7. punkts. Turklāt telesakaru pakalpojumu sniedzējiem divas reizes gadā jāziņo Zinātnes un IKT ministrijai par saziņas apstiprinājuma datu izpaušanu.
([223]) Sk. *CPPA* 13-3. panta 7. punktu kopā ar *CPPA* 9-2. pantu. Konkrētāk, personas ir jāinformē 30 dienu laikā pēc tam, kad ir pieņemts lēmums sākt (nesākt) kriminālvajāšanu, vai 30 dienu laikā no dienas, kad pagājis viens gads pēc tam, kad pieņemts lēmums apturēt apsūdzību (lai gan jebkurā gadījumā paziņojums jāsniedz 30 dienu laikā no dienas, kad pagājis viens gads pēc informācijas vākšanas), sk. *CPPA* 13-3. panta 1. punktu.
([224]) *CPPA* 13-3. panta 2. un 3. punkts.
([225]) *CPPA* 13-3. panta 4. punkts.
([226]) *CPPA* 13-3. panta 5. punkts. Pēc personas pieprasījuma prokuroram vai kriminālpolicijas ierēdnim 30 dienu laikā pēc pieprasījuma saņemšanas jāsniedz rakstiska informācija par iemesliem, ja vien nav piemērojams kāds no izņēmumiem paziņojuma atlikšanai (*CPPA* 13-3. panta 6. punkts).
([227]) Piemēram, nemieri, ar narkotikām saistīti noziegumi, ar sprāgstvielām saistīti noziegumi, kā arī noziegumi, kas saistīti ar valsts drošību, diplomātiskajām attiecībām vai militārajām bāzēm un iekārtām, sk. *CPPA* 5. panta 1. punktu. Sk. arī II pielikuma 2.2.2.2. iedaļu.
([228]) *CPPA* 3. panta 2. punkts un 5. panta 1. punkts.
([229]) *CPPA* Izpildes dekrēta 2. pants.
([230]) *CPPA* 4. pants.
([231]) *CPPA* 6. panta 1., 2. un 5.–6. punkts.
([232]) Ordera pieprasījuma pieteikumā jāapraksta: 1) pamatotie iemesli (*prima facie*) aizdomām, ka viens no uzskaitītajiem noziegumiem ir plānots, tiek izdarīts vai ir izdarīts, kā arī visi apliecinošie materiāli; 2) saziņu ierobežojošie pasākumi, kā arī to mērķobjekts, darbības joma, mērķis un spēkā esības laikposms; un 3) vieta, kur pasākumi tiks veikti, un tas, kā tie tiks veikti (*CPPA* 6. panta 4. punkts un *CPPA* Izpildes dekrēta 4. panta 1. punkts). Orderī jānorāda pasākumi, kā arī to mērķobjekts, darbības joma, spēkā esības laikposms, īstenošanas vieta un veids (*CPPA* 6. panta 6. punkts).
([233]) Saziņu ierobežojoša pasākuma mērķobjektam jābūt īpašiem pasta sūtījumiem vai telesakariem, ko nosūta vai saņem aizdomās turētais, vai pasta sūtījumiem vai telesakariem, ko aizdomās turētais nosūta vai saņem noteiktā laikposmā (*CPPA* 5. panta 2. punkts).

un pastāv ārkārtas situācija, kuras dēļ nav iespējams veikt parasto procedūru ([234]). Tomēr šādā gadījumā ordera pieprasījuma pieteikums ir jāiesniedz uzreiz pēc pasākuma veikšanas ([235]). Saziņu ierobežojošus pasākumus var veikt tikai ne ilgāk kā divus mēnešus ([236]), un to veikšanu var pagarināt tikai ar tiesas apstiprinājumu, ja joprojām pastāv atbilstība pasākumu veikšanas nosacījumiem ([237]). Pagarinātais laikposms kopumā nedrīkst pārsniegt vienu gadu vai trīs gadus noteiktiem sevišķi smagiem noziegumiem (piem., noziegumiem, kas saistīti ar nemieriem, ārvalstu agresiju, valsts drošību) ([238]).

(160) Līdzīgi kā tas ir saziņas apstiprinājuma datu vākšanas gadījumā, *CPPA* ir pieprasīts telesakaru pakalpojumu sniedzējiem ([239]) un tiesībaizsardzības iestādēm ([240]) veikt saziņu ierobežojošo pasākumu izpildes uzskaiti un tajā ir paredzēta attiecīgās personas informēšana, ko izņēmuma kārtā var atlikt, ja tas ir nepieciešams svarīgu sabiedrības interešu dēļ ([241]).

(161) Visbeidzot, par vairāku *CPPA* noteikto ierobežojumu un garantiju neievērošanu (tostarp, piem., par pienākumu saņemt orderi, veikt uzskaiti un paziņošanu personai neizpildi) gan attiecībā uz saziņas apstiprinājuma datu vākšanu, gan saziņu ierobežojošu pasākumu izmantošanu piemēro krimināLsodus ([242]).

(162) Tādējādi krimināltiesību aizsardzības iestāžu pilnvaras vākt saziņas datus, pamatojoties uz *CPPA* (gan saziņas, gan saziņas apstiprinājuma datu saturu), ir paredzētas ar skaidriem un precīziem noteikumiem un uz tām attiecas vairākas garantijas. Šīs garantijas jo īpaši nodrošina minēto pasākumu izpildes pārraudzību gan *ex ante* (ar iepriekšēju tiesas apstiprinājumu), gan *ex post* (ar uzskaites un ziņošanas prasībām) un atvieglo personu piekļuvi efektīviem tiesiskās aizsardzības līdzekļiem (nodrošinot, ka personas ir informētas par to datu vākšanu).

3.2.1.3. Pieprasījumi par abonenta datu brīvprātīgu izpaušanu

(163) Papildus 153.–162. apsvērumā aprakstītajiem obligātajiem pasākumiem Korejas tiesībaizsardzības iestādes var pieprasīt telesakaru pakalpojumu sniedzējiem brīvprātīgi vākt "saziņas datus", lai atbalstītu krimināllietu iztiesāšanu tiesā, izmeklēšanu vai soda izpildi (*TBA* 83. panta 3. punkts). Šāda iespēja pastāv tikai attiecībā uz ierobežotām datu kopām, t. i., lietotāju vārdu, uzvārdu, iedzīvotāju reģistrācijas numuru, adresi un tālruņa numuru, datumiem, kuros lietotāji sāk vai beidz lietot abonementu, kā arī lietotāja identifikācijas kodiem (t. i., kodiem, ko izmanto, lai identificētu datorsistēmu vai sakaru tīklu likumīgo lietotāju) ([243]). Tā kā par "lietotājiem" uzskata tikai tās personas, kas tieši slēdz līgumus par pakalpojumiem ar Korejas telesakaru pakalpojumu sniedzēju ([244]), ES personas, kuru datus nosūta uz Korejas Republiku, parasti neietilpst šajā kategorijā ([245]).

(164) Šādai brīvprātīgai izpaušanai piemēro dažādus ierobežojumus gan attiecībā uz tiesībaizsardzības iestādes pilnvaru īstenošanu, gan attiecībā uz telesakaru operatora atbildi. Ir noteikta vispārīga prasība, ka tiesībaizsardzības iestādēm jārīkojas saskaņā ar konstitucionālajiem nepieciešamības un samērīguma principiem (Konstitūcijas 12. panta 1. punkts un 37. panta 2. punkts), tostarp arī tad, kad tās pieprasa brīvprātīgi sniegt informāciju. Turklāt tām ir jāizpilda *PIPA* prasības, jo īpaši, ka personas dati jāvāc minimālā apmērā, proti, tikai tādā apmērā, kāds ir

([234]) *CPPA* 8. panta 1. punkts. Tomēr informācijas vākšanai ārkārtas situācijās vienmēr jānotiek saskaņā ar "ārkārtas cenzūras / sarunu noklausīšanās paziņojumu", un iestādei, kas veic vākšanu, ir jāreģistrē visi ārkārtas pasākumi (*CPPA* 8. panta 4. punkts).

([235]) Vākšana ir nekavējoties jāpārtrauc, ja tiesībaizsardzības iestāde 36 stundu laikā nav saņēmusi tiesas atļauju (*CPPA* 8. panta 2. punkts), un šādā gadījumā savāktā informācija principā tiks iznīcināta, kā skaidrots II pielikuma 2.2.2.2. iedaļā. Tiesa ir arī jāinformē par gadījumu, kad ārkārtas pasākumi ir veikti tik īsā laikā, ka atļauja nav vajadzīga (piem., ja aizdomās turētais tiek aizturēts uzreiz pēc pārtveršanas uzsākšanas, sk. *CPPA* 8. panta 5. punktu). Šādā gadījumā tiesā jāiesniedz informācija par īstenošanas mērķi, mērķobjektu, darbības jomu, laikposmu, vietu un vākšanas metodi, kā arī pamatojumi, kāpēc nav iesniegts tiesas atļaujas pieprasījums (*CPPA* 8. panta 6.–7. punkts).

([236]) *CPPA* 6. panta 7. punkts. Ja pasākumu mērķis minētajā laikposmā tiek sasniegts agrāk, pasākumi nekavējoties jāpārtrauc.

([237]) *CPPA* 6. panta 7.–8. punkts.

([238]) *CPPA* 6. panta 8. punkts.

([239]) *CPPA* 9. panta 3. punkts.

([240]) *CPPA* Izpildes dekrēta 18. panta 1. punkts.

([241]) Konkrēti, prokuroram 30 dienu laikā pēc tam, kad izvirzīta apsūdzība vai izdots rīkojums, kas paredz, ka persona nav apsūdzēta vai aizturēta, par to jāpaziņo attiecīgajai personai (*CPPA* 9-2. panta 1. punkts). Paziņojumu var atlikt ar apgabala prokuratūras vadītāja apstiprinājumu, ja tas varētu nopietni apdraudēt valsts drošību vai sagraut sabiedrisko drošību un kārtību, vai ja tas varētu radīt būtisku kaitējumu citu personu dzīvībai un veselībai (*CPPA* 9-2. panta 4.–6. punkts).

([242]) *CPPA* 16. un 17. pants.

([243]) *TBA* 83. panta 3. punkts. Sk. arī II pielikuma 2.2.3. iedaļu.

([244]) *TBA* 2. panta 9. punkts.

([245]) Sk. arī II pielikuma 2.2.3. iedaļu.

nepieciešamas, lai sasniegtu leģitīmo nolūku, un tādā veidā, lai pēc iespējas samazinātu ietekmi uz personu privātumu (kā noteikts *PIPA* 3. panta 1. un 6. punktā). Konkrētāk, saskaņā ar *TBA* sagatavotie saziņas datu iegūšanas pieprasījumi ir jāiesniedz rakstiski un tajos jānorāda pieprasījuma iemesli, saistība ar attiecīgo lietotāju un pieprasīto datu apjoms ([246]).

(165) Telesakaru pakalpojumu sniedzējiem nav obligāti jāizpilda šādi pieprasījumi, un tie var tos izpildīt tikai saskaņā ar *PIPA*. Tas jo īpaši nozīmē, ka tiem ir jālīdzsvaro dažādās attiecīgās intereses un tie var nesniegt datus, ja, to darot, iespējams, negodīgi tiktu aizskartas personas vai trešās personas intereses ([247]). Tā tas būtu, piemēram, gadījumā, ja būtu skaidrs, ka pieprasījuma iesniedzēja iestāde ir ļaunprātīgi izmantojusi savas pilnvaras ([248]). Telesakaru operatoriem jāveic izpaustās informācijas uzskaite saskaņā ar *TBA* un divas reizes gadā jāziņo par to zinātnes un IKT ministram ([249]).

(166) Turklāt saskaņā ar Paziņojuma Nr. 2021-5 (I pielikums) 3. iedaļu telesakaru pakalpojumu sniedzējiem būtībā ir jāinformē attiecīgā persona, kad tie brīvprātīgi izpilda pieprasījumu ([250]). Tas savukārt ļaus personai izmantot savas tiesības un, ja tās dati ir izpausti nelikumīgi, saņemt tiesisko aizsardzību vai nu pret pārzini (piem., par datu izpaušanu, kas veikta, pārkāpjot *PIPA*, vai par tāda pieprasījuma izpildi, kurš ir bijis acīm redzami nesamērīgs), vai pret tiesībaizsardzības iestādi (piem., par rīcību, ar ko pārkāpj nepieciešamības un samērīguma ierobežojumus, vai par *TBA* procedūras noteikumu neievērošanu).

3.2.2. *Savāktās informācijas turpmāka izmantošana*

(167) Uz Korejas krimināltiesību aizsardzības iestāžu savākto personas datu apstrādi attiecas visas PIPA prasības, tostarp attiecībā uz nolūka ierobežojumu (*PIPA* 3. panta 1.–2. punkts), izmantošanas likumīgumu un sniegšanu trešām personām (*PIPA* 15., 17. un 18. pants), starptautisku nodošanu (*PIPA* 17. un 18. pants kopā ar Paziņojuma Nr. 2021-5 2. iedaļu) ([251]), samērīgumu / datu minimizēšanu (*PIPA* 3. panta 1. un 6. punkts) un glabāšanas ierobežojumu (*PIPA* 21. pants) ([252]).

(168) Attiecībā uz saziņas saturu, kas iegūts, īstenojot saziņu ierobežojošus pasākumus, *CPPA* ir skaidri ierobežota tā iespējamā izmantošana, attiecinot to tikai uz smagu noziegumu izmeklēšanu, kriminālvajāšanu vai novēršanu ([253]), šādu noziegumu disciplinārlietām, prasībām par kaitējuma atlīdzināšanu, ko tiesā cēlusi saziņā iesaistītā persona, vai ja to īpaši atļauj citi tiesību akti ([254]). Turklāt saturu, kas savākts no internetā pārraidītajiem telesakariem, var saglabāt tikai ar tās tiesas apstiprinājumu, kura ir atļāvusi saziņu ierobežojošus pasākumus ([255]), lai to izmantotu smagu noziegumu izmeklēšanai, kriminālvajāšanai vai novēršanai ([256]). Vispārīgākā nozīmē *CPPA* ir aizliegts izpaust konfidenciālu informāciju, kas iegūta no saziņu ierobežojošiem pasākumiem, un izmantot šādu informāciju to personu reputācijas graušanai, uz kurām attiecas pasākumi ([257]).

3.2.3. *Pārraudzība*

(169) Korejā krimināltiesību aizsardzības iestāžu darbību pārrauga dažādas struktūras ([258]).

([246]) *TBA* 83. panta 4. punkts. Ja steidzamības dēļ nav iespējams iesniegt rakstisku pieprasījumu, rakstisks pieprasījums ir jāiesniedz, tiklīdz vairs nav steidzamības iemesla (*TBA* 83. panta 4. punkts).

([247]) *PIPA* 18. panta 2. punkts.

([248]) Augstākās tiesas 2016. gada 10. marta Lēmums Nr. 2012Da105482. Sk. arī II pielikuma 2.2.3. iedaļu par šo Augstākās tiesas lēmumu.

([249]) *TBA* 83. panta 5.–6. punkts.

([250]) Šai prasībai piemēro ierobežotus un kvalificētus izņēmumus, jo īpaši, ja un tik ilgi, kamēr paziņojums apdraudētu notiekošu kriminālizmeklēšanu vai varētu kaitēt citas personas dzīvībai vai veselībai, kad šīs tiesības vai intereses ir acīm redzami svarīgākas par datu subjekta tiesībām. Sk. Paziņojuma 3. iedaļas iii) punkta 1. apakšpunktu.

([251]) Konkrētāk, Korejas publiskajām iestādēm ar juridiski saistošu instrumentu ir jānodrošina aizsardzības līmenis, kas līdzvērtīgs *PIPA*, sk. arī 90. apsvērumu.

([252]) Sk. arī II pielikuma 1.2. iedaļu.

([253]) Sk. 158. apsvērumu.

([254]) *CPPA* 12. pants. Sk. II pielikuma 2.2.2.2. iedaļu.

([255]) Prokuroram vai policijas ierēdnim, kas īsteno saziņu ierobežojošus pasākumus, 14 dienu laikā pēc pasākumu beigām jāizvēlas saglabājamā telesaziņa un jāpieprasa tiesas apstiprinājums (policijas ierēdņa gadījumā pieteikumu iesniedz prokuroram, kurš savukārt iesniedz pieprasījumu tiesā), sk. *CPPA* 12-2. panta 1. un 2. punktu.

([256]) Šādas atļaujas pieteikumā jāietver informācija par saziņu ierobežojošiem pasākumiem, pasākumu rezultātu kopsavilkums, saglabāšanas iemesli (kopā ar apliecinošiem materiāliem) un saglabājamā telesaziņa (*CPPA* 12-2. panta 3. punkts). Ja pieteikums netiek iesniegts, iegūtie dati ir jādzēš 14 dienu laikā pēc saziņu ierobežojošu pasākumu beigām (*CPPA* 12-2. panta 5. punkts) un, ja pieteikums ir noraidīts, – septiņu dienu laikā (*CPPA* 12-2. panta 5. punkts). Abos gadījumos septiņu dienu laikā tiesā, kas ir apstiprinājusi datu vākšanu, jāiesniedz ziņojums par dzēšanu.

([257]) *CPPA* Izpildes dekrēta 11. panta 2. punkts.

([258]) Sk. II pielikuma 2.3. iedaļu.

(170) Pirmkārt, policijas iekšējo pārraudzību veic ģenerālinspektors ([259]), kas veic likumības pārbaudi, cita starpā attiecībā uz iespējamiem cilvēktiesību pārkāpumiem. Ģenerālinspektora amats tika izveidots, lai īstenotu Likumu par publiskā sektora revīzijām, kurā izteikts aicinājums izveidot pašrevīzijas struktūras un noteiktas īpašas prasības attiecībā uz to sastāvu un uzdevumiem. Konkrētāk, likumā ir noteikts, ka uz diviem līdz pieciem gadiem ir jāieceļ tāds pašrevīzijas struktūras vadītājs, kas nav strādājis šajā iestādē (piem., bijušie tiesneši, profesori) ([260]), ka to var atlaist tikai pamatotu iemeslu dēļ (piem., ja viņš nevar pildīt pienākumus veselības stāvokļa dēļ vai ja attiecībā uz viņu ir ierosināta disciplinārlieta) ([261]) un ka pēc iespējas lielākā mērā jānodrošina viņa neatkarība ([262]). Par pašrevīzijas kavēšanu piemēro administratīvus naudas sodus ([263]). Revīzijas ziņojumi (kas var ietvert ieteikumus, pieprasījumus ierosināt disciplinārlietu un kompensācijas vai korekcijas pieprasījumus) tiek paziņoti attiecīgās publiskās iestādes vadītājam, Revīzijas un inspekcijas padomei (“*BAI*”) ([264]) un parasti tiek publiskoti ([265]). Ziņojuma izpildes rezultāti arī ir jāpaziņo *BAI* ([266]) (sk. 173. apsvērumu par *BAI* pārraudzības uzdevumu un pilnvarām).

(171) Otrkārt, *PIPC* pārrauga, vai krimināltiesību aizsardzības iestāžu veiktā datu apstrāde atbilst *PIPA* un citiem tiesību aktiem, kas aizsargā personu privātumu, tostarp tiesību aktiem, kas reglamentē (elektronisko) pierādījumu vākšanu kriminmāltiesību aizsardzības nolūkos, kā aprakstīts 3.2.1. iedaļā ([267]). Jo īpaši, tā kā *PIPC* veiktā pārraudzība attiecas uz datu vākšanas un apstrādes likumīgumu un godprātību (*PIPA* 3. panta 1. punkts), kas netiktu ievērota, ja personas datiem piekļūst un tos izmanto, pārkāpjot minētos tiesību aktus ([268]), *PIPC* var arī izmeklēt un pieprasīt ievērot 3.2.1. iedaļā aprakstītos ierobežojumus un garantijas ([269]). Pildot šo pārraudzības uzdevumu, *PIPC* var izmantot visas savas izmeklēšanas un korektīvās pilnvaras, kas sīki aprakstītas 2.4.2. iedaļā. Jau pirms nesen īstenotās *PIPA* reformas (t. i., tās iepriekšējā publiskā sektora uzraudzības uzdevumā) *PIPC* veica vairākas pārraudzības darbības attiecībā uz personas datu apstrādi, ko veica kriminmāltiesību aizsardzības iestādes, piem., saistībā ar aizdomās turēto nopratināšanu (2013. gada 26. augusta spriedums lietā Nr. 2013-16), attiecībā uz paziņojumu sniegšanu personām par administratīvo naudas sodu uzlikšanu (2015. gada 26. janvāra spriedums lietā Nr. 2015-02-04), datu kopīgošanu ar citām iestādēm (2018. gada 9. jūlija spriedums lietā Nr. 2018-15-146, 2018. gada 10. decembra spriedums lietā Nr. 2018-25-308; 2019. gada 29. janvāra spriedums lietā Nr. 2019-02-015), pirkstu nospiedumu vai fotogrāfiju vākšanu (2019. gada 9. septembra spriedums lietā Nr. 2019-17-273), dronu izmantošanu (2020. gada 13. janvāra spriedums lietā Nr. 2020-01-004). Šajās lietās *PIPC* izmeklēja, vai tiek ievēroti vairāki *PIPA* noteikumi (piem., apstrādes likumīgums, nolūka ierobežojuma un datu minimizēšanas principi), kā arī citu tiesību aktu, piem., Kriminālprocesa likuma, attiecīgie noteikumi un vajadzības gadījumā sniedza ieteikumus, lai nodrošinātu, ka apstrāde atbilst datu aizsardzības prasībām.

(172) Treškārt, neatkarīgu pārraudzību nodrošina Valsts cilvēktiesību komisija (“NHRC”) ([270]), kas var izmeklēt tiesību uz privātumu un tiesību uz korespondences privātumu pārkāpumus savu vispārējo pilnvaru ietvaros, lai aizsargātu Konstitūcijas 10.–22. pantā noteiktās pamattiesības. *NHRC* sastāvā ir 11 komisāri, kuriem ir jāatbilst īpašai kvalifikācijai ([271]) un kurus ieceļ prezidents saskaņā ar likumā noteikto kārtību. Konkrētāk, četrus komisārus ieceļ pēc tam, kad tos izvirzījusi Nacionālā asambleja, četrus – pēc tam, kad tos izvirzījis prezidents, un trīs – pēc tam, kad tos izvirzījis Augstākās tiesas priekšsēdētājs ([272]). Prezidents no komisāru vidus ieceļ priekšsēdētāju, kas jāapstiprina Nacionālajai asamblejai ([273]). Komisārus (tajā skaitā priekšsēdētāju) ieceļ uz atjaunojamu trīs gadu termiņu, un viņus var atlaist tikai tad, ja viņiem ir piespriests cietumsods vai viņi vairs nespēj pildīt savus

([259]) Sk. II pielikuma 2.3.1. iedaļu. Sk. arī https://www.police.go.kr/eng/knpa/org/org01.jsp.
([260]) Līdzīgi ieceļ revidentus, pamatojoties uz īpašiem nosacījumiem, kas izklāstīti likumā, sk. Likuma par publiskā sektora revīzijām 16. pantu un turpmākos pantus.
([261]) Likuma par publiskā sektora revīzijām 8.–11. pants.
([262]) Likuma par publiskā sektora revīzijām 7. pants.
([263]) Likuma par publiskā sektora revīzijām 41. pants.
([264]) Likuma par publiskā sektora revīzijām 23. panta 1. punkts.
([265]) Likuma par publiskā sektora revīzijām 26. pants.
([266]) Likuma par publiskā sektora revīzijām 23. panta 3. punkts.
([267]) Sk. *PIPA* 7-8. panta 3. un 4. punktu un 7-9. panta 5. punktu.
([268]) Sk. *PIPC* Paziņojuma Nr. 2021-5 6. iedaļu (I pielikums).
([269]) Sk. arī II pielikuma 2.3.4. iedaļu.
([270]) Likuma par Valsts cilvēktiesību komisiju (“*NHRC* likums”) 1. pants.
([271]) Lai komisāru varētu iecelt, komisāram: 1) vismaz desmit gadus ir jābūt strādājušam universitātē vai pilnvarotā pētniecības institūtā vismaz par asociēto profesoru; 2) vismaz desmit gadus ir jābūt strādājušam par tiesnesi, prokuroru vai advokātu; 3) vismaz desmit gadus ir jābūt bijušam iesaistītam ar cilvēktiesībām saistītās darbībās (piem., bezpeļņas, nevalstiskās vai starptautiskās organizācijās); 4) ir jābūt pilsoniskās sabiedrības grupu izvirzītam kandidātam (*NHRC* likuma 5. panta 3. punkts). Turklāt pēc iecelšanas komisāriem ir aizliegts vienlaicīgi ieņemt amatu Nacionālajā asamblejā, vietējās padomēs vai jebkurā valsts vai pašvaldības iestādē (kā valsts amatpersonai), sk. *NHRC* likuma 10. pantu.
([272]) *NHRC* likuma 5. panta 1. un 2. punkts.
([273]) *NHRC* likuma 5. panta 5. punkts.

pienākumus ilgstošas fiziskas vai garīgas nespējas dēļ (šajā gadījumā divām trešdaļām komisāru ir jāpiekrīt atlaišanai) ([274]). Izmeklēšanas ietvaros *NHRC* var pieprasīt attiecīgo materiālu iesniegšanu, veikt pārbaudes un uzaicināt personas sniegt liecības ([275]). Korektīvo pilnvaru ietvaros *NHRC* var izdot (publiski) ieteikumus konkrētas politikas un prakses uzlabošanai vai koriģēšanai, uz kuriem publiskām iestādēm ir jāatbild ar ierosinātu īstenošanas plānu ([276]). Ja attiecīgā iestāde neīsteno ieteikumus, tai par to jāinformē komisija ([277]), kura savukārt var informēt Nacionālo asambleju par šo neizpildi un/vai publiskot to. Saskaņā ar Korejas valdības oficiālo apliecinājumu (II pielikuma 2.3.5. iedaļa) Korejas iestādes parasti ievēro *NHRC* ieteikumus un tām ir spēcīgs stimuls to darīt, jo to veiktā īstenošana tiek novērtēta vispārējā, pastāvīgā novērtējumā, kas tiek veikts premjerministra biroja vadībā. Gada dati par *NHRC* darbību liecina, ka tā aktīvi pārrauga krimināltiesību aizsardzības iestāžu darbību, pamatojoties uz atsevišķiem lūgumrakstiem vai arī veicot *ex officio* izmeklēšanas ([278]).

(173) Ceturtkārt, publisko iestāžu darbību likumības vispārēju pārraudzību veic *BAI*, kas pārbauda valsts ieņēmumus un izdevumus, kā arī vispārīgākā nozīmē pārrauga publisko iestāžu pienākumu izpildi ar mērķi uzlabot valsts pārvaldes darbību ([279]). *BAI* ir oficiāli izveidota Korejas Republikas prezidenta pakļautībā, bet tā saglabā neatkarīgu statusu attiecībā uz saviem pienākumiem ([280]). Turklāt tai ir piešķirta pilnīga neatkarība attiecībā uz tās darbinieku iecelšanu, atlaišanu un organizēšanu, kā arī sava budžeta veidošanu ([281]). *BAI* sastāvā ir priekšsēdētājs (kuru ieceļ prezidents ar Nacionālās asamblejas piekrišanu) ([282]) un seši komisāri (kurus ieceļ prezidents pēc priekšsēdētāja ieteikuma) ([283]), kuriem jāatbilst īpašām likumā noteiktām kvalifikācijām ([284]) un kurus var atlaist tikai tad, ja ir impīčmenta gadījums, viņiem ir piespriests cietumsods vai viņi vairs nespēj pildīt savus pienākumus ilgstošas fiziskas vai garīgas nespējas dēļ ([285]). *BAI* katru gadu veic vispārēju revīziju, bet tā var veikt arī īpašas revīzijas par īpašiem jautājumiem. Veicot revīziju vai pārbaudi, *BAI* var pieprasīt iesniegt dokumentus un pieprasīt personu piedalīšanos ([286]). *BAI* var sniegt ieteikumus, pieprasīt ierosināt disciplinārlietas vai iesniegt kriminālsūdzību ([287]).

(174) Visbeidzot, Nacionālā asambleja veic publisko iestāžu parlamentāro pārraudzību, veicot izmeklēšanu un pārbaudes ([288]) attiecībā uz to darbībām ([289]). Tā var pieprasīt atklāt dokumentus, likt ierasties lieciniekiem ([290]), ieteikt

([274]) *NHRC* likuma 7. panta 1. punkts un 8. pants.
([275]) *NHRC* likuma 36. pants. Saskaņā ar likuma 6. panta 7. punktu materiālu vai priekšmetu iesniegšanu var noraidīt, ja tas apdraudētu valsts konfidencialitāti, kas varētu būtiski ietekmēt valsts drošību vai diplomātiskās attiecības vai varētu radīt nopietnu šķērsli krimināllizmeklēšanā vai nepabeigtā lietas iztiesāšanā. Šādos gadījumos komisija vajadzības gadījumā var pieprasīt papildu informāciju no attiecīgās aģentūras vadītāja (kam tas ir godprātīgi jāievēro), lai varētu novērtēt, vai atteikums sniegt informāciju ir pamatots.
([276]) *NHRC* likuma 25. panta 1. un 3. punkts.
([277]) *NHRC* likuma 25. panta 4. punkts.
([278]) Piemēram, no 2015. līdz 2019. gadam *NHRC* katru gadu saņēma 1 380–1 699 lūgumrakstus pret krimināltiesību aizsardzības iestādēm un izskatīja tikpat lielu daudzumu (piem., 2018. gadā tā izskatīja 1 546 sūdzības pret policiju un 2019. gadā – 1 249); tā veica arī vairākas *ex officio* izmeklēšanas, kas sīkāk aprakstītas *NHRC* 2018. gada ziņojumā (pieejams tīmekļa vietnē https://www.humanrights.go.kr/site/program/board/basicboard/view?menuid=002003003001&pagesize=10&boardtypeid=7017&boardid=7602641) un 2019. gada ziņojumā (pieejams tīmekļa vietnē https://www.humanrights.go.kr/site/program/board/basicboard/view?menuid=002003003001&pagesize=10&boardtypeid=7017&boardid=7606217).
([279]) Likuma par Revīzijas un inspekcijas padomi ("*BAI* likums") 20. un 24. pants. Sk. II pielikuma 2.3.2. iedaļu.
([280]) *BAI* likuma 2. panta 1. punkts.
([281]) *BAI* likuma 2. panta 2. punkts.
([282]) *BAI* likuma 4. panta 1. punkts.
([283]) *BAI* likuma 5. panta 1. un 6. punkts.
([284]) Piemēram, vismaz desmit gadus ir strādājis par tiesnesi, prokuroru vai advokātu, vismaz astoņus gadus ir strādājis par valsts ierēdni vai profesoru, vai augstākos amatos universitātē, vai vismaz desmit gadus ir strādājis biržas sarakstos iekļautā sabiedrībā vai valsts finansētā iestādē (no tiem vismaz piecus gadus ir bijis izpilddirektors), sk. *BAI* likuma 7. pantu. Turklāt komisāriem ir aizliegts piedalīties politiskajās darbībās un vienlaicīgi ieņemt amatus Nacionālajā asamblejā, administratīvajās aģentūrās, organizācijās, kurām *BAI* veic revīziju un pārbaudi, vai jebkuru citu amatu vai darbvietu, par kuru saņem atalgojumu (*BAI* likuma 9. pants).
([285]) *BAI* likuma 8. pants.
([286]) Sk., piem., *BAI* likuma 27. pantu.
([287]) *BAI* likuma 24. pants un 31.–35. pants.
([288]) Likuma par Nacionālo asambleju 128. pants un Likuma par pārbaudēm un izmeklēšanu valsts pārvaldes jomā 2., 3. un 15. pants. Tas attiecas ne tikai uz valsts lietu ikgadējām pārbaudēm kopumā, bet arī uz konkrētu jautājumu izmeklēšanu.
([289]) Sk. pielikuma 2.2.3. iedaļu.
([290]) Likuma par pārbaudēm un izmeklēšanu valsts pārvaldes jomā 10. panta 1. punkts. Sk. arī Likuma par Nacionālo asambleju 128. un 129. pantu.

korektīvus pasākumus (ja tā secina, ka ir veiktas nelikumīgas vai neatbilstošas darbības) ([291]) un publiskot savu konstatējumu rezultātus ([292]). Ja Nacionālā asambleja pieprasa veikt korektīvus pasākumus, kas var ietvert, piemēram, kompensācijas piešķiršanu, disciplinārlietas ierosināšanu vai iekšējo procedūru uzlabošanu, attiecīgajai publiskajai iestādei ir nekavējoties jārīkojas un jāziņo par rezultātiem Nacionālajai asamblejai ([293]).

3.2.4. *Tiesiskā aizsardzība*

(175) Korejas sistēma piedāvā dažādus (juridiskus) tiesiskās aizsardzības līdzekļus, tostarp kompensāciju par kaitējumu.

(176) Pirmkārt, *PIPA* nodrošina personām piekļuves tiesības, tiesības pieprasīt datu labošanu, dzēšanu un izmantošanas apturēšanu attiecībā uz personas datiem, kas apstrādāti krimināltiesību aizsardzības nolūkos ([294]).

(177) Otrkārt, personas var izmantot dažādus tiesiskās aizsardzības mehānismus, kuri norādīti *PIPA*, ja krimināltiesību aizsardzības iestāde to datus apstrādājusi, pārkāpjot *PIPA* vai citos tiesību aktos (t. i., *CPA* vai *CPPA*, sk. 171. apsvērumu) noteiktos ierobežojumus un garantijas, kas attiecas uz personas datu vākšanu. Konkrētāk, personas var iesniegt sūdzību *PIPC* (tostarp izmantojot Privātuma jautājumu zvanu centru, ko pārvalda Korejas Interneta un drošības aģentūra ([295])) vai Personas informācijas strīdu starpniecības komitejā ([296]). Uz šīm tiesību aizsardzības iespējām neattiecas turpmākas pieņemamības prasības. Pamatojoties uz Administratīvo lietu iztiesāšanas likumu, personas var tālāk pārsūdzēt/apstrīdēt *PIPC* lēmumus vai bezdarbību (sk. 132. apsvērumu).

(178) Treškārt, jebkura persona ([297]) var iesniegt sūdzību *NHRC* par to, ka Korejas krimināltiesību aizsardzības iestāde ir pārkāpusi tiesības uz privātumu un datu aizsardzību. *NHRC* var ieteikt labot vai uzlabot visus attiecīgos statūtus, iestādes, politiku vai praksi ([298]), vai īstenot tiesisko aizsardzību, piemēram, starpniecību ([299]), cilvēktiesību pārkāpuma izbeigšanu, kaitējuma atlīdzināšanu un pasākumus, ar ko novērš to pašu vai līdzīgu pārkāpumu atkārtošanu ([300]). Saskaņā ar Korejas valdības oficiālo apliecinājumu (II pielikuma 2.4.2. iedaļa) tas var ietvert arī nelikumīgi savākto personas datu dzēšanu. Lai gan *NHRC* nav pilnvaru izdot saistošus lēmumus, tā piedāvā neoficiālāku, lētāku un viegli pieejamu tiesiskās aizsardzības līdzekli, jo īpaši tāpēc, ka atbilstoši II pielikuma 2.4.2. iedaļas skaidrojumam tā neprasa faktiski pierādīt kaitējumu kā priekšnosacījumu sūdzības izmeklēšanai ([301]). Tas nodrošina, ka personu sūdzības par to datu vākšanu var izmeklēt pat tad, ja persona nevar parādīt, ka tās dati faktiski tika vākti (piemēram, ja personai par to vēl nav paziņots). *NHRC* gada darbības ziņojumi liecina, ka personas praksē arī izmanto šo līdzekli, lai apstrīdētu krimināltiesību aizsardzības iestāžu darbības, tostarp attiecībā uz personas datu apstrādi ([302]). Ja kāda persona nav apmierināta ar *NHRC* īstenotās procedūras iznākumu, tā var

([291]) Likuma par pārbaudēm un izmeklēšanu valsts pārvaldes jomā 16. panta 2. punkts.
([292]) Likuma par pārbaudēm un izmeklēšanu valsts pārvaldes jomā 12-2. pants.
([293]) Likuma par pārbaudēm un izmeklēšanu valsts pārvaldes jomā 16. panta 3. punkts.
([294]) Šīs tiesības var izmantot tieši attiecībās ar kompetento iestādi vai netieši ar *PIPC* starpniecību (*PIPA* 35. panta 2. punkts). Kā sīkāk aprakstīts 76.–78. apsvērumā, izņēmumus šīm tiesībām piemēros tikai tad, kad tas būs nepieciešams svarīgu (sabiedrības) interešu aizsardzībai.
([295]) *PIPA* 62. pants.
([296]) *PIPA* 40.–50. pants un *PIPA* Izpildes dekrēta 48-2.–57. pants. Sk. arī II pielikuma 2.4.1. iedaļu.
([297]) Kā skaidrots II pielikuma 2.4.2. iedaļā, lai gan *NHRC* likuma 4. pants attiecas uz valstspiederīgajiem un ārvalstniekiem, kas uzturas Korejas Republikā, termins "uzturēties" drīzāk atspoguļo jurisdikcijas, nevis teritorijas jēdzienu. Tādējādi, ja valsts iestādes Korejā pārkāpj ārpus Korejas esoša ārvalstnieka pamattiesības, šī persona var iesniegt sūdzību *NHRC*. Šāds gadījums būtu, ja Korejas publiskās iestādes nelikumīgi piekļūtu ārvalstnieka personas datiem, kas nosūtīti Korejai. Sk. jo īpaši skaidrojumu, kas sniegts tīmekļa vietnē https://www.humanrights.go.kr/site/program/board/basicboard/list?boardtypeid=7025&menuid=002004005001&pagesize=10&currentpage=2.
([298]) *NHRC* likuma 44. pants.
([299]) Persona var arī pieprasīt izskatīt sūdzību, izmantojot starpniecību, sk. *NHRC* likuma 42. pantu un turpmākos pantus.
([300]) *NHRC* likuma 42. panta 4. punkts. Turklāt *NHRC* var pieņemt steidzamus atvieglošanas pasākumus tāda notiekoša pārkāpuma gadījumā, kas varētu radīt grūti novēršamu kaitējumu, ja tam netiktu pievērsta uzmanība, sk. *NHRC* likuma 48. pantu.
([301]) Sūdzība principā jāiesniedz viena gada laikā no pārkāpuma, tomēr *NHRC* joprojām var izlemt izmeklēt sūdzību, kas ir iesniegta pēc minētā termiņa, kamēr nav beidzies noilguma termiņš saskaņā ar krimināltiesībām vai civiltiesībām (*NHRC* likuma 32. panta 1. punkta 4. apakšpunkts).
([302]) Piemēram, *NHRC* iepriekš ir izskatījusi sūdzības un sniegusi ieteikumus attiecībā uz nelikumīgu konfiskāciju un ar personas informēšanu par konfiskāciju saistītās prasības pārkāpumu (sk. 80. un 91. lpp. *NHRC* 2018. gada ziņojumā, kas pieejams tīmekļa vietnē https://www.humanrights.go.kr/site/program/board/basicboard/view?menuid=002003003001&pagesize=10&boardtypeid=7017&boardid=7604746), kā arī personas informācijas nelikumīgu apstrādi, ko veikusi policija, prokuratūras un tiesas (sk. 157. un 158. lpp. *NHRC* 2019. gada ziņojumā, kas pieejams tīmekļa vietnē https://www.humanrights.go.kr/site/program/board/basicboard/view?menuid=002003003001&pagesize=10&boardtypeid=7017&boardid=7603308, un 76. lpp. 2019. gada ziņojumā, kas pieejams tīmekļa vietnē https://www.humanrights.go.kr/site/program/board/basicboard/view?menuid=002003003001&pagesize=10&boardtypeid=7017&boardid=7606217).

apstrīdēt *NHRC* lēmumus (piem., lēmumu neturpināt sūdzības izmeklēšanu ([303])) un ieteikumus Korejas tiesās saskaņā ar Administratīvo lietu iztiesāšanas likumu (sk. 181. apsvērumu) ([304]). Turklāt procedūras īstenošana *NHRC* var vēl vairāk atvieglot piekļuvi tiesām, jo persona, pamatojoties uz *NHRC* konstatējumiem, var saskaņā ar 181.–183. apsvērumā aprakstītajām procedūrām meklēt papildu tiesisko aizsardzību pret publisko iestādi, kas nelikumīgi apstrādājusi tās datus.

(179) Visbeidzot, ir pieejami dažādi tiesiskās aizsardzības līdzekļi, kas sniedz personām iespēju izmantot 3.2.1. iedaļā aprakstītos ierobežojumus un garantijas, lai iegūtu tiesisko aizsardzību ([305]).

(180) Attiecībā uz konfiskāciju (ieskaitot datu) *CPA* ir paredzēta iespēja iebilst pret ordera izpildi vai apstrīdēt to ar "kvazisūdzību", iesniedzot lūgumrakstu kompetentajā tiesā ar prasību atcelt vai grozīt prokurora vai policijas ierēdņa rīkojumu ([306]).

(181) Vispārīgākā nozīmē personas var apstrīdēt publisko iestāžu (tostarp krimināltiesību aizsardzības iestāžu) darbību ([307]) vai bezdarbību ([308]) saskaņā ar Administratīvo lietu iztiesāšanas likumu ([309]). Administratīva darbība tiek uzskatīta par "apstrīdamu rīcību", ja tā tieši ietekmē civiltiesības un pienākumus ([310]), kā tas ir personas datu vākšanas pasākumu gadījumā (kā apstiprinājusi Korejas valdība (II pielikuma 2.4.3. iedaļa)), neskatoties uz to, vai tā ir tieša (piem., pārtverot paziņojumus) vai kā saistoši informācijas izpaušanas pieprasījumi (piem., pakalpojumu sniedzējam), vai lūgumi brīvprātīgi sadarboties. Lai sūdzība saskaņā ar Administratīvo lietu iztiesāšanas likumu būtu pieņemama, personai ir jābūt tiesiskai interesei celt prasību ([311]). Saskaņā ar Augstākās tiesas judikatūru jēdziens "tiesiska interese" tiek interpretēts kā "juridiski aizsargāta interese", t. i., tieša un īpaša interese, kas aizsargāta ar likumiem un noteikumiem, uz kuriem tiek balstīti administratīvie rīkojumi (proti, tās nav vispārējas, netiešas un abstraktas sabiedrības intereses) ([312]). Personām šāda tiesiska interese ir gadījumos, kuros tiek pārkāpti ierobežojumi un garantijas, kas attiecas uz to personas datu vākšanu krimināltiesību aizsardzības nolūkos (saskaņā ar īpašiem tiesību aktiem vai *PIPA*). Pamatojoties uz Administratīvo lietu iztiesāšanas likumu, tiesa var nolemt atcelt vai grozīt nelikumīgu rīkojumu, izdot konstatējumu par spēkā neesamību (t. i., konstatējumu, ka rīkojumam nav juridiska spēka, vai par tā neesību tiesību sistēmā) vai izdot konstatējumu, ka bezdarbība ir nelikumīga ([313]). Galīgais spriedums saskaņā ar Administratīvo lietu iztiesāšanas likumu ir saistošs pusēm ([314]).

([303]) Piemēram, ja *NHRC* izņēmuma kārtā nevar pārbaudīt noteiktus materiālus vai objektus, jo tie attiecas uz valsts noslēpumu, kam var būt būtiska ietekme uz valsts drošību vai diplomātiskajām attiecībām, vai ja pārbaude radītu nopietnu šķērsli krimināllizmeklēšanā vai nepabeigtā lietas iztiesāšanā un ja tā neļautu *NHRC* veikt izmeklēšanu, kura nepieciešama, lai novērtētu saņemtā lūgumraksta būtību, tā saskaņā ar *NHRC* likuma 39. pantu informē personu par iemesliem, kāpēc sūdzība tika noraidīta. Šajā gadījumā persona var apstrīdēt *NHRC* lēmumu saskaņā ar Administratīvo lietu iztiesāšanas likumu.

([304]) Sk., piem., Seulas Augstās tiesas 2008. gada 18. aprīļa Lēmumu Nr. 2007Nu27259, kas apstiprināts ar Augstākās tiesas 2008. gada 9. oktobra Lēmumu Nr. 2008Du7854; Seulas Augstās tiesas 2018. gada 2. februāra Lēmumu Nr. 2017Nu69382.

([305]) Sk. II pielikuma 2.4.3. iedaļu.

([306]) *CPA* 417. pants kopā ar *CPA* 414. panta 2. punktu. Sk. arī Augstākās tiesas 1997. gada 29. septembra Lēmumu Nr. 97Mo66.

([307]) Administratīvo lietu iztiesāšanas likumā ir norādīts jēdziens "rīcība", t. i., publisku pilnvaru īstenošana vai atteikums īstenot tās konkrētā gadījumā.

([308]) Saskaņā ar Administratīvo lietu iztiesāšanas likumu tas attiecas uz to, ka administratīvā aģentūra ilgstoši nav veikusi noteiktu rīcību, neskatoties uz juridisko pienākumu to darīt.

([309]) Administratīvo apstrīdēšanu kā neoficiālāku tiesiskās aizsardzības līdzekli vispirms var veikt administratīvo pārsūdzību komisijās, kas izveidotas noteiktu publisko iestāžu pakļautībā (piem., *NIS*, *NHRC*), vai Centrālajā administratīvo pārsūdzību komisijā, kura izveidota Pretkorupcijas un civiltiesību komisijas pakļautībā (Administratīvo pārsūdzību likuma 6. pants un Administratīvo lietu iztiesāšanas likuma 18. panta 1. punkts). Tomēr prasību var iesniegt arī tieši Korejas tiesās, pamatojoties uz Administratīvo lietu iztiesāšanas likumu.

([310]) Augstākās tiesas 1999. gada 22. oktobra Lēmums Nr. 98Du18435, Augstākās tiesas 2000. gada 8. septembra Lēmums Nr. 99Du1113 un Augstākās tiesas 2012. gada 27. septembra Lēmums Nr. 2010Du3541.

([311]) Administratīvo lietu iztiesāšanas likuma 12., 35. un 36. pants. Turklāt pieprasījums rīkojuma atcelšanai/grozīšanai un pieprasījums apstiprināt bezdarbības nelikumību jāiesniedz 90 dienu laikā no dienas, kad personai ir kļuvis zināms par rīkojumu/bezdarbību, un principā ne vēlāk kā vienu gadu pēc tam, kad ir izdots rīkojums vai notikusi bezdarbība, izņemot gadījumus, kad ir attaisnojoši iemesli (Administratīvo lietu iztiesāšanas likuma 20. pants un 38. panta 2. punkts). Augstākā tiesa ir plaši interpretējusi jēdzienu "attaisnojoši iemesli" un pieprasa novērtēt, vai ir sociāli pieņemami atļaut iesniegt novēlotu sūdzību, ņemot vērā visus lietas apstākļus (Augstākās tiesas 1991. gada 28. jūnija Lēmums Nr. 90Nu6521). Kā apstiprinājusi Korejas valdība II pielikuma 2.4.3. iedaļā, tas ietver (bet ne tikai) kavēšanās iemeslus, par kuriem attiecīgā persona nevar tikt saukta pie atbildības (t. i., situācijas, kas ir ārpus sūdzības iesniedzēja kontroles, piem., ja viņš nav ticis informēts par viņa personas informācijas vākšanu), vai *force majeure* (piem., dabas katastrofa, karš).

([312]) Augstākās tiesas 2006. gada 26. marta Lēmums Nr. 2006Du330.

([313]) Administratīvo lietu iztiesāšanas likuma 2. un 4. pants.

([314]) Administratīvo lietu iztiesāšanas likuma 30. panta 1. punkts.

(182) Papildus valsts darbību apstrīdēšanai administratīvajā tiesas procesā personas var iesniegt arī konstitucionālu sūdzību Konstitucionālajā tiesā par to pamattiesību pārkāpumu, kas radies valsts varas īstenošanas vai neīstenošanas dēļ (izņemot tiesu spriedumus) ([315]). Ja ir pieejami citi tiesiskās aizsardzības līdzekļi, tie ir jāizmanto vispirms. Saskaņā ar Konstitucionālās tiesas judikatūru ārvalstnieki var iesniegt konstitucionālu sūdzību tiktāl, ciktāl viņu pamattiesības tiek atzītas saskaņā ar Korejas Konstitūciju (sk. skaidrojumus 1.1. iedaļā) ([316]). Konstitucionālā tiesa var atzīt par spēkā neesošu tādas valsts varas īstenošanu, kas izraisījusi pārkāpumu, vai apstiprināt, ka noteikta bezdarbība ir pretrunā Konstitūcijai ([317]). Šajā gadījumā attiecīgajai iestādei ir jāveic pasākumi, lai izpildītu tiesas nolēmumu.

(183) Turklāt Korejas tiesās personas var iegūt kompensāciju par kaitējumu. Pirmkārt, saskaņā ar 39. pantu (sk. arī 135. apsvērumu) tas ietver iespēju pieprasīt kompensāciju par *PIPA* pārkāpumiem, ko izdarījušas krimināltiesību aizsardzības iestādes. Vispārīgākā nozīmē personas, pamatojoties uz Valsts kompensāciju likumu, var pieprasīt kompensāciju par tādu kaitējumu, ko nodarījušas valsts amatpersonas, pārkāpjot likumu savu oficiālo pienākumu izpildē (sk. arī 135. apsvērumu) ([318]).

(184) Mehānismi, kas aprakstīti 176.–183. apsvērumā sniedz datu subjektiem efektīvus administratīvos un tiesiskos aizsardzības līdzekļus, kas jo īpaši ļauj viņiem īstenot savas tiesības, tostarp tiesības piekļūt saviem personas datiem vai panākt šādu datu labošanu vai dzēšanu.

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

(185) Korejas Republikas tiesību aktos ir noteikti vairāki ierobežojumi un garantijas attiecībā uz piekļuvi personas datiem un to izmantošanu valsts drošības nolūkos, kā arī ir paredzēti pārraudzības un tiesiskās aizsardzības mehānismi, kas atbilst šā lēmuma 141.–143. apsvērumā minētajām prasībām. Nosacījumi, saskaņā ar kuriem var notikt šāda piekļuve, un garantijas, kas piemērojamas šo pilnvaru izmantošanai, ir sīki novērtēti turpmākajās iedaļās.

3.3.1. *Juridiskais pamats, ierobežojumi un garantijas*

(186) Korejas Republikā personas datiem valsts drošības nolūkos var piekļūt, pamatojoties uz *CPPA*, *TBA* un Likumu par terorisma apkarošanu iedzīvotāju un sabiedriskās drošības aizsardzības nolūkā (“Terorisma apkarošanas likums”) ([319]). Galvenā iestāde ([320]), kura ir kompetenta valsts drošības jomā, ir Valsts izlūkdienests (“*NIS*”) ([321]). *NIS* veiktajai personas datu vākšanai un izmantošanai jāatbilst attiecīgajām juridiskajām prasībām (tostarp *PIPA* un

([315]) Konstitucionālās tiesas likuma 68. panta 1. punkts. Konstitucionālas sūdzības jāiesniedz 90 dienu laikā pēc tam, kad persona ir uzzinājusi par pārkāpumu, un viena gada laikā pēc tā izdarīšanas. Kā skaidrots arī II pielikuma 2.4.3. iedaļā, ņemot vērā to, ka saskaņā ar Konstitucionālās tiesas likuma 40. pantu Administratīvo lietu iztiesāšanas likuma procedūru piemēro tiesvedībai, kura veikta saskaņā ar Konstitucionālās tiesas likumu, sūdzība joprojām būs pieņemama, ja ir “attaisnojoši iemesli”, kā interpretēts saskaņā ar 312. zemsvītras piezīmē aprakstīto Augstākās tiesas judikatūru. Ja vispirms jāizlieto citi tiesiskās aizsardzības līdzekļi, konstitucionālā sūdzība jāiesniedz 30 dienu laikā pēc galīgā lēmuma pieņemšanas saistībā ar šādu tiesiskās aizsardzības līdzekli (Konstitucionālās tiesas likuma 69. pants).

([316]) Konstitucionālās tiesas 2001. gada 29. novembra Lēmums Nr. 99HeonMa194.

([317]) Konstitucionālās tiesas likuma 75. panta 3. punkts.

([318]) Valsts kompensāciju likuma 2. panta 1. punkts.

([319]) Sk. II pielikuma 3.1. iedaļu.

([320]) Izņēmuma kārtā policija un prokuratūra arī var vākt personas informāciju valsts drošības nolūkos (sk. 327. zemsvītras piezīmi un II pielikuma 3.2.1.2. iedaļu). Turklāt Korejas Militārajai izlūkošanas aģentūrai (Aizsardzības drošības atbalsta pavēlniecībai, kas izveidota Aizsardzības ministrijas pakļautībā) ir pilnvaras valsts drošības jomā. Tomēr, kā skaidrots II pielikuma 3.1. iedaļā, tā ir atbildīga tikai par militāro izlūkošanu un civiliedzīvotāju novērošanu veic tikai tad, ja tas ir nepieciešams militāro funkciju veikšanai. Konkrētāk, tā var izmeklēt tikai militārpersonas, militārpersonu civilos darbiniekus, militārajās mācībās iesaistītas personas, militārajās rezerves vienībās vai rekrutēšanas dienestā iesaistītas personas un karagūstekņus (Militārās tiesas likuma 1. pants). Kad Aizsardzības drošības atbalsta pavēlniecība vāc saziņas informāciju valsts drošības nolūkos, uz to attiecas ierobežojumi un garantijas, kas noteiktas *CPPA* un tā Izpildes dekrētā.

([321]) *NIS* ir pilnvarots vākt, apkopot un izplatīt informāciju par ārvalstīm (t. i., vispārīgu informāciju par tendencēm un norisēm, kas saistītas ar ārvalstīm vai valsts dalībnieku darbībām); izlūkdatus, kas saistīti ar spiegošanas (ietverot militāro un rūpniecisko spiegošanu), terorisma un starptautisko noziedzīgo sindikātu darbību apkarošanu; izlūkdatus par noteiktu veidu noziegumiem, kas vērsti pret sabiedrības un valsts drošību (piem., iekšējie nemieri, ārvalstu agresija), un izlūkdatus, kuri saistīti ar uzdevumu nodrošināt kiberdrošību un nepieļaut vai apkarot kiberuzbrukumus un kiberdraudus (*NIS* likuma 4. panta 2. punkts). Sk. arī II pielikuma 3.1. iedaļu.

CPPA) ([322]) un vispārīgajām pamatnostādnēm, ko sagatavojis prezidents un pārskatījusi Nacionālā asambleja ([323]). Vispārējs princips paredz, ka *NIS* ir jāsaglabā politiskā neitralitāte un jāaizsargā personu brīvība un tiesības ([324]). Turklāt *NIS* darbinieki nedrīkst ne ļaunprātīgi izmantot savas oficiālās pilnvaras, lai piespiestu kādu iestādi, organizāciju vai personu darīt to, ko viņiem nav pienākuma darīt (saskaņā ar likumu), ne arī traucēt kādai personai īstenot savas tiesības ([325]).

3.3.1.1. Piekļuve saziņas informācijai

(187) Pamatojoties uz *CPPA*, Korejas publiskās iestādes ([326]) var vākt saziņas apstiprinājuma datus (t. i., telesakaru datumu, to sākuma un beigu laiku, veikto un saņemto zvanu skaitu, kā arī otras puses abonenta numuru, izmantošanas biežumu, žurnāldatnes par telesakaru pakalpojumu izmantošanu un atrašanās vietas informāciju, sk. 155. apsvērumu) un saziņas saturu (izmantojot saziņu ierobežojošus pasākumus, sk. 155. apsvērumu) valsts drošības nolūkos (kā noteikts *NIS* pilnvarās, sk. iepriekš 322. zemsvītras piezīmi). Šīs pilnvaras attiecas uz šādu divu veidu informāciju: 1) saziņu, kurā viena vai abas puses ir Korejas valstspiederīgās ([327]), un 2) saziņu, ko veic a) valstis, kas ir naidīgi noskaņotas pret Korejas Republiku, b) ārvalstu aģentūras, grupas vai valstspiederīgie, par kuriem pastāv aizdomas, ka tie ir iesaistīti darbībās, kuras vērstas pret Koreju ([328]), vai c) tādu grupu dalībnieki, kas darbojas Korejas pussalā, bet faktiski ārpus Korejas Republikas suverenitātes, un to jumta grupas, kuras atrodas ārvalstīs ([329]). Tādējādi ES personu saziņa, kas nosūtīta no Savienības uz Korejas Republiku, pamatojoties uz šo lēmumu, var tikt vākta saskaņā ar *CPPA* valsts drošības nolūkos (ievērojot 188.–192. apsvērumā norādītos nosacījumus), ja tā ir starp ES personu un Korejas valstspiederīgo vai ja tā ir saistīta tikai ar saziņu starp personām, kuras nav Korejas valstspiederīgās un ietilpst vienā no trim minētajām kategorijām – 2. punkta a), b) un c) apakšpunktā minētajā kategorijā.

(188) Abos scenārijos saziņas apstiprinājuma datu vākšana var tikt veikta tikai nolūkā novērst draudus valsts drošībai ([330]), bet saziņu ierobežojošus pasākumus var veikt tikai tad, ja pastāv nopietns risks valsts drošībai un vākšana ir nepieciešama, lai to novērstu ([331]). Turklāt piekļūšanu saziņas saturam var izmantot tikai kā galēju pasākumu un ir jācenšas līdz minimumam samazināt saziņas privātuma pārkāpumu ([332]), tādējādi nodrošinot, ka tas ir samērīgs ar noteikto valsts drošības mērķi. Gan saziņas satura, gan saziņas apstiprinājuma datu vākšana drīkst ilgt tikai četrus mēnešus, un tā nekavējoties jāpārtrauc, ja noteiktais mērķis ir sasniegts ātrāk ([333]). Ja joprojām pastāv atbilstība attiecīgajiem nosacījumiem, laikposmu var pagarināt ar iepriekšēju tiesas atļauju (attiecībā uz 189. apsvērumā minētajiem pasākumiem) vai priekšsēdētāja atļauju (attiecībā uz 190. apsvērumā minētajiem pasākumiem) ([334]) uz laiku līdz četriem mēnešiem.

(189) Tādas pašas procesuālās garantijas attiecas uz saziņas apstiprinājuma datu vākšanu un saziņas saturu ([335]). Jo īpaši, ja vismaz viena no saziņā iesaistītajām personām ir Korejas valstspiederīgā, izlūkošanas aģentūrai ir jāiesniedz rakstisks pieprasījums Augstākajai prokuratūrai, kurai savukārt ir jāpieprasa Augstās tiesas vecākā priekšsēdētāja

([322]) Sk. arī *NIS* likuma 14., 22. un 23. pantu.
([323]) *NIS* likuma 4. panta 2. punkts.
([324]) *NIS* likuma 3. panta 1. punkts, 6. panta 2. punkts, 11. un 21. pants. Sk. arī noteikumus par interešu konfliktiem, jo īpaši *NIS* likuma 10. un 12. pantu.
([325]) *NIS* likuma 13. pants.
([326]) Tas ietver izlūkošanas aģentūras (t. i., *NIS* un Aizsardzības drošības atbalsta pavēlniecību) un policiju/prokuratūru.
([327]) *CPPA* 7. panta 1. punkta 1. apakšpunkts.
([328]) Kā skaidrojusi Korejas valdība II pielikuma 244. zemsvītras piezīmē, tās ir darbības, kas apdraud valsts pastāvēšanu un drošību, demokrātisko kārtību vai cilvēku izdzīvošanu un brīvību.
([329]) *CPPA* 7. panta 1. punkta 2. apakšpunkts.
([330]) *CPPA* 13-4. pants.
([331]) *CPPA* 7. panta 1. punkts.
([332]) *CPPA* 3. panta 2. punkts. Turklāt saziņu ierobežojoši pasākumi ir nekavējoties jāpārtrauc, tiklīdz tie vairs nav nepieciešami, tādējādi nodrošinot, ka personas saziņas noslēpumu pārkāpums ir ierobežots līdz minimumam (*CPPA* Izpildes dekrēta 2. pants).
([333]) *CPPA* 7. panta 2. punkts.
([334]) Pieteikums apstiprinājuma saņemšanai, lai pagarinātu novērošanas pasākumus, jāiesniedz rakstiski, norādot iemeslus, kāpēc tiek pieprasīts pagarinājums, un iesniedzot apliecinošus materiālus (*CPPA* 7. panta 2. punkts un *CPPA* Izpildes dekrēta 5. pants).
([335]) Sk. *CPPA* 13-4. panta 2. punktu un *CPPA* Izpildes dekrēta 37. panta 4. punktu, saskaņā ar kuru saziņas satura vākšanai piemērojamās procedūras attiecas arī uz saziņas apstiprinājuma datu vākšanu. Sk. arī II pielikuma 3.2.1.1.1. iedaļu.

orderis ([336]). *CPPA* ir uzskaitīta informācija, kura jāiekļauj prokuroram iesniedzamajā pieprasījumā, ordera pieprasījuma pieteikumā un pašā orderī un kura jo īpaši ietver pieprasījuma pamatojumu un galvenos iemeslus aizdomām, apliecinošos materiālus, kā arī informāciju par ierosinātā pasākuma mērķi, mērķobjektu (t. i., mērķpersonu(-ām)), darbības jomu un ilgumu ([337]). Vākšanu bez ordera var veikt tikai tad, ja ir sazvērestības akts, kas apdraud valsts drošību, vai pastāv ārkārtas situācija, kuras dēļ nav iespējams veikt iepriekš minētās procedūras ([338]). Tomēr arī šādā gadījumā ordera pieprasījuma pieteikums ir jāiesniedz uzreiz pēc pasākuma veikšanas ([339]). Tādēļ *CPPA* ir skaidri noteikts apjoms un nosacījumi šādu veidu vākšanai un tai piemēro īpašas (procesuālās) garantijas (tostarp iepriekšēju tiesas apstiprinājumu), kuras nodrošina, ka šādu pasākumu izmantošana ir ierobežota līdz tam, kas ir nepieciešams un samērīgs. Turklāt prasība sniegt detalizētu informāciju gan ordera pieprasījuma pieteikumā, gan pašā orderī izslēdz neselektīvas piekļuves iespēju.

(190) Attiecībā uz saziņu starp personām, kuras nav Korejas valstspiederīgās un kuras ietilpst kādā no trim īpašajām kategorijām, kas uzskaitītas 187. apsvērumā, pieteikums jāiesniedz *NIS* direktoram, kuram pēc ierosināto pasākumu atbilstības pārbaudes jāpieprasa iepriekšējs rakstisks apstiprinājums no Korejas Republikas prezidenta ([340]). Izlūkošanas aģentūras sagatavotajā pieteikumā jāiekļauj tā pati detalizētā informācija, kas tiesas ordera pieprasījuma pieteikumā (sk. 189. apsvērumu), jo īpaši pieprasījuma pamatojums un galvenie iemesli aizdomām, apliecinošie materiāli un informācija par ierosināto pasākumu mērķiem, mērķpersonu(-ām), darbības jomu un ilgumu ([341]). Lai gan ārkārtas situācijās ([342]) izlūkošanas aģentūrai ir jāiesniedz pieteikums prezidenta apstiprinājumam tūlīt pēc ārkārtas pasākumu veikšanas ([343]), tai vispirms ir jāsaņem iepriekšējs apstiprinājums no ministra, kura pārziņā ir attiecīgā izlūkošanas aģentūra. Arī attiecībā uz tādas saziņas vākšanu, kas notiek tikai starp personām, kuras nav Korejas valstspiederīgās, *CPPA* ir ierobežota šādu pasākumu izmantošana līdz tam, kas ir nepieciešams un samērīgs, skaidri nosakot ierobežotās personu kategorijas, uz kurām var attiecināt šādus pasākumus, un norādot sīki izstrādātus kritērijus, attiecībā uz kuriem izlūkošanas aģentūrām ir jāpierāda atbilstība, kad tās sagatavo pamatojumu informācijas vākšanas pieteikumam. Turklāt tas atkal izslēdz neselektīvas piekļuves iespēju. Kamēr nav iepriekšēja neatkarīga šādu pasākumu apstiprinājuma, neatkarīgu pārraudzību nodrošina *ex post*, jo īpaši *PIPC* un *NHRC* (sk., piem., 199.–200. apsvērumu).

(191) Turklāt *CPPA* ir paredzētas vairākas papildu garantijas, kas veicina *ex post* pārraudzību un atvieglo personu piekļuvi efektīviem tiesiskās aizsardzības līdzekļiem. Pirmkārt, attiecībā uz jebkāda veida vākšanu valsts drošības nolūkos *CPPA* ir paredzētas atšķirīgas uzskaites un ziņošanas prasības. Jo īpaši, pieprasot privātiem operatoriem sadarbību, izlūkošanas aģentūrām ir jāsniedz tiesas orderis / prezidenta atļauja vai ārkārtas cenzūras paziņojuma vāka kopija, kas šai vienībai, kurai pieprasīta piespiedu sadarbība, ir jāglabā savos dokumentos ([344]). Ja privātie

([336]) *CPPA* 6. panta 5. un 8. punkts un 7. panta 1. punkta 1. apakšpunkts un 3. punkts kopā ar *CPPA* Izpildes dekrēta 7. panta 3. un 4. punktu.

([337]) Sk. *CPPA* 7. panta 3. punktu un 6. panta 4. punktu (attiecībā uz izlūkošanas aģentūras pieprasījumu), *CPPA* Izpildes dekrēta 4. pantu (attiecībā uz pieteikumu, ko iesniedz prokurors) un *CPPA* 7. panta 3. punktu un 6. panta 6. punktu (attiecībā uz orderi).

([338]) *CPPA* 8. pants.

([339]) *CPPA* 8. panta 2. un 8. punkts. Vākšana nekavējoties jāpārtrauc, ja 36 stundu laikā no pasākumu sākšanas nav saņemta tiesas atļauja. Gadījumos, kad novērošana ir pabeigta īsā laikā, nesaņemot tiesas atļauju, kompetentās augstākās prokuratūras vadītājam ir jānosūta izlūkošanas aģentūras sagatavots paziņojums par ārkārtas pasākumu kompetentās tiesas vadītājam, kas uz šā pamata var pārbaudīt vākšanas likumību (*CPPA* 8. panta 5. un 7. punkts). Šajā paziņojumā jānorāda mērķis, mērķobjekts, darbības joma, laikposms, izpildes vieta un novērošanas metode, kā arī iemesli pieprasījuma neiesniegšanai pirms pasākuma veikšanas (*CPPA* 8. panta 6. punkts). Kopumā izlūkošanas aģentūras ārkārtas pasākumus var veikt tikai saskaņā ar "ārkārtas cenzūras / sarunu noklausīšanās paziņojumu", un tām ir jāveic šādu pasākumu uzskaite (*CPPA* 8. panta 4. punkts).

([340]) *CPPA* Izpildes dekrēta 8. panta 1. un 2. punkts.

([341]) *CPPA* Izpildes dekrēta 8. panta 3. punkts kopā ar *CPPA* 6. panta 4. punktu.

([342]) Proti, gadījumos, kad pasākuma mērķis ir sazvērestība, kas apdraud valsts drošību, nav pietiekami daudz laika saņemt prezidenta apstiprinājumu un ārkārtas pasākumu nepieņemšana var kaitēt valsts drošībai (CPPA 8. panta 8. punkts).

([343]) *CPPA* 8. panta 9. punkts. Vākšana nekavējoties jāpārtrauc, ja atļauja nav saņemta 36 stundu laikā no pieteikuma iesniegšanas brīža.

([344]) *CPPA* 9. panta 2. punkts un *CPPA* Izpildes dekrēta 12. pants. Sk. *CPPA* Izpildes dekrēta 13. pantu par iespēju pieprasīt pasta nodaļām un telesakaru pakalpojumu sniedzējiem sniegt piespiedu kārtā palīdzību. Privātie operatori, kam pieprasīta informācijas izpaušana, var atteikties to darīt, ja ordera/atļaujas vai ārkārtas cenzūras paziņojumā ir norādīts nepareizs identifikators (piem., tālruņa numurs pieder citai personai, nevis norādītajai personai). Jebkurā gadījumā tiem ir aizliegts atklāt paroles, ko izmanto saziņā (*CPPA* 9. panta 4. punkts).

operatori tiek piespiesti sadarboties, gan publiskai iestādei, kas iesniedz pieprasījumu, gan attiecīgajam operatoram jāveic uzskaite, reģistrējot pasākumu mērķi un mērķobjektu, kā arī veikšanas datumu ([345]). Turklāt izlūkošanas aģentūrām ir jāziņo *NIS* direktoram par savākto informāciju un novērošanas darbības rezultātiem ([346]).

(192) Otrkārt, personas ir jāinformē par to, ka to dati (saziņas apstiprinājuma dati vai saziņas saturs) tiek vākts valsts drošības nolūkos, ja tas attiecas uz saziņu, kurā vismaz viena no pusēm ir Korejas valstspiederīgā ([347]). Šis paziņojums jāiesniedz rakstiski 30 dienu laikā no datu vākšanas beigām (tostarp, ja dati tika iegūti saskaņā ar ārkārtas procedūru), un to var atlikt tikai tad, ja un tik ilgi, kamēr tas varētu apdraudēt valsts drošību vai nodarīt kaitējumu cilvēku dzīvībai un fiziskajai drošībai ([348]). Neatkarīgi no šāda paziņojuma personas var saņemt tiesisko aizsardzību, izmantojot dažādus līdzekļus, kā sīkāk izklāstīts 3.3.4. iedaļā.

3.3.1.2. Informācijas vākšana par personām, kas tiek turētas aizdomās par terorismu

(193) Terorisma apkarošanas likumā ir paredzēts, ka *NIS* var vākt datus par personām, kas tiek turētas aizdomās par terorismu ([349]), saskaņā ar ierobežojumiem un garantijām, kuras noteiktas citos tiesību aktos ([350]). Konkrētāk, *NIS* var iegūt saziņas datus (pamatojoties uz *CPPA*) un citu personas informāciju (iesniedzot brīvprātīgas izpaušanas pieprasījumu) ([351]). Saziņas informācijas (t. i., saziņas satura vai saziņas apstiprinājuma datu) vākšanai piemēro 3.3.1.1. iedaļā aprakstītos ierobežojumus un garantijas, tostarp prasību par tiesas apstiprināta ordera saņemšanu. Attiecībā uz pieprasījumiem brīvprātīgi izpaust par terorismu aizdomās turamo citu veidu personas datus, *NIS* ir jāievēro Konstitūcijā un *PIPA* noteiktās prasības par nepieciešamību un samērīgumu (sk. 164. apsvērumu) ([352]). Pārziņi, kas saņem šādus pieprasījumus, var tos izpildīt brīvprātīgi saskaņā ar *PIPA* noteiktajiem nosacījumiem (piem., saskaņā ar datu minimizēšanas principu un ietekmes uz personas privātumu samazināšanu) ([353]). Šādā gadījumā tām ir arī jāievēro prasība informēt attiecīgo personu saskaņā ar Paziņojumu Nr. 2021-5 (sk. 166. apsvērumu).

([345]) Attiecībā uz saziņu ierobežojošiem pasākumiem šāda uzskaite jāglabā trīs gadus, sk. *CPPA* 9. panta 3. punktu un *CPPA* Izpildes dekrēta 17. panta 2. punktu. Attiecībā uz saziņas apstiprinājuma datiem izlūkošanas aģentūrām ir jāreģistrē fakts, ka šāds datu pieprasījums ir iesniegts, kā arī rakstiskais pieprasījums un iestāde, kas uz to paļāvusies (*CPPA* 13. panta 5. punkts un 13-4. panta 3. punkts). Telesakaru pakalpojumu sniedzējiem ir jāglabā uzskaite septiņus gadus un divreiz gadā jāziņo zinātnes un IKT ministram par šādas informācijas izpaušanas biežumu (*CPPA* 9. panta 3. punkts kopā ar *CPPA* 13. panta 7. punktu un *CPPA* Izpildes dekrēta 37. panta 4. punktu un 39. pantu).

([346]) *CPPA* Izpildes dekrēta 18. panta 3. punkts.

([347]) *CPPA* 9-2. panta 3. punkts un 13-4. pants. Paziņojumā jāietver: 1) fakts, ka informācija ir vākta, 2) izpildaģentūra un 3) izpildes laikposms.

([348]) *CPPA* 9-2. panta 4. punkts. Šajā gadījumā paziņojums jāsniedz 30 dienu laikā no dienas, kad atlikšanas pamatojumi vairs nepastāv, sk. *CPPA* 13-4. panta 2. punktu un 9-2. panta 6. punktu.

([349]) T. i., teroristu grupas dalībnieki (kā noteikusi Apvienoto Nāciju Organizācija, sk. Terorisma apkarošanas likuma 2. panta 2. punktu); personas, kas popularizē un izplata teroristu grupas idejas vai taktiku, piesaista līdzekļus terorismam vai iegulda līdzekļus tajā, vai iesaistās citās darbībās, kas saistītas ar terorisma sagatavošanu, konspirāciju, propagandēšanu vai kūdīšanu uz to; vai personas, par kurām pastāv pamatotas aizdomas, ka tās ir veikušas šādas darbības (Terorisma apkarošanas likuma 2. panta 3. punkts). Terorisma apkarošanas likuma 2. panta 1. punktā jēdziens "terorisms" ir definēts kā rīcība, ko veic, lai kavētu valsts, pašvaldības vai ārvalstu valdības (tostarp starptautisku organizāciju) pilnvaru īstenošanu vai lai piespiestu to rīkoties bez juridiska pienākuma to darīt vai draudētu sabiedrībai. Šāda rīcība var būt, piemēram, nogalināšana, personas nolaupīšana vai ķīlnieku sagrābšana, kuģu vai gaisa kuģu nolaupīšana, sagrābšana, iznīcināšana vai bojāšana, bioķīmisku, sprāgstošu vai aizdedzinošu ieroču izmantošana nolūkā izraisīt nāvi, smagus miesas ievainojumus vai bojājumus un kodolmateriālu vai radioaktīvu materiālu ļaunprātīga izmantošana.

([350]) Terorisma apkarošanas likuma 9. panta 1. un 3. punkts.

([351]) Lai gan Terorisma apkarošanas likumā ir minēta iespēja vākt informāciju par iebraukšanu Korejas Republikā un izbraukšanu no tās, pamatojoties uz Imigrācijas likumu un Muitas likumu, šajos tiesību aktos pašlaik nav paredzētas šādas pilnvaras (sk. II pielikuma 3.2.2.1. iedaļu). Jebkurā gadījumā tās principā neattiecas uz datiem, kas nosūtīti, pamatojoties uz šo lēmumu, jo tās parasti attiecas uz informāciju, kuru Korejas iestādes vāc tieši (nevis piekļuvi datiem, kas iepriekš nosūtīti no Savienības Korejā esošiem pārziņiem). Turklāt Terorisma apkarošanas likumā kā juridiskais pamats informācijas vākšanai par finanšu darījumiem ir norādīts *ARUSFTI*. Tomēr, kā skaidrots 200. zemsvītras piezīmē, dati, kurus var iegūt, pamatojoties uz šo likumu, neietilpst šā lēmuma darbības jomā. Visbeidzot, Terorisma apkarošanas likumā arī paredzēts, ka *NIS* var vākt atrašanās vietas informāciju, izmantojot nesaistošus pieprasījumus, un šādā gadījumā atrašanās vietas informācijas sniedzēji varētu brīvprātīgi izpaust šādu informāciju saskaņā ar nosacījumiem, kas norādīti *PIPA* (kā aprakstīts 193. apsvērumā) un Atrašanās vietas informācijas likumā. Tomēr, kā skaidrots arī 17. zemsvītras piezīmē, atrašanās vietas informācija, pamatojoties uz šo lēmumu, netiks nodota no Savienības Korejā esošiem pārziņiem, bet gan drīzāk iegūta Korejā.

([352]) Sk. II pielikuma 3.2.2.2. iedaļu.

([353]) Sk. *PIPA* 58. panta 4. punktu, kurā noteikts, ka personas informāciju apstrādā tikai tādā minimālajā apjomā, kāds nepieciešams, lai sasniegtu paredzēto nolūku, un *PIPA* 3. panta 6. punktu, kurā paredzēts, ka personas informācija jāapstrādā tādā veidā, kas līdz minimumam samazina iespēju pārkāpt personas privātumu. Sk. arī *PIPA* 59. panta 2. un 3. punktu, saskaņā ar kuru pārziņiem ir aizliegts bez pilnvarojuma izpaust personas informāciju trešām personām.

3.3.1.3. Pieprasījumi par abonenta datu brīvprātīgu izpaušanu

(194) Pamatojoties uz *TBA*, telesakaru pakalpojumu sniedzēji var brīvprātīgi izpaust abonenta datus (sk. 163. apsvērumu), ja to pieprasa izlūkošanas aģentūra, kas plāno vākt šādu informāciju nolūkā novērst draudus valsts drošībai ([354]). Attiecībā uz šādiem *NIS* pieprasījumiem piemēro tādus pašus ierobežojumus (saskaņā ar Konstitūciju, *PIPA* un *TBA*) kā krimināltiesību aizsardzības jomā, kā norādīts 164. apsvērumā ([355]). Telesakaru pakalpojumu sniedzējiem nav obligāti jāizpilda šie pieprasījumi, un tie var izpildīt tos tikai saskaņā ar *PIPA* norādītajiem nosacījumiem (piem., saskaņā ar datu minimizēšanas principu un ietekmes uz personas privātumu samazināšanu, sk. arī 193. apsvērumu). Attiecībā uz uzskaiti un attiecīgās personas informēšanu attiecas tādas pašas prasības kā krimināltiesību aizsardzības jomā (sk. 165. un 166. apsvērumu).

3.3.2. *Savāktās informācijas turpmāka izmantošana*

(195) Tādu personas datu apstrādei, ko Korejas iestādes vāc valsts drošības nolūkos, piemēro nolūka ierobežojuma principu (*PIPA* 3. panta 1. un 2. punkts), apstrādes likumīguma un godprātības principu (*PIPA* 3. panta 1. punkts), samērīguma / datu minimizēšanas principu (*PIPA* 3. panta 1. un 6. punkts un 58. pants), precizitātes principu (*PIPA* 3. panta 3. punkts), pārredzamības principu (*PIPA* 3. panta 5. punkts), drošības principu (*PIPA* 58. panta 4. punkts) un glabāšanas ierobežojuma principu (*PIPA* 58. panta 4. punkts) ([356]). Iespējamā personas datu izpaušana trešajām personām (ieskaitot trešās valstis) var notikt tikai saskaņā ar šiem principiem (jo īpaši nolūka ierobežojuma un datu minimizēšanas principiem) pēc tam, kad ir novērtēta atbilstība nepieciešamības un samērīguma principiem (Konstitūcijas 37. panta 2. punkts), un ņemot vērā ietekmi uz attiecīgo personu tiesībām (*PIPA* 3. panta 6. punkts).

(196) Attiecībā uz saziņas saturu un saziņas apstiprinājuma datiem *CPPA* ir vēl vairāk ierobežota šādu datu izmantošana līdz tiesvedībai tiesā, ja ar saziņu saistītā persona paļaujas uz tiem prasībā par kaitējuma atlīdzināšanu vai izmantošana ir atļauta saskaņā ar citiem tiesību aktiem ([357]).

3.3.3. *Pārraudzība*

(197) Korejas valsts drošības iestāžu darbību uzrauga dažādas struktūras ([358]).

(198) Pirmkārt, Terorisma apkarošanas likumā ir paredzēti īpaši pārraudzības mehānismi terorisma apkarošanas darbībām, tostarp tādu personas datu vākšanai, kas tiek turētas aizdomās par terorismu. Konkrētāk, izpildvaras līmenī terorisma apkarošanas darbības pārrauga Terorisma apkarošanas komisija ([359]), kurai *NIS* direktors ziņo par izmeklēšanu un terorismā aizdomās turamo personu izsekošanu, kas veikta, lai vāktu terorisma apkarošanas darbībām nepieciešamo informāciju vai materiālus ([360]). Turklāt cilvēktiesību aizsardzības uzraugs (*"HRPO"*) īpaši pārrauga terorisma apkarošanas darbību atbilstību pamattiesībām ([361]). Terorisma apkarošanas komisijas priekšsēdētājs ieceļ *HRPO* no personām, kas atbilst īpašām kvalifikācijām, kuras uzskaitītas Terorisma apkarošanas likuma Izpildes dekrētā ([362]), uz (atjaunojamu) divu gadu termiņu, un to var atbrīvot no amata tikai īpašu, ierobežotu un nopietnu iemeslu dēļ ([363]). Pildot savu pārraudzības uzdevumu, *HRPO* var sniegt vispārīgus ieteikumus cilvēktiesību

([354]) *TBA* 83. panta 3. punkts.
([355]) Sk. arī II pielikuma 3.2.3. iedaļu.
([356]) Sk. II pielikuma 1.2. iedaļu.
([357]) *CPPA* 5. panta 1. un 2. punkts, 12. un 13-5. pants.
([358]) Skatīt II pielikuma 3.3. iedaļu.
([359]) Terorisma apkarošanas likuma 5. panta 3. punkts. Komisiju vada premjerministrs, un tās sastāvā ir vairāki ministri un valsts aģentūru vadītāji, piemēram, ārlietu, tieslietu, valsts aizsardzības un iekšlietu un drošības ministrs, *NIS* direktors un valsts policijas aģentūras ģenerālkomisārs (Terorisma apkarošanas likuma Izpildes dekrēta 3. panta 1. punkts).
([360]) Terorisma apkarošanas likuma 9. panta 4. punkts.
([361]) Terorisma apkarošanas likuma 7. pants.
([362]) Tas var būt ikviens, kuram ir advokāta kvalifikācija un vismaz desmit gadu darba pieredze vai kuram ir eksperta līmeņa zināšanas cilvēktiesību jomā un kurš strādā vai ir strādājis (vismaz) par asociēto profesoru vismaz desmit gadus, vai ir strādājis par augstāko valsts amatpersonu valsts aģentūrās vai pašvaldībās, vai kuram ir vismaz desmit gadu darba pieredze cilvēktiesību jomā, piemēram, nevalstiskā organizācijā (Terorisma apkarošanas likuma Izpildes dekrēta 7. panta 1. punkts).
([363]) Piemēram, ja tā ir norādīts saistībā ar tā pienākumu izpildi uzsāktā kriminālietā, ja ir izpausta konfidenciāla informācija vai ir ilgstoša garīga vai fiziska darbnespēja (Terorisma apkarošanas likuma Izpildes dekrēta 7. panta 3. punkts).

aizsardzības uzlabošanai ([364]) un konkrētus ieteikumus korektīviem pasākumiem, ja ir konstatēts cilvēktiesību pārkāpums ([365]). Publiskajām iestādēm jāinformē *HRPO* par turpmākiem pasākumiem, kas veikti saskaņā ar tā ieteikumiem ([366]).

(199) Otrkārt, *PIPC* pārrauga valsts drošības iestāžu atbilstību datu aizsardzības noteikumiem, kas ietver gan piemērojamos *PIPA* noteikumus (sk. 149. apsvērumu), gan ierobežojumus un garantijas, ko piemēro personas datu vākšanai saskaņā ar citiem tiesību aktiem (*CPPA*, Terorisma apkarošanas likumu un *TBA*, sk. arī 171. apsvērumu) ([367]). Pildot šo pārraudzības uzdevumu, *PIPC* var izmantot visas savas izmeklēšanas un korektīvās pilnvaras, kas sīki aprakstītas 2.4.2. iedaļā.

(200) Treškārt, valsts drošības iestāžu darbība ir pakļauta NHRC neatkarīgai pārraudzībai saskaņā ar procedūrām, kas aprakstītas 172. apsvērumā ([368]).

(201) Ceturtkārt, *BAI* pārraudzības uzdevums aptver arī valsts drošības iestādes, lai gan *NIS* izņēmuma gadījumos var atteikties sniegt noteiktu informāciju vai materiālus, t. i., ja tie ietver valsts noslēpumus un nodošana atklātībai nopietni ietekmētu valsts drošību ([369]).

(202) Visbeidzot, *NIS* darbību parlamentāro pārraudzību veic Nacionālā asambleja (izmantojot specializētu Izlūkošanas komiteju) ([370]). *CPPA* nosaka īpašu pārraudzības uzdevumu Nacionālajai asamblejai attiecībā uz saziņu ierobežojošu pasākumu izmantošanu valsts drošības nolūkos ([371]). Konkrētāk, Nacionālā asambleja var veikt sarunu noklausīšanās iekārtu pārbaudes uz vietas un var pieprasīt gan *NIS*, gan telesakaru operatoriem, kas ir izpauduši saziņas saturu, ziņot par to. Nacionālā asambleja var veikt arī vispārējus pārraudzības uzdevumus (saskaņā ar 174. apsvērumā aprakstītajām procedūrām). *NIS* likumā ir noteikts, ka *NIS* direktoram nekavējoties jāsniedz atbilde, kad Izlūkošanas komiteja pieprasa ziņojumu par kādu konkrētu jautājumu ([372]), paredzot īpašus noteikumus attiecībā uz noteiktu īpaši sensitīvu informāciju. Konkrētāk, *NIS* direktors var atteikties sniegt atbildi vai sniegt liecību komitejai tikai ārkārtas apstākļos, t. i., ja pieprasījums ir saistīts ar valsts noslēpumiem militāro, diplomātisko vai Ziemeļkorejas jautājumu jomā un nodošana atklātībai varētu nopietni ietekmēt valsts "nacionālo likteni" ([373]). Šajā gadījumā Izlūkošanas komiteja var pieprasīt paskaidrojumu no premjerministra un, ja septiņu dienu laikā netiek sniegts paskaidrojums, atbildi vai liecību nedrīkst atteikt.

3.3.4. *Tiesiskā aizsardzība*

(203) Arī valsts drošības jomā Korejas sistēma piedāvā dažādus (juridiskus) tiesiskās aizsardzības līdzekļus, tostarp kompensāciju par kaitējumu. Šie mehānismi sniedz datu subjektiem efektīvus administratīvos un tiesiskos aizsardzības līdzekļus, kas jo īpaši ļauj viņiem īstenot to tiesības, tostarp tiesības piekļūt saviem personas datiem vai panākt šādu datu labošanu vai dzēšanu.

(204) Pirmkārt, saskaņā ar *PIPA* 3. panta 5. punktu un 4. panta 1., 3. un 4. punktu personas attiecībās ar valsts drošības iestādēm var izmantot savas piekļuves tiesības, tiesības pieprasīt datu labošanu, dzēšanu un izmantošanas apturēšanu. Paziņojuma Nr. 2021-5 (šā lēmuma I pielikums) 6. iedaļā ir sīkāk paskaidrots, kā šīs tiesības piemēro saistībā ar datu apstrādi valsts drošības nolūkos. Konkrētāk, valsts drošības iestāde var ierobežot vai liegt īstenot tiesības tikai tādā apmērā un tik ilgi, cik tas ir nepieciešams un samērīgi, lai aizsargātu svarīgu sabiedrības interešu mērķi (piem., tādā apmērā un tik ilgi, cik tiesību piešķiršana apdraudētu notiekošo izmeklēšanu vai valsts drošību),

([364]) Terorisma apkarošanas likuma Izpildes dekrēta 8. panta 1. punkts.
([365]) Terorisma apkarošanas likuma Izpildes dekrēta 9. panta 1. punkts. *HRPO* autonomi lemj par ieteikumu pieņemšanu, bet par šādiem ieteikumiem ir jāziņo Terorisma apkarošanas komisijas priekšsēdētājam.
([366]) Terorisma apkarošanas likuma Izpildes dekrēta 9. panta 2. punkts. Kā norādīts Korejas valdības oficiālajā apliecinājumā, ja *HRPO* ieteikums netiek īstenots, tā pārraudzība tiek nodota Terorisma apkarošanas komisijai, tostarp premjerministram, lai gan līdz šim šādi gadījumi, kad *HRPO* ieteikumi nav īstenoti, nav bijuši (sk. II pielikuma 3.3.1. iedaļu).
([367]) II pielikuma 3.3.4. iedaļa.
([368]) Konkrētāk, attiecībā uz *NIS NHRC* iepriekš ir veikusi *ex officio* izmeklēšanu un izskatījusi vairākas individuālas sūdzības. Sk., piem., *NHRC* 2018. gada ziņojuma 128. lpp. (pieejams tīmekļa vietnē https://www.humanrights.go.kr/site/program/board/basicboard/view?menuid=002003003001&pagesize=10&boardtypeid=7017&boardid=7604746) un *NHRC* 2019. gada ziņojuma 70. lpp. (pieejams tīmekļa vietnē https://www.humanrights.go.kr/site/program/board/basicboard/view?menuid=002003003001&pagesize=10&boardtypeid=7017&boardid=7606217).
([369]) *NIS* likuma 13. panta 1. punkts.
([370]) Likuma par Nacionālo asambleju 36. pants un 37. panta 1. punkta 15. apakšpunkts.
([371]) *CPPA* 15. pants.
([372]) *NIS* likuma 15. panta 2. punkts.
([373]) *NIS* likuma 17. panta 2. punkts. "Valsts noslēpumi" ir (klasificēti) fakti, pierādījumi vai informācija, kuru nedrīkst izpaust nevienai citai valstij vai organizācijai, lai nepieļautu nopietnu kaitējumu valsts drošībai, un attiecībā uz kuru ir atļauta tikai ierobežota piekļuve. Sk. *NIS* likuma 13. panta 4. punktu.

vai ja tiesību piešķiršana varētu radīt kaitējumu trešās personas dzīvībai vai veselībai. Tādējādi, izmantojot šādu ierobežojumu, personas tiesības un intereses jālīdzsvaro ar attiecīgajām sabiedrības interesēm, un šāds ierobežojums nekādā gadījumā nedrīkst ietekmēt tiesību būtību (Konstitūcijas 37. panta 2. punkts). Ja pieprasījums tiek noraidīts vai ierobežots, persona nekavējoties jāinformē par iemesliem.

(205) Otrkārt, personām ir tiesības iegūt tiesisko aizsardzību saskaņā ar *PIPA*, ja valsts drošības iestāde viņu datus ir apstrādājusi, pārkāpjot *PIPA* vai ierobežojumus un garantijas, kas noteikti citos tiesību aktos, kuri reglamentē personas datu vākšanu (jo īpaši *CPPA*, sk. 171. apsvērumu) ([374]). Šīs tiesības var izmantot, iesniedzot sūdzību *PIPC* (tostarp izmantojot Privātuma jautājumu zvanu centru, ko pārvalda Korejas Interneta un drošības aģentūra) ([375]). Turklāt, lai atvieglotu piekļuvi tiesiskai aizsardzībai pret Korejas valsts drošības iestādēm, ES personas var iesniegt sūdzību *PIPC* caur savas valsts datu aizsardzības iestādi ([376]). Šajā gadījumā pēc izmeklēšanas pabeigšanas *PIPC* personu informēs caur valsts datu aizsardzības iestādi (attiecīgā gadījumā ietverot informāciju par noteiktajiem korektīvajiem pasākumiem). Pamatojoties uz Administratīvo lietu iztiesāšanas likumu, personas var tālāk pārsūdzēt/apstrīdēt *PIPC* lēmumus vai bezdarbību (sk. 132. apsvērumu).

(206) Treškārt, personas var iesniegt sūdzību *HRPO* attiecībā uz viņu tiesību uz privātumu / datu aizsardzību pārkāpumu saistībā ar terorisma apkarošanas darbībām (t. i., saskaņā ar Terorisma apkarošanas likumu) ([377]), un tas var ieteikt korektīvus pasākumus. Tā kā *HRPO* nepiemēro pieņemamības prasības, sūdzība tiks izskatīta pat tad, ja attiecīgā persona nevar pierādīt, ka faktiski ir cietusi (piem., tāpēc, ka valsts drošības iestāde, iespējams, ir nelikumīgi vākusi tās datus) ([378]). Attiecīgajai iestādei jāinformē *HRPO* par visiem pasākumiem, ko tā veikusi, lai īstenotu tā ieteikumus.

(207) Ceturtkārt, personas var iesniegt sūdzību *NHRC* attiecībā uz viņu datu vākšanu, ko veic valsts drošības iestādes, un saņemt tiesisko aizsardzību saskaņā ar 178. apsvērumā aprakstīto procedūru ([379]).

(208) Visbeidzot, ir pieejami dažādi tiesiskās aizsardzības līdzekļi ([380]), kas sniedz personām iespēju izmantot 3.3.1. iedaļā aprakstītos ierobežojumus un garantijas, lai iegūtu tiesisko aizsardzību. Konkrētāk, pamatojoties uz Administratīvo lietu iztiesāšanas likumu, personas var apstrīdēt valsts drošības iestāžu veikto darbību likumību (saskaņā ar 181. apsvērumā aprakstīto procedūru vai Konstitucionālās tiesas likumu (sk. 182. apsvērumu)). Turklāt tās var saņemt kompensāciju par kaitējumu, pamatojoties uz Valsts kompensāciju likumu (kā sīkāk aprakstīts 183. apsvērumā).

4. **SECINĀJUMS**

(209) Komisija uzskata, ka Korejas Republika, izmantojot *PIPA*, īpašos konkrētām nozarēm piemērojamos noteikumus (kā analizēts 2. iedaļā) un Paziņojumā Nr. 2021-5 (I pielikums) norādītās papildu garantijas, nodrošina no Eiropas Savienības nosūtīto personas datu aizsardzības līmeni, kurš pēc būtības ir līdzvērtīgs tam, kādu garantē Regula (ES) 2016/679.

(210) Komisija arī uzskata, ka kopumā pārraudzības mehānismi un tiesiskās aizsardzības līdzekļi, kas paredzēti Korejas tiesību aktos, ļauj apzināt datu aizsardzības noteikumu pārkāpumus, kurus Korejā izdara pārziņi, un novērst tos praksē, kā arī sniedz datu subjektam tiesisko aizsardzību, kas nodrošina, ka viņš var piekļūt saviem personas datiem un, galu galā, labot vai dzēst šos datus.

([374]) *PIPA* 58. panta 4. punkts un 4. panta 5. punkts. Sk. II pielikuma 3.4.2. iedaļu.
([375]) *PIPA* 62. pants un 63. panta 2. punkts.
([376]) Paziņojums Nr. 2021-5 (I pielikuma 6. iedaļa).
([377]) Terorisma apkarošanas likuma Izpildes dekrēta 8. panta 1. punkta 2. apakšpunkts.
([378]) Skatīt II pielikuma 3.4.1. iedaļu.
([379]) Piemēram, *NHRC* regulāri saņem sūdzības par Valsts izlūkdienestu, sk. *NHRC* 2019. gada pārskatā statistiku par 2015.–2019. gadā saņemto sūdzību skaitu, 70. lpp. (pieejams tīmekļa vietnē https://www.humanrights.go.kr/site/program/board/basicboard/view?menuid=002003003001&pagesize=10&boardtypeid=7017&boardid=7606217).
([380]) Skatīt II pielikuma 3.4.4. iedaļu.

(211) Visbeidzot, pamatojoties uz pieejamo informāciju par Korejas tiesību sistēmu, tostarp II pielikumā ietvertajiem Korejas valdības apliecinājumiem, garantijām un saistībām, Komisija uzskata, ka jebkāda Korejas publisko iestāžu sabiedrisko interešu nolūkos un jo īpaši krimināltiesību aizsardzības un valsts drošības nolūkos veiktā iejaukšanās to personu pamattiesībās, kuru personas datus nosūta no Eiropas Savienības uz Korejas Republiku, būs ierobežota līdz tādam apmēram, kāds ir absolūti nepieciešams attiecīgā leģitīmā mērķa sasniegšanai, un ka pastāv efektīva tiesiskā aizsardzība pret šādu iejaukšanos.

(212) Tāpēc, ņemot vērā šajā lēmumā norādītos konstatējumus, būtu jāuzskata, ka Korejas Republika nodrošina pietiekamu aizsardzības līmeni Regulas (ES) 2016/679 45. panta nozīmē, interpretējot to atbilstoši Eiropas Savienības Pamattiesību hartai, attiecībā uz personas datiem, kas tiek nosūtīti no Eiropas Savienības uz Korejas Republiku personas informācijas datu pārziņiem Korejas Republikā, uz kuriem attiecas *PIPA*, izņemot reliģiskas organizācijas tiktāl, ciktāl tās apstrādā personas datus savu misionāru darbību nolūkā, politiskās partijas tiktāl, ciktāl tās apstrādā personas datus saistībā ar kandidātu izvirzīšanu, un pārziņus, kurus pārrauga Finanšu pakalpojumu komisija attiecībā uz personas kredītinformācijas apstrādi saskaņā ar Kredītinformācijas likumu, ciktāl tie apstrādā šādu informāciju.

5. ŠĀ LĒMUMA SEKAS UN DATU AIZSARDZĪBAS IESTĀŽU RĪCĪBA

(213) 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 nelikumību.

(214) 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. Konkrētāk, pārzinis vai apstrādātājs Eiropas Savienībā var nosūtīt datus pārziņiem Korejas Republikā bez jebkādas turpmākas atļaujas saņemšanas.

(215) Vienlaikus būtu jāatgādina, ka saskaņā ar Regulas (ES) 2016/679 58. panta 5. punktu un kā Tiesa paskaidrojusi spriedumā *Schrems* lietā ([381]), ja valsts datu aizsardzības iestāde, tostarp pēc sūdzības saņemšanas, apšauba Komisijas lēmuma par aizsardzības līmeņa pietiekamību atbilstību personas pamattiesībām uz privātumu un datu aizsardzību, tai valsts tiesību aktos ir jānodrošina tiesiskās aizsardzības līdzeklis, kas ļauj celt šādus iebildumus valsts tiesā, kurai var būt pienākums lūgt Tiesai sniegt prejudiciālu nolēmumu ([382]).

6. ŠĀ LĒMUMA PĀRRAUDZĪBA UN PĀRSKATĪŠANA

(216) Saskaņā ar Eiropas Savienības Tiesas judikatūru ([383]) 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 trešā valsts joprojām nodrošina pēc būtības līdzvērtīgu aizsardzības līmeni. Vajadzība pēc šāda vērtējuma katrā ziņā rodas, ja Komisija saņem informāciju, kura rada šaubas par to.

(217) Tāpēc Komisijai būtu pastāvīgi jāuzrauga situācija Korejas Republikā attiecībā uz personas datu apstrādes tiesisko regulējumu un faktisko praksi, kas novērtēta šajā lēmumā, tostarp tas, kā Korejas iestādes izpilda II pielikumā ietvertos apliecinājumus, garantijas un saistības. Lai atvieglotu šo procesu, Korejas iestādes tiek aicinātas ātri informēt Komisiju par būtiskām ar šo lēmumu saistītām norisēm – gan attiecībā uz personas datu apstrādi, ko veic uzņēmēji un publiskās iestādes, gan attiecībā uz ierobežojumiem un garantijām, kas piemērojami, kad publiskās iestādes piekļūst personas datiem.

([381]) Spriedums lietā *Schrems*, 65. punkts.

([382]) Spriedums lietā *Schrems*, 65. punkts: "Šajā ziņā valsts likumdevēja ziņā ir paredzēt tiesiskās aizsardzības līdzekļus, kas valsts uzraudzības iestādei ļauj valstu tiesās izvirzīt iebildes, ko tā uzskata par pamatotām, lai šīs tiesas – ja arī tās piekrīt šīs iestādes šaubām par Komisijas lēmuma spēkā esamību – iesniegtu lūgumu sniegt prejudiciālu nolēmumu šī lēmuma spēkā esamības izvērtēšanas nolūkos."

([383]) Spriedums lietā *Schrems*, 76. punkts.

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

(219) Piemērojot Regulas (ES) 2016/679 45. panta 3. punktu ([384]) un ņemot vērā faktu, ka ar Korejas tiesību sistēmu nodrošinātais aizsardzības līmenis var mainīties, Komisijai pēc šā lēmuma pieņemšanas būtu periodiski jāpārbauda, vai konstatējumi par Korejas Republikas nodrošinātā aizsardzības līmeņa pietiekamību joprojām ir faktiski un juridiski pamatoti.

(220) Tālab šis lēmums būtu pirmo reizi jāpārskata pēc trim gadiem no dienas, kad tas stājies spēkā. Pēc pirmās pārskatīšanas un atkarībā no tās rezultātiem Komisija ciešā sadarbībā ar komiteju, kas izveidota saskaņā ar Regulas (ES) 2016/679 93. panta 1. punktu, pieņems lēmumu par to, vai būtu jāsaglabā triju gadu cikls. Jebkurā gadījumā turpmākās pārskatīšanas būtu jāveic vismaz reizi četros gados ([385]). Pārskatīšanā būtu jāiekļauj visi šā lēmuma darbības aspekti un jo īpaši šā lēmuma I pielikumā ietverto papildu garantiju piemērošana, īpašu uzmanību pievēršot pieejamiem aizsardzības pasākumiem datu tālākas nosūtīšanas gadījumā; būtiski jaunumi judikatūrā; noteikumi par pseidonimizētas informācijas apstrādi statistikas, zinātniskās pētniecības un arhivēšanas nolūkos sabiedrības interesēs; kā arī izņēmumu piemērošana saskaņā ar *PIPA* 28. panta 7. punktu. individuālo tiesību īstenošanas iedarbīgums, tostarp nesen reformētajā *PIPC*, un izņēmumu piemērošana šīm tiesībām; daļējo atbrīvojumu piemērošana saskaņā ar *PIPA*; kā arī ierobežojumi un garantijas attiecībā uz valdības piekļuvi (kā izklāstīts šā lēmuma II pielikumā), ietverot *PIPC* sadarbību ar ES datu aizsardzības iestādēm personu sūdzību jomā. Tajā būtu arī jāapskata, cik efektīvi tiek veikta pārraudzība un izpilde saistībā ar *PIPA* un kriminmāltiesību aizsardzības un valsts drošības jomā (jo īpaši tā, ko veic *PIPC* un *NHRC*).

(221) Lai veiktu pārskatīšanu, Komisijai būtu jātiekas ar *PIPC* un vajadzības gadījumā arī ar citām Korejas iestādēm, kas atbild par valdības piekļuvi datiem, tostarp ar attiecīgām pārraudzības struktūrām. Būtu jānodrošina iespēja arī Eiropas Datu aizsardzības kolēģijas pārstāvjiem apmeklēt šādas sanāksmes. Pārskatīšanas ietvaros Komisijai būtu jāprasa, lai *PIPC* sniedz vispusīgu informāciju par visiem aspektiem, kas ir būtiski konstatējumam par aizsardzības līmeņa pietiekamību, tostarp par ierobežojumiem un garantijām attiecībā uz valdības piekļuvi datiem ([386]). Komisijai arī būtu jāprasa paskaidrojumi par jebkuru informāciju, kas ir būtiska šim lēmumam un ko tā saņēmusi no Korejas iestāžu vai citu Korejā esošu ieinteresēto personu publiskiem ziņojumiem, Eiropas Datu aizsardzības kolēģijas, individuālām datu aizsardzības iestādēm, pilsoniskās sabiedrības grupām, plašsaziņas līdzekļu ziņojumiem vai jebkuriem citiem pieejamiem informācijas avotiem.

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

7. ŠĀ LĒMUMA APTURĒŠANA, ATCELŠANA VAI GROZĪŠANA

(223) Ja pieejamā informācija, jo īpaši informācija, kas iegūta, uzraugot šo lēmumu, vai informācija, ko sniedz Koreja vai dalībvalstu iestādes, atklāj, ka Korejas Republikas nodrošinātais aizsardzības līmenis, iespējams, vairs nav pietiekams, Komisijai par to būtu ātri jāinformē Korejas kompetentās iestādes un jāpieprasa, lai noteiktā un saprātīgā termiņā tiktu veikti attiecīgi pasākumi.

(224) Ja līdz noteiktā termiņa beigām Korejas kompetentās iestādes nav veikušas minētos pasākumus vai kā citādi apmierinoši neparāda, ka šā lēmuma pamatā joprojām ir pietiekams aizsardzības līmenis, Komisija uzsāks Regulas (ES) 2016/679 93. panta 2. punktā minēto procedūru, lai daļēji vai pilnībā apturētu vai atceltu šo lēmumu.

(225) Alternatīvi Komisija uzsāks minēto procedūru, lai grozītu šo lēmumu, jo īpaši piemērojot papildu nosacījumus datu nosūtīšanai vai ierobežojot aizsardzības līmeņa pietiekamības konstatējuma darbības jomu tikai attiecībā uz tādu datu nosūtīšanu, kam joprojām tiek nodrošināts pietiekams aizsardzības līmenis.

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

([385]) Regulas (ES) 2016/679 45. panta 3. punkts paredz, ka periodiska pārskatīšana jāveic vismaz reizi četros gados. Sk. arī Eiropas Datu aizsardzības kolēģija, Pietiekamības atsauces, WP 254 rev. 01.

([386]) Sk. šā lēmuma II pielikumu.

(226) 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 ietvertās papildu garantijas un/vai ka netiek nenodrošināta to efektīva izpilde, vai ka Korejas iestādes neievēro šā lēmuma II pielikumā ietvertos apliecinājumus, garantijas un saistības.

(227) Komisijai būtu jāapsver šā lēmuma grozīšanas, apturēšanas vai atcelšanas procedūras sākšana arī gadījumā, ja pārskatīšanas kontekstā vai citādi Korejas kompetentās iestādes nesniedz informāciju vai paskaidrojumus, kas nepieciešami, lai novērtētu no Eiropas Savienības uz Korejas Republiku 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.

(228) Pienācīgi pamatotu nenovēršamu steidzamu iemeslu dēļ Komisija izmantos iespēju saskaņā ar Regulas (ES) 2016/679 93. panta 3. punktā minēto procedūru pieņemt nekavējoties piemērojamus īstenošanas aktus, ar kuriem aptur, atceļ vai groza lēmumu.

8. **NOSLĒGUMA APSVĒRUMI**

(229) Eiropas Datu aizsardzības kolēģija ir publiskojusi savu atzinumu ([387]), un tas tika ņemts vērā, sagatavojot šo lēmumu.

(230) Šajā lēmumā paredzētie pasākumi ir saskaņā ar atzinumu, ko sniegusi komiteja, kura izveidota ar Regulas (ES) 2016/679 93. panta 1. punktu,

IR PIEŅĒMUSI ŠO LĒMUMU.

1. pants

1. Regulas (ES) 2016/679 45. panta nolūkā Korejas Republika nodrošina pietiekamu aizsardzības līmeni personas datiem, ko nosūta no Eiropas Savienības uz vienībām Korejas Republikā, uz kurām attiecas Likums par personas informācijas aizsardzību, kas papildināts ar I pielikumā izklāstītajām papildu garantijām, kopā ar II pielikumā ietvertajiem oficiālajiem apliecinājumiem, garantijām un saistībām.

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 kādam no tajā uzskaitītajiem nolūkiem, proti:

a) reliģiskas organizācijas tiktāl, ciktāl tās apstrādā personas datus savu misionāru darbību nolūkā;

b) politiskās partijas tiktāl, ciktāl tās apstrādā personas datus saistībā ar kandidātu izvirzīšanu;

c) vienības, kuras pārrauga Finanšu pakalpojumu komisija attiecībā uz personas kredītinformācijas apstrādi saskaņā ar Kredītinformācijas likumu, ciktāl tās apstrādā šādu informāciju.

2. pants

Lai aizsargātu personas attiecībā uz viņu personas datu apstrādi, ikreiz, kad kompetentās iestādes dalībvalstīs īsteno savas pilnvaras atbilstoši Regulas (ES) 2016/679 58. pantam attiecībā uz datu nosūtīšanu šā lēmuma 1. pantā noteiktajā piemērošanas jomā, attiecīgā dalībvalsts nekavējoties informē Komisiju.

3. pants

1. Komisija nepārtraukti uzrauga to, kā tiek piemērots tiesiskais regulējums, kas ir šā lēmuma pamatā, tai skaitā nosacījumi, ar kādiem tiek veikta datu tālāka nosūtīšana, tiek īstenotas individuālās tiesības un Korejas publiskajām iestādēm ir piekļuve datiem, kuri nosūtīti, balstoties uz šo lēmumu, lai novērtētu, vai Korejas Republika turpina nodrošināt pietiekamu aizsardzības līmeni 1. panta nozīmē.

([387]) Atzinums 32/2021 par Eiropas Komisijas Īstenošanas lēmuma projektu saskaņā Regulu (ES) 2016/679 par personas datu pietiekamu aizsardzību Korejas Republikā, pieejams šajā saitē: https://edpb.europa.eu/our-work-tools/our-documents/opinion-art-70/opinion-322021-regarding-european-commission-draft_en.

2. Dalībvalstis un Komisija informē viena otru par gadījumiem, kad Personas informācijas aizsardzības komisija vai jebkura cita Korejas 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 Korejas publisko iestāžu iejaukšanās personu tiesībās uz viņu personas datu aizsardzību pārsniedz absolūti nepieciešamo vai ka nav efektīvas tiesiskās aizsardzības pret šādu iejaukšanos.

4. Trīs gadus 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 Korejas iestādēm veiktās pārskatīšanas ietvaros.

5. Ja Komisija ir konstatējusi pazīmes, ka vairs netiek nodrošināts pietiekams aizsardzības līmenis, Komisija informē Korejas kompetentās iestādes. Vajadzības gadījumā Komisija var lemt par šā lēmuma apturēšanu, grozīšanu vai atcelšanu vai tā piemērošanas jomas ierobežošanu saskaņā ar Regulas (ES) 2016/679 45. panta 5. punktu jo īpaši gadījumos, kad pazīmes liecina, ka:

a) Korejā esoši pārziņi, kuri saņēmuši personas datus no Eiropas Savienības atbilstoši šim lēmumam, nenodrošina papildu garantijas, kas izklāstītas I pielikumā, vai ka pārraudzība un izpilde šajā ziņā ir nepietiekama;

b) Korejas publiskās iestādes nepilda 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 Korejas publiskās iestādes krimināltiesību aizsardzības vai valsts drošības nolūkos.

Komisija var arī pieņemt šādus pasākumus, ja Korejas valdības nesadarbošanās liedz Komisijai noteikt, vai Korejas Republika turpina nodrošināt pietiekamu aizsardzības līmeni.

4. pants

Šis lēmums ir adresēts dalībvalstīm.

Briselē, 2021. gada 17. decembrī

Komisijas vārdā –
Komisijas loceklis
Didier REYNDERS

I PIELIKUMS

PAPILDU PROCESUĀLIE NOTEIKUMI PAR TO, KĀ INTERPRETĒT UN PIEMĒROT LIKUMU PAR PERSONAS INFORMĀCIJAS AIZSARDZĪBU SAISTĪBĀ AR KOREJAI NOSŪTĪTO PERSONAS DATU APSTRĀDI

Satura rādītājs

I. Izklāsts

Koreja un Eiropas Savienība (turpmāk "ES") ir iesaistījušās apspriedēs par aizsardzības līmeņa pietiekamību, kuru rezultātā Eiropas Komisija konstatēja, ka Koreja garantē personas datiem pietiekamu aizsardzības līmeni saskaņā ar VDAR 45. pantu.

Šajā sakarā Personas informācijas aizsardzības komisija pieņēma šo paziņojumu, pamatojoties uz Likuma par personas informācijas aizsardzību (turpmāk "*PIPA*") 5. pantu (Valsts pienākumi utt.) un 14. pantu (Starptautiskā sadarbība) ([1]), lai precizētu dažu likuma noteikumu interpretāciju, piemērošanu un izpildi, cita starpā attiecībā uz tādu personas datu apstrādi, kas nosūtīti Korejai, pamatojoties uz ES lēmumu par aizsardzības līmeņa pietiekamību.

Tā kā šim paziņojumam ir tādu administratīvu noteikumu statuss, ko pieņem un paziņo kompetentā administratīvā aģentūra, lai precizētu standartus attiecībā uz Likuma par personas informācijas aizsardzību interpretāciju, piemērošanu un izpildi Korejas tiesību sistēmā, tam ir juridiski saistošs spēks attiecībā uz personas informācijas pārzini tādā nozīmē, ka jebkurš šā paziņojuma pārkāpums var tikt uzskatīts par attiecīgo *PIPA* noteikumu pārkāpumu. Turklāt, ja no šā paziņojuma pārkāpuma izriet personas tiesību un interešu aizskārums, attiecīgajām personām ir tiesības saņemt tiesisko aizsardzību Personas informācijas aizsardzības komisijā vai tiesā.

Attiecīgi, ja personas informācijas pārzinis, kas apstrādā uz Koreju nosūtīto personas informāciju saskaņā ar ES lēmumu par aizsardzības līmeņa pietiekamību, neveic pasākumus, kas atbilst šim paziņojumam, tiks uzskatīts, ka "ir būtisks pamats uzskatīt, ka ir noticis pārkāpums attiecībā uz personas informāciju un ka bezdarbība var radīt grūti novēršamu kaitējumu" saskaņā ar likuma 64. panta 1. un 2. punktu. Šādos gadījumos Personas informācijas aizsardzības komisija

([1]) Likuma par personas informācijas aizsardzību 14. pants paredz Korejas valdības pilnvaras izstrādāt politiku nolūkā uzlabot personas informācijas aizsardzības līmeni starptautiskajā vidē un novērst datu subjektu tiesību pārkāpumus personas informācijas pārrobežu nosūtīšanas dēļ.

vai saistītās centrālās administratīvās aģentūras var uzdot attiecīgajam personas informācijas pārzinim veikt korektīvus pasākumus utt. saskaņā ar pilnvarām, kas piešķirtas ar šo noteikumu, un atkarībā no konkrētiem tiesību aktu pārkāpumiem var piemērot arī attiecīgu sodu (sodus, administratīvos naudas sodus utt.).

II. **Terminu definīcijas**

Šajos noteikumos lietoto terminu definīcijas ir šādas:

i) "likums" – Likums par personas informācijas aizsardzību (Likums Nr. 16930, grozīts 2020. gada 4. februārī un piemērots 2020. gada 5. augustā);

ii) "Prezidenta dekrēts" – Likuma par personas informācijas aizsardzību Izpildes dekrēts (Prezidenta 2020. gada 3. marta dekrēts Nr. 30509, ar kuru groza citus likumus);

iii) "datu subjekts" – persona, kuru, pamatojoties uz apstrādāto informāciju, var identificēt un kura tādējādi kļūst par šīs informācijas subjektu;

iv) "personas informācijas pārzinis" – publiska iestāde, juridiska persona, organizācija, fiziska persona utt., kas savas darbības ietvaros tieši vai netieši apstrādā personas informāciju;

v) "ES" – ES (2020. gada februāra beigās 27 dalībvalstis ([2]), tostarp Beļģija, Vācija, Francija, Itālija, Luksemburga, Nīderlande, Dānija, Īrija, Grieķija, Portugāle, Spānija, Austrija, Somija, Zviedrija, Kipra, Čehijas Republika, Igaunija, Ungārija, Latvija, Lietuva, Malta, Polija, Slovākija, Slovēnija, Rumānija, Bulgārija un Horvātija), kā arī ES asociētās valstis, pamatojoties uz EEZ līgumu (Islande, Lihtenšteina, Norvēģija);

vi) "VDAR" – ES vispārējais tiesību akts par personas informācijas (datu) aizsardzību, t. i., Vispārīgā datu aizsardzības regula (Regula (ES) 2016/679);

vii) "lēmums par aizsardzības līmeņa pietiekamību" – saskaņā ar VDAR 45. panta 3. punktu Eiropas Komisija nolēmusi, ka trešā valsts, trešās valsts teritorija, viena vai vairākas jomas vai starptautiska organizācija garantē pietiekamu personas informācijas aizsardzības līmeni.

III. **Papildu procesuālie noteikumi**

1. **Ierobežojums attiecībā uz personas informācijas izmantošanu un sniegšanu ārpus nolūka (likuma 3., 15. un 18. pants)**

< Likums par personas informācijas aizsardzību

(Likums Nr. 16930, daļēji grozīts 2020. gada 4. februārī)>

3. pants (Personas informācijas aizsardzības principi) 1. Personas informācijas pārzinis skaidri norāda personas informācijas apstrādes nolūkus un vāc personas informāciju likumīgi un godprātīgi, kā arī minimālā apjomā, kāds nepieciešams, lai sasniegtu šādus nolūkus.

2. Personas informācijas pārzinis apstrādā personas informāciju piemērotā veidā, kas vajadzīgs nolūkiem, kādiem personas informācija tiek apstrādāta, un neizmanto to ārpus šiem nolūkiem.

15. pants (Personas informācijas vākšana un izmantošana) 1. Personas informācijas pārzinis var vākt personas informāciju jebkurā no turpmāk minētajiem gadījumiem un to izmantot saskaņā ar vākšanas nolūku:

1) ja ir saņemta piekrišana no datu subjekta;

2) ja tiesību aktos ir paredzēti īpaši noteikumi vai ja datu vākšana ir neizbēgama, lai izpildītu juridiskos pienākumus;

3) ja datu vākšana ir neizbēgama, lai publiska iestāde veiktu savus pienākumus saskaņā ar tās jurisdikciju, kā noteikts statūtos utt.;

4) ja datu vākšana ir neizbēgama, lai izpildītu ar datu subjektu noslēgtu līgumu;

([2]) Līdz pārejas perioda beigām ES ietver arī Apvienoto Karalisti, kā paredzēts Līguma par Lielbritānijas un Ziemeļīrijas Apvienotās Karalistes izstāšanos no Eiropas Savienības un Eiropas Atomenerģijas kopienas (2019/C 384 I/01) 126., 127. un 132. pantā.

5) ja datu vākšanu uzskata par acīm redzami nepieciešamu datu subjekta vai trešās personas dzīvības, veselības vai īpašuma interešu aizsardzībai pret nenovēršamu apdraudējumu, ja datu subjekts vai viņa juridiskais pārstāvis nespēj paust savu gribu vai nav iespējams saņemt iepriekšēju piekrišanu, jo nav zināmas adreses utt.;

6) ja datu vākšana ir nepieciešama, lai īstenotu personas informācijas pārziņa pamatotās intereses gadījumos, kad tās nepārprotami prevalē pār datu subjekta tiesībām. Šādos gadījumos apstrāde ir atļauta tikai tiktāl, ciktāl tā ir būtiski saistīta ar personas informācijas pārziņa pamatotajām interesēm un nepārsniedz samērīgu darbības jomu.

18. pants (Ierobežojums attiecībā uz personas informācijas izmantošanu un sniegšanu ārpus nolūka) 1. Personas informācijas pārzinis nedrīkst izmantot personas informāciju, pārsniedzot 15. panta 1. punktā un 39-3. panta 1. un 2. punktā paredzēto darbības jomu, vai sniegt to jebkurai trešai personai, pārsniedzot 17. panta 1. un 3. punktā paredzēto darbības jomu.

2. Neskarot 1. punktu, jebkurā no turpmākajos apakšpunktos minētajām situācijām personas informācijas pārzinis var izmantot personas informāciju vai to sniegt trešai personai citos nolūkos, ja vien šāda rīcība nevarētu negodīgi aizskart datu subjekta vai trešās personas intereses. Tādā gadījumā uz informācijas un komunikācijas pakalpojumu sniedzējiem [kā noteikts Likuma par informācijas un komunikācijas tīkla izmantošanas veicināšanu un datu aizsardzību 2. panta 1. punkta 3. apakšpunktā utt.; turpmāk piemēro šos pašus noteikumus], kuri veic lietotāju personas informācijas apstrādi [kā noteikts Likuma par informācijas un komunikācijas tīkla izmantošanas veicināšanu un datu aizsardzību 2. panta 1. punkta 4. apakšpunktā utt.; turpmāk piemēro šos pašus noteikumus], attiecas tikai 1. un 2. apakšpunkts, un 5.–9. apakšpunkts attiecas tikai uz publiskām iestādēm:

1) ja no datu subjekta ir saņemta papildu piekrišana;

2) ja tiesību aktos ir paredzēti citi īpaši noteikumi;

3) ja datu vākšanu uzskata par acīm redzami nepieciešamu datu subjekta vai trešās personas dzīvības, veselības vai īpašuma interešu aizsardzībai pret nenovēršamu apdraudējumu, ja datu subjekts vai viņa juridiskais pārstāvis nespēj paust savu gribu vai nav iespējams saņemt iepriekšēju piekrišanu, jo nav zināmas adreses;

4) svītrots;<ar Likumu Nr. 16930, 2020. g. 4. febr.>

5) ja nav iespējams pildīt pienākumus, kas ir tās jurisdikcijā, kā paredzēts jebkurā likumā, izņemot gadījumus, kad personas informācijas pārzinis personas informāciju izmanto citiem, nevis paredzētajiem nolūkiem, vai sniedz to trešai personai, un ja Komisija to apspriež un pieņem par to lēmumu;

6) ja personas informācija ir jāsniedz ārvalstu valdībai vai starptautiskai organizācijai, lai izpildītu līgumu vai citu starptautisku konvenciju;

7) ja datu vākšana ir nepieciešama nozieguma izmeklēšanai, apsūdzības izvirzīšanai un kriminālvajāšanai;

8) ja datu vākšana ir nepieciešama, lai tiesa varētu veikt ar tiesas prāvu saistītus pienākumus;

9) ja datu vākšana ir nepieciešama soda, probācijas un aizgādības izpildei.

Izlaists 3. un 4. punkts.

5. Ja personas informācijas pārzinis sniedz personas informāciju trešai personai nolūkiem, kas nav paredzēti nevienā no 2. punktā minētajiem gadījumiem, personas informācijas pārzinis pieprasa, lai personas informācijas saņēmējs ierobežotu izmantošanas nolūku un metodi un citus nepieciešamus aspektus vai sagatavotu nepieciešamās garantijas nolūkā nodrošināt personas informācijas drošību. Šādos gadījumos persona, kas saņem šādu pieprasījumu, veic nepieciešamos pasākumus, lai nodrošinātu personas informācijas drošību.

i) Likuma 3. panta 1. un 2. punktā ir noteikts princips, ka personas informācijas pārzinim ir jāvāc tikai tā personas informācija, kas nepieciešama, lai likumīgi apstrādātu personas informāciju, un to drīkst izmantot tikai paredzētajam nolūkam ([3]).

ii) Saskaņā ar šo principu likuma 15. panta 1. punktā ir noteikts, ka tad, ja personas informācijas pārzinis vāc personas informāciju, to var izmantot vākšanas nolūkā, un 18. panta 1. punktā ir noteikts, ka personas informāciju nedrīkst izmantot, pārsniedzot vākšanas nolūku, vai sniegt trešai personai.

([3]) Tā kā šajos noteikumos ir izklāstīti vispārējie principi, kas piemērojami jebkurai personas informācijas apstrādei, tostarp gadījumos, kad šādu apstrādi īpaši reglamentē citi likumi, šajā iedaļā sniegtie skaidrojumi attiecas arī uz gadījumiem, kad personas datus apstrādā, pamatojoties uz citiem tiesību aktiem (sk., piemēram, Kredītinformācijas likuma 15. panta 1. punktu, kurā ir konkrēta atsauce uz šiem noteikumiem).

iii) Turklāt, pat ja personas informāciju var izmantot citiem nolūkiem nekā paredzēts vai sniegt trešai personai izņēmuma gadījumos ([4]), kas aprakstīti likuma 18. panta 2. punkta apakšpunktā, ir jāpieprasa ierobežot izmantošanas nolūku vai metodi, lai personas informāciju varētu apstrādāt droši saskaņā ar 5. pantu, vai jāveic pasākumi, kas nepieciešami, lai nodrošinātu personas informācijas drošību.

iv) Iepriekš minētos noteikumus vienādi piemēro tādas personas informācijas apstrādei, kas Korejas tiesiskās jurisdikcijas teritorijā saņemta no trešās valsts neatkarīgi no datu subjekta valstspiederības.

v) Piemēram, ja ES esošs personas informācijas pārzinis nosūta personas informāciju Korejā esošam personas informācijas pārzinim saskaņā ar Eiropas Komisijas lēmumu par aizsardzības līmeņa pietiekamību, ES esošā personas informācijas pārziņa personas informācijas nosūtīšanas nolūku uzskata par Korejā esošā personas informācijas pārziņa personas informācijas vākšanas nolūku, un šādos gadījumos Korejā esošais personas informācijas pārzinis var izmantot personas informāciju vai nodot to trešai personai tikai datu vākšanas nolūkā, izņemot izņēmuma gadījumus, kas aprakstīti likuma 18. panta 2. punkta apakšpunktos.

2. **Ierobežojums attiecībā uz personas datu tālāku nosūtīšanu (likuma 17. panta 3. un 4. punkts un 18. pants)**

< Likums par personas informācijas aizsardzību

(Likums Nr. 16930, daļēji grozīts 2020. gada 4. februārī)>

17. pants (Personas informācijas sniegšana) 1. izlaists

2. Personas informācijas pārzinis, saņemot piekrišanu saskaņā ar 1. punkta 1. apakšpunktu, informē datu subjektu par turpmāk uzskaitītajiem jautājumiem. Tas pats attiecas uz gadījumiem, kad tiek mainīts kāds no turpmāk minētajiem parametriem:

1) personas informācijas saņēmējs;

2) nolūks, kādā personas informācijas saņēmējs izmanto šādu informāciju;

3) ziņas par sniedzamo personas informāciju;

4) laikposms, kurā saņēmējs saglabā un izmanto personas informāciju;

5) fakts, ka datu subjektam ir tiesības atteikt piekrišanu, un nelabvēlīga situācija, kas izriet no piekrišanas atteikuma, ja tāda ir.

3. Personas informācijas pārzinis informē datu subjektu par 2. punktā paredzētajiem jautājumiem un saņem datu subjekta piekrišanu, lai sniegtu personas informāciju trešai personai ārvalstīs, un neslēdz līgumu par personas informācijas pārrobežu nosūtīšanu, pārkāpjot šo likumu.

4. Personas informācijas pārzinis var sniegt personas informāciju bez datu subjekta piekrišanas apjomā, kas ir pamatoti saistīts ar nolūkiem, kādiem personas informācija sākotnēji tika vākta, saskaņā ar Prezidenta dekrētā paredzētajiem jautājumiem un ņemot vērā to, vai datu subjektam ir radīta nelabvēlīga situācija, vai ir veikti nepieciešamie drošības pasākumi, piemēram, šifrēšana, utt.

※ Attiecībā uz 18. pantu sk. 3., 4. un 5. lpp.

< **Likuma par personas informācijas aizsardzību Izpildes dekrēts**

([Izpildes datums: 2021. g. 5. febr.] [Prezidenta 2020. gada 4. augusta dekrēts Nr. 30892, ar kuru groza citus likumus])>

14-2. pants (Standarti par personas informācijas papildu izmantošanu/sniegšanu utt.)

1. Ja personas informācijas pārzinis izmanto vai sniedz personas informāciju (turpmāk "personas informācijas papildu izmantošana vai sniegšana") bez datu subjekta piekrišanas saskaņā ar likuma 15. panta 3. punktu vai likuma 17. panta 4. punktu, personas informācijas pārzinis izvērtē šādus jautājumus:

1) vai tas ir pamatoti saistīts ar sākotnējo nolūku, kādam personas informācija tika vākta;

2) vai personas informācijas papildu izmantošana vai sniegšana ir paredzama, ņemot vērā apstākļus, kādos personas informācija tika vākta, un apstrādes praksi;

3) vai ar personas informācijas papildu izmantošanu vai sniegšanu negodīgi neaizskar datu subjekta intereses; kā arī

4) vai ir veikti drošības garantēšanai nepieciešamie pasākumi, piemēram, pseidonimizācija vai šifrēšana.

([4]) Informācijas un komunikācijas pakalpojumu sniedzējiem piemēro tikai 18. panta 2. punkta 1. un 2. apakšpunktu. 5.–9. apakšpunkts ir piemērojams tikai publiskām iestādēm.

2. Personas informācijas pārzinis iepriekš atklāj kritērijus to jautājumu novērtēšanai, kas minēti Privātuma politikas 1. punkta apakšpunktos saskaņā ar likuma 30. panta 1. punktu, un privātuma amatpersona saskaņā ar likuma 31. panta 1. punktu pārbauda, vai personas informācijas pārzinis izmanto vai sniedz papildu personas informāciju saskaņā ar attiecīgajiem standartiem.

i) Ja personas informācijas pārzinis sniedz personas informāciju trešai personai ārvalstīs, viņam ir iepriekš jāinformē datu subjekti par visiem likuma 17. panta 2. punktā minētajiem jautājumiem un jāsaņem viņu piekrišana, izņemot gadījumus, uz kuriem attiecas 1. vai 2. punkts. Nebūtu jānoslēdz neviens līgums par personas datu pārrobežu sniegšanu, pārkāpjot šo likumu.

1. Ja personas informācija ir sniegta apjomā, kas ir pamatoti saistīts ar sākotnējo vākšanas nolūku saskaņā ar likuma 17. panta 4. punktu. Tomēr šo noteikumu var piemērot tikai tādos gadījumos, kad ir nodrošināta atbilstība Izpildes dekrēta 14-2. pantā paredzētajiem personas informācijas papildu izmantošanas un sniegšanas standartiem. Turklāt personas informācijas pārzinim jāizvērtē, vai personas informācijas sniegšana datu subjektiem var radīt nelabvēlīgu situāciju un vai pārzinis ir veicis nepieciešamos pasākumus drošības garantēšanai, piemēram, šifrēšanu.

2. Ja personas informāciju var sniegt trešai personai izņēmuma gadījumos, kas minēti likuma 18. panta 2. punktā (sk. 3.–5. lpp.) Tomēr pat šādos gadījumos, ja ar šādas personas informācijas sniegšanu varētu negodīgi aizskart datu subjekta vai trešās personas intereses, personas informāciju trešai personai nevar sniegt. Turklāt personas informācijas sniedzējs pieprasa, lai personas informācijas saņēmējs ierobežotu personas informācijas izmantošanas nolūku vai metodi vai veiktu pasākumus, kas nepieciešami, lai nodrošinātu šīs personas informācijas drošu apstrādi.

ii) Ja personas informāciju sniedz trešai personai ārvalstīs, tā nevar saņemt Likumā par personas informācijas aizsardzību paredzēto un Korejā garantēto aizsardzības līmeni dažādu valstu personas informācijas aizsardzības sistēmu atšķirību dēļ. Līdz ar to šādi gadījumi tiks uzskatīti par "gadījumiem, kad datu subjektam var tikt radīta nelabvēlīga situācija", kā minēts likuma 17. panta 4. punktā, vai par "gadījumiem, kad negodīgi tiek aizskartas datu subjekta vai trešās personas intereses", kā minēts likuma 18. panta 2. punktā un tā paša likuma Izpildes dekrēta 14-2. pantā ([5]). Tādēļ, lai izpildītu šo noteikumu prasības, personas informācijas pārzinim un trešai personai ir nepārprotami jānodrošina likumā paredzētajam līdzvērtīgs aizsardzības līmenis, tostarp jānodrošina, ka datu subjekts izmanto savas tiesības juridiski saistošos dokumentos, piemēram, līgumos, pat pēc personas informācijas nosūtīšanas uz ārvalstīm.

3. **Paziņojums par datiem, ja personas dati nav iegūti no datu subjekta (likuma 20. pants)**

< Likums par personas informācijas aizsardzību

(Likums Nr. 16930, daļēji grozīts 2020. gada 4. februārī)>

20. pants (Paziņojums par avotiem, no kuriem iegūta personas informācija, kas savākta no trešām personām, utt.) 1. Ja personas informācijas pārzinis apstrādā personas informāciju, kas savākta no trešām personām, personas informācijas pārzinis pēc datu subjekta pieprasījuma nekavējoties informē datu subjektu par šādiem jautājumiem:

1) par savāktās personas informācijas avotu;

2) par personas informācijas apstrādes nolūku;

3) par to, ka datu subjektam ir tiesības pieprasīt personas informācijas apstrādes apturēšanu, kā noteikts 37. pantā.

2. Neskarot 1. punktu, ja personas informācijas pārzinis, kas atbilst Prezidenta dekrētā noteiktajiem kritērijiem, ņemot vērā apstrādāto personas informācijas veidu un apjomu, darbinieku skaitu, pārdošanas apjomu utt., vāc personas informāciju no trešām personām un to apstrādā saskaņā ar 17. panta 1. punkta 1. apakšpunktu, personas informācijas pārzinis informē datu subjektu par 1. punktā minētajiem jautājumiem: ar noteikumu, ka tas neattiecas uz gadījumiem, kad personas informācijas pārziņa savāktā informācija neietver nekādu personas informāciju, piemēram, kontaktinformāciju, ar kuras palīdzību datu subjektam var nosūtīt paziņojumu.

([5]) Saskaņā ar *PIPA* 18. panta 2. punkta 2. apakšpunktu tas attiecas arī uz gadījumiem, kad personas informācija tiek izpausta trešām personām ārvalstīs, pamatojoties uz citu likumu (piemēram, Kredītinformācijas likuma) noteikumiem.

3. Nepieciešamos jautājumus saistībā ar datu subjektam sniedzamās informācijas paziņošanas laiku, metodi un procedūru saskaņā ar 2. punkta galveno teikumu nosaka Prezidenta dekrētā.

4. Šā panta 1. punktu un 2. punkta pamatklauzulu nepiemēro šādos gadījumos: ar noteikumu, ka tas tā ir tikai tad, ja tas saskaņā ar šo likumu nepārprotami prevalē pār datu subjektu tiesībām:

1) ja personas informācija, uz kuru attiecas paziņošanas prasība, ir iekļauta personas informācijas datnēs, kas minētas kādā no 32. panta 2. punkta apakšpunktiem;

2) ja šāda paziņošana var nodarīt kaitējumu jebkuras citas personas dzīvībai vai veselībai vai negodīgi kaitēt jebkuras citas personas īpašumam un citām interesēm.

i) Ja personas informācijas pārzinis saņem personas informāciju, kas nosūtīta no ES, pamatojoties uz tās lēmumu par aizsardzības līmeņa pietiekamību ([6]), viņam bez nepamatotas kavēšanās un jebkurā gadījumā ne vēlāk kā vienu mēnesi pēc nosūtīšanas ir jāpaziņo datu subjektam 1.–5. punktā minētā informācija.

1) To personu vārds, uzvārds un kontaktinformācija, kuras nosūta un saņem personas informāciju.

2) Nosūtītās personas informācijas vienības vai kategorijas.

3) Personas informācijas vākšanas un izmantošanas nolūks (ko datu nosūtītājs noteicis saskaņā ar šā paziņojuma 1. punktu).

4) Personas informācijas saglabāšanas laikposms.

5) Informācija par datu subjekta tiesībām attiecībā uz personas informācijas apstrādi, tiesību īstenošanas metodi un procedūru un jebkādu nelabvēlīgu situāciju, ja tiesību īstenošana tādu rada.

ii) Turklāt, ja personas informācijas pārzinis sniedz i) punktā minēto personas informāciju trešai personai Korejas Republikā vai ārvalstīs, viņam pirms personas informācijas sniegšanas ir jāpaziņo datu subjektam 1.–5. punktā sniegtā informācija.

1) To personu vārds, uzvārds un kontaktinformācija, kuras sniedz un saņem personas informāciju.

2) Sniegtās personas informācijas vienības vai kategorijas.

3) Valsts, kurai sniedz personas informāciju, paredzētais datums un sniegšanas metode (tikai gadījumos, kad personas informāciju sniedz trešai personai ārvalstīs).

4) Personas informācijas sniedzēja nolūks un personas informācijas sniegšanas juridiskais pamats.

5) Informācija par datu subjekta tiesībām attiecībā uz personas informācijas apstrādi, tiesību īstenošanas metodi un procedūru un jebkādu nelabvēlīgu situāciju, ja tiesību īstenošana tādu rada.

iii) Personas informācijas pārzinis nevar piemērot i) vai ii) punktu nevienā no turpmāk 1.–4. punktā minētajiem gadījumiem.

1) Ja personas informācija, kas jāpaziņo, ir iekļauta kādā no turpmāk minētajām personas informācijas datnēm, kas norādītas likuma 32. panta 2. punktā, ciktāl ar šo noteikumu aizsargātās intereses nepārprotami prevalē pār datu subjekta tiesībām, un tikai tikmēr, kamēr paziņošana apdraudētu attiecīgo interešu īstenošanu, piemēram, apdraudētu notiekošu krimināllizmeklēšanu vai apdraudētu valsts drošību.

2) Ja un kamēr paziņošana var kaitēt citas personas dzīvībai vai veselībai vai negodīgi aizskart citas personas īpašuma intereses gadījumos, kad šīs tiesības vai intereses nepārprotami prevalē pār datu subjekta tiesībām.

3) Ja datu subjekta rīcībā jau ir informācija, ko personas informācijas pārzinis paziņo saskaņā ar i) vai ii) punktu.

4) Ja personas informācijas pārzinim nav nekādas datu subjekta kontaktinformācijas vai ja saziņa ar datu subjektu ietver pārmērīgas pūles, cita starpā saistībā ar apstrādi saskaņā ar *PIPA* 3. iedaļā izklāstītajiem nosacījumiem. Nosakot, vai ir iespējams sazināties ar datu subjektu vai arī tas ietver pārmērīgas pūles, būtu jāņem vērā iespēja sadarboties ar ES esošu datu nosūtītāju.

([6]) Pienākumi, kas minēti i), ii) un iii) punktā, ir vienādi piemērojami arī tad, ja pārzinis, kas saņem personas informāciju no ES, pamatojoties uz lēmumu par aizsardzības līmeņa pietiekamību, apstrādā šādu informāciju, pamatojoties uz citiem likumiem, piemēram, Kredītinformācijas likumu.

4. **Īpašā izņēmuma piemērošanas joma pseidonimizētas informācijas apstrādei (Likuma 28-2., 28-3., 28-4., 28-5., 28-6. un 28-7. pants, 3. pants un 58-2. pants)**

< Likums par personas informācijas aizsardzību

(Likums Nr. 16930, daļēji grozīts 2020. gada 4. februārī)>

III nodaļa. Personas informācijas apstrāde

3. IEDAĻA. Īpaši gadījumi saistībā ar pseidonimizētiem datiem

28-2. pants (Pseidonimizētu datu apstrāde) 1. Personas informācijas pārzinis var apstrādāt pseidonimizētu informāciju bez datu subjektu piekrišanas statistikas, zinātniskās pētniecības un arhivēšanas nolūkos sabiedrības interesēs utt.

2. Personas informācijas pārzinis, sniedzot pseidonimizētu informāciju trešai personai saskaņā ar 1. punktu, neiekļauj informāciju, ko var izmantot, lai identificētu konkrētu personu.

28-3. pants (Pseidonimizētu datu apvienošanas ierobežojums) 1. Neskarot 28-2. pantu, pseidonimizētu informāciju, ko dažādi personas informācijas pārziņi apstrādā statistikas, zinātniskās pētniecības un reģistru saglabāšanas nolūkos sabiedrības interesēs utt., apvieno specializēta iestāde, ko norīkojusi Aizsardzības komisija vai saistītās centrālās administratīvās aģentūras vadītājs.

2. Personas informācijas pārzinis, kas plāno apvienoto informāciju izpaust ārpus organizācijas, kura apvienoja datus, saņem specializētās iestādes vadītāja apstiprinājumu pēc tam, kad informācija ir pārveidota pseidonimizētā informācijā vai 58-2. pantā minētajā formātā.

3. Nepieciešamos jautājumus, tostarp apvienošanas procedūras un metodes saskaņā ar 1. punktu, standartus un procedūras specializētas iestādes vadības un uzraudzības iecelšanai vai atcelšanai, kā arī eksportēšanas un apstiprināšanas standartus un procedūras saskaņā ar 2. punktu nosaka Prezidenta dekrētā.

28-4. pants (Pienākums veikt drošības pasākumus attiecībā uz pseidonimizētiem datiem) 1. Personas informācijas pārzinis, apstrādājot pseidonimizētu informāciju, veic tādus tehniskus, organizatoriskus un fiziskus pasākumus kā atsevišķa tādas papildu informācijas glabāšana un pārvaldība, kas vajadzīga, lai atjaunotu sākotnējo stāvokli, kas var būt nepieciešams, lai garantētu drošību, kā noteikts Prezidenta dekrētā, lai personas informāciju nevarētu pazaudēt, nozagt, izpaust, viltot, pārveidot vai sabojāt.

2. Personas informācijas pārzinis, kas plāno apstrādāt pseidonimizētu informāciju, sagatavo un glabā informāciju par Prezidenta dekrētā paredzētajiem jautājumiem, tostarp par pseidonimizētās informācijas apstrādes nolūku un trešo personu, kas ir saņēmēja, ja tiek sniegta pseidonimizēta informācija, lai pārvaldītu pseidonimizētas informācijas apstrādi.

28-5. pants (Aizliegtas darbības saistībā ar pseidonimizētas informācijas apstrādi) 1. Pseidonimizētu informāciju neapstrādā, lai identificētu konkrētu personu.

2. Ja pseidonimizētās informācijas apstrādes laikā tiek ģenerēta informācija, pēc kuras var identificēt konkrētu personu, personas informācijas pārzinis pārtrauc informācijas apstrādi un nekavējoties izgūst un iznīcina informāciju.

28-6. pants (Administratīvo papildmaksu noteikšana par pseidonimizētas informācijas apstrādi) 1. Komisija datu pārzinim, kurš ir apstrādājis datus, lai identificētu konkrētu personu, pārkāpjot 28-5. panta 1. punktu, var piemērot sodu, kas līdzvērtīgs mazāk nekā trim simtdaļām no kopējā pārdošanas apjoma: ar noteikumu, ka gadījumā, ja nav pārdošanas apjoma vai ir grūtības aprēķināt ieņēmumus no pārdošanas, par datu pārzinim var piemērot naudas sodu, kas nepārsniedz 400 miljonus vonu vai trīs simtdaļas no kapitāla summas, atkarībā no tā, kura summa ir lielāka.

2. Jautājumiem, kas vajadzīgi administratīvo papildmaksu piemērošanai un iekasēšanai, *mutatis mutandis* piemēro 34-2. panta 3.–5. punktu.

28-7. pantu (Piemērošanas joma) @20., 21., 27. pantu, 34. panta 1. punktu, 35.–37. pantu, 39-3. pantu, 39-4. pantu, 39-6.–39-8. pantu pseidonimizētajai informācijai nepiemēro.

I nodaļa. Vispārīgi noteikumi

3. pants (Personas informācijas aizsardzības principi) 1. Personas informācijas pārzinis skaidri norāda personas informācijas apstrādes nolūkus un vāc personas informāciju likumīgi un godprātīgi, kā arī minimālā apjomā, kāds nepieciešams, lai sasniegtu šādus nolūkus.

2. Personas informācijas pārzinis apstrādā personas informāciju piemērotā veidā, kas vajadzīgs nolūkiem, kādiem personas informācija tiek apstrādāta, un neizmanto to ārpus šiem nolūkiem.

3. Personas informācijas pārzinis nodrošina, ka personas informācija ir precīza, pilnīga un atjaunināta, ciktāl tas nepieciešams saistībā ar nolūkiem, kādiem personas informācija tiek apstrādāta.

4. Personas informācijas pārzinis personas informāciju pārvalda droši saskaņā ar personas informācijas apstrādes metodēm, veidiem utt., ņemot vērā datu subjekta tiesību pārkāpuma iespējamību un attiecīgo risku nopietnību.

5. Personas informācijas pārzinis publisko savu privātuma politiku un citus jautājumus, kas saistīti ar personas informācijas apstrādi, un garantē datu subjekta tiesības, piemēram, tiesības piekļūt savai personas informācijai.

6. Personas informācijas pārzinis apstrādā personas informāciju tā, lai līdz minimumam samazinātu iespēju pārkāpt datu subjekta privātumu.

7. Ja joprojām ir iespējams personas informācijas vākšanas nolūkus sasniegt, apstrādājot anonimizētu vai pseidonimizētu personas informāciju, personas informācijas pārzinis cenšas apstrādāt personas informāciju, izmantojot anonimizāciju, ja ir iespējama anonimizācija, vai pseidonimizāciju, ja personas informācijas vākšanas nolūkus nav iespējams sasniegt, izmantojot anonimizāciju.

8. Personas informācijas pārzinis, ievērojot un veicot pienākumus, kas paredzēti šajā likumā un citos saistītos likumos, cenšas iegūt datu subjektu uzticību.

IX nodaļa. Papildu noteikumi

58-2. pants (Atbrīvojums no piemērošanas) Šis likums neattiecas uz informāciju, pēc kuras vairs nevar identificēt konkrētu personu, kad to apvieno ar citu informāciju, saprātīgi ņemot vērā laiku, izmaksas, tehnoloģiju utt. <Šis pants ir no jauna iekļauts ar Likumu Nr. 16930, 2020. gada 4. februāris>

i) III nodaļas 3. iedaļa "Īpaši gadījumi attiecībā uz pseidonimizētiem datiem" (28-2.–28-7. pants) ļauj bez datu subjekta piekrišanas apstrādāt pseidonimizētu informāciju, lai apkopotu statistiku, veiktu zinātnisko pētniecību, saglabātu publiskos reģistrus utt. (28-2. pants), bet šādos gadījumos ir obligāti jāparedz atbilstošas garantijas un aizliegumi, kas nepieciešami datu subjektu tiesību aizsardzībai (28-4. pants un 28-5. pants), un pārkāpumu izdarītājiem var piemērot soda sankcijas (28-6. pants), un nav piemērojamas citos gadījumos saskaņā ar *PIPA* pieejamas noteiktas garantijas (28-7. pants).

ii) Šos noteikumus nepiemēro gadījumos, kad pseidonimizētu informāciju apstrādā citiem nolūkiem, nevis statistikas apkopošanai, zinātniskai pētniecībai, publisko reģistru saglabāšanai utt. Piemēram, ja ES privātpersonas personas informācija, kas nosūtīta Korejai saskaņā ar Eiropas Komisijas lēmumu par aizsardzības līmeņa pietiekamību, tiek pseidonimizēta citiem nolūkiem, nevis statistikas apkopošanai, zinātniskai pētniecībai, publisko reģistru saglabāšanai utt., nepiemēro III nodaļas 3. iedaļas īpašos noteikumus ([7]).

iii) Ja personas informācijas pārzinis apstrādā pseidonimizētu informāciju, lai apkopotu statistiku, veiktu zinātnisko pētniecību, saglabātu publiskos reģistrus utt., un ja pseidonimizētā informācija nav iznīcināta, tiklīdz ir sasniegts konkrētais apstrādes nolūks saskaņā ar Konstitūcijas 37. pantu un Likuma 3. pantu (Personas informācijas aizsardzības principi), tas šo informāciju anonimizē, lai nodrošinātu, ka tā pati par sevi vai apvienojumā ar citu informāciju vairs neidentificē konkrētu personu, saprātīgi ņemot vērā laiku, izmaksas, tehnoloģiju utt., saskaņā ar *PIPA* 58-2. pantu.

5. **Korektīvie pasākumi utt. (likuma 64. panta 1., 2. un 4. punkts)**

< Likums par personas informācijas aizsardzību

(Likums Nr. 16930, daļēji grozīts 2020. gada 4. februārī)>

64. pants (Korektīvie pasākumi) 1. Ja Aizsardzības komisija uzskata, ka pastāv būtisks pamats uzskatīt, ka ir noticis pārkāpums attiecībā uz personas informāciju un ka bezdarbība var radīt grūti novēršamu kaitējumu, tā var uzdot šā likuma pārkāpējam (izņemot centrālās administratīvās aģentūras, pašvaldības, Nacionālo asambleju, tiesu, Konstitucionālo tiesu un Valsts vēlēšanu komisiju) veikt kādu no turpmāk minētajiem pasākumiem:

1) apturēt pārkāpumu attiecībā uz personas informāciju;

2) uz laiku apturēt personas informācijas apstrādi;

([7]) Līdzīgi Kredītinformācijas likuma 40-3. panta izņēmums attiecas tikai uz pseidonimizētas kredītinformācijas apstrādi statistikas apkopošanas, zinātniskās pētniecības un publisko reģistru saglabāšanas nolūkos.

3) citus pasākumus, kas nepieciešami, lai aizsargātu personas informāciju un novērstu ar personas informāciju saistītus pārkāpumus.

2. Ja saistītas centrālās administratīvās aģentūras vadītājs uzskata, ka ir būtisks pamats uzskatīt, ka ir noticis pārkāpums attiecībā uz personas informāciju un ka bezdarbība var radīt grūti novēršamu kaitējumu, viņš var likt personas informācijas pārzinim veikt jebkuru no 1. punktā paredzētajiem pasākumiem saskaņā ar attiecīgās centrālās administratīvās aģentūras jurisdikcijas statūtiem.

4. Ja centrālā administratīvā aģentūra, pašvaldība, Nacionālā asambleja, tiesa, Konstitucionālā tiesa vai Valsts vēlēšanu komisija pārkāpj šo likumu, Aizsardzības komisija var ieteikt attiecīgās aģentūras vadītājam veikt jebkuru no 1. punktā paredzētajiem pasākumiem. Šādos gadījumos pēc ieteikuma saņemšanas aģentūra to izpilda, ja vien nepastāv ārkārtas apstākļi.

i) Pirmkārt, judikatūrā ([8]) ([9]) jēdziens "grūti novēršams kaitējums" tiek interpretēts kā gadījums, kas varētu radīt kaitējumu personas personiskajām tiesībām vai privātumam.

ii) Tādējādi "būtisks pamats uzskatīt, ka ir noticis pārkāpums attiecībā uz personas informāciju un ka bezdarbība var radīt grūti novēršamu kaitējumu", kā paredzēts 64. panta 1. un 2. punktā, attiecas uz gadījumiem, kad tiek uzskatīts, ka ar likuma pārkāpumu var tikt pārkāptas personas tiesības un brīvība attiecībā uz personas informāciju. Tas būs piemērojams vienmēr, kad tiks pārkāpts kāds no personas informācijas aizsardzības tiesību aktos iekļautajiem principiem, tiesībām un pienākumiem ([10]).

iii) Saskaņā ar Likuma par personas informācijas aizsardzību 64. panta 4. punktu pasākums saistībā ar "šā likuma pārkāpumu", t. i., prasība pret *PIPA* pārkāpumu.

Centrālā administratīvā aģentūra u. c. kā publiska iestāde, kurai ir saistošs tiesiskums, nedrīkst pārkāpt nevienu tiesību aktu, un tai ir pienākums veikt korektīvu pasākumu, cita starpā nekavējoties pārtraukt darbību un kompensēt kaitējumu izņēmuma gadījumā, kad nelikumīga darbība tomēr ir notikusi.

Līdz ar to, pat ja Aizsardzības komisija neiejaucas saskaņā ar *PIPA* 64. panta 4. punktu, centrālajai administratīvajai aģentūrai u. c., ja tā uzzina par jebkādu tiesību akta pārkāpumu, ir jāveic korektīvi pasākumi pārkāpumu novēršanai.

Jo īpaši, ja Aizsardzības komisija ir ieteikusi korektīvu pasākumu, centrālajai administratīvajai aģentūrai parasti būs objektīvi skaidrs, ka tā ir pārkāpusi tiesību aktus. Tādējādi, lai pamatotu, kāpēc tā uzskata, ka Aizsardzības komisijas ieteikums nebūtu jāievēro, centrālajai administratīvajai aģentūrai u. c. ir jāsniedz skaidrs pamatojums, ar ko iespējams pierādīt, ka tā nav pārkāpusi tiesību aktu. Ieteikums ir jāievēro, ja vien Aizsardzības komisija nenolemj, ka pārkāpums patiešām nav pieļauts.

Ņemot to vērā, Likuma par personas informācijas aizsardzību 64. panta 4. punktā minētajiem "ārkārtas apstākļiem" ir jābūt stingri ierobežotiem, ietverot ārkārtas apstākļus, kuros centrālajām administratīvajām aģentūrām u. c. ir pamatots iemesls pierādīt, ka "šis likums faktiski nav ticis pārkāpts", piemēram, "gadījumos, kad ir ārkārtas (faktiski vai juridiski) apstākļi", par ko Aizsardzības komisija nav zinājusi, sākotnēji sniedzot savu ieteikumu, un Aizsardzības komisija konstatē, ka pārkāpums patiešām nav pieļauts.

6. ***PIPA* piemērošana personas datu apstrādei valsts drošības nolūkos, tostarp pārkāpumu izmeklēšanai un izpildei saskaņā ar *PIPA* (*PIPA* 7-8. pants, 7-9. pants, 58. pants, 3. pants, 4. pants un 62. pants)**

< Likums par personas informācijas aizsardzību

(Likums Nr. 16930, daļēji grozīts 2020. gada 4. februārī)>

7-8. pants (Aizsardzības komisijas darbs) 1. Aizsardzības komisija veic šādu darbu: [..]

3) jautājumi, kas attiecas uz datu subjektu tiesību pārkāpumu izmeklēšanu un no tās izrietošajiem rīkojumiem;

4) sūdzību izskatīšana vai korektīvas procedūras saistībā ar personas informācijas apstrādi un starpniecību strīdos par personas informāciju;

[..]

([8]) (Augstākās tiesas 1999. gada 26. janvāra spriedums 97Da10215,10222) Ja apsūdzētā kriminālie fakti tiek atklāti ar mediju starpniecību, tie var radīt neatgriezenisku psihisku un fizisku kaitējumu ne tikai cietušajam, t. i., prasības iesniedzējiem, bet arī viņa apkārtējiem cilvēkiem, tostarp ģimenēm.

([9]) (Seulas Augstās tiesas 2008. gada 16. janvāra spriedums 2006Na92006) Ja tiek publicēts apmelojošs raksts, tas var radīt būtisku neatgriezenisku kaitējumu iesaistītajai personai.

([10]) Tie paši principi, kas izklāstīti ii) punktā, attiecas uz Kredītinformācijas likuma 45-4. pantu.

7-9. pants (Jautājumi, uz kuriem attiecas Aizsardzības komisijas apspriedes un lēmums) 1. Aizsardzības komisija apspriežas un lemj par šādiem jautājumiem: [..]

5) jautājumi par tiesību aktu interpretāciju un darbību saistībā ar personas informācijas aizsardzību;

[..]

58. pants (Daļēja piemērošanas izslēgšana) 1. III–VII nodaļa neattiecas uz šādu personas informāciju:

1) personas informācija, kas savākta saskaņā ar Statistikas likumu, lai to apstrādātu publiskās iestādēs;

2) personas informācija, kas savākta vai pieprasīta, lai analizētu ar valsts drošību saistītu informāciju;

3) personas informācija, ko apstrādā uz laiku, ja tā ir steidzami nepieciešama sabiedrības drošumam, sabiedriskajai drošībai un sabiedrības veselībai utt.;

4) personas informācija, ko vāc vai izmanto savām vajadzībām, attiecīgi preses ziņojumiem, reliģisko organizāciju misionāru darbībām un politisko partiju kandidātu izvirzīšanai.

[Izlaists 2. un 3. punkts]

4. Ja personas informācijas apstrāde notiek saskaņā ar 1. punktu, personas informācijas pārzinis apstrādā personas informāciju tikai tādā apjomā, kāds nepieciešams, lai sasniegtu paredzēto nolūku, un minimālajā laikposmā, un veic arī nepieciešamos pasākumus, piemēram, tehniskus, pārvaldības un fiziskus aizsardzības pasākumus, individuālu sūdzību izskatīšanu un citus pasākumus, kas nepieciešami šādas personas informācijas drošai pārvaldībai un pienācīgai apstrādei.

3. pants (Personas informācijas aizsardzības principi) 1. Personas informācijas pārzinis skaidri norāda personas informācijas apstrādes nolūkus un vāc personas informāciju likumīgi un godprātīgi, kā arī minimālā apjomā, kāds nepieciešams, lai sasniegtu šādus nolūkus.

2. Personas informācijas pārzinis apstrādā personas informāciju piemērotā veidā, kas vajadzīgs nolūkiem, kādiem personas informācija tiek apstrādāta, un neizmanto to ārpus šiem nolūkiem.

3. Personas informācijas pārzinis nodrošina, ka personas informācija ir precīza, pilnīga un atjaunināta, ciktāl tas nepieciešams saistībā ar nolūkiem, kādiem personas informācija tiek apstrādāta.

4. Personas informācijas pārzinis personas informāciju pārvalda droši saskaņā ar personas informācijas apstrādes metodēm, veidiem utt., ņemot vērā datu subjekta tiesību pārkāpuma iespējamību un attiecīgo risku nopietnību.

5. Personas informācijas pārzinis publisko savu privātuma politiku un citus jautājumus, kas saistīti ar personas informācijas apstrādi, un garantē datu subjekta tiesības, piemēram, tiesības piekļūt savai personas informācijai.

6. Personas informācijas pārzinis apstrādā personas informāciju tā, lai līdz minimumam samazinātu iespēju pārkāpt datu subjekta privātumu.

7. Ja joprojām ir iespējams personas informācijas vākšanas nolūkus sasniegt, apstrādājot anonimizētu vai pseidonimizētu personas informāciju, personas informācijas pārzinis cenšas apstrādāt personas informāciju, izmantojot anonimizāciju, ja ir iespējama anonimizācija, vai pseidonimizāciju, ja personas informācijas vākšanas nolūkus nav iespējams sasniegt, izmantojot anonimizāciju.

8. Personas informācijas pārzinis, ievērojot un veicot pienākumus, kas paredzēti šajā likumā un citos saistītos likumos, cenšas iegūt datu subjektu uzticību.

4. pants (Datu subjektu tiesības) Datu subjektam attiecībā uz savas personas informācijas apstrādi ir šādas tiesības:

1) tiesības tikt informētam par šādas personas informācijas apstrādi;

2) tiesības noteikt, vai dot piekrišanu, un piekrišanas apjomu attiecībā uz šādas personas informācijas apstrādi;

3) tiesības pārliecināties, vai personas informācija tiek apstrādāta, un pieprasīt piekļuvi (tostarp kopiju izsniegšanu; turpmāk tekstā piemēro šos pašus noteikumus) šādai personas informācijai;

4) tiesības apturēt šādas personas informācijas apstrādi un pieprasīt tās labošanu, dzēšanu un iznīcināšanu;

5) tiesības uz atbilstošu tiesisko aizsardzību, izmantojot ātru un taisnīgu procedūru, par jebkuru kaitējumu, kas radies šādas personas informācijas apstrādes rezultātā.

62. pants (Ziņošana par pārkāpumiem) 1. Jebkura persona, kas cieš no tiesību vai interešu pārkāpumiem saistībā ar tās personas informāciju, personas informācijas apstrādes gaitā, ko veic personas informācijas pārzinis, var ziņot par šādu pārkāpumu Aizsardzības komisijai.

2. Aizsardzības komisija var norīkot specializētu iestādi, lai efektīvi saņemtu un apstrādātu ziņojumus par pieprasījumiem saskaņā ar 1. punktu, kā noteikts Prezidenta dekrētā. Šādos gadījumos šāda specializētā iestāde izveido un uztur personas informācijas pārkāpumu zvanu centru (turpmāk "privātuma jautājumu zvanu centrs").

3. Privātuma jautājumu zvanu centrs pilda šādus pienākumus:

1) saņem ziņojumus par pieprasījumiem un sniedz konsultācijas saistībā ar personas informācijas apstrādi;

2) izmeklē un apstiprina incidentus un uzklausa saistīto pušu viedokļus;

3) pilda ar 1. un 2. apakšpunktu saistītos pienākumus.

4. Aizsardzības komisija vajadzības gadījumā var nosūtīt savu valsts amatpersonu uz specializēto iestādi, kas izraudzīta saskaņā ar 2. punktu, atbilstīgi Valsts amatpersonu likuma 32-4. pantam, lai efektīvi izmeklētu un apstiprinātu incidentus saskaņā ar 3. punkta 2. apakšpunktu.

i) Personas informācijas vākšanu valsts drošības nolūkos reglamentē īpaši tiesību akti, ar kuriem pilnvaro kompetentās iestādes (piemēram, Valsts izlūkdienestu) pārtvert saziņu vai pieprasīt izpaušanu, ievērojot konkrētus nosacījumus un garantijas (turpmāk "valsts drošības tiesību akti"). Šie valsts drošības tiesību akti ietver, piemēram, Saziņas privātuma aizsardzības likumu, Likumu par terorisma apkarošanu iedzīvotāju un sabiedriskās drošības aizsardzības nolūkā vai Telesakaru darījumdarbības likumu. Turklāt personas informācijas vākšanai un turpmākai apstrādei ir jāatbilst *PIPA* prasībām. Šajā sakarā *PIPA* 58. panta 1. punkta 2. apakšpunktā ir noteikts, ka III–VII nodaļu nepiemēro personas informācijai, kas savākta vai pieprasīta, lai analizētu ar valsts drošību saistītu informāciju. Tāpēc šis daļējais izņēmums attiecas uz personas informācijas apstrādi valsts drošības nolūkos.

Vienlaikus šādas personas informācijas apstrādei piemēro *PIPA* I nodaļu (Vispārīgi noteikumi), II nodaļu (Personas informācijas aizsardzības politikas izstrāde u. c.), VIII nodaļu (Kolektīvās prasības iesniegšana par datu pārkāpumiem), IX nodaļu (Papildu noteikumi) un X nodaļu (Noteikumi par soda sankcijām). Tas ietver vispārīgos datu aizsardzības principus, kas izklāstīti 3. pantā (Personas informācijas aizsardzības principi), un individuālās tiesības, kas garantētas *PIPA* 4. pantā (Datu subjektu tiesības).

Turklāt *PIPA* 58. panta 4. punktā ir paredzēts, ka šāda informācija ir jāapstrādā minimālajā apjomā, kāds nepieciešams paredzētā nolūka sasniegšanai, un minimālajā laikposmā; turklāt tajā noteikts, ka personas informācijas pārzinim ir jāievieš nepieciešamie pasākumi, lai nodrošinātu datu drošu pārvaldību un pienācīgu apstrādi, piemēram, tehniskus, pārvaldības un fiziskus aizsardzības pasākumus, kā arī pasākumi individuālu sūdzību atbilstīgai izskatīšanai.

Visbeidzot, ir piemērojami noteikumi, kas reglamentē *PIPC* uzdevumus un pilnvaras (tostarp *PIPA* 60.–65. pants par sūdzību izskatīšanu un ieteikumu un korektīvo pasākumu pieņemšanu), kā arī noteikumi par administratīvajiem sodiem un krimināsodiem (*PIPA* 70. pants un turpmākie panti). Saskaņā ar *PIPA* 7-8. panta 1. punkta 3. un 4. apakšpunktu un 7-9. panta 1. punkta 5. apakšpunktu šīs izmeklēšanas un korektīvās pilnvaras, tostarp, ja tās tiek izmantotas saistībā ar sūdzību izskatīšanu, attiecas arī uz iespējamiem tādu noteikumu pārkāpumiem, kas ietverti īpašos tiesību aktos, kuros noteikti ierobežojumi un garantijas attiecībā uz personas informācijas vākšanu, piemēram, valsts drošības tiesību aktos. Ņemot vērā PIPA 3. panta 1. punktā noteiktās prasības likumīgai un godprātīgai personas informācijas vākšanai, šāds pārkāpums ir "šā likuma" pārkāpums 63. un 64. panta nozīmē, kas ļauj PIPC veikt izmeklēšanu un veikt korektīvus pasākumus ([11]). Šo pilnvaru īstenošana, ko veic *PIPC*, papildina, bet neaizstāj Valsts cilvēktiesību komisijas pilnvaras saskaņā ar Likumu par Valsts cilvēktiesību komisiju.

PIPA pamatprincipu, tiesību un pienākumu piemērošana personas informācijas apstrādei valsts drošības nolūkos atspoguļo Konstitūcijā paredzētās garantijas, lai aizsargātu personas tiesības kontrolēt savu personas informāciju. Kā atzinusi Konstitucionālā tiesa, tas ietver personas tiesības ([12]) "personiski izlemt, kad, kam un cik lielā mērā viņas informācija tiks izpausta vai izmantota un kurš to izpaudīs vai izmantos. Tās ir pamattiesības ([13]), [..], kas ir spēkā, lai aizsargātu personisko lēmumu pieņemšanas brīvību pret risku, ko rada valsts funkciju un informācijas komunikācijas tehnoloģijas paplašināšana." Jebkurš šo tiesību ierobežojums, piemēram, ja tas nepieciešams valsts drošības aizsardzībai, prasa līdzsvara nodrošināšanu starp personas tiesībām un interesēm un attiecīgajām sabiedrības interesēm, un tas nedrīkst ietekmēt tiesību būtību (Konstitūcijas 37. panta 2. punkts).

([11]) Attiecībā uz korektīvajiem pasākumiem saskaņā ar 64. pantu sk. arī 5. iedaļu iepriekš.
([12]) Konstitucionālās tiesas 2005. gada 26. maija spriedums, 99HunMa513, 2004HunMa190.
([13]) Konstitucionālās tiesas 2005. gada 21. jūlija spriedums, 2003HunMa282.

Tāpēc, apstrādājot personas informāciju valsts drošības nolūkos, pārzinis (piemēram, *NIS*) cita starpā:

1) skaidri norāda nolūkus, kādos personas informācija tiek apstrādāta, un likumīgi un godprātīgi vāc personas informāciju minimālā apjomā, kāds nepieciešams, lai sasniegtu šādus nolūkus (*PIPA* 3. panta 1. punkts); konkrēti, tas vāc un turpmāk apstrādā personas informāciju, tikai lai pildītu pienākumus saskaņā ar attiecīgajiem likumiem, piemēram, Likumu par Valsts izlūkdienestu;

2) apstrādā personas informāciju tikai tādā apjomā, kāds nepieciešams, lai sasniegtu paredzēto mērķi, un minimālajā laikposmā (*PIPA* 58. panta 4. punkts); īstenojot apstrādes nolūku, pārzinis neatgriezeniski iznīcina personas informāciju, ja vien turpmāka saglabāšana nav īpaši paredzēta likumā, un tādā gadījumā attiecīgo personas informāciju glabā un pārvalda atsevišķi no citas personas informāciju, to neizmanto citiem nolūkiem, kā vien tiem, kas noteikti likumos, un iznīcina saglabāšanas laikposma beigās;

3) apstrādā personas informāciju pienācīgā veidā, kas nepieciešams nolūkiem, kādos personas informācija tiek apstrādāta, un to nedrīkst izmantot ārpus šiem nolūkiem (*PIPA* 3. panta 2. punkts);

4) nodrošina, ka personas informācija ir precīza, pilnīga un atjaunināta, ciktāl tas vajadzīgs saistībā ar nolūkiem, kādiem personas informācija tiek apstrādāta (*PIPA* 3. panta 3. punkts);

5) pārvalda personas informāciju drošā veidā saskaņā ar personas informācijas apstrādes metodēm, veidiem utt., ņemot vērā datu subjekta tiesību pārkāpumu iespējamību un attiecīgo risku smagumu (*PIPA* 3. panta 4. punkts);

6) publisko savu privātuma politiku un citus jautājumus, kas saistīti ar personas informācijas apstrādi (*PIPA* 3. panta 5. punkts);

7) apstrādā personas informāciju tādā veidā, lai līdz minimumam samazinātu iespēju pārkāpt datu subjekta privātumu (*PIPA* 3. panta 6. punkts).

ii) Saskaņā ar *PIPA* 58. panta 4. punktu pārzinis (piemēram, iestādes, kuru kompetencē ir valsts drošība, piemēram, *NIS*) veic nepieciešamos pasākumus, piemēram, ievieš tehniskus, pārvaldības un fiziskus aizsardzības pasākumus, lai nodrošinātu atbilstību šiem principiem un personas informācijas pienācīgu apstrādi. Tas var ietvert, piemēram, īpašus pasākumus, lai nodrošinātu personas informācijas drošību, piemēram, ierobežojumus attiecībā uz piekļuvi personas informācijai, piekļuves kontroli, reģistrus, īpašu apmācību darbiniekiem par personas informācijas apstrādi utt.

Turklāt saskaņā ar *PIPA* 3. panta 5. punktu un 4. pantu datu subjektiem cita starpā ir šādas tiesības attiecībā uz personas informāciju, ko apstrādā valsts drošības nolūkos:

1) tiesības saņemt apstiprinājumu par to, vai personas informācija tiek apstrādāta, kā arī informāciju par apstrādi, un piekļūt šai informācijai, tostarp saņemt kopijas *PIPA* 4. panta 1. un 3. punkts);

2) tiesības apturēt personas informācijas apstrādi un tiesības labot, dzēst un iznīcināt to (*PIPA* 4. panta 4. punkts).

iii) Datu subjekts, izmantojot šīs tiesības, tiešā veidā pārzinim vai netiešā veidā Aizsardzības komisijai var iesniegt pieprasījumu vai pilnvarot savu pārstāvi iesniegt šādu pieprasījumu. Ja datu subjekts iesniedz pieprasījumu, pārzinis nekavējoties piešķir tiesības; tomēr ar noteikumu, ka tas var atlikt, ierobežot vai liegt tiesības, ja informācijas vākšana ir īpaši paredzēta vai neizbēgama, lai izpildītu citus likumus, tādā apmērā un tik ilgi, cik tas ir nepieciešams un samērīgs, lai aizsargātu svarīgu sabiedrības interešu mērķi (piemēram, tiktāl un tik ilgi, kamēr tiesību piešķiršana apdraudētu notiekošu izmeklēšanu vai apdraudētu valsts drošību), vai ja tiesību piešķiršana var radīt kaitējumu trešās personas dzīvībai vai veselībai vai nepamatotu trešās personas īpašuma un citu interešu pārkāpumu. Ja pieprasījums tiek noraidīts vai ierobežots, datu pārzinis nekavējoties informē datu subjektu par iemesliem. Pārzinis sagatavo metodi un procedūru, lai datu subjekti varētu iesniegt pieprasījumus, un tos publiski paziņo, lai datu subjekti varētu par tiem uzzināt.

Turklāt saskaņā ar *PIPA* 58. panta 4. punktu (prasība nodrošināt individuālu sūdzību atbilstīgu izskatīšanu) un *PIPA* 4. panta 5. punktu (tiesības uz atbilstošu tiesisko aizsardzību, izmantojot ātru un taisnīgu procedūru, par kaitējumu, kas radies personas informācijas apstrādes rezultātā) datu subjektiem ir tiesības uz tiesisko aizsardzību. Tas ietver tiesības ziņot par iespējamu pārkāpumu Personas informācijas pārkāpumu ziņojuma centram (saskaņā ar *PIPA* 62. panta 3. punktu), iesniegt sūdzību *PIPC* saskaņā ar *PIPA* 62. pantu par jebkuru pārkāpumu attiecībā uz tiesībām vai interesēm, kas saistītas ar personas informāciju, un tiesības saņemt tiesisko aizsardzību pret *PIPC* lēmumiem vai bezdarbību saskaņā ar Administratīvo lietu iztiesāšanas likumu. Turklāt datu subjekti var saņemt tiesisko aizsardzību saskaņā ar Administratīvo lietu iztiesāšanas likumu, ja ir noticis viņu tiesību vai interešu pārkāpums pārziņa rīkojuma vai bezdarbības dēļ (piemēram, nelikumīga personas datu vākšana), vai saņemt kompensāciju par kaitējumu saskaņā ar Valsts kompensāciju likumu. Šie tiesiskās aizsardzības līdzekļi ir pieejami gan gadījumos, kad, iespējams, tiek pārkāpti noteikumi, kas ietverti konkrētos tiesību aktos, kuros noteikti ierobežojumi un garantijas attiecībā uz personas informācijas vākšanu, piemēram, valsts drošības tiesību aktos, gan *PIPA* noteikumu pārkāpumu gadījumos.

Persona no ES var iesniegt sūdzību *PIPC* ar savas valsts datu aizsardzības iestādes starpniecību, un *PIPC* informēs personu ar valsts datu aizsardzības iestādes starpniecību pēc tam, kad izmeklēšana un korektīvie pasākumi (attiecīgā gadījumā) būs pabeigti.

II PIELIKUMS

2021. gada 18. maijs

Viņa Ekselencei Didjē Reindersam, Eiropas Komisijas tiesiskuma komisāram

Jūsu Ekselence!

Es atzinīgi vērtēju konstruktīvās sarunas starp Koreju un Eiropas Komisiju, kuru mērķis bija izveidot regulējumu personas datu nosūtīšanai no ES uz Koreju.

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

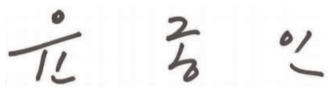
Šis dokuments attiecas uz daudzām Korejas valdības ministrijām un aģentūrām, un attiecībā uz dokumenta saturu attiecīgās ministrijas un aģentūras (Personas informācijas aizsardzības komisija, Tieslietu ministrija, Valsts izlūkdienests, Korejas Valsts cilvēktiesību komisija, Valsts terorisma apkarošanas centrs, Korejas Finanšu ziņu vākšanas vienība) ir atbildīgas par dokumenta daļām, kas ietilpst to attiecīgo kompetenču jomā. Atbilstošās ministrijas un aģentūras un attiecīgie to pārstāvju paraksti ir redzami 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,

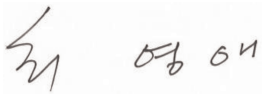


Yoon Jong In
Personas informācijas aizsardzības komisijas priekšsēdētājs

Šo dokumentu ir sagatavojusi Personas informācijas aizsardzības komisija un turpmāk minētās iesaistītās ministrijas un aģentūras.

Park Jie Won
Valsts izlūkdienesta priekšsēdētājs (direktors)

Lee Jung Soo
Tieslietu ministrijas ģenerāldirektors



Choi Young Ae
Korejas Valsts cilvēktiesību komisijas priekšsēdētājs

Kim Hyuck Soo
Valsts terorisma apkarošanas centra direktors

Kim, Jeong Kag
Komisārs, Korejas Finanšu ziņu vākšanas vienība

Tiesiskais regulējums attiecībā uz personas datu vākšanu un izmantošanu, ko Korejas publiskās iestādes veic tiesībaizsardzības un valsts drošības nolūkos

Šajā dokumentā ir sniegts pārskats par to, kāds tiesiskais regulējums paredzēts, lai Korejas publiskās iestādes varētu vākt un izmantot personas datus krimināltiesību aizsardzības un valsts drošības nolūkos (turpmāk – "valdības piekļuve"), jo īpaši attiecībā uz pieejamajiem juridiskajiem pamatiem, piemērojamiem nosacījumiem (ierobežojumiem) un garantijām, tostarp neatkarīgu pārraudzību un individuālās tiesiskās aizsardzības iespējām.

1. VISPĀRĒJIE TIESĪBU PRINCIPI ATTIECĪBĀ UZ VALDĪBAS PIEKĻUVI

1.1. Konstitucionālā sistēma

Korejas Republikas Konstitūcija nosaka tiesības uz privātumu kopumā (17. pants) un jo īpaši tiesības uz korespondences privātumu (18. pants). Valsts pienākums ir garantēt šīs pamattiesības ([1]). Turklāt Konstitūcijā ir noteikts, ka pilsoņu tiesības un brīvības var ierobežot tikai ar tiesību aktu un tikai tad, ja tas ir nepieciešams valsts drošībai vai likumības un kārtības uzturēšanai sabiedrības labklājības labad ([2]). Pat tad, ja šādi ierobežojumi ir noteikti, tie nedrīkst ietekmēt brīvības vai tiesību būtību ([3]). Korejas tiesas ir piemērojušas šos noteikumus lietās par valdības iejaukšanos privātumā. Piemēram, Augstākā tiesa secināja, ka ar civilpersonu uzraudzīšanu tika pārkāptas pamattiesības uz privātumu, uzsverot, ka pilsoņiem ir "tiesības uz pašnoteikšanos attiecībā uz personas informāciju" ([4]). Citā lietā Konstitucionālā tiesa lēma, ka privātums ir pamattiesības, kas nodrošina aizsardzību pret valsts iejaukšanos pilsoņu privātajā dzīvē un tās novērošanu ([5]).

Korejas Konstitūcijā turklāt ir garantēts, ka neviena persona netiek aizturēta, apcietināta, pārmeklēta, nopratināta un netiek konfiscētas lietas, izņemot gadījumus, kas paredzēti tiesību aktos ([6]). Turklāt kratīšanu un konfiskāciju var veikt, tikai pamatojoties uz tiesneša izdotu orderi, pēc prokurora pieprasījuma un ievērojot noteikto kārtību ([7]). Izņēmuma gadījumos, t. i., ja noziedzīga nodarījuma izdarīšanas laikā aizdomās turētais tiek aizturēts (*flagrante delicto*) vai ja pastāv risks, ka persona, ko tur aizdomās par tāda nozieguma izdarīšanu, par kuru draud brīvības atņemšana uz trim gadiem vai ilgāk, var izbēgt vai iznīcināt pierādījumus, izmeklēšanas iestādes var veikt kratīšanu bez ordera vai konfiskāciju, un tādā gadījumā tām ir jāpieprasa orderis *ex post* ([8]). Šie vispārējie principi ir sīkāk izstrādāti īpašos tiesību aktos, kas attiecas uz kriminālprocesu un saziņas aizsardzību (sīkāku pārskatu sk. turpmāk).

Attiecībā uz ārvalstniekiem Konstitūcijā ir noteikts, ka viņu statuss tiek garantēts saskaņā ar starptautiskajām tiesībām un līgumiem ([9]). Privātuma tiesības garantē vairāki starptautiskie nolīgumi, kuru līgumslēdzēja puse ir Koreja, piemēram, Starptautiskais pakts par pilsoniskajām un politiskajām tiesībām (17. pants), Konvencija par personu ar invaliditāti tiesībām (22. pants) un Konvencija par bērna tiesībām (16. pants). Turklāt, lai gan Konstitūcijā principā ir atsauces uz "pilsoņu" tiesībām, Konstitucionālā tiesa ir nolēmusi, ka arī ārvalstniekiem ir pamattiesības ([10]). Konkrētāk, Tiesa nosprieda, ka cilvēka cieņas un vērtības aizsardzība, kā arī tiesības meklēt laimi ir jebkura cilvēka, nevis tikai pilsoņu

([1]) Korejas Republikas Konstitūcijas, kas izsludināta 1948. gada 17. jūlijā (turpmāk "Konstitūcija"), 10. pants.
([2]) Konstitūcijas 37. panta 2. punkts.
([3]) Konstitūcijas 37. panta 2. punkts.
([4]) Korejas Augstākās tiesas 1998. gada 24. jūlija Lēmums Nr. 96DA42789.
([5]) Konstitucionālās tiesas 2003. gada 30. oktobra Lēmums Nr. 2002Hun-Ma51. Līdzīgi 2005. gada 26. maija Lēmumā Nr. 99Hun-Ma513 un Nr. 2004Hun-Ma190 (konsolidēts) Konstitucionālā tiesa precizēja, ka "tiesības kontrolēt savu personas informāciju ir informācijas subjekta tiesības personiski izlemt, kad, kam un cik lielā mērā viņa informācija tiks izpausta vai izmantota un kurš to izpaudīs vai izmantos. Lai gan tās nav precizētas Konstitūcijā, tās ir pamattiesības aizsargāt personisko lēmumu pieņemšanas brīvību pret risku, ko rada valsts funkciju un informācijas komunikācijas tehnoloģijas paplašināšana."
([6]) Konstitūcijas 12. panta 1. punkts, pirmais teikums.
([7]) Konstitūcijas 16. pants un 12. panta 3. punkts.
([8]) Konstitūcijas 12. panta 3. punkts.
([9]) Konstitūcijas 6. panta 2. punkts.
([10]) Konstitucionālās tiesas 1994. gada 29. decembra Lēmums Nr. 93Hun-MA120. Sk. arī, piemēram, Konstitucionālās tiesas 2018. gada 31. maija Lēmumu Nr. 2014Hun-Ma346, kurā Tiesa konstatēja, ka ir pārkāptas Sudānas valstspiederīgā konstitucionālās tiesības saņemt palīdzību no juridiskā padomdevēja lidostā. Citā lietā Konstitucionālā tiesa konstatēja, ka brīvība izvēlēties savu likumīgo darba vietu ir cieši saistīta ar tiesībām tiekties uz laimi, kā arī cilvēka cieņu un vērtību, un tādēļ tā nav paredzēta tikai pilsoņiem, bet to var garantēt arī ārvalstniekiem, kuri ir likumīgi nodarbināti Korejas Republikā (Konstitucionālās tiesas 2011. gada 29. septembra Lēmums Nr. 2007Hun-Ma1083).

tiesības ([11]). Tiesa arī precizēja, ka tiesības kontrolēt savu informāciju tiek uzskatītas par pamattiesībām, kuru pamatā ir tiesības uz cieņu un laimi, kā arī tiesības uz privāto dzīvi ([12]). Lai gan judikatūrā līdz šim nav īpaši aplūkotas personu, kuras nav Korejas valstspiederīgās, tiesības uz privātumu, zinātnieki ir plaši pieņēmuši, ka Konstitūcijas 12.–22. pantā (kas ietver tiesības uz privātumu, kā arī personas brīvību) ir noteiktas "cilvēku tiesības".

Visbeidzot, Konstitūcijā ir paredzētas arī tiesības pieprasīt taisnīgu kompensāciju no publiskajām iestādēm ([13]). Turklāt, pamatojoties uz Konstitucionālās tiesas likumu, ikviena persona, kuras Konstitūcijā garantētās pamattiesības tiek pārkāptas, īstenojot valsts varu (izņemot tiesu spriedumus), var iesniegt Konstitucionālajā tiesā konstitucionālu sūdzību ([14]).

1.2. **Vispārīgi datu aizsardzības noteikumi**

Korejas Republikas vispārējais datu aizsardzības likums – Likums par personas informācijas aizsardzību (turpmāk "*PIPA*") – attiecas gan uz privāto, gan publisko sektoru. Attiecībā uz publiskajām iestādēm *PIPA* īpaši atsaucas uz pienākumu izstrādāt politiku, lai novērstu "personas informācijas ļaunprātīgu un nepareizu izmantošanu, nediskrētu novērošanu un izsekošanu utt., kā arī lai veicinātu cilvēka cieņu un personas privātuma respektēšanu" ([15]).

Uz personas datu apstrādi tiesībaizsardzības nolūkos attiecas visas *PIPA* prasības. Tas nozīmē, piemēram, ka krimināltiesību aizsardzības iestādēm ir jāievēro pienākumi attiecībā uz likumīgu apstrādi, t. i., personas informācijas vākšanai, izmantošanai vai sniegšanai (*PIPA* 15.–18. pants) jāizmanto viens no *PIPA* uzskaitītajiem juridiskajiem pamatiem, kā arī jāievēro nolūka ierobežojuma (*PIPA* 3. panta 1. un 2. punkts), samērīguma / datu minimizēšanas (*PIPA* 3. panta 1. un 6. punkts), ierobežotas datu saglabāšanas (*PIPA* 21. pants), datu drošības, tostarp paziņošanas par datu aizsardzības pārkāpumiem (*PIPA* 3. panta 4. punkts, 29. un 34. pants) un pārredzamības (*PIPA* 3. panta 1. un 5. punkts, 20., 30. un 32. pants) princips. Īpašas garantijas attiecas uz sensitīvu informāciju (*PIPA* 23. pants). Turklāt saskaņā ar *PIPA* 3. panta 5. punktu un 4. pantu, kā arī *PIPA* 35.–39-2. pantu personas var izmantot savas piekļuves, labošanas, dzēšanas un apturēšanas tiesības attiecībā uz tiesībaizsardzības iestādēm.

Lai gan *PIPA* tādējādi pilnībā attiecas uz personas datu apstrādi krimināltiesību aizsardzības nolūkos, tas ietver izņēmumu, ja personas datus apstrādā valsts drošības nolūkos. Saskaņā ar PIPA 58. panta 1. punkta 2. apakšpunktu *PIPA* 15.–50. pants neattiecas uz personas informāciju, kas savākta vai pieprasīta, lai analizētu ar valsts drošību saistītu informāciju ([16]). Savukārt joprojām piemēro *PIPA* I nodaļu (Vispārīgi noteikumi), II nodaļu (Personas informācijas aizsardzības politikas izstrāde u. c.), VIII nodaļu (Kolektīvās prasības iesniegšana par datu pārkāpumiem), IX nodaļu (Papildu noteikumi) un X nodaļu (Noteikumi par soda sankcijām). Tas ietver vispārīgos datu aizsardzības principus, kas izklāstīti 3. pantā (Personas informācijas aizsardzības principi), un individuālās tiesības, kas garantētas *PIPA* 4. pantā (Datu subjektu tiesības). Tas nozīmē, ka galvenie principi un tiesības tiek garantēti arī šajā jomā. Turklāt *PIPA* 58. panta 4. punktā ir paredzēts, ka šāda informācija ir jāapstrādā minimālajā apjomā, kāds nepieciešams paredzētā nolūka sasniegšanai, un minimālajā laikposmā; tajā arī noteikts, ka personas informācijas pārzinim ir jāievieš nepieciešamie pasākumi, lai nodrošinātu datu drošu pārvaldību un pienācīgu apstrādi, piemēram, tehniski, pārvaldības un fiziski aizsardzības pasākumi, kā arī pasākumi individuālu sūdzību atbilstīgai izskatīšanai.

Paziņojumā Nr. 2021-1 par papildu procesuālajiem noteikumiem Likuma par personas informācijas aizsardzību interpretācijai un piemērošanai Personas informācijas aizsardzības komisija (turpmāk "*PIPC*") ir sīkāk precizējusi, kā *PIPA* piemēro personas datu apstrādei valsts drošības nolūkos, ņemot vērā šo daļējo atbrīvojumu ([17]). Tas jo īpaši ietver personu tiesības (piekļuve, labošana, apturēšana un dzēšana), kā arī to iespējamo ierobežojumu pamatojumus. Saskaņā ar Paziņojumu *PIPA* pamatprincipu, tiesību un pienākumu piemērošana personas datu apstrādei valsts drošības nolūkos atspoguļo Konstitūcijā paredzētās garantijas, lai aizsargātu personas tiesības kontrolēt savu personas informāciju. Jebkurš

([11]) Konstitucionālās tiesas 2001. gada 29. novembra Lēmums Nr. 99HeonMa494.
([12]) Sk., piemēram, Konstitucionālās tiesas Lēmumu Nr. 99HunMa513.
([13]) Konstitūcijas 29. panta 1. punkts.
([14]) Konstitucionālās tiesas likuma 68. panta 1. punkts.
([15]) *PIPA* 5. panta 1. punkts
([16]) *PIPA* 58. panta 1. punkta 2. apakšpunkts.
([17]) *PIPC* Paziņojums Nr. 2021-1 par papildu procesuālajiem noteikumiem Likuma par personas informācijas aizsardzību interpretācijai un piemērošanai, III iedaļas 6. punkts.

šo tiesību ierobežojums, piemēram, ja tas nepieciešams valsts drošības aizsardzībai, prasa līdzsvara nodrošināšanu starp personas tiesībām un interesēm un attiecīgajām sabiedrības interesēm, un tas nedrīkst ietekmēt tiesību būtību (Konstitūcijas 37. panta 2. punkts).

2. VALDĪBAS PIEKĻUVE TIESĪBAIZSARDZĪBAS NOLŪKOS

2.1. **Kompetentās publiskās iestādes tiesībaizsardzības jomā**

Pamatojoties uz Kriminālprocesa likumu (turpmāk "*CPA*"), Saziņas privātuma aizsardzības likumu (turpmāk "*CPPA*") un Telesakaru darījumdarbības likumu (turpmāk "*TBA*"), policija, prokurori un tiesas var vākt personas datus krimināltiesību aizsardzības nolūkos. Ciktāl Likumā par Valsts izlūkdienestu piešķirtas šīs pilnvaras arī Valsts izlūkdienestam (turpmāk "NIS"), tam ir jāievēro iepriekš minētie likumi ([18]). Visbeidzot, Likums par konkrētu finanšu darījumu informācijas paziņošanu un izmantošanu (turpmāk "*ARUSFTI*") nodrošina juridisko pamatu finanšu iestādēm izpaust informāciju Korejas Finanšu ziņu vākšanas vienībai (turpmāk "*KOFIU*") nolūkā novērst nelikumīgi iegūtu līdzekļu legalizāciju un terorisma finansēšanu. Šī specializētā aģentūra savukārt var sniegt šādu informāciju tiesībaizsardzības iestādēm. Tomēr šie informācijas izpaušanas pienākumi attiecas tikai uz tiem datu pārziņiem, kuri apstrādā personas kredītinformāciju saskaņā ar Kredītinformācijas likumu un ir pakļauti Finanšu pakalpojumu komisijas uzraudzībai. Tā kā šādu pārziņu veiktā personas kredītinformācijas apstrāde neietilpst lēmuma par aizsardzības līmeņa pietiekamību tvērumā, saskaņā ar *ARUSFTI* piemērojamie ierobežojumi un garantijas šajā dokumentā nav sīkāk aprakstīti.

2.2. **Juridiskais pamats un ierobežojumi**

CPA (sk. 2.2.1. iedaļu), *CPPA* (sk. 2.2.2. iedaļu) un Telesakaru darījumdarbības likums (sk. 2.2.3. iedaļu) nodrošina juridisko pamatu personas informācijas vākšanai tiesībaizsardzības nolūkos un nosaka piemērojamos ierobežojumus un garantijas.

2.2.1. *Kratīšana un konfiskācija*

2.2.1.1. Juridiskais pamats

Prokurori un vecākie kriminālpolicijas ierēdņi var pārbaudīt priekšmetus, pārmeklēt personas vai konfiscēt priekšmetus tikai tad, ja 1) personu tur aizdomās par nozieguma izdarīšanu (aizdomās turētais), 2) ir nepieciešams veikt izmeklēšanu un 3) pārbaudītos priekšmetus, pārmeklējamās personas un visus konfiscētos priekšmetus uzskata par saistītiem ar lietu ([19]). Tiesas var arī veikt kratīšanu un konfiscēt jebkurus priekšmetus, kas izmantojami kā pierādījums vai ko var konfiscēt, ja vien šādus priekšmetus vai personas uzskata par saistītiem ar konkrētu lietu ([20]).

2.2.1.2. Ierobežojumi un garantijas

Kā vispārējs pienākums prokuroriem un kriminālpolicijas ierēdņiem ir jāievēro aizdomās turētā, kā arī jebkuras citas iesaistītās personas cilvēktiesības ([21]). Turklāt obligātos pasākumus, kas nepieciešami, lai sasniegtu izmeklēšanas mērķi, var veikt tikai tad, ja tas skaidri paredzēts *CPA* un tikai tādā mērā, kādā tas ir nepieciešams ([22]).

Policijas ierēdņu vai prokuroru veikta kratīšana, pārbaude vai konfiskācija krimināllizmeklēšanas ietvaros var notikt, tikai pamatojoties uz tiesas izdotu orderi ([23]). Iestāde, kas pieprasa orderi, iesniedz materiālus, kas pierāda, ka persona var tikt turēta aizdomās par nozieguma izdarīšanu, ka ir nepieciešama kratīšana, pārbaude vai konfiskācija un ka pastāv attiecīgie konfiscējamie priekšmeti ([24]). Orderī cita starpā jāietver aizdomās turētā vārds, uzvārds un noziedzīgā nodarījuma nosaukums, pārmeklējamā vieta, persona vai priekšmeti vai konfiscējamie priekšmeti, izdošanas datums un spēkā esības laikposms ([25]). Ja notiekošās tiesvedības ietvaros kratīšana un konfiskācija tiek veikta citā veidā, nevis atklātā tiesas sēdē, iepriekš ir jāsaņem tiesas izdots orderis ([26]). Attiecīgo personu un tās aizstāvjus iepriekš informē par kratīšanu vai konfiskāciju, un tā var būt klāt ordera izpildes laikā ([27]).

([18]) Sk. NIS likuma 3. pantu (Likums Nr. 12948), kas attiecas uz konkrētu noziegumu, piemēram, nemieru, dumpju un ar valsts drošību saistītu noziegumu (piemēram, spiegošanas) krimināllizmeklēšanu. Šādā kontekstā tiktu piemērotas *CPA* procedūras attiecībā uz kratīšanu un konfiskāciju, savukārt *CPPA* reglamentētu saziņas datu vākšanu (sk. 3. daļu par noteikumiem, kas attiecas uz piekļuvi saziņai valsts drošības nolūkos).
([19]) *CPA* 215. panta 1. un 2. punkts.
([20]) *CPA* 106. panta 1. punkts, 107. un 109. pants.
([21]) *CPA* 198. panta 2. punkts.
([22]) *CPA* 199. panta 1. punkts.
([23]) *CPA* 215. panta 1. un 2. punkts.
([24]) Kriminālprocesuālo noteikumu 108. panta 1. punkts.
([25]) *CPA* 114. panta 1. punkts kopā ar *CPA* 219. pantu
([26]) *CPA* 113. pants.
([27]) *CPA* 121. un 122. pants.

Veicot kratīšanu vai konfiskāciju un ja meklēšana jāveic datora diskā vai citā datu nesējā, principā tiks konfiscēti tikai paši dati (kopēti vai izdrukāti), nevis viss datu nesējs ([28]). Pašu datu nesēju var konfiscēt tikai tad, ja tiek uzskatīts, ka pieprasītos datus nav iespējams izdrukāt vai kopēt atsevišķi, vai ja tiek uzskatīts, ka citādi nav iespējams sasniegt kratīšanas mērķi ([29]). Attiecīgā persona nekavējoties jāinformē par konfiskāciju ([30]). Attiecībā uz šo paziņošanas prasību saskaņā ar *CPA* nav nekādu izņēmumu.

Kratīšana, pārbaude un konfiskācija bez ordera var notikt tikai noteiktās situācijās. Pirmkārt, tādā gadījumā, ja nav iespējams iegūt orderi noziedzīga nodarījuma izdarīšanas vietā pastāvošās steidzamības dēļ ([31]). Tomēr pēc tam nekavējoties ir jāsaņem orderis ([32]). Otrkārt, kratīšanu un pārbaudes bez ordera uz vietas var veikt tad, ja aizdomās turētais tiek aizturēts vai arestēts ([33]). Visbeidzot, prokurors vai vecākais kriminālpolicijas ierēdnis var konfiscēt priekšmetu bez ordera, ja aizdomās turētais vai trešā persona to ir izmetusi vai ja tas ir atdots brīvprātīgi ([34]).

Pierādījumus, kas iegūti, pārkāpjot *CPA*, uzskatīs par nepieņemamiem ([35]). Turklāt Krimināllikumā ir noteikts, ka par personu vai personas dzīvesvietas, apsargātas ēkas, konstrukcijas, automobiļa, kuģa, gaisa kuģu vai aizņemtas telpas nelikumīgu kratīšanu soda ar brīvības atņemšanu uz laiku, kas nepārsniedz trīs gadus ([36]). Tādēļ šis noteikums attiecas arī uz gadījumiem, kad nelikumīgas kratīšanas laikā tiek konfiscēti priekšmeti, piemēram, datu nesēji.

2.2.2. *Saziņas informācijas vākšana*

2.2.2.1. Juridiskais pamats

Saziņas informācijas vākšanu reglamentē īpašs likums, proti, *CPPA*. Konkrētāk, *CPPA* ir noteikts vispārējs aizliegums cenzēt jebkuru sūtījumu, noklausīties telesaziņu, sniegt saziņas apstiprinājuma datus vai ierakstīt vai noklausīties jebkādas citu personu sarunas, kas nav publiskotas, izņemot saskaņā ar *CPA*, *CPPA* vai Militārās tiesas likumu ([37]). Jēdziens "saziņa" *CPPA* nozīmē ietver gan parasto pastu, gan telesaziņu ([38]). Šajā sakarā *CPPA* nošķirti "saziņu ierobežojoši pasākumi" ([39]) un "saziņas apstiprinājuma datu" vākšana.

Saziņu ierobežojošu pasākumu jēdziens ietver "cenzūru", t. i., tradicionālā pasta satura vākšanu, kā arī "noklausīšanos", t. i., telesakaru satura tiešu pārtveršanu (iegūšanu vai ierakstīšanu) ([40]). Saziņas apstiprinājuma datu jēdziens ietver "telesakaru ierakstu datus", kas ietver telesakaru datumu, to sākuma un beigu laiku, veikto un saņemto zvanu skaitu, kā arī otras puses abonenta numuru, izmantošanas biežumu, žurnāldatnes par telesakaru pakalpojumu izmantošanu un atrašanās vietas informāciju (piemēram, no pārraides torņiem, kuros uztver signālus) ([41]).

([28]) *CPA* 106. panta 3. punkts.
([29]) *CPA* 106. panta 3. punkts.
([30]) *CPA* 219. pants kopā ar *CPA* 106. panta 4. punktu.
([31]) *CPA* 216. panta 3. punkts.
([32]) *CPA* 216. panta 3. punkts.
([33]) *CPA* 216. panta 1. un 2. punkts.
([34]) *CPA* 218. pants. Saistībā ar personas informāciju tas attiecas tikai un informācijas brīvprātīgu iesniegšanu, ko veic tikai pati persona, nevis personas informācijas pārzinis, kuram ir šāda informācija (tam būtu nepieciešams īpašs juridiskais pamats saskaņā ar Likumu par personas informācijas aizsardzību). Brīvprātīgi iesniegtus priekšmetus kā pierādījumus tiesvedībā atzīst tikai tad, ja nav pamatotu šaubu par to, ka izpaušana ir brīvprātīga, kas prokuroram ir jāpierāda. Sk. Augstākās tiesas 2016. gada 10. marta Lēmumu Nr. 2013Do11233.
([35]) *CPA* 308-2. pants.
([36]) Krimināllikuma 321. pants.
([37]) *CPPA* 3. pants. Militārās tiesas likums principā reglamentē informācijas vākšanu par militārpersonām, un to var piemērot civilpersonām tikai ierobežotā skaitā gadījumu (piemēram, ja militārpersonas un civilpersonas izdarītu noziegumu kopā vai ja persona izdara noziegumu pret militārpersonām, tiesvedību var uzsākt militārajā tiesā, sk. 2. pantu Militārās tiesas likumā). Vispārīgie noteikumi, kas reglamentē kratīšanu un konfiskāciju, ir līdzīgi *CPA*, sk., piemēram, 146.–149. pantu un 153.–156. pantu Militārās tiesas likumā. Piemēram, pasta sūtījumus var savākt tikai tad, ja tas ir nepieciešams izmeklēšanai, un pamatojoties uz Militārās tiesas izdotu orderi. Ja tiktu vākta elektroniskā saziņa, piemērotu *CPPA* noteiktos ierobežojumus un garantijas.
([38]) *CPPA* 2. panta 1. punkts, t. i., "visu veidu skaņu, vārdu, simbolu vai attēlu pārraide vai uztveršana, izmantojot vadu, bezvadu, šķiedru kabeļu vai citas elektromagnētiskās sistēmas, tostarp tālruņa, e-pasta, dalības informācijas pakalpojuma, faksimila un radio peidžeru sistēmas".
([39]) *CPPA* 2. panta 7. punkts un 3. panta 2. punkts.
([40]) "Cenzūra" ir "pasta sūtījuma atvēršana bez attiecīgās puses piekrišanas vai informācijas par tā saturu iegūšana, ierakstīšana vai neizpaušana, izmantojot citus līdzekļus" (*CPPA* 2. panta 6. punkts). "Noklausīšanās" ir "telesakaru satura iegūšana vai ierakstīšana, noklausoties vai kopīgi lasot saziņas skaņas, vārdus, simbolus vai attēlus, izmantojot elektroniskas un mehāniskas ierīces, bez attiecīgās puses piekrišanas vai traucējot to pārraidīšanu un saņemšanu" (*CPPA* 2. panta 7. punkts).
([41]) *CPPA* 2. panta 11. punkts.

CPPA ir noteikti ierobežojumi un garantijas attiecībā uz abu veidu datu vākšanu, un par vairāku šo prasību neievērošanu tiek piemēroti krimināls odi ([42]).

2.2.2.2. Ierobežojumi un garantijas, kas piemērojami saziņas satura vākšanai (saziņu ierobežojoši pasākumi)

Saziņas satura vākšana var notikt tikai kā papildu līdzeklis kriminālizmeklēšanas atvieglošanai (t. i., kā galējais pasākums), un ir jāpieliek pūles, lai līdz minimumam samazinātu iejaukšanos cilvēku saziņas noslēpumos ([43]). Saskaņā ar šo vispārējo principu saziņu ierobežojošus pasākumus var izmantot tikai tad, ja citādi ir grūti novērst nozieguma izdarīšanu, aizturēt noziedznieku vai vākt pierādījumus ([44]). Tiesībaizsardzības iestādēm, kas vāc saziņas saturu, jāpārtrauc to darīt, tiklīdz turpmāka piekļuve vairs netiek uzskatīta par nepieciešamu, tādējādi nodrošinot, ka saziņas privātuma pārkāpumi ir iespējami ierobežoti ([45]).

Turklāt saziņu ierobežojošus pasākumus var izmantot tikai tad, ja ir pamatots iemesls aizdomām, ka tiek plānoti, izdarīti vai ir izdarīti konkrēti *CPPA* īpaši uzskaitīti smagi noziegumi. Tie ietver tādus noziegumus kā nemieri, ar narkotikām saistīti noziegumi vai noziegumi, kas saistīti ar sprāgstvielām, kā arī noziegumi, kas saistīti ar valsts drošību, diplomātiskajām attiecībām vai militārajām bāzēm un iekārtām ([46]). Saziņu ierobežojoša pasākuma mērķim ir jābūt konkrētiem pasta sūtījumiem vai telesakariem, ko aizdomās turētais nosūta vai saņem, vai pasta sūtījumiem vai telesakariem, ko aizdomās turētais nosūta vai saņem noteiktā laikposmā ([47]).

Pat tad, ja šīs prasības ir izpildītas, satura datu vākšana var notikt, tikai pamatojoties uz tiesas izdotu orderi. Konkrētāk, prokurors var lūgt tiesai atļaut vākt satura datus par aizdomās turēto vai personu, uz kuru attiecas izmeklēšana ([48]). Arī kriminālpolicijas ierēdnis var lūgt atļauju prokuroram, kurš savukārt var pieprasīt tiesas orderi ([49]). Ordera pieprasījums jāiesniedz rakstiski, un tajā jāiekļauj konkrēti elementi. Jo īpaši tajā ir jānorāda 1) pamatoti iemesli aizdomām, ka kāds no uzskaitītajiem noziegumiem ir plānots, tiek izdarīts vai ir izdarīts, kā arī jebkādi materiāli, kas rada *prima facie* aizdomas; 2) saziņu ierobežojošie pasākumi, kā arī to mērķobjekts, darbības joma, mērķis un spēkā esības laikposms; un 3) vieta, kur pasākumi tiktu īstenoti, un tas, kā tie tiktu īstenoti ([50]).

Ja ir izpildītas juridiskās prasības, tiesa var piešķirt rakstisku atļauju veikt saziņu ierobežojošus pasākumus attiecībā uz aizdomās turēto vai personu, uz kuru attiecas izmeklēšana ([51]). Šajā orderī ir norādīti pasākumu veidi, kā arī to mērķobjekts, darbības joma, spēkā esības laikposms, izpildes vieta un veids, kā tos īstenot ([52]).

Saziņu ierobežojošus pasākumus var veikt tikai divus mēnešus ([53]). Ja pasākumu mērķis minētajā laikposmā tiek sasniegts agrāk, pasākumi nekavējoties jāpārtrauc. Savukārt, ja vajadzīgie nosacījumi joprojām tiek pildīti, divu mēnešu laikā var iesniegt lūgumu pagarināt saziņu ierobežojošo pasākumu spēkā esības laikposmu. Šādā pieprasījumā jāiekļauj materiāli, kas prima facie pamato pasākumu pagarināšanu ([54]). Pagarinātais laikposms kopumā nedrīkst pārsniegt vienu gadu vai trīs gadus attiecībā uz noteiktiem īpaši smagiem noziegumiem (piemēram, noziegumiem, kas saistīti ar nemieriem, ārvalstu agresiju, valsts drošību utt.) ([55]).

Tiesībaizsardzības iestādes var piespiest sakaru operatoru sniegt palīdzību, iesniedzot tam rakstisku tiesas atļauju ([56]). Sakaru operatoriem ir jāsadarbojas un jāsaglabā saņemtā atļauja to datnēs ([57]). Tie var atteikties sadarboties, ja informācija par konkrēto personu, kā norādīts tiesas rakstiskajā atļaujā (piemēram, personas tālruņa numurs), ir nepareiza. Turklāt tiem jebkuros apstākļos ir aizliegts izpaust telesakaros izmantotās paroles ([58]).

([42]) *CPPA* 16. un 17. pants. Tas attiecas, piemēram, uz vākšanu bez ordera, uzskaites neveikšanu, vākšanas nepārtraukšanu, kad ārkārtas stāvoklis vairs nepastāv, vai nepaziņošanu attiecīgajai personai.
([43]) *CPPA* 3. panta 2. punkts.
([44]) *CPPA* 5. panta 1. punkts.
([45]) *CPPA* Izpildes dekrēta 2. pants.
([46]) *CPPA* 5. panta 1. punkts.
([47]) *CPPA* 5. panta 2. punkts.
([48]) *CPPA* 6. panta 1. punkts.
([49]) *CPPA* 6. panta 2. punkts.
([50]) *CPPA* 6. panta 4. punkts un *CPPA* Izpildes dekrēta 4. panta 1. punkts.
([51]) *CPPA* 6. panta 5. punkts un 6. panta 8. punkts.
([52]) *CPPA* 6. panta 6. punkts.
([53]) *CPPA* 6. panta 7. punkts.
([54]) *CPPA* 6. panta 7. punkts.
([55]) *CPPA* 6. panta 8. punkts.
([56]) *CPPA* 9. panta 2. punkts.
([57]) *CPPA* 15-2. pants un *CPPA* Izpildes dekrēta 12. pants.
([58]) *CPPA* 9. panta 4. punkts.

Ikvienam, kas veic saziņu ierobežojošus pasākumus vai lūdz sadarboties, ir jāglabā dokumentācija, kurā norādīti pasākumu mērķi, to izpilde, sadarbības nodrošināšanas datums un mērķobjekts ([59]). Arī tiesībaizsardzības iestādēm, kas īsteno saziņu ierobežojošus pasākumus, ir jāglabā dokumentācija, kurā izklāstīta sīkāka informācija un gūtie rezultāti ([60]). Kriminālpolicijas ierēdņiem šī informācija ir jāsniedz prokuroram, slēdzot izmeklēšanu ([61]).

Ja prokurors izdod apsūdzību attiecībā uz lietu, kurā ir izmantoti saziņu ierobežojošie pasākumi, vai izdod rīkojumu neapsūdzēt vai neaizturēt attiecīgo personu (t. i., ne tikai apsūdzības atlikšana), prokuroram ir jāinformē persona, uz kuru attiecas saziņu ierobežojošie pasākumi, par to, ka ir izpildīti saziņu ierobežojošie pasākumi, izpildaģentūra un izpildes laikposms. Šāds paziņojums jāsniedz rakstiski 30 dienu laikā no rīkojuma izdošanas dienas ([62]). Paziņojumu var atlikt, ja tas var nopietni apdraudēt valsts drošību vai traucēt sabiedrisko drošību un kārtību, vai ja tas var radīt būtisku kaitējumu citu cilvēku dzīvībai un veselībai ([63]). Plānojot atlikt paziņojumu, prokuroram vai kriminālpolicijas ierēdnim jāsaņem apgabala prokuratūras vadītāja apstiprinājums ([64]). Tiklīdz atlikšanas iemesli vairs nepastāv, paziņojums jāsniedz 30 dienu laikā no attiecīgā brīža ([65]).

CPPA ir noteikta arī īpaša procedūra saziņas satura vākšanai ārkārtas situācijās. Jo īpaši tiesībaizsardzības iestādes var vākt saziņas saturu gadījumā, ja ir gaidāma organizētās noziedzības vai citas smagas noziedzības, kas var tieši izraisīt nāvi vai smagu ievainojumu, plānošana vai izpilde un pastāv ārkārtas situācija, kuras dēļ nav iespējams veikt parasto procedūru (kā izklāstīts iepriekš) ([66]). Šādā ārkārtas situācijā policijas ierēdnis vai prokurors var veikt saziņu ierobežojošus pasākumus bez tiesas iepriekšējas atļaujas, bet tūlīt pēc izpildes ir jāiesniedz pieteikums tiesas atļaujas saņemšanai. Ja tiesībaizsardzības iestāde 36 stundu laikā no brīža, kad veikti ārkārtas pasākumi, nesaņem tiesas atļauju, vākšana nekavējoties jāpārtrauc, un tam parasti seko savāktās informācijas iznīcināšana ([67]). Policijas ierēdņi, kas veic ārkārtas novērošanu, to dara prokurora uzraudzībā, vai gadījumā, ja prokurora norādījumu iepriekšēja saņemšana nav iespējama steidzamības dēļ, policijai tūlīt pēc izpildes sākšanas ir jāsaņem prokurora apstiprinājums ([68]). Noteikumi par personas informēšanu, kā aprakstīts iepriekš, attiecas arī uz saziņas satura vākšanu ārkārtas situācijās.

Informācijas vākšana ārkārtas situācijās vienmēr jāveic saskaņā ar "ārkārtas cenzūras / sarunu noklausīšanās paziņojumu", un iestādei, kas veic vākšanu, ir jāreģistrē visi ārkārtas pasākumi ([69]). Tiesai iesniedzamajai prasībai piešķirt atļauju ārkārtas pasākumu veikšanai jāpievieno rakstisks dokuments, kurā norādīti nepieciešamie saziņu ierobežojošie pasākumi, mērķobjekts, priekšmets, darbības joma, izpildes vieta, metode, kā arī paskaidrojumi par to, kā attiecīgie saziņu ierobežojošie pasākumi atbilst *CPPA* 5. panta 1. punktam ([70]), kā arī apliecinošie dokumenti.

Gadījumos, kad ārkārtas pasākumi ir pabeigti īsā laikā, tādējādi izslēdzot iespēju pieprasīt tiesas atļauju (piemēram, ja aizdomās turētais tiek aizturēts tūlīt pēc pārtveršanas uzsākšanas, kas tādēļ tiek izbeigta), kompetentās prokuratūras vadītājs kompetentajai tiesai nosūta paziņojumu par ārkārtas pasākumu ([71]). Paziņojumā jānorāda mērķis, mērķobjekts, darbības joma, izpildes vieta un vākšanas metode, kā arī iemesli, kāpēc nav iesniegts tiesas atļaujas pieprasījums ([72]). Šis paziņojums ļauj saņēmējai tiesai pārbaudīt vākšanas likumību, un tas ir jāievada ārkārtas pasākumu paziņojumu reģistrā.

([59]) *CPPA* 9. panta 3. punkts.
([60]) *CPPA* Izpildes dekrēta 18. panta 1. punkts.
([61]) *CPPA* Izpildes dekrēta 18. panta 2. punkts.
([62]) *CPPA* 9-2. panta 1. punkts.
([63]) *CPPA* 9-2. panta 4. punkts.
([64]) *CPPA* 9-2. panta 5. punkts.
([65]) *CPPA* 9-2. panta 6. punkts.
([66]) *CPPA* 8. panta 1. punkts.
([67]) *CPPA* 8. panta 2. punkts.
([68]) *CPPA* 8. panta 3. punkts un *CPPA* Izpildes dekrēta 16. panta 3. punkts.
([69]) *CPPA* 8. panta 4. punkts.
([70]) Proti, ir pamatots iemesls aizdomām, ka tiek plānoti vai tiek izdarīti konkrēti smagi noziegumi, vai tie ir izdarīti, un citādi nav iespējams novērst nozieguma izdarīšanu, aizturēt noziedzīgu nodarījuma veicēju vai vākt pierādījumus.
([71]) *CPPA* 8. panta 5. punkts.
([72]) *CPPA* 8. panta 6. un 7. punkts.

Vispārīga prasība ir tāda, ka saziņas saturu, kas iegūts, izpildot saziņu ierobežojošus pasākumus saskaņā ar *CPPA*, var izmantot tikai ar mērķi izmeklēt un novērst konkrētus iepriekš minētos noziegumus, kā arī saukt pie atbildības par to veikšanu, disciplinārlietās par tiem pašiem noziegumiem, saistībā ar prasību par kaitējuma atlīdzināšanu, ko cēlusi saziņas puse, vai gadījumos, kad to atļauj citi tiesību akti ([73]).

Ja tiek vākti internetā pārraidītu telesakaru dati, piemēro īpašas garantijas ([74]). Šādu informāciju var izmantot tikai nolūkā izmeklēt *CPPA* 5. panta 1. punktā uzskaitītos smagos noziegumus. Lai saglabātu informāciju, ir jāsaņem apstiprinājums no tiesas, kas atļāvusi saziņu ierobežojošus pasākumus ([75]). Saglabāšanas pieprasījumā jāietver informācija par saziņu ierobežojošiem pasākumiem, pasākumu rezultātu kopsavilkums, saglabāšanas iemesli (kopā ar apliecinošiem materiāliem) un saglabājamā telesaziņa ([76]). Ja šāda pieprasījuma nav, iegūtā telesaziņa ir jādzēš 14 dienu laikā pēc tam, kad ir beigušies saziņu ierobežojošie pasākumi ([77]). Ja pieprasījums tiek noraidīts, telesaziņa jāiznīcina septiņu dienu laikā ([78]). Ja telesaziņa tiek izdzēsta, septiņu dienu laikā tiesā, kas atļāvusi saziņu ierobežojošus pasākumus, jāiesniedz ziņojums, izklāstot dzēšanas iemeslus, kā arī ar pasākumiem saistītu informāciju un termiņus.

Raugoties vispārīgāk, ja informācija ir iegūta nelikumīgi, izmantojot saziņu ierobežojošus pasākumus, tā netiks atzīta par pierādījumu tiesā vai disciplinārlietā ([79]). *CPPA* arī aizliegts jebkurai personai, kas veic saziņu ierobežojošus pasākumus, izpaust konfidenciālu informāciju, kas iegūta, īstenojot šādus pasākumus, un izmantot iegūto informāciju, lai grautu to personu reputāciju, uz kurām attiecas šie pasākumi ([80]).

2.2.2.3. Ierobežojumi un garantijas, kas piemērojami saziņas apstiprinājuma informācijas vākšanai

Pamatojoties uz *CPPA*, tiesībaizsardzības iestādes var pieprasīt telesakaru operatoriem sniegt saziņas apstiprinājuma datus, ja tas ir nepieciešams, lai veiktu izmeklēšanu vai piemērotu sodu ([81]). Atšķirībā no satura datu vākšanas iespēja vākt saziņas apstiprinājuma datus neaprobežojas tikai ar noteiktiem konkrētiem noziegumiem. Tomēr, tāpat kā satura datu gadījumā, saziņas apstiprinājuma datu vākšanai ir nepieciešama iepriekšēja rakstiska tiesas atļauja, ievērojot tos pašus nosacījumus, kas aprakstīti iepriekš ([82]). Ja steidzamības dēļ nav iespējams saņemt tiesas atļauju, saziņas apstiprinājuma datus var vākt bez ordera, un tādā gadījumā atļauja ir jāsaņem tūlīt pēc datu pieprasīšanas un par to jāpaziņo telesakaru pakalpojumu sniedzējam ([83]). Ja turpmāka atļauja netiek saņemta, savāktā informācija ir jāiznīcina ([84]).

Prokuroriem, kriminālpolicijas ierēdņiem un tiesām ir jāglabā dokumentācija par pieprasījumiem sniegt saziņas apstiprinājuma datus ([85]). Turklāt telesakaru pakalpojumu sniedzējiem divreiz gadā ir jāziņo par saziņas apstiprinājuma datu izpaušanu zinātnes un IKT ministram un jāglabā to uzskaite septiņus gadus no datu izpaušanas dienas ([86]).

Personas principā tiek informētas par to, ka ir savākti saziņas apstiprinājuma dati ([87]). Šādas informācijas sniegšanas termiņš ir atkarīgs no izmeklēšanas apstākļiem ([88]). Tiklīdz ir pieņemts lēmums par kriminālvajāšanu / tās neveikšanu, paziņojums jāsniedz 30 dienu laikā. Savukārt, ja apsūdzība tiek apturēta, paziņojums jāsniedz 30 dienu laikā pēc tam, kad pagājis viens gada pēc šāda lēmuma pieņemšanas. Jebkurā gadījumā paziņojums jāsniedz 30 dienu laikā pēc tam, kad pagājis viens gada pēc informācijas savākšanas.

Paziņojumu var atlikt, ja tas var 1) apdraudēt valsts drošību, sabiedrisko drošību un kārtību, 2) izraisīt nāvi vai miesas bojājumus, 3) kavēt taisnīgu tiesvedību (piemēram, izraisīt pierādījumu iznīcināšanu vai apdraudējumu lieciniekiem)

([73]) *CPPA* 12. pants.
([74]) *CPPA* 12-2. pants.
([75]) Prokuroram vai policijas ierēdnim, kas īsteno saziņu ierobežojošus pasākumus, 14 dienu laikā pēc pasākumu beigām jāizvēlas saglabājamā telesaziņa un jāpieprasa tiesas apstiprinājums (policijas ierēdņa gadījumā pieteikumu iesniedz prokuroram, kurš savukārt iesniedz pieprasījumu tiesā), sk. *CPPA* 12-2. panta 1. un 2. punktu.
([76]) *CPPA* 12-2. panta 3. punkts.
([77]) *CPPA* 12-2. panta 5. punkts.
([78]) *CPPA* 12-2. panta 5. punkts.
([79]) *CPPA* 4. pants.
([80]) *CPPA* Izpildes dekrēta 11. panta 2. punkts.
([81]) *CPPA* 13. panta 1. punkts.
([82]) *CPPA* 13. un 6. pants.
([83]) *CPPA* 13. panta 2. punkts. Tāpat kā attiecībā uz steidzamiem saziņu ierobežojošiem pasākumiem ir jāsagatavo dokuments, kurā izklāstīta sīka informācija par lietu (aizdomās turētais, veicamie pasākumi, iespējamais noziegums, kā arī steidzamība). Sk. *CPPA* Izpildes dekrēta 37. panta 5. punktu.
([84]) *CPPA* 13. panta 3. punkts.
([85]) *CPPA* 13. panta 5. un 6. punkts.
([86]) *CPPA* 13. panta 7. punkts.
([87]) Sk. *CPPA* 13-3. panta 7. punktu kopā ar 9-2. pantu.
([88]) *CPPA* 13-3. panta 1. punkts.

vai 4) apmelot aizdomās turēto, cietušos vai citas ar lietu saistītas personas vai aizskart to privātumu ([89]). Paziņošanai, pamatojoties uz kādu no iepriekš minētajiem iemesliem, ir vajadzīga kompetentās apgabala prokuratūras direktora atļauja ([90]). Ja atlikšanas iemesli jeb pamatojumi vairs nepastāv, paziņojums jāsniedz 30 dienu laikā no minētā brīža ([91]).

Personas, kurām sniegts paziņojums, var iesniegt prokuroram vai kriminālpolicijas ierēdnim rakstisku pieprasījumu par saziņas apstiprinājuma datu vākšanas iemesliem ([92]). Šādā gadījumā prokuroram vai kriminālpolicijas ierēdnim ir rakstiski jānorāda iemesli 30 dienu laikā pēc pieprasījuma saņemšanas, ja vien nav piemērojams kāds no iepriekš minētajiem iemesliem (izņēmums attiecībā uz paziņošanas atlikšanu) ([93]).

2.2.3. *Telesakaru uzņēmumu brīvprātīga informācijas izpaušana*

TBA 83. panta 3. punkts ļauj telesakaru uzņēmumiem brīvprātīgi izpildīt tiesas, prokurora vai izmeklēšanas iestādes vadītāja pieprasījumu (kas iesniegts, lai atbalstītu kriminālllietu, izmeklēšanu vai soda izpildi) atklāt "saziņas datus". *TBA* kontekstā "saziņas dati" ietver lietotāju vārdu, uzvārdu, iedzīvotāju reģistrācijas numuru, adresi un tālruņa numuru, datumus, kuros lietotāji sāk vai beidz lietot abonementu, kā arī lietotāju identifikācijas kodus (t. i., kodus, ko izmanto, lai identificētu datorsistēmu vai saziņas tīklu likumīgo lietotāju) ([94]). *TBA* vajadzībām par lietotājiem uzskata tikai tās personas, kas tieši slēdz līgumus par Korejas telesakaru pakalpojumu sniedzēja nodrošinātiem pakalpojumiem ([95]). Tādējādi situācijas, kad ES fiziskas personas, kuru dati ir nosūtīti Korejas Republikai, tiktu uzskatītas par lietotājiem saskaņā ar *TBA*, visticamāk, būtu ļoti ierobežotas, jo šīs personas parasti neslēgtu tiešu līgumu ar Korejas telesakaru operatoru.

Pieprasījumi saņemt saziņas datus, pamatojoties uz *TBA*, jāiesniedz rakstiski, norādot pieprasījuma iemeslus, saiti uz attiecīgo lietotāju un pieprasīto datu apjomu ([96]). Ja steidzamības dēļ rakstisku pieprasījumu nav iespējams iesniegt, rakstisks pieprasījums jāiesniedz, tiklīdz ir zudis steidzamības iemesls ([97]). Telesakaru uzņēmumiem, kas izpilda pieprasījumus par saziņas datu sniegšanu, ir jāsaglabā virsgrāmatas, kurās ir ieraksti, kas norāda, ka ir sniegti saziņas dati, kā arī saistītie materiāli, piemēram, rakstisks pieprasījums ([98]). Turklāt telesakaru uzņēmumiem divreiz gadā ir jāziņo par saziņas datu sniegšanu zinātnes un IKT ministram ([99]).

Telesakaru uzņēmumiem nav pienākuma izpildīt pieprasījumus atklāt saziņas datus, pamatojoties uz *TBA*. Tāpēc katrs pieprasījums operatoram ir jāizvērtē, ņemot vērā piemērojamās datu aizsardzības prasības saskaņā ar *PIPA*. Telesakaru uzņēmumam jo īpaši ir jāņem vērā datu subjekta intereses, un tas nedrīkst izpaust informāciju, ja tas varētu negodīgi aizskart personas vai trešās personas intereses ([100]). Turklāt saskaņā ar Paziņojumu Nr. 2021-1 par papildu procesuālajiem noteikumiem Likuma par personas informācijas aizsardzību interpretācijai un piemērošanai attiecīgā persona ir jāinformē par informācijas izpaušanu. Izņēmuma gadījumos šādu paziņošanu var atlikt, jo īpaši, ja un kamēr paziņošana apdraudētu noziedzīgu nodarījumu izmeklēšanu vai varētu kaitēt citas personas dzīvībai vai veselībai, ja minētās tiesības vai intereses nepārprotami prevalē pār datu subjekta tiesībām ([101]).

Augstākā tiesa 2016. gadā apstiprināja, ka apstāklis, ka telesakaru uzņēmumi brīvprātīgi sniedz saziņas datus bez ordera, pamatojoties uz *TBA*, pats par sevi nepārkāpj telesakaru pakalpojuma lietotāja tiesības uz pašnoteikšanos informācijas jomā. Tajā pašā laikā Tiesa precizēja, ka šāds pārkāpums rastos tad, ja būtu acīm redzams, ka pieprasījuma iesniedzēja aģentūra ir ļaunprātīgi izmantojusi savas pilnvaras pieprasīt saziņas datu izpaušanu, tādējādi pārkāpjot attiecīgās personas vai trešās personas intereses ([102]). Raugoties vispārīgāk, visiem tiesībaizsardzības iestāžu pieprasījumiem par brīvprātīgu informācijas izpaušanu ir jāatbilst likumīguma, nepieciešamības un samērīguma principiem, kas izriet no Korejas Konstitūcijas (12. panta 1. punkts un 37. panta 2. punkts).

([89]) *CPPA* 13-3. panta 2. punkts.
([90]) *CPPA* 13-3. panta 3. punkts.
([91]) *CPPA* 13-3. panta 4. punkts.
([92]) *CPPA* 13-3. panta 5. punkts.
([93]) *CPPA* 13-3. panta 6. punkts.
([94]) *TBA* 83. panta 3. punkts.
([95]) *TBA* 2. panta 9. punkts.
([96]) *TBA* 83. panta 4. punkts.
([97]) *TBA* 83. panta 4. punkts.
([98]) *TBA* 83. panta 5. punkts.
([99]) *TBA* 83. panta 6. punkts.
([100]) *PIPA* 18. panta 2. punkts
([101]) *PIPC* Paziņojums Nr. 2021-1 par papildu procesuālajiem noteikumiem Likuma par personas informācijas aizsardzību interpretācijai un piemērošanai, III iedaļas 2. punkta iii) apakšpunkts.
([102]) Augstākās tiesas 2016. gada 10. marta Lēmums Nr. 2012Da105482.

2.3. **Pārraudzība**

Krimināltiesību aizsardzības iestāžu pārraudzību veic, izmantojot dažādus mehānismus gan iekšēji, gan ārējas struktūras.

2.3.1. *Pašrevīzija*

Saskaņā ar Likumu par publiskā sektora revīzijām publiskās iestādes tiek mudinātas izveidot iekšēju pašrevīzijas struktūru, kuras uzdevums cita starpā būtu veikt likumības pārbaudi ([103]). Šādu revīzijas struktūru vadītājiem pēc iespējas ir jāgarantē neatkarība ([104]). Konkrētāk, viņus ieceļ amatā no personu vidus ārpus attiecīgās iestādes (piemēram, bijušos tiesnešus, profesorus) uz laiku no diviem līdz pieciem gadiem, un viņus var atlaist tikai pamatotu iemeslu dēļ (piemēram, ja viņi nespēj pildīt pienākumus garīgu vai fizisku traucējumu dēļ, ja viņus sauc pie disciplināras atbildības) ([105]). Revidentus ieceļ, pamatojoties uz īpašiem likumā paredzētiem nosacījumiem ([106]). Revīzijas ziņojumos var iekļaut ieteikumus vai kompensācijas vai korekcijas pieprasījumus, kā arī rājienus un ieteikumus vai pieprasījumus saukt pie disciplināras atbildības ([107]). Par tiem 60 dienu laikā pēc revīzijas pabeigšanas paziņo tās publiskās iestādes vadītājam, uz kuru attiecas revīzija, kā arī Revīzijas un inspekcijas padomei (sk. 2.3.2. iedaļu) ([108]). Attiecīgajai iestādei jāīsteno vajadzīgie pasākumi un par rezultātiem jāziņo Revīzijas un inspekcijas padomei ([109]). Turklāt revīzijas rezultāti parasti ir publiski pieejami ([110]). Par atteikšanos veikt pašrevīziju vai tās kavēšanu piemēro administratīvus naudas sodus ([111]). Krimināltiesību jomā, lai ievērotu iepriekš minētos tiesību aktus, Valsts policijas aģentūra izmanto ģenerālinspektora sistēmu iekšējo revīziju veikšanai, tostarp attiecībā uz iespējamiem cilvēktiesību pārkāpumiem ([112]).

2.3.2. *Revīzijas un inspekcijas padome*

Revīzijas un inspekcijas padome (turpmāk "*BAI*") var pārbaudīt publisko iestāžu darbību un, pamatojoties uz šādām pārbaudēm, sniegt ieteikumus, pieprasīt disciplināratbildību vai iesniegt krimināllapsūdzību ([113]). *BAI* ir izveidota Korejas Republikas prezidenta pakļautībā, bet attiecībā uz tās pienākumiem saglabā neatkarīgu statusu ([114]). Turklāt likumā, ar ko izveidota *BAI*, ir prasīts, lai *BAI* tiktu piešķirta maksimāla neatkarība attiecībā uz tās personāla iecelšanu, atlaišanu un organizāciju, kā arī tās budžeta veidošanu ([115]). *BAI* priekšsēdētāju ieceļ prezidents ar Nacionālās asamblejas piekrišanu ([116]). Pārējos sešus komisārus pēc priekšsēdētāja ieteikuma ieceļ prezidents uz četriem gadiem ([117]). Komisāriem (tostarp priekšsēdētājam) ir jābūt ar konkrētu kvalifikāciju, kas noteikta tiesību aktos ([118]), un viņus var atlaist tikai tad, ja ir impīčmenta gadījums, viņiem ir piespriests cietumsods vai viņi nespēj pildīt savus pienākumus ilgstošas garīgas vai fiziskas nespējas dēļ ([119]). Turklāt komisāriem ir aizliegts piedalīties politiskajā darbībā un vienlaikus ieņemt amatus Nacionālajā asamblejā, administratīvajās aģentūrās, organizācijās, kuru revīziju un pārbaudi veic *BAI*, vai jebkuru citu atalgotu amatu ([120]).

BAI katru gadu veic vispārēju revīziju, bet tā var veikt arī īpašas revīzijas par īpašiem jautājumiem. *BAI* var pieprasīt iesniegt dokumentus pārbaudes gaitā un pieprasīt personu piedalīšanos ([121]). Revīzijas ietvaros *BAI* pārbauda valsts ieņēmumus un izdevumus, kā arī pārrauga publisko iestāžu un valsts amatpersonu pienākumu vispārēju ievērošanu,

([103]) Likuma par publiskā sektora revīzijām 3. un 5. pants.
([104]) Likuma par publiskā sektora revīzijām 7. pants.
([105]) Likuma par publiskā sektora revīzijām 8.–11. pants.
([106]) Likuma par publiskā sektora revīzijām 16. pants un turpmākie panti.
([107]) Likuma par publiskā sektora revīzijām 23. panta 2. punkts.
([108]) Likuma par publiskā sektora revīzijām 23. panta 1. punkts.
([109]) Likuma par publiskā sektora revīzijām 23. panta 3. punkts.
([110]) Likuma par publiskā sektora revīzijām 26. pants.
([111]) Likuma par publiskā sektora revīzijām 41. pants.
([112]) Sk. jo īpaši Revīzijas un inspekcijas ģenerāldirektora nodaļas: https://www.police.go.kr/eng/knpa/org/org01.jsp.
([113]) Revīzijas un inspekcijas padomes likuma (turpmāk "BAI likums") 24. pants un 31.–35. pants.
([114]) *BAI* likuma 2. panta 1. punkts.
([115]) *BAI* likuma 2. panta 2. punkts.
([116]) *BAI* likuma 4. panta 1. punkts.
([117]) *BAI* likuma 5. panta 1. punkts un 6. pants.
([118]) Piemēram, vismaz desmit gadu darba pieredze tiesneša, prokurora vai advokāta amatā, vismaz astoņu gadu darba pieredze valsts ierēdņa vai profesora, vai augstākā amatā universitātē vai vismaz desmit gadu darba pieredze biržu sarakstos iekļautā sabiedrībā vai valsts finansētā iestādē (no tiem vismaz piecu gadu darba pieredze izpilddirektora amatā), sk. BAI likuma 7. pantu.
([119]) *BAI* likuma 8. pants.
([120]) *BAI* likuma 9. pants.
([121]) Sk., piem., *BAI* likuma 27. pantu.

lai uzlabotu valsts pārvaldes darbību ([122]). Tādējādi tās veiktā pārraudzība neaprobežojas tikai ar budžeta aspektiem un ietver arī likumības pārbaudi.

2.3.3. *Nacionālā asambleja*

Nacionālā asambleja var izmeklēt un pārbaudīt publiskās iestādes ([123]). Izmeklēšanas vai pārbaudes laikā Nacionālā asambleja var pieprasīt izpaust dokumentu saturu un izsaukt lieciniekus ([124]). Ikvienam, kas sniedz nepatiesu liecību Nacionālās asamblejas izmeklēšanas laikā, piemēro krimināLsodus (ieslodzījums uz laiku līdz desmit gadiem) ([125]). Pārbaužu procesu un rezultātus var publiskot ([126]). Ja Nacionālā asambleja konstatē nelikumīgas vai nepareizas darbības, tā var pieprasīt, lai attiecīgā publiskā iestāde veic korektīvus pasākumus, tostarp piešķir kompensāciju, veic disciplinārus pasākumus un uzlabo savas iekšējās procedūras ([127]). Pēc šāda pieprasījuma iestādei jārīkojas nekavējoties un par rezultātiem jāziņo Nacionālajai asamblejai ([128]).

2.3.4. *Personas informācijas aizsardzības komisija*

Personas informācijas aizsardzības komisija (turpmāk "*PIPC*") uzrauga personas informācijas apstrādi, ko veic krimināltiesību aizsardzības iestādes saskaņā ar *PIPA*. Turklāt saskaņā ar *PIPA* 7-8. panta 3. un 4. punktu un 7-9. panta 5. punktu *PIPC* veikta uzraudzība attiecas arī uz iespējamiem tādu noteikumu pārkāpumiem, ar kuriem nosaka ierobežojumus un garantijas attiecībā uz personas informācijas vākšanu, tostarp tādu noteikumu pārkāpumiem, kas ietverti īpašos tiesību aktos, kuri reglamentē (elektronisko) pierādījumu vākšanu krimināltiesību aizsardzības nolūkos (sk. 2.2. iedaļu). Ņemot vērā *PIPA* 3. panta 1. punktā noteiktās prasības likumīgai un godprātīgai personas informācijas vākšanai, jebkurš šāds pārkāpums ir arī *PIPA* pārkāpums, kas ļauj *PIPC* veikt izmeklēšanu un veikt korektīvus pasākumus ([129]).

Veicot pārraudzības funkciju, *PIPC* ir piekļuve visai attiecīgajai informācijai ([130]) *PIPC* var sniegt padomus tiesībaizsardzības iestādēm, lai uzlabotu personas informācijas aizsardzības līmeni to apstrādes darbībās, noteikt korektīvus pasākumus (piemēram, apturēt datu apstrādi vai veikt nepieciešamos pasākumus personas informācijas aizsardzībai) vai ieteikt iestādei veikt disciplinārus pasākumus ([131]). Visbeidzot, krimināLsodi ir paredzēti par konkrētiem *PIPA* pārkāpumiem, piemēram, personas informācijas nelikumīgu izmantošanu vai izpaušanu trešām personām vai sensitīvas informācijas nelikumīgu apstrādi ([132]). Šajā sakarā *PIPC* var nodot lietu kompetentai izmeklēšanas iestādei (tostarp prokuroram) ([133]).

2.3.5. *Valsts cilvēktiesību komisija*

Valsts cilvēktiesību komisija (turpmāk "*NHRC*"), kas ir neatkarīga struktūra, kuras uzdevums ir aizsargāt un veicināt pamattiesības ([134]), ir pilnvarota izmeklēt un novērst Konstitūcijas 10.–22. panta pārkāpumus, tostarp attiecībā uz tiesībām uz privātumu un korespondences privātumu. *NHRC* sastāvā ir 11 komisāri, kurus ieceļ Nacionālā asambleja (četrus), prezidents (četrus) un Augstākās tiesas priekšsēdētājs (trīs) ([135]). Lai komisāru varētu iecelt, komisāram: 1) vismaz desmit gadus ir jābūt strādājušam universitātē vai pilnvarotā pētniecības institūtā vismaz par asociēto profesoru; 2) vismaz desmit gadus ir jābūt strādājušam par tiesnesi, prokuroru vai advokātu; 3) vismaz desmit gadus ir jābūt bijušam iesaistītam ar cilvēktiesībām saistītās darbībās (piem., bezpeļņas, nevalstiskās vai starptautiskās organizācijās); vai 4) ir jābūt pilsoniskās sabiedrības grupu izvirzītam kandidātam ([136]). Prezidents no komisāru vidus ieceļ

([122]) *BAI* likuma 20. un 24. pants.
([123]) Likuma par Nacionālo asambleju 128. pants un Likuma par pārbaudēm un izmeklēšanu valsts pārvaldes jomā 2., 3. un 15. pants. Tas ietver ikgadējas valsts lietu pārbaudes kopumā un konkrētu jautājumu izmeklēšanu.
([124]) Likuma par pārbaudēm un izmeklēšanu valsts pārvaldes jomā 10. panta 1. punkts. Sk. arī Likuma par Nacionālo asambleju 128. un 129. pantu.
([125]) Likuma par liecību sniegšanu, novērtēšanu utt. Nacionālajā asamblejā 14. pants.
([126]) Likuma par pārbaudēm un izmeklēšanu valsts pārvaldes jomā 12-2. pants.
([127]) Likuma par pārbaudēm un izmeklēšanu valsts pārvaldes jomā 16. panta 2. punkts.
([128]) Likuma par pārbaudēm un izmeklēšanu valsts pārvaldes jomā 16. panta 3. punkts.
([129]) *PIPC* Paziņojumu Nr. 2021-1 par papildu procesuālajiem noteikumiem Likuma par personas informācijas aizsardzību interpretācijai un piemērošanai.
([130]) *PIPA* 63. pants.
([131]) *PIPA* 61. panta 2. punkts, 65. panta 1. punkts, 65. panta 2. punkts un 64. panta 4. punkts.
([132]) *PIPA* 70.–74. pants.
([133]) *PIPA* 65. panta 1. punkts
([134]) Likuma par Valsts cilvēktiesību komisiju (turpmāk "NHRC likums") 1. pants.
([135]) *NHRC* likuma 5. panta 1. un 2. punkts.
([136]) *NHRC* likuma 5. panta 3. punkts.

priekšsēdētāju, kas jāapstiprina Nacionālajai asamblejai ([137]). Komisārus (tostarp priekšsēdētāju) ieceļ uz atjaunojamu trīs gadu termiņu, un viņus var atlaist tikai tad, ja viņiem piespriesta brīvības atņemšanas vai viņi vairs nespēj pildīt savus pienākumus ilgstošas fiziskas vai garīgas nespējas dēļ (šajā gadījumā divām trešdaļām komisāru ir jāpiekrīt atlaišanai) ([138]). *NHRC* komisāriem ir aizliegts vienlaikus ieņemt amatu Nacionālajā asamblejā, vietējās padomēs vai jebkurā valsts vai pašvaldības iestādē (kā valsts amatpersonai) ([139]).

NHRC var uzsākt izmeklēšanu pēc savas iniciatīvas vai pamatojoties uz personas lūgumrakstu. Izmeklēšanas ietvaros *NHRC* var pieprasīt iesniegt attiecīgus materiālus, veikt pārbaudes un uzaicināt personas liecināt ([140]). Pēc izmeklēšanas *NHRC* var sniegt ieteikumus, lai uzlabotu vai labotu konkrētu politiku un praksi, un var tos publiskot ([141]). Publiskajām iestādēm jāpaziņo *NHRC* par šādu ieteikumu īstenošanas plānu 90 dienu laikā pēc to saņemšanas ([142]). Turklāt, ja ieteikumi netiek īstenoti, attiecīgajai iestādei par to jāinformē Komisija ([143]). Savukārt *NHRC* var paziņot par šādu ieteikumu neīstenošanu Nacionālajai asamblejai un/vai to publiskot. Publiskās iestādes kopumā ievēro *NHRC* ieteikumus, un tām ir spēcīgs stimuls to darīt, jo šo ieteikumu īstenošana ir novērtēta vispārējā novērtējumā, ko veic Valdības politikas koordinācijas birojs premjerministra biroja pakļautībā.

2.4. **Individuāla tiesiskā aizsardzība**

2.4.1. *Tiesiskās aizsardzības mehānismi, kas pieejami saskaņā ar PIPA*

Personas saskaņā ar *PIPA* var izmantot savas piekļuves, labošanas, dzēšanas un apturēšanas tiesības attiecībā uz personas informāciju, ko apstrādā krimināltiesību aizsardzības iestādes. Piekļuvi var pieprasīt tieši no attiecīgās iestādes vai netieši ar *PIPC* starpniecību ([144]). Kompetentā iestāde var ierobežot vai liegt piekļuvi tikai tad, ja tas ir paredzēts tiesību aktos, ja tas varētu nodarīt kaitējumu trešās personas dzīvībai vai veselībai vai, iespējams, izraisīt nepamatotu citas personas īpašuma tiesību un citu interešu pārkāpumu (t. i., ja otras personas intereses būtu svarīgākas par tās personas interesēm, kura iesniedz pieprasījumu) ([145]). Ja piekļuves pieprasījums tiek noraidīts, persona jāinformē par norādījuma iemesliem un to, kā to pārsūdzēt ([146]). Tāpat pieprasījumu labot vai dzēst var noraidīt, ja tas ir paredzēts citos tiesību aktos, un šādā gadījumā persona ir jāinformē par noraidījuma iemesliem un iespēju to pārsūdzēt ([147]).

Attiecībā uz tiesisko aizsardzību personas var iesniegt sūdzību *PIPC*, tostarp ar Korejas Interneta un drošības aģentūras pārvaldītā privātuma jautājumu zvanu centra starpniecību ([148]). Turklāt persona var saņemt starpniecības pakalpojumu, vēršoties Personas informācijas strīdu starpniecības komitejā ([149]). Šie tiesiskās aizsardzības līdzekļi ir pieejami gan gadījumos, kad, iespējams, tiek pārkāpti noteikumi, kas ietverti konkrētos tiesību aktos, kuros noteikti ierobežojumi un garantijas attiecībā uz personas informācijas vākšanu (2.2. iedaļa), gan *PIPA*. Turklāt personas var apstrīdēt *PIPC* lēmumus vai bezdarbību saskaņā ar Administratīvo lietu iztiesāšanas likumu (sk. 2.4.3. iedaļu).

([137]) *NHRC* likuma 5. panta 5. punkts.
([138]) *NHRC* likuma 7. panta 1. punkts un 8. pants.
([139]) *NHRC* likuma 10. pants.
([140]) *NHRC* likuma 36. pants. Saskaņā ar likuma 36. panta 7. punktu materiālu vai priekšmetu iesniegšanu var noraidīt, ja tā kaitētu valsts konfidencialitātei, varētu būtiski ietekmēt valsts drošību vai diplomātiskās attiecības vai radītu nopietnus šķēršļus kriminālizmeklēšanai vai tiesas procesam. Šādos gadījumos Komisija var pieprasīt papildu informāciju no attiecīgās aģentūras vadītāja (kuram jārīkojas labticīgi), ja nepieciešams pārbaudīt, vai atteikums sniegt informāciju ir pamatots.
([141]) *NHRC* likuma 25. panta 1. punkts.
([142]) *NHRC* likuma 25. panta 3. punkts.
([143]) *NHRC* likuma 25. panta 4. punkts.
([144]) *PIPA* 35. panta 2. punkts
([145]) *PIPA* 35. panta 4. punkts
([146]) *PIPA* Izpildes dekrēta 42. panta 2. punkts.
([147]) *PIPA* 36. panta 1. un 2. punkts un *PIPA* Izpildes dekrēta 43. panta 3. punkts.
([148]) *PIPA* 62. pants.
([149]) *PIPA* 40.–50. pants un *PIPA* Izpildes dekrēta 48-2.–57. pants.

2.4.2. *Valsts cilvēktiesību komisijas nodrošinātā tiesiskā aizsardzība*

NHRC izskata personu (gan Korejas valstspiederīgo, gan ārvalstnieku) sūdzības par cilvēktiesību pārkāpumiem, ko pieļāvušas publiskās iestādes ([150]). Uz personām neattiecas atbilstības prasība kā nosacījums sūdzības iesniegšanai *NHRC* ([151]). Līdz ar to *NHRC* sūdzību izskatīs pat tad, ja attiecīgā persona pieņemamības posmā faktiski nevarēs pierādīt kaitējumu. Tādēļ, lai sūdzību varētu pieņemt *NHRC*, saistībā ar personas datu vākšanu krimināltiesību aizsardzības nolūkos personai nebūtu jāpierāda, ka Korejas publiskās iestādes faktiski ir piekļuvušas tās personas informācijai. Persona var arī lūgt atrisināt sūdzību, izmantojot starpniecību ([152]).

Lai izmeklētu sūdzību, *NHRC* var izmantot savas izmeklēšanas pilnvaras, tostarp pieprasot iesniegt attiecīgus materiālus, veicot pārbaudes un uzaicinot personas liecināt ([153]). Ja izmeklēšanā atklāj, ka ir noticis attiecīgo tiesību aktu pārkāpums, *NHRC* var ieteikt īstenot tiesiskās aizsardzības līdzekļus vai labot vai uzlabot attiecīgos statūtus, iestādi, politiku vai praksi ([154]). Ierosinātie tiesiskās aizsardzības līdzekļi var ietvert starpniecību, cilvēktiesību pārkāpuma izbeigšanu, kompensāciju par kaitējumu un pasākumus, kas paredzēti, lai novērstu tādu pašu vai līdzīgu pārkāpumu atkārtošanos ([155]). Gadījumā, ja saskaņā ar piemērojamiem noteikumiem personas informācija ir vākta pretlikumīgi, koriģējošie pasākumi var ietvert savāktās personas informācijas dzēšanu. Ja tiek uzskatīts, ka ir ļoti iespējams, ka pārkāpums turpinās, un tiek uzskatīts, ka, ja tas netiks koriģēts, radīsies grūti novēršams kaitējums, *NHRC* var pieņemt steidzamus pasākumus ([156]).

Lai gan *NHRC* nav pilnvaru izmantot piespiedu līdzekļus, tās lēmumus (piemēram, lēmumu neturpināt sūdzības izmeklēšanu) ([157]) un ieteikumus var apstrīdēt Korejas tiesās saskaņā ar Administratīvo lietu iztiesāšanas likumu (sk. 2.4.3. iedaļu turpmāk tekstā) ([158]). Turklāt, ja *NHRC* konstatējumi atklāj, ka publiskā iestāde ir nelikumīgi savākusi personas datus, persona varētu pieprasīt papildu tiesisko aizsardzību Korejas tiesās pret šo publisko iestādi, piemēram, apstrīdot datu vākšanu saskaņā ar Administratīvo lietu iztiesāšanas likumu, iesniedzot konstitucionālu sūdzību saskaņā ar Konstitucionālās tiesas likumu vai pieprasot kaitējuma kompensāciju saskaņā ar Valsts kompensāciju likumu (sk. 2.4.3. iedaļu turpmāk tekstā).

2.4.3. *Tiesiskā aizsardzība*

Personas var izmantot ierobežojumus un garantijas, kas aprakstīti iepriekšējās iedaļās, lai Korejas tiesās saņemtu tiesisko aizsardzību, izmantojot dažādas iespējas.

Pirmkārt, saskaņā ar *CPA* attiecīgā persona un tās padomdevējs var būt klāt brīdī, kad tiek izpildīts kratīšanas vai konfiskācijas orderis, un tādējādi var celt iebildumus rīkojuma izpildes brīdī ([159]). Turklāt *CPA* ir paredzēts tā dēvētais "kvazisūdzības" mehānisms, kas ļauj personām iesniegt prasību kompetentajā tiesā ar lūgumu atcelt vai grozīt prokurora vai policijas ierēdņa rīkojumu par konfiskāciju ([160]). Tas ļauj personām apstrīdēt pasākumus, kas veikti, lai izpildītu konfiskācijas orderi.

([150]) Lai gan *NHRC* likuma 4. pants attiecas uz Korejas Republikā dzīvojošiem pilsoņiem un ārvalstniekiem, termins "dzīvojošs" atspoguļo jurisdikcijas, nevis teritorijas jēdzienu. Tādējādi, ja valsts iestādes Korejā pārkāpj ārpus Korejas esoša ārvalstnieka pamattiesības, šī persona var iesniegt sūdzību *NHRC*. Sk., piemēram, attiecīgo jautājumu *NHRC* bieži uzdoto jautājumu lapā, kas pieejama tīmekļa vietnē https://www.humanrights.go.kr/site/program/board/basicboard/list?boardtypeid=7025&menuid=002004005001&pagesize=10&currentpage=2. Šāds gadījums būtu, ja Korejas publiskās iestādes nelikumīgi piekļūtu ārvalstnieka personas datiem, kas nosūtīti Korejai.

([151]) Sūdzība principā jāiesniedz viena gada laikā no pārkāpuma, tomēr *NHRC* joprojām var izlemt izmeklēt sūdzību, kas ir iesniegta pēc minētā termiņa, kamēr nav beidzies noilguma termiņš saskaņā ar krimināltiesībām vai civiltiesībām (*NHRC* likuma 32. panta 1. punkta 4. apakšpunkts).

([152]) *NHRC* likuma 42. un turpmākie panti.

([153]) *NHRC* likuma 36. un 37. pants.

([154]) *NHRC* likuma 44. pants.

([155]) *NHRC* likuma 42. panta 4. punkts.

([156]) *NHRC* likuma 48. pants.

([157]) Piemēram, ja *NHRC* izņēmuma kārtā nevar pārbaudīt konkrētus materiālus vai objektus, jo tie ir saistīti ar valsts noslēpumiem, kas var būtiski ietekmēt valsts drošību vai diplomātiskās attiecības, vai ja pārbaude radītu nopietnus šķēršļus krimināllizmeklēšanai vai tiesas procesam (sk. 166. zemsvītras piezīmi) un ja iepriekš minētais liedz *NHRC* veikt izmeklēšanu, kas vajadzīga, lai novērtētu saņemtā lūgumraksta pamatotību, tā informēs personu par sūdzības noraidīšanas iemesliem saskaņā ar *NHRC* likuma 39. pantu. Šajā gadījumā persona var apstrīdēt *NHRC* lēmumu saskaņā ar Administratīvo lietu iztiesāšanas likumu.

([158]) Sk., piem., Seulas Augstās tiesas 2008. gada 18. aprīļa Lēmumu Nr. 2007Nu27259, kas apstiprināts ar Augstākās tiesas 2008. gada 9. oktobra Lēmumu Nr. 2008Du7854; Seulas Augstās tiesas 2018. gada 2. februāra Lēmumu Nr. 2017Nu69382.

([159]) *CPA* 121. un 219. pants.

([160]) *CPA* 417. pants kopā ar CPA 414. panta 2. punktu. Sk. arī Augstākās tiesas 1997. gada 29. septembra Lēmumu Nr. 97Mo66.

Turklāt Korejas tiesās personas var iegūt kompensāciju par kaitējumu. Pamatojoties uz Valsts kompensāciju likumu, personas var pieprasīt kompensāciju par kaitējumu, ko nodarījušas valsts amatpersonas, savu oficiālo pienākumu izpildē pārkāpjot likumu ([161]). Prasību saskaņā ar Valsts kompensāciju likumu var iesniegt specializētajā "Kompensāciju padomē" vai tieši Korejas tiesās ([162]). Ja cietušais ir ārvalstnieks, piemēro Valsts kompensāciju likumu, ja vien šī pilsoņa izcelsmes valsts līdzvērtīgi nodrošina valsts kompensāciju Korejas valstspiederīgajiem ([163]). Saskaņā ar judikatūru šis nosacījums ir izpildīts, ja prasības attiecībā uz kompensācijas pieprasīšanu citā valstī "nav ievērojami nesamērīgas, salīdzinot Korejas un citas valsts praksi" un "nav kopumā stingrākas par Korejas noteiktajām prasībām, un starp tām nav materiālu un būtisku atšķirību" ([164]). Civillikumā ir reglamentētas valsts saistības attiecībā uz kompensāciju, un attiecīgi valsts saistības ietver arī nemateriālu kaitējumu (piemēram, garīgās ciešanas) ([165]).

Datu aizsardzības noteikumu pārkāpumu gadījumā saskaņā ar *PIPA* tiek nodrošināts papildu tiesiskās aizsardzības līdzeklis. Saskaņā ar *PIPA* 39. pantu ikviena persona, kurai nodarīts kaitējums *PIPA* pārkāpuma vai personas informācijas nozaudēšanas, zādzības, izpaušanas, viltošanas, pārveidošanas vai bojāšanas dēļ, tiesā var saņemt kompensāciju par kaitējumu. Nav līdzīgas prasības attiecībā uz savstarpīgumu kā saskaņā ar Valsts kompensāciju likumu.

Papildus kaitējuma kompensācijai saskaņā ar Administratīvo lietu iztiesāšanas likumu var saņemt administratīvus aizsardzības līdzekļus pret administratīvo aģentūru darbībām vai bezdarbību. Ikviena persona var apstrīdēt rīkojumu (t. i., valsts varas īstenošanu vai atteikšanos to īstenot konkrētā gadījumā) vai bezdarbību (administratīvās aģentūras ilgstoša atteikšanās pieņemt noteiktu rīkojumu, kas ir pretrunā ar juridisku pienākumu to darīt), no kā var izrietēt nelikumīgas darbības atcelšana/grozīšana, atzīšana par spēkā neesošu (t. i., konstatējums, ka rīkojumam nav juridisku spēka, vai konstatējums par tā neesību tiesību sistēmā) vai konstatējums, ka bezdarbība ir nelikumīga ([166]). Lai varētu apstrīdēt administratīvo rīkojumu, tam ir tieši jāietekmē civiltiesības un pienākumi ([167]). Tas ietver personas datu vākšanas pasākumus neatkarīgi no tā, vai tie ir tieši (piemēram, saziņas pārtveršana), vai izmantojot izpaušanas pieprasījumu (piemēram, pakalpojumu sniedzējam).

Iepriekš minētās prasības vispirms var iesniegt administratīvo pārsūdzību komisijās, kas izveidotas dažās publiskajās iestādēs (piemēram, *NIS, NHRC*), vai Centrālajā administratīvo pārsūdzību komisijā, kas izveidota Pretkorupcijas un civiltiesību komisijas pakļautībā ([168]). Šāda administratīva pārsūdzība ir alternatīvs un neformālāks veids, kā apstrīdēt publiskās iestādes rīkojumu vai bezdarbību. Tomēr prasību var iesniegt arī tieši Korejas tiesās saskaņā ar Administratīvo lietu iztiesāšanas likumu.

Pieprasījumu atsaukt/grozīt rīkojumu saskaņā ar Administratīvo lietu iztiesāšanas likumu var iesniegt jebkura persona, kurai ir tiesiska interese pieprasīt atcelšanu/grozījumu vai atjaunot tās tiesības ar atcelšanu/grozījumu, ja rīkojums vairs nav spēkā ([169]). Tiesvedību, kas, paredzēta, lai apstiprinātu spēkā neesamību, var ierosināt persona, kurai ir likumīgas intereses iegūt šādu apliecinājumu, savukārt tiesvedību, kas paredzēta, lai apstiprinātu bezdarbības nelikumību, var ierosināt jebkura persona, kura ir iesniegusi pieteikumu par rīkojuma izdošanu un kurai ir tiesiska interese prasīt, lai tiktu apstiprināta bezdarbības nelikumība ([170]). Saskaņā ar Augstākās tiesas judikatūru jēdziens "tiesiska interese" tiek interpretēts kā "juridiski aizsargāta interese", t. i., tieša un īpaša interese, kas aizsargāta ar likumiem un noteikumiem, uz kuriem tiek balstīti administratīvi rīkojumi (proti, tās nav vispārējas, netiešas un abstraktas sabiedrības intereses) ([171]). Tādēļ personām ir tiesiska interese gadījumā, ja tiek pārkāpti ierobežojumi un garantijas attiecībā uz personas datu vākšanu krimināltiesību aizsardzības nolūkos (saskaņā ar konkrētiem likumiem vai *PIPA*). Galīgais spriedums saskaņā ar Administratīvo lietu iztiesāšanas likumu ir saistošs pusēm ([172]).

Pieprasījums par rīkojuma atcelšanu/grozīšanu un pieprasījums apstiprināt bezdarbības nelikumību jāiesniedz 90 dienu laikā no dienas, kad persona uzzinājusi par rīkojumu, un principā ne vēlāk kā vienu gadu pēc rīkojuma

([161]) Valsts kompensāciju likuma 2. panta 1. punkts.
([162]) Valsts kompensāciju likuma 9. un 12. pants. Ar likumu izveidotas apgabala padomes (kuras vada attiecīgās prokuratūras prokurora vietnieks), Centrālā padome (kuru vada tieslietu ministra vietnieks) un Īpašā padome (ko vada valsts aizsardzības ministra vietnieks un kura atbild par kompensācijas pieprasījumiem par kaitējumu, ko nodarījušas militārpersonas vai militārpersonu civilie darbinieki). Kompensācijas pieprasījumus principā izskata apgabala padomes, kurām noteiktos apstākļos ir jānosūta lietas Centrālajai/Īpašajai padomei, piemēram, ja kompensācija pārsniedz noteiktu summu vai ja persona iesniedz pieteikumu atkārtotai izskatīšanai. Visās padomēs ir tieslietu ministra iecelti locekļi (piemēram, no Tieslietu ministrijas amatpersonām, tiesu amatpersonām, juristiem un personām, kurām ir speciālas zināšanas attiecībā uz valsts kompensāciju), un uz tām attiecas īpaši noteikumi par interešu konfliktu (sk. Valsts kompensāciju likuma Izpildes dekrēta 7. pantu).
([163]) Valsts kompensāciju likuma 7. pants.
([164]) Augstākās tiesas 2015. gada 11. jūnija Lēmums Nr. 2013Da208388.
([165]) Sk. Valsts kompensāciju likuma 8. pantu, kā arī Civillikuma 751. pantu.
([166]) Administratīvo lietu iztiesāšanas likuma 2. un 4. pants.
([167]) Augstākās tiesas 1999. gada 22. oktobra Lēmums Nr. 98Du18435, Augstākās tiesas 2000. gada 8. septembra Lēmums Nr. 99Du1113 un Augstākās tiesas 2012. gada 27. septembra Lēmums Nr. 2010Du3541.
([168]) Administratīvo pārsūdzību likuma 6. pants un Administratīvo lietu iztiesāšanas likuma 18. panta 1. punkts.
([169]) Administratīvo lietu iztiesāšanas likuma 12. pants.
([170]) Administratīvo lietu iztiesāšanas likuma 35. un 36. pants.
([171]) Augstākās tiesas 2006. gada 26. marta Lēmums Nr. 2006Du330.
([172]) Administratīvo lietu iztiesāšanas likuma 30. panta 1. punkts.

izdošanas/izlaišanas dienas, ja vien nav attaisnojošu iemeslu ([173]). Saskaņā ar Augstākās tiesas judikatūru jēdziens "attaisnojoši iemesli" ir jāinterpretē plaši, un ir jānovērtē, vai ir sociāli pieņemami pieļaut sūdzības novēlotu iesniegšanu, ņemot vērā visus lietas apstākļus ([174]). Piemēram, tas ietver (cita starpā) kavēšanās iemeslus, par kuriem attiecīgo pusi nevar saukt pie atbildības (t. i., situācijas, kas nav atkarīgas no sūdzības iesniedzēja, piemēram, ja viņam nav paziņots par viņa personas informācijas vākšanu) vai *force majeure* (piemēram, dabas katastrofa, karš).

Visbeidzot, personas var arī iesniegt konstitucionālu sūdzību Konstitucionālajā tiesā ([175]). Pamatojoties uz Konstitucionālās tiesas likumu, ikviena persona, kuras Konstitūcijā garantētās pamattiesības, tiek pārkāptas valsts varas īstenošanas vai neīstenošanas dēļ (izņemot tiesu spriedumus), var lūgt izskatīt konstitucionālu sūdzību. Ja ir pieejami citi tiesiskās aizsardzības līdzekļi, tie ir jāizmanto vispirms. Saskaņā ar Konstitucionālās tiesas judikatūru ārvalstnieki var iesniegt konstitucionālu sūdzību tiktāl, ciktāl viņu pamattiesības tiek atzītas saskaņā ar Korejas Konstitūciju (sk. skaidrojumus 1.1. iedaļā) ([176]). Konstitucionālas sūdzības jāiesniedz 90 dienu laikā pēc tam, kad persona ir uzzinājusi par pārkāpumu, un viena gada laikā pēc tā izdarīšanas. Ņemot vērā to, ka Administratīvo lietu iztiesāšanas likuma procedūru piemēro tiesvedībai saskaņā ar Konstitucionālās tiesas likumu ([177]), sūdzība joprojām būs pieņemama, ja būs "attaisnojoši iemesli", kā tas interpretēts saskaņā ar iepriekš aprakstīto Augstākās tiesas judikatūru.

Ja vispirms ir jāizmanto citi tiesiskās aizsardzības līdzekļi, konstitucionāla sūdzība jāiesniedz 30 dienu laikā pēc galīgā lēmuma par šādu tiesiskās aizsardzības līdzekli ([178]). Konstitucionālā tiesa var atzīt par spēkā neesošu tādas valsts varas īstenošanu, kas izraisījusi pārkāpumu, vai apstiprināt, ka noteikta bezdarbība ir pretrunā Konstitūcijai ([179]). Šajā gadījumā attiecīgajai iestādei ir jāveic pasākumi, lai izpildītu tiesas nolēmumu.

3. VALDĪBAS PIEKĻUVE VALSTS DROŠĪBAS NOLŪKOS

3.1. Kompetentās publiskās iestādes valsts drošības jomā

Korejas Republikā ir divas specializētas izlūkošanas aģentūras: *NIS* un Aizsardzības drošības atbalsta pavēlniecība. Arī policija un prokuratūra var vākt personas informāciju valsts drošības nolūkos.

NIS ir izveidots ar Likumu par Valsts izlūkdienestu (turpmāk "NIS likums"), un tas darbojas tiešā prezidenta pakļautībā un uzraudzībā ([180]). *NIS* jo īpaši vāc, apkopo un izplata informāciju par ārvalstīm (un Ziemeļkoreju) ([181]), izlūkdatus, kas saistīti ar uzdevumu apkarot spiegošanu (tostarp militāro un rūpniecisko spiegošanu), terorismu un starptautisko noziedzīgo sindikātu darbībām, izlūkdatus par noteiktu veidu noziegumu, kas vērsti pret sabiedrības un valsts drošību (piemēram, iekšzemes nemieri, ārvalstu agresija), un izlūkdatus saistībā ar uzdevumu nodrošināt kiberdrošību un nepieļaut vai apkarot kiberuzbrukumus un kiberdraudus ([182]). *NIS* likumā, ar ko izveidots *NIS* un noteikti tā uzdevumus, ir paredzēti arī vispārēji principi, kas reglamentē visas tā darbības. Vispārējs princips paredz, ka NIS ir jāsaglabā politiskā neitralitāte un jāaizsargā personu brīvība un tiesības ([183]). *NIS* priekšsēdētāja uzdevums ir izstrādāt vispārējas pamatnostādnes, kurās izklāstīti *NIS* pienākumu izpildes principi, darbības joma un procedūras attiecībā uz informācijas vākšanu un izmantošanu, un par tiem jāziņo Nacionālajai asamblejai ([184]). Nacionālā asambleja (ar Izlūkošanas komitejas starpniecību) var pieprasīt, lai pamatnostādnes tiktu labotas vai papildinātas, ja tā uzskata, ka tās ir nelikumīgas vai netaisnīgas. Vispārīgāk runājot, direktors un *NIS* personāls, veicot savus pienākumus, nedrīkst piespiest nevienu iestādi, organizāciju vai personu darīt ko tādu, ko tai nav pienākuma darīt, un traucēt personai īstenot savas tiesības, ļaunprātīgi izmantojot savas oficiālās pilnvaras ([185]). Turklāt jebkurai *NIS* veiktai pasta cenzūrai, telesakaru pārtveršanai, atrašanās

([173]) Administratīvo lietu iztiesāšanas likuma 20. pants. Šis termiņš attiecas arī uz prasību apstiprināt bezdarbības nelikumību, sk. Administratīvo lietu iztiesāšanas likuma 38. panta 2. punktu.
([174]) Augstākās tiesas 1991. gada 28. jūnija Lēmums Nr. 90Nu6521.
([175]) Konstitucionālās tiesas likuma 68. panta 1. punkts.
([176]) Konstitucionālās tiesas 2001. gada 29. novembra Lēmums Nr. 99HeonMa194.
([177]) Konstitucionālās tiesas likuma 40. pants.
([178]) Konstitucionālās tiesas likuma 69. pants.
([179]) Konstitucionālās tiesas likuma 75. panta 3. punkts.
([180]) *NIS* likuma 2. pants un 4. panta 2. punkts.
([181]) Šis jēdziens attiecas nevis uz informāciju par personām, bet gan uz vispārēju informāciju par ārvalstīm (tendences, norises) un trešo valstu valsts struktūru darbībām.
([182]) *NIS* likuma 3. panta 1. punkts.
([183]) 3. panta 1. punkts, 6. panta 2. punkts, 11., 21. pants Sk. arī noteikumus par interešu konfliktiem, jo īpaši 10. un 12. pantu.
([184]) *NIS* likuma 4. panta 2. punkts.
([185]) *NIS* likuma 13. pants.

vietas informācijas vākšanai, saziņas apstiprinājuma datu vākšanai vai privātās saziņas ierakstīšanai vai noklausīšanās gadījumam ir jāatbilst *CPPA*, Atrašanās vietas informācijas likumam vai *CPA* ([186]). Par jebkādu varas ļaunprātīgu izmantošanu vai informācijas vākšanu, pārkāpjot šos tiesību aktus, piemēro krimināsodus ([187]).

Aizsardzības drošības atbalsta pavēlniecība ir militāra izlūkošanas aģentūra, kas izveidota Aizsardzības ministrijas pakļautībā. Tā ir atbildīga par drošības jautājumiem militārajos spēkos, militāro kriminālizmeklēšanu (saskaņā ar Militārās tiesas likumu) un militāro izlūkošanu. Kopumā Aizsardzības drošības atbalsta pavēlniecība neveic civilpersonu novērošanu, ja vien tas nav nepieciešams militāro funkciju veikšanai. Personas, par kurām var veikt izmeklēšanu, ir militārpersonas, militārpersonu civilie darbinieki, militārajās mācībās iesaistītas personas, militārajās rezerves vienībās vai rekrutēšanas dienestā iesaistītas personas un karagūstekņi ([188]). Vācot saziņas datus valsts drošības nolūkos, Aizsardzības drošības atbalsta pavēlniecībai piemēro ierobežojumus un garantijas, kas noteikti *CPPA* un tā Izpildes dekrētā.

3.2. **Juridiskais pamats un ierobežojumi**

CPPA, Likums par terorisma apkarošanu iedzīvotāju un sabiedriskās drošības aizsardzības nolūkā (turpmāk "Terorisma apkarošanas likums") un *TBA* nodrošina juridisko pamatu personas informācijas vākšanai valsts drošības nolūkos un nosaka piemērojamos ierobežojumus un garantijas ([189]). Šie ierobežojumi un garantijas, kas aprakstīti nākamajās iedaļās, nodrošina, ka informācijas vākšana un apstrāde tiek veikta tikai tādā mērā, kādā tā ir absolūti nepieciešams leģitīma mērķa sasniegšanai. Ir izslēgta personas informācijas masveida un neselektīva vākšana valsts drošības nolūkos.

3.2.1. *Saziņas informācijas vākšana*

3.2.1.1. Izlūkošanas aģentūru veiktā saziņas informācijas vākšana

3.2.1.1.1. Juridiskais pamats

CPPA pilnvaro izlūkošanas aģentūras vākt saziņas datus un pieprasa, lai sakaru pakalpojumu nodrošinātāji sadarbotos šo aģentūru pieprasījumu izpildei ([190]). Kā aprakstīts 2.2.2.1. iedaļā, *CPPA* ir nošķirta saziņas satura vākšana (t. i., "saziņu ierobežojoši pasākumi", piemēram, "noklausīšanās" vai "cenzūras" ([191]) pasākumi) un "saziņas apstiprinājumu datu" vākšana ([192]).

Šo divu veidu informācijas vākšanas robežvērtības atšķiras, bet piemērojamās procedūras un garantijas lielā mērā ir identiskas ([193]). Saziņas apstiprinājuma datu (vai metadatu) vākšana var notikt, lai novērstu draudus valsts drošībai ([194]). Augstākas robežvērtības attiecas uz saziņu ierobežojošu pasākumu izpildi (t. i., lai vāktu saziņas saturu), ko var veikt tikai tad, ja ir gaidāms, ka valsts drošība tiks nopietni apdraudēta un izlūkdatu vākšana ir nepieciešama, lai novērstu šādas briesmas (t. i., ja pastāv nopietns risks valsts drošībai un vākšana ir nepieciešama, lai to novērstu) ([195]). Turklāt piekļuve saziņas saturam ir atļauta tikai kā galējais pasākums, lai nodrošinātu valsts drošību, un ir jāpieliek pūles, lai līdz minimumam samazinātu saziņas privātuma pārkāpumus ([196]). Pat tad, kad ir saņemts attiecīgs apstiprinājums/atļauja, šādi pasākumi ir nekavējoties jāpārtrauc, tiklīdz tie vairs nav vajadzīgi, tādējādi nodrošinot, ka jebkādi personas saziņas noslēpumu pārkāpumi tiek ierobežoti līdz minimumam ([197]).

3.2.1.1.2. Ierobežojumi un garantijas, ko piemēro tādas saziņas informācijas vākšanai, kurā iesaistīts vismaz viens Korejas valstspiederīgais

Saziņas informācijas (gan satura, gan metadatu) vākšana gadījumos, kad viena vai abas saziņā iesaistītās personas ir

([186]) *NIS* likuma 14. pants.
([187]) *NIS* likuma 22. un 23. pants.
([188]) Militārās tiesas likuma 1. pants.
([189]) Izmeklējot ar valsts drošību saistītus noziegumus, policija un *NIS* rīkosies, pamatojoties uz *CPA*, savukārt uz Aizsardzības drošības atbalsta pavēlniecību attiecas Militārās tiesas likums.
([190]) *CPPA* 15-2. pants.
([191]) *CPPA* 2. panta 6. un 7. punkts.
([192]) *CPPA* 2. panta 11. punkts.
([193]) Sk. arī *CPPA* 13-4. panta 2. punktu un *CPPA* Izpildes dekrēta 37. panta 4. punktu, kur ir noteikts, ka saziņas satura vākšanai piemērojamās procedūras *mutatis mutandis* attiecas uz saziņas apstiprinājuma datu vākšanu.
([194]) *CPPA* 13-4. pants.
([195]) *CPPA* 7. panta 1. punkts.
([196]) *CPPA* 3. panta 2. punkts.
([197]) *CPPA* Izpildes dekrēta 2. pants.

Korejas valstspiederīgās, var notikt tikai ar Augstās tiesas vecākā priekšsēdētāja atļauju ([198]). Izlūkošanas aģentūras pieprasījums rakstiski jāiesniedz prokuroram vai Augstākajai prokuratūrai ([199]). Tajā jānorāda vākšanas iemesli (t. i., ka paredzams nopietns valsts drošības apdraudējums vai ka vākšana ir vajadzīga, lai novērstu draudus valsts drošībai) un jāiekļauj materiāli, kas pamato šos iemeslus un izveido *prima facie* lietu, kā arī ziņas par pieprasījumu (t. i., mērķi, mērķpersona(-as), darbības joma, faktiskais vākšanas laikposms, kā arī tas, kā un kur notiks vākšana) ([200]). Savukārt prokurors / Augstākā prokuratūra lūdz atļauju Augstās tiesas vecākajam priekšsēdētājam ([201]). Priekšsēdētājs var piešķirt rakstisku atļauju tikai tad, ja viņš uzskata, ka pieteikums ir pamatots, un noraidīs pieprasījumu, ja uzskatīs to par nepamatotu ([202]). Orderī norāda vākšanas veidu, mērķi, mērķobjektu, darbības jomu un faktisko laikposmu, kā arī to, kur un kā tā var notikt ([203]).

Īpašus noteikumus piemēro, ja pasākuma mērķis ir izmeklēt sazvērestības aktu, kas apdraud valsts drošību, un pastāv ārkārtas situācija, kuras dēļ nav iespējams veikt iepriekš minētās procedūras ([204]). Ja šie nosacījumi ir izpildīti, izlūkošanas aģentūras var veikt novērošanas pasākumus bez iepriekšēja tiesas apstiprinājuma ([205]). Tomēr tūlīt pēc ārkārtas pasākumu izpildes izlūkošanas aģentūrai ir jālūdz tiesas atļauja. Ja atļauja nav saņemta 36 stundu laikā no pasākumu veikšanas brīža, tie nekavējoties jāpārtrauc ([206]). Informācijas vākšana ārkārtas situācijās vienmēr jāveic saskaņā ar "ārkārtas cenzūras / sarunu noklausīšanās paziņojumu", un izlūkošanas aģentūrai, kas veic vākšanu, ir jāreģistrē visi ārkārtas pasākumi ([207]).

Gadījumos, kad novērošana ir pabeigta īsā laikā, izslēdzot iespēju pieprasīt tiesas atļauju, kompetentās augstākās prokuratūras vadītājam ir jānosūta izlūkošanas aģentūras sagatavotais paziņojums par ārkārtas pasākumu kompetentās tiesas vadītājam, kurš saglabā ārkārtas pasākumu reģistru ([208]). Tas ļauj tiesai pārbaudīt vākšanas likumību.

3.2.1.1.3. Ierobežojumi un garantijas, ko piemēro tādas saziņas informācijas vākšanai, kurā iesaistītas tikai personas, kas nav Korejas valstspiederīgās

Lai vāktu informāciju par saziņu tikai starp personām, kas nav Korejas valstspiederīgās, izlūkošanas aģentūrām iepriekš jāsaņem rakstisks apstiprinājums no prezidenta ([209]). Šādas saziņas dati tiks vākti valsts drošības nolūkos tikai tad, ja tie ietilpst vienā no vairākām uzskaitītajām kategorijām, t. i., saziņa starp tādu valstu valdības amatpersonām vai citām personām, kas ir naidīgas pret Korejas Republiku, saziņa starp ārvalstu aģentūrām, grupām vai valstspiederīgajiem, kurus tur aizdomās par iesaistīšanos pret Koreju vērstās darbībās ([210]), vai starp Korejas pussalas grupu locekļiem, kas faktiski ir ārpus Korejas Republikas suverenitātes, un to jumta grupām, kas atrodas ārvalstīs ([211]). Savukārt, ja viena saziņas puse ir Korejas valstspiederīgais un otra – persona, kas nav Korejas valstspiederīgā, saskaņā ar 3.2.1.1.2. iedaļā aprakstīto procedūru ir vajadzīgs tiesas apstiprinājums.

Izlūkošanas aģentūras vadītājam ir jāiesniedz *NIS* direktoram plānoto pasākumu plāns ([212]). *NIS* direktors pārbauda, vai plāns ir piemērots, un, ja tas tā ir, iesniedz to apstiprināšanai prezidentam ([213]). Plānā iekļaujamā informācija ir tāda pati kā informācija, kas vajadzīga, lai iesniegtu pieteikumu tiesas atļaujai vākt informāciju par Korejas valstspiederīgajiem (kā aprakstīts iepriekš) ([214]). Jo īpaši tajā ir jānorāda vākšanas iemesli (t. i., ka paredzams nopietns valsts drošības apdraudējums vai ka vākšana ir vajadzīga, lai novērstu draudus valsts drošībai), galvenie aizdomu iemesli, kā arī jāiekļauj

([198]) *CPPA* 7. panta 1. punkta 1. apakšpunkts. Kompetentā tiesa ir augstā tiesa, kuras jurisdikcijā ir vienas vai abu pušu domicils vai mītnesvieta, uz kurām attiecas novērošana.
([199]) *CPPA* Izpildes dekrēta 7. panta 3. punkts.
([200]) *CPPA* 7. panta 3. punkts un 6. panta 4. punkts.
([201]) *CPPA* Izpildes dekrēta 7. panta 4. punkts. Prokurora pieprasījumā tiesai ir jānorāda galvenie aizdomu iemesli un, ja vienlaikus tiek pieprasītas vairākas atļaujas, to pamatojums (sk. *CPPA* Izpildes dekrēta 4. pantu).
([202]) *CPPA* 7. panta 3. punkts, 6. panta 5. punkts un 6. panta 9. punkts.
([203]) *CPPA* 7. panta 3. punkts un 6. panta 6. punkts.
([204]) *CPPA* 8. pants.
([205]) *CPPA* 8. panta 1. punkts.
([206]) *CPPA* 8. panta 2. punkts.
([207]) *CPPA* 8. panta 4. punkts. Sk. 2.2.2.2. iedaļu iepriekš tekstā par ārkārtas pasākumiem tiesībaizsardzības kontekstā.
([208]) *CPPA* 8. panta 5. un 7. punkts. Šajā paziņojumā jānorāda mērķis, mērķobjekts, darbības joma, laikposms, izpildes vieta un novērošanas metode, kā arī iemesli pieprasījuma neiesniegšanai pirms pasākuma veikšanas (*CPPA* 8. panta 6. punkts).
([209]) *CPPA* 7. panta 1. punkta 2. apakšpunkts.
([210]) Tas attiecas uz darbībām, kas apdraud valsts pastāvēšanu un drošību, demokrātisko kārtību vai cilvēku izdzīvošanu un brīvību.
([211]) Turklāt, ja viena puse ir persona, kas aprakstīta *CPPA* 7. panta 1. punkta 2. apakšpunktā, bet otra puse nav zināma vai to nevar precizēt, piemēro 7. panta 1. punkta 2. apakšpunktā noteikto procedūru.
([212]) *CPPA* Izpildes dekrēta 8. panta 1. punkts. *NIS* direktoru ieceļ prezidents pēc tam, kad to ir apstiprinājis Parlaments (*NIS* likuma 7. pants).
([213]) *CPPA* Izpildes dekrēta 8. panta 2. punkts.
([214]) *CPPA* Izpildes dekrēta 8. panta 3. punkts kopā ar *CPPA* 6. panta 4. punktu.

materiāli, kas pamato šos iemeslus un izveido *prima facie* lietu, kā arī ziņas par pieprasījumu (t. i., mērķi, mērķpersona (-as), darbības joma, faktiskais vākšanas laikposms, kā arī tas, kā un kur notiks vākšana). Ja vienlaikus tiek pieprasītas vairākas atļaujas, jānorāda to mērķis un pamatojums ([215]).

Ārkārtas situācijās ([216]) ir jāsaņem iepriekšēja atļauja no ministra, kura pakļautībā ir attiecīgā izlūkošanas aģentūra. Tomēr šajā gadījumā izlūkošanas aģentūrai ir jālūdz prezidenta piekrišana tūlīt pēc ārkārtas pasākumu veikšanas. Ja izlūkošanas aģentūra 36 stundu laikā pēc pieteikuma iesniegšanas nesaņem apstiprinājumu, vākšana nekavējoties jāpārtrauc ([217]). Šādos gadījumos savāktā informācija vienmēr tiks iznīcināta.

3.2.1.1.4. Vispārīgi ierobežojumi un garantijas

Pieprasot privātu vienību sadarbību, izlūkošanas aģentūrām tām ir jāsniedz tiesas orderis / prezidenta atļauja vai ārkārtas cenzūras paziņojuma vāka kopija, kas vienībai kura ir spiesta sadarboties, ir jāglabā tās dokumentos ([218]). Vienības, kurām pieprasīts izpaust informāciju izlūkošanas aģentūrām, pamatojoties uz *CPPA*, var atteikties to darīt, ja pilnvarojums vai ārkārtas cenzūras paziņojums attiecas uz nepareizu identifikatoru (piemēram, tālruņa numurs, kas pieder citai personai, nevis identificētajai personai). Turklāt visos gadījumos saziņai izmantotās paroles nedrīkst izpaust ([219]).

Izlūkošanas aģentūras var uzticēt saziņu ierobežojošu pasākumu īstenošanu vai saziņas apstiprinājuma informācijas vākšanu pasta nodaļai vai telesakaru pakalpojumu sniedzējam (kā noteikts Telesakaru darījumdarbības likumā) ([220]). Gan attiecīgajai izlūkošanas aģentūrai, gan pakalpojumu sniedzējam, kas saņem sadarbības pieprasījumu, trīs gadus jāglabā reģistri, kuros norādīts pasākumu pieprasīšanas mērķis, izpildes vai sadarbības datums un pasākumu priekšmets (piemēram, pasts, tālrunis, e-pasts) ([221]). Telesakaru pakalpojumu sniedzējiem, kas sniedz saziņas apstiprinājuma datus, informācija par datu vākšanas biežumu savās datnēs jāglabā septiņus gadus un divreiz gadā jāziņo zinātnes un IKT ministram ([222]).

Izlūkošanas aģentūrām ir jāziņo *NIS* direktoram par apkopoto informāciju un novērošanas rezultātiem ([223]). Attiecībā uz saziņas apstiprinājuma datu vākšanu ir jāveic uzskaite par to, ka ir iesniegts šādu datu pieprasījums, kā arī par pašu rakstisko pieprasījumu un iestādi, kas to ir izmantojusi ([224]).

Gan saziņas satura, gan saziņas apstiprinājuma datu vākšana var ilgt ne ilgāk kā četrus mēnešus, un, ja tajā laikā tiek sasniegts izvirzītais mērķis, tā nekavējoties jāpārtrauc ([225]). Ja atļaujas piešķiršanas nosacījumi joprojām ir spēkā, laikposmu ar tiesas atļauju vai ar priekšsēdētāja piekrišanu var pagarināt uz laiku, kas nepārsniedz četrus mēnešus. Pieteikums, lai saņemtu apstiprinājumu novērošanas pasākumu pagarināšanai, jāiesniedz rakstiski, norādot iemeslus, kāpēc tiek pieprasīts pagarinājums, un sniedzot apliecinošus materiālus ([226]).

Atkarībā no vākšanas juridiskā pamata personas parasti tiek informētas, ja tiek vākta viņu saziņa. Konkrētāk, neatkarīgi no tā, vai savāktā informācija attiecas uz saziņas saturu vai saziņas apstiprinājuma datiem, un neatkarīgi no tā, vai informācija ir iegūta parastajā procedūrā vai ārkārtas situācijā, izlūkošanas aģentūras vadītājam 30 dienu laikā no dienas, kad pabeigta novērošana, rakstiski jāpaziņo attiecīgajai personai par novērošanas pasākumu ([227]). Paziņojumā

([215]) *CPPA* Izpildes dekrēta 8. panta 3. punkts un 4. pants.
([216]) Proti, gadījumos, kad pasākuma mērķis ir sazvērestība, kas apdraud valsts drošību, nav pietiekami daudz laika saņemt prezidenta apstiprinājumu un ārkārtas pasākumu nepieņemšana var kaitēt valsts drošībai (CPPA 8. panta 8. punkts).
([217]) *CPPA* 8. panta 9. punkts.
([218]) *CPPA* 9. panta 2. punkts un *CPPA* Izpildes dekrēta 12. pants.
([219]) *CPPA* 9. panta 4. punkts.
([220]) *CPPA* Izpildes dekrēta 13. pants.
([221]) *CPPA* 9. panta 3. punkts un *CPPA* Izpildes dekrēta 17. panta 2. punkts. Šis laikposms neattiecas uz saziņas apstiprinājuma datiem (sk. *CPPA* Izpildes dekrēta 39. pantu).
([222]) *CPPA* 13. panta 7. punkts un *CPPA* Izpildes dekrēta 39. pants.
([223]) *CPPA* Izpildes dekrēta 18. panta 3. punkts.
([224]) *CPPA* 13. panta 5. punkts un 13-4. panta 3. punkts.
([225]) *CPPA* 7. panta 2. punkts.
([226]) *CPPA* 7. panta 2. punkts un *CPPA* Izpildes dekrēta 5. pants.
([227]) *CPPA* 9-2. panta 3. punkts. Saskaņā ar *CPPA* 13-4. pantu tas attiecas gan uz saziņas satura, gan uz saziņas apstiprinājuma datu vākšanu.

jāietver: 1) fakts, ka informācija ir vākta, 2) izpildaģentūra un 3) izpildes laikposms. Tomēr, ja ir iespējams, ka paziņojums apdraudētu valsts drošību vai kaitētu cilvēku dzīvībai un fiziskajai drošībai, paziņojumu var atlikt ([228]). Tiklīdz atlikšanas iemesli vairs nepastāv, paziņojums jāsniedz 30 dienu laikā ([229]).

Tomēr šī paziņošanas prasība attiecas tikai uz informācijas vākšanu, ja vismaz viena no pusēm ir Korejas valstspiederīgā. Tādējādi personas, kas nav Korejas valstspiederīgās, tiks informētas tikai tad, kad tiks vākti dati, kas attiecas uz viņu saziņu ar Korejas valstspiederīgajiem. Tādēļ paziņošanas prasība nepastāv, ja tiek vākta saziņa tikai starp personām, kas nav Korejas valstspiederīgās.

Jebkuras saziņas saturu, kā arī saziņas apstiprinājuma datus, kas iegūti, veicot novērošanu, pamatojoties uz *CPPA*, var izmantot tikai 1) noteiktu noziegumu izmeklēšanai, novēršanai vai kriminālvajāšanai par tiem, 2) disciplinārai tiesvedībai, 3) tiesvedībai, ja ar saziņu saistītā puse izmanto šos datus prasībā par kaitējuma atlīdzināšanu, vai 4) pamatojoties uz citiem tiesību aktiem ([230]).

3.2.1.2. Policijas/prokuroru veiktā saziņas informācijas vākšana valsts drošības nolūkos

Policija/prokurors var vākt saziņas datus (gan saziņas saturu, gan saziņas apstiprinājuma datus) valsts drošības nolūkos saskaņā ar tādiem pašiem nosacījumiem, kā aprakstīts 3.2.1.1. iedaļā. Rīkojoties ārkārtas situācijās ([231]), piemērojamā procedūra ir tā, kas tika aprakstīta iepriekš attiecībā uz saziņas satura vākšanu tiesībaizsardzības nolūkos ārkārtas situācijās (t. i., *CPPA* 8. pants).

3.2.2. *Informācijas vākšana par personām, kas tiek turētas aizdomās par terorismu*

3.2.2.1. Juridiskais pamats

Terorisma apkarošanas likums pilnvaro *NIS* direktoru vākt informāciju par personām, kas tiek turētas aizdomās par terorismu ([232]). "Persona, kas tiek turēta aizdomās par terorismu" ir teroristu grupas ([233]) dalībniece, persona, kas ir popularizējusi teroristu grupu (veicinot un izplatot teroristu grupas idejas vai taktiku), piesaistījusi līdzekļus terorismam vai ieguldījusi līdzekļus terorisma īstenošanai ([234]) vai iesaistīta citās terorisma sagatavošanas, konspirācijas, propagandas vai kūdīšanas darbībās, vai persona, kuru ir pamats turēt aizdomās par šādu darbību veikšanu ([235]). Parasti ikvienai valsts amatpersonai, kas īsteno Terorisma apkarošanas likumu, ir jāievēro Korejas Konstitūcijā paredzētās pamattiesības ([236]).

Terorisma apkarošanas likumā kā tādā nav noteiktas īpašas pilnvaras, ierobežojumi un garantijas attiecībā uz informācijas vākšanu par personām, kas tiek turētas aizdomās par terorismu, bet ir atsauce uz procedūrām citos likumos. Pirmkārt, pamatojoties uz Terorisma apkarošanas likumu, *NIS* direktors var vākt 1) informāciju par iebraukšanu Korejas Republikā un izbraukšanu no tās, 2) informāciju par finanšu darījumiem un 3) informāciju par saziņu. Atkarībā no pieprasītās informācijas veida attiecīgās procesuālās prasības ir noteiktas attiecīgi Imigrācijas likumā un Muitas likumā, *ARUSFTI* vai *CPPA* ([237]). Lai vāktu informāciju par iebraukšanu Korejā un izbraukšanu no tās, Terorisma apkarošanas likumā sniegta atsauce uz procedūrām, kas izklāstītas Imigrācijas likumā un Muitas likumā. Tomēr pašlaik šajos likumos

([228]) *CPPA* 9-2. panta 4. punkts.
([229]) *CPPA* 13-4. panta 2. punkts un 9-2. panta 6. punkts.
([230]) *CPPA* 5. panta 1. un 2. punkts, 12. un 13-5. pants.
([231]) Tas ir, ja pasākuma mērķis ir sazvērestība, kas apdraud valsts drošību, un pastāv ārkārtas situācija, kas liedz īstenot parasto apstiprināšanas procedūru (*CPPA* 8. panta 1. punkts).
([232]) Terorisma apkarošanas likuma 9. pants.
([233]) "Teroristu grupa" ir teroristu grupa, ko Apvienoto Nāciju Organizācija iekļāvusi sarakstā (Terorisma apkarošanas likuma 2. panta 2. punkts).
([234]) "Terorisms" ir definēts Terorisma apkarošanas likuma 2. panta 1. punktā kā rīcība, ko veic, lai traucētu īstenot valsts, pašvaldības vai ārvalstu valdības (tostarp pašvaldību un starptautisku organizāciju) pilnvaras vai lai liktu tai veikt jebkādu darbību, kas tai nav obligāta, vai sabiedrības apdraudēšana. Tas ietver a) personas nogalināšanu vai risku personas dzīvībai, nodarot miesas bojājumus, vai personas aizturēšanu, ieslodzīšanu, nolaupīšanu vai tās sagrābšanu par ķīlnieku; b) noteikta veida uzvedību, kas vērsta pret gaisa kuģi (piemēram, gaisa kuģa katastrofas izraisīšanu, nolaupīšanu vai gaisa kuģa bojāšanu lidojumā); c) noteikta veida uzvedību, kas saistīta ar kuģi (piemēram, ekspluatācijā esoša kuģa vai jūras struktūras sagrābšanu, ekspluatācijā esoša kuģa vai jūras struktūras iznīcināšanu vai tās bojājumu radīšanu, kas apdraud tās drošību, tostarp ekspluatācijā esošā kuģī vai jūras struktūrā ielādētas kravas bojājumu radīšanu); d) bioķīmiska, sprādzienbīstama vai aizdedzinoša ieroča vai ierīces novietošanu, detonēšanu vai izmantošanu jebkādā citā veidā ar nolūku izraisīt nāvi, smagus ievainojumus vai nopietnus materiālus bojājumus vai radīt šādu ietekmi uz noteikta veida transportlīdzekļiem vai iekārtām (piemēram, vilcieni, tramvaji, mehāniskie transportlīdzekļi, publiskie parki un stacijas, iekārtas elektrības, gāzes un telesakaru nodrošināšanai u. c.); e) noteikta veida darbības, kas saistītas ar kodolmateriāliem, radioaktīviem materiāliem vai kodoliekārtām (piemēram, kaitē cilvēku dzīvībai, veselībai vai īpašumam vai citādi traucē sabiedrisko drošību, iznīcinot kodolreaktoru vai neatbilstoši izmantojot radioaktīvos materiālus utt.).
([235]) Terorisma apkarošanas likuma 2. panta 3. punkts.
([236]) Terorisma apkarošanas likuma 3. panta 3. punkts.
([237]) Terorisma apkarošanas likuma 9. panta 1. punkts.

šādas pilnvaras nav paredzētas. Attiecībā uz saziņas informācijas un finanšu darījumu informācijas vākšanu Terorisma apkarošanas likumā ir minēti ierobežojumi un garantijas, kas minētas *CPPA* (un sīkāk izklāstītas turpmāk tekstā), un *ARUSFTI* (kuras, kā jau izklāstīts 2.1. iedaļā, nav būtiskas lēmuma par aizsardzības līmeņa pietiekamību nolūkiem).

Turklāt Terorisma apkarošanas likuma 9. panta 3. punktā ir noteikts, ka *NIS* direktors personas informāciju vai atrašanās vietas informāciju par personu, kas tiek turēta aizdomās par terorismu, var pieprasīt no personas informācijas pārziņa ([238]) vai atrašanās vietas informācijas sniedzēja ([239]). Šī iespēja attiecas tikai uz brīvprātīgas izpaušanas pieprasījumiem, uz kuriem personas informācijas pārziņiem un atrašanās vietas informācijas sniedzējiem nav pienākuma atbildēt, un jebkurā gadījumā atbildi var sniegt tikai saskaņā ar *PIPA* un Atrašanās vietas informācijas likumu (sk. 3.2.2.2. iedaļu).

3.2.2.2. Ierobežojumi un garantijas, ko piemēro brīvprātīgai informācijas atklāšanai saskaņā ar *PIPA* un Atrašanās vietas informācijas likumu

Brīvprātīgas sadarbības pieprasījumiem saskaņā ar Terorisma apkarošanas likumu jāattiecas tikai uz informāciju par personām, kas tiek turētas aizdomās par terorismu (sk. 3.2.2.1. iedaļu iepriekš). Jebkuram šādam *NIS* pieprasījumam jāatbilst likumīguma, nepieciešamības un samērīguma principiem, kas izriet no Korejas Konstitūcijas (12. panta 1. punkts un 37. panta 2. punkts) ([240]), kā arī *PIPA* prasībām attiecībā uz personas informācijas vākšanu (*PIPA* 3. panta 1. punkts, sk. 1.2. iedaļu). Turklāt *NIS* likumā ir noteikts, ka *NIS* nedrīkst piespiest nevienu iestādi, organizāciju vai fizisko personu darīt neko tādu, kas nav to pienākums, un nevienai personai traucēt īstenot tās tiesības, ļaunprātīgi izmantojot savas oficiālās pilnvara ([241]). Par šā aizlieguma pārkāpumu var piemērot krimināsodus ([242]).

Personas informācijas pārziņiem un atrašanās vietas informācijas sniedzējiem, kas saņem pieprasījumus no *NIS*, pamatojoties uz Terorisma apkarošanas likumu, nav pienākuma izpildīt šos pieprasījumus. Tie var izpildīt tos brīvprātīgi, bet tiem ir atļauts to darīt tikai saskaņā ar *PIPA* un Atrašanās vietas informācijas likumu. Attiecībā uz atbilstību *PIPA* pārzinim jo īpaši ir jāņem vērā datu subjekta intereses, un tas nedrīkst izpaust informāciju, ja tas varētu negodīgi aizskart personas vai trešās personas intereses ([243]). Turklāt saskaņā ar Paziņojumu Nr. 2021-1 par papildu procesuālajiem noteikumiem Likuma par personas informācijas aizsardzību interpretācijai un piemērošanai attiecīgā persona ir jāinformē par informācijas izpaušanu. Izņēmuma gadījumos šādu paziņošanu var atlikt, jo īpaši, ja un kamēr paziņošana apdraudētu noziedzīgu nodarījumu izmeklēšanu vai varētu kaitēt citas personas dzīvībai vai veselībai, ja minētās tiesības vai intereses nepārprotami prevalē pār datu subjekta tiesībām ([244]).

3.2.2.3. Ierobežojumi un garantijas saskaņā ar *CPPA*

Pamatojoties uz Terorisma apkarošanas likumu, izlūkošanas aģentūras var vākt saziņas informāciju (gan saziņas saturu, gan saziņas apstiprinājuma datus) tikai tad, ja tas nepieciešams terorisma apkarošanas darbībām, t. i., darbībām, kas saistītas ar terorisma novēršanu un pretpasākumiem. *CPPA* procedūras, kas aprakstītas 3.2.1. iedaļā, attiecas uz saziņas informācijas vākšanu terorisma novēršanas nolūkā.

3.2.3. *Telesakaru uzņēmumu brīvprātīga informācijas izpaušana*

Pamatojoties uz *TBA*, telesakaru uzņēmumi var izpildīt pieprasījumu izpaust "saziņas datus", kas saņemti no izlūkošanas aģentūras, kura plāno vākt informāciju, lai novērstu draudus valsts drošībai ([245]). Jebkuram šādam pieprasījumam jāatbilst likumīguma, nepieciešamības un samērīguma principiem, kas izriet no Korejas Konstitūcijas (12. panta 1. punkts un 37. panta 2. punkts) ([246]), kā arī *PIPA* prasībām attiecībā uz personas informācijas vākšanu (*PIPA* 3. panta 1. punkts, sk. 1.2. iedaļu iepriekš tekstā). Turklāt piemēro tos pašus ierobežojumus un garantijas, ko piemēro attiecībā uz brīvprātīgu informācijas izpaušanu tiesībaizsardzības nolūkos (sk. 2.2.3. iedaļu) ([247]).

([238]) Kā definēts *PIPA* 2. pantā, t. i., publiska iestāde, juridiska persona, organizācija, fiziska persona utt., kas tieši vai netieši apstrādā personas informāciju, lai uzturētu personas informācijas datnes oficiālos vai darījumdarbības nolūkos.

([239]) Kā definēts 5. pantā Likumā par atrašanās vietas informācijas aizsardzību, izmantošanu utt. (turpmāk "Atrašanās vietas informācijas likums"), t. i., ikviens, kas saņēmis Korejas Komunikācijas komisijas atļauju iesaistīties atrašanās vietas informācijas darījumdarbībā.

([240]) Sk. arī Terorisma apkarošanas likuma 3. panta 2. un 3. punktu.

([241]) *NIS* likuma 11. panta 1. punkts.

([242]) *NIS* likuma 19. pants.

([243]) *PIPA* 18. panta 2. punkts

([244]) *PIPC* Paziņojums Nr. 2021-1 par papildu procesuālajiem noteikumiem Likuma par personas informācijas aizsardzību interpretācijai un piemērošanai, III iedaļas 2. punkta iii) apakšpunkts.

([245]) *TBA* 83. panta 3. punkts.

([246]) Sk. arī Terorisma apkarošanas likuma 3. panta 2. un 3. punktu.

([247]) Jo īpaši pieprasījumam ir jābūt rakstiskam, un tajā jānorāda pieprasījuma iemesli, kā arī saite uz attiecīgo lietotāju un pieprasītās informācijas apjoms, un telesakaru pakalpojumu sniedzējam ir jāveic uzskaite un divreiz gadā jāziņo zinātnes un IKT ministram.

Telesakaru uzņēmumiem nav pienākuma izpildīt pieprasījumu, bet tie var to darīt brīvprātīgi un tikai saskaņā ar *PIPA*. Šajā sakarā tie paši pienākumi, tai skaitā attiecībā uz personas informēšanu, attiecas uz telesakaru uzņēmumiem, kad tie saņem pieprasījumus no krimināltiesību aizsardzības iestādēm, kā sīkāk paskaidrots 2.2.3. iedaļā.

3.3. **Pārraudzība**

Korejas izlūkošanas aģentūru darbību pārrauga dažādas struktūras. Aizsardzības drošības atbalsta pavēlniecības uzraudzību veic Valsts aizsardzības ministrija saskaņā ar ministrijas Direktīvu par iekšējās revīzijas īstenošanu. *NIS* uzrauga izpildvara, Nacionālā asambleja un citas neatkarīgas struktūras, kā sīkāk paskaidrots turpmāk.

3.3.1. *Cilvēktiesību aizsardzības uzraugs*

Ja izlūkošanas aģentūras vāc informāciju par personām, kas tiek turētas aizdomās par terorismu, Terorisma apkarošanas likums paredz pārraudzību, ko veic Terorisma apkarošanas komisija un cilvēktiesību aizsardzības uzraugs (turpmāk "HRPO") ([248]).

Terorisma apkarošanas komisija cita starpā izstrādā politiku attiecībā uz terorisma apkarošanas darbībām un pārrauga terorisma apkarošanas pasākumu īstenošanu, kā arī dažādu kompetento iestāžu darbības terorisma apkarošanas jomā ([249]). Komisiju vada premjerministrs, un tās sastāvā ir vairāki ministri un valsts aģentūru vadītāji, tostarp ārlietu ministrs, tieslietu ministrs, valsts aizsardzības ministrs, iekšlietu un drošības ministrs, *NIS* direktors, Valsts policijas aģentūras ģenerālkomisārs un Finanšu pakalpojumu komisijas priekšsēdētājs ([250]). Veicot izmeklēšanu terorisma apkarošanas jomā un izsekojot personas, kas tiek turētas aizdomās par terorismu, lai vāktu informāciju vai materiālus, kas vajadzīgi terorisma apkarošanas darbībām, NIS direktoram ir jāziņo Terorisma apkarošanas komisijas priekšsēdētājam (t. i., premjerministram) ([251]).

Turklāt ar Terorisma apkarošanas likumu izveidots *HRPO* amats, lai aizsargātu personu pamattiesības pret pārkāpumiem, ko izraisījušas terorisma apkarošanas darbības ([252]). *HRPO* ieceļ Terorisma apkarošanas komisijas priekšsēdētājs no to personu vidus, kuras atbilst Terorisma apkarošanas likuma Izpildes dekrētā uzskaitītajām kvalifikācijām (t. i., jebkura persona, kurai ir advokāta kvalifikācija, ar vismaz desmit gadu darba pieredzi vai ar speciālām zināšanām cilvēktiesību jomā, un kura vismaz desmit gadus ir strādājusi (vismaz) kā asociētais profesors vai ir strādājusi kā augsta amatpersona valsts aģentūrās vai pašvaldībās, vai ar vismaz desmit gadu pieredzi cilvēktiesību jomā, piemēram, nevalstiskajā organizācijā) ([253]). *HRPO* ieceļ uz diviem gadiem (ar iespēju pagarināt pilnvaru termiņu), un to var atcelt no amata tikai konkrētu, ierobežotu pamatojumu un pamatota iemesla dēļ, piemēram, ja tas ir apsūdzēts krimināllietā saistībā ar tā pienākumiem, ja tas ir izpaudis konfidenciālu informāciju vai ilgstošas garīgas vai fiziskas darbnespējas dēļ ([254]).

Attiecībā uz pilnvarām *HRPO* var sniegt ieteikumus, lai uzlabotu cilvēktiesību aizsardzību, ko veic terorisma apkarošanas darbībās iesaistītās aģentūras, un izskatīt civilus lūgumrakstus (sk. 3.4.3. iedaļu) ([255]). Ja var pamatoti konstatēt cilvēktiesību pārkāpumu oficiālo pienākumu izpildē, *HRPO* var ieteikt atbildīgās aģentūras vadītājam novērst šādu pārkāpumu ([256]). Savukārt atbildīgajai aģentūrai ir jāinformē *HRPO* par darbībām, kas veiktas, lai īstenotu šādu ieteikumu ([257]). Ja aģentūra neīstenotu *HRPO* ieteikumu, šis jautājums tiktu nodots izskatīšanai komisijai, tostarp tās priekšsēdētājam, proti, premjerministram. Līdz šim nav bijuši gadījumi, kad *HRPO* ieteikumi nav īstenoti.

3.3.2. *Nacionālā asambleja*

Kā aprakstīts 2.3.2. iedaļā, Nacionālā asambleja var izmeklēt un pārbaudīt publiskās iestādes un šajā sakarā pieprasīt dokumentu publiskošanu un izsaukt lieciniekus. Attiecībā uz jautājumiem, kas ir *NIS* jurisdikcijā, šo parlamentāro pārraudzību veic Nacionālās asamblejas Izlūkošanas komiteja ([258]). *NIS* direktors, kas pārrauga aģentūras pienākumu

([248]) Terorisma apkarošanas likuma 7. pants.
([249]) Terorisma apkarošanas likuma 5. panta 3. punkts.
([250]) Terorisma apkarošanas likuma Izpildes dekrēta 3. panta 1. punkts.
([251]) Terorisma apkarošanas likuma 9. panta 4. punkts.
([252]) Terorisma apkarošanas likuma 7. pants.
([253]) Terorisma apkarošanas likuma Izpildes dekrēta 7. panta 1. punkts.
([254]) Terorisma apkarošanas likuma Izpildes dekrēta 7. panta 3. punkts.
([255]) Terorisma apkarošanas likuma Izpildes dekrēta 8. panta 1. punkts.
([256]) Terorisma apkarošanas likuma Izpildes dekrēta 9. panta 1. punkts. *HRPO* autonomi lemj par ieteikumu pieņemšanu, bet par šādiem ieteikumiem ir jāziņo Terorisma apkarošanas komisijas priekšsēdētājam.
([257]) Terorisma apkarošanas likuma Izpildes dekrēta 9. panta 2. punkts.
([258]) Likuma par Nacionālo asambleju 36. pants un 37. panta 1. punkta 16. apakšpunkts.

izpildi, ziņo Izlūkošanas komitejai (kā arī prezidentam) ([259]). Pati Izlūkošanas komiteja var arī pieprasīt ziņojumu par konkrētu jautājumu, uz kuru *NIS* direktoram ir jāatbild nekavējoties ([260]). Viņš var atteikties sniegt atbildi vai liecināt Izlūkošanas komitejai tikai attiecībā uz valsts noslēpumiem, kas saistīti ar militāriem, diplomātiskiem vai Ziemeļkorejas jautājumiem, ja sabiedrības informētība var nopietni ietekmēt valsts likteni ([261]). Šādā gadījumā Izlūkošanas komiteja var pieprasīt paskaidrojumu no premjerministra. Ja šādu paskaidrojumu neiesniedz septiņu dienu laikā pēc pieprasījuma iesniegšanas, atbildi vai liecību vairs nevar noraidīt.

Ja Nacionālā asambleja konstatē nelikumīgas vai nepareizas darbības, tā var pieprasīt, lai attiecīgā publiskā iestāde veic korektīvus pasākumus, tostarp piešķir kompensāciju, veic disciplinārus pasākumus un uzlabo savas iekšējās procedūras ([262]). Pēc šāda pieprasījuma iestādei jārīkojas nekavējoties un par rezultātiem jāziņo Nacionālajai asamblejai. Pastāv īpaši noteikumi par parlamentāro pārraudzību attiecībā uz saziņu ierobežojošu pasākumu izmantošanu (t. i., saziņas satura vākšanu) saskaņā ar *CCPA* ([263]). Attiecībā uz pēdējo minēto Nacionālā asambleja var lūgt izlūkošanas aģentūru vadītājus sniegt ziņojumu par jebkādiem īpašiem saziņu ierobežojošiem pasākumiem. Turklāt tā var veikt kabeļu noklausīšanās iekārtu pārbaudes uz vietas. Visbeidzot, izlūkošanas aģentūrām, kas vākušas informāciju, un operatoriem, kas ir izpauduši satura informāciju valsts drošības nolūkos, pēc Nacionālās asamblejas pieprasījuma ir jāziņo par šādu izpaušanu.

3.3.3. *Revīzijas un inspekcijas padome*

BAI veic tādas pašas pārraudzības funkcijas attiecībā uz izlūkošanas aģentūrām kā krimināltiesību aizsardzības jomā (sk. 2.3.2. iedaļu) ([264]).

3.3.4. *Personas informācijas aizsardzības komisija*

Attiecībā uz datu apstrādi valsts drošības nolūkos, tostarp vākšanas posmu, *PIPC* veic papildu pārraudzību. Kā sīkāk paskaidrots 1.2. iedaļā, tas ietver *PIPA* 3. pantā un 58. panta 4. punktā izklāstītos vispārējos principus un pienākumus, kā arī *PIPA* 4. pantā garantēto individuālo tiesību īstenošanu. Turklāt saskaņā ar *PIPA* 7-8. panta 3. un 4. punktu un 7-9. panta 5. punktu *PIPC* pārraudzība attiecas arī uz iespējamiem tādu noteikumu pārkāpumiem, kas ietverti īpašos tiesību aktos, kuros noteikti ierobežojumi un garantijas attiecībā uz personas informācijas vākšanu, piemēram, *CPPA*, Terorisma apkarošanas likums un *TBA*. Ņemot vērā *PIPA* 3. panta 1. punktā noteiktās prasības likumīgai un godprātīgai personas informācijas vākšanai, jebkāds šo likumu pārkāpums ir *PIPA* pārkāpums. Tādējādi *PIPC* ir pilnvaras izmeklēt ([265]) to tiesību pārkāpumus, kas reglamentē piekļuvi datiem valsts drošības nolūkos, kā arī *PIPA* apstrādes noteikumus, sniegt padomus par uzlabojumiem, noteikt korektīvus pasākumus, ieteikt disciplināratbildību un nodot iespējamos pārkāpumus attiecīgajām izmeklēšanas iestādēm ([266]).

3.3.5. *Valsts cilvēktiesību komisija*

NHRC veikta pārraudzība attiecas uz izlūkošanas aģentūrām tāpat kā uz citām valsts iestādēm (sk. 2.3.2. iedaļu).

3.4. **Individuāla tiesiskā aizsardzība**

3.4.1. *Cilvēktiesību aizsardzības uzrauga nodrošinātā tiesiskā aizsardzība*

Attiecībā uz personas informācijas vākšanu saistībā ar terorisma apkarošanas darbībām *HRPO*, kas darbojas Terorisma apkarošanas komisijas paspārnē, nodrošina īpašu tiesiskās aizsardzības līdzekli. *HRPO* izskata civilus lūgumrakstus, kas saistīti ar cilvēktiesību pārkāpumiem terorisma apkarošanas darbību rezultātā ([267]). Tas var ieteikt koriģējošus pasākumus, un attiecīgajai aģentūrai ir jāziņo uzraugam par visiem pasākumiem, kas veikti, lai īstenotu šādu ieteikumu. Uz personām neattiecas atbilstības prasība kā nosacījums sūdzības iesniegšanai *HRPO*. Līdz ar to *HRPO* sūdzību izskatīs pat tad, ja attiecīgā persona pieņemamības posmā faktiski nevarēs pierādīt kaitējumu.

([259]) *NIS* likuma 18. pants.
([260]) *NIS* likuma 15. panta 2. punkts.
([261]) *NIS* likuma 17. panta 2. punkts. "Valsts noslēpumi" ir definēti kā "fakti, pierādījumi vai informācija, kas klasificēti kā valsts noslēpumi, kuriem piekļūt atļauts ierobežotam personu lokam un kurus nedrīkst izpaust nevienai citai valstij vai organizācijai, lai izvairītos no nopietna kaitējuma valsts drošībai", sk. *NIS* likuma 13. panta 4. punktu.
([262]) Likuma par pārbaudēm un izmeklēšanu valsts pārvaldes jomā 16. panta 2. punkts.
([263]) *CPPA* 15. pants.
([264]) Tāpat kā Nacionālās asamblejas Izlūkošanas komitejas gadījumā, *NIS* direktors var atteikties sniegt atbildi *BAI* tikai par jautājumiem, kas ir valsts noslēpumi, un ja sabiedrības informētība varētu nopietni kaitēt valsts drošībai (*NIS* likuma 13. panta 1. punkts).
([265]) *PIPA* 63. pants.
([266]) *PIPA* 61. panta 2. punkts, 65. panta 1. punkts, 65. panta 2. punkts un 64. panta 4. punkts.
([267]) Terorisma apkarošanas likuma Izpildes dekrēta 8. panta 1. punkta 2. apakšpunkts.

3.4.2. *Tiesiskās aizsardzības mehānismi, kas pieejami saskaņā ar PIPA*

Personas var izmantot savas piekļuves, labošanas, dzēšanas un apturēšanas tiesības saskaņā ar *PIPA* attiecībā uz personas informāciju, ko apstrādā valsts drošības nolūkos ([268]). Pieprasījumus izmantot šīs tiesības var iesniegt tieši izlūkošanas aģentūrai vai netieši ar *PIPC* starpniecību. Izlūkošanas aģentūra var atlikt, ierobežot vai liegt tiesību izmantošanu tiktāl un tik ilgi, cik šāda rīcība ir nepieciešama un samērīga, lai aizsargātu svarīgu sabiedrības interešu mērķi (piemēram, tiktāl un tik ilgi, kamēr tiesību piešķiršana apdraudētu notiekošu izmeklēšanu vai apdraudētu valsts drošību), vai gadījumos, kad tiesību piešķiršana var radīt kaitējumu trešās personas dzīvībai vai veselībai. Ja pieprasījums tiek noraidīts vai ierobežots, persona nekavējoties jāinformē par iemesliem.

Turklāt saskaņā ar *PIPA* 58. panta 4. punktu (prasība nodrošināt individuālu sūdzību atbilstīgu izskatīšanu) un *PIPA* 4. panta 5. punktu (tiesības uz atbilstošu tiesisko aizsardzību, izmantojot ātru un taisnīgu procedūru, par kaitējumu, kas radies personas informācijas apstrādes rezultātā), personām ir tiesības uz tiesisko aizsardzību. Tas ietver tiesības ziņot par iespējamu pārkāpumu privātuma jautājumu zvanu centrā, ko vada Korejas Interneta un drošības aģentūra, un iesniegt sūdzību *PIPC* ([269]). Šie tiesiskās aizsardzības līdzekļi ir pieejami gan gadījumos, kad, iespējams, tiek pārkāpti noteikumi, kas ietverti konkrētos tiesību aktos, kuros noteikti ierobežojumi un garantijas attiecībā uz personas informācijas vākšanu, piemēram, valsts drošības nolūkos, gan *PIPA* noteikumu pārkāpumu gadījumos. Kā paskaidrots Paziņojumā Nr. 2021-1, persona no ES var iesniegt sūdzību *PIPC* ar savas valsts datu aizsardzības iestādes starpniecību. Šādā gadījumā *PIPC* informēs personu ar valsts datu aizsardzības iestādes starpniecību, tiklīdz izmeklēšana būs pabeigta (tostarp attiecīgā gadījumā sniedzot informāciju par piemērotajiem korektīvajiem pasākumiem). *PIPC* lēmumus vai bezdarbību var pārsūdzēt Korejas tiesās saskaņā ar Administratīvo lietu iztiesāšanas likumu.

3.4.3. *Valsts cilvēktiesību komisijas nodrošinātā tiesiskā aizsardzība*

Iespēja saņemt individuālu tiesisko aizsardzību *NHRC* attiecas uz izlūkošanas aģentūrām tādā pašā veidā kā uz citām valsts iestādēm (sk. 2.4.2. iedaļu).

3.4.4. *Tiesiskā aizsardzība*

Tāpat kā attiecībā uz krimināltiesību aizsardzības iestāžu darbībām, personas var iegūt tiesisko aizsardzību pret izlūkošanas aģentūrām saistībā ar iepriekš minēto ierobežojumu un garantiju pārkāpumiem, izmantojot dažādas iespējas.

Pirmkārt, personas var saņemt kompensāciju par kaitējumu saskaņā ar Valsts kompensāciju likumu. Piemēram, vienā gadījumā tika piešķirta kompensācija par nelikumīgu novērošanu, ko veica Aizsardzības atbalsta pavēlniecība (Aizsardzības drošības atbalsta pavēlniecības priekštece) ([270]).

Otrkārt, Administratīvo lietu iztiesāšanas likums ļauj personām apstrīdēt administratīvo aģentūru, tostarp izlūkošanas aģentūru, rīkojumus un bezdarbību ([271]).

Visbeidzot, personas var iesniegt Konstitucionālajā tiesā konstitucionālu sūdzību par pasākumiem, ko izlūkošanas aģentūras veikušas, pamatojoties uz Konstitucionālās tiesas likumu.

([268]) *PIPA* 3. panta 5. punkts un 4. panta 1., 3. un 4. punkts.
([269]) *PIPA* 62. pants un 63. panta 2. punkts.
([270]) Augstākās tiesas 1998. gada 24. jūlija Lēmums Nr. 96Da42789.
([271]) Administratīvo lietu iztiesāšanas likuma 3. un 4. pants.