Euroopan unionin
virallinen lehti

L 44

Suomenkielinen laitos

Lainsäädäntö

65. vuosikerta

24. helmikuuta 2022

Sisältö

[1] ETA:n kannalta merkityksellinen teksti.

FI

Säädökset, joiden otsikot on painettu laihalla kirjasintyypillä, ovat maatalouspolitiikan alaan kuuluvia juoksevien asioiden hoitoon liittyviä säädöksiä, joiden voimassaoloaika on yleensä rajoitettu.

Kaikkien muiden säädösten otsikot on painettu lihavalla kirjasintyypillä ja merkitty tähdellä.

II

(Muut kuin lainsäätämisjärjestyksessä hyväksyttävät säädökset)

PÄÄTÖKSET

KOMISSION TÄYTÄNTÖÖNPANOPÄÄTÖS (EU) 2022/254,

annettu 17 päivänä joulukuuta 2021,

Euroopan parlamentin ja neuvoston asetuksen (EU) 2016/679 nojalla Korean tasavallan tietosuojalain mukaisen henkilötietojen suojan riittävästä tasosta

(tiedoksiannettu numerolla C(2021) 9316)

(ETA:n kannalta merkityksellinen teksti)

EUROOPAN KOMISSIO, joka

ottaa huomioon Euroopan unionin toiminnasta tehdyn sopimuksen,

ottaa huomioon luonnollisten henkilöiden suojelusta henkilötietojen käsittelyssä sekä näiden tietojen vapaasta liikkuvuudesta ja direktiivin 95/46/EY kumoamisesta 27 päivänä huhtikuuta 2016 annetun Euroopan parlamentin ja neuvoston asetuksen (EU) 2016/679 (yleinen tietosuoja-asetus) ([1]) ja erityisesti sen 45 artiklan 3 kohdan,

sekä katsoo seuraavaa:

1. JOHDANTO

(1) Asetuksessa (EU) 2016/679 vahvistetaan säännöt, joita sovelletaan henkilötietojen siirtoon unioniin sijoittautuneilta rekisterinpitäjiltä tai henkilötietojen käsittelijöiltä kolmansiin maihin ja kansainvälisille järjestöille, siltä osin kuin tällaiset siirrot kuuluvat sen soveltamisalaan. Henkilötietojen kansainvälistä siirtoa koskevat säännöt vahvistetaan asetuksen V luvussa (44–50 artikla). Kansainvälisen yhteistyön ja kaupan kehittämiseksi on tarpeen siirtää henkilötietoja Euroopan unionin ulkopuolisiin maihin tai niistä unioniin. Samalla on kuitenkin varmistettava, että kolmansiin maihin tehtävien siirtojen yhteydessä ei heikennetä henkilötietojen suojan tasoa unionissa ([2]).

(2) Asetuksen (EU) 2016/679 45 artiklan 3 kohdan mukaan komissio voi päättää täytäntöönpanosäädöksellä, että jokin kolmas maa tai kolmannen maan alue tai yksi tai useampi tietty sektori tai kansainvälinen järjestö varmistaa riittävän tietosuojan. Tämän edellytyksen täyttyessä henkilötietoja voidaan siirtää kyseiselle kolmannelle maalle ilman erillistä lupaa, kuten asetuksen (EU) 2016/679 45 artiklan 1 kohdassa ja johdanto-osan 103 kappaleessa säädetään.

(3) Kuten asetuksen (EU) 2016/679 45 artiklan 2 kohdassa säädetään, tietosuojan riittävyyttä koskevan päätöksen tekemisen on perustuttava kattavaan analyysiin kolmannen maan oikeusjärjestyksestä. Analyysissa on tarkasteltava sekä tietojen tuojia koskevia sääntöjä että niitä rajoituksia ja suojatoimia, jotka koskevat viranomaisten pääsyä henkilötietoihin. Komission on arvioinnissaan määritettävä, vastaako kyseisen kolmannen maan takaama tietosuojan taso ”olennaisilta osin” Euroopan unionissa taattua suojan tasoa (asetuksen (EU) 2016/679 johdanto-osan 104 kappale). Tätä on arvioitava suhteessa unionin lainsäädäntöön ja erityisesti asetukseen (EU) 2016/679 sekä Euroopan unionin tuomioistuimen oikeuskäytäntöön ([3]).

([1]) EUVL L 119, 4.5.2016, s. 1.
([2]) Ks. asetuksen (EU) 2016/679 johdanto-osan 101 kappale.
([3]) Ks. viimeksi asia C-311/18, Facebook Ireland ja Schrems (”Schrems II”), ECLI:EU:C:2020:559.

(4) Kuten Euroopan unionin tuomioistuin on selventänyt, tämä ei edellytä, että tietosuojan tason pitäisi olla täysin sama ([4]). Erityisesti keinot, joita kyseisellä kolmannella maalla on käytettävissään henkilötietojen suojaamiseksi, voivat erota unionissa käytetyistä menetelmistä, kunhan ne käytännössä varmistavat tehokkaasti tietosuojan riittävän tason ([5]). Tietosuojan tason riittävyyttä koskeva vaatimus ei sen vuoksi edellytä unionin sääntöjen kopiointia kohta kohdalta. Sen sijaan on kyse siitä, onko ulkomaisen järjestelmän antama tietosuoja kokonaisuutena vaaditun tason mukainen. Tällöin selvitetään, mikä on yksityisyyteen liittyvien oikeuksien sisältö ja pannaanko ne täytäntöön ja valvotaanko niiden toteutumista tehokkaasti ([6]). Myös Euroopan tietosuojaneuvosto on antanut ohjeistusta tietosuojan riittävyyden tutkimisesta ([7]).

(5) Komissio on analysoinut huolellisesti Korean lainsäädäntöä ja käytäntöjä. Johdanto-osan (8)–(208) kappaleessa esitettyjen havaintojen perusteella komissio katsoo, että Korean tasavalta takaa riittävän suojan henkilötiedoille, jotka unioniin sijoittautunut rekisterinpitäjä tai henkilötietojen käsittelijä ([8]) siirtää sellaisille Koreassa oleville yksiköille (esim. luonnollisille tai oikeushenkilöille, organisaatioille, julkisille laitoksille), joihin sovelletaan Korean tietosuojalakia (*Personal Information Protection Act*, eli 29 päivänä maaliskuuta 2011 annettu laki N:o 10465, sellaisena kuin se on viimeksi muutettuna 4 päivänä helmikuuta 2020 annetulla lailla N:o 16930). Tämä koskee sekä asetuksessa (EU) 2016/679 tarkoitettuja rekisterinpitäjiä että henkilötietojen käsittelijöitä, jäljempänä 'toimeksisaajat' (*outsourcees*) ([9]). Tietosuojan riittävyyttä koskeva päätelmä ei kata henkilötietojen käsittelyä, jota uskonnolliset organisaatiot suorittavat lähetystyön yhteydessä tai joka liittyy poliittisten puolueiden ehdokasasetteluun, eikä rahoituspalvelukomission valvonnan alaisuuteen kuuluvien rekisterinpitäjien luottotietolain nojalla suorittamaa henkilökohtaisten luottotietojen käsittelyä.

(6) Tässä päätelmässä otetaan huomioon lisätakeet, jotka esitetään ilmoituksessa N:o 2021-5 (liite I) ja Korean hallituksen komissiolle antamissa virallisissa lausunnoissa, vakuutuksissa ja sitoumuksissa (liite II).

(7) Tämän päätöksen seurauksena tiedonsiirrot Korean tasavaltaan sijoittautuneille rekisterinpitäjille ja henkilötietojen käsittelijöille voidaan toteuttaa ilman eri hyväksyntää. Päätös ei rajoita asetuksen (EU) 2016/679 suoraa soveltamista tällaisiin yksiköihin silloin kun kyseisen asetuksen 3 artiklassa säädetyt alueellista soveltamista koskevat edellytykset täyttyvät.

2. HENKILÖTIETOJEN KÄSITTELYYN SOVELLETTAVAT SÄÄNNÖT

2.1 Korean tasavallan tietosuojakehys

(8) Yksityisyydensuojaa ja tietosuojaa koskeva Korean säännöstö perustuu 17 päivänä heinäkuuta 1948 annettuun perustuslakiin. Vaikka perustuslaissa ei nimenomaisesti mainita oikeutta henkilötietojen suojaan, se kuitenkin tunnustetaan perusoikeudeksi, jonka perustan muodostavat perustuslailliset oikeudet ihmisarvoon ja onnellisuuden tavoitteluun (10 §), oikeus yksityiselämään (17 §) ja oikeus viestinnän yksityisyyteen (18 §). Tämän ovat vahvistaneet sekä korkein oikeus ([10]) että perustuslakituomioistuin ([11]). Perusoikeuksia ja -vapauksia (mukaan lukien oikeutta yksityisyyteen) voidaan rajoittaa vain lain nojalla, jos se on tarpeen kansallisen turvallisuuden, lain ja yleisen järjestyksen tai yleisen hyvinvoinnin ylläpitämiseksi, eikä tällainen rajoittaminen saa vaikuttaa kyseisen vapauden tai oikeuden olennaiseen sisältöön (37 §:n 2 momentti).

([4]) Asia C-362/14, Maximilian Schrems v. Data Protection Commissioner ("Schrems"), ECLI:EU:C:2015:650, 73 kohta.
([5]) Tuomio asiassa Schrems, 74 kohta.
([6]) Ks. komission tiedonanto Euroopan parlamentille ja neuvostolle: *Henkilötietojen vaihtaminen ja suojaaminen globalisoituneessa maailmassa*, COM(2017) 7, 10.1.2017, kohta 3.1, s. 6–7.
([7]) Euroopan tietosuojaneuvosto: *Tietosuojan riittävyyden viitearvot*, WP 254 rev. 01., saatavilla seuraavassa osoitteessa: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=614108
([8]) Tämä päätös on merkityksellinen ETA:n kannalta. Euroopan talousalueesta tehdyn sopimuksen (ETA-sopimus) mukaan Euroopan unionin sisämarkkinat ulottuvat kolmeen ETA-valtioon (Islanti, Liechtenstein ja Norja). ETA:n sekakomitean 6 päivänä heinäkuuta 2018 antama päätös, jolla asetus (EU) 2016/679 otettiin osaksi ETA-sopimuksen liitettä XI, tuli voimaan 20 päivänä heinäkuuta 2018. Asetus kuuluu näin ollen kyseisen sopimuksen soveltamisalaan. Kyseistä päätöstä sovellettaessa viittauksia EU:hun ja EU:n jäsenvaltioihin olisi näin ollen pidettävä myös viittauksina ETA-valtioihin.
([9]) Ks. tämän päätöksen 2.2.3 kohta.
([10]) Ks. esim. korkeimman oikeuden päätös 2014Da77970, 15.10.2015 (englanninkielinen tiivistelmä "Lawmaker's disclosure of teachers' trade union members case" osoitteessa https://www.privacy.go.kr/eng/enforcement_01.do) oikeuskäytäntöviittauksineen, ml. päätös 2012Da49933, 24.7.2014.
([11]) Ks. erityisesti perustuslakituomioistuimen päätös 99Hun-ma513, 26.5.2005 (englanninkielinen tiivistelmä osoitteessa http://www.koreanlii.or.kr/w/index.php/99Hun-Ma513?ckattempt=2) ja päätös 2014JHun-ma449 2013 Hun-Ba68 (konsolidoitu), 23.12.2015 (englanninkielinen tiivistelmä "Change of resident registration number case" osoitteessa https://www.privacy.go.kr/eng/enforcement_01.do).

(9) Perustuslaissa viitataan useaan otteeseen Korean kansalaisten oikeuksiin, mutta perustuslakituomioistuin on todennut, että perusoikeudet koskevat myös ulkomaalaisia. ([12]). Perustuslakituomioistuin on erityisesti katsonut, että ihmisarvon ja ihmisyyden suojelu sekä oikeus onnellisuuden tavoitteluun kuuluvat kaikille ihmisille eivätkä ainoastaan maan kansalaisille ([13]). Lisäksi Korean hallituksen virallisten lausuntojen ([14]) mukaan yleisesti tunnustetaan, että perustuslain 12–22 §:ssä säädetään perustavanlaatuisista ihmisoikeuksista (joihin kuuluu myös oikeus yksityisyyteen) ([15]). Vaikka toistaiseksi ei ole annettu oikeuskäytäntöä, joka koskisi nimenomaisesti ulkomaiden kansalaisten oikeutta yksityisyyteen, tätä päätelmää tukee se, että kyseinen oikeus perustuu ihmisarvon suojelua ja onnen tavoittelua koskeviin oikeuksiin ([16]).

(10) Korea on myös antanut useita tietosuojaa koskevia lakeja, joissa säädetyt takeet koskevat kaikkia yksilöitä näiden kansalaisuudesta riippumatta ([17]). Tämän päätöksen kannalta merkitykselliset Korean lait ovat:

— tietosuojalaki (*Personal Information Protection Act*);

— laki luottotietojen käytöstä ja suojaamisesta (*Act on the Use and Protection of Credit Information*) ([18]);

— viestinnän tietosuojalaki (*Communications Privacy Protection Act*).

(11) Tietosuojalaissa vahvistetaan Korean tasavallan yleinen tietosuojakehys. Sitä on täydennetty täytäntöönpanoasetuksella (presidentin asetus N:o 23169, annettu 29 päivänä syyskuuta 2011, sellaisena kuin se on viimeksi muutettuna presidentin asetuksella N:o 30892, annettu 4 päivänä elokuuta 2020), jäljempänä '(tietosuojalain) täytäntöönpanoasetus', joka tietosuojalain tavoin on oikeudellisesti sitova ja täytäntöönpanokelpoinen.

(12) Korean tietosuojalautakunta (*Personal Information Protection Commission*, PIPC) on lisäksi antanut muita sääntöjä tietosuojalain tulkinnasta ja soveltamisesta lakisääteisillä ilmoituksilla (*Notification*). Tietosuojalautakunta on antanut tietosuojalain 5 §:n (Valtion velvollisuudet) ja 14 §:n (Kansainvälinen yhteistyö) nojalla 1 päivänä syyskuuta 2020 ilmoituksen N:o 2021-5 tiettyjen tietosuojalain säännösten tulkinnasta, soveltamisesta ja täytäntöönpanosta (sellaisena kuin se on muutettuna 21 päivänä tammikuuta 2021 annetulla ilmoituksella N:o 2021-1 ja 16 päivänä marraskuuta 2021 annetulla ilmoituksella N:o 2021-5). Kyseisessä ilmoituksessa esitetään selvennyksiä, joita sovelletaan kaikkeen tietosuojalain nojalla tapahtuvaan henkilötietojen käsittelyyn, sekä lisätakeita Koreaan tämän päätöksen perusteella siirrettäviä henkilötietoja varten. Ilmoitus sitoo rekisterinpitäjiä oikeudellisesti, ja sen täytäntöönpanosta vastaavat sekä tietosuojalautakunta että tuomioistuimet ([19]). Ilmoituksessa vahvistettujen sääntöjen rikkominen merkitsee niiden tietosuojalain säännösten rikkomista, joita säännöt täydentävät. Sen vuoksi tietosuojalain säännösten arvioinnin yhteydessä arvioidaan myös lisätakeiden sisältöä. Tietosuojalautakunta on lisäksi laatinut tietosuojalakia koskevan käsikirjan ja ohjeita (*PIPA Handbook and Guidelines*), joissa selostetaan, miten tietosuojalautakunta soveltaa henkilötietojen suojaa koskevia sääntöjä ja valvoo niiden noudattamista ([20]).

([12]) Perustuslakituomioistuimen päätös 93 Hun-MA120, 29.12.1994.
([13]) Perustuslakituomioistuimen päätös 99HeonMa494, 29.11.2001.
([14]) Ks. liitteen II kohta 1.1.
([15]) Ks. myös tietosuojalain 1 §, jossa viitataan nimenomaisesti "yksilöiden vapauksiin ja oikeuksiin". Laissa myös todetaan, että sen tarkoituksena on "säännellä henkilökohtaisten tietojen käsittelyä ja suojelua yksilöiden vapauksien ja oikeuksien suojelemiseksi sekä yksilöiden ihmisarvon ja arvokkuuden toteuttamiseksi". Tietosuojalain 5 §:n 1 momentissa säädetään vastaavasti, että on valtion velvollisuus "laatia politiikkatoimenpiteitä niiden haittavaikutusten estämiseksi, jotka johtuvat siitä, että henkilökohtaisia tietoja kerätään enemmän kuin on tarpeen tai että niitä käytetään väärin, tai epäasianmukaisesta tarkkailusta ja seuraamisesta jne., sekä taata ihmisarvo ja oikeus yksityisyyteen".
([16]) Perustuslain 6 §:n 2 momentissa säädetään lisäksi, että ulkomaiden kansalaisten asema taataan kansainvälisen oikeuden ja kansainvälisten sopimusten mukaisesti. Korea on osapuolena useissa kansainvälisissä sopimuksissa, joissa taataan oikeus yksityisyyteen, kuten kansalaisoikeuksia ja poliittisia oikeuksia koskeva kansainvälinen yleissopimus (17 §), yleissopimus vammaisten henkilöiden oikeuksista (22 §) ja yleissopimus lapsen oikeuksista (16 §).
([17]) Näihin kuuluu myös sääntöjä, joilla on merkitystä henkilötietojen suojan kannalta mutta joita ei sovelleta tilanteessa, jossa henkilötietoja kerätään unionissa ja siirretään Koreaan asetuksen (EU) 2016/679 nojalla, kuten laki paikkatietojen suojelusta, käytöstä jne. (*Act on the Protection, Use, etc. of Location Information*).
([18]) Tämän lain tarkoituksena on vaalia moitteetonta luottotietoihin liittyvää liiketoimintaa edistämällä luottotietojen tehokasta käyttöä ja järjestelmällistä hallintaa ja suojaamalla yksityisyyttä luottotietojen väärinkäytöltä (lain 1 §).
([19]) Korean tuomioistuimet ovat antaneet päätöksiä tietosuojalautakunnan antamien lakisääteisten ilmoitusten noudattamisesta useissa asioissa, joissa ne ovat muun muassa katsoneet korealaisten rekisterinpitäjien rikkoneen kyseisiä sääntöjä (ks. esim. korkeimman oikeuden päätös 2018Da219406, 25.10.2018, jossa tuomioistuin määräsi rekisterinpitäjän maksamaan yksilöille korvauksia vahingoista, joita näille oli aiheutunut siksi, että rekisterinpitäjä oli rikkonut henkilötietojen turvallisuuden varmistamista koskevista toimenpiteistä annettua ilmoitusta (*Notification for the standard for measures to ensure the safety of personal information*); ks. myös korkeimman oikeuden päätös 2018Da219352, 25.10.2018; korkeimman oikeuden päätös 2011Da24555, 16.5.2016; Soulin keskisen piirioikeuden (*Seoul Central District Court*) päätös 2014Gahap511956, 13.10.2016. Soulin keskisen piirioikeuden päätös 2009Gahap43176, 26.1.2010.
([20]) Tietosuojalain 12 §:n 1 momentti.

(13) Laissa luottotietojen käytöstä ja suojaamisesta, jäljempänä 'luottotietolaki', vahvistetaan lisäksi säännöt, joita sovelletaan sekä "tavanomaisiin" kaupallisiin toimijoihin että rahoitusalan erikoistuneisiin yhteisöihin silloin kun ne käsittelevät henkilökohtaisia luottotietoja eli tietoja, joita tarvitaan rahoitus- tai liiketoimien osapuolten luottokelpoisuuden määrittämiseksi. Näitä tietoja ovat muun muassa nimi, yhteystiedot, rahoitustoimet, luottoluokitus, vakuutustilanne tai lainasaldo silloin kun näitä tietoja käytetään henkilön luottokelpoisuuden määrittämiseen ([21]). Silloin kun näitä tietoja käytetään muussa tarkoituksessa (esimerkiksi henkilöstöhallintoa varten), sovelletaan tietosuojalakia kaikilta osin. Luottotietolain tietosuojasäännösten noudattamista valvoo osittain tietosuojalautakunta (kaupan alan organisaatioiden osalta ks. lain 45-3 §) ja osittain rahoituspalvelukomissio ([22]) (rahoitusalan, kuten luottoluokituslaitosten, pankkien, vakuutusyhtiöiden, säästöpankkien, luottorahoitukseen erikoistuneiden yritysten, finanssipalveluyritysten, arvopaperirahoitusyritysten ja luotto-osuuskuntien osalta ks. lain 45 §:n 1 momentti yhdessä sen täytäntöönpanoasetuksen 36-2 §:n ja rahoituspalvelukomissiosta annetun lain (*Act on the Financial Services Commission*) 38 §:n kanssa). Tältä osin tämän päätöksen soveltamisala rajoittuu niihin kaupan alan organisaatioihin, jotka kuuluvat tietosuojalautakunnan valvonnan alaisuuteen ([23]). Tässä yhteydessä sovellettavia luottotietolain erityissääntöjä käsitellään 2.3.11 kohdassa (jos erityissääntöjä ei ole, sovelletaan tietosuojalaissa vahvistettuja yleisiä sääntöjä).

2.2 **Korean tietosuojalain aineellinen ja henkilöllinen soveltamisala**

(14) Ellei muissa laeissa nimenomaisesti toisin säädetä, henkilötietojen suojaan sovelletaan tietosuojalakia (6 §). Sen aineellinen ja henkilöllinen soveltamisala on määritetty käsitteitä 'henkilötieto', 'käsittely' ja 'rekisterinpitäjä' koskevien määritelmien avulla.

2.2.1 *Henkilötietojen määritelmä*

(15) Tietosuojalain 2 §:n 1 momentissa esitetyn määritelmän mukaan henkilötiedoilla tarkoitetaan elävään henkilöön liittyviä tietoja, joiden perusteella henkilö voidaan tunnistaa joko suoraan, kuten nimi, asukasrekisterinumero tai kuva, tai epäsuorasti, eli kun tiedot, joista henkilöä ei voida suoraan tunnistaa, voidaan helposti yhdistää muihin tietoihin. Se, miten "helposti" tietoja voidaan yhdistää, riippuu siitä, miten todennäköistä tällainen tietojen yhdistäminen on, kun otetaan huomioon mahdollisuus saada muita tietoja sekä henkilön tunnistamiseen tarvittava aika, kustannukset ja teknologia.

(16) Tietosuojalain mukaan henkilötietoja ovat myös pseudonymisoidut tiedot eli tiedot, joiden perusteella tietyn henkilön tunnistaminen on mahdollista vain jos käytetään tai jos tietoihin yhdistetään muita tietoja, joiden avulla ne palautetaan alkuperäiseen tilaansa (lain 2 §:n 1 momentin c alakohta). Vastaavasti tiedot, jotka on täysin anonymisoitu, on suljettu lain soveltamisalan ulkopuolelle (58 §:n 2 momentti). Tämä koskee tietoja, joista ei voida tunnistaa tiettyä henkilöä edes yhdistämällä ne muihin tietoihin, kun otetaan huomioon tunnistamiseen kohtuudella tarvittava aika, kustannukset ja teknologia.

(17) Tämä vastaa asetuksen (EU) 2016/679 aineellista soveltamisalaa ja siinä määriteltyjä käsitteitä "henkilötiedot, pseudonymisointi" ([24]) ja "anonymisoidut tiedot" ([25]).

([21]) Luottotietolain 2 §:n 1 momentti.

([22]) Rahoituspalvelukomissio (*Financial Services Commission*) on Korean rahoitussektorin valvontaviranomainen ja vastaa siten myös luottotietolain noudattamisen valvonnasta.

([23]) Jos tilanne muuttuu tulevaisuudessa esimerkiksi siten, että tietosuojalautakunnan toimivaltaa laajennetaan kattamaan kaikenlainen luottotietolain nojalla tapahtuva henkilökohtaisten luottotietojen käsittely, voitaisiin harkita tämän tietosuojan riittävyyttä koskevan päätöksen muuttamista niin, että se kattaisi myös yksiköt, jotka nyt kuuluvat rahoituspalvelukomission valvonnan alaisuuteen.

([24]) Tietosuojalain mukaan "pseudonymisoidulla käsittelyllä" tarkoitetaan esimerkiksi käsittelymenetelmiä, joissa osa henkilötiedoista poistetaan tai korvataan joko osittain tai kokonaan niin, että yksittäistä henkilöä ei voida tunnistaa ilman lisätietoja (lain 2 §:n 1–2 momentti). Tämä vastaa asetuksen (EU) 2016/679 4 artiklan 5 kohdassa esitettyä 'pseudonymisoimisen' määritelmää, jonka mukaan sillä tarkoitetaan "henkilötietojen käsittelemistä siten, että henkilötietoja ei voida enää yhdistää tiettyyn rekisteröityyn käyttämättä lisätietoja, edellyttäen että tällaiset lisätiedot säilytetään erillään ja niihin sovelletaan teknisiä ja organisatorisia toimenpiteitä, joilla varmistetaan, ettei henkilötietojen yhdistämistä tunnistettuun tai tunnistettavissa olevaan luonnolliseen henkilöön tapahdu".

([25]) Erityisesti asetuksen (EU) 2016/679 johdanto-osan 26 kappaleessa selvennetään, että asetusta ei sovelleta anonymisoituihin tietoihin eli tietoihin, jotka eivät liity tunnistettuun tai tunnistettavissa olevaan luonnolliseen henkilöön. Tämä taas riippuu siitä, mitä keinoja rekisterinpitäjän tai muun henkilön voidaan kohtuullisen todennäköisesti odottaa käyttävän luonnollisen henkilön tunnistamiseksi suoraan tai epäsuorasti. Jotta voidaan selvittää, voidaanko tällaisia keinoja kohtuullisen todennäköisesti käyttää luonnollisen henkilön tunnistamiseen, on otettava huomioon kaikki objektiiviset tekijät, kuten tunnistamisesta aiheutuvat kulut ja tunnistamiseen tarvittava aika sekä käsittelyajankohtana käytettävissä oleva teknologia ja tekninen kehitys.

2.2.2 *Käsittelyn määritelmä*

(18) ”Käsittely” määritellään tietosuojalaissa väljästi niin, että se kattaa ”henkilötietojen keräämisen, generoimisen, yhdistämisen, yhteenkytkemisen, tallettamisen, säilyttämisen, varastoinnin, lisäarvoa tuottavan käsittelyn, editoinnin, hakemisen, tulostamisen, korjaamisen, palauttamisen, käytön, luovuttamisen, paljastamisen ja poistamisen sekä muut vastaavat toimet” ([26]). Vaikka tietyissä tietosuojalain säännöksissä viitataan vain tietyntyyppiseen käsittelyyn, kuten ”käyttöön”, ”toimittamiseen” tai ”keräämiseen” ([27]), ”käytön” tulkitaan sisältävän kaikenlaisen muun käsittelyn kuin ”keräämisen” tai (kolmannelle osapuolelle) ”luovuttamisen”. ”Käytön” laajalla tulkinnalla varmistetaan, että suojeluun ei jää aukkoja erilaisten käsittelytoimien osalta. Näin ollen käsittelyn käsite vastaa asetuksessa (EU) 2016/679 käytettyä käsitettä.

2.2.3 *Rekisterinpitäjä ja toimeksisaaja*

(19) Tietosuojalakia sovelletaan rekisterinpitäjiin. Samoin kuin asetuksessa (EU) 2016/679, tällä tarkoitetaan kaikkia julkisia laitoksia, oikeushenkilöitä, organisaatioita tai henkilöitä, jotka käsittelevät henkilötietoja suoraan tai välillisesti henkilötietorekisteriä varten osana muuta toimintaansa ([28]). Tässä yhteydessä ’henkilötietorekisterillä’ tarkoitetaan mitä tahansa ”henkilötietokokoelmaa tai -kokoelmia, jotka on järjestetty systemaattisesti jonkin säännön mukaan, niin että henkilötiedot ovat helposti saatavilla” (tietosuojalain 2 §:n 4 momentti) ([29]). Rekisterinpitäjällä on velvollisuus kouluttaa sisäisesti käsittelyyn sen johdolla osallistuvat henkilöt, kuten yrityksen virkamiehet tai työntekijät, ja huolehtia asianmukaisesta valvonnasta ja tarkastuksista (tietosuojalain 28 §:n 1 momentti).

(20) Silloin kun rekisterinpitäjä (nk. *outsourcer* eli ulkoistaja) ulkoistaa henkilötietojen käsittelyn kolmannelle osapuolelle (nk. *outsourcee* eli toimeksisaaja), sovelletaan erityisiä velvoitteita. Ulkoistamista on ensinnäkin säänneltävä oikeudellisesti sitovalla järjestelyllä (tyypillisesti sopimuksella) ([30]), jossa mainitaan ulkoistettavan työn laajuus, käsittelyn tarkoitus, sovellettavat tekniset ja hallinnolliset suojatoimet, rekisterinpitäjän suorittama valvonta, vastuu (kuten vastuu sopimusvelvoitteiden rikkomisesta aiheutuvien vahinkojen korvaamisesta) sekä kaikenlaista alihankintaa koskevat rajoitukset ([31]) (tietosuojalain 26 §:n 1 ja 2 momentti yhdessä sen täytäntöönpanoasetuksen 28 §:n 1 momentin kanssa) ([32]).

(21) Lisäksi rekisterinpitäjän on julkaistava ja pidettävä jatkuvasti ajan tasalla tiedot ulkoistetusta työstä ja siitä, mille toimeksisaajalle työ on ulkoistettu, tai, siltä osin kuin ulkoistamisprosessi koskee suoramarkkinointitoimintaa, ilmoitettava asiaankuuluvat tiedot suoraan yksilöille (tietosuojalain 26 §:n 2 ja 3 momentti yhdessä sen täytäntöönpanoasetuksen 28 §:n 2–5 momentin kanssa) ([33]).

(22) Lisäksi rekisterinpitäjällä on velvollisuus ”opettaa” toimeksisaajalle tarvittavat turvatoimet ja valvoa muun muassa tarkastusten avulla, että toimeksisaaja noudattaa sekä kaikkia rekisterinpitäjälle tietosuojalaissa asetettuja velvollisuuksia että ulkoistamissopimukseen perustuvia velvollisuuksia ([34]) (tietosuojalain 26 §:n 4 momentti yhdessä sen täytäntöönpanoasetuksen 28 §:n 6 momentin kanssa). Jos toimeksisaaja aiheuttaa vahinkoa tietosuojalain rikkomisen seurauksena, rekisterinpitäjän katsotaan olevan vastuussa sen toiminnasta tai laiminlyönnistä samalla tavoin kuin työntekijän osalta (tietosuojalain 26 §:n 6 momentti).

([26]) Tietosuojalain 2 §:n 2 momentti.

([27]) Esimerkiksi tietosuojalain 15–19 §:ssä viitataan ainoastaan henkilötietojen keräämiseen, käyttöön ja luovuttamiseen.

([28]) Tietosuojalain 2 §:n 5 momentti. Laissa tarkoitettuja julkisia laitoksia ovat kaikki keskushallinnon osastot tai virastot ja niihin liittyvät elimet, paikallishallinnon elimet, koulut ja paikallishallinnon rahoittamat julkiset yhtiöt, maan kansalliskokouksen hallintoelimet ja oikeuslaitos (ml. perustuslakituomioistuin) (tietosuojalain 2 §:n 6 momentti yhdessä sen täytäntöönpanoasetuksen 2 §:n kanssa).

([29]) Tämä vastaa asetuksen (EU) 2016/679 aineellista soveltamisalaa. Asetuksen (EU) 2016/679 2 artiklan 1 kohdan mukaan asetusta sovelletaan ”henkilötietojen käsittelyyn, joka on osittain tai kokonaan automaattista, sekä sellaisten henkilötietojen käsittelyyn muussa kuin automaattisessa muodossa, jotka muodostavat rekisterin osan tai joiden on tarkoitus muodostaa rekisterin osa”. Asetuksen (EU) 2016/679 4 artiklan 6 kohdan mukaan ’rekisterillä’ tarkoitetaan ”mitä tahansa jäsenneltyä henkilötietoja sisältävää tietojoukkoa, josta tiedot ovat saatavilla tietyin perustein”. Tämän mukaisesti asetuksen johdanto-osan 15 kappaleessa selitetään, että luonnollisten henkilöiden suojelun olisi koskettava myös ”henkilötietojen automaattista käsittelyä sekä niiden manuaalista käsittelyä, jos henkilötiedot sisältyvät tai ne on tarkoitus sisällyttää rekisteriin. Tämän asetuksen soveltamisalaan ei ole tarkoitus sisällyttää sellaisia asiakirjoja tai asiakirjakokoelmia kansilehtineen, joita ei ole järjestetty tiettyjen perusteiden mukaisesti.”

([30]) Ks. *PIPA Handbook*, lll luvun 2 kohta, jossa tarkastellaan tietosuojalain 26 pykälää (s. 203–212). Käsikirjan mukaan 26 §:n 1 momentissa viitataan sitoviin järjestelyihin, kuten sopimuksiin.

([31]) Tietosuojalain 26 §:n 5 momentin mukaan henkilötietojen käsittelijä ei saa käyttää mitään ulkoistettuun työhön kuulumattomia henkilötietoja eikä luovuttaa henkilötietoja kolmannelle osapuolelle. Tämän vaatimuksen laiminlyönti voi johtaa rikosoikeudellisiin seuraamuksiin tietosuojalain 71 §:n 2 kohdan nojalla.

([32]) Tämän vaatimuksen laiminlyönti voi johtaa sakkojen määräämiseen, ks. tietosuojalain 75 §:n 4 momentin 4 kohta.

([33]) Tämän vaatimuksen laiminlyönti voi johtaa sakkojen määräämiseen, ks. tietosuojalain 75 §:n 2 momentin 1 kohta ja 4 momentin 5 kohta.

([34]) Ks. myös tietosuojalain 26 §:n 7 momentti, jonka mukaan lain 15–25, 27–31, 33–38 ja 50 pykälää sovelletaan henkilötietojen käsittelijään soveltuvin osin.

(23) Vaikka Korean tietosuojalaissa ei ole erotettu toisistaan ”rekisterinpitäjän” ja ”käsittelijän” käsitteitä, ulkoistamista koskevat säännöt sisältävät olennaisilta osin vastaavat velvoitteet ja suojatoimet kuin ne, joilla asetuksessa (EU) 2016/679 säännellään rekisterinpitäjien ja henkilötietojen käsittelijöiden suhdetta.

2.2.4 *Tieto- ja viestintäpalvelujen tarjoajia koskevat erityissäännökset*

(24) Tietosuojalakia sovelletaan henkilötietojen käsittelyyn riippumatta siitä, kuka on rekisterinpitäjä. Tiettyihin säännöksiin sisältyy kuitenkin erityissääntöjä (*lex specialis*), joita sovelletaan silloin kun ”käyttäjien” tietoja käsittelevät ”tieto- ja viestintäpalvelujen tarjoajat” ([35]). ”Käyttäjillä” tarkoitetaan tieto- ja viestintäpalveluja käyttäviä luonnollisia henkilöitä (Laki tieto- ja viestintäverkon käytön ja tietosuojan edistämisestä (*Act on the Promotion of Information and Communications Network Utilisation and Data Protection*), jäljempänä ’tietoverkkolaki’, 2 §:n 1 momentin 4 kohta). Tämä tarkoittaa henkilöitä, jotka joko käyttävät suoraan korealaisen televiestintäpalvelujen tarjoajan televiestintäpalveluja tai tietopalveluja ([36]), joita tarjoaa sellainen kaupallinen (eli voittoa tavoitteleva) yksikkö, joka puolestaan tukeutuu Koreassa toimiluvan/rekisteröinnin nojalla toimivan televiestintäpalvelujen tarjoajan palveluihin ([37]). Kummassakin tapauksessa yksikkö, jota tietosuojalain erityissäännökset sitovat, on se, joka tarjoaa verkkopalvelua suoraan kyseiselle henkilölle (käyttäjälle).

(25) Vastaavasti päätelmä tietosuojan riittävyydestä kattaa tietosuojan tason yksinomaan niiden henkilötietojen osalta, jotka unionin rekisterinpitäjä/käsittelijä siirtää jollekin yksikölle kolmanteen maahan (tässä tapauksessa Korean tasavaltaan). Jälkimmäisessä tapauksessa unionissa olevilla henkilöillä on yleensä suora suhde ainoastaan unionissa olevaan ”tietojen viejään”, mutta ei korealaiseen tieto- ja viestintäpalvelujen tarjoajaan ([38]). Sen vuoksi tieto- ja viestintäpalvelujen käyttäjien henkilötietoja koskevia tietosuojalain erityissäännöksiä sovelletaan tämän päätöksen nojalla siirrettäviin henkilötietoihin vain rajoitetusti.

2.2.5 *Tietosuojalain eräitä säännöksiä koskevat poikkeukset*

(26) Tietosuojalain 58 §:n 1 momentin mukaan neljä tietojenkäsittelyn luokkaa on vapautettu sen tiettyjen säännösten (15–57 §) soveltamisesta ([39]). Vapautus kattaa erityisesti ne tietosuojalain säännökset, jotka koskevat erityisiä käsittelyperusteita, tiettyjä tietosuojavelvoitteita, yksilön oikeuksien käyttöön liittyviä yksityiskohtaisia sääntöjä sekä sääntöjä, joilla säännellään henkilötietoihin liittyvien riitojen ratkaisua erityisessä sovittelulautakunnassa. Muita tietosuojalain perussäännöksiä kuitenkin sovelletaan, erityisesti yleisiä säännöksiä, jotka koskevat tietosuojaperiaatteita (3 § – muun muassa käsittelyn lainmukaisuus, käsittelytarkoituksen määrittely ja sen rajoittaminen, kerättävien tietojen minimointi, tietojen täsmällisyys ja turvallisuus) ja yksilön oikeuksia (4 § – oikeus saada pääsy tietoihin ja oikaista tai poistaa ne tai keskeyttää niiden käsittely). Lisäksi tietosuojalain 58 §:n 4 momentissa asetetaan näille käsittelytoimille erityisiä velvoitteita, jotka koskevat tietojen minimointia, niiden säilyttämisen rajoittamista, turvatoimia ja valitusten käsittelyä ([40]). Näin ollen luonnolliset henkilöt voivat tehdä valituksen tietosuojalautakunnalle, jos näitä periaatteita ja velvoitteita ei noudateta, ja lautakunnalla on valtuudet toteuttaa laiminlyöntien perusteella toimia niiden noudattamisen varmistamiseksi.

([35]) Ks. erityisesti tietosuojalain 18 §:n 2 momentti ja VI luku.

([36]) Tietopalvelut kattavat sekä tietopalvelut että niiden tarjoamiseen tarvittavat välityspalvelut.

([37]) Ks. tietoverkkolain 2 §:n 1 momentin 3 kohta (yhdessä 2 §:n 1 momentin 2 ja 4 kohdan kanssa) ja televiestintäyrityksiä koskevan lain 2 §:n 6 ja 8 momentti.

([38]) Siltä osin kuin korealaisilla tieto- ja viestintäpalvelujen tarjoajilla olisi suora suhde EU:ssa oleviin henkilöihin (verkkopalveluja tarjoamalla), tämä voisi johtaa asetuksen (EU) 2016/679 suoraan soveltamiseen sen 3 artiklan 2 kohdan a alakohdan nojalla.

([39]) Tietosuojalain 58 §:n 2 momentissa säädetään lisäksi, että 15 ja 22 pykälää, 27 §:n 1–2 momenttia ja 34 ja 37 pykälää ei sovelleta henkilötietojen käsittelyyn, joka tehdään julkisille paikoille asennettujen ja siellä käytettävien visuaalisten tietojenkäsittelylaitteiden avulla. Kyseinen säännös koskee videovalvonnan käyttöä Koreassa eli henkilötietojen suoraa keräämistä Koreassa olevilta henkilöiltä, joten sillä ei ole merkitystä tämän päätöksen kannalta, joka koskee henkilötietojen siirtoja unionin rekisterinpitäjiltä/käsittelijöiltä korealaisille yksiköille. Lisäksi tietosuojalain 58 §:n 3 momentin mukaan 15 pykälää (henkilötietojen kerääminen ja käyttö), 30 pykälää (velvollisuus laatia julkinen tietosuojaseloste) ja 31 pykälää (velvollisuus nimittää tietosuojavastaava) ei sovelleta henkilötietoihin, joita käsitellään ystävyysryhmien tai -yhdistysten (esimerkiksi harrastusseurojen) toiminnan yhteydessä. Koska tällaisia ryhmiä pidetään luonteeltaan henkilökohtaisina eikä niillä ole mitään yhteyttä kaupalliseen tai ammattitoimintaan, jäsenten tietojen keräämiseen ja käyttöön tässä yhteydessä ei tarvita erityistä oikeusperustaa (kuten asianomaisten henkilöiden suostumusta). Kaikkia muita tietosuojalain säännöksiä kuitenkin sovelletaan (esim. tietojen minimointi, käyttötarkoituksen rajoittaminen, käsittelyn lainmukaisuus, turvallisuus ja yksilön oikeudet). Vapautus ei kuitenkaan koske käsittelyä, joka tavalla tai toisella ylittää sen, mikä on tarpeen tällaisen sosiaalisen ryhmän perustamiseksi.

([40]) Tietosuojalain 58 §:n 4 momentissa säädetään erityisesti, että henkilötietoja on käsiteltävä vain sen verran kuin asianomaisen tarkoituksen saavuttamiseksi on tarpeen ja mahdollisimman lyhyen aikaa ja että on toteutettava tarvittavat järjestelyt tällaisten henkilötietojen turvallisen hallinnan ja asianmukaisen käsittelyn varmistamiseksi. Viimeksi mainittu velvoite sisältää tekniset, hallinnolliset ja fyysiset suojatoimet sekä toimenpiteet valitusten asianmukaisen käsittelyn varmistamiseksi.

(27) Ensinnäkin osittainen vapautus kattaa henkilötiedot, jotka kerätään julkisten laitosten käsiteltäväksi tilastolain (*Statistics Act*) nojalla. Korean hallitukselta saatujen selvitysten mukaan tässä yhteydessä käsiteltävät henkilötiedot koskevat yleensä Korean kansalaisia ja sisältäisivät ulkomaalaisten henkilötietoja vain poikkeuksellisesti eli siltä osin kuin on kyse maahantuloa ja maastalähtöä koskevista tilastoista tai ulkomaisista sijoituksista. Myöskään näissä tapauksissa tällaisia tietoja ei kuitenkaan yleensä siirretä unionin rekisterinpitäjiltä/käsittelijöiltä, vaan Korean viranomaiset keräävät ne suoraan ([41]). Lisäksi tilastolain nojalla suoritettavaan tietojenkäsittelyyn sovelletaan useita samankaltaisia edellytyksiä ja suojatoimia kuin ne, joista säädetään asetuksen (EU) 2016/679 johdanto-osan 162 kappaleessa. Tilastolaissa säädetään muun muassa erityisistä velvoitteista, joiden tarkoituksena on varmistaa tietojen täsmällisyys, yhdenmukaisuus ja puolueettomuus, turvata luottamuksellisuus yksilöiden kannalta ja suojata tilastokyselyihin vastanneiden tietoja, myös jotta voidaan estää tietojen käyttö muihin tarkoituksiin kuin tilastojen laatimiseen, ja vahvistaa henkilöstön jäseniä koskevat salassapitovaatimukset ([42]). Tilastoja käsittelevien viranomaisten on noudatettava myös muun muassa tietojen minimoinnin, käyttötarkoituksen rajoittamisen ja turvallisuuden periaatteita (tietosuojalain 3 § ja 58 §:n 4 momentti) ja annettava yksilöille mahdollisuus käyttää oikeuksiaan (pääsy tietoihin ja oikeus oikaista tai poistaa ne ja keskeyttää niiden käsittely, ks. tietosuojalain 4 §). Lisäksi tietoja on käsiteltävä anonymisoidussa tai pseudonymisoidussa muodossa, jos se on käyttötarkoituksen saavuttamiseksi mahdollista (tietosuojalain 3 §:n 7 momentti).

(28) Toiseksi tietosuojalain 58 §:n 1 momentissa viitataan henkilötietoihin, jotka kerätään tai joita pyydetään kansalliseen turvallisuuteen liittyvien tietojen analysointia varten. Tämän osittaisen vapautuksen soveltamisalaa ja seurauksia käsitellään yksityiskohtaisemmin tämän päätöksen johdanto-osan (149) kappaleessa.

(29) Kolmanneksi osittainen vapautus koskee henkilötietojen väliaikaista käsittelyä, silloin kun se on tarpeen kiireellisissä tapauksissa yleiseen turvallisuuteen ja esimerkiksi kansanterveyteen liittyvistä syistä. Tätä tietoluokkaa tulkitaan Korean tietosuojalaissa ahtaasti, ja komission saamien tietojen mukaan sitä ei ole koskaan käytetty. Sitä sovelletaan vain kiireellisiä toimia edellyttävissä hätätapauksissa, esimerkiksi kun on jäljitettävä tartuntatautien aiheuttajia tai luonnonkatastrofien uhrien pelastamiseksi ja auttamiseksi ([43]). Myös tällaisissa tilanteissa osittainen vapautus koskee ainoastaan henkilötietojen väliaikaista käsittelyä toimien toteuttamiseen tarvittavana aikana. Tilanteet, joissa vapautusta voitaisiin soveltaa tämän päätöksen soveltamisalaan kuuluviin tiedonsiirtoihin, ovat vieläkin rajoitetumpia, koska on hyvin epätodennäköistä, että unionista korealaisille toimijoille siirrettävät henkilötiedot olisivat sellaisia, että niiden myöhempi käsittely olisi tarpeen ”kiireellisesti” tällaisissa hätätilanteissa.

(30) Neljänneksi osittaista vapautusta sovelletaan myös silloin kun henkilötietoja keräävät tai käyttävät tiedotusvälineet tai uskonnolliset organisaatiot lähetystyön yhteydessä tai poliittiset puolueet ehdokasasettelua varten. Vapautusta sovelletaan vain siltä osin kuin tiedotusvälineet, uskonnolliset organisaatiot tai poliittiset puolueet käsittelevät henkilötietoja näitä erityistarkoituksia varten (eli journalistinen tai lähetystyöhön liittyvä toiminta ja puolueiden ehdokasasettelu). Jos ne käsittelevät henkilötietoja muita tarkoituksia, kuten henkilöstöhallinnon tai sisäisen hallinnon tarkoituksia varten, sovelletaan tietosuojalakia kaikilta osin.

(31) Kun tiedotusvälineet käsittelevät henkilötietoja journalistisia tarkoituksia varten, sananvapauden ja muiden oikeuksien (mm. oikeus yksityisyyteen) tasapainottamisesta säädetään lehtitietojen aiheuttamien vahinkojen sovittelusta ja niihin liittyvistä oikeussuojakeinoista annetussa laissa (*Act on Arbitration and Remedies, etc. for Damage Caused by Press Reports*), jäljempänä ’joukkoviestintälaki’ ([44]). Joukkoviestintälain 5 §:ssä säädetään esimerkiksi, että tiedotusvälineet (eli lähetystoimintaa harjoittava organisaatio, sanoma- tai aikakauslehti tai verkkojulkaisu), internetin uutispalvelu tai internetissä multimediatuotteita julkaiseva yleisradio-organisaatio ei saa loukata yksilöiden yksityisyyttä. Jos yksityisyydenloukkauksia kuitenkin tapahtuu, ne on korjattava viipymättä laissa säädettyjen

([41]) Tältä osin tilastolain 33 §:ssä vaaditaan, että julkisten laitosten on suojattava tilastokyselyihin vastanneiden tietoja, myös jotta voidaan estää tietojen käyttö muihin tarkoituksiin kuin tilastojen laatimiseen.
([42]) Tilastolain 2 §:n 2–3 momentti, 30 §:n 2 momentti sekä 33 ja 34 §.
([43]) *PIPA Handbook*, 58 pykälää koskeva kohta.
([44]) Esimerkiksi joukkoviestintälain 4 §:ssä säädetään, että lehtitietojen on oltava puolueettomia ja objektiivisia, yleisen edun mukaisia, ihmisarvoa ja arvokkuutta kunnioittavia, eikä niissä saa loukata muita henkilöitä tai heidän oikeuksiaan, yleistä moraalia tai yhteiskuntaetiikkaa.

menettelyjen mukaisesti. Henkilöille, joille on aiheutunut vahinkoa lehtitietojen vuoksi, myönnetään laissa tiettyjä oikeuksia, kuten vastine- ja oikaisuoikeus ja oikeus vaatia täydentävää raportointia (jos henkilön on väitetty syyllistyneen rikokseen, jonka osalta hänet myöhemmin vapautetaan syytteistä) ([45]). Tiedotusvälineet voivat käsitellä yksityishenkilöiden vaatimukset joko suoraan (näitä kysymyksiä käsittelevän valtuutetun välityksellä) ([46]), sovittelu- tai välitysmenettelyllä (erityisessä tiedotusvälineiden välityslautakunnassa (*Press Arbitration Commission*)) ([47]) tai tuomioistuimissa. Yksityishenkilöt voivat myös saada korvausta, jos heille on aiheutunut taloudellista vahinkoa tai jos heidän henkilötietojensa suojaa on loukattu tai heille on aiheutunut muuta henkistä kärsimystä tiedotusvälineiden (tahallisen tai laiminlyönnistä johtuvan) laittoman teon vuoksi ([48]). Tiedotusvälineet on vapautettu lain nojalla vastuusta siltä osin kuin lehtitiedot, joissa puututaan yksilön oikeuksiin, eivät ole sosiaalisten normien vastaisia ja tiedot on julkaistu joko asianomaisen henkilön suostumuksella tai yleisen edun nimissä (ja on olemassa riittävät perusteet katsoa, että tiedot ovat todenmukaisia) ([49]).

(32) Henkilötietojen käsittelyyn journalistisia tarkoituksia varten sovelletaan näin ollen joukkoviestintälain nojalla erityisiä suojatoimia. Sen sijaan uskonnollisia organisaatioita tai poliittisia puolueita koskevien poikkeusten osalta ei ole säädetty tällaisista suojatoimista samalla tavoin kuin asetuksen (EU) 2016/679 85, 89 ja 91 artiklassa. Sen vuoksi komissio katsoo aiheelliseksi sulkea tämän päätöksen soveltamisalan ulkopuolelle uskonnolliset organisaatiot siltä osin kuin ne käsittelevät henkilötietoja lähetystyöhön liittyviä tarkoituksia varten ja poliittiset puolueet siltä osin kuin ne käsittelevät henkilötietoja ehdokasasettelua varten.

2.3 **Suojatoimet, oikeudet ja velvollisuudet**

2.3.1 *Tietojenkäsittelyn lainmukaisuus ja asianmukaisuus*

(33) Henkilötietojen käsittelyn olisi oltava lainmukaista ja asianmukaista.

(34) Tämä periaate todetaan Korean tietosuojalain 3 §:n 1 ja 2 momentissa, minkä lisäksi se vahvistetaan myös lain 59 §:ssä, jossa kielletään henkilötietojen käsittely ”petoksella tai epäasianmukaisin tai perusteettomin keinoin”, ”ilman oikeudellisia toimivaltuuksia” tai ”toimivaltuudet ylittäen” ([50]). Näitä lainmukaisen käsittelyn yleisiä periaatteita täsmennetään tietosuojalain 15–19 §:ssä, joissa esitetään käsittelyn eri oikeusperustat (tietojen kerääminen, käyttö ja luovuttaminen kolmansille osapuolille) sekä edellytykset, joiden täyttyessä käyttötarkoitus voi muuttua (18 §).

([45]) Joukkoviestintälain 15–17 §.

([46]) Jokaisella tiedotusvälineellä on oltava oma valtuutettu, jonka tehtävänä on ehkäistä ja korjata tiedotusvälineen toiminnasta mahdollisesti aiheutuvat vahingot (esim. antamalla suosituksia virheellisten tai muiden mainetta vahingoittavien lehtitietojen oikaisemisesta), ks. joukkoviestintälain 6 §.

([47]) Välityslautakuntaan kuuluu 40–90 jäsentä, jotka kulttuuri-, urheilu- ja matkailuministeri nimittää. Tehtävään voidaan valita tuomareita, asianajajia ja henkilöitä, jotka ovat osallistuneet uutisten keräämiseen tai raportointiin vähintään 10 vuoden ajan tai joilla on muuta tiedotusvälineiden toimintaan liittyvää asiantuntemusta. Välityslautakunnan jäsenet eivät voi samanaikaisesti olla virkamiehiä, poliittisten puolueiden jäseniä tai toimittajia. Joukkoviestintälain 8 §:n mukaan välityslautakunnan jäsenten on suoritettava tehtävänsä itsenäisesti eivätkä he saa ottaa vastaan mitään ohjeita näihin tehtäviin liittyen. Lisäksi käytössä on erityiset säännöt, joiden tarkoituksena on estää eturistiriidat. Lautakunnan jäsenet eivät esimerkiksi saa käsitellä tapauksia, joissa on osallisena heidän puolisonsa tai sukulaisensa (joukkoviestintälain 10 §). Lautakunta voi käsitellä riita-asiat joko sovittelu- tai välitysmenettelyssä tai antaa suosituksia rikkomusten korjaamiseksi (joukkoviestintälain 5 §).

([48]) Joukkoviestintälain 30 §.

([49]) Joukkoviestintälain 5 §.

([50]) Tietosuojalain 59 §:ssä kielletään kaikkia henkilöitä, ”jotka käsittelevät tai ovat joskus käsitelleet henkilötietoja – – hankkimasta henkilötietoja tai suostumusta henkilötietojen käsittelyyn petoksella tai epäasianmukaisin tai perusteettomin keinoin”, ”paljastamasta liiketoiminnan yhteydessä saatuja henkilötietoja tai luovuttamasta niitä kolmannen osapuolen käyttöön ilman valtuutusta”. Lisäksi kielletään ”toisen henkilön tietojen vahingoittaminen, tuhoaminen, muuttaminen, väärentäminen tai paljastaminen ilman oikeudellista valtuutusta tai valtuudet ylittäen”. Kiellon rikkominen voi johtaa rikosoikeudellisten seuraamusten määräämiseen, ks. tietosuojalain 71 §:n 5 ja 6 momentti sekä 72 §:n 2 momentti. Tietosuojalain 70 §:n 2 momentin nojalla on lisäksi mahdollista määrätä rikosoikeudellinen rangaistus sellaisten henkilötietojen hankkimisesta, joita kolmannet osapuolet ovat käsitelleet petoksella tai muilla perusteettomilla keinoilla tai menetelmillä, tai tietojen luovuttamisesta kolmannelle osapuolelle voitontavoittelua tai perusteettomia tarkoituksia varten, sekä yllyttämisestä tällaiseen toimintaan tai tällaisen toiminnan järjestämisestä.

(35) Tietosuojalain 15 §:n 1 momentin mukaan rekisterinpitäjä voi kerätä henkilötietoja (keräämisen käyttötarkoituksen puitteissa) vain tietyin oikeudellisin perustein. Näitä ovat 1) rekisteröidyn suostumus ([51]) (1 kohta); 2) sopimuksen tekeminen rekisteröidyn kanssa ja sen täytäntöönpano (4 kohta); 3) lakiin perustuva erityislupa tai lakisääteisen velvoitteen noudattaminen (2 kohta); julkisen laitoksen tarve ([52]) suorittaa lakisääteiset tehtävänsä sille annetun toimivallan puitteissa; 4) ilmeinen tarve suojella rekisteröidyn tai kolmannen osapuolen henkeä, terveyttä tai omaisuutta välittömältä vaaralta (vain jos rekisteröity ei itse kykene ilmaisemaan tahtoaan tai ennakkosuostumusta ei ole mahdollista saada) (5 kohta); 5) tarve toteuttaa rekisterinpitäjän ”perusteltu etu”, jos se on ”selvästi suurempi” kuin rekisteröidyn etu (ja vain jos käsittelyllä on ”olennainen yhteys” oikeutettuun etuun eikä se ylitä sitä, mikä on kohtuullista) (6 kohta) ([53]). Nämä käsittelyperusteet vastaavat olennaisilta osin asetuksen (EU) 2016/679 6 artiklassa säädettyjä perusteita, sillä myös viimeksi mainittu ”perusteltu etu” vastaa asetuksen 6 artiklan 1 kohdan f alakohdassa tarkoitettua ”oikeutettua etua”.

(36) Kun henkilötiedot on kerätty, niitä voidaan käyttää keräämistarkoituksen puitteissa (tietosuojalain 15 §:n 1 momentti) tai keräämistarkoitukseen ”kohtuudella liittyvissä puitteissa”, ottaen huomioon rekisteröidylle mahdollisesti aiheutuvat haitat ja edellyttäen, että tarvittavat turvatoimet (esim. salaus) on toteutettu (tietosuojalain 15 §:n 3 momentti). Sen määrittämiseksi, millainen käyttötarkoitus ”kohtuudella liittyy” alkuperäisen keräämistarkoitukseen, tietosuojalain täytäntöönpanoasetuksessa vahvistetaan erityiset kriteerit, jotka vastaavat asetuksen (EU) 2016/679 6 artiklan 4 kohdassa esitettyjä vaatimuksia. Tässä yhteydessä edellytetään erityisesti, että uusi käyttötarkoitus on alkuperäisen tarkoituksen kannalta huomattavan relevantti; uuden käyttötarkoituksen on oltava ennustettavissa (esimerkiksi niiden olosuhteiden perusteella, joissa tiedot kerättiin); ja tiedot on mahdollisuuksien mukaan pseudonymisoitava ([54]). Kriteerit, joita rekisterinpitäjä soveltaa tässä arvioinnissa, on ilmoitettava etukäteen tietosuojaselosteessa ([55]). Lisäksi tietosuojavastaavalle (ks. johdanto-osan kappale (94)) asetetaan nimenomaisesti velvoite tarkistaa, että myöhempi käsittely tapahtuu näiden edellytysten puitteissa.

([51]) Suostumuksen on oltava vapaaehtoinen, tietoinen ja yksilöity, ja se on ilmaistava jollakin laissa ennalta määrätyllä tavalla. Suostumusta ei saa missään tapauksessa hankkia petoksella tai epäasianmukaisin tai perusteettomin keinoin (tietosuojalain 59 §:n 1 momentti). Ensinnäkin rekisteröidyillä on tietosuojalain 4 §:n 2 kohdan mukaan oikeus ”suostua tai olla suostumatta” ja ”valita suostumuksen laajuus”, ja heille olisi annettava sitä koskevat tiedot (tietosuojalain 15 §:n 2 momentti, 16 §:n 2 ja 3 momentti, 17 §:n 2 momentti ja 18 §:n 3 momentti). Tietosuojalain 22 §:n 5 momentissa esitetään lisää suojatoimia kieltämällä rekisterinpitäjää epäämästä tavaroiden tai palvelujen toimittamista, jos tämä voisi heikentää yksilön valinnanvapautta suostumuksen antamisessa. Tämä koskee tilanteita, joissa vain tietyntyyppinen käsittely edellyttää suostumusta (kun taas toiset perustuvat sopimukseen), ja kattaa myös tavaroiden tai palvelujen toimittamisen yhteydessä kerättyjen henkilötietojen myöhemmän käsittelyn. Toiseksi rekisterinpitäjän on tietosuojalain 15 §:n 2 momentin, 17 §:n 2 ja 3 momentin ja 18 §:n 3 momentin mukaan ilmoitettava rekisteröidylle käsiteltävien henkilötietojen ”yksityiskohdat” (kuten se, että on kyse arkaluonteisista tiedoista, ks. tietosuojalain täytäntöönpanoasetuksen 17 §:n 2 momentin 2 a kohta), käsittelyn tarkoitus, tietojen säilyttämisaika ja mahdolliset tietojen vastaanottajat. Tällaiset pyynnöt on esitettävä ”nimenomaisen tunnistettavasti”, eli erottamalla suostumusta edellyttävät asiat niistä, joihin sitä ei tarvita (tietosuojalain 22 §:n 1–4 momentti). Kolmanneksi tietosuojalain täytäntöönpanoasetuksen 17 §:n 1 momentin 1–6 kohdassa säädetään, millä tavoin rekisterinpitäjän on hankittava suostumus. Esimerkiksi kirjallinen suostumus voidaan hankkia rekisteröidyn allekirjoituksen tai sähköpostivastauksen muodossa. Tietosuojalaissa ei anneta yksilöille yleistä oikeutta peruuttaa suostumuksensa, vaan heillä on sen sijaan oikeus vaatia henkilötietojensa käsittelyn keskeyttämistä, minkä seurauksena käsittely lopetetaan ja tiedot tuhotaan (ks. johdanto-osan 78 kappale, jossa käsitellään oikeutta keskeyttää käsittely).

([52]) Tietosuojalautakunnalta saatujen tietojen mukaan julkiset laitokset voivat vedota tähän perusteeseen vain jos henkilötietojen käsittely on välttämätöntä, eli kyseisen laitoksen olisi mahdotonta tai kohtuuttoman vaikeaa hoitaa tehtävänsä ilman asianomaisten tietojen käsittelyä.

([53]) Tietosuojalain 39-3 §:ssä asetetaan tieto- ja viestintäpalvelujen tarjoajille erityiset (tiukemmat) velvoitteet näiden palvelujen käyttäjien henkilötietojen keräämistä ja käyttöä varten. Siinä edellytetään erityisesti, että palveluntarjoaja hankkii käyttäjän suostumuksen annettuaan tälle tietoa henkilötietojen keräämisen/käytön tarkoituksesta sekä siitä, mitä tietoja kerätään ja kuinka kauan niitä käsitellään (tietosuojalain 39-3 §:n 1 momentti). Sama pätee myös silloin, kun mikä tahansa näistä seikoista muuttuu. Suostumuksen hankkimista koskevan velvoitteen laiminlyönnistä voidaan määrätä rikosoikeudellisia seuraamuksia (tietosuojalain 71 §:n 4–5 momentti). Poikkeustapauksissa tieto- ja viestintäpalvelujen tarjoajat voivat kerätä tai käyttää käyttäjien henkilötietoja myös ilman ennakkosuostumusta. Näin on 1) silloin kun tavanomaista suostumusta on taloudellisista ja teknisistä syistä selvästi vaikea saada sellaisten henkilötietojen osalta, joita tarvitaan tieto- ja viestintäpalvelujen tarjoamista koskevan sopimuksen täytäntöönpanoa varten (esimerkiksi kun henkilötietoja saadaan väistämättä sopimuksen täyttämisen, kuten laskutus- ja maksutietojen sekä päätylokien yhteydessä); 2) kun se on tarpeen tieto- ja viestintäpalvelujen tarjoamisesta aiheutuvien maksujen suorittamiseksi; tai 3) kun se on mahdollista muiden lakien nojalla (esimerkiksi sähköistä kaupankäyntiä koskevan kuluttajansuojalain (*Act on Consumer Protection in Electronic Commerce*) 21 §:n 1 momentin 6 kohdassa säädetään, että elinkeinonharjoittajat voivat kerätä henkilötietoja alaikäisen lailliselta huoltajalta sen varmistamiseksi, että alaikäisen puolesta on saatu pätevä suostumus) (tietosuojalain 39-3 §:n 2 momentti). Tieto- ja viestintäpalvelujen tarjoajat eivät missään tapauksessa voi kieltäytyä tarjoamasta palveluja pelkästään sillä perusteella, että käyttäjä antaa vain vaaditut vähimmäistiedot (eli tiedot, jotka tarvitaan asianomaisen palvelun olennaisten osien suorittamiseksi), ks. tietosuojalain 39-3 §:n 3 momentti.

([54]) Tietosuojalain täytäntöönpanoasetuksen 14-2 §.

([55]) Tietosuojalain täytäntöönpanoasetuksen 14-2 §:n 2 momentti.

(37) Samantapaisia (mutta tiukempia) sääntöjä sovelletaan tietojen luovuttamiseen kolmannelle osapuolelle. Tietosuojalain 17 §:n 1 momentin mukaan henkilötietojen luovuttaminen kolmannelle osapuolelle on sallittua suostumuksen perusteella ([56]) tai keräämistarkoituksen puitteissa, jos tiedot on kerätty jonkin tietosuojalain 15 §:n 1 momentin 2, 3 tai 5 kohdassa mainitun oikeusperustan nojalla. Tämä sulkee pois erityisesti tietojen luovuttamisen rekisterinpitäjän ”perustellun edun” perusteella. Tämän lisäksi tietosuojalain 17 §:n 4 momentissa sallitaan tietojen luovuttaminen kolmannelle osapuolelle keräämistarkoitukseen ”kohtuudella liittyvissä puitteissa”, ottaen jälleen huomioon rekisteröidylle mahdollisesti aiheutuvat haitat ja edellyttäen, että tarvittavat turvatoimet (esim. salaus) on toteutettu. Johdanto-osan (36) kappaleessa kuvatut tekijät on otettava huomioon myös arvioitaessa sitä, kattavatko keräämistarkoitus ja siihen liittyvät suojatoimet kohtuullisesti myös luovuttamisen (eli arvioimalla tietosuojapolitiikan läpinäkyvyyttä ja tietosuojavastaavan osallistumista).

(38) Se, että korealainen rekisterinpitäjä ottaa vastaan henkilötietoja unionista, katsotaan tietosuojalain 15 §:ssä tarkoitetuksi ”keräämiseksi”. Ilmoituksessa N:o 2021-5 (tämän päätöksen liitteessä I oleva I jakso) selvennetään, että tarkoitus, jota varten asianomainen EU:n yksikkö siirsi tiedot, on korealaisen rekisterinpitäjän kannalta tietojen keräämistarkoitus. Tästä seuraa, että henkilötietoja unionista vastaanottavien korealaisten rekisterinpitäjien on periaatteessa käsiteltävä kyseisiä tietoja siirron tarkoituksen mukaisesti, kuten tietosuojalain 17 §:ssä säädetään.

(39) Erityisiä rajoituksia sovelletaan, jos rekisterinpitäjä aikoo käyttää henkilötietoja tai luovuttaa ne kolmannelle osapuolelle muuhun kuin keräämistarkoitukseen ([57]). Tietosuojalain 18 §:n 2 momentin mukaan yksityinen rekisterinpitäjä voi poikkeuksellisesti ([58]) käyttää henkilötietoja tai luovuttaa ne kolmannelle osapuolelle eri tarkoitukseen 1) rekisteröidyn täydentävän (erillisen) suostumuksen perusteella; 2) jos tästä säädetään erityissäännöksissä; tai 3) jos se on ilmeisen tarpeellista, jotta voidaan suojella rekisteröidyn tai kolmannen osapuolen henkeä, terveyttä tai omaisuutta välittömältä vaaralta (vain jos rekisteröity ei itse kykene ilmaisemaan tahtoaan tai ennakkosuostumusta ei ole mahdollista saada) ([59]).

(40) Myös julkiset laitokset voivat tietyissä tilanteissa käyttää henkilötietoja tai luovuttaa niitä kolmannelle osapuolelle muuta kuin alkuperäistä tarkoitusta varten. Näin on muun muassa silloin kun niiden olisi muutoin mahdotonta hoitaa lakisääteiset tehtävänsä laissa säädetyllä tavalla, edellyttäen että tietosuojalautakunta antaa luvan. Julkiset laitokset voivat myös luovuttaa henkilötietoja toiselle viranomaiselle tai tuomioistuimelle, jos se on tarpeen rikosten tutkintaa ja syytteeseenpanoa varten tai jotta tuomioistuin voi hoitaa käynnissä olevaan oikeudenkäyntiin liittyvät tehtävänsä tai rikosoikeudellisen rangaistuksen tai huostaanotto- tai säilöönottomääräyksen täytäntöönpanoa varten ([60]). Julkiset laitokset voivat myös luovuttaa henkilötietoja vieraan valtion hallitukselle tai kansainväliselle organisaatiolle perussopimukseen tai kansainväliseen sopimukseen perustuvan oikeudellisen velvoitteen noudattamiseksi; tällöin niiden on noudatettava rajatylittäville tiedonsiirroille asetettuja vaatimuksia (ks. johdanto-osan (90) kappale).

(41) Tämä tarkoittaa, että käsittelyn lainmukaisuuden ja asianmukaisuuden periaatteet on pantu Korean oikeudellisessa kehyksessä täytäntöön olennaisilta osin asetusta (EU) 2016/679 vastaavalla tavalla, eli sallimalla käsittely ainoastaan oikeutettujen ja selkeästi määriteltyjen perusteiden nojalla. Lisäksi käsittely sallitaan kaikissa mainituissa tapauksissa vain jos se todennäköisesti ei ”loukkaa oikeudettomasti” rekisteröidyn tai kolmannen osapuolen etuja, mikä edellyttää etujen tasapainottamista. Lisäksi tietosuojalain 18 §:n 5 momentissa säädetään täydentävistä suojatoimista silloin kun rekisterinpitäjä luovuttaa henkilötietoja kolmannelle osapuolelle. Tämä voi edellyttää käyttötarkoituksen tai -tavan rajoittamista tai erityisten turvatoimien toteuttamista. Myös kolmannen osapuolen on puolestaan toteutettava vaaditut toimenpiteet.

([56]) Tietosuojalain 17 §:n 1 momentin 1 kohdan rikkominen voi johtaa rikosoikeudellisten seuraamusten määräämiseen (tietosuojalain 71 §:n 1 momentti).

([57]) ”Aiottu tarkoitus” on tarkoitus, jota varten tiedot kerättiin. Jos tiedot esimerkiksi kerättiin asianomaisen henkilön suostumuksella, aiottu tarkoitus on se, joka hänelle ilmoitettiin tietosuojalain 15 §:n 2 momentin nojalla.

([58]) Vrt. tietosuojalain 18 §:n 1 momentti. Tietosuojalain 18 §:n 1 ja 2 momentin rikkominen voi johtaa rikosoikeudellisten seuraamusten määräämiseen (tietosuojalain 71 §:n 2 momentti).

([59]) Tieto- ja viestintäpalvelujen tarjoajat voivat käyttää henkilötietoja tai luovuttaa niitä kolmannelle osapuolelle muuta kuin alkuperäistä tarkoitusta varten vain tietosuojalain 18 §:n 2 momentin 1 ja 2 kohdassa esitettyjen perusteiden nojalla (eli kun on saatu täydentävä suostumus tai asiasta on erikseen säädetty). Ks. tietosuojalain 18 §:n 2 momentti.

([60]) Lukuun ottamatta tapauksia, joissa käsittely on tarpeen rikosten tutkintaa tai syytteeseenpanoa varten, julkisten laitosten, jotka käyttävät henkilötietoja tai luovuttavat niitä kolmannelle osapuolelle muuta kuin keräämistarkoitusta varten (esimerkiksi silloin kun se on laissa erikseen sallittu tai kun se on tarpeen sopimuksen täytäntöönpanoa varten), on julkaistava käsittelyn oikeusperustat, sen tarkoitus ja soveltamisala verkkosivustollaan tai virallisessa lehdessä ja pidettävä kirjaa käsittelytoimista (tietosuojalain 18 §:n 4 momentti yhdessä sen täytäntöönpanoasetuksen 15 §:n kanssa).

(42) Lopuksi todetaan, että tietosuojalain 28-2 §:ssä sallitaan pseudonymisoitujen tietojen (myöhempi) käsittely ilman asianomaisen henkilön suostumusta tilastollisia ja tieteellisiä tarkoituksia varten ([61]) sekä tietojen arkistointi yleisen edun mukaisia tarkoituksia varten, edellyttäen että noudatetaan erityisiä suojatoimia. Samoin kuin asetuksella (EU) 2016/679 ([62]), myös Korean tietosuojalailla helpotetaan näin henkilötietojen (myöhempää) käsittelyä tällaisia tarkoituksia varten, edellyttäen että käytössä on asianmukaiset suojatoimet yksilöiden oikeuksien suojaamiseksi. Sen sijaan että tietosuojalaissa säädettäisiin pseudonymisoinnista mahdollisena suojatoimena, siinä asetetaan se ennakkoedellytykseksi tietyille käsittelytoimille, jotka liittyvät tilastollisiin ja tieteellisiin tarkoituksiin ja yleisen edun mukaisiin arkistointitarkoituksiin (sen ansiosta tietoja voidaan käsitellä ilman suostumusta tai yhdistää eri tietokokonaisuuksia).

(43) Lisäksi tietosuojalaissa säädetään useista erityisistä suojatoimista, jotka koskevat erityisesti vaadittuja teknisiä ja organisatorisia toimenpiteitä, tietojen kirjaamista, tietojen yhteiskäyttöä koskevia rajoituksia ja mahdolliseen uudelleentunnistamiseen liittyviä riskejä. Johdanto-osan (44) – (48) kappaleessa esitettyjen eri suojatoimien yhdistelmällä varmistetaan, että henkilötietojen käsittelyyn sovelletaan tässä yhteydessä olennaisilta osin samanlaisia suojatoimia kuin ne, joita edellytetään asetuksen (EU) 2016/679 mukaisesti.

(44) Ensimmäiseksi on mainittava tärkein seikka eli se, että tietosuojalain 28-5 §:n 1 momentissa kielletään pseudonymisoitujen tietojen käsittely yksittäisen henkilön tunnistamiseksi. Jos pseudonymisoitujen tietojen käsittelyn yhteydessä kuitenkin syntyy tietoja, jotka saattaisivat johtaa yksittäisen henkilön tunnistamiseen, rekisterinpitäjän on välittömästi keskeytettävä käsittely ja tuhottava tällaiset tiedot (tietosuojalain 28-5 §:n 2 momentti). Näiden säännösten laiminlyönti on rikos, josta voidaan määrätä hallinnollisia sakkoja ([63]). Tämä tarkoittaa, että myös niissä tilanteissa, joissa yksittäisen henkilön tunnistaminen olisi *käytännössä* mahdollista, se on *oikeudellisesti* kielletty.

(45) Toiseksi, kun on kyseessä pseudonymisoitujen tietojen (myöhempi) käsittely tällaisia tarkoituksia varten, rekisterinpitäjän on toteutettava erityiset tekniset, hallinnolliset ja fyysiset suojatoimet tietojen turvallisuuden varmistamiseksi (muun muassa säilyttämällä ja hallinnoimalla erikseen niitä tietoja, jotka ovat tarpeen pseudonymisoitujen tietojen palauttamiseksi alkuperäiseen tilaansa) ([64]). Lisäksi on pidettävä kirjaa käsitellyistä pseudonymisoiduista tiedoista, käsittelytarkoituksesta, käyttöhistoriasta ja mahdollisista kolmansista osapuolista, joille tietoja on luovutettu (tietosuojalain täytäntöönpanoasetuksen 29-5 §:n 2 momentti).

(46) Kolmantena ja viimeisenä seikkana tietosuojalaissa säädetään erityisistä suojatoimista, jotta voidaan estää kolmansia osapuolia tunnistamasta yksittäisiä henkilöitä siinä tapauksessa, että tietoja luovutetaan niille. Erityisesti säädetään, että silloin kun pseudonymisoituja tietoja luovutetaan kolmannelle osapuolelle tilastointia, tieteellistä tutkimusta tai yleisen edun mukaista arkistointia varten, rekisterinpitäjä ei saa sisällyttää luovutettaviin tietoihin tietoja, joita voitaisiin käyttää yksittäisen henkilön tunnistamiseen (tietosuojalain 28-2 §:n 2 momentti) ([65]).

(47) Mainittakoon myös, että vaikka tietosuojalaissa sallitaan (eri rekisterinpitäjien käsittelemien) pseudonymisoitujen tietojen yhdistäminen tilastointia, tieteellistä tutkimusta tai yleisen edun mukaista arkistointia varten, nämä valtuudet varataan siinä tähän erikoistuneille laitoksille, joilla on käytössään erityiset turvajärjestelyt (tietosuojalain 28-3 §:n 1 momentti) ([66]). Kun rekisterinpitäjä hakee pseudonymisoitujen tietojen yhdistämistä, sen on toimitettava dokumentaatio muun muassa yhdistettävistä tiedoista ja yhdistämisen tarkoituksesta sekä yhdistettyjen tietojen

([61]) Tietosuojalain 2 §:n 8 momentissa olevan määritelmän mukaan tieteellisellä tutkimuksella tarkoitetaan ”tutkimusta, jossa sovelletaan tieteellisiä menetelmiä, kuten teknologian kehittämistä ja esittelyä, perustutkimusta, soveltavaa tutkimusta ja yksityisin varoin rahoitettua tutkimusta”. Määritelmä vastaa asetuksen (EU) 2016/679 johdanto-osan 159 kappaleessa lueteltuja seikkoja.

([62]) Ks. asetuksen (EU) 2016/679 5 artiklan 1 kohdan b alakohta ja 89 artiklan 1–2 kohta sekä johdanto-osan 50 ja 157 kappale.

([63]) Ks. tietosuojalain 28-6 §:n 1 momentti, 71 §:n 4–3 momentti ja 75 §:n 2 momentin 4-4 kohta.

([64]) Tietosuojalain täytäntöönpanoasetuksen 28-4 ja 29-5 §. Tämän velvoitteen laiminlyönti voi johtaa hallinnollisten ja rikosoikeudellisten sakkojen määräämiseen, ks. tietosuojalain 73 §:n 1 momentti ja 75 §:n 2 momentin 6 kohta.

([65]) Näiden vaatimusten rikkominen voi johtaa rikosoikeudellisten seuraamusten määräämiseen (tietosuojalain 71 §:n 2 momentti). Korean tietosuojalautakunta aloitti näiden uusien sääntöjen noudattamisen valvonnan välittömästi muun muassa antamalla 28. huhtikuuta 2021 päätöksen, jossa se määräsi sakkoja ja korjaavia toimenpiteitä yritykselle, joka muiden tietosuojalain säännösten rikkomisen ohella ei noudattanut lain 28-2 §:n 2 momenttia, ks. https://www.pipc.go.kr/np/cop/bbs/selectBoardArticle.do?bbsId=BS074&mCode=C020010000&nttId=7298&fbclid=IwAR3SKcMQi6G5pR9k4I7j6GNXtc8aBVDOwcURevvvzQtYI7AS40UKYXoOXo8.

([66]) Nimeämistä tällaiseksi erikoistuneeksi laitokseksi (*Expert Data Combination Agency*) haetaan tietosuojalautakunnalta hakemuksella, johon liitetään muun muassa tiedot tiloista ja laitteista, joiden avulla pseudonymisoitujen tietojen yhdistäminen voidaan suorittaa turvallisesti, ja jossa vahvistetaan, että hakijalla on palveluksessaan vähintään kolme kokoaikaista työntekijää, joilla on henkilötietojen suojaan liittyvä pätevyys tai kokemus (tietosuojalain täytäntöönpanoasetuksen 29-2 §:n 1 ja 2 momentti). Yksityiskohtaiset vaatimukset, jotka koskevat esimerkiksi henkilöstön pätevyyttä, käytettävissä olevia tiloja, turvatoimia, sisäisiä toimintaperiaatteita ja menettelyjä sekä toiminnan rahoitusta, on vahvistettu tietosuojalautakunnan ilmoituksessa N:o 2020-9, joka koskee pseudonymisoitujen tietojen yhdistämistä ja luovuttamista (*Combination and Release of Pseudonymised Information (Schedule I)*). Tietosuojalautakunta voi peruuttaa nimeämisen (kuulemisen jälkeen) tietyin perustein, esimerkiksi jos laitos ei enää täytä asetettuja turvallisuusvaatimuksia tai jos tietoja yhdistettäessä on tapahtunut tietoturvaloukkaus (tietosuojalain täytäntöönpanoasetuksen 29-2 §:n 5 ja 6 momentti). Tietosuojalautakunnan on julkaistava tiedot kaikista nimeämisistä (ja nimeämisen peruutuksista) (tietosuojalain täytäntöönpanoasetuksen 29-2 §:n 7 momentti).

käsittelyä varten ehdotetuista turvatoimista ([67]). Jotta tietojen yhdistäminen voitaisiin hyväksyä, rekisterinpitäjän on lähetettävä tiedot erikoistuneelle laitokselle ja toimitettava pseudonymisoinnissa käytetty ”yhdistelmäavain” Korean internet- ja turvallisuusvirastolle (*Internet and Security Agency*) ([68]). Virasto luo tähän yhdistelmäavaimeen liittyvät linkkitiedot (joiden avulla eri hakijoiden yhdistelmäavaimet voidaan linkittää toisiinsa tietokokonaisuuksien yhdistämiseksi) ja toimittaa ne erikoistuneelle laitokselle ([69]).

(48) Yhdistämistä pyytävä rekisterinpitäjä voi analysoida yhdistettyjä tietoja erikoistuneen laitoksen tiloissa, joissa sovelletaan erityisiä teknisiä, fyysisiä ja hallinnollisia turvatoimia (tietosuojalain täytäntöönpanoasetuksen 29-3 §). Rekisterinpitäjät, jotka toimittavat jonkin tietokokonaisuuden tällaista yhdistämistä varten, voivat viedä yhdistetyt tiedot erikoistuneen laitoksen ulkopuolelle vasta kun yhdistetyt tiedot on pseudonymisoitu tai anonymisoitu uudestaan ja asianomaisen laitoksen luvalla (tietosuojalain 28-3 §:n 2 momentti) ([70]). Luvan myöntämistä varten laitos arvioi yhdistettyjen tietojen ja käsittelytarkoituksen välisiä yhteyksiä ja tarkistaa, onko tällaisten tietojen käyttöä varten laadittu erityinen turvallisuussuunnitelma ([71]). Yhdistettyjä tietoja ei saa viedä laitoksen ulkopuolelle, jos niihin sisältyy tietoja, jotka voivat johtaa yksittäisen henkilön tunnistamiseen ([72]). Myös tietosuojalautakunta valvoo erikoistuneen laitoksen toteuttamaa pseudonymisoitujen tietojen yhdistämistä ja luovuttamista (tietosuojalain täytäntöönpanoasetuksen 29-4 §:n 3 momentti).

2.3.2 *Erityisten henkilötietoryhmien käsittely*

(49) ”Erityisiä tietoryhmiä” käsiteltäessä olisi sovellettava erityisiä suojatoimia.

(50) Korean tietosuojalaissa säädetään erikseen arkaluonteisten tietojen ([73]) käsittelystä. Tällaiset tiedot ovat henkilötietoja, jotka paljastavat yksittäisen henkilön poliittiseen tai uskonnolliseen vakaumukseen, ammattiliiton tai puolueen jäsenyyteen tai siitä eroamiseen, poliittisiin mielipiteisiin, terveydentilaan tai sukupuolielämään liittyviä tietoja tai muita henkilökohtaisia tietoja, joiden paljastuminen todennäköisesti vaarantaisi ”huomattavasti” hänen yksityisyytensä ja jotka on määritelty arkaluonteisiksi presidentin asetuksella ([74]). Tietosuojalautakunnalta saatujen selvitysten mukaan sukupuolielämää koskevien tietojen katsotaan kattavan myös yksilön seksuaalisen suuntautumisen ja seksuaaliset mieltymykset ([75]). Tietosuojalain täytäntöönpanoasetuksen 18 §:ssä määritetään myös muita arkaluonteisia tietoryhmiä, kuten geneettisistä testeistä saadut DNA-tiedot ja rikosrekisteritiedot. Tietosuojalain täytäntöönpanoasetuksen äskettäisen muutoksen yhteydessä arkaluonteisten tietoryhmien käsitettä on edelleen laajennettu sisällyttämällä siihen myös henkilötiedot, joista käy ilmi rotu tai etninen alkuperä, ja biometriset tiedot ([76]). Tämän muutoksen tuloksena tietosuojalaissa esitetty arkaluonteisten tietojen käsite vastaa olennaisilta osin asetuksen (EU) 2016/679 9 artiklassa olevaa käsitettä.

(51) Tietosuojalain 23 §:n 1 momentin mukaan ja samaan tapaan kuin asetuksen (EU) 2016/679 9 artiklan 1 kohdassa säädetään, arkaluonteisten tietojen käsittely on pääsääntöisesti kielletty, ellei sovelleta jotakin erikseen mainittua poikkeusta ([77]). Kyseisissä poikkeuksissa rajoitetaan käsittely tapauksiin, joissa rekisterinpitäjä ilmoittaa siitä rekisteröidylle tietosuojalain 15 ja 17 §:n mukaisesti ja saa tältä erillisen suostumuksen (erillisen suhteessa muiden henkilötietojen käsittelyä koskevaan suostumukseen), tai joissa käsittelyä edellytetään tai se sallitaan lain nojalla. Myös viranomaiset voivat käsitellä biometrisiä tietoja, geneettisistä testeistä saatuja DNA-tietoja,

([67]) *Notification 2020-9 on Combination and Release of Pseudonymised Information*, 8 §:n 1–2 momentti.
([68]) *Notification 2020-9 on Combination and Release of Pseudonymised Information*, 2 §:n 3 ja 6 momentti ja 9 §:n 1 momentti.
([69]) *Notification 2020-9 on Combination and Release of Pseudonymised Information*, 2 §:n 4 momentti ja 9 §:n 2–3 momentti. Erikoistuneen laitoksen on tuhottava yhdistelmäavaimeen liittyvät linkkitiedot välittömästi yhdistämisen jälkeen (*Notification*, 9 §:n 4 momentti).
([70]) Tietokokonaisuuksien yhdistämistä koskevien vaatimusten rikkominen voi johtaa rikosoikeudellisten seuraamusten määräämiseen (tietosuojalain 71 §:n 4-2 momentti). Ks. myös tietosuojalain täytäntöönpanoasetuksen 29-2 §:n 4 momentti.
([71]) Yhdistettyjen tietojen luovuttamismenettely esitetään asiaa koskevan ilmoituksen (*Notification 2020-9 on Combination and Release of Pseudonymised Information*) 11 §:ssä. Erikoistuneen laitoksen on muun muassa perustettava erityinen luovuttamista käsittelevä tarkastelukomitea (*release review committee*), jonka jäsenillä on oltava perusteelliset tiedot ja kokemus tietosuojasta.
([72]) Tietosuojalain täytäntöönpanoasetuksen 29-2 §:n 4 momentti ja ilmoitus N:o 2020-9, 11 §.
([73]) Myös Korean perustuslakituomioistuin on tunnustanut tarpeen varmistaa erityisen vahva suojelu silloin kun käsitellään arkaluonteisia eli esimerkiksi terveydentilaa tai sukupuolista käyttäytymistä koskevia tietoja, ks. perustuslakituomioistuimen päätös HunMa 1139, 31.5.2007.
([74]) Tietosuojalain 23 §:n 1 momentti.
([75]) Ks. myös *PIPA Handbook*, lll luvun 2 kohta, jossa tarkastellaan tietosuojalain 23 pykälää (s. 157–164).
([76]) Tällä tarkoitetaan henkilötietoja, jotka perustuvat erityiseen tekniseen tietojenkäsittelyyn, joka koskee yksilön fyysisiä, fysiologisia tai käyttäytymiseen liittyviä ominaisuuksia kyseisen henkilön yksiselitteistä tunnistamista varten.
([77]) Näiden vaatimusten laiminlyönti voi johtaa seuraamusten määräämiseen tietosuojalain 71 §:n 3 kohdan nojalla.

rodun tai etnisen alkuperän paljastavia henkilötietoja ja rikosrekisteritietoja yksinomaan näiden viranomaisten käytettävissä olevien perusteiden nojalla (esimerkiksi jos käsittely on tarpeen rikostutkintaa tai käynnissä olevan oikeuskäsittelyn jatkamista varten) ([78]). Arkaluonteisten tietojen käsittelyä varten on yleensä käytettävissä vähemmän oikeusperustoja kuin muuntyyppisten henkilötietojen käsittelyä varten, ja Korean lainsäädännössä ne ovat vielä rajoittavampia kuin ne, joista säädetään asetuksen (EU) 2016/679 9 artiklan 2 kohdassa.

(52) Lisäksi tietosuojalain 23 §:n 2 momentissa (jonka noudattamatta jättäminen voi johtaa seuraamuksiin ([79])) korostetaan asianmukaisten turvatoimien merkitystä arkaluonteisten tietojen käsittelyssä, jotta voidaan estää niiden ”katoaminen, varastaminen, paljastaminen, väärentäminen, muuttaminen ja vahingoittuminen”. Tämä on tietosuojalain 29 §:ään perustuva yleinen vaatimus, mutta 3 §:n 4 momentissa selvennetään, että turvallisuustasoa on mukautettava sen mukaan, minkä tyyppisiä henkilötietoja käsitellään. Tämä tarkoittaa, että on otettava huomioon erityisesti arkaluonteisten tietojen käsittelyyn liittyvät riskit. Lisäksi tietojenkäsittely on aina suoritettava niin, että voidaan ”minimoida rekisteröidyn yksityisyyden loukkaamisen mahdollisuus”, ja mahdollisuuksien mukaan ”anonymisoidussa muodossa” (tietosuojalain 3 §:n 6 ja 7 momentti). Nämä vaatimukset ovat erityisen tärkeitä silloin kun käsitellään arkaluonteisia tietoja.

2.3.3 *Käyttötarkoituksen rajaaminen*

(53) Henkilötietoja olisi kerättävä tiettyä käsittelytarkoitusta varten ja tavalla, joka ei ole ristiriidassa kyseisen tarkoituksen kanssa.

(54) Tämä periaate vahvistetaan tietosuojalain 3 §:n 1 ja 2 momentissa, joiden mukaan rekisterinpitäjän on ”täsmennettävä ja ilmoitettava” käsittelyn tarkoitus ja käsiteltävä henkilötietoja kyseisen tarkoituksen kannalta asianmukaisella tavalla. Tietoja ei saa käyttää muuhun kuin kyseiseen tarkoitukseen. Käyttötarkoituksen rajoittamista koskeva yleinen periaate vahvistetaan myös tietosuojalain 15 §:n 1 momentissa, 18 §:n 1 momentissa, 19 §:ssä ja käsittelijöiden (nk. toimeksisaajien) osalta 26 §:n 1 momentin 1 kohdassa sekä 5 ja 7 momentissa. Periaatteessa henkilötietoja voidaan käyttää ja luovuttaa kolmannelle osapuolelle ainoastaan sen käyttötarkoituksen puitteissa, jota varten ne alun perin kerättiin (15 §:n 1 momentti ja 17 §:n 1 momentin 2 kohta). Käsittely yhteensopivaa käyttötarkoitusta eli ”alkuperäiseen keräämistarkoitukseen kohtuudella liittyvää käyttötarkoitusta” varten voidaan sallia vain jos siitä ei aiheudu haittaa asianomaisille rekisteröidyille ja jos käytössä on tarvittavat turvatoimet (kuten salaus) (tietosuojalain 15 §:n 3 momentti ja 17 §:n 4 momentti). Sen määrittämiseksi, millainen myöhemmän käsittelyn tarkoitus on ”yhteensopiva” alkuperäisen tarkoituksen kanssa, tietosuojalain täytäntöönpanoasetuksessa luetellaan erityiset kriteerit, jotka vastaavat asetuksen (EU) 2016/679 6 artiklan 4 kohdassa esitettyjä vaatimuksia, ks. johdanto-osan (36) kappale.

(55) Kuten johdanto-osan (38) kappaleessa selitettiin, silloin kun korealaiset rekisterinpitäjät vastaanottavat henkilötietoja unionista, keräämistarkoitus on se tarkoitus, jota varten tiedot siirretään. Rekisterinpitäjä voi muuttaa tarkoitusta vain tietyissä erikseen luetelluissa poikkeustapauksissa (tietosuojalain 18 §:n 2 momentin 1–3 kohta, ks. myös johdanto-osan (39) kappale). Siltä osin kuin käyttötarkoituksen muuttaminen sallitaan laissa, myös tällaisten lakien on oltava yksityisyyttä ja tietosuojaa koskevien perusoikeuksien sekä Korean perustuslaissa vahvistettujen tarpeellisuutta ja oikeasuhteisuutta koskevien periaatteiden mukaisia. Tietosuojalain 18 §:n 2 ja 5 momentissa säädetään lisäksi täydentävistä suojatoimista, erityisesti vaatimuksesta, jonka mukaan tällainen käsittelytarkoituksen muutos ei saa ”oikeudettomasti loukata rekisteröidyn etua”, eli etujen tasapainottamista edellytetään aina. Tämä tietosuojan taso vastaa olennaisilta osin sitä suojelutasoa, joka perustuu asetuksen (EU) 2016/679 5 artiklan 1 kohdan b alakohtaan ja 6 artiklaan, luettuna yhdessä johdanto-osan 50 kappaleen kanssa.

2.3.4 *Tietojen täsmällisyys ja minimointi*

(56) Henkilötietojen olisi oltava täsmällisiä, ja ne olisi tarvittaessa pidettävä ajan tasalla. Tietojen on myös oltava asianmukaisia ja olennaisia, eivätkä ne saa olla liian laajoja siihen tarkoitukseen nähden, jota varten niitä käsitellään.

([78]) Tietosuojalain täytäntöönpanoasetuksen 18 §:n mukaan siinä lueteltuihin tietoryhmiin ei sovelleta lain 23 §:n 1 momenttia silloin kun niitä käsittelee julkinen laitos tietosuojalain 18 §:n 2 momentin 5–9 kohdan nojalla.

([79]) Ks. tietosuojalain 73 §:n 1 kohta 75 §:n 2 momentin 6 kohta.

(57) Täsmällisyysperiaate tunnustetaan myös Korean tietosuojalain 3 §:n 3 momentissa, jonka mukaan henkilötietojen on oltava ”täsmällisiä, täydellisiä ja ajantasaisia siltä osin kuin on tarpeen niiden tarkoitusten kannalta”, joita varten tietoja käsitellään. Tietojen minimointia edellytetään tietosuojalain 3 §:n 1 ja 6 momentissa ja 16 §:n 1 momentissa, joiden mukaan rekisterinpitäjä voi kerätä henkilötietoja (ainoastaan) ”sen verran kuin on tarpeen” aiottua tarkoitusta varten ja että sillä on tältä osin todistustaakka. Jos tietojen keräämisen tarkoitus voidaan täyttää käsittelemällä tietoja anonymisoidussa muodossa, rekisterinpitäjien olisi pyrittävä toimimaan niin (tietosuojalain 3 §:n 7 momentti).

2.3.5 *Säilytyksen rajoittaminen*

(58) Henkilötietoja olisi periaatteessa säilytettävä ainoastaan niin kauan kuin on tarpeen niiden käsittelytarkoituksen kannalta.

(59) Säilytyksen rajoittamisen periaate vahvistetaan tämän suuntaisesti tietosuojalain 21 §:n 1 momentissa ([80]), jonka mukaan rekisterinpitäjän on ”tuhottava” ([81]) henkilötiedot viipymättä sen jälkeen kun käsittelyn tarkoitus on saavutettu tai kun säilyttämisaika on kulunut umpeen (sen mukaan, kumpi ajankohta on aikaisempi), paitsi jos laissa edellytetään tietojen säilyttämistä edelleen ([82]). Viimeksi mainitussa tapauksessa asianomaisia henkilötietoja on ”säilytettävä ja käsiteltävä erillään muista henkilötiedoista” (tietosuojalain 21 §:n 3 momentti).

(60) Tietosuojalain 21 §:n 1 momenttia ei sovelleta, kun pseudonymisoituja tietoja käsitellään tilastointia, tieteellistä tutkimusta tai yleisen edun mukaista arkistointia varten ([83]). Jotta säilytyksen rajoittamista koskevan periaatteen noudattaminen voitaisiin varmistaa myös tässä tapauksessa, rekisterinpitäjien on ilmoituksen 2021-5 mukaan anonymisoitava tiedot tietosuojalain 58-2 §:n mukaisesti, jos niitä ei ole käsittelytarkoituksen saavuttamisen jälkeen tuhottu ([84]).

2.3.6 *Tietoturva*

(61) Henkilötietoja olisi käsiteltävä tavalla, jolla varmistetaan niiden turvallisuus, mukaan lukien suojaaminen luvattomalta tai laittomalta käsittelyltä sekä vahingossa tapahtuvalta häviämiseltä, tuhoutumiselta tai vahingoittumiselta. Tätä varten toiminnanharjoittajien olisi toteutettava asianmukaisia teknisiä tai organisatorisia toimenpiteitä henkilötietojen suojaamiseksi mahdollisilta uhkilta. Näitä toimenpiteitä arvioitaessa olisi otettava huomioon uusin tekniikka, toimenpiteisiin liittyvät kustannukset sekä käsittelyn luonne, laajuus, konteksti ja tarkoitus sekä yksilöiden oikeuksiin kohdistuvat riskit.

(62) Vastaava turvallisuusperiaate vahvistetaan Korean tietosuojalain 3 §:n 4 momentissa, jonka mukaan rekisterinpitäjien on ”hallinnoitava henkilötietoja turvallisesti ottaen huomioon muun muassa käsittelymenetelmät ja tietojen tyyppi sekä rekisteröidyn oikeuksien loukkaamisen mahdollisuus ja siihen liittyvien riskien vakavuus”. Lisäksi rekisterinpitäjän on ”käsiteltävä henkilötietoja niin, että voidaan minimoida mahdollisuus rekisteröidyn yksityisyyden loukkaamiseen”. Tässä yhteydessä henkilötietoja olisi mahdollisuuksien mukaan pyrittävä käsittelemään anonymisoidussa tai pseudonymisoidussa muodossa (tietosuojalain 3 §:n 6 ja 7 momentti).

(63) Näitä yleisiä vaatimuksia täsmennetään tietosuojalain 29 §:ssä, jonka mukaan kaikkien rekisterinpitäjien on ”toteutettava tarvittavat tekniset, hallinnolliset ja fyysiset toimenpiteet sisäisen hallintasuunnitelman perustamista ja kirjautumistietojen tallentamista varten, jotta voidaan varmistaa presidentin asetuksessa tarkoitettu henkilötietojen turvallisuus ja estää niiden katoaminen, varastaminen, paljastaminen, väärentäminen, muuttaminen

([80]) Tietosuojalain 8 § (yhdessä sen täytäntöönpanoasetuksen 8-2 §:n kanssa), 11 § (yhdessä täytäntöönpanoasetuksen 12 §:n 2 momentin kanssa).

([81]) Henkilötietojen tuhoamismenetelmistä säädetään täytäntöönpanoasetuksen 16 §:ssä. Tietosuojalain 21 §:n 2 momentin mukaan menetelmien on sisällettävä ”tarvittavat toimenpiteet, joilla voidaan estää tietojen palauttaminen” (*recovery and revival*).

([82]) Näiden vaatimusten laiminlyönti voi johtaa rikosoikeudellisiin seuraamuksiin (tietosuojalain 73 §:n 1–2 kohta). Tietosuojalain 39-6 §:ssä säädetään lisävaatimuksesta, jonka mukaan tieto- ja viestintäpalvelujen tarjoajien on poistettava sellaisten käyttäjien henkilötiedot, jotka eivät ole käyttäneet tarjottuja palveluja vähintään vuoteen (paitsi jos laissa säädetään pidemmästä säilytysajasta tai jos kyseinen henkilö sitä vaatii). Käyttäjille on ilmoitettava heidän tietojensa aiotusta poistamisesta 30 päivää ennen yhden vuoden määräajan päättymistä (tietosuojalain 39-6 §:n 2 momentti ja sen täytäntöönpanoasetuksen 48-5 §:n 3 momentti). Jos laissa edellytetään säilyttämisen jatkamista, asianomaiset tiedot on säilytettävä erillään käyttäjien muista tiedoista, ja niitä saa käyttää tai luovuttaa ainoastaan kyseisen lain mukaisesti (täytäntöönpanoasetuksen 48-5 §:n 1–2 momentti).

([83]) Tietosuojalain 28-7 §.

([84]) Ilmoitus N:o 2021-5 (Liite I), 4 kohta.

ja vahingoittuminen". Tietosuojalain täytäntöönpanoasetuksen 30 §:n 1 momentissa täsmennetään kyseiset toimenpiteet mainitsemalla 1) sisäisen hallintasuunnitelman laatiminen ja täytäntöönpano henkilötietojen turvallisen käsittelyn varmistamiseksi, 2) pääsynvalvonta ja -rajoitukset, 3) salausteknologian käyttöönotto henkilötietojen turvallista säilyttämistä ja siirtämistä varten, 4) kirjautumistietojen tallentaminen, 5) turvallisuusohjelmat, ja 6) fyysiset toimenpiteet, kuten turvallinen säilytys- tai lukitusjärjestelmä ([85]).

(64) Lisäksi tietoturvaloukkauksien tapahtuessa sovelletaan erityisiä velvoitteita (tietosuojalain 34 § yhdessä täytäntöönpanoasetuksen 39 ja 40 §:n kanssa) ([86]). Rekisterinpitäjän on erityisesti ilmoitettava tietoturvaloukkauksen kohteeksi joutuneille käyttäjille viipymättä sitä koskevat yksityiskohtaiset tiedot ([87]), mukaan lukien tiedot rekisterinpitäjän toteuttamista (pakollisista) vastatoimista ja siitä, mitä rekisteröidyt voivat tehdä vahinkojen minimoimiseksi (tietosuojalain 34 §:n 1 ja 2 momentti) ([88]). Jos tietoturvaloukkaus koskee vähintään tuhatta rekisteröityä, rekisterinpitäjän on viipymättä ilmoitettava siitä ja toteutetuista vastatoimista tietosuojalautakunnalle ja Korean internet- ja turvallisuusvirastolle, joka voi antaa teknistä apua (tietosuojalain 34 §:n 3 momentti yhdessä sen täytäntöönpanoasetuksen 39 §:n kanssa). Rekisterinpitäjät ovat vastuussa tietoturvaloukkauksista aiheutuvista vahingoista vahingonkorvausvastuusta annetun lain (*Civil Act on tort liability*) mukaisesti (ks. myös oikeussuojakeinoja koskeva 2.5 kohta) ([89]).

(65) Rekisterinpitäjällä on oltava turvallisuusvelvoitteiden noudattamisessa apunaan tietosuojavastaava, jonka tehtäviin kuuluu muun muassa sisäisen valvontajärjestelmän luominen "henkilötietojen paljastamisen ja väärinkäytön estämiseksi" (tietosuojalain 31 §:n 2 momentin 4 kohta). Rekisterinpitäjällä on myös velvollisuus "valvoa asianmukaisesti" niitä henkilöstönsä jäseniä, jotka käsittelevät henkilötietoja, mukaan lukien niiden turvallinen hallinnointi; tämä käsittää työntekijöiden tarvittavan koulutuksen (tietosuojalain 28 §:n 1 ja 2 momentti). Jos käsittelystä vastaa alihankkija, rekisterinpitäjän on asetettava toimeksisaajalle muun muassa henkilötietojen turvallista hallinnointia koskevia vaatimuksia ("tekniset ja hallinnolliset suojatoimet") ja valvottava niiden noudattamista tarkastusten avulla (tietosuojalain 26 §:n 1 ja 4 momentti yhdessä sen täytäntöönpanoasetuksen 28 §:n 1 momentin 3, 4 ja 6 kohdan kanssa).

2.3.7 *Läpinäkyvyys*

(66) Rekisteröidyille olisi ilmoitettava heidän henkilötietojensa käsittelyn pääkohdat.

([85]) Siltä osin kuin on kyse tieto- ja viestintäpalvelujen tarjoajien suorittamasta henkilötietojen käsittelystä, tietosuojalain 39-5 §:ssä säädetään nimenomaisesti, että käyttäjien henkilötietoja käsittelevien henkilöiden lukumäärän on oltava mahdollisimman pieni. Lisäksi tieto- ja viestintäpalvelujen tarjoajien on varmistettava, että käyttäjien henkilötietoja ei paljasteta tieto- ja viestintäverkossa yleisölle (tietosuojalain 39-10 §:n 1 momentti). Paljastuneet tiedot on poistettava tai suojattava tietokannassa tietosuojalautakunnan pyynnöstä (tietosuojalain 39-10 §:n 2 momentti). Tieto- ja viestintäpalvelujen tarjoajiin (sekä käyttäjien henkilötietoja vastaanottaviin kolmansiin osapuoliin) sovelletaan yleensäkin täydentäviä turvallisuusvelvoitteita, jotka yksilöidään täytäntöönpanoasetuksen 48-2 §:ssä. Niitä ovat muun muassa turvallisuustoimenpiteitä koskevan sisäisen hallintasuunnitelman laatiminen ja täytäntöönpano, pääsynvalvontaan liittyvät toimenpiteet, salaus ja ohjelmiston käyttö haittaohjelmien havaitsemiseksi.

([86]) Lisäksi yleisellä säännöksellä on kielletty henkilötietojen vahingoittaminen, tuhoaminen, muuttaminen, väärentäminen tai luovuttaminen ilman oikeudellista valtuutusta, ks. tietosuojalain 59 §:n 3 kohta.

([87]) Vaatimusta ilmoittaa tietoturvaloukkauksesta yksittäisille rekisteröidyille ei sovelleta, jos tietoturvaloukkaus koskee pseudonymisoitujen tietojen käsittelyä tilastointia, tieteellistä tutkimusta tai yleisen edun mukaista arkistointia varten (tietosuojalain 28-7 §, jossa säädetään 34 §:n 1 momenttia ja 39-4 §:ää koskevasta poikkeuksesta). Henkilökohtainen ilmoittaminen edellyttäisi, että rekisterinpitäjä tunnistaisi rekisteröidyt pseudonymisoidusta tietoaineistosta, mikä on nimenomaisesti kielletty tietosuojalain 28-5 §:ssä. Yleistä velvollisuutta ilmoittaa tietoturvaloukkauksesta (tietosuojalautakunnalle) sovelletaan kuitenkin myös tällaisessa tapauksessa.

([88]) Ilmoittamista koskevat vaatimukset, mukaan lukien ilmoittamisen ajankohta ja mahdollisuus tehdä ilmoitus "vaiheittain", täsmennetään tietosuojalain täytäntöönpanoasetuksen 40 §:ssä. Tieto- ja viestintäpalvelujen tarjoajiin sovellettavat säännöt ovat tiukemmat, sillä niiden on ilmoitettava rekisteröidyille ja tietosuojalautakunnalle 24 tunnin kuluessa siitä kun ne saavat tiedon henkilötietojen katoamisesta, varastamisesta tai luovuttamisesta ilman oikeudellista valtuutusta (tietosuojalain 39-4 §:n 1 momentti). Ilmoituksessa on oltava yksityiskohtaiset tiedot henkilötiedoista, jotka on luovutettu ilman oikeudellista valtuutusta, tapahtuman ajankohta, toimenpiteet jotka käyttäjä voi toteuttaa, palveluntarjoajan toteuttamat vastatoimet sekä sen osaston yhteystiedot, jolle käyttäjä voi esittää kysymyksiä (tietosuojalain 39-4 §:n 1 momentin 1–5 kohta). Perustellusta syystä eli jos palveluntarjoajalla esimerkiksi ei ole käyttäjän yhteystietoja, voidaan käyttää myös muita ilmoitustapoja, kuten tiedon julkaiseminen verkkosivustolla (tietosuojalain 39-4 §:n 1 momentti yhdessä täytäntöönpanoasetuksen 48-4 §:n 4 momentin ja sitä seuraavien momenttien kanssa). Tällaiset perustellut syyt on ilmoitettava tietosuojalautakunnalle (tietosuojalain 34-4 §:n 3 momentti).

([89]) Ks. esim. korkeimman oikeuden päätökset 2011Da59834, 2011Da59858 ja 2011Da59841, 26.12.2012. Englanninkielinen tiivistelmä on saatavilla osoitteessa http://library.scourt.go.kr/SCLIB_data/decision/9-69%202012.12.26.2011Da59834.htm.

(67) Tämä varmistetaan Korean järjestelmässä eri tavoin. Tietosuojalaissa säädetään paitsi oikeudesta tiedonsaantiin yleensä (4 §:n 1 kohta) ja kolmansilta osapuolilta kerättyjen henkilötietojen osalta erikseen (20 §:n 1 momentti) sekä oikeudesta saada pääsy omiin tietoihin (35 §). Lisäksi siinä säädetään käsittelyn läpinäkyvyyttä koskevasta yleisestä vaatimuksesta (3 §:n 1 momentti) ja erityisvaatimuksesta, joka koskee läpinäkyvyyttä silloin kun käsittely perustuu suostumukseen (15 §:n 2 momentti, 17 §:n 2 momentti ja 18 §:n 3 momentti) ([90]). Tämän lisäksi tietosuojalain 20 §:n 2 momentissa edellytetään, että tiettyjen rekisterinpitäjien (joiden osalta käsittely ylittää tietyt kynnysarvot ([91])) on ilmoitettava niille rekisteröidyille, joiden henkilötiedot ne ovat saaneet kolmannelta osapuolelta, tietojen lähde ja käyttötarkoitus sekä se, että rekisteröidyllä on oikeus vaatia käsittelyn keskeyttämistä, paitsi jos tällainen ilmoittaminen osoittautuu mahdottomaksi yhteystietojen puuttumisen vuoksi. Ilmoitusvelvollisuuteen liittyvät poikkeukset koskevat tiettyjä viranomaisten henkilötietorekistereitä ja erityisesti rekistereitä, joiden tietoja käsitellään kansallista turvallisuutta tai muita erityisen tärkeitä ("vakavia") kansallisia etuja tai lainvalvontatarkoituksia varten. Poikkeuksia sovelletaan myös, jos ilmoittaminen todennäköisesti vahingoittaisi jonkun toisen henkilön henkeä tai terveyttä tai aiheuttaisi oikeudettomasti vahinkoa toisen henkilön omaisuudelle ja muille eduille, kuitenkin vain siinä tapauksessa, että asiaan liittyvä julkinen tai yleinen etu on "selvästi suurempi" kuin asianomaisten rekisteröityjen oikeudet (tietosuojalain 20 §:n 4 momentti). Tämä edellyttää asianomaisten etujen tasapainottamista.

(68) Lisäksi tietosuojalain 3 §:n 5 momentissa säädetään, että rekisterinpitäjien on julkistettava tietosuojaselosteensa (ja muut henkilötietojen käsittelyyn liittyvät asiat). Tätä vaatimusta täsmennetään tarkemmin tietosuojalain 30 §:ssä yhdessä täytäntöönpanoasetuksen 31 §:n kanssa. Mainittujen säännösten mukaan julkisessa tietosuojaselosteessa on mainittava 1) minkätyyppisiä henkilötietoja käsitellään, 2) käsittelyn tarkoitus, 3) säilytysaika, 4) onko henkilötietoja toimitettu kolmannelle osapuolelle ([92]), 5) mahdollinen alihankinta, 6) tiedot rekisteröidyn oikeuksista ja niiden käyttämisestä ja 7) yhteystiedot (mukaan lukien tietosuojavastaavan tai sen sisäisen osaston nimi, joka vastaa tietosuojasääntöjen noudattamisesta ja valitusten käsittelystä). Tietosuojaseloste on saatettava julkisesti saataville siten, että rekisteröidyt "voivat tunnistaa sen helposti" (tietosuojalain 30 §:n 2 momentti) ([93]), ja se on pidettävä jatkuvasti ajan tasalla (täytäntöönpanoasetuksen 31 §:n 2 momentti).

(69) Julkisilla laitoksilla on lisäksi velvollisuus rekisteröidä tietosuojalautakunnassa erityisesti seuraavat tiedot: 1) julkisen laitoksen nimi, 2) henkilötietorekisterin käsittelyn perusteet ja tarkoitukset, 3) rekisteröitävien henkilötietojen yksityiskohdat, 4) käsittelymenetelmä, 5) säilytysaika, 6) niiden rekisteröityjen määrä, joiden henkilötietoja säilytetään, 7) rekisteröityjen pyyntöjä käsittelevä osasto ja 8) henkilötietojen vastaanottajat, silloin kun tietoja toimitetaan rutiininomaisesti tai toistuvasti (tietosuojalain 32 §:n 1 momentti) ([94]). Tietosuojalautakunta julkaisee rekisteröidyt henkilötietorekisterit, ja julkisten laitosten on myös mainittava ne tietosuojaselosteessaan (tietosuojalain 30 §:n 1 momentti ja 32 §:n 4 momentti).

(70) Jotta voitaisiin parantaa läpinäkyvyyttä niiden unionin rekisteröityjen kannalta, joiden henkilötietoja siirretään Koreaan tämän päätöksen perusteella, ilmoituksen N:o 2021-5 (liite I) 3 kohdan i ja ii alakohdassa säädetään läpinäkyvyyttä koskevista lisävaatimuksista. Kun korealaiset rekisterinpitäjät vastaanottavat henkilötietoja unionista tämän päätöksen perusteella, niiden on ensinnäkin ilmoitettava asianomaisille rekisteröidyille viipymättä (ja viimeistään kuukauden kuluessa tietojen siirtämisestä) niiden yksiköiden nimi ja yhteystiedot, jotka lähettävät ja vastaanottavat tietoja, mitä henkilötietoja (tai henkilötietoryhmiä) siirretään, tarkoitus jota varten korealainen

([90]) Etenkin silloin kun henkilötietoja käsitellään asianomaisen henkilön suostumuksen perusteella, rekisterinpitäjän on ilmoitettava henkilölle käsittelyn tarkoitus, käsiteltäviä tietoja koskevat yksityiskohdat, tietojen vastaanottaja, niiden säilyttämis- ja käyttöaika sekä se, että henkilöllä on oikeus olla antamatta suostumustaan (ja siitä mahdollisesti aiheutuva haitta).

([91]) Tietosuojalain täytäntöönpanoasetuksen 15-2 §:n 1 momentin mukaan tämä koskee rekisterinpitäjiä, jotka käsittelevät vähintään 50 000 rekisteröidyn arkaluonteisia tietoja, tai vähintään miljoonan rekisteröidyn "tavanomaisia" henkilötietoja. Tietosuojalain täytäntöönpanoasetuksen 15-2 §:n 2 momentissa säädetään ilmoitusmenettelyistä ja -ajankohdasta ja 15-2 §:n 3 momentissa vaatimuksesta pitää kirjaa tietyistä siihen liittyvistä seikoista. Lisäksi sovelletaan erityissääntöjä tiettyihin tieto- ja viestintäpalvelujen tarjoajien ryhmiin (ne, joiden myyntitulot edeltävänä vuonna olivat vähintään 10 miljardia wonia tai jotka säilyttivät/hallinnoivat edellisen vuoden kolmen viimeisen kuukauden aikana päivittäin keskimäärin vähintään miljoonan käyttäjän henkilötietoja), joiden on ilmoitettava käyttäjille säännöllisesti näiden henkilötietojen käyttöhistoria, paitsi jos se osoittautuu mahdottomaksi yhteystietojen puuttumisen vuoksi (tietosuojalain 39-8 § ja täytäntöönpanoasetuksen 48-6 §).

([92]) Korean hallitukselta saatujen tietojen mukaan tähän sisältyy velvollisuus luetella tietosuojaselosteessa vastaanottaja/vastaanottajat erikseen.

([93]) Täydentävistä yksityiskohdista säädetään täytäntöönpanoasetuksen 31 §:n 3 momentissa.

([94]) Rekisteröintivaatimusta ei sovelleta tietyntyyppisiin henkilötietorekistereihin, esimerkiksi jos niihin talletettavat tiedot koskevat kansallista turvallisuutta, diplomaattisalaisuuksia, rikostutkintaa, syytteeseenpanoa, rangaistuksia tai verorikosten tutkintaa tai jos rekisteri koskee yksinomaan työn suorittamiseen liittyviä sisäisiä asioita (tietosuojalain 32 §:n 2 momentti).

rekisterinpitäjä kerää tiedot, tietojen säilytysaika ja Korean tietosuojalain nojalla käytettävissä olevat oikeudet. Toiseksi, kun henkilötietoja luovutetaan unionista tämän päätöksen perusteella kolmannelle osapuolelle, rekisteröidyille on ilmoitettava muun muassa tietojen vastaanottaja, mitä henkilötietoja tai tietoryhmiä luovutetaan, maa johon tiedot luovutetaan (tarvittaessa) sekä Korean tietosuojalain nojalla käytettävissä olevat oikeudet ([95]). Näin ilmoituksella N:o 2021-5 varmistetaan, että EU:n luonnolliset henkilöt saavat edelleen tiedon siitä, mitkä rekisterinpitäjät käsittelevät heidän tietojaan ja voivat käyttää oikeuksiaan suhteessa asianomaisiin yksiköihin.

(71) Ilmoituksen (liite I) 3 kohdan iii alakohdassa sallitaan tietyt rajoitetut ja ehdolliset poikkeukset näistä läpinäkyvyyttä koskevista lisävaatimuksista; poikkeukset vastaavat olennaisilta osin asetuksen (EU) 2016/679 säännöksiä. Poikkeuksissa säädetään erityisesti, että ilmoitusta unionin rekisteröidyille ei vaadita, 1) jos ja niin kauan kuin ilmoittamista on tarpeen rajoittaa tietyistä yleistä etua koskevista syistä (esimerkiksi kun tietoja käsitellään kansalliseen turvallisuuteen liittyviä tarkoituksia tai käynnissä olevaa rikostutkintaa varten), siltä osin kuin nämä yleisen edun mukaiset tavoitteet ovat selvästi rekisteröidyn oikeuksia tärkeämpiä; 2) rekisteröity on jo saanut tiedot; 3) jos ja niin kauan kuin ilmoittaminen todennäköisesti vahingoittaisi asianomaisen tai jonkun toisen henkilön henkeä tai terveyttä tai loukkaisi oikeudettomasti toisen henkilön omistusoikeuksia, kun nämä oikeudet tai edut ovat selvästi rekisteröidyn oikeuksia tärkeämpiä; tai 4) kun asianomaisten henkilöiden yhteystietoja ei ole tai heille ilmoittaminen aiheuttaisi kohtuutonta vaivaa. Määritettäessä sitä, onko rekisteröityyn mahdollista ottaa yhteyttä tai aiheutuuko siitä kohtuutonta vaivaa, on otettava huomioon mahdollisuus tehdä yhteistyötä unionissa olevan tietojen viejän kanssa.

(72) Näin ollen johdanto-osan (67)–(71) kappaleessa esitetyillä säännöillä varmistetaan läpinäkyvyyden osalta olennaisilta osin samantasoinen tietosuoja kuin asetuksessa (EU) 2016/679.

2.3.8 *Yksilön oikeudet*

(73) Rekisteröidyillä olisi oltava tietyt oikeudet, joihin voidaan vedota rekisterinpitäjää tai henkilötietojen käsittelijää vastaan, kuten oikeus saada pääsy tietoihin, oikeus vastustaa niiden käsittelyä ja oikeus saada tiedot oikaistuiksi ja poistetuiksi. Toisaalta näitä oikeuksia voidaan rajoittaa siltä osin kuin rajoitukset ovat tarpeen ja oikeasuhteisia yleisen edun mukaisten tärkeiden tavoitteiden turvaamiseksi.

(74) Tietosuojalain 3 §:n 5 momentin mukaan rekisterinpitäjän on taattava lain 4 §:ssä luetellut rekisteröidyn oikeudet, joita täsmennetään lain 35–37, 39 ja 39-2 §:ssä.

(75) Ensinnäkin rekisteröidyillä on oikeus tiedonsaantiin ja oikeus saada pääsy omiin tietoihinsa. Kun rekisterinpitäjä on kerännyt henkilötietoja kolmannelta osapuolelta – näin on aina silloin kun tiedot on siirretty unionista – rekisteröidyillä on yleensä oikeus saada tietoa 1) siitä, mistä lähteestä henkilötiedot on kerätty (eli tietojen siirtäjästä), 2) käsittelyn tarkoituksesta ja 3) siitä, että rekisteröidyllä on oikeus vaatia käsittelyn keskeyttämistä (tietosuojalain 20 §:n 1 momentti). Rajoitettuja poikkeuksia sovelletaan silloin kun ilmoittaminen todennäköisesti vahingoittaisi toisen henkilön henkeä tai terveyttä tai ”aiheuttaisi oikeudettomasti vahinkoa toisen henkilön omaisuudelle ja muille eduille”, mutta vain jos nämä kolmannen osapuolen edut ovat ”nimenomaisesti tärkeämpiä” kuin rekisteröidyn oikeudet (tietosuojalain 20 §:n 4 momentin 2 kohta).

(76) Lisäksi tietosuojalain 35 §:n 1 ja 3 momentissa yhdessä sen täytäntöönpanoasetuksen 41 §:n 4 momentin kanssa säädetään, että rekisteröidyillä on oikeus saada pääsy henkilötietoihinsa ([96]). Pääsyoikeus tarkoittaa oikeutta saada vahvistus siihen, että tietoja käsitellään, ja tietoa siitä, minkä tyyppisiä tietoja käsitellään, mitä tarkoitusta varten ja kuinka kauan tietoja säilytetään. Lisäksi rekisteröidyllä on oikeus saada tietoa henkilötietojen

([95]) Ilmoitus N:o 2021-5, 3 kohdan ii alakohta (liite I).

([96]) Rekisterinpitäjä voi lykätä pääsyoikeuden myöntämistä ”hyvästä syystä” (eli asianmukaisin perustein, esimerkiksi jos tarvitaan lisäaikaa sen arvioimiseksi, voidaanko oikeus myöntää) (tietosuojalain 35 §:n 3 momentti yhdessä sen täytäntöönpanoasetuksen 42 §:n 2 momentin kanssa). Nämä perustelut on kuitenkin annettava rekisteröidylle tiedoksi 10 päivän kuluessa ja annettava tietoa siitä, miten päätökseen voi hakea muutosta; pääsy on myönnettävä heti kun lykkäykselle ei ole enää perusteita.

mahdollisesta luovuttamisesta kolmannelle osapuolelle ja oikeus saada kopio käsiteltävistä henkilötiedoista (tietosuojalain 4 §:n 3 momentti yhdessä sen täytäntöönpanoasetuksen 41 §:n 1 momentin kanssa) ([97]). Pääsyoikeutta voidaan rajoittaa (osittainen pääsy) ([98]) tai se voidaan evätä kokonaan vain jos niin säädetään laissa ([99]) tai jos pääsyoikeuden myöntäminen todennäköisesti vahingoittaisi kolmannen osapuolen henkeä tai terveyttä tai aiheuttaisi oikeudettomasti vahinkoa toisen henkilön omaisuudelle ja muille eduille (tietosuojalain 35 §:n 4 momentti) ([100]). Viimeksi mainittu seikka edellyttää, että on löydettävä oikea tasapaino asianomaisen henkilön ja toisen henkilön perustuslailla suojattujen yksilön oikeuksien ja vapauksien välillä. Kun pääsyoikeutta rajoitetaan tai kun se evätään kokonaan, rekisterinpitäjän on ilmoitettava rekisteröidylle päätöksen perusteet ja muutoksenhakukeinot (tietosuojalain täytäntöönpanoasetuksen 41 §:n 5 momentti ja 42 §:n 2 momentti).

(77) Toiseksi rekisteröidyillä on oikeus saada henkilötietonsa oikaistuksi tai poistetuksi ([101]), ”ellei muissa säännöksissä nimenomaisesti toisin säädetä” (tietosuojalain 36 §:n 1 ja 2 momentti) ([102]). Pääsyoikeutta koskevan pyynnön saatuaan rekisterinpitäjän on tutkittava asia viipymättä, toteutettava tarvittavat toimenpiteet ([103]) ja ilmoitettava niistä rekisteröidylle 10 päivän kuluessa. Jos pyyntöön ei voida suostua, rekisteröidylle on ilmoitettava myös epäämisen syyt ja muutoksenhakukeinot (tietosuojalain 36 §:n 4 momentti yhdessä sen täytäntöönpanoasetuksen 43 §:n 3 momentin kanssa) ([104]).

(78) Rekisteröidyillä on myös oikeus viipymättä keskeyttää henkilötietojensa käsittely ([105]), paitsi jos sovelletaan jotakin erikseen lueteltua poikkeusta (tietosuojalain 37 §:n 1 ja 2 momentti) ([106]). Rekisterinpitäjä voi evätä pyynnön, 1) jos se nimenomaisesti sallitaan laissa tai on tarpeen (”välttämätöntä”) lakisääteisten velvoitteiden noudattamiseksi, 2) jos keskeyttäminen todennäköisesti vahingoittaisi kolmannen osapuolen henkeä tai terveyttä tai aiheuttaisi oikeudettomasti vahinkoa toisen henkilön omaisuudelle ja muille eduille, 3) jos julkisen laitoksen olisi mahdoton suorittaa lakisääteisiä tehtäviään kyseisiä tietoja käsittelemättä, tai 4) jos rekisteröity ei nimenomaisesti irtisano rekisterinpitäjän kanssa tehtyä sopimusta, vaikka sopimuksen täyttäminen olisi mahdotonta ilman tällaista tietojen käsittelyä. Tässä tapauksessa rekisterinpitäjän on viipymättä ilmoitettava rekisteröidylle epäämisen syyt ja muutoksenhakukeinot (tietosuojalain 37 §:n 2 momentti yhdessä täytäntöönpanoasetuksen 44 §:n 2 momentin kanssa). Tietosuojalain 37 §:n 4 momentin mukaan rekisterinpitäjän on käsittelyn keskeyttämistä koskevan pyynnön noudattamiseksi viipymättä ”toteutettava tarvittavat toimenpiteet, mukaan lukien asianomaisten henkilötietojen tuhoaminen” ([107]).

(79) Oikeutta käsittelyn keskeyttämiseen sovelletaan myös silloin kun henkilötietoja käytetään suoramarkkinointitarkoituksiin eli tavaroiden tai palvelujen myynnin edistämiseen. Lisäksi tällainen myöhempi käsittely edellyttää yleensä rekisteröidyn (täydentävää) suostumusta (tietosuojalain 15 §:n 1 momentin 1 kohta ja 17 §:n 2 momentin 1 kohta) ([108]). Tällaista suostumusta pyytäessään rekisterinpitäjän on ilmoitettava rekisteröidylle erityisesti siitä,

([97]) Pääsyn julkisen laitoksen käsittelemiin henkilötietoihin voi myöntää joko kyseinen laitos suoraan, tai pääsyä voidaan pyytää tietosuojalautakunnalta, joka toimittaa hakemuksen viipymättä edelleen (tietosuojalain 35 §:n 2 momentti ja täytäntöönpanoasetuksen 41 §:n 3 momentti).

([98]) Tietosuojalain täytäntöönpanoasetuksen 42 §:n 1 momentin mukaan rekisterinpitäjän on myönnettävä osittainen pääsyoikeus, jos ainakin osa tiedoista jää kieltäytymisperusteiden soveltamisalan ulkopuolelle.

([99]) Tällaisten lakien on oltava yksityisyyttä ja tietosuojaa koskevien perusoikeuksien sekä Korean perustuslaissa vahvistettujen tarpeellisuutta ja oikeasuhteisuutta koskevien periaatteiden mukaisia.

([100]) Julkiset laitokset voivat evätä pääsyn myös siinä tapauksessa, että sen myöntäminen vaikeuttaisi vakavasti tiettyjen toimien suorittamista, kuten vireillä olevat tarkastukset tai verojen määrittäminen, kerääminen tai palauttaminen (tietosuojalain 35 §:n 4 momentti).

([101]) Tässä tapauksessa rekisterinpitäjän on toteutettava toimenpiteet, joilla estetään henkilötietojen palauttaminen, ks. tietosuojalain 36 §:n 3 momentti.

([102]) Tällaisten säännösten on täytettävä perustuslain vaatimukset, joiden mukaan perusoikeutta voidaan rajoittaa vain jos se on tarpeen kansallisen turvallisuuden, lain ja yleisen järjestyksen tai yleisen hyvinvoinnin ylläpitämiseksi, eikä rajoittaminen saa vaikuttaa vapauden tai oikeuden olennaiseen sisältöön (perustuslain 37 §:n 2 momentti).

([103]) Tietosuojalain täytäntöönpanoasetuksen 43 §:n 2 momentissa säädetään erityisestä menettelystä, jota sovelletaan kun rekisterinpitäjä käsittelee toisen rekisterinpitäjän toimittamia henkilötietoja.

([104]) Henkilötietojen oikaisemiseksi tai poistamiseksi tarvittavien toimenpiteiden laiminlyönti ja tällaisten tietojen jatkuva käyttö tai toimittaminen kolmannelle osapuolelle voi johtaa rikosoikeudellisiin seuraamuksiin (tietosuojalain 73 §:n 2 momentti).

([105]) Tietosuojalain täytäntöönpanoasetuksen 44 §:n 2 momentin mukaan rekisterinpitäjän on ilmoitettava rekisteröidylle siitä, että se on asianmukaisesti keskeyttänyt käsittelyn, 10 päivän kuluessa pyynnön vastaanottamisesta.

([106]) Julkisten laitosten osalta oikeutta käsittelyn keskeyttämiseen voidaan käyttää suhteessa rekisteröityihin henkilötietorekistereihin (tietosuojalain 37 § yhdessä sen 32 §:n kanssa). Tällaista rekisteröintiä ei vaadita tietyissä rajoitetuissa tapauksissa, esimerkiksi jos rekisteriin talletettavat tiedot koskevat kansallista turvallisuutta, rikostutkintaa tai diplomaattisuhteita (tietosuojalain 32 §:n 2 momentti).

([107]) Käsittelyn keskeyttämisen laiminlyönti voi johtaa rikosoikeudellisiin seuraamuksiin (tietosuojalain 73 §:n 3 kohta).

([108]) Riitojenratkaisukomitea (ks. johdanto-osan 133 kappale) on käsitellyt useita tapauksia, joissa rekisteröidyt ovat valittaneet, että heidän tietojaan on käytetty suoramarkkinointitarkoituksiin ilman heidän suostumustaan. Rekisterinpitäjiä on muun muassa määrätty maksamaan rekisteröidyille korvauksia ja poistamaan kyseiset henkilötiedot (ks. esim. riitojenratkaisukomitean päätös 20R10-024(2020.11.18), 20R08-015(2020,8,28), 20R07-031(2020.9.1)).

että tietoja on tarkoitus käyttää suoramarkkinointiin – eli että häneen voidaan ottaa yhteyttä tavaroiden tai palvelujen myynnin edistämiseksi – ”nimenomaisen tunnistettavasti” (tietosuojalain 22 §:n 2 ja 4 momentti yhdessä sen täytäntöönpanoasetuksen 17 §:n 2 momentin 1 kohdan kanssa).

(80) Rekisterinpitäjän on pyrittävä helpottamaan yksilön oikeuksien käyttämistä ottamalla käyttöön sitä varten erityiset menettelyt ja ilmoittamalla niistä julkisesti (tietosuojalain 38 §:n 4 momentti) ([109]). Tämä tarkoittaa myös menettelyjä, joilla voidaan vastustaa pyynnön epäämistä (tietosuojalain 38 §:n 5 momentti). Rekisterinpitäjän on huolehdittava sitä että oikeuksien käyttämistä koskeva menettely on rekisteröidyn kannalta helppokäyttöinen ja ettei se ole vaikeampi kuin henkilötietojen keräämisessä käytettävä menettely; tähän sisältyy myös velvollisuus ilmoittaa menettelystä rekisterinpitäjän verkkosivustolla (tietosuojalain täytäntöönpanoasetuksen 41 §:n 2 momentti, 43 §:n 1 momentti ja 44 §:n 1 momentti) ([110]). Rekisteröity voi valtuuttaa edustajan tekemään tällaisen pyynnön puolestaan (tietosuojalain 38 §:n 1 momentti yhdessä sen täytäntöönpanoasetuksen 45 §:n kanssa). Rekisterinpitäjällä on oikeus periä tietojen toimittamisesta maksu (ja postikulut, jos henkilötietojen kopiot pyydetään lähettämään postitse), jonka suuruus on määritettävä ”[pyynnön] käsittelystä aiheutuvien todellisten kustannusten mukaan”; maksua (ja postikuluja) ei saa periä, jos rekisterinpitäjä on itse aiheuttanut pyynnön (tietosuojalain 38 §:n 3 momentti yhdessä sen täytäntöönpanoasetuksen 47 §:n kanssa).

(81) Tietosuojalaki ja sen täytäntöönpanoasetus eivät sisällä yleisiä säännöksiä rekisteröityyn vaikuttavista päätöksistä, jotka perustuisivat yksinomaan henkilötietojen automaattiseen käsittelyyn. Unionissa kerättyjen henkilötietojen osalta mahdollisen automatisoituun käsittelyyn perustuvan päätöksen tekee kuitenkin yleensä unionissa toimiva rekisterinpitäjä (jolla on suora suhde kyseiseen rekisteröityyn), ja näin ollen kyseiseen päätökseen sovelletaan asetusta (EU) 2016/679 ([111]). Tähän kuuluvat siirtotilanteet, joissa tietojen käsittelyn suorittaa ulkomainen (esimerkiksi korealainen) toiminnanharjoittaja, joka toimii unionin rekisterinpitäjän puolesta (käsittelijänä) (tai unionin käsittelijän alihankkijana vastaanotettuaan tiedot ne keränneeltä unionin rekisterinpitäjältä); päätöksen tekee tämän perusteella unionin rekisterinpitäjä. Siksi se, ettei Korean tietosuojalaissa ole säännöksiä automatisoidusta päätöksenteosta, ei todennäköisesti vaikuta tämän päätöksen nojalla siirrettyjen henkilötietojen suojan tasoon.

(82) Säännöksiä, jotka koskevat pyynnöstä sovellettavaa läpinäkyvyyttä (tietosuojalain 20 §) ja yksilön oikeuksia (35–37 §) sekä tieto- ja viestintäpalvelujen tarjoajilta edellytettävää henkilökohtaista ilmoitusta (39-8 §), ei poikkeuksellisesti sovelleta pseudonymisoituihin tietoihin, kun niitä käsitellään tilastointia, tieteellistä tutkimusta tai yleisen edun mukaista arkistointia varten (28-7 §) ([112]). Tämä on perusteltua asetuksen (EU) 2016/679 11 artiklan 2 kohdan (yhdessä johdanto-osan 57 kappaleen kanssa) mukaisesti siksi, että voidakseen varmistaa läpinäkyvyyden tai myöntää rekisteröidylle oikeuksia rekisterinpitäjän olisi voitava selvittää, liittyvätkö jotkin tiedot pyynnön esittävään henkilöön (ja jos liittyvät, niin mitkä). Tämä taas kielletään tietosuojalaissa nimenomaisesti (28-5 §:n 1 momentti). Jos tällainen uudelleentunnistus edellyttäisi koko tietojoukon pseudonymisoinnin poistamista, se myös altistaisi kaikkien muiden yksilöiden henkilötiedot suurentuneelle riskille. Siinä missä asetuksessa (EU) 2016/679 viitataan tilanteisiin, joissa uudelleentunnistaminen on käytännössä mahdotonta, Korean tietosuojalaissa on omaksuttu tiukempi lähestymistapa, jonka mukaan siinä nimenomaisesti kielletään uudelleentunnistaminen aina kun käsitellään pseudonymisoituja tietoja.

(83) Johdanto-osan (74)–(82) kappaleessa kuvattu Korean järjestelmä sisältää näin ollen rekisteröidyn oikeuksia koskevat säännöt, jotka olennaisilta osin vastaavat asetukseen (EU) 2016/679 perustuvaa tietosuojan tasoa.

([109]) Ks. myös tietosuojalain 30 §:n 1 momentin 5 kohta tietosuojaselosteesta, jossa on kerrottava muun muassa rekisteröidylle kuuluvista oikeuksista ja siitä, miten niitä voi käyttää.

([110]) Ks. myös tietosuojalain 39-7 §:n 2 momentti, joka koskee tieto- ja viestintäpalvelujen tarjoajia.

([111]) Vastaavasti siinä poikkeuksellisessa tapauksessa, että korealaisella toiminnanharjoittajalla on suora suhde EU:n rekisteröityyn, tämä on tyypillisesti seurausta siitä, että korealainen toiminnanharjoittaja on kohdentanut toimiaan Euroopan unionissa olevaan henkilöön tarjoamalla tälle tavaroita tai palveluja tai seuraamalla tämän käyttäytymistä. Tässä tapauksessa korealainen toiminnanharjoittaja itse kuuluu asetuksen (EU) 2016/679 (3 artiklan 2 kohta) soveltamisalaan, minkä vuoksi sen on suoraan noudatettava EU:n tietosuojalainsäädäntöä.

([112]) Ks. myös ilmoitus N:o 2021-5, jossa vahvistetaan, että tietosuojalain III jaksoa (mm. 28-7 §) sovelletaan ainoastaan silloin kun pseudonymisoituja tietoja käsitellään tilastointia, tieteellistä tutkimusta tai yleisen edun mukaista arkistointia varten, ks. tämän päätöksen liitteessä I oleva 4 kohta.

2.3.9 *Tietojen siirtäminen edelleen*

(84) Unionista Korean tasavallassa oleville toiminnanharjoittajille siirrettyjen henkilötietojen suojan tasoa ei saa heikentää siirtämällä näitä tietoja edelleen kolmannessa maassa sijaitseville vastaanottajille.

(85) Tällaiset ”jatkosiirrot” ovat korealaisen rekisterinpitäjän näkökulmasta Korean tasavallasta tehtäviä kansainvälisiä siirtoja. Tältä osin Korean tietosuojalaissa erotetaan toisistaan käsittelyn ulkoistaminen toimeksisaajalle (käsittelijälle) ja henkilötietojen luovuttaminen kolmannelle osapuolelle ([113]).

(86) Kun henkilötietojen käsittely on ulkoistettu kolmannessa maassa sijaitsevalle yksikölle, korealaisen rekisterinpitäjän on ensinnäkin varmistettava, että noudatetaan ulkoistusta koskevia tietosuojalain säännöksiä (26 §). Tämä tarkoittaa sellaisen oikeudellisesti sitovan välineen laatimista, jossa muun muassa rajataan toimeksisaajan suorittama käsittely ainoastaan ulkoistetun työn tarkoitukseen, edellytetään teknisiä ja hallinnollisia suojatoimia ja rajoitetaan alihankintaa (tietosuojalain 26 §:n 1 momentti). Lisäksi edellytetään, että ulkoistettua työtä koskevat tiedot on julkaistava. Rekisterinpitäjällä on myös velvollisuus ”opettaa” toimeksisaajalle tarvittavat turvatoimet ja valvoa muun muassa tarkastusten avulla, että toimeksisaaja noudattaa sekä kaikkia rekisterinpitäjälle tietosuojalaissa asetettuja velvollisuuksia että ulkoistamissopimukseen perustuvia velvollisuuksia ([114]).

(87) Jos toimeksisaaja aiheuttaa vahinkoa käsittelemällä tietoja tietosuojalain vastaisella tavalla, rekisterinpitäjän katsotaan olevan vastuussa vahingoista samalla tavoin kuin omien työntekijöidensä osalta (tietosuojalain 26 §:n 6 momentti). Korealainen rekisterinpitäjä on edelleen vastuussa ulkoistetuista henkilötiedoista, ja sen on varmistettava, että ulkomainen henkilötietojen käsittelijä käsittelee niitä Korean tietosuojalain mukaisesti. Jos toimeksisaaja käsittelee tietoja Korean tietosuojalain vastaisella tavalla, korealainen rekisterinpitäjä voidaan saattaa vastuuseen siitä, että se on laiminlyönyt velvollisuutensa varmistaa Korean tietosuojalain noudattaminen esimerkiksi toimeksisaajaa valvomalla. Ulkoistamissopimukseen sisältyvät suojatoimet ja korealaisen rekisterinpitäjän vastuu toimeksisaajan toiminnasta takaavat suojelun jatkuvuuden silloin kun henkilötietojen käsittely ulkoistetaan Korean ulkopuolella sijaitsevalle yksikölle.

(88) Toiseksi korealaiset rekisterinpitäjät voivat luovuttaa henkilötietoja Korean ulkopuolella sijaitsevalle kolmannelle osapuolelle. Korean tietosuojalaissa on useita oikeusperustoja, joiden nojalla henkilötietoja voidaan luovuttaa kolmannelle osapuolelle yleensä. Silloin kun kolmas osapuoli sijaitsee Korean ulkopuolella, rekisterinpitäjän on kuitenkin periaatteessa ([115]) saatava tietojen luovuttamiseen rekisteröidyn suostumus ([116]) sen jälkeen kun rekisteröidylle on annettu tiedot 1) siitä, minkätyyppisistä henkilötiedoista on kyse, 2) henkilötietojen vastaanottajasta, 3) mikä on siirron tarkoitus eli mitä tarkoitusta varten vastaanottaja käsittelee tietoja, 4) kuinka kauan vastaanottaja säilyttää tietoja käsittelyä varten, ja 5) että rekisteröidyllä on oikeus olla antamatta suostumustaan (tietosuojalain 17 §:n 2 ja 3 momentti). Ilmoituksen N:o 2021-5 läpinäkyvyyttä koskevassa kohdassa (ks. johdantoosan (70) kappale) edellytetään, että rekisteröidyille on ilmoitettava, mihin kolmanteen maahan heidän tietojaan luovutetaan. Näin varmistetaan, että unionin rekisteröidyt voivat tehdä täysin tietoon perustuvan päätöksen siitä, suostuvatko he tietojensa luovuttamiseen. Rekisterinpitäjä ei myöskään saa tehdä sopimusta tietoja vastaanottavan kolmannen osapuolen kanssa Korean tietosuojalain vastaisesti. Tämä tarkoittaa, että sopimuksessa ei saa määrätä velvoitteista, jotka olisivat ristiriidassa rekisterinpitäjälle tietosuojalaissa asetettujen vaatimusten kanssa ([117]).

([113]) Tieto- ja viestintäpalvelujen tarjoajiin sovelletaan erityisiä sääntöjä. Tietosuojalain 39-12 §:n mukaan tieto- ja viestintäpalvelujen tarjoajien on periaatteessa saatava käyttäjän suostumus kaikkiin henkilötietojen kansainvälisiin siirtoihin. Jos henkilötietojen siirto tapahtuu osana käsittelytoimien ulkoistamista, mukaan lukien tietojen säilyttäminen, suostumusta ei vaadita, jos asianomaisille rekisteröidyille on ilmoitettu etukäteen joko suoraan tai helposti saatavilla olevalla julkisella ilmoituksella, 1) mitä tietoja siirretään, 2) maa johon tiedot siirretään (sekä siirron päivämäärä ja toteutustapa), 3) vastaanottajan nimi ja 4) tarkoitus, jota varten vastaanottaja käyttää ja säilyttää tietoja (tietosuojalain 39-12 §:n 3 momentti). Lisäksi tässä tapauksessa sovelletaan ulkoistamista koskevia yleisiä vaatimuksia. Jokaisen siirron yhteydessä on toteutettava erityisiä suojatoimia, jotka koskevat turvallisuutta ja valitusten ja riitojen käsittelyä, sekä muita toimenpiteitä käyttäjien tietojen suojaamiseksi (tietosuojalain täytäntöönpanoasetuksen 48-10 §).

([114]) Ks. myös tietosuojalain 26 §:n 7 momentti, jonka mukaan lain 15–25, 27–31, 33–38 ja 50 pykälää sovelletaan henkilötietojen käsittelijään soveltuvin osin.

([115]) Tieto- ja viestintäpalvelujen tarjoajat voivat luovuttaa käyttäjien tietoja kolmansille osapuolille vain näiden suostumuksella (tietosuojalain 39-12 §:n 2 momentti).

([116]) Kuten alaviitteessä 51 tarkemmin selitetään, suostumuksen on oltava vapaaehtoinen, tietoinen ja yksilöity, jotta se olisi pätevä.

([117]) Ks. myös tietosuojalain 39-12 §:n 1 momentti, joka koskee tieto- ja viestintäpalvelujen tarjoajia.

(89) Henkilötietoja voidaan luovuttaa kolmannelle osapuolelle (ulkomaille) ilman rekisteröidyn suostumusta, jos luovuttamisen tarkoitus ”liittyy kohtuullisesti” tietojen keräämisen alkuperäiseen tarkoitukseen (tietosuojalain 17 §:n 4 momentti, ks. johdanto-osan (36) kappale). Kun rekisterinpitäjä pohtii, luovutetaanko henkilötietoja tällaiseen ”liitännäiseen” tarkoitukseen vai ei, on otettava huomioon luovuttamisesta rekisteröidylle mahdollisesti aiheutuva vahinko ja se, onko toteutettu tarvittavat turvatoimet (kuten salaus). Koska se kolmas maa, johon henkilötietoja siirretään, ei välttämättä tarjoa samanlaista tietosuojaa kuin Korean tietosuojalaki, ilmoituksessa N:o 2021-5 olevassa 2 kohdassa todetaan, että tällaiset haitat ovat mahdollisia ja että ne voidaan välttää vain jos korealainen rekisterinpitäjä ja ulkomainen vastaanottaja varmistavat sitovalla välineellä (kuten sopimuksella) Korean tietosuojalakia vastaavan tietosuojan tason, myös rekisteröityjen oikeuksien osalta.

(90) Erityissääntöjä sovelletaan ”ilman tarkoitusta” tehtävään luovuttamiseen eli tietojen luovuttamiseen kolmannelle osapuolelle uutta (alkuperäiseen liittymätöntä) tarkoitusta varten. Tämä voidaan toteuttaa ainoastaan jonkin tietosuojalain 18 §:n 2 momentissa mainitun perusteen nojalla, kuten johdanto-osan (39) kappaleessa selitetään. Tietojen luovuttaminen kolmannelle osapuolelle on kuitenkin suljettu pois myös mainituissa tapauksissa, jos se todennäköisesti ”loukkaa oikeudettomasti” rekisteröidyn tai kolmannen osapuolen etuja, mikä edellyttää etujen tasapainottamista. Lisäksi rekisterinpitäjän on tietosuojalain 18 §:n 5 momentin nojalla sovellettava täydentäviä suojatoimia, joihin voi sisältyä esimerkiksi se, että kolmatta osapuolta pyydetään rajoittamaan käsittelyn käyttötarkoitusta tai -tapaa tai toteuttamaan erityisiä turvatoimia. Koska se kolmas maa, johon henkilötietoja siirretään, ei välttämättä tarjoa samanlaista tietosuojaa kuin Korean tietosuojalaki, ilmoituksessa N:o 2021-5 olevassa 2 kohdassa todetaan, että tällaiset rekisteröidyn tai kolmannen osapuolen etujen ”oikeudettomat loukkaukset” ovat mahdollisia ja että ne voidaan välttää vain jos korealainen rekisterinpitäjä ja ulkomainen vastaanottaja varmistavat sitovalla välineellä (kuten sopimuksella) Korean tietosuojalakia vastaavan tietosuojan tason, myös rekisteröityjen oikeuksien osalta.

(91) Siksi johdanto-osan (86)–(90) kappaleessa olevilla säännöillä varmistetaan tietosuojan jatkuvuus olennaisilta osin vastaavalla tavalla kuin asetuksessa (EU) 2016/679, kun henkilötietoja siirretään Korean tasavallasta edelleen (toimeksisaajalle tai kolmannelle osapuolelle).

2.3.10 *Vastuuvelvollisuus*

(92) Vastuuvelvollisuutta koskevan periaatteen mukaisesti tietoja käsittelevien yksiköiden on otettava käyttöön asianmukaiset tekniset ja organisatoriset toimenpiteet, jotta ne voivat tehokkaasti noudattaa tietosuojavelvoitteitaan ja osoittaa erityisesti toimivaltaiselle valvontaviranomaiselle noudattavansa velvoitteita.

(93) Lisäksi rekisterinpitäjän on tietosuojalain 3 §:n 6 ja 8 momentin mukaan käsiteltävä henkilötietoja ”niin, että voidaan minimoida rekisteröidyn yksityisyyden loukkaamisen mahdollisuus” ja pyrittävä saamaan rekisteröidyn luottamus noudattamalla tietosuojalaissa ja muissa siihen liittyvissä säännöksissä säädettyjä velvollisuuksia ja vastuutehtäviä. Tämä tarkoittaa muun muassa sisäisen hallintasuunnitelman laatimista (tietosuojalain 29 §) sekä henkilöstön asianmukaista koulutusta ja valvontaa (28 §).

(94) Vastuuvelvollisuuden varmistamiseksi tietosuojalaissa (31 § yhdessä sen täytäntöönpanoasetuksen 32 §:n kanssa) asetetaan rekisterinpitäjille velvollisuus nimetä tietosuojavastaava, ”joka vastaa kattavasti henkilötietojen käsittelystä”. Tietosuojavastaavan tehtävänä on erityisesti 1) laatia ja panna täytäntöön henkilötietojen suojaa koskeva suunnitelma ja laatia tietosuojaperiaatteet, 2) tehdä säännöllisesti henkilötietojen käsittelyn tilannetta ja käytäntöjä koskevia tarkastuksia mahdollisten puutteiden korjaamiseksi, 3) käsitellä valitukset ja suorittaa korjaustoimet, 4) laatia sisäinen valvontajärjestelmä henkilötietojen luvattoman luovuttamisen tai väärinkäytön estämiseksi, 5) laatia ja panna täytäntöön koulutusohjelma, 6) suojata, valvoa ja hallinnoida henkilötietorekistereitä, ja 7) tuhota henkilötiedot sen jälkeen kun käsittelyn tarkoitus on saavutettu tai säilytysaika päättynyt. Tietosuojavastaava voi näitä tehtäviä suorittaessaan tarkastaa henkilötietojen käsittelyn ja siihen liittyvien järjestelmien tilanteen ja pyytää niitä koskevia tietoja (tietosuojalain 31 §:n 3 momentti). Jos tietosuojavastaava havaitsee, että tietosuojalakia tai muita asiaankuuluvia tietosuojasäännöksiä on rikottu, hänen on välittömästi ryhdyttävä korjaaviin toimenpiteisiin ja tarvittaessa raportoitava toimenpiteistä rekisterinpitäjän johdolle (”johtajalle”) (tietosuojalain 31 §:n 4 momentti). Tietosuojalain 31 §:n 5 momentin mukaan tietosuojavastaavalle ei saa aiheutua perusteetonta haittaa näiden tehtävien suorittamisesta.

(95) Rekisterinpitäjien on myös aktiivisesti pyrittävä tekemään yksityisyydensuojaa koskeva vaikutustenarviointi, jos henkilötietorekisterin toimintaan liittyy yksityisyydensuojaa koskeva riski (tietosuojalain 33 §:n 8 momentti). Arvioitaessa rekisteröityjen oikeuksiin kohdistuvien riskien vakavuutta on otettava huomioon muun muassa sellaisia tekijöitä kuin käsiteltävien tietojen tyyppi ja luonne (erityisesti se, onko kyse arkaluonteisista tiedoista), tietojen määrä, säilytysaika ja tietoturvaloukkausten todennäköisyys (tietosuojalain 33 §:n 1 ja 2 momentti yhdessä sen täytäntöönpanoasetuksen 35, 36 ja 38 §:n kanssa). Yksityisyydensuojaa koskevan vaikutustenarvioinnin tarkoituksena on varmistaa, että yksityisyydensuojaan liittyvät riskitekijät sekä mahdolliset turva- ja muut vastatoimet analysoidaan ja kehittämistä kaipaavat seikat tuodaan esiin (tietosuojalain 33 §:n 1 momentti yhdessä sen täytäntöönpanoasetuksen 38 §:n kanssa).

(96) Julkisten laitosten on tehtävä vaikutustenarviointi, kun ne käsittelevät tiettyjä henkilötietorekistereitä, joihin liittyy suurempi riski mahdollisista tietoturvaloukkauksista (tietosuojalain 33 §:n 1 momentti). Tietosuojalain täytäntöönpanoasetuksen 35 §:n mukaan tämä koskee muun muassa rekistereitä, jotka sisältävät arkaluonteista tietoa vähintään 50 000 rekisteröidystä, rekistereitä, joita verrataan muihin rekistereihin ja joissa on tämän seurauksena tietoa vähintään 500 000 rekisteröidystä, sekä rekisterit, joissa on tietoa vähintään miljoonasta rekisteröidystä. Julkisen laitoksen laatiman vaikutustenarvioinnin tulokset on toimitettava tietosuojalautakunnalle (tietosuojalain 33 §:n 1 momentti), joka voi antaa siitä lausunnon (tietosuojalain 33 §:n 3 momentti).

(97) Tietosuojalain 13 §:ssä säädetään myös, että tietosuojalautakunnan on laadittava toimintapolitiikkoja, jotka tarvitaan rekisterinpitäjien ”itsesääntelyyn perustuvien tietosuojatoimien” edistämiseksi ja tukemiseksi, muun muassa antamalla tietosuojaa koskevaa koulutusta, edistämällä ja tukemalla tietosuojan alalla toimivia organisaatioita ja auttamalla rekisterinpitäjiä itsesääntelysääntöjen laatimisessa ja täytäntöönpanossa. Tietosuojalautakunnan on myös laadittava ePRIVACY-merkintäjärjestelmä ja edistettävä sen käyttöönottoa. Tältä osin tietosuojalaissa (32-2 § yhdessä sen täytäntöönpanoasetuksen 34-2–34-8 §:n kanssa) säädetään mahdollisuudesta varmentaa, että jonkin rekisterinpitäjän henkilötietojen käsittely- ja tietosuojajärjestelmä(t) vastaa(vat) tietosuojalain vaatimuksia. Näiden sääntöjen mukaan asiaa koskeva sertifiointi ([118]) voidaan myöntää (3 vuodeksi), jos rekisterinpitäjä täyttää tietosuojalautakunnan määrittämät kriteerit, joihin sisältyy henkilötietojen suojaa koskevien hallinnollisten, teknisten ja fyysisten suojatoimien laatiminen ([119]). Tietosuojalautakunnan on tutkittava sertifioinnin kannalta merkitykselliset rekisterinpitäjän järjestelmät vähintään kerran vuodessa, jotta sertifiointi pysyy voimassa – se voidaan myös peruuttaa (tietosuojalain 32 §:n 4 momentti yhdessä täytäntöönpanoasetuksen 34-5 §:n kanssa; ns. seurannan hallinnointi).

(98) Näin ollen Korean lainsäädäntökehyksessä on toteutettu vastuuvelvollisuuden periaate siten, että tietosuojan taso vastaa olennaisilta osin asetukseen (EU) 2016/679 mukaista suojelun tasoa. Siinä muun muassa säädetään erilaisista mekanismeista, joiden avulla voidaan varmistaa ja osoittaa tietosuojalain noudattaminen.

2.3.11 *Henkilökohtaisten luottotietojen käsittelyä koskevat erityissäännöt*

(99) Kuten edellä johdanto-osan (13) kappaleessa todetaan, laissa luottotietojen käytöstä ja suojaamisesta (*Act on the Use and Protection of Credit Information*), jäljempänä ’luottotietolaki’, vahvistetaan säännöt, joita sovelletaan kaupallisten toimijoiden suorittamaan henkilökohtaisten luottotietojen käsittelyyn. Henkilökohtaisia luottotietoja käsitellessään kaupallisten toimijoiden on näin ollen noudatettava Korean tietosuojalain yleisiä vaatimuksia, ellei luottotietolaissa ole säädetty yksityiskohtaisempia sääntöjä. Näin on esimerkiksi silloin kun ne käsittelevät luottokorttiin tai pankkitiliin liittyviä tietoja yksittäisen henkilön kanssa liiketoimen yhteydessä. Luottotietolaki on (sekä henkilökohtaisten että muiden) luottotietojen käsittelyä koskeva alakohtainen säädös. Sen lisäksi, että siinä säädetään tietyistä tietosuojaa koskevista suojatoimista (muun muassa läpinäkyvyyden ja turvallisuuden osalta), sillä säännellään yleisemmin niitä erityisolosuhteita, joissa luottotietoja voidaan käsitellä. Tämä näkyy erityisesti niissä yksityiskohtaisissa vaatimuksissa, jotka koskevat tietojen käyttöä, niiden luovuttamista kolmannelle osapuolelle ja säilytysaikaa.

(100) Samoin kuin tietosuojalaki, myös luottotietolaki perustuu käsittelyn lainmukaisuuden ja oikeasuhteisuuden periaatteeseen. Luottotietolain 15 §:n 1 momentissa vahvistetaan ensinnäkin yleisenä vaatimuksena, että henkilökohtaisten luottotietojen kerääminen sallitaan ainoastaan kohtuullisin ja asianmukaisin keinoin ja mahdollisimman vähäisessä määrin tiettyä tarkoitusta varten. Tämä vastaa tietosuojalain 3 §:n 1 ja 2 momentin säännöksiä. Toiseksi luottotietolaissa säädetään erityisesti henkilökohtaisten luottotietojen käsittelyn lainmukaisuudesta rajoittamalla tällaisten tietojen keräämistä, käyttöä ja luovuttamista kolmannelle osapuolelle ja yleisesti sitomalla nämä käsittelytoimet asianomaisen henkilön suostumukseen.

([118]) Jos rekisterinpitäjä aikoo viitata sertifiointiin tai edistää sitä liiketoiminnassaan, se voi lisäksi käyttää tietosuojalautakunnan laatimaa henkilötietojen suojamerkkiä. Ks. tietosuojalain täytäntöönpanoasetuksen 34-7 §.

([119]) Marraskuusta 2018 lähtien on laadittu henkilötietojen ja tietoturvan turvallisuushallintajärjestelmää (Personal Information & Information Security Management System, ISMS-P), jossa varmennetaan, että rekisterinpitäjillä on käytössään kattava hallintajärjestelmä.

(101) Henkilökohtaisia luottotietoja voidaan kerätä jonkin tietosuojalaissa säädetyn perusteen tai jonkin luottotietolaissa säädetyn erityisen perusteen nojalla. Koska asetuksen (EU) 2016/679 45 artiklassa varaudutaan siihen, että unionissa sijaitseva rekisterinpitäjä tai henkilötietojen käsittelijä siirtää henkilötietoja, mutta säännös ei kata Koreassa sijaitsevan rekisterinpitäjän toteuttamaa henkilötietojen keräämistä suoraan (esimerkiksi asianomaisilta yksilöiltä tai verkkosivulta), tämän päätöksen kannalta on merkitystä ainoastaan suostumuksella ja tietosuojalain nojalla käytettävissä olevilla tietojen keräämisen perusteilla. Näihin perusteisiin kuuluvat erityisesti tilanteet, joissa siirto on tarpeen yksilön kanssa tehdyn sopimuksen täytäntöönpanoa varten tai korealaisen rekisterinpitäjän oikeutettujen etujen vuoksi (tietosuojalain 15 §:n 1 momentin 4 ja 6 kohta) ([120]).

(102) Sen jälkeen kun henkilökohtaiset luottotiedot on kerätty, niitä voidaan käyttää 1) siihen alkuperäiseen tarkoitukseen, jota varten asianomainen henkilö ne (suoraan) antoi ([121]); 2) tarkoitukseen, joka on yhteensopiva keräämisen alkuperäisen tarkoituksen kanssa ([122]); 3) sen selvittämiseen, voidaanko asianomaisen henkilön kanssa aloittaa hänen pyytämänsä liikesuhde tai jatkaa sitä ([123]); 4) tilastointia, tutkimusta ja yleisen edun mukaista arkistointia varten ([124]), jos tiedot pseudonymisoidaan ([125]); 5) jos saadaan lisäsuostumus tai 6) laissa säädetyllä tavalla.

(103) Jos kaupallinen toimija aikoo luovuttaa henkilökohtaisia luottotietoja kolmannelle osapuolelle, sen on saatava luovuttamiseen asianomaisen henkilön suostumus ([126]) sen jälkeen kun se on ilmoittanut tälle tietojen vastaanottajan ja sen, mitä tarkoitusta varten vastaanottaja käsittelisi tietoja, tiedot luovutettavista tiedoista ja niiden säilytysajan sekä sen, että henkilöllä on oikeus olla antamatta suostumustaan (luottotietolain 32 §:n 1 momentti ja sen täytäntöönpanoasetuksen 28 §:n 2 momentti) ([127]). Suostumusta koskevaa vaatimusta ei sovelleta erityistilanteissa, eli silloin kun henkilökohtaisia luottotietoja luovutetaan ([128]) 1) toimeksisaajalle ulkoistamistarkoituksessa ([129]); 2) kolmannelle osapuolelle yrityksen luovutuksen, jakautumisen tai sulautumisen vuoksi; 3) tilastointia, tutkimusta ja yleisen edun mukaista arkistointia varten, jos tiedot pseudonymisoidaan; 4) tarkoitukseen, joka on yhteensopiva keräämisen alkuperäisen tarkoituksen kanssa; 5) kolmannelle osapuolelle, joka käyttää tietoja velan perimiseen asianomaiselta henkilöltä ([130]); 6) tuomioistuimen määräyksen noudattamiseksi; 7)

([120]) Luottotietolakiin sisältyy myös muita oikeusperustoja tietojen keräämistä varten, esimerkiksi silloin kun keräämistä edellytetään laissa, tai kun julkinen laitos julkistaa tiedot tiedonvälityksen vapautta koskevan lainsäädännön nojalla, tai kun tiedot ovat saatavilla sosiaalisessa verkostossa. Jotta kaupallinen toimija voisi vedota viimeksi mainittuun perusteeseen, sen on voitava muun muassa osoittaa, että tietojen kerääminen rajoittuu rekisteröidyn antamaan suostumukseen ja perustuu kohtuulliseen (”objektiiviseen”) tulkintaan ja että siinä otetaan huomioon tietojen luonne, aikomus ja tarkoitus saattaa ne saataville sosiaalisessa verkostossa ja se, onko keräämisen tarkoitus kyseisen tarkoituksen kannalta ”erittäin merkityksellinen” (luottotietolain täytäntöönpanoasetuksen 13 §). Kuten johdanto-osan (101) kappaleessa selitetään, näillä perusteilla ei kuitenkaan periaatteessa ole merkitystä siirron kannalta.

([121]) Esimerkiksi silloin kun luottotietoja luodaan/annetaan asianomaisen henkilön kanssa toteutettavan liiketoimen yhteydessä. Tämän perusteen nojalla henkilökohtaisia luottotietoja ei kuitenkaan voida käyttää suoramarkkinointitarkoituksiin (ks. luottotietolain 33 §:n 1 momentin 3 kohta).

([122]) Sen määrittämiseksi, onko tarkoitus yhteensopiva alkuperäisen keräämistarkoituksen kanssa, on otettava huomioon seuraavat tekijät: 1) tarkoitusten keskinäinen suhde (”merkityksellisyys”); 2) tapa, jolla tiedot on kerätty; 3) käytön vaikutus yksilöön; ja se, 4) onko toteutettu asianmukaiset turvatoimet, kuten pseudonymisointi (vrt. luottotietolain 32 §:n 6 momentin 9-4 kohta).

([123]) Rekisterinpitäjä voi esimerkiksi joutua ottamaan huomioon henkilöltä saadut henkilökohtaiset luottotiedot tehdäkseen lainapäätöksen tekemistä varten.

([124]) Luottotietolain 33 § yhdessä 32 §:n 6 momentin 9-2, 9-4 ja 10 kohdan kanssa.

([125]) Pseudonymisoinnilla tarkoitetaan luottotietolain 2 §:n 15 kohdassa olevan määritelmän mukaan henkilökohtaisten luottotietojen käsittelyä siten, että tiedoista ei voida tunnistaa yksilöitä muuten kuin yhdessä lisätietojen kanssa. Vaikka luottotietolaissa säädetään erityisistä suojatoimista silloin kun pseudonymisoituja tietoja käsitellään tilastointia, tutkimusta ja yleisen edun mukaista arkistointia varten (40-2 §), kyseisiä sääntöjä ei sovelleta kaupallisiin organisaatioihin. Sen sijaan niihin sovelletaan tietosuojalain III jaksossa vahvistettuja erityisvaatimuksia, kuten johdanto-osan (42)–(48) kappaleessa kuvataan. Lisäksi luottotietolain 40-3 §:ssä vapautetaan pseudonymisoitujen tietojen käsittely läpinäkyvyyttä ja yksilön oikeuksia koskevista vaatimuksista (silloin kun käsittely tapahtuu tilastointia, tieteellistä tutkimusta tai yleisen edun mukaista arkistointia varten). Vastaavista poikkeuksista säädetään tietosuojalain 28-7 §:ssä ja niihin sovellettavista suojatoimista tietosuojalain III jaksossa, joita käsitellään lähemmin johdanto-osan (42)–(48) kappaleessa.

([126]) Tätä ei sovelleta silloin kun henkilökohtaisia luottotietoja luovutetaan kolmannelle osapuolelle niiden tarkentamista ja päivittämistä varten, jos luovuttaminen tapahtuu alkuperäisen käsittelytarkoituksen puitteissa (luottotietolain 32 §:n 1 momentti). Näin voi olla esimerkiksi silloin kun päivitettyjä tietoja toimitetaan luottoluokituslaitokselle sen varmistamiseksi, että sen tiedot ovat ajan tasalla.

([127]) Jos edellä mainittujen tietojen toimittaminen on käytännössä hankalaa, voi riittää, että henkilö ohjataan ottamaan yhteyttä vastaanottajana olevaan kolmanteen osapuoleen tarvittavien tietojen antamista varten.

([128]) Koska luottotietolaissa ei erikseen säännellä henkilökohtaisten luottotietojen luovuttamista ulkomaille, tällaisen luovuttamisen yhteydessä on noudatettava tietojen edelleen siirtämistä varten säädettyjä suojatoimia (ilmoituksessa N:o 2021-5 oleva 2 kohta).

([129]) Henkilökohtaisten luottotietojen käsittely voidaan ulkoistaa ainoastaan kirjallisen sopimuksen perusteella ja tietosuojalain 26 §:n 1–3 ja 5 momentissa säädettyjen vaatimusten mukaisesti, kuten johdanto-osan (20) kappaleessa esitetään (luottotietolain 17 § ja sen täytäntöönpanoasetuksen 14 §). Toimeksisaaja saa käyttää tietoja ainoastaan ulkoistetun tehtävän suorittamista varten, ja ulkoistavan yrityksen on otettava käyttöön erityiset turvatoimet (esim. salaus) ja annettava toimeksisaajalle koulutusta siitä, miten estetään luottotietojen katoaminen, varastaminen, paljastaminen, muuttaminen tai vaarantuminen.

([130]) Ks. myös luottotietolain täytäntöönpanoasetuksen 28 §:n 10 momentin 1, 2 ja 6 kohta.

syyttäjälle/poliisiviranomaiselle hätätilanteessa, kun asianomaisen henkilön henki tai terveys on vaarassa eikä ole aikaa hankkia tuomioistuimen päätöstä ([131]); 8) toimivaltaisille veroviranomaisille verolainsäädännön noudattamiseksi; tai 9) muun lainsäädännön noudattamiseksi. Jos tietoja luovutetaan jollakin näistä perusteista, rekisteröidylle on ilmoitettava siitä etukäteen (luottotietolain 32 §:n 7 momentti).

(104) Luottotietolaissa säännellään myös erikseen sitä, kuinka kauan henkilökohtaisia luottotietoja voidaan käsitellä niiden perusteiden nojalla, jotka koskevat tietojen käyttöä tai luovuttamista kolmannelle osapuolelle sen jälkeen kun liikesuhde asianomaiseen henkilöön on päättynyt ([132]). Vain sellaiset tiedot voidaan säilyttää, jotka olivat tarpeen kyseisen liikesuhteen luomiseksi tai ylläpitämiseksi, edellyttäen että sovelletaan täydentäviä suojatoimia (tiedot on säilytettävä erillään niiden henkilöiden luottotiedoista, joiden kanssa liikesuhde on edelleen voimassa, ne on suojattava erityisin turvatoimin ja niiden on oltava ainoastaan valtuutettujen henkilöiden saatavilla) ([133]). Kaikki muut tiedot on poistettava (luottotietolain täytäntöönpanoasetuksen 17-2 §:n 1 momentin 2 kohta). Sen määrittämiseksi, mitkä tiedot olivat tarpeen liikesuhdetta varten, on otettava huomioon muun muassa se, olisiko liikesuhde voitu luoda ilman kyseisiä tietoja ja liittyvätkö tiedot suoraan asianomaiselle henkilölle toimitettuihin tavaroihin tai palveluihin (luottotietolain täytäntöönpanoasetuksen 17-2 §:n 2 momentti).

(105) Myös silloin kun henkilökohtaisia luottotietoja saa periaatteessa säilyttää liikesuhteen päättymisen jälkeen, ne on poistettava kolmen kuukauden kuluessa siitä kun myöhemmän käsittelyn tarkoitus on saavutettu ([134]) tai viimeistään viiden vuoden kuluttua (luottotietolain 20-2 §). Henkilökohtaisia luottotietoja voidaan säilyttää yli viiden vuoden ajan vain rajatuissa tilanteissa, erityisesti jos se on tarpeen lakisääteisen velvoitteen noudattamiseksi; yksittäisen henkilön hengen, terveyden tai omaisuuden suojaamiseksi; pseudonymisoitujen tietojen arkistointia varten (kun tietoja on käytetty tieteellistä tutkimusta, tilastointia tai yleisen edun mukaista arkistointia varten); vakuutukseen liittyviin tarkoituksiin (erityisesti vakuutusmaksuja tai vakuutuspetosten ehkäisemistä varten) ([135]). Näissä poikkeustapauksissa sovelletaan erityisiä suojatoimia (kuten asianomaiselle henkilölle tehtävä ilmoitus myöhemmästä käytöstä, säilytettävien tietojen erottaminen niiden henkilöiden tiedoista, joiden kanssa liikesuhde on edelleen voimassa, ja pääsyoikeuksien rajoittaminen, ks. luottotietolain täytäntöönpanoasetuksen 17-2 §:n 1 ja 2 momentti).

(106) Luottotietolaissa myös täsmennetään tietojen täsmällisyyttä ja laatua koskevia periaatteita edellyttämällä, että henkilökohtaiset luottotiedot ”rekisteröidään ja että niitä muutetaan ja hallinnoidaan” niin, että ne ovat täsmälliset ja ajantasaiset (luottotietolain 18 §:n 1 momentti ja sen täytäntöönpanoasetuksen 15 §:n 3 momentti) ([136]). Kun kaupalliset toimijat toimittavat luottotietoja tietyille muille yksiköille (kuten luottoluokituslaitoksille), niiden on myös erityisesti tarkistettava tietojen täsmällisyys sen varmistamiseksi, että vastaanottaja rekisteröi ja hallinnoi ainoastaan täsmällisiä tietoja (luottotietolain täytäntöönpanoasetuksen 15 §:n 1 momentti yhdessä luottotietolain 18 §:n 1 momentin kanssa). Luottotietolaissa edellytetään yleisesti, että henkilökohtaisten luottotietojen keräämisestä, käytöstä, luovuttamisesta kolmannelle osapuolelle ja poistamisesta on pidettävä kirjaa (luottotietolain 20 §:n 2 momentti) ([137]).

(107) Henkilökohtaisten luottotietojen käsittelyyn sovelletaan myös erityisiä tietoturvavaatimuksia. Luottotietolaissa edellytetään erityisesti sellaisten teknisten, fyysisten ja organisatoristen toimenpiteiden toteuttamista, joilla voidaan estää luvaton pääsy tietojärjestelmiin sekä käsiteltävien tietojen muuttaminen ja poistaminen ja muut niihin liittyvät riskit (esimerkiksi pääsynvalvonnan avulla, ks. luottotietolain 19 § ja sen täytäntöönpanoasetuksen 16 §). Lisäksi vaihdettaessa henkilökohtaisia luottotietoja kolmannen osapuolen kanssa on tehtävä sopimus, jossa määrätään erityisistä turvatoimista (luottotietolain 19 §:n 2 momentti). Jos tapahtuu henkilökohtaisia luottotietoja koskeva tietoturvaloukkaus, on toteutettava toimenpiteet vahinkojen minimoimiseksi, ja asianomaisille henkilöille on ilmoitettava asiasta viipymättä (luottotietolain 39-4 §:n 1 ja 2 momentti). Lisäksi tietosuojalautakunnalle on annettava tiedoksi asianomaisille henkilöille annettu ilmoitus ja toteutetut toimenpiteet (luottotietolain 39-4 §:n 4 momentti).

([131]) Tässä tapauksessa tuomioistuimen päätöstä on haettava viipymättä. Jos sitä ei saada 36 tunnin kuluessa, vastaanotetut tiedot on poistettava viipymättä (luottotietolain 32 §:n 6 momentin 6 kohta).

([132]) Esimerkiksi siksi, että sopimusvelvoitteet on täytetty tai että jompikumpi osapuoli on käyttänyt oikeuttaan irtisanoa sopimus. Ks. luottotietolain täytäntöönpanoasetuksen 17-2 §:n 5 momentti).

([133]) Luottotietolain 20-2 §:n 1 momentti ja sen täytäntöönpanoasetuksen 17-2 §:n 1 momentin 1 kohta.

([134]) Määräajan asettamisessa on otettu huomioon, että tietoja ei yleensä ole mahdollista poistaa välittömästi, vaan se edellyttää tiettyjä työvaiheita, joiden toteuttaminen vie jonkin verran aikaa (kuten poistettavien tietojen erottaminen muista tiedoista ja poiston suorittaminen tietojärjestelmien vakautta heikentämättä).

([135]) Luottotietolain 20-2 §:n 2 momentti.

([136]) Luottotietolain 18 §:n 2 momentissa ja sen täytäntöönpanoasetuksen 15 §:n 4 momentissa säädetään kirjanpitovaatimusta koskevista yksityiskohtaisemmista säännöistä, jotka koskevat muun muassa tietoja, joista voi aiheutua asianomaiselle vahinkoa, kuten rikostaustaa tai konkurssia koskevat tiedot.

([137]) Muiden vastuuvelvollisuusmekanismien osalta luottotietolaissa edellytetään, että tietyt organisaatiot (kuten osuuskunnat ja julkiset yhtiöt, ks. luottotietolain täytäntöönpanoasetuksen 21 §:n 2 momentti) nimittävät ”luottotietovastaavan” (*credit information administrator/guardian*), jonka vastaa luottotietolain noudattamisesta ja hoitaa tietosuojalaissa tarkoitetun tietosuojavastaavan (*privacy officer*) tehtäviä (luottotietolain 20 §:n 3 ja 4 momentti).

(108) Luottotietolaissa säädetään myös erityisistä läpinäkyvyyttä koskevista velvoitteista silloin kun hankitaan suostumus henkilökohtaisten luottotietojen käyttöä tai luovuttamista varten (luottotietolain 32 §:n 4 momentti ja 34-2 § ja sen täytäntöönpanoasetuksen 30-3 §) ja yleisemmin ennen tietojen toimittamista kolmannelle osapuolelle (luottotietolain 32 §:n 7 momentti) ([138]). Lisäksi yksilöillä on oikeus saada pyynnöstä tietoja luottotietojensa käytöstä ja luovuttamisesta kolmansille osapuolille pyyntöä edeltävien kolmen vuoden ajalta (mukaan lukien tällaisen käytön/luovuttamisen tarkoitus ja päivämäärät) ([139]).

(109) Luottotietolain nojalla yksilöillä on myös oikeus saada pääsy henkilökohtaisiin luottotietoihinsa (38 §:n 1 momentti) ja saada virheelliset tiedot oikaistuiksi (38 §:n 2 ja 3 momentti) ([140]). Sen lisäksi, että tietosuojalaissa säädetään tietojen poistamista koskevasta yleisestä oikeudesta (ks. johdanto-osan (77) kappale), luottotietolaissa säädetään henkilökohtaisia luottotietoja koskevasta erityisestä oikeudesta, jonka nojalla tiedot on poistettava, kun niitä on säilytetty yli johdanto-osan (104) kappaleessa mainitun ajan eli yli viisi vuotta (henkilökohtaiset luottotiedot, jotka olivat tarpeen liikesuhteen luomiseksi tai ylläpitämiseksi) tai yli kolme kuukautta (muuntyyppiset henkilökohtaiset luottotiedot) ([141]). Tietojen poistamista koskeva pyyntö voidaan poikkeuksellisesti evätä, jos tietojen säilyttämistä on tarpeen jatkaa johdanto-osan (105) kappaleessa kuvatuissa olosuhteissa. Jos yksilö pyytää tietojen poistamista, mutta sovelletaan jotakin poikkeusta, kyseisiin luottotietoihin on sovellettava erityisiä suojatoimia (luottotietolain 38-3 §:n 3 momentti ja sen täytäntöönpanoasetuksen 33-3 §). Tiedot on esimerkiksi säilytettävä erillään muista tiedoista, pääsy niihin on myönnettävä vain valtuutetuille henkilöille ja niihin on sovellettava erityisiä turvatoimia.

(110) Edellä johdanto-osan (109) kappaleessa mainittujen oikeuksien lisäksi tietosuojalaissa taataan yksilöille oikeus pyytää rekisterinpitäjää lopettamaan yhteydenpito heihin suoramarkkinointitarkoituksissa (37 §:n 2 momentti) ja oikeus siirtää tiedot järjestelmästä toiseen. Viimeksi mainitun osalta tietosuojalaissa säädetään, että yksilöillä on oikeus pyytää, että heidän henkilökohtaiset luottotietonsa toimitetaan heille itselleen tai tietylle kolmannelle osapuolelle (kuten rahoituslaitokselle tai luottoluokitusyritykselle). Henkilökohtaiset luottotiedot on käsiteltävä ja toimitettava kolmannelle osapuolelle muodossa, jota voidaan käsitellä tietojenkäsittelylaitteella (kuten tietokoneella).

(111) Siltä osin kuin luottotietolaissa on erityissäännöksiä suhteessa tietosuojalakiin, komissio katsoo, että kyseisillä säännöillä varmistetaan tietosuojan taso, joka vastaa olennaisilta osin asetuksessa (EU) 2016/679 taattua suojan tasoa.

2.4 **Valvonta ja täytäntöönpano**

(112) Sen varmistamiseksi, että tietosuojan riittävä taso taataan käytännössä, olisi oltava riippumaton valvontaviranomainen, jonka tehtävänä on valvoa tietosuojasääntöjen noudattamista ja varmistaa niiden täytäntöönpano. Kyseisen viranomaisen olisi toimittava riippumattomasti ja puolueettomasti tehtäviään suorittaessaan ja toimivaltuuksiaan käyttäessään.

2.4.1 *Riippumaton valvonta*

(113) Korean tasavallassa tietosuojalain noudattamisen valvonnasta ja täytäntöönpanosta vastaava viranomainen on tietosuojalautakunta. Se koostuu puheenjohtajasta, varapuheenjohtajasta ja seitsemästä jäsenestä. Presidentti nimittää puheenjohtajan ja varapuheenjohtajan pääministerin suosituksen perusteella. Presidentti nimittää myös jäsenet: kaksi puheenjohtajan suosituksesta ja viisi kansalliskokouksen suosituksesta (näistä viidestä kaksi

([138]) Tähän sisältyy yleinen ilmoittamisvaatimus (luottotietolain 32 §:n 7 momentti) ja erityinen läpinäkyvyyttä koskeva velvoite siinä tapauksessa, että tietyn henkilön luottokelpoisuuden määrittämisessä käytetyt tiedot luovutetaan tietyille yksiköille, kuten luottoluokituslaitoksille ja luottotietoja kerääville virastoille (luottotietolain 35-3 § ja sen täytäntöönpanoasetuksen 30-3 §), tai kun liikesuhde evätään tai lopetetaan kolmannelta osapuolelta saatujen henkilökohtaisten luottotietojen perusteella (luottotietolain 36 § ja sen täytäntöönpanoasetuksen 31 §).

([139]) Luottotietolain 35 §. Tietyille kaupallisille organisaatioille, kuten osuuskunnille ja julkisille yhtiöille (luottotietolain täytäntöönpanoasetuksen 21 §:n 2 momentti) on asetettu läpinäkyvyyttä koskevia lisävaatimuksia, joiden nojalla niiden on saatettava määrätyt tiedot julkisesti saataville (luottotietolain 31 §) ja ilmoitettava asianomaisille henkilöille näiden luottoluokitukselle mahdollisesti aiheutuvista haitoista, kun ne toteuttavat luottoriskejä aiheuttavia rahoitustoimia (luottotietolain 35-2 §).

([140]) Pääsyoikeutta ja oikeutta tietojen oikaisemiseen koskevien edellytysten ja poikkeusten osalta sovelletaan tietosuojalain sääntöjä (ks. johdanto-osan (76)–(77) kappale). Lisäksi luottotietolain 38 §:n 4–8 momentissa ja sen täytäntöönpanoasetuksen 33 §:ssä säädetään täydentävistä säännöistä. Niiden mukaan kaupallisen toimijan on ilmoitettava asianomaiselle henkilölle tämän virheellisten luottotietojen oikaisemisesta ja poistamisesta. Lisäksi näistä korjauksista on ilmoitettava kaikille kolmansille osapuolille, joille kyseiset tiedot on luovutettu edeltävien kuuden kuukauden aikana, ja tämä ilmoitus on annettava tiedoksi myös asianomaiselle itselleen. Jos asianomainen ei ole tyytyväinen tapaan, jolla oikaisupyyntö on käsitelty, hän voi esittää pyynnön tietosuojalautakunnalle, joka tarkistaa rekisterinpitäjän toimet ja voi määrätä korjaavia toimenpiteitä.

([141]) Tietosuojalain 38-3 §.

nimitetään presidentin puolueen edustajien suosituksesta ja kolme muiden puolueiden edustajien suosituksesta (tietosuojalain 7-2 §:n 2 momentti); näin pyritään torjumaan nimitysmenettelyn puolueellisuutta ([142]). Menettely vastaa vaatimuksia, joita sovelletaan tietosuojaviranomaisten jäsenten nimittämiseen unionissa (asetuksen (EU) 2016/679 53 artiklan 1 kohta). Tietosuojalautakunnan jäsenten on myös pidättäydyttävä kaikesta voittoa tavoittelevasta liiketoiminnasta ja poliittisesta toiminnasta eivätkä he saa olla julkishallinnon tai kansalliskokouksen palveluksessa (tietosuojalain 7-6 § ja 7-7 §:n 1 momentin 3 kohta) ([143]). Kaikkiin lautakunnan jäseniin sovelletaan myös erityisiä sääntöjä, jotka estävät heitä osallistumasta asioiden käsittelyyn tapauksissa, joissa eturistiriita on mahdollinen (tietosuojalain 7-11 §). Tietosuojalautakuntaa avustaa sihteeristö (7-13 §), ja se voi perustaa (kolmesta jäsenestä koostuvia) alakomiteoita käsittelemään vähäisiä rikkomuksia ja toistuvia asioita (tietosuojalain 7-12 §).

(114) Tietosuojalautakunnan jäsenten toimikausi on kolme vuotta, ja se voidaan uusia kerran (tietosuojalain 7-4 §:n 1 momentti). Jäsenet voidaan erottaa tehtävästään vain erityisissä olosuhteissa eli jos he eivät enää kykene hoitamaan tehtäviään pitkäaikaisen fyysisen tai psyykkisen toimintakyvyttömyyden vuoksi, tai jos he ovat rikkoneet lakia tai jos jokin virantoimituksesta pidättämiseen oikeuttava peruste täyttyy ([144]) (tietosuojalain 7-5 §). Tämä antaa heille institutionaalisen suojan heidän hoitaessaan tehtäviään.

(115) Tietosuojalain 7 §:n 1 momentissa taataan nimenomaisesti tietosuojalautakunnan riippumattomuus, ja 7-5 §:n 2 momentissa edellytetään, että lautakunnan jäsenten on hoidettava tehtävänsä riippumattomasti ja lain ja omantuntonsa mukaisesti ([145]). Kuvatuilla institutionaalisilla ja menettelyllisillä suojatoimilla, jotka koskevat muun muassa tietosuojalautakunnan jäsenten nimittämistä ja erottamista, varmistetaan lautakunnan täydellinen riippumattomuus suhteessa ulkopuoliseen vaikuttamiseen tai ohjeisiin. Keskushallinnon virastona tietosuojalautakunta laatii itse vuotuisen talousarvionsa (jonka valtiovarainministeriö tarkistaa osana valtion kokonaistalousarviota ennen kuin kansalliskokous vahvistaa sen) ja vastaa omasta henkilöstöhallinnostaan. Tietosuojalautakunnan budjetti on tällä hetkellä noin 35 miljoonaa euroa, ja sillä on 154 työntekijää (joista 40 on erikoistunut tieto- ja viestintätekniikkaan, 32 tutkintaan ja 40 on oikeudellisia asiantuntijoita).

(116) Tietosuojalautakunnan tehtävät ja toimivalta määritellään lähinnä tietosuojalain 7-8 ja 7-9 §:ssä sekä 61–66 §:ssä ([146]). Tietosuojalautakunnan tehtäviin kuuluu erityisesti neuvonnan antaminen tietosuojaa koskevista laeista ja asetuksista, tietosuojaa koskevien politiikkatoimien ja ohjeiden laatiminen, yksilön oikeuksiin kohdistuvien loukkausten tutkinta, valitusten käsittely ja riitojen sovittelu, tietosuojalain noudattamisen valvonta, tietosuojaa koskevan koulutuksen ja tietämyksen edistäminen sekä tietojenvaihto ja yhteistyö kolmansien maiden tietosuojaviranomaisten kanssa ([147]).

(117) Tietyt tietosuojalautakunnan tehtävät on siirretty Korean internet- ja turvallisuusvirastolle (tietosuojalain 68 § yhdessä sen täytäntöönpanoasetuksen 62 §:n kanssa): 1) koulutus ja suhdetoiminta, 2) asiantuntijoiden koulutus ja yksityisyydensuojaa koskevien vaikutustenarviointien kriteerit, 3) nk. yksityisyydensuojan arviointilaitoksen nimeämistä koskevien pyyntöjen käsittely, 4) epäsuoraa pääsyä viranomaisten hallussa oleviin henkilötietoihin koskevien pyyntöjen käsittely (tietosuojalain 35 §:n 2 momentti), ja 5) yksityisyydensuojaa koskevan puhelinpalvelun (Privacy Call Centre) kautta tuleviin valituksiin liittyvien aineistojen pyytäminen ja

([142]) Tietosuojalautakunnan jäseniksi voidaan nimittää ainoastaan henkilöitä, jotka täyttävät seuraavat vaatimukset: henkilötietoasioista vastaavat johtavassa asemassa olevat virkamiehet; entiset tuomarit, syyttäjät tai vähintään 10 vuotta asianajajan tehtävissä toimineet henkilöt; entiset johtajat, joilla on yli kolmen vuoden kokemus tietosuoja-asioista julkisen laitoksen tai organisaation palveluksessa tai joita tällainen laitos tai organisaatio suosittelee; ja entiset apulaisprofessorit, joilla on vähintään viiden vuoden ammatillinen tietämys tietosuoja-asioista akateemisessa instituutiossa (tietosuojalain 7-2 §).

([143]) Ks. myös tietosuojalain täytäntöönpanoasetuksen 4-2 §.

([144]) Ks. tietosuojalain 7-7 §, jonka mukaan tietosuojalautakunnan jäseniksi ei voida nimittää ulkomaiden kansalaisia eikä poliittisten puolueiden jäseniä. Sama koskee henkilöitä, joille on määrätty tietyntyyppisiä rikosoikeudellisia seuraamuksia tai jotka on edeltävien viiden vuoden aikana erotettu virastaan kurinpitoseuraamuksella (tietosuojalain 7-7 § yhdessä virkamieslain (*Public Officials Act*) 33 §:n kanssa).

([145]) Tietosuojalain 7 §:n 2 momentissa viitataan pääministerin yleiseen toimivaltaan, jonka perusteella hän voi hallinnon organisaatiota koskevan lain (*Government Organisation Act*) 18 §:n nojalla ja presidentin suostumuksella keskeyttää minkä tahansa keskushallinnon antaman päätöksen soveltamisen tai peruuttaa sen; tämä toimivalta ei kuitenkaan kata tietosuojalautakunnan tutkinta- tai täytäntöönpanovaltuuksia (ks. tietosuojalain 7 §:n 2 momentin 1 ja 2 kohta). Korean hallitukselta saatujen selvitysten mukaan edellä mainitun, hallituksen organisaatiota koskevan lain 18 §:n tarkoituksena on antaa pääministerille mahdollisuus toimia poikkeuksellisissa olosuhteissa, esimerkiksi sovitella eri viranomaisten välisiä erimielisyyksiä. Pääministeri ei kuitenkaan ole koskaan käyttänyt tätä toimivaltaa siitä lähtien kun kyseinen säännös hyväksyttiin vuonna 1963.

([146]) Tietosuojalautakunta voi pyytää lausuntoja virkamiehiltä, tietosuoja-alan asiantuntijoilta, kansalaisjärjestöiltä ja elinkeinoelämän toimijoilta, jos se on tarpeen sille tietosuojalain 7-9 §:n 1 momentin nojalla kuuluvien tehtävien hoitamiseksi. Lisäksi tietosuojalautakunta voi pyytää asiaankuuluvia aineistoja, antaa parannussuosituksia ja tarkistaa niiden täytäntöönpanon (tietosuojalain 7-9 §:n 2–5 momentti).

([147]) Ks. myös tietosuojalain 9 § (kolmen vuoden välein laadittava henkilötietojen suojaa koskeva yleissuunnitelma), 12 § (henkilötietojen suojaa koskevat yleisohjeet) ja 13 § (itsesääntelyn edistämistä ja tukemista koskevat toimintapolitiikat).

tarkastusten suorittaminen. Privacy Call Centren kautta tulevien valitusten käsittelyn yhteydessä Korean internet- ja turvallisuusvirasto välittää tapauksen joko tietosuojalautakunnalle tai syyttäjälle, jos se katsoo, että lakia on rikottu. Mahdollisuus tehdä valitus Privacy Call Centren kautta ei estä yksityishenkilöitä tekemästä valitusta suoraan tietosuojalautakunnalle tai kääntymästä sen puoleen, jos he katsovat, että Korean internet- ja turvallisuusvirasto ei ole käsitellyt heidän valitustaan tyydyttävällä tavalla.

2.4.2 *Noudattamisen valvonta, ml. seuraamukset*

(118) Jotta voitaisiin varmistaa tietosuojalain noudattaminen, lainsäätäjä on antanut tietosuojalautakunnalle sekä tutkinta- että täytäntöönpanovaltuudet, joiden nojalla se voi toteuttaa erilaisia toimenpiteitä suositusten antamisesta hallinnollisiin sakkoihin. Näitä valtuuksia täydennetään rikosoikeudellisten seuraamusten järjestelmällä.

(119) Tutkintavaltuuksien osalta voidaan todeta, että jos epäillään tietosuojalain rikkomista tai jos sellaisesta on ilmoitettu tai jos se on tarpeen rekisteröityjen oikeuksien suojaamiseksi, tietosuojalautakunta voi suorittaa tutkimuksia paikalla ja vaatia rekisterinpitäjiltä kaikkia asiaankuuluvia aineistoja (kuten esineitä ja asiakirjoja) (tietosuojalain 63 § yhdessä sen täytäntöönpanoasetuksen 60 §:n kanssa) ([148]).

(120) Täytäntöönpanovaltuuksien osalta tietosuojalautakunta voi tietosuojalain 61 §:n 2 momentin nojalla antaa rekisterinpitäjille neuvoja siitä, miten henkilötietojen suojan tasoa voitaisiin parantaa tiettyjen käsittelytoimien yhteydessä. Rekisterinpitäjien on pyrittävä noudattamaan näitä neuvoja vilpittömässä mielessä ja ilmoitettava toimien tuloksista tietosuojalautakunnalle. Tietosuojalautakunta voi myös määrätä toteutettavaksi korjaavia toimenpiteitä, jos on perusteltu syy olettaa, että tietosuojalakia on rikottu ja että toimien laiminlyönti todennäköisesti aiheuttaisi vaikeasti korjattavissa olevaa vahinkoa (tietosuojalain 64 §:n 1 momentti) ([149]). Ilmoituksen N:o 2021-5 (liite I) 5 kohdassa selvennetään sitovasti, että nämä edellytykset täyttyvät aina kun rikotaan sellaisia tietosuojalain säännöksiä, joilla suojataan yksilöiden oikeutta yksityisyyteen henkilötietojen osalta ([150]). Tietosuojalautakunnalla on muun muassa valtuudet määrätä, että rikkomiseen johtanut toiminta on lopetettava tai kyseinen tietojenkäsittely väliaikaisesti keskeytettävä, tai muita tarvittavia toimenpiteitä. Korjaavien toimenpiteiden laiminlyönti voi johtaa enintään 50 miljoonan wonin sakkojen määräämiseen (tietosuojalain 75 §:n 2 momentin 13 kohta).

(121) Tietosuojalain 64 §:n 4 momentissa säädetään eräiden viranomaisten (mm. kansalliskokouksen, keskushallinnon virastojen, paikallishallinnon elinten ja tuomioistuinten) osalta, että tietosuojalautakunta voi ”suosittaa” johdantoosan (120) kappaleessa mainittuja korvaavia toimenpiteitä ja että kyseisten viranomaisten on noudatettava tällaista suositusta, paitsi jos on kyse poikkeuksellisista olosuhteista. Ilmoituksessa N:o 2021-5 olevan 5 kohdan mukaan tällä tarkoitetaan tosiasiallisia tai oikeudellisia poikkeusolosuhteita, joista tietosuojalautakunta ei ollut tietoinen suosituksen antaessaan. Kyseinen viranomainen voi vedota tällaisiin poikkeuksellisiin olosuhteisiin vain jos se pystyy selkeästi osoittamaan, ettei sääntöjä ole rikottu ja tietosuojalautakunta vahvistaa, että tämä pitää paikkansa. Muussa tapauksessa viranomaisen on noudatettava tietosuojalautakunnan suositusta ja ”toteutettava korjaavat toimenpiteet, joihin voi kuulua myös toiminnan välitön lopettaminen, ja korvattava vahingot siinä poikkeuksellisessa tapauksessa, että lainvastainen toimenpide on kuitenkin tapahtunut”.

(122) Tietosuojalautakunta voi myös pyytää muita hallintovirastoja, joilla on alakohtaisen lainsäädännön nojalla erityistoimivaltaa (esimerkiksi terveyden tai koulutuksen alalla), tutkimaan (epäiltyjä) tietosuojalain rikkomisia (joko itse tai yhdessä tietosuojalautakunnan kanssa) ja määräämään korjaavia toimenpiteitä toimivaltansa piiriin kuuluville rekisterinpitäjille (tietosuojalain 63 §:n 4 ja 5 momentti). Siinä tapauksessa tietosuojalautakunta määrittää tutkinnan perusteet, tavoitteen ja laajuuden ([151]). Asianomaisen hallintoviranomaisen on puolestaan esitettävä tietosuojalautakunnalle tarkastussuunnitelma ja annettava sille tiedoksi tarkastuksen tulokset. Tietosuojalautakunta voi suosittaa jotakin tiettyä korjaavaa toimenpidettä, ja viranomaisen on pyrittävä toteuttamaan se. Tällainen pyyntö ei kuitenkaan rajoita tietosuojalautakunnan toimivaltaa toteuttaa omia tutkimuksia tai määrätä seuraamuksia.

([148]) Tietosuojalautakunnalla on myös oikeus päästä rekisterinpitäjän tiloihin tarkastamaan liiketoiminnan tila, kirjanpito, asiakirjat jne. (tietosuojalain 63 §:n 2 momentti). Ks. myös luottotietolain 45-3 § ja sen täytäntöönpanoasetuksen 36-4 §, joissa säädetään kyseiseen lakiin perustuvista tietosuojalautakunnan toimivaltuuksista.

([149]) Ks. myös luottotietolain 45-4 §, jossa säädetään kyseiseen lakiin perustuvista tietosuojalautakunnan toimivaltuuksista.

([150]) Ilmoituksen 5 kohdassa todetaan, että tietosuojalain 64 §:n 1 ja 2 momentissa olevalla ilmaisulla ”merkittävä peruste katsoa, että on tapahtunut henkilötietoja koskeva tietoturvaloukkaus, jonka edellyttämien toimenpiteiden laiminlyönti aiheuttaisi todennäköisesti vaikeasti korjattavissa olevan vahingon” tarkoitetaan, että yksilöiden henkilötietojen suojaa koskevaan lainsäädäntöön sisältyviä periaatteita, oikeuksia ja velvollisuuksia on loukattu. Samaa sovelletaan tietosuojalautakunnan valtuuksiin, joista säädetään luottotietolain 45-4 §:ssä.

([151]) Viestinnän tietosuojalain täytäntöönpanoasetuksen 60 §.

(123) Korjaavien valtuuksiensa lisäksi tietosuojalautakunta voi määrätä 10–50 miljoonan wonin hallinnolliset sakot tietosuojalain eri säännösten rikkomisen perusteella (tietosuojalain 75 §) ([152]). Tämä tarkoittaa muun muassa käsittelyn lainmukaisuutta koskevien vaatimusten noudattamatta jättämistä, tarvittavien turvatoimien tai tietoturvaloukkauksista rekisteröidyille tehtävän ilmoituksen laiminlyöntiä, tietosuojaselosteen laatimista ja julkaisemista tai tietosuojavastaavan nimittämistä koskevan vaatimuksen laiminlyöntiä tai rekisteröidyn oikeuksien käyttöä koskevan pyynnön täyttämättä jättämistä sekä eräitä menettelyyn liittyviä rikkomuksia (yhteistyöstä kieltäytyminen tutkinnan yhteydessä). Jos sama rekisterinpitäjä rikkoo useita tietosuojalain säännöksiä, kustakin rikkomuksesta voidaan määrätä erillinen sakko, jonka suuruuden määrittämisessä otetaan huomioon niiden rekisteröityjen lukumäärä, joihin rikkomus vaikuttaa.

(124) Jos on olemassa perusteltu syy epäillä tietosuojalain tai ”jonkin muun tietosuojaa koskevan säännöksen” rikkomista, tietosuojalautakunta voi myös tehdä rikosilmoituksen toimivaltaiselle tutkintavirastolle (esimerkiksi syyttäjälle, ks. tietosuojalain 65 §:n 1 momentti). Tietosuojalautakunta voi myös ohjeistaa rekisterinpitäjää toteuttamaan kurinpitotoimenpiteitä rikkomisesta vastuussa olevaa henkilöä kohtaan (myös vastaavaa johtajaa kohtaan, ks. tietosuojalain 65 §:n 2 momentti). Tällaisen ohjeen saatuaan rekisterinpitäjän on noudatettava ([153]) sitä ja annettava tietosuojalautakunnalle kirjallisesti tiedoksi toimenpiteen tulos (tietosuojalain 65 § yhdessä sen täytäntöönpanoasetuksen 58 §:n kanssa).

(125) Tietosuojalautakunta voi julkaista verkkosivullaan tai yleisessä valtakunnallisessa päivälehdessä tiedot rikkomisesta ja siihen syyllistyneestä yksiköstä ja rikkomisen perusteella määrätyistä toimenpiteistä, kun on kyse ohjeista (tietosuojalain 61 §), korjaavista toimenpiteistä (64 §), syytetoimista tai kurinpitotoimia koskevista ohjeista (65 §) ja hallinnollisten sakkojen määräämisestä 75 §:n nojalla (tietosuojalain 66 § yhdessä sen täytäntöönpanoasetuksen 61 §:n 1 momentin kanssa) ([154]).

(126) Tietosuojalain (ja muiden ”tietosuojaa koskevien säännösten”) tietosuojavaatimusten noudattamista tuetaan myös rikosoikeudellisilla seuraamuksilla. Tätä varten tietosuojalain 70–73 §:ssä on seuraamuksia koskevia säännöksiä, joiden nojalla voidaan määrätä joko sakkoja (20–100 miljoonaa wonia) tai vankeusrangaistus (enimmäisrangaistuksen kesto on 2–10 vuotta). Asianomaisia rikoksia ovat muun muassa henkilötietojen käyttö tai niiden luovuttaminen kolmannelle osapuolelle ilman tarvittavaa suostumusta, arkaluonteisten tietojen käsittely tietosuojalain 23 §:n 1 momentissa säädetyn kiellon vastaisesti, sovellettavien turvallisuusvaatimusten laiminlyönti, jonka seurauksena on henkilötietojen katoaminen, varastaminen, paljastaminen, väärentäminen, muuttaminen tai vahingoittuminen, sekä henkilötietojen oikaisemiseksi tai poistamiseksi tai niiden käsittelyn keskeyttämiseksi tarvittavien toimenpiteiden toteuttamatta jättäminen tai henkilötietojen laiton siirtäminen kolmanteen maahan ([155]). Tietosuojalain 74 §:n mukaisesti vastuu kuuluu kaikissa mainituissa tapauksissa sekä rekisterinpitäjän työntekijälle ja sen puolesta toimivalle toiminnanharjoittajalle tai sen edustajalle että rekisterinpitäjälle itselleen ([156]).

(127) Sen lisäksi, että tietosuojalaissa säädetään rikosoikeudellisista seuraamuksista, henkilötietojen väärinkäyttö voi olla rikos myös rikoslain nojalla. Näin on erityisesti silloin kun kyseessä on kirjeiden, asiakirjojen tai sähköisten rekisterien salassapitovelvollisuuden rikkominen (316 §), ammattisalaisuuden piiriin kuuluvien tietojen paljastaminen (317 §), tietokoneen avulla tehty petos (347-2 §) sekä kavallus ja luottamusaseman väärinkäyttö (355 §).

(128) Korean järjestelmässä yhdistetään näin ollen erilaisia seuraamuksia korjaavista toimenpiteistä ja hallinnollisista sakoista rikosoikeudellisiin seuraamuksiin, joilla on todennäköisesti erityisen vahva pelotevaikutus rekisterinpitäjiin ja tietojen käsittelijöihin. Tietosuojalautakunta alkoi käyttää valtuuksiaan heti sen jälkeen kun se perustettiin

([152]) Jos rekisterinpitäjän käyttämät henkilötietojen käsittelyä ja suojaamista koskevat järjestelmät on todettu tietosuojalain vaatimusten mukaisiksi, mutta tietosuojalain täytäntöönpanoasetuksen 34-2 §:n 1 momentin mukaiset sertifiointikriteerit eivät ole täyttyneet, tai jos jotakin ”[henkilö]tietojen suojaa koskevaa säännöstä” on vakavasti rikottu, tietosuojalautakunta voi lisäksi perua sertifioinnin (tietosuojalain 32-2 §:n 3 ja 5 momentti). Tietosuojalautakunnan on ilmoitettava peruuttamisesta asianomaiselle rekisterinpitäjälle ja tiedotettava siitä myös julkisesti joko verkkosivustollaan tai virallisessa lehdessä (tietosuojalain täytäntöönpanoasetuksen 34-4 §). Luottotietolain rikkomisen perusteella voidaan määrätä myös hallinnollisia sakkoja (luottotietolain 52 §) ja rikosoikeudellisia seuraamuksia (50 §).

([153]) Tietosuojalain täytäntöönpanoasetuksen 58 §:n 2 momentin mukaan rekisterinpitäjän on esitettävä tietosuojalautakunnalle perustelut, jos ohjeen noudattaminen on asiaan liittyvien olosuhteiden vuoksi ”mahdotonta”.

([154]) Kun tietosuojalautakunta päättää tällaisten tietojen julkaisemisesta, sen on otettava huomioon rikkomisen sisältö ja vakavuus, sen kesto ja mahdollinen toistuvuus sekä siitä aiheutuvat seuraukset (vahinkojen laajuus). Asianomaiselle yksilölle on ilmoitettava julkaisemisesta etukäteen ja sille on annettava mahdollisuus puolustautua. Ks. tietosuojalain täytäntöönpanoasetuksen 61 §:n 2 ja 3 momentti.

([155]) Ks. tietosuojalain 71 §:n 2 kohta yhdessä 18 §:n 1 momentin kanssa (tietosuojalain 18 §:n 1 momentissa tarkoitettujen, 17 §:n 3 momentissa säädettyjen ehtojen noudattamatta jättäminen). Ks. myös tietosuojalain 75 §:n 2 momentin 1 kohta yhdessä 17 §:n 2 momentin kanssa (tietosuojalain 17 §:n 2 momentissa säädetyn ja sen 3 momentissa tarkoitetun, tarvittavien tietojen ilmoittamista asianomaiselle henkilölle koskevan velvollisuuden laiminlyönti).

([156]) Tietosuojalain 74-2 §:ssä säädetään lisäksi sellaisten varojen, tavaroiden tai muiden voittojen menetetyksi tuomitsemisesta, jotka on saatu tietosuojavaatimusten loukkauksen seurauksena, tai jos menetetyksi tuomitseminen on mahdotonta, laittomasti saadun hyödyn ”takaisin perimisestä”.

vuonna 2020. Tietosuojalautakunnan vuosiraportti 2021 osoittaa, että lautakunta on antanut useita suosituksia, hallinnollisia sakkoja ja korjaavia määräyksiä sekä julkisella sektorilla (34 viranomaiselle) että yksityisille toimijoille (noin 140 yritykselle) ([157]). Merkittävistä tapauksista voidaan mainita esimerkiksi joulukuussa 2020 eräälle yritykselle määrätty 6,7 miljoonan wonin sakko tietosuojalain eri säännösten rikkomisen vuoksi (mm. turvallisuutta, kolmannelle osapuolelle luovuttamista koskevaa suostumusta ja läpinäkyvyyttä koskevat vaatimukset) ([158]). Huhtikuussa 2021 taas muuan tekoälyteknologiayritys sai 103,3 miljoonan wonin sakot (muun muassa käsittelyn lainmukaisuutta, erityisesti suostumusta, ja pseudonymisoitujen tietojen käsittelyä koskevien vaatimusten rikkomisen vuoksi) ([159]). Elokuussa 2021 tietosuojalautakunta saattoi päätökseen kolmen yrityksen toimintaa koskevan tutkimuksen, jonka seurauksena määrättiin korjaavia toimenpiteitä ja jopa 6,47 miljardin wonin sakot (muun muassa siitä syystä, että rekisteröidyille ei ollut ilmoitettu henkilötietojen luovuttamisesta kolmansille osapuolille ja niiden siirtämisestä kolmansiin maihin) ([160]). Etelä-Korealla oli jo ennen äskettäin toteutettua uudistusta vahvaa näyttöä täytäntöönpanon valvonnasta, sillä vastuuviranomaiset ovat hyödyntäneet kattavasti eri toimenpiteitä muun muassa määräämällä hallinnollisia sakkoja ja korjaavia toimenpiteitä tai nimeämällä julkisesti rikkomuksiin syyllistyneitä rekisterinpitäjiä, kuten viestintäpalvelujen tarjoajia (*Korea Communications Commission*), tai kaupallisia operaattoreita, rahoituslaitoksia, viranomaisia, yliopistoja ja sairaaloita (sisäasiain- ja turvallisuusministeriö) ([161]). Tämän perusteella komissio katsoo, että Korean järjestelmä varmistaa tietosuojasääntöjen tuloksellisen täytäntöönpanon käytännössä ja takaa siten tietosuojan tason, joka olennaisilta osin vastaa asetuksessa (EU) 2016/679 säädettyä tasoa.

2.5 **Oikeussuojakeinot**

(129) Jotta voidaan varmistaa yksilön oikeuksien asianmukainen suojelu ja täytäntöönpano, rekisteröidyllä olisi oltava tehokkaat hallinnolliset ja oikeudelliset oikeussuojakeinot ja myös oikeus saada vahingonkorvausta.

(130) Korean järjestelmä tarjoaa yksilöille erilaisia mekanismeja, joiden avulla he voivat tehokkaasti valvoa oikeuksiaan ja käyttää (oikeudellisia) muutoksenhakukeinoja.

(131) Jos yksilöt katsovat, että heidän tietosuojaoikeuksiaan tai -etujaan on loukattu, he voivat kääntyä ensin asianomaisen rekisterinpitäjän puoleen. Tietosuojalain 30 §:n 1 momentin 5 kohdan mukaan rekisterinpitäjän tietosuojaselosteessa on kerrottava muun muassa rekisteröidylle kuuluvista oikeuksista ja siitä, miten niitä voi käyttää. Lisäksi siinä on oltava yhteystiedot valitusten tekemistä varten, kuten tietosuojavastaavan tai tietosuojasta vastaavan yksikön nimi ja puhelinnumero. Tietosuojavastaava vastaa rekisterinpitäjän organisaatiossa valitusten käsittelystä ja korjaavien toimenpiteiden hyväksymisestä, jos yksityisyyden loukkaus on tapahtunut, sekä vahingonkorvauksista (tietosuojalain 31 §:n 2 momentin 3 kohta ja 4 momentti). Viimeksi mainitulla on merkitystä esimerkiksi tietoturvaloukkauksen tapauksessa, sillä rekisterinpitäjän on ilmoitettava rekisteröidylle yhteystiedot esimerkiksi mahdollisista vahingoista ilmoittamista varten (tietosuojalain 34 §:n 1 momentin 5 kohta).

(132) Tietosuojalaissa säädetään myös eri oikeussuojakeinoista, joita yksilöt voivat käyttää rekisterinpitäjiä vastaan. Ensinnäkin henkilö, joka katsoo, että rekisterinpitäjä on loukannut hänen tietosuojaoikeuksiaan tai -etujaan, voi ilmoittaa siitä suoraan tietosuojalautakunnalle ja/tai jollekin sen nimeämälle erikoistuneelle laitokselle, jonka tehtävänä on ottaa vastaan ja käsitellä valituksia. Yksi tällainen laitos on Korean internet- ja turvallisuusvirasto, joka ylläpitää tätä tarkoitusta varten erityistä yksityisyydensuojaa koskevaa puhelinpalvelua (Privacy Call Centre) (tietosuojalain 62 §:n 1 ja 2 momentti yhdessä sen täytäntöönpanoasetuksen 59 §:n kanssa). Puhelinpalvelu tutkii ja toteaa rikkomuksia, antaa henkilötietojen käsittelyyn liittyvää neuvontaa (tietosuojalain 62 §:n 3 momentti)

([157]) Ks. tietosuojalautakunnan vuosikertomus 2021, ss. 50–55 (saatavilla vain koreaksi), osoitteessa https://www.pipc.go.kr/np/cop/bbs/selectBoardArticle.do?bbsId=BS074&mCode=C020010000&nttId=7511#LINK.

([158]) Ks. (saatavilla vain koreaksi) https://www.pipc.go.kr/np/cop/bbs/selectBoardArticle.do?bbsId=BS074&mCode=C020010000&nttId=6954#LINK.

([159]) Ks. (saatavilla vain koreaksi) https://www.pipc.go.kr/np/cop/bbs/selectBoardArticle.do?bbsId=BS074&mCode=C020010000&nttId=7298&fbclid=IwAR3SKcMQi6G5pR9k4I7j6GNXtc8aBVDOwcURevvvzQtYI7AS40UKYXoOXo8.

([160]) Ks. (saatavilla vain koreaksi): https://www.pipc.go.kr/np/cop/bbs/selectBoardArticle.do?bbsId=BS074&mCode=C020010000&nttId=7497#LINK.

([161]) Ks. esim. vuosikertomus 2020 (saatavilla vain koreaksi) https://www.pipc.go.kr/np/cop/bbs/selectBoardList.do?bbsId=BS079&mCode=D070020000 ja englanninkieliset esimerkit osoitteessa https://www.privacy.go.kr/eng/enforcement_02.do.

ja voi myös ilmoittaa rikkomuksista tietosuojalautakunnalle (mutta se ei voi itse toteuttaa täytäntöönpanotoimia). Puhelinpalvelu vastaanottaa runsaasti valituksia/pyyntöjä (esim. 177 457 vuonna 2020, 159 255 vuonna 2019 ja 164 497 vuonna 2018) ([162]). Tietosuojalautakunnalta saatujen tietojen mukaan lautakunta itse sai elokuun 2020 ja elokuun 2021 välisenä aikana noin 1 000 valitusta. Valituksen saatuaan tietosuojalautakunta voi esittää parannusehdotuksia tai määrätä korjaavia toimenpiteitä tai viedä asian toimivaltaisen tutkintaviraston (ml. syyttäjän) käsiteltäväksi tai antaa neuvoja kurinpitotoimista (tietosuojalain 61, 64 ja 65 §). Tietosuojalautakunnan päätöksiin (esim. kieltäytyminen valituksen käsiteltäväksi ottamisesta tai valituksen asiasisällön hylkääminen) voi hakea muutosta hallinnollisista riita-asioista annetun lain (*Administrative Litigation Act*) nojalla ([163]).

(133) Toiseksi rekisteröidyt voivat tehdä valituksen riitojenratkaisukomitealle (*Dispute Mediation Committee*) (tietosuojalain 40–50 § yhdessä sen täytäntöönpanoasetuksen 48-14–57 §:n kanssa). Komitean jäsenet nimittää tietosuojalautakunnan puheenjohtaja tietosuojalautakunnan johtotason jäsenten sekä tiettyihin ryhmiin kuuluvien tietosuoja-asiantuntijoiden joukosta (tietosuojalain 40 §:n 2, 3 ja 7 momentti ja sen täytäntöönpanoasetuksen 48-14 §) ([164]). Mahdollisuus turvautua sovitteluun riitojenratkaisukomiteassa tarjoaa vaihtoehtoisen oikeussuojakeinon, joka ei rajoita yksilön oikeutta kääntyä sen sijaan tietosuojalautakunnan tai tuomioistuinten puoleen. Riitojenratkaisukomitea voi pyytää riidan osapuolia toimittamaan asian käsittelyä varten tarvittavaa aineistoa ja/tai kutsua todistajia kuultavaksi (tietosuojalain 45 §). Kun asia on selvitetty, komitea laatii sovintoehdotuksen ([165]), jolle on saatava jäsenten enemmistön hyväksyntä. Sovintoehdotuksessa voidaan määrätä rikkomisen lopettamisesta ja tarvittavista korjaavista toimenpiteistä (kuten oikeuksien palauttamisesta tai vahingonkorvauksesta) sekä tarvittavista toimenpiteistä, joiden tarkoituksena on estää saman tai vastaavanlaisen rikkomisen toistuminen (tietosuojalain 47 §:n 1 momentti). Jos riidan osapuolet hyväksyvät sovintoehdotuksen, sillä on sama oikeusvaikutus kuin tuomioistuimessa tehdyllä sovinnolla (tietosuojalain 47 §:n 5 momentti). Kumpikin osapuoli voi viedä asian tuomioistuimen käsiteltäväksi, vaikka sovittelu olisi vielä kesken; siinä tapauksessa sovittelu keskeytetään (tietosuojalain 48 §:n 2 momentti) ([166]). Tietosuojalautakunnan ilmoittamien vuotuisten lukujen perusteella yksilöt käyttävät säännöllisesti riitojenratkaisukomitean menettelyä, joka johtaakin usein onnistuneeseen lopputulokseen. Esimerkiksi vuonna 2020 komitea käsitteli 126 tapausta ja ratkaisi niistä 89 (77 tapauksessa osapuolet pääsivät sopuun jo ennen sovittelumenettelyn päättymistä ja 12 tapauksessa osapuolet hyväksyivät sovitteluehdotuksen), eli sovitteluaste oli 70,6 prosenttia ([167]). Vuonna 2019 komitea käsitteli 139 tapausta ja ratkaisi niistä 92, eli sovitteluaste oli 62,2 prosenttia.

(134) Jos vahingonkärsijöitä on vähintään 50 tai heidän tietosuojaoikeuksiaan on rikottu samalla tai samantapaisella tavalla saman(tyyppisen) tapahtuman seurauksena ([168]), rekisteröity tai tietosuojaorganisaatio voi lisäksi hakea kollektiivista riitojenratkaisua tällaisen yhteisön puolesta; muut rekisteröidyt voivat puolestaan liittyä tällaiseen sovitteluun, josta riitojenratkaisukomitea ilmoittaa julkisesti (tietosuojalain 49 §:n 1–3 momentti yhdessä sen täytäntöönpanoasetuksen 52–54 §:n kanssa) ([169]). Riitojenratkaisukomitea voi valita yhteisön edustajaksi

([162]) Ks. tietosuojalautakunnan vuosikertomus 2021, s. 174. Vuonna 2020 valitukset koskivat muun muassa tietojen keräämistä ilman suostumusta, läpinäkyvyysvelvoitteiden laiminlyöntiä, tietosuojalain rikkomista, johon henkilötietojen käsittelijät olivat syyllistyneet, riittämättömiä turvatoimia, rekisteröityjen pyyntöihin vastaamatta jättämistä sekä yleisiä tiedusteluja.

([163]) Muutosta voidaan hakea erityisesti siihen, miten hallintoviranomainen on käyttänyt julkista valtaa tai kieltäytynyt käyttämästä sitä (hallinnollisista riita-asioista annetun lain 2 §:n 1 momentin 1 kohta ja 3 §:n 1 kohta). Lisätietoja menettelyyn liittyvistä näkökohdista, muun muassa valitusten käsiteltäväksi ottamisen edellytyksistä, on johdanto-osan (181) kappaleessa.

([164]) Kaikkien jäsenten toimikausi on määräaikainen, ja heidät voidaan erottaa tehtävästä vain perustellusta syystä (ks. tietosuojalain 40 §:n 5 momentti ja 41 §). Lisäksi tietosuojalain 42 §:ssä säädetään suojatoimista eturistiriitojen välttämiseksi.

([165]) Ks. tietosuojalain 44 §. Komitea voi myös tehdä ratkaisuehdotuksen ja suosittaa asian ratkaisemista ilman sovittelua (tietosuojalain 46 §).

([166]) Lisäksi komitea voi hylätä sovitteluhakemuksen, jos se katsoo, että riita ei luonteensa vuoksi sovellu soviteltavaksi tai että sovitteluhakemus on tehty vilpillisessä mielessä (tietosuojalain 48 §).

([167]) Ks. tietosuojalautakunnan vuosikertomus 2021, s. 179–180. Tapaukset koskivat muun muassa tietojen keräämistä ilman suostumusta, käyttötarkoituksen rajoittamisen periaatetta ja rekisteröityjen oikeuksia.

([168]) Ks. tietosuojalain 49 §:n 1 momentti, jonka mukaan tässä tapauksessa edellytetään, että rekisteröidyille on aiheutunut vahinkoa tai että heidän oikeuksiaan on loukattu ”identtisellä tai samantapaisella tavalla”, ja tietosuojalain täytäntöönpanoasetuksen 52 §:n 2 kohta, jossa edellytetään, että ”[t]apaukseen liittyvät oikeudelliset tai tosiseikat ovat merkittäviltä osin samat”.

([169]) Jos rekisterinpitäjä hyväksyy kollektiivisen riitojenratkaisun tuloksen, siitä voivat hyötyä myös muut kuin menettelyn osapuolet, sillä riitojenratkaisukomitea voi neuvoa rekisterinpitäjää laatimaan ja esittämään korvaussuunnitelman, joka kattaa (myös) muut kuin menettelyn osapuolet (tietosuojalain 49 §:n 5 momentti).

vähintään yhden henkilön, joka parhaiten edustaa yhteisön yhteistä etua (tietosuojalain 49 §:n 4 momentti). Jos rekisterinpitäjä kieltäytyy kollektiivisesta riitojenratkaisusta tai ei hyväksy sovittelutuomiota, tietyt organisaatiot ([170]) voivat nostaa rikkomisesta ryhmäkanteen (tietosuojalain 51–57 §).

(135) Kolmanneksi, jos rekisteröidylle aiheutuu ”vahinkoa” yksityisyydenloukkauksen seurauksena, hänellä on oikeus asianmukaisiin oikeussuojakeinoihin ”viipymättä ja oikeudenmukaisen menettelyn mukaisesti” (tietosuojalain 4 §:n 5 kohta ja 39 §) ([171]). Rekisterinpitäjä voi vapautua korvausvastuusta osoittamalla, ettei vahinko johtunut sen virheestä (”vilpillisestä aikomuksesta” tai laiminlyönnistä). Jos rekisteröidylle aiheutuu vahinkoa hänen henkilötietojensa katoamisen, varastamisen, paljastamisen, väärentämisen, muuttamisen tai vahingoittumisen vuoksi, tuomioistuin voi määrätä korvauksen, jonka määrä on enintään kolminkertainen tosiasialliseen vahinkoon nähden, ottamalla huomioon useita eri tekijöitä (tietosuojalain 39 §:n 3 ja 4 momentti). Vaihtoehtoisesti rekisteröity voi vaatia ”kohtuullista korvausta”, jonka määrä voi olla enintään 3 miljoonaa wonia (tietosuojalain 39-2 §:n 1 ja 2 momentti). Lisäksi korvausta voidaan vaatia siviililain nojalla ”keneltä tahansa henkilöltä, joka aiheuttaa toiselle henkilölle menetyksiä tai vammoja lainvastaisella teolla, joko tahallisesti tai laiminlyönnin seurauksena” ([172]) tai henkilöltä, ”joka on vahingoittanut toista henkilöä tai hänen vapauttaan tai mainettaan tai aiheuttanut hänelle henkistä ahdistusta” ([173]). Korkein oikeus on vahvistanut tällaisen tietosuojasääntöjen rikkomisesta johtuvan vahingonkorvausvastuun ([174]). Jos vahinko on aiheutunut viranomaisen lainvastaisesta teosta, korvausvaatimus voidaan esittää myös valtion korvauksista annetun lain nojalla ([175]). Kyseisen lain nojalla tehtävä vaatimus käsitellään joko ns. korvausneuvostossa tai suoraan Korean tuomioistuimissa ([176]). Valtion korvausvastuu kattaa myös aineettomat vahingot (kuten henkisen kärsimyksen) ([177]). Jos uhri on ulkomaalainen, valtion korvauksista annettua lakia sovelletaan, jos uhrin lähtömaa korvaa vastaavasti Korean kansalaisille aiheutuneet vahingot ([178]).

(136) Neljänneksi korkein oikeus on tunnustanut, että rekisteröidyillä on oikeus vaatia kieltomääräystä, jos heidän perustuslaillisia oikeuksiaan, kuten oikeutta henkilötietojen suojaan, on loukattu ([179]). Tällaisessa tapauksessa tuomioistuin voi esimerkiksi määrätä rekisterinpitäjät keskeyttämään tai lopettamaan lainvastaisen toiminnan. Lisäksi tietosuojaoikeuksien, myös tietosuojalailla suojattujen oikeuksien, täytäntöönpanoa voidaan vaatia siviilikanteen avulla. Korkein oikeus on tunnustanut tämän yksityisten osapuolten välisiä suhteita koskevan perustuslaillisen yksityisyydensuojan horisontaalisen soveltamisen ([180]).

([170]) Näitä ovat erilaiset kuluttajaryhmät tai tietynkokoiset voittoa tavoittelemattomat kansalaisjärjestöt, joiden jäsenyysehdoissa todetaan niiden toiminnan tarkoitukseksi tietosuoja (viimeksi mainittuihin sovelletaan tosin lisävaatimusta, jonka mukaan ryhmäkanteen nostamista on pyytänyt vähintään 100 rekisteröityä, jotka ovat joutuneet saman(tyyppisen) rikkomisen kohteeksi). Ks. tietosuojalain 51 §.

([171]) Luottotietolain 43–43-3 §:ssä säädetään myös kyseisen lain rikkomiseen perustuvasta korvausvastuusta.

([172]) Siviililain 750 §.

([173]) Siviililain 751 §:n 1 momentti.

([174]) Ks. esim. korkeimman oikeuden päätös 2015Da251539, 251546, 251553, 251560, 251577, 30.5.2018. Korkein oikeus on myös vahvistanut, että tietoturvaloukkausten perusteella voidaan myöntää vahingonkorvaus siviililain nojalla, ks. korkeimman oikeuden päätös 2011Da59834, 59858, 59841, 26.12.2012 (englanninkielinen tiivistelmä saatavilla osoitteessa http://library.scourt.go.kr/SCLIB_data/decision/9-69%202012.12.26.2011Da59834.htm). Kyseisessä tapauksessa korkein oikeus selvensi, että arvioitaessa sitä, voidaanko henkilölle aiheutunut henkinen kärsimys katsoa vahingoksi, josta on saatava korvaus, olisi tarkasteltava useita tekijöitä, kuten vuotaneiden tietojen tyyppi ja ominaispiirteet, henkilön tunnistettavuus tietoturvaloukkauksen seurauksena, kolmansien osapuolten mahdollisuus päästä käsiksi tietoihin, henkilötietojen leviämisen laajuus ja se, aiheutuiko siitä lisää yksilön oikeuksien loukkauksia sekä henkilötietojen hallinnoinnin ja suojauksen laatu.

([175]) Valtion korvauksista annetun lain perusteella yksilöt voivat vaatia korvausta vahingoista, joita virkamies on aiheuttanut suorittaessaan virkatehtäviään lainvastaisesti (lain 2 §:n 1 momentti).

([176]) Valtion korvauksista annetun lain 9 ja 12 §. Lailla perustetaan piirineuvostot (*District Councils*, joiden puheenjohtajana toimii kyseisen alueen syyttäjänviraston apulaissyyttäjä), keskusneuvosto (*Central Council*, jonka puheenjohtajana toimii apulaisoikeusministeri) ja erityisneuvosto (*Special Council*, joka vastaa puolustusvoimien sotilas- tai siviilihenkilöstön aiheuttamien vahinkojen korvaamisesta ja jonka puheenjohtajana toimii apulaispuolustusministeri). Vahingonkorvaushakemukset käsitellään pääsääntöisesti piirineuvostoissa, joiden on tietyissä olosuhteissa toimitettava tapaukset edelleen keskus- tai erityisneuvoston käsiteltäväksi, esimerkiksi jos korvaus ylittää tietyn määrän tai jos hakija pyytää asian uudelleenkäsittelyä. Jäsenet kaikkiin neuvostoihin nimittää oikeusministeri (mm. oikeusministeriön virkamiesten, oikeusvirkamiesten, juristien ja valtion korvauksiin perehtyneiden asiantuntijoiden joukosta) ja heihin sovelletaan erityisiä eturistiriitoja koskevia sääntöjä (ks. valtion korvauksista annetun lain täytäntöönpanoasetuksen 7 §).

([177]) Ks. valtion korvauksista annetun lain 8 § (jossa viitataan siviililakiin) sekä siviililain 751 §.

([178]) Valtion korvauksista annetun lain 7 §.

([179]) Korkeimman oikeuden päätös 93Da40614, 12.4.1996, ja päätös 2008Da42430, 2.9.2011 (englanninkielinen tiivistelmä saatavilla osoitteessa https://www.scourt.go.kr/eng/supreme/decisions/NewDecisionsView.work?seq=696&pageIndex=1&mode=6&searchWord=).

([180]) Ks. esimerkiksi korkeimman oikeuden päätös 2008Da42430, 2.9.2011, (englanninkielinen tiivistelmä saatavilla osoitteessa https://www.scourt.go.kr/eng/supreme/decisions/NewDecisionsView.work?seq=696&pageIndex=1&mode=6&searchWord=).

(137) Lopuksi todettakoon, että yksilöt voivat tehdä rikosilmoituksen yleiselle syyttäjälle tai rikospoliisille rikosprosessilain nojalla (*Criminal Procedure Act*, 223 §) ([181]).

(138) Korean järjestelmä tarjoaa näin ollen erilaisia muutoksenhakukeinoja, joista toiset ovat helposti saatavilla ja kustannuksiltaan kohtuullisia (esimerkiksi yhteydenotto Privacy Call Centre -puhelinpalveluun tai (kollektiivinen) sovittelu) ja toiset tarjoavat hallinnollisia (tietosuojalautakunta) ja oikeudellisia ratkaisuja, joihin kuuluu myös mahdollisuus saada vahingonkorvausta.

3. KOREAN TASAVALLAN VIRANOMAISTEN PÄÄSY EUROOPAN UNIONISTA SIIRRETTYIHIN HENKILÖTIETOIHIN JA NÄIDEN TIETOJEN KÄYTTÖ

(139) Komissio on arvioinut myös niitä rajoituksia ja suojatoimia, mukaan lukien Korean lainsäädännön mukaiset valvonta- ja oikeussuojamekanismit, jotka koskevat sitä, kuinka viranomaiset voivat kerätä ja käyttää korealaisille rekisterinpitäjille siirrettyjä henkilötietoja yleisen edun mukaisia tarkoituksia ja erityisesti lainvalvontatarkoituksia ja kansalliseen turvallisuuteen liittyviä tarkoituksia varten, jäljempänä 'viranomaisten pääsy tietoihin'. Korean hallitus on tältä osin antanut komissiolle virallisia vahvistusilmoituksia, vakuutuksia ja sitoumuksia, jotka on allekirjoitettu korkeimmalla ministeri- ja virastotasolla ja jotka sisältyvät tämän päätöksen liitteeseen II.

(140) Kun komissio arvioi, vastaavatko edellytykset, joiden nojalla viranomaiset käyttävät Koreaan tämän päätöksen nojalla siirrettyjä tietoja, "olennaisilta osin" asetuksen (EU) 2016/679 45 artiklan 1 kohdassa esitettyjä vaatimuksia, sellaisena kuin Euroopan unionin tuomioistuin on niitä tulkinnut perusoikeuskirjan valossa, se ottaa huomioon erityisesti seuraavat kriteerit.

(141) Ensinnäkin kaikista henkilötietojen suojaa koskevan oikeuden rajoituksista on säädettävä lailla, ja näiden rajoitusten laajuus on määritettävä jo siinä oikeusperustassa, joka mahdollistaa puuttumisen näihin oikeuksiin ([182]).

(142) Toiseksi, sen oikeasuhteisuutta koskevan vaatimuksen täyttämiseksi, jonka mukaan henkilötietojen suojaa koskevia poikkeuksia ja rajoituksia on sovellettava vain siltä osin kuin se on ehdottoman välttämätöntä demokraattisessa yhteiskunnassa, jotta voidaan saavuttaa yleisen edun mukaiset tavoitteet, jotka vastaavat unionin tunnustamia tavoitteita, asianomaisen kolmannen maan lainsäädännössä, jossa sallitaan puuttuminen henkilötietojen suojaan, on vahvistettava selkeät ja täsmälliset säännöt, joilla säännellään kyseisten toimenpiteiden soveltamisalaa ja soveltamista ja vahvistetaan vähimmäistakeet, niin että henkilöillä, joiden tietoja on siirretty, on riittävät takeet, joiden nojalla heidän henkilötietojaan suojataan tehokkaasti väärinkäytön riskiltä ([183]). Tällaisessa lainsäädännössä on erityisesti ilmoitettava, missä olosuhteissa ja millä edellytyksillä tällaisten henkilötietojen käsittelyä koskeva toimenpide voidaan toteuttaa ([184]), ja säädettävä, että tällaisten vaatimusten täyttämiseen on sovellettava riippumatonta valvontaa ([185]).

(143) Kolmanneksi kyseisen lainsäädännön ja sen vaatimusten on oltava oikeudellisesti velvoittavia kansallisen lain nojalla. Tämä koskee ensinnäkin kyseisen kolmannen maan viranomaisia, mutta näiden oikeudellisten vaatimusten on myös oltava täytäntöönpanokelpoisia tuomioistuimessa kyseisiä viranomaisia vastaan ([186]). Rekisteröidyillä on erityisesti oltava mahdollisuus nostaa kanne riippumattomassa ja puolueettomassa tuomioistuimessa, jotta he voivat saada pääsyn henkilötietoihinsa tai saada ne oikaistuiksi tai poistetuiksi ([187]).

3.1 Yleinen oikeudellinen kehys

(144) Korean viranomaisten suorittamaan henkilötietojen keräämiseen ja käyttöön sovellettavat rajoitukset ja suojatoimet perustuvat yleisen perustuslaillisen kehyksen ohella erityislakeihin, joilla säännellään viranomaisten toimintaa lainvalvonnan ja kansallisen turvallisuuden alalla, sekä sääntöihin, joita sovelletaan erityisesti henkilötietojen käsittelyyn.

([181]) Kuten johdanto-osan (127) kappaleessa selitetään, tietojen väärinkäyttö voi olla myös rikoslaissa tarkoitettu rikos.
([182]) Ks. Schrems II, 174–175 kohta oikeuskäytäntöviittauksineen. Ks. jäsenvaltioiden viranomaisten pääsyn osalta myös asia C-623/17, Privacy International, ECLI:EU:C:2020:790, 65 kohta; ja yhdistetyt asiat C-511/18, C-512/18 ja C-520/18, La Quadrature du Net ym., ECLI:EU:C:2020:791, 175 kohta.
([183]) Ks. Schrems II, 176 ja 181 kohta oikeuskäytäntöviittauksineen. Ks. jäsenvaltioiden viranomaisten pääsyn osalta myös Privacy International, 68 kohta; ja La Quadrature du Net and Others, 132 kohta.
([184]) Ks. Schrems II, 176 kohta. Ks. jäsenvaltioiden viranomaisten pääsyn osalta myös Privacy International, 68 kohta; ja La Quadrature du Net and Others, 132 kohta.
([185]) Ks. Schrems II, 179 kohta.
([186]) Ks. Schrems II, 181–182 kohta.
([187]) Ks. Schrems I, 95 kohta, ja Schrems II, 194 kohta. Euroopan unionin tuomioistuin on tältä osin erityisesti korostanut, että perusoikeuskirjan 47 artiklan (oikeus tehokkaisiin oikeussuojakeinoihin riippumattomassa ja puolueettomassa tuomioistuimessa) noudattaminen liittyy unionissa vaadittavaan tietosuojan tasoon ja että komission on todettava sen noudattaminen ennen kuin se tekee tietosuojan riittävyyttä koskevan päätöksen asetuksen (EU) 2016/679 45 artiklan 1 kohdan nojalla (Schrems II, 186 kohta).

(145) Ensinnäkin Korean viranomaisten pääsyä henkilötietoihin säännellään Korean perustuslakiin perustuvien yleisten periaatteiden – lainmukaisuuden, tarpeellisuuden ja oikeasuhteisuuden – mukaan ([188]). Näiden periaatteiden mukaan erityisesti perusoikeuksia ja -vapauksia (mukaan lukien oikeus yksityisyyteen ja oikeus kirjesalaisuuteen) ([189]) voidaan rajoittaa ainoastaan lailla silloin kun se on välttämätöntä kansallisen turvallisuuden, lain ja järjestyksen tai yleisen hyvinvoinnin turvaamiseksi. Tällaiset rajoitukset eivät saa vaikuttaa kyseessä olevan vapauden olennaiseen sisältöön. Etsintöjen ja takavarikkojen osalta perustuslaissa säädetään erikseen, että niitä voidaan suorittaa vain laissa säädetyin edellytyksin tuomarin antaman päätöksen perusteella ja asianmukaista menettelyä noudattaen ([190]). Yksilöt voivat myös vedota oikeuksiinsa ja vapauksiinsa perustuslakituomioistuimessa, jos he katsovat, että viranomaiset ovat loukanneet niitä toimivaltaansa käyttäessään ([191]). Vastaavasti yksilöillä, joille on aiheutunut vahinkoa virkamiehen virkatehtäviä suorittaessaan tekemästä lainvastaisesta teosta, on oikeus vaatia asianmukaista korvausta ([192]).

(146) Toiseksi, kuten 3.2.1 ja 3.3.1 kohdassa tarkemmin kuvataan, johdanto-osan (145) kappaleessa mainitut yleiset periaatteet on otettu huomioon myös niissä erityislaeissa, joilla säännellään lainvalvontaviranomaisten ja kansallisten turvallisuusviranomaisten toimivaltuuksia. Esimerkiksi rikosprosessilaissa säädetään, että rikostutkinnassa voidaan käyttää pakkokeinoja vain jos rikosprosessilaissa nimenomaisesti niin säädetään ja vain sen verran kuin on välttämätöntä tutkinnan tarkoituksen saavuttamiseksi ([193]). Vastaavasti viestinnän tietosuojalain 3 §:ssä kielletään pääsy yksityiseen viestintään muutoin kuin lain nojalla ja siinä säädettyjä rajoituksia ja suojatoimia noudattaen. Kansallisen turvallisuuden osalta kansallisesta tiedustelupalvelusta annetussa laissa (*National Intelligence Service Act*) säädetään, että pääsy viestintään tai paikkatietoihin on toteutettava lain mukaisesti ja että toimivallan väärinkäytöstä ja lain rikkomisesta voidaan määrätä rikosoikeudellinen seuraamus ([194]).

(147) Kolmanneksi viranomaisten suorittamaan henkilötietojen käsittelyyn sovelletaan tietosuojalaissa vahvistettuja tietosuojasääntöjä, myös silloin kun käsittely tapahtuu lainvalvontaan ja kansalliseen turvallisuuteen liittyviä tarkoituksia varten ([195]). Tietosuojalain 5 §:n 1 momentissa säädetään yleisenä periaatteena, että viranomaisten on laadittava politiikkatoimenpiteitä, joiden avulla voidaan estää ”henkilötietojen väärinkäyttö, epäasianmukainen tarkkailu ja seuraaminen jne. sekä taata ihmisarvo ja oikeus yksityisyyteen”. Lisäksi rekisterinpitäjien on käsiteltävä henkilötietoja niin, että minimoidaan mahdollisuus loukata rekisteröidyn yksityisyyttä (tietosuojalain 3 §:n 6 momentti).

(148) Lainvalvontatarkoituksessa tapahtuvaan henkilötietojen käsittelyyn sovelletaan kaikkia 2 kohdassa yksityiskohtaisesti kuvattuja tietosuojalain vaatimuksia. Tämä tarkoittaa niin keskeisiä periaatteita (kuten käsittelyn lainmukaisuus ja asianmukaisuus, käyttötarkoituksen rajoittaminen, kerättävien tietojen minimointi ja tietojen täsmällisyys, säilyttämisen rajoittaminen sekä käsittelyn turvallisuus ja läpinäkyvyys), kuin velvollisuuksia (esimerkiksi tietoturvaloukkauksista ilmoittaminen, arkaluonteiset tiedot) ja oikeuksia (pääsyoikeus ja oikeus oikaista ja poistaa tiedot ja keskeyttää niiden käsittely).

(149) Henkilötietojen käsittelyä kansalliseen turvallisuuteen liittyviä tarkoituksia varten ei säännellä tietosuojalaissa yhtä laajasti, mutta myös siihen sovelletaan keskeisiä periaatteita sekä valvontaa, noudattamisen valvontaa ja oikeussuojakeinoja koskevia sääntöjä ([196]). Tietosuojalain 3 ja 4 §:ssä vahvistetaan erityisesti yleiset tietosuojaperiaatteet (lainmukaisuus ja asianmukaisuus, käsittelytarkoituksen rajoittaminen, kerättävien tietojen minimointi, tietojen täsmällisyys ja käsittelyn turvallisuus ja läpinäkyvyys) ja yksilön oikeudet (tiedonsaantioikeus, pääsyoikeus omiin tietoihin ja oikeus oikaista tai poistaa ne sekä keskeyttää niiden käsittely) ([197]). Tietosuojalain 4 §:n 5 momentissa myönnetään lisäksi yksilöille oikeus asianmukaisiin oikeussuojakeinoihin viipymättä ja oikeudenmukaisen menettelyn mukaisesti. Tätä täydennetään yksityiskohtaisemmilla velvoitteilla, joiden mukaan henkilötietoja saa

([188]) Ks. liitteen II kohta 1.1.
([189]) Perustuslain 37 §:n 2 momentti.
([190]) Perustuslain 16 § ja 12 §:n 3 momentti. Perustuslain 12 §:n 3 momentissa säädetään lisäksi poikkeuksellisista olosuhteista, joissa etsintöjä tai takavarikkoja voidaan suorittaa ilman tuomioistuimen päätöstä (joskin päätös vaaditaan jälkikäteen), esimerkiksi silloin kun rikosepäilty saadaan kiinni verekseltään (*flagrante delicto*) tai silloin kun rikoksesta voidaan määrätä vähintään kolmen vuoden vankeusrangaistus ja on olemassa riski, että todisteita hävitetään tai että epäilty pakenee.
([191]) Perustuslakituomioistuimesta annetun lain 68 §:n 1 momentti.
([192]) Perustuslain 29 §:n 1 momentti.
([193]) Rikosprosessilain 199 §:n 1 momentti. Yleensäkin viranomaisten on rikosprosessilakiin perustuvia valtuuksiaan käyttäessään kunnioitettava epäillyn ja kaikkien muiden asianosaisten perusoikeuksia (rikosprosessilain 198 §:n 2 momentti).
([194]) Kansallisesta tiedustelupalvelusta annetun lain 14 §.
([195]) Ks. liitteen II kohta 1.2.
([196]) Tietosuojalain 58 §:n 1 momentin 2 kohta. Ks. myös ilmoituksessa N:o 2021-5 oleva 6 kohta (liite I). Tätä tietosuojalain eräitä säännöksiä koskevaa poikkeusta sovelletaan vain silloin kun henkilötietoja käsitellään ”kansalliseen turvallisuuteen liittyviä tarkoituksia varten”. Kun tietojenkäsittelyn perusteena oleva kansalliseen turvallisuuteen liittyvä tilanne on päättynyt, poikkeusta ei voida enää soveltaa, vaan sovelletaan kaikkia tietosuojalain vaatimuksia.
([197]) Näitä oikeuksia voidaan rajoittaa vain lain nojalla siltä osin ja niin pitkäksi aikaa kuin se on tarpeen ja oikeasuhteista yleisen edun mukaisen tärkeän tavoitteen suojelemiseksi, tai kun oikeuden myöntäminen voisi vahingoittaa kolmannen osapuolen henkeä tai terveyttä tai loukata oikeudettomasti kolmannen osapuolen omaisuutta ja muita etuja. Ks. ilmoituksessa N:o 2021-5 oleva 6 kohta.

käsitellä vain sen verran kuin on välttämätöntä tarkoituksen saavuttamiseksi ja mahdollisimman lyhyen aikaa, minkä lisäksi on toteutettava tarvittavat toimenpiteet turvallisen tiedonhallinnan ja asianmukaisen käsittelyn varmistamiseksi (kuten tekniset, hallinnolliset ja fyysiset suojatoimet) sekä toimenpiteet yksilöiden valitusten asianmukaista käsittelyä varten ([198]). Lisäksi Korean perustuslaissa vahvistettuja lainmukaisuuden, tarpeellisuuden ja oikeasuhteisuuden periaatteita (ks. johdanto-osan (145) kappale) sovelletaan myös silloin kun henkilötietoja käsitellään kansalliseen turvallisuuteen liittyviä tarkoituksia varten.

(150) Yksilöt voivat oikeussuojakeinojen käyttämiseksi vedota näihin yleisiin periaatteisiin ja suojatoimiin riippumattomissa valvontaelimissä (esim. tietosuojalautakunta ja/tai kansallinen ihmisoikeuskomissio, ks. johdanto-osan (177)–(178) kappale) ja tuomioistuimissa (ks. johdanto-osan (179)–(183) kappale).

3.2 **Korean viranomaisten pääsy tietoihin ja niiden käyttö lainvalvontatarkoituksia varten**

(151) Korean tasavallan lainsäädännössä asetetaan useita rajoituksia, jotka koskevat henkilötietoihin pääsyä ja niiden käyttöä lainvalvontatarkoituksia varten sekä tähän liittyviä valvonta- ja oikeussuojamekanismeja. Nämä säännökset vastaavat vaatimuksia, joihin viitataan tämän päätöksen johdanto-osan (141)–(143) kappaleessa. Seuraavassa arvioidaan yksityiskohtaisesti edellytyksiä, joiden täyttyessä pääsy henkilötietoihin voi toteutua, ja näiden toimivaltuuksien käyttöön sovellettavia suojatoimia.

3.2.1 *Oikeusperustat, rajoitukset ja suojatoimet*

(152) Korean viranomaiset voivat kerätä tämän päätöksen nojalla unionista siirrettäviä ja korealaisten rekisterinpitäjien käsittelemiä henkilötietoja ([199]) lainvalvontatarkoituksia varten etsinnän tai takavarikon yhteydessä (rikosprosessilain nojalla), hankkimalla viestintätietoja (viestinnän tietosuojalain nojalla) tai hankkimalla tilaajatietoja vapaaehtoista luovuttamista koskevien pyyntöjen avulla (televiestintäyrityksiä koskevan lain nojalla) ([200]).

3.2.1.1 Etsinnät ja takavarikot

(153) Rikosprosessilain mukaan etsintä tai takavarikko voidaan toteuttaa vain jos henkilöä epäillään rikoksesta ja toimenpiteet ovat tarpeen tutkintaa varten ja tutkinnan ja etsinnän kohteena olevan henkilön tai tarkastettavan tai takavarikoitavan esineen välillä on todettu yhteys ([201]). Lisäksi etsintä tai takavarikko (kuten muutkin pakkokeinot) voidaan hyväksyä/toteuttaa vain siinä määrin kuin se on välttämätöntä ([202]). Jos etsinnän kohteena on tietokoneen kovalevy tai muu tallennusväline, periaatteessa takavarikko voi koskea ainoastaan tarvittavia tietoja (jotka kopioidaan tai tulostetaan) eikä koko tallennusvälinettä ([203]). Tallennusväline voidaan takavarikoida vain jos katsotaan, että tarvittavien tietojen tulostaminen tai kopioiminen erikseen olisi käytännössä mahdotonta tai että etsinnän tarkoituksen toteuttaminen muulla tavoin olisi käytännössä mahdotonta ([204]). Siksi rikosprosessilaissa on näiden toimenpiteiden soveltamisalaa ja soveltamista koskevat selkeät ja täsmälliset säännöt, joilla voidaan varmistaa, että yksilön oikeuksiin puuttuminen etsinnän ja takavarikon yhteydessä rajoittuu siihen, mikä on välttämätöntä tietyn rikostutkinnan kannalta ja oikeasuhteista sen tavoitteisiin nähden.

([198]) Tietosuojalain 58 §:n 4 momentti.

([199]) Ks. liitteen II kohta 2.1. Korean hallituksen virallinen edustusto (liitteen II kohta 2.1) viittaa myös mahdollisuuteen kerätä rahoitustoimia koskevia tietoja rahanpesun ja terrorismin rahoituksen ehkäisemiseksi tiettyjen rahoitustoimien raportoinnista ja käytöstä annetun lain (*Act on Reporting and Using Specified Financial Transaction Information*), jäljempänä 'rahoitustoimia koskevasta raportoinnista annettu laki', nojalla. Rahoitustoimia koskevasta raportoinnista annetun lain mukaan tietojen luovuttamisvelvollisuus koskee kuitenkin ainoastaan niitä rekisterinpitäjiä, jotka käsittelevät henkilötietoja tietosuojalain nojalla ja rahoituspalvelukomission valvonnassa (ks. johdanto-osan (13) kappale). Koska tällaisten rekisterinpitäjien suorittama henkilökohtaisten luottotietojen käsittely ei kuulu tämän päätöksen soveltamisalaan, rahoitustoimien raportoinnista annetulla lailla ei ole merkitystä tämän arvioinnin kannalta.

([200]) Viestinnän tietosuojalain 3 §:ssä mainitaan myös sotilastuomioistuinlaki (*Military Court Act*) mahdollisena oikeusperustana viestintätietojen keräämiselle. Kyseisellä lailla kuitenkin säännellään sotilashenkilöstöä koskevien tietojen keräämistä, ja sitä voidaan soveltaa siviilihenkilöihin vain rajoitetuissa tapauksissa (esim. jos sotilas- ja siviilihenkilöt tekevät rikoksen yhdessä, tai jos henkilö tekee rikoksen puolustusvoimia vastaan, menettely voidaan panna vireille sotilastuomioistuimessa, ks. kyseisen lain 2 §). Joka tapauksessa laissa vahvistetut etsintää ja takavarikkoa koskevat yleiset säännökset ovat samantapaiset kuin rikosprosessilaissa (ks. esim. sotilastuomioistuinlain 146–149 § ja 153–156 §). Niissä säädetään muun muassa, että postilähetyksiä voidaan kerätä vain jos se on tarpeen tutkintaa varten ja sotilastuomioistuimen päätöksen nojalla. Siltä osin kuin sähköistä viestintää kerätään kyseisen lain nojalla, sovelletaan viestinnän tietosuojalaissa säädettyjä rajoituksia ja suojatoimia. Ks. liitteen II kohta 2.2.2.2 ja alaviite 50.

([201]) Rikosprosessilain 215 §:n 1 ja 2 momentti. Ks. myös rikosprosessilain 106 §:n 1 momentti sekä 107 ja 109 §, joiden mukaan tuomioistuimet voivat toteuttaa etsintöjä ja takavarikkoja, jos asianomaisten esineiden tai henkilöiden katsotaan liittyvän tiettyyn tapaukseen. Ks. liitteen II kohta 2.2.1.2.

([202]) Rikosprosessilain 199 §:n 1 momentti.

([203]) Rikosprosessilain 106 §:n 3 momentti.

([204]) Rikosprosessilain 106 §:n 3 momentti.

(154) Menettelyllisten suojatoimien osalta rikosprosessilaissa edellytetään, että tuomioistuin antaa päätöksen etsintää tai takavarikkoa varten ([205]). Etsintä tai takavarikko ilman tuomioistuimen päätöstä on sallittu vain poikkeuksellisesti, eli kiireellisissä tapauksissa ([206]), kun rikoksesta epäilty pidätetään tai otetaan kiinni rikospaikalla ([207]), tai kun rikoksesta epäilty tai kolmas henkilö heittää pois tai luovuttaa vapaaehtoisesti jonkin esineen (henkilötietojen osalta tämä tarkoittaa, että asianomainen luovuttaa tiedot itse) ([208]). Laittomasta etsinnästä ja takavarikosta voidaan määrätä rikosoikeudellisia seuraamuksia ([209]), ja rikosprosessilain vastaisesti hankittu näyttö hylätään ([210]). Asianomaisille henkilöille on myös aina ilmoitettava etsinnästä tai takavarikosta (myös heidän tietojensa takavarikoinnista) viipymättä. ([211]) Tämä helpottaa yksilön aineellisten oikeuksien ja oikeussuojakeinojen käyttöä (ks. erityisesti mahdollisuus riitauttaa takavarikointipäätöksen täytäntöönpano, ks. johdanto-osan (180) kappale).

3.2.1.2 Pääsy viestintätietoihin

(155) Viestinnän tietosuojalain nojalla Korean lainvalvontaviranomaiset voivat toteuttaa kahdenlaisia toimenpiteitä ([212]): ne voivat ensinnäkin kerätä televalvontatietoja (*communication confirmation data*) ([213]), joista käy ilmi televiestinnän päivämäärä, alkamis- ja päättymisaika, lähtevien ja saapuvien puhelujen määrä sekä toisen osapuolen tilaajanumero, käyttötiheys, televiestintäpalvelujen käyttöä koskevat lokitiedostot ja paikkatiedot (esimerkiksi tukiasema, josta signaalit on vastaanotettu); ja toiseksi toteuttaa ”yhteydenpidon rajoittamista koskevia toimenpiteitä” (*communication-restricting measures*), jotka kattavat sekä perinteisten postilähetysten että televiestinnän sisällön haltuunoton ([214]).

(156) Televalvontatietoihin voidaan myöntää pääsy vain jos se on tarpeen rikostutkinnan suorittamiseksi tai rangaistuksen täytäntöönpanemiseksi ([215]) tuomioistuimen antaman päätöksen perusteella ([216]). Viestinnän tietosuojalaissa edellytetään tältä osin yksityiskohtaisten tietojen antamista sekä päätöstä koskevassa hakemuksessa (esim. pyynnön perustelut ja sen suhde kohteeseen/tilaajaan ja tarvittavat tiedot) että itse päätöksessä (esim. toimenpiteen tavoite, kohde ja soveltamisala) ([217]). Tietojen kerääminen ilman tuomioistuimen päätöstä on mahdollista vain

([205]) Rikosprosessilain 215 §:n 1 ja 2 momentti sekä 113 §. Kun viranomainen hakee tällaista tuomioistuimen päätöstä, sen on esitettävä todisteet, jotka osoittavat, miksi kyseistä henkilöä epäillään rikoksesta ja miksi etsintä, tarkastus tai takavarikko on tarpeen ja että takavarikoitavaksi ehdotetut esineet ovat olemassa (rikosprosessista annetun asetuksen 108 §:n 1 momentti). Päätöksessä on täsmennettävä muun muassa rikoksesta epäillyn nimi ja rikos, josta häntä epäillään; paikka, henkilö tai etsityt tai takavarikoitavat esineet; päätöksen antamispäivä; ja soveltamisaika (rikosprosessilain 114 §:n 1 momentti yhdessä 219 §:n kanssa). Ks. liitteen II kohta 2.2.1.2.

([206]) Eli silloin kun tuomioistuimen päätöksen saaminen on mahdotonta rikospaikalla kiireen vuoksi (rikosprosessilain 216 §:n 3 momentti), missä tapauksessa päätös on kuitenkin hankittava viipymättä jälkikäteen (rikosprosessilain 216 §:n 3 momentti).

([207]) Rikosprosessilain 216 §:n 1 ja 2 momentti.

([208]) Rikosprosessilain 218 §. Lisäksi, kuten liitteen II kohdassa 2.2.1.2 selitetään, vapaaehtoisesti luovutetut esineet hyväksytään todisteiksi oikeudenkäynnissä vain jos ei ole perusteltua epäilystä luovutuksen vapaaehtoisuudesta, mikä syyttäjän on osoitettava.

([209]) Rikoslain 321 §.

([210]) Rikosprosessilain 308-2 §. Lisäksi asianomainen henkilö (ja hänen avustajansa) voi olla läsnä, kun etsintä- tai takavarikkopäätös pannaan täytäntöön, ja hän voi myös vastustaa sitä päätöksen täytäntöönpanohetkellä (rikosprosessilain 121 ja 219 §).

([211]) Rikosprosessilain 121 ja 122 § (etsinnän osalta), ja 219 § yhdessä 106 §:n 4 momentin kanssa (takavarikon osalta).

([212]) Ks. liitteen II kohta 2.2.2.1. Televiestintäpalvelujen tarjoajilla on velvollisuus avustaa näiden toimenpiteiden toteuttamisessa, kun niille esitetään tuomioistuimen antama lupa toimenpiteiden toteuttamiseen (viestinnän tietosuojalain 9 §:n 2 momentti), ja niiden on säilytettävä lupa (viestinnän tietosuojalain 15-2 § ja sen täytäntöönpanoasetuksen 12 §). Televiestintäpalvelujen tarjoajat voivat kieltäytyä yhteistyöstä, jos tuomioistuimen kirjallisessa luvassa esitetyt kohdehenkilön tiedot (esimerkiksi puhelinnumero) ovat virheellisiä. Ne eivät missään tapauksessa saa paljastaa televiestinnässä käytettäviä salasanoja (viestinnän tietosuojalain 9 §:n 4 momentti).

([213]) Viestinnän tietosuojalain 2 §:n 11 momentti.

([214]) Ks. viestinnän tietosuojalain 2 §:n 6 momentti, jossa viitataan ”sensuuriin” (postin avaaminen ilman asianomaisen osapuolen lupaa tai sen sisällön hankkiminen, tallentaminen tai pidättäminen muilla keinoin) ja 2 §:n 7 momentti, jossa viitataan ”kuunteluun” (televiestinnän sisällön hankkiminen tai tallentaminen kuuntelemalla tai lukemalla yhteisesti viestintään sisältyviä ääniä, sanoja, symboleita tai kuvia elektronisin ja mekaanisin laittein ilman asianomaisen suostumusta tai puuttumalla viestinnän lähettämiseen ja vastaanottamiseen).

([215]) Viestinnän tietosuojalain 13 §:n 1 momentti. Ks. myös liitteen II kohta 2.2.2.3. Lisäksi reaaliaikaisia paikannustietoja ja televalvontatietoja, jotka liittyvät tiettyyn tukiasemaan, saa kerätä vain vakavien rikosten tutkintaa varten tai jos muutoin olisi vaikeaa estää rikoksen toteuttamista tai kerätä todisteita (viestinnän tietosuojalain 13 §:n 2 momentti). Tämä liittyy siihen, että silloin kun toimenpiteillä puututaan yksityisyyteen erityisen merkittävästi, on sovellettava täydentäviä suojatoimia oikeasuhteisuuden periaatteen mukaisesti.

([216]) Viestinnän tietosuojalain 13 ja 6 §.

([217]) Ks. viestinnän tietosuojalain 13 §:n 3 ja 9 momentti yhdessä 6 §:n 4 ja 6 momentin kanssa.

jos tuomioistuimen lupaa ei voida hankkia asian kiireellisyyden vuoksi. Tällöin päätös on hankittava ja toimitettava televiestintäpalvelujen tarjoajalle välittömästi tietojen pyytämisen jälkeen ([218]). Jos tuomioistuin kieltäytyy antamasta lupaa jälkikäteen, kerätyt tiedot on tuhottava ([219]).

(157) Televalvontatietojen keräämisessä sovellettavia täydentäviä suojatoimia ovat viestinnän tietosuojalaissa säädetyt erityiset kirjanpitoa ja läpinäkyvyyttä koskevat vaatimukset ([220]). Etenkin lainvalvontaviranomaisten ([221]) ja televiestintäpalvelujen tarjoajien ([222]) on pidettävä kirjaa esitetyistä pyynnöistä ja niiden perusteella luovutetuista tiedoista. Lisäksi lainvalvontaviranomaisten on periaatteessa ilmoitettava yksilöille siitä, että heiltä on kerätty televalvontatietoja ([223]). Tällaista ilmoittamista voidaan lykätä ainoastaan poikkeustapauksissa toimivaltaisen piirisyyttäjänviraston johtajan luvalla ([224]). Lykkäys voidaan myöntää vain, jos ilmoittaminen todennäköisesti 1) vaarantaisi kansallisen turvallisuuden tai yleisen turvallisuuden ja järjestyksen, 2) aiheuttaisi kuoleman tai ruumiinvamman, 3) estäisi oikeudenmukaisen oikeudenkäynnin toteutumisen (esimerkiksi siksi, että se johtaisi todisteiden hävittämiseen tai todistajien uhkailuun), tai 4) loukkaisi epäillyn, uhrien tai muiden tapaukseen liittyvien henkilöiden kunniaa tai heidän yksityisyyttään. Näissä tapauksissa ilmoitus on annettava 30 päivän kuluessa siitä kun lykkäyksen syyt ovat lakanneet olemasta ([225]). Ilmoituksen jälkeen yksilöillä oikeus saada tietoa siitä, miksi heidän tietojaan on kerätty ([226]).

(158) Yhteydenpidon rajoittamiseen sovelletaan tiukempia sääntöjä, joiden mukaan tällaisia toimenpiteitä voidaan käyttää vain jos on olemassa merkittävä syy epäillä, että suunnitteilla on tiettyjä viestinnän tietosuojalaissa erikseen lueteltuja vakavia rikoksia tai että sellaisia rikoksia on tehty ([227]). Lisäksi yhteydenpitoa voidaan rajoittaa vain viimesijaisena keinona, jos rikoksen estäminen, rikollisen pidättäminen tai todisteiden kerääminen olisi muutoin vaikeaa ([228]). Toimenpiteet on lopetettava heti kun niitä ei enää tarvita, jotta voidaan varmistaa, että viestinnän yksityisyyttä rajoitetaan mahdollisimman vähän. ([229]) Tietoja, jotka on saatu laittomasti yhteydenpidon rajoittamista koskevien toimenpiteiden avulla, ei hyväksytä todisteeksi oikeudenkäynnissä tai kurinpitomenettelyssä ([230]).

(159) Menettelyllisten suojatoimien osalta viestinnän tietosuojalaissa edellytetään, että tuomioistuin antaa päätöksen yhteydenpidon rajoittamista koskevien toimenpiteiden toteuttamisesta ([231]). Viestinnän tietosuojalaissa myös edellytetään, että päätöstä koskevassa hakemuksessa ja itse päätöksessä on yksityiskohtaiset tiedot ([232]), muun muassa pyynnön perustelut sekä se, mitä viestintätietoja on tarkoitus kerätä (niiden on kuuluttava tutkinnan kohteena olevalle epäillylle) ([233]). Tällaisia toimenpiteitä voidaan toteuttaa ilman tuomioistuimen päätöstä vain jos on kyseessä järjestäytyneen rikollisuuden aiheuttama välitön vaara tai jos on tapahtumassa muu vakava rikos,

([218]) Viestinnän tietosuojalain 13 §:n 2 momentti.
([219]) Viestinnän tietosuojalain 13 §:n 3 momentti.
([220]) Ks. liitteen II kohta 2.2.2.3 kohta.
([221]) Viestinnän tietosuojalain 13 §:n 5 ja 6 momentti.
([222]) Viestinnän tietosuojalain 13 §:n 7 momentti. Lisäksi televiestintäpalvelujen tarjoajien on kahdesti vuodessa raportoitava televalvontatietojen luovuttamisesta tiede- ja tieto- ja viestintätekniikkaministeriölle.
([223]) Ks. viestinnän tietosuojalain 13-3 §:n 7 momentti yhdessä 9-2 §:n kanssa. Yksilöille on ilmoitettava 30 päivän kuluessa erityisesti silloin, kun on tehty syyttämis- tai syyttämättäjättämispäätös, tai 30 päivän kuluessa siitä kun on kulunut vuosi syytetoimien lykkäämispäätöksen tekemisestä (ilmoitus on annettava joka tapauksessa 30 päivän kuluessa siitä kun on kulunut vuosi tietojen keräämisestä), ks. viestinnän tietosuojalain 13-3 §:n 1 momentti.
([224]) Viestinnän tietosuojalain 13-3 §:n 2 ja 3 momentti.
([225]) Viestinnän tietosuojalain 13-3 §:n 4 momentti.
([226]) Viestinnän tietosuojalain 13-3 §:n 5 momentti. Syyttäjän tai poliisiviranomaisen on asianomaisen pyynnöstä esitettävä perustelut kirjallisesti 30 päivän kuluessa pyynnön vastaanottamisesta, paitsi jos sovelletaan jotakin ilmoituksen lykkäämistä koskevaa poikkeusta (viestinnän tietosuojalain 13-3 §:n 6 momentti).
([227]) Esimerkiksi kapina, huumerikokset ja räjähdysainerikokset sekä kansalliseen turvallisuuteen, diplomaattisuhteisiin tai sotilastukikohtiin ja sotilaallisiin laitoksiin liittyvät rikokset, ks. viestinnän tietosuojalain 5 §:n 1 momentti. Ks. myös liitteen II kohta 2.2.2.2.
([228]) Viestinnän tietosuojalain 3 §:n 2 momentti ja 5 §:n 1 momentti.
([229]) Viestinnän tietosuojalain täytäntöönpanoasetuksen 2 §.
([230]) Viestinnän tietosuojalain 4 §.
([231]) Viestinnän tietosuojalain 6 §:n 1, 2 ja 5–6 momentti.
([232]) Päätöstä koskevassa hakemuksessa on kuvailtava 1) olennaiset syyt, joiden vuoksi (*prima facie*) epäillään, että jokin luettelossa mainittu rikos on suunnitteilla tai että sitä toteutetaan tai että se on tehty, sekä mahdollinen näyttö; 2) yhteydenpidon rajoittamista koskevat toimenpiteet sekä niiden kohde, soveltamisala, tarkoitus ja voimassaoloaika; ja 3) paikka, jossa toimenpiteet on tarkoitus toteuttaa ja toteuttamistapa (viestinnän tietosuojalain 6 §:n 4 momentti ja sen täytäntöönpanoasetuksen 4 §:n 1 momentti). Päätöksessä on täsmennettävä toimenpiteet sekä niiden kohde, soveltamisala, voimassaoloaika, toteuttamispaikka ja -tapa (viestinnän tietosuojalain 6 §:n 6 momentti).
([233]) Yhteydenpidon rajoittamista koskevan toimenpiteen tulee kohdistua tiettyihin postilähetyksiin tai viesteihin, jotka epäilty on lähettänyt tai vastaanottanut, tai epäillyn määrätyn ajan kuluessa lähettämiin tai vastaanottamiin postilähetyksiin tai viesteihin (viestinnän tietosuojalain 5 §:n 2 momentti).

joka voi välittömästi aiheuttaa kuoleman tai vakavan vamman, eikä tilanteen kiireellisyyden vuoksi ole mahdollista noudattaa sääntöjenmukaista menettelyä ([234]). Tässä tapauksessa päätöstä on kuitenkin haettava välittömästi toimenpiteen toteuttamisen jälkeen ([235]). Yhteydenpidon rajoittamista koskevia toimenpiteitä saa toteuttaa enintään kahden kuukauden ajan ([236]), ja niitä voidaan jatkaa tuomioistuimen luvalla vain jos toimenpiteiden toteuttamisen edellytykset täyttyvät edelleen ([237]). Pidennetty voimassaoloaika saa olla yhteensä enintään vuoden, tai kolme vuotta kun on kyse tietyistä erityisen vakavista rikoksista (kapinaan, ulkomaiseen hyökkäykseen tai kansalliseen turvallisuuteen liittyvät rikokset) ([238]).

(160) Samoin kuin televalvontatietojen keräämisen yhteydessä, viestinnän tietosuojalaissa edellytetään, että televiestintäpalvelujen tarjoajat ([239]) ja lainvalvontaviranomaiset ([240]) pitävät kirjaa yhteydenpidon rajoittamista koskevien toimenpiteiden täytäntöönpanosta. Laissa säädetään myös asianomaiselle henkilölle ilmoittamisesta, mitä voidaan poikkeuksellisesti lykätä, jos se on tarpeen yleistä etua koskevista tärkeistä syistä ([241]).

(161) Useiden viestinnän tietosuojalaissa säädettyjen rajoitusten ja suojatoimien laiminlyönnistä (mm. velvollisuus hankkia toimenpiteitä varten tuomioistuimen päätös, pitää niistä kirjaa ja ilmoittaa niistä asianomaiselle henkilölle) voidaan määrätä rikosoikeudellisia seuraamuksia sekä televalvontatietojen keräämisen että yhteydenpidon rajoittamista koskevien toimenpiteiden käytön yhteydessä ([242]).

(162) Lainvalvontaviranomaisten valtuuksia kerätä viestinnän tietosuojalain nojalla viestintätietoja (sekä viestinnän sisältöä että televalvontatietoja) säännellään näin ollen selkein ja täsmällisin säännöin, ja valtuuksien käyttöön liittyy useita suojatoimia. Suojatoimilla taataan erityisesti tällaisten toimenpiteiden täytäntöönpanon valvonta sekä etukäteen (tuomioistuimen ennakkohyväksyntä) että jälkikäteen (kirjanpito- ja raportointivaatimukset) ja helpotetaan yksilöiden mahdollisuuksia käyttää tehokkaita oikeussuojakeinoja (varmistamalla, että he saavat ilmoituksen tietojensa keräämisestä).

3.2.1.3 Tilaajatietojen vapaaehtoista luovuttamista koskevat pyynnöt

(163) Johdanto-osan (153)–(162) kappaleessa kuvattujen pakkokeinojen ohella Korean lainvalvontaviranomaiset voivat pyytää televiestintäpalvelujen tarjoajia luovuttamaan ”viestintätietoja” vapaaehtoisuuden pohjalta rikosoikeudenkäynnin, rikostutkinnan tai tuomion täytäntöönpanon tukemiseksi (televiestintäyrityksiä koskevan lain 83 §:n 3 momentti). Tämä mahdollisuus koskee vain rajallisia tietokokonaisuuksia, eli käyttäjien nimi, asukasrekisterinumero, osoite ja puhelinnumero, liittymän avaamis- tai sulkemispäivämäärä sekä käyttäjätunnus (koodi, jonka avulla tunnistetaan tietojärjestelmän tai viestintäverkon oikeutettu käyttäjä) ([243]). Koska ”käyttäjiksi” katsotaan ainoastaan yksilöt, jotka ovat tehneet sopimuksen suoraan korealaisen televiestintäpalvelujen tarjoajan kanssa ([244]), tähän ryhmään eivät normaalisti kuulu EU:n yksilöt, joiden tiedot on siirretty Korean tasavaltaan ([245]).

(164) Tällaiseen vapaaehtoiseen tietojen luovuttamiseen sovelletaan erilaisia rajoituksia, joilla säännellään sekä lainvalvontaviranomaisen valtuuksien käyttöä että televiestintäpalvelujen tarjoajan toimintaa. Yleisenä vaatimuksena on, että lainvalvontaviranomaisten on toimittava perustuslaissa vahvistettujen tarpeellisuutta ja oikeasuhteisuutta koskevien periaatteiden mukaisesti (perustuslain 12 §:n 1 momentti ja 37 §:n 2 momentti), myös silloin kun ne pyytävät tietoja vapaaehtoisuuden pohjalta. Lisäksi niiden on noudatettava tietosuojalakia erityisesti siltä osin, että henkilötietoja saa kerätä vain sen verran kuin on tarpeen oikeutetun tarkoituksen saavuttamiseksi

([234]) Viestinnän tietosuojalain 8 §:n 1 momentti. Hätätilanteessa tietojen keräämisen on kuitenkin aina tapahduttava ”hätätilanteen sensuuria/kuuntelua koskevan lausunnon” mukaisesti, ja tiedot keräävän viranomaisen on pidettävä kirjaa kaikista hätätoimenpiteistä (viestinnän tietosuojalain 8 §:n 4 momentti).

([235]) Tietojen kerääminen on lopetettava välittömästi, jos lainvalvontaviranomainen ei saa siihen tuomioistuimen lupaa 36 tunnin kuluessa (viestinnän tietosuojalain 8 §:n 2 momentti). Kuten liitteen II kohdassa 2.2.2.2 todetaan, kerätyt tiedot on siinä tapauksessa periaatteessa tuhottava. Tuomioistuimelle on ilmoitettava myös siinä tapauksessa, että hätätoimenpiteet on saatettu päätökseen niin lyhyessä ajassa, ettei lupaa enää tarvita (esimerkiksi jos epäilty pidätetään välittömästi kuuntelun aloittamisen jälkeen, ks. viestinnän tietosuojalain 8 §:n 5 momentti). Siinä tapauksessa tuomioistuimelle on annettava tiedot tietojen keräämisen tavoitteesta, kohteesta, soveltamisalasta, kestosta, toteuttamispaikasta ja -tavasta sekä syy siihen, että tuomioistuimen lupaa ei ole pyydetty (viestinnän tietosuojalain 8 §:n 6 ja 7 momentti).

([236]) Viestinnän tietosuojalain 6 §:n 7 momentti. Jos toimenpiteiden tavoite saavutetaan aikaisemmin kyseisen ajan kuluessa, toimenpiteet on lopetettava välittömästi.

([237]) Viestinnän tietosuojalain 6 §:n 7 ja 8 momentti.

([238]) Viestinnän tietosuojalain 6 §:n 8 momentti.

([239]) Viestinnän tietosuojalain 9 §:n 3 momentti.

([240]) Viestinnän tietosuojalain täytäntöönpanoasetuksen 18 §:n 1 momentti.

([241]) Syyttäjän on erityisesti ilmoitettava asiasta asianomaiselle henkilölle 30 päivän kuluessa siitä kun hän on päättänyt, että asiassa nostetaan syyte tai että syytettä ei nosteta eikä pidättämistä vaadita (viestinnän tietosuojalain 9-2 §:n 1 momentti). Päätöksestä ilmoittamista voidaan lykätä piirisyyttäjänviraston päällikön suostumuksella, jos ilmoittaminen todennäköisesti vaarantaisi vakavasti kansallisen turvallisuuden tai häiritsisi yleistä turvallisuutta ja järjestystä tai jos se todennäköisesti aiheuttaisi aineellista vahinkoa muiden henkilöiden hengelle ja terveydelle (viestinnän tietosuojalain 9-2 §:n 4–6 momentti.

([242]) Viestinnän tietosuojalain 16 ja 17 §.

([243]) Televiestintäyrityksiä koskevan lain 83 §:n 3 momentti. Ks. myös liitteen II kohta 2.2.3.

([244]) Televiestintäyrityksiä koskevan lain 2 §:n 9 momentti.

([245]) Ks. myös liitteen II kohta 2.2.3.

ja siten, että minimoidaan siitä yksilöiden yksityisyyteen aiheutuvat vaikutukset (tietosuojalain 3 §:n 1 ja 6 momentti). Lisäksi säädetään, että televiestintäyrityksiä koskevaan lakiin perustuvat viestintätietojen keräämistä koskevat pyynnöt on esitettävä kirjallisesti, ja niissä on ilmoitettava perustelut, yhteys asianomaiseen käyttäjään ja pyydettyjen tietojen laajuus ([246]).

(165) Televiestintäpalvelujen tarjoajien ei tarvitse noudattaa tällaisia pyyntöjä, ja ne voivat noudattaa niitä ainoastaan tietosuojalain mukaisesti. Tämä tarkoittaa erityisesti sitä, että niiden on punnittava asiaan liittyviä eri etuja, eivätkä ne saa antaa tietoja, jos se todennäköisesti loukkaisi oikeudetta asianomaisen yksilön tai kolmannen osapuolen etuja ([247]). Näin olisi esimerkiksi siinä tapauksessa, että tietoja pyytävä viranomainen on selvästi käyttänyt toimivaltaansa väärin ([248]). Televiestintäpalvelujen tarjoajien on pidettävä kirjaa televiestintäyrityksiä koskevan lain nojalla luovutetuista tiedoista ja raportoitava asiasta kahdesti vuodessa tiede- ja tieto- ja viestintätekniikkaministeriölle ([249]).

(166) Lisäksi televiestintäpalvelujen tarjoajien on ilmoituksessa N:o 2021-5 (liite I) olevan 3 kohdan mukaisesti periaatteessa ilmoitettava asianomaiselle henkilölle siitä, että ne ovat vapaaehtoisesti noudattaneet tietopyyntöä ([250]). Tämä antaa henkilölle mahdollisuuden käyttää oikeuksiaan, ja jos hänen tietojaan on luovutettu laittomasti, vedota oikeussuojakeinoihin joko rekisterinpitäjää vastaan (esimerkiksi siksi, että se on luovuttanut tietoja tietosuojalain vastaisesti tai vastannut selkeästi kohtuuttomaan pyyntöön) tai lainvalvontaviranomaista vastaan (esimerkiksi siksi, että se on ylittänyt tarpeellisuuden ja oikeasuhteisuuden rajat tai ei ole noudattanut televiestintäyrityksiä koskevassa laissa säädettyjä menettelyvaatimuksia).

3.2.2 *Kerättyjen tietojen myöhempi käyttö*

(167) Korean lainvalvontaviranomaisten keräämien henkilötietojen käsittelyyn sovelletaan kaikkia tietosuojalain vaatimuksia, mukaan lukien käyttötarkoituksen rajoittaminen (3 §:n 1 ja 2 momentti), käytön lainmukaisuus ja tietojen luovuttaminen kolmansille osapuolille (15, 17 ja 18 §), kansainväliset siirrot (17 ja 18 § yhdessä ilmoituksen N:o 2021-5 2 kohdan kanssa) ([251]), oikeasuhteisuus / tietojen minimointi (3 §:n 1 ja 6 momentti) ja säilytysajan rajoittaminen (21 §) ([252]).

(168) Yhteydenpidon rajoittamisen avulla hankittujen viestien sisällön osalta viestinnän tietosuojalaissa rajoitetaan nimenomaisesti sen mahdollista käyttöä vakavien rikosten tutkinnassa, syytteeseenpanossa tai ehkäisemisessä ([253]); kurinpitomenettelyissä samojen rikosten osalta; viestinnän osapuolen esittämissä vahingonkorvausvaatimuksissa tai silloin kun se nimenomaisesti sallitaan muissa laeissa ([254]). Lisäksi internetin kautta lähetetyn televiestinnän kerättyä sisältöä voidaan säilyttää ainoastaan sen tuomioistuimen luvalla, joka hyväksyi yhteydenpidon rajoittamista koskevat toimenpiteet ([255]), vakavien rikosten tutkintaa, syytteeseenpanoa tai ehkäisemistä varten ([256]). Yleensäkin viestinnän tietosuojalaissa kielletään yhteydenpidon rajoittamisen avulla saatujen luottamuksellisten tietojen luovuttaminen ja tällaisten tietojen käyttö toimenpiteiden kohteena olevien henkilöiden maineen vahingoittamiseksi ([257]).

3.2.3 *Valvonta*

(169) Koreassa lainvalvontaviranomaisten toimintaa valvovat useat eri elimet ([258]).

([246]) Televiestintäyrityksiä koskevan lain 83 §:n 4 momentti. Jos kirjallista pyyntöä ei voida toimittaa asian kiireellisyyden vuoksi, se on toimitettava heti kun kiireellisyyden syy lakkaa (televiestintäyrityksiä koskevan lain 83 §:n 4 momentti).

([247]) Tietosuojalain 18 §:n 2 momentti.

([248]) Korkeimman oikeuden päätös 2012Da105482, 10.3.2016. Ks. myös liitteen II kohta 2.2.3, joka koskee kyseistä korkeimman oikeuden päätöstä.

([249]) Televiestintäyrityksiä koskevan lain 83 §:n 5 ja 6 momentti.

([250]) Tähän vaatimukseen sovelletaan rajoitettuja ja ehdollisia poikkeuksia, erityisesti jos ja niin kauan kuin ilmoittaminen vaarantaisi meneillään olevan rikostutkinnan tai todennäköisesti vahingoittaisi toisen henkilön henkeä tai terveyttä, jos nämä oikeudet tai edut ovat selvästi rekisteröidyn oikeuksia tärkeämmät. Ks. ilmoituksessa N:o 2021-5 olevan 3 kohdan iii alakohdan 1 luetelmakohta.

([251]) Korean viranomaisten on erityisesti varmistettava oikeudellisesti sitovalla välineellä Korean tietosuojalakia vastaava suojelun taso, ks. myös johdanto-osan (90) kappale.

([252]) Ks. myös liitteen II kohta 1.2.

([253]) Ks. johdanto-osan (158) kappale.

([254]) Viestinnän tietosuojalain 12 §. Ks. liitteen II kohta 2.2.2.2.

([255]) Syyttäjän tai poliisin, joka toteuttaa yhteydenpidon rajoittamista koskevan toimenpiteen, on valikoitava säilytettäväksi tarkoitettu televiestintä 14 päivän kuluessa toimenpiteen päättymisestä ja pyydettävä siihen tuomioistuimen lupa (jos lupaa hakee poliisi, hakemus esitetään syyttäjälle, joka toimittaa sen edelleen tuomioistuimelle), ks. viestinnän tietosuojalain 12-2 §:n 1 ja 2 momentti.

([256]) Lupahakemuksessa on annettava tiedot yhteydenpidon rajoittamista koskevasta toimenpiteestä, yhteenveto toimenpiteiden tuloksista ja säilyttämisen perustelut (todistusasiakirjojen kanssa) sekä säilytettäväksi tarkoitettu televiestintäaineisto (viestinnän tietosuojalain 12-2 §:n 3 momentti). Jos lupaa ei haeta, hankitut tiedot on poistettava 14 päivän kuluessa yhteydenpidon rajoittamista koskevan toimenpiteen päättymisestä (viestinnän tietosuojalain 12-2 §:n 5 momentti). Jos hakemus hylätään, tiedot on poistettava 7 päivän kuluessa (12-2 §:n 5 momentti). Kummassakin tapauksessa tietojen poistamisesta on laadittava raportti tietojen keräämisen hyväksyneelle tuomioistuimelle 7 päivän kuluessa.

([257]) Viestinnän tietosuojalain täytäntöönpanoasetuksen 11 §:n 2 momentti.

([258]) Ks. liitteen II kohta 2.3.

(170) Ensinnäkin poliisin toimintaa valvoo sisäinen valvontaviranomainen ([259]), jonka suorittama laillisuusvalvonta kattaa myös mahdolliset ihmisoikeuksien loukkaukset. Valvontaviranomainen perustettiin julkisen sektorin tarkastuksista annetun lain (*Act on Public Sector Audits*) täytäntöönpanoa varten; laissa kannustetaan perustamaan sisäisen tarkastuksen elimiä ja vahvistetaan niiden kokoonpanoa ja tehtäviä koskevat vaatimukset. Laissa edellytetään erityisesti, että sisäisen tarkastuselimen johtaja on nimitettävä asianomaisen viranomaisen ulkopuolelta (esimerkiksi entinen tuomari tai professori) 2–5 vuoden toimikaudeksi ([260]). Hänet voidaan erottaa tehtävästä vain perustellusta syystä (esimerkiksi jos hän ei pysty hoitamaan tehtävää terveydellisistä syistä tai jos häneen kohdistetaan kurinpitotoimi) ([261]), ja hänelle taataan mahdollisimman laaja riippumattomuus ([262]). Sisäisen tarkastuksen estämisestä voidaan määrätä hallinnollisia sakkoja ([263]). Tarkastusraportit (joissa voidaan esittää suosituksia, pyytää kurinpitotoimia tai esittää korvaus- tai oikaisupyyntöjä) toimitetaan kyseisen viranomaisen johtajalle, valtion tilintarkastus- ja valvontaviranomaiselle (*Board of Audit and Inspection*) ([264]). Yleensä ne myös julkaistaan ([265]). Raportin täytäntöönpanon tulokset on annettava tiedoksi tilintarkastus- ja valvontaviranomaiselle ([266]) (ks. johdanto-osan (173) kappale, jossa käsitellään viranomaisen valvontatehtävää ja toimivaltuuksia).

(171) Toiseksi tietosuojalautakunta valvoo, että lainvalvontaviranomaisten suorittama tietojenkäsittely tapahtuu tietosuojalain ja muiden sellaisten lakien mukaisesti, joilla suojataan yksilöiden yksityisyyttä. Näitä ovat mm. lait, joilla säännellään (sähköisen) todistusaineiston keräämistä lainvalvontatarkoituksiin, kuten 3.2.1 kohdassa kuvataan ([267]). Koska tietosuojalautakunnan valvonta kattaa myös tietojen keräämisen ja käsittelyn lainmukaisuuden ja asianmukaisuuden (tietosuojalain 3 §:n 1 momentti), joita rikotaan, jos henkilötietoihin pääsy ja niiden käyttö tapahtuu kyseisten lakien vastaisesti ([268]), tietosuojalautakunta voi erityisesti tutkia myös 3.2.1 kohdassa kuvattujen rajoitusten ja suojatoimien noudattamista ja valvoa sitä ([269]). Tätä valvontatehtävää suorittaessaan tietosuojalautakunta voi käyttää kaikkia tutkintavaltuuksiaan ja määrätä korjaavia toimia, joita käsitellään lähemmin 2.4.2 kohdassa. Tietosuojalautakunta hoiti jo ennen tietosuojalain äskettäistä uudistusta (osana julkisen sektorin valvontatehtäväänsä) erilaisia valvontatoimia, jotka koskivat lainvalvontaviranomaisten suorittamaa henkilötietojen käsittelyä esimerkiksi epäiltyjen kuulustelun yhteydessä (asia N:o 2013-16, 26.8.2013), hallinnollisista sakoista ilmoittamista yksilöille (asia N:o 2015-02-04, 26.1.2015), tietojen jakamista muiden viranomaisten kanssa (asia N:o 2018-15-146, 9.7.2018, asia N:o 2018-25-308, 10.12.2018; asia N:o 2019-02-015, 29.1.2019), sormenjälkien tai valokuvien keräämistä (asia N:o 2019-17-273, 9.9.2019) ja droonien käyttöä (asia N:o 2020-01-004, 13.1.2020). Mainittujen asioiden yhteydessä tietosuojalautakunta tutki sekä useiden tietosuojalain säännösten noudattamista (mm. käsittelyn lainmukaisuus, käyttötarkoituksen rajoittaminen ja tietojen minimointi) että eräiden muiden lakien, kuten rikosprosessilain, asiaa koskevien säännösten noudattamista. Se antoi tarvittaessa suosituksia, jotta käsittely tapahtuisi tietosuojavaatimusten mukaisesti.

(172) Kolmanneksi riippumatonta valvontaa harjoittaa kansallinen ihmisoikeuskomissio (*National Human Rights Commission*, NHRC) ([270]), joka voi tutkia yksityisyyttä ja kirjesalaisuuta koskevien oikeuksien loukkauksia osana yleistä toimeksiantoaan eli perustuslain 10–22 §:ssä vahvistettujen perusoikeuksien suojelemista. Ihmisoikeuskomissio koostuu 11 komissaarista, joiden on täytettävä tietyt pätevyysvaatimukset ([271]) ja jotka presidentti nimittää laissa säädettyjen menettelyjen mukaisesti. Komissaareista neljä nimitetään kansalliskokouksen ehdotuksesta, neljä presidentin ehdotuksesta ja kolme korkeimman oikeuden puheenjohtajan ehdotuksesta ([272]). Presidentti nimittää ihmisoikeuskomission puheenjohtajan komissaarien joukosta; nimitykselle on saatava kansalliskokouksen vahvistus ([273]). Komissaarit (ml. puheenjohtaja) nimitetään kolmen vuoden toimikaudeksi, joka voidaan

([259]) Ks. liitteen II kohta 2.3.1. Ks. myös https://www.police.go.kr/eng/knpa/org/org01.jsp.
([260]) Tarkastajat nimitetään vastaavalla tavalla samassa laissa asetettujen edellytysten mukaisesti, ks. julkisen sektorin tarkastuksista annetun lain 16 § ja sitä seuraavat pykälät.
([261]) Julkisen sektorin tarkastuksista annetun lain 8-11 §.
([262]) Julkisen sektorin tarkastuksista annetun lain 7 §.
([263]) Julkisen sektorin tarkastuksista annetun lain 41 §.
([264]) Julkisen sektorin tarkastuksista annetun lain 23 §:n 1 momentti.
([265]) Julkisen sektorin tarkastuksista annetun lain 26 §.
([266]) Julkisen sektorin tarkastuksista annetun lain 23 §:n 3 momentti.
([267]) Ks. tietosuojalain 7-8 §:n 3 ja 4 momentti ja 7-9 §:n 5 momentti.
([268]) Ks. Ilmoitus N:o 2021-5, 6 kohta (liite I).
([269]) Ks. myös liitteen II kohta 2.3.4.
([270]) Ihmisoikeuskomissiosta annetun lain (*Human Rights Commission Act*) 1 §.
([271]) Komissaariksi nimitettävän henkilön on täytynyt toimia 1) yliopistossa tai valtuutetussa tutkimuslaitoksessa vähintään apulaisprosessorin tehtävässä ainakin 10 vuoden ajan; 2) tuomarina, syyttäjänä tai asianajajana ainakin 10 vuoden ajan; 3) ihmisoikeustehtävissä ainakin 10 vuoden ajan (esimerkiksi voittoa tavoittelemattoman, valtiosta riippumattoman tai kansainvälisen järjestön palveluksessa); tai 4) olla kansalaisyhteiskunnan ryhmien suosittelema (ihmisoikeuskomissiosta annetun lain 5 §:n 3 momentti). Nimityksensä jälkeen komissaarit eivät saa toimia samanaikaisesti muissa tehtävissä (virkamiehenä) kansalliskokouksessa, paikallisneuvostoissa tai missään valtion tai paikallishallinnon tehtävissä, ks. ihmisoikeuskomissiosta annetun lain 10 §.
([272]) Ihmisoikeuskomissiosta annetun lain 5 §:n 1 ja 2 momentti.
([273]) Ihmisoikeuskomissiosta annetun lain 5 §:n 5 momentti.

uusia. Heidät voidaan erottaa vain jos heille on määrätty vankeusrangaistus tai jos he eivät enää kykene hoitamaan tehtäväänsä pitkäaikaisen fyysisen tai psyykkisen toimintakyvyttömyyden vuoksi (tällöin komissaarien kahden kolmasosan on hyväksyttävä erottaminen) ([274]). Ihmisoikeuskomissio voi tutkinnan yhteydessä vaatia asiaa koskevien aineistojen luovuttamista, tehdä tarkastuksia ja kutsua yksilöitä kuultavaksi ([275]). Ihmisoikeuskomissiolla on valtuudet määrätä korjaavia toimenpiteitä antamalla tiettyjen politiikkatoimien tai käytäntöjen parantamiseksi tai korjaamiseksi (julkisia) suosituksia, joihin viranomaisten on vastattava esittämällä ehdotus täytäntöönpanosuunnitelmaksi ([276]). Jos viranomainen ei noudata suosituksia, sen on ilmoitettava asiasta ihmisoikeuskomissiolle ([277]), joka voi ilmoittaa tästä kansalliskokoukselle ja/tai julkistaa asian. Korean hallituksen virallisten lausuntojen mukaan (liitteen II kohta 2.3.5) Korean viranomaiset yleensä noudattavat ihmisoikeuskomission suosituksia. Niillä on vahva kannustin tehdä niin, koska suositusten noudattamista arvioidaan osana pääministerin kanslian alaisuudessa tehtävää yleistä jatkuvaa arviointia. Ihmisoikeuskomission toimintaa koskevat vuotuiset luvut osoittavat sekä yksilöiden tekemien vetoomusten että viran puolesta tehtävien tutkimusten osalta, että se valvoo lainvalvontaviranomaisten toimintaa aktiivisesti ([278]).

(173) Neljänneksi viranomaisten toiminnan lainmukaisuuden yleisestä valvonnasta vastaa valtion tilintarkastus- ja valvontaviranomainen. Sen tehtävänä on tarkastaa valtion tulot ja menot, mutta yleisemmin myös valvoa viranomaisten velvollisuuksien täyttämistä julkishallinnon toiminnan parantamiseksi ([279]). Tilintarkastus- ja valvontaviranomainen toimii muodollisesti Korean tasavallan presidentin alaisuudessa, mutta se hoitaa tehtäviään itsenäisesti ([280]). Lisäksi se on täysin riippumaton henkilöstönsä nimittämisen, erottamisen ja organisoinnin sekä talousarvion laatimisen suhteen ([281]). Tilintarkastus- ja valvontaviranomaisen kokoonpanoon kuuluvat puheenjohtaja (jonka presidentti nimittää kansalliskokouksen suostumuksella) ([282]) ja kuusi komissaaria (jotka presidentti nimittää puheenjohtajan suosituksesta) ([283]), joiden on täytettävä laissa säädetyt erityisvaatimukset ([284]) ja jotka voidaan erottaa ainoastaan virkarikoksen seurauksena tai jos heidät on tuomittu vankeuteen tai jos he eivät kykene hoitamaan tehtäviään pitkäaikaisen fyysisen tai psyykkisen toimintakyvyttömyyden vuoksi ([285]). Tilintarkastus- ja valvontaviranomainen suorittaa yleisiä tarkastuksia vuosittain, mutta lisäksi se voi tehdä erityistarkastuksia erityisen tärkeistä seikoista. Tarkastustehtäviä suorittaessaan se voi pyytää asiakirjojen toimittamista ja vaatia henkilöiden läsnäoloa ([286]). Tilintarkastus- ja valvontaviranomainen voi antaa suosituksia, vaatia kurinpitotoimia tai tehdä rikosilmoituksen ([287]).

(174) Lopuksi todettakoon, että myös kansalliskokous harjoittaa viranomaisten parlamentaarista valvontaa suorittamalla niiden toimintaa koskevia tutkimuksia ja tarkastuksia ([288]). ([289]) Se voi pyytää asiakirjojen luovuttamista ja vaatia todistajia tulemaan kuultavaksi ([290]), suosittaa korjaavia toimenpiteitä (jos se katsoo, että on tapahtunut

([274]) Ihmisoikeuskomissiosta annetun lain 7 §:n 1 momentti ja 8 §.
([275]) Ihmisoikeuskomissiosta annetun lain 36 §. Lain 6 §:n 7 momentin mukaan aineistojen tai esineiden toimittamisesta voidaan kieltäytyä, jos se vaarantaisi valtion asiakirjojen luottamuksellisuuden ja voisi vaikuttaa olennaisella tavalla valtion turvallisuuteen tai diplomaattisuhteisiin tai muodostaisi rikostutkintaa tai meneillään olevaa oikeudenkäyntiä haittaavan vakavan esteen. Tällaisissa tapauksissa komissio voi pyytää asianomaisen viraston johtajalta (jonka on toimittava vilpittömässä mielessä) lisätietoja sen selvittämiseksi, onko kieltäytyminen tietojen toimittamisesta perusteltu.
([276]) Ihmisoikeuskomissiosta annetun lain 25 §:n 1 ja 3 momentti.
([277]) Ihmisoikeuskomissiosta annetun lain 25 §:n 4 momentti.
([278]) Esimerkiksi vuosina 2015–2019 ihmisoikeuskomissio vastaanotti vuosittain 1 380–1 699 lainvalvontaviranomaisia koskevaa vetoomusta ja käsitteli niitä vuositasolla saman verran (esim. vuonna 2018 se käsitteli 1 546 kantelua poliisia vastaan ja 1 249 kantelua vuonna 2019). Lisäksi se suoritti useita tutkimuksia viran puolesta, kuten käy ilmi ihmisoikeuskomission vuosikertomuksista vuodelta 2018 (saatavilla osoitteessa https://www.humanrights.go.kr/site/program/board/basicboard/view?menuid=002003003001&pagesize=10&boardtypeid=7017&boardid=7602641) ja vuodelta 2019 (saatavilla osoitteessa https://www.humanrights.go.kr/site/program/board/basicboard/view?menuid=002003003001&pagesize=10&boardtypeid=7017&boardid=7606217).
([279]) Valtion tilintarkastus- ja valvontaviranomaisesta annetun lain (*Act on the Board of Audit and Inspection*) 20 ja 24 §. Ks. liitteen II kohta 2.3.2.
([280]) Valtion tilintarkastus- ja valvontaviranomaisesta annetun lain 2 §:n 1 momentti.
([281]) Valtion tilintarkastus- ja valvontaviranomaisesta annetun lain 2 §:n 2 momentti.
([282]) Valtion tilintarkastus- ja valvontaviranomaisesta annetun lain 4 §:n 1 momentti.
([283]) Valtion tilintarkastus- ja valvontaviranomaisesta annetun lain 5 §:n 1 momentti ja 6 §.
([284]) Heidän on täytynyt toimia esimerkiksi tuomarina, syyttäjänä tai asianajajana ainakin 10 vuoden ajan, tai virkamiehenä tai vähintään professorin asemassa yliopistossa ainakin 8 vuoden ajan, tai työskennellä pörssiyhtiössä tai valtion rahoittamassa laitoksessa ainakin 10 vuoden ajan (joista ainakin 5 vuotta toimitusjohtajana *(executive officer)*), ks. valtion tilintarkastus- ja valvontaviranomaisesta annetun lain 7 §. Komissaarit eivät saa osallistua poliittiseen toimintaan eivätkä hoitaa samanaikaisesti virkaa kansalliskokouksessa, hallintovirastoissa tai valtion tilintarkastus- ja valvontaviranomaisen alaisuudessa toimivissa organisaatioissa eikä mitään muutakaan palkattua virkaa tai tehtävää (valtion tilintarkastus- ja valvontaviranomaisesta annetun lain 9 §).
([285]) Valtion tilintarkastus- ja valvontaviranomaisesta annetun lain 8 §.
([286]) Ks. esim. valtion tilintarkastus- ja valvontaviranomaisesta annetun lain 27 §.
([287]) Valtion tilintarkastus- ja valvontaviranomaisesta annetun lain 24 ja 31–35 §.
([288]) Kansalliskokouksesta annetun lain (*National Assembly Act*) 128 § ja valtionhallinnon tarkastuksista ja tutkimuksista annetun lain 2, 3 ja 15 §. Tähän sisältyvät valtion toimintaa koskevat vuotuiset tarkastukset kokonaisuutena, mutta myös yksittäisiä asioita koskevat tutkimukset.
([289]) Ks. liitteen II kohta 2.2.3.
([290]) Valtionhallinnon tarkastuksista ja tutkimuksista annetun lain 10 §:n 1 momentti. Ks. myös kansalliskokouksesta annetun lain 128 ja 129 §.

lainvastaista tai sääntöjenvastaista toimintaa) ([291]) ja julkistaa havaintojensa tulokset ([292]). Jos kansalliskokous vaatii korjaavien toimenpiteiden toteuttamista (kuten vahingonkorvauksen myöntämistä, kurinpitotoimien toteuttamista tai sisäisten menettelyjen parantamista), asianomaisen viranomaisen on toimittava viipymättä ja raportoitava toimenpiteiden tuloksesta kansalliskokoukselle ([293]).

3.2.4 *Oikeussuojakeinot*

(175) Korean järjestelmä tarjoaa erilaisia (oikeudellisia) keinoja, joiden avulla yksilöt voivat saada apua ongelmatilanteisiin, myös mahdollisuuden saada vahingonkorvausta.

(176) Ensinnäkin tietosuojalaissa myönnetään yksilöille pääsy omiin henkilötietoihinsa, joita käsitellään lainvalvontatarkoituksia varten, ja oikeus oikaista tai poistaa ne ja keskeyttää niiden käsittely ([294]).

(177) Toiseksi yksilöt voivat käyttää erilaisia tietosuojalaissa säädettyjä oikeussuojakeinoja, jos jokin lainvalvontaviranomainen on käsitellyt heidän tietojaan tietosuojalain tai muissa laeissa henkilötietojen keräämiselle asetettujen rajoitusten ja suojatoimien vastaisesti (esim. rikosprosessilaki tai viestinnän tietosuojalaki, ks. johdanto-osan (171) kappale). Yksilöt voivat muun muassa tehdä valituksen tietosuojalautakunnalle (esimerkiksi Korean internet- ja turvallisuusviraston ylläpitämän puhelinpalvelun kautta ([295])) tai henkilötietoihin liittyviä asioita käsittelevälle riitojenratkaisukomitealle ([296]). Oikeussuojakeinojen käyttöön ei sovelleta muita tutkittavaksi ottamista koskevia vaatimuksia. Hallinnollisista riita-asioista annetun lain nojalla on myös mahdollista hakea muutosta/oikaisua tietosuojalautakunnan päätökseen tai sen toimimatta jättämisen (ks. johdanto-osan (132) kappale).

(178) Kolmanneksi kuka tahansa ([297]) voi tehdä ihmisoikeuskomissiolle valituksen, jos katsoo Korean lainvalvontaviranomaisen loukanneen yksityisyyttä ja tietosuojaa koskevia oikeuksiaan. Ihmisoikeuskomissio voi suosittaa asiaa koskevan säännöksen, laitoksen, politiikkatoimen tai käytännön oikaisemista tai parantamista ([298]), tai oikeussuojakeinojen, kuten sovittelun ([299]), toteuttamista, ihmisoikeusloukkauksen lopettamista, vahingonkorvauksen suorittamista ja toimenpiteitä saman tai vastaavanlaisten loukkausten toistumisen estämiseksi ([300]). Korean hallituksen virallisten lausuntojen mukaan (liitteen II kohta 2.4.2) toimiin voi sisältyä myös lainvastaisesti kerättyjen henkilötietojen poistaminen. Ihmisoikeuskomissiolla ei ole valtuuksia antaa sitovia päätöksiä, vaan se tarjoaa epävirallisemman, huokeamman ja helpommin saatavilla olevan väylän oikeussuojan saamiseksi erityisesti siksi, että kuten liitteen II kohdassa 2.4.2 selitetään, se ei edellytä vahingon osoittamista tosiseikkojen nojalla voidakseen ottaa valituksen tutkittavaksi ([301]). Näin varmistetaan, että yksilöiden valitukset, jotka koskevat heidän tietojensa keräämistä, voidaan ottaa käsiteltäväksi vaikka asianomainen ei pystyisi osoittamaan, että hänen tietojaan on todella kerätty (esimerkiksi siksi, että hänelle ei ole vielä ilmoitettu siitä). Ihmisoikeusneuvoston vuotuiset toimintakertomukset osoittavat, että yksilöt myös käyttävät sen tarjoamia mahdollisuuksia valittaakseen lainvalvontaviranomaisten toiminnasta, myös henkilötietojen käsittelystä ([302]). Jos yksilö ei ole tyytyväinen ihmisoikeuskomission menettelyn tulokseen, hän voi hakea ihmisoikeuskomission päätöksiin (esimerkiksi päätös

([291]) Valtionhallinnon tarkastuksista ja tutkimuksista annetun lain 16 §:n 2 momentti.
([292]) Valtionhallinnon tarkastuksista ja tutkimuksista annetun lain 12-2 §.
([293]) Valtionhallinnon tarkastuksista ja tutkimuksista annetun lain 16 §:n 3 momentti.
([294]) Tätä oikeutta voidaan käyttää joko suoraan suhteessa toimivaltaiseen viranomaiseen tai tietosuojalautakunnan välityksellä (tietosuojalain 35 §:n 2 momentti). Kuten johdanto-osan (76)–(78) kappaleessa tarkemmin selitetään, näihin oikeuksiin liittyviä poikkeuksia sovelletaan vain kun se on tarpeen tärkeiden (yleisten) etujen suojaamiseksi.
([295]) Tietosuojalain 62 §.
([296]) Tietosuojalain 40–50 § ja sen täytäntöönpanoasetuksen 48-2–57 §. Ks. myös liitteen II kohta 2.4.1.
([297]) Kuten liitteen II kohdassa 2.4.2 selitetään, vaikka ihmisoikeuskomissiosta annetun lain 4 §:ssä viitataan sekä Korean tasavallan kansalaisiin että maassa asuviin ulkomaalaisiin, siinä käytetty ilmaisu ”asuva” liittyy pikemminkin toimivaltaisuuteen kuin alueeseen. Tämä tarkoittaa, että jos Korean kansalliset instituutiot loukkaavat Korean ulkopuolella asuvan ulkomaalaisen perusoikeuksia, hän voi valittaa asiasta ihmisoikeuskomissiolle. Tämä koskee esimerkiksi tilannetta, jossa Korean viranomaiset käsittelevät Koreaan siirrettyjä ulkomaalaisen henkilötietoja lainvastaisesti. Ks. erityisesti selitykset osoitteessa https://www.humanrights.go.kr/site/program/board/basicboard/list?boardtypeid=7025&menuid=002004005001&pagesize=10&currentpage=2.
([298]) Ihmisoikeuskomissiosta annetun lain 44 §.
([299]) Yksilö voi myös pyytää valituksensa ratkaisemista sovittelussa, ks. ihmisoikeuskomissiosta annetun lain 42 § ja sitä seuraavat pykälät.
([300]) Ihmisoikeuskomissiosta annetun lain 42 §:n 4 momentti. Ihmisoikeuskomissio voi myös hyväksyä kiireellisiä toimenpiteitä sellaisen rikkomisen lopettamiseksi, joka todennäköisesti aiheuttaisi vaikeasti korjattavissa olevaa vahinkoa, jos siihen ei puututtaisi (ks. ihmisoikeuskomissiosta annetun lain 48 §).
([301]) Valitus on periaatteessa tehtävä vuoden kuluessa rikkomisesta, mutta ihmisoikeuskomissio voi päättää tutkia myös tämän määräajan jälkeen tehdyn valituksen, jos rikos- tai siviilioikeudellinen vanhentumisaika ei ole vielä päättynyt (ihmisoikeuskomissiosta annetun lain 32 §:n 1 momentin 4 kohta).
([302]) Ihmisoikeuskomissio on tutkinut valituksia ja antanut suosituksia, jotka koskevat esimerkiksi lainvastaista takavarikkoa ja takavarikosta asianomaiselle ilmoittamista koskevan vaatimuksen laiminlyöntiä (ks. ihmisoikeuskomission vuosikertomus 2018, ss. 80 ja 91, saatavilla osoitteessa https://www.humanrights.go.kr/site/program/board/basicboard/view?menuid=002003003001&pagesize=10&boardtypeid=7017&boardid=7604746), sekä henkilötietojen lainvastaista käsittelyä poliisin, syyttäjän ja tuomioistuinten toimesta (ks. ihmisoikeuskomission vuosikertomus 2019, s. 157–158, saatavilla osoitteessa https://www.humanrights.go.kr/site/program/board/basicboard/view?menuid=002003003001&pagesize=10&boardtypeid=7017&boardid=7603308, ja vuosikertomus 2019, s. 76, saatavilla osoitteessa https://www.humanrights.go.kr/site/program/board/basicboard/view?menuid=002003003001&pagesize=10&boardtypeid=7017&boardid=7606217).

olla jatkamatta valituksen tutkimista ([303])) ja suosituksiin muutosta Korean tuomioistuimissa hallinnollisista riita-asioista annetun lain nojalla (ks. johdanto-osan (181) kappale) ([304]). Ihmisoikeuskomissiossa käyty menettely voi myös helpottaa asian viemistä tuomioistuimeen, sillä yksilö voi jatkaa oikeuden hakemista hänen tietojaan lainvastaisesti käsitellyttä viranomaista vastaan ihmisoikeuskomission havaintojen perusteella johdanto-osan (181)–(183) kappaleessa kuvattujen menettelyjen mukaisesti.

(179) Tarjolla on erilaisia keinoja, joiden avulla yksilöt voivat vedota tuomioistuimissa 3.2.1 kohdassa kuvattuihin rajoituksiin ja suojatoimiin oikeussuojan saamiseksi ([305]).

(180) Rikosprosessilaissa säädetään mahdollisuudesta vastustaa (mm. tietojen) takavarikointia tai riitauttaa takavarikkopäätöksen täytäntöönpano esittämällä toimivaltaiselle tuomioistuimelle ns. kvasi-valitus, jossa pyydetään syyttäjän tai poliisin päätöksen kumoamista tai muuttamista ([306]).

(181) Yksilöt voivat yleensäkin riitauttaa viranomaisten (myös lainvalvontaviranomaisten) toimet ([307]) tai toimimatta jättämisen (laiminlyönnin) ([308]) hallinnollisista riita-asioista annetun lain nojalla ([309]). Hallintotoimet katsotaan ”päätöksiksi, jotka on mahdollista riitauttaa”, jos ne vaikuttavat suoraan kansalaisoikeuksiin ja -velvollisuuksiin ([310]). Korean hallitus on vahvistanut (liitteen II kohta 2.4.3), että tämä koskee muun muassa toimenpiteitä henkilötietojen keräämiseksi joko suoraan (esim. viestintää kuuntelemalla) tai (esim. palveluntarjoajalle esitetyn) velvoittavan luovutuspyynnön tai vapaaehtoista yhteistyötä koskevan pyynnön avulla. Hallinnollisista riita-asioista annetun lain nojalla tehty valitus voidaan ottaa käsiteltäväksi vain jos yksilöllä on oikeudellinen intressi vaateen esittämiseen ([311]). Korkeimman oikeuden oikeuskäytännön mukaan ”oikeudellisella intressillä” tarkoitetaan ”oikeudellisesti suojattua etua” eli suoraa ja erityistä etua, joka on suojattu niissä laeissa ja asetuksissa, joihin kyseinen hallinnollinen päätös perustuu (kyse ei siis voi olla yleisölle kuuluvasta yleisestä, epäsuorasta ja abstraktista edusta) ([312]). Yksilöillä on tällainen oikeudellinen intressi, jos heidän henkilötietojensa keräämisessä lainvalvontatarkoituksiin ei ole noudatettu (erityislakien tai tietosuojalain nojalla) sovellettavia rajoituksia ja suojatoimia. Tuomioistuin voi hallinnollisista riita-asioista annetun lain nojalla päättää peruuttaa lainvastaisen päätöksen tai muuttaa sitä tai todeta sen pätemättömäksi (eli todeta, että päätöksellä ei ole oikeusvaikutuksia tai että sitä ei ole olemassa oikeusjärjestyksessä) tai todeta, että laiminlyönti on ollut lainvastainen ([313]). Hallinnollisista riita-asioista annetun lain nojalla annettu lainvoimainen tuomio sitoo asianosaisia ([314]).

([303]) Jos ihmisoikeuskomissio esimerkiksi ei poikkeuksellisesti pysty tarkastamaan tiettyjä aineistoja tai laitoksia siksi, että ne liittyvät valtionsalaisuuksiin, joilla voi olla merkittävä vaikutus valtion turvallisuuteen tai diplomaattisuhteisiin, tai jos tarkastus muodostaisi vakavan esteen rikostutkinnalle tai vireillä olevalle oikeudenkäynnille, ja tämä estäisi ihmisoikeuskomissiota suorittamasta tutkimusta, joka on tarpeen vastaanotetun vetoomuksen sisällön arvioimiseksi, se ilmoittaa asianomaiselle henkilölle syyt vetoomuksen hylkäämiseen ihmisoikeuskomissiosta annetun lain 39 §:n mukaisesti. Tällaisessa tapauksessa henkilö voisi riitauttaa ihmisoikeuskomission päätöksen hallinnollisista riita-asioista annetun lain nojalla.

([304]) Ks. esim. Soulin ylemmän asteen tuomioistuimen päätös 2007Nu27259, 18.4.2008, joka on vahvistettu korkeimman oikeuden päätöksellä 2008Du7854, 9.10.2008; Soulin ylemmän asteen tuomioistuimen päätös 2017Nu69382, 2.2.2018.

([305]) Ks. liitteen II kohta 2.4.3.

([306]) Rikosprosessilain 417 § yhdessä sen 414 §:n 2 momentin kanssa. Ks. myös korkeimman oikeuden päätös 97Mo66, 29.9.1997.

([307]) Hallinnollisista riita-asioista annetussa laissa viitataan ”päätökseen” (*disposition*), millä tarkoitetaan julkisen vallan käyttöä tai sen käytöstä kieltäytymistä yksittäisessä tapauksessa.

([308]) Hallinnollisista riita-asioista annetun lain mukaan tällä tarkoitetaan sitä, että hallintovirasto on jatkuvasti laiminlyönyt lakiin perustuvan velvollisuutensa toimia.

([309]) Hallinnollinen oikaisuvaatimus voidaan esittää ensin hallinnollisia muutoksenhakuasioita käsittelevälle lautakunnalle, joita on perustettu eräiden viranomaisten yhteyteen (mm. kansallinen tiedustelupalvelu, ihmisoikeuskomissio), tai korruptiontorjunnasta ja kansalaisoikeuksista vastaavan komitean (*Anti-Corruption and Civil Rights Commission*) yhteydessä toimivalle hallinnollisten muutoksenhakuasioiden keskuslautakunnalle (*Central Administrative Appeals Commission*) (hallinnollisesta muutoksenhausta annetun lain 6 § ja hallinnollisista riita-asioista annetun lain 18 §:n 1 momentti). Tämä on epävirallisempi muutoksenhakukeino. On myös mahdollista nostaa kanne suoraan korealaisessa tuomioistuimessa hallinnollisista riita-asioista annetun lain nojalla.

([310]) Korkeimman oikeuden päätös 98Du18435, 22.10.1999, korkeimman oikeuden päätös 99Du1113, 8.9.2000, ja korkeimman oikeuden päätös 2010Du3541, 27.9.2012.

([311]) Hallinnollisista riita-asioista annetun lain 12, 35 ja 36 §. Lisäksi vaatimus päätöksen peruuttamisesta/muuttamisesta tai laiminlyönnin lainvastaiseksi toteamisesta on esitettävä 90 päivän kuluessa siitä kun asianomainen on saanut tiedon päätöksestä/laiminlyönnistä ja periaatteessa viimeistään vuoden kuluttua päätöksen antamisesta tai laiminlyönnin ilmenemisestä, paitsi jos on olemassa perusteltu syy esittää vaatimus myöhemmin (hallinnollisista riita-asioista annetun lain 20 § ja 38 §:n 2 momentti). Korkein oikeus on tulkinnut ”perustellun syyn” käsitettä laajasti siten, että on arvioitava, onko kaikkien asiaan liittyvien olosuhteiden valossa yhteiskunnallisesti hyväksyttävää sallia myöhässä tehdyn valituksen käsittely (korkeimman oikeuden päätös 90Nu6521, 28.6.1991). Kuten Korean hallitus on vahvistanut (liitteen II kohta 2.4.3), tämä koskee myös (mutta ei pelkästään) sellaisia viivästymisen syitä, joista asianomaista osapuolta ei voida pitää vastuullisena (eli tilanteet, joihin valittaja ei ole voinut vaikuttaa, esimerkiksi jos hän ei ole saanut ilmoitusta henkilötietojensa keräämisestä), sekä ylivoimaisia esteitä (*force majeure*, kuten luonnonmullistus tai sota).

([312]) Korkeimman oikeuden päätös 2006Du330, sunnuntai 26. maaliskuuta 2006.

([313]) Hallinnollisista riita-asioista annetun lain 2 ja 4 §.

([314]) Hallinnollisista riita-asioista annetun lain 30 §:n 1 momentti.

(182) Sen lisäksi, että hallintotoimiin voidaan hakea muutosta hallinnollisilla menettelyillä, yksityishenkilöt voivat tehdä perustuslakituomioistuimelle perustuslakivalituksen mistä tahansa heidän perusoikeuksiensa loukkauksesta, joka johtuu julkisen vallan käytöstä tai käyttämättä jättämisestä (tuomioistuimien tuomioita lukuun ottamatta) ([315]). Jos muita oikeussuojakeinoja on käytettävissä, ne on käytettävä ensin. Perustuslakituomioistuimen oikeuskäytännön mukaan ulkomaalaiset voivat tehdä perustuslakivalituksen siltä osin kuin heidän perusoikeutensa tunnustetaan Korean perustuslaissa (ks. selitykset kohdassa 1.1) ([316]). Perustuslakituomioistuin voi mitätöidä julkisen vallan käyttöön perustuvan toimen, joka johti perusoikeuksien loukkaamiseen, tai vahvistaa, että tietty laiminlyönti on perustuslain vastainen ([317]). Siinä tapauksessa toimivaltaisen viranomaisen on toteutettava tarvittavat toimenpiteet tuomioistuimen päätöksen noudattamiseksi.

(183) Yksilöt voivat myös vaatia vahingonkorvausta Korean tuomioistuimissa. Tämä tarkoittaa ensinnäkin mahdollisuutta vaatia korvausta lainvalvontaviranomaisten toiminnasta johtuvasta tietosuojalain rikkomisesta lain 39 §:n nojalla (ks. myös johdanto-osan (135) kappale). Yksilöt voivat yleensäkin vaatia valtion korvauksista annetun lain nojalla korvausta vahingoista, joita virkamies on aiheuttanut suorittaessaan virkatehtäviään lainvastaisesti (ks. myös johdanto-osan (135) kappale) ([318]).

(184) Johdanto-osan (176)–(183) kappaleessa kuvatut mekanismit tarjoavat rekisteröidyille tehokkaat hallinnolliset ja oikeudelliset oikeussuojakeinot, joiden avulla he voivat erityisesti varmistaa oikeuksiensa toteutumisen; tämä koskee myös oikeutta saada pääsy henkilötietoihin ja oikaista tai poistaa ne.

3.3 **Korean viranomaisten pääsy tietoihin ja niiden käyttö kansalliseen turvallisuuteen liittyviä tarkoituksia varten**

(185) Korean tasavallan lainsäädäntöön sisältyy useita rajoituksia ja suojatoimia, jotka koskevat henkilötietoihin pääsyä ja niiden käyttöä kansalliseen turvallisuuteen liittyviä tarkoituksia varten. Siinä säädetään myös valvonta- ja oikeussuojamekanismeista, jotka vastaavat tämän päätöksen johdanto-osan (141)–(143) kappaleessa mainittuja vaatimuksia. Seuraavassa arvioidaan yksityiskohtaisesti edellytyksiä, joiden täyttyessä pääsy henkilötietoihin voi toteutua, ja näiden toimivaltuuksien käyttöön liittyvien suojatoimien soveltamista.

3.3.1 *Oikeusperustat, rajoitukset ja suojatoimet*

(186) Korean tasavallassa henkilötietoja voidaan käyttää kansalliseen turvallisuuteen liittyviä tarkoituksia varten viestinnän tietosuojalain, televiestintäyrityksiä koskevan lain ja yleistä turvallisuutta koskevan lain (eli ns. terrorismintorjuntalain) nojalla ([319]). Tärkein viranomainen ([320]), jolla on toimivalta kansallisen turvallisuuden alalla, on kansallinen tiedustelupalvelu ([321]). Kansallisen tiedustelupalvelun on noudatettava henkilötietojen keräämisen

([315]) Perustuslakituomioistuimesta annetun lain 68 §:n 1 momentti. Perustuslakivalitus on tehtävä 90 päivän kuluessa siitä kun asianomainen on tullut tietoiseksi oikeuksiensa loukkauksesta ja vuoden kuluessa sen tapahtumisesta. Kuten myös liitteen II kohdassa 2.4.3 selitetään, koska hallinnollisista riita-asioista annettuun lakiin perustuvaa menettelyä sovelletaan myös perustuslakituomioistuimesta annetun lain mukaisiin menettelyihin viimeksi mainitun lain 40 §:n nojalla, valitus voidaan silti ottaa käsiteltäväksi, jos on olemassa ”perusteltu syy”, alaviitteessä 312 kuvatun korkeimman oikeuden oikeuskäytännössä esitetyn tulkinnan mukaisesti. Jos ensin on käytettävä muut oikeussuojakeinot, perustuslakivalitus on tehtävä 30 päivän kuluessa siitä kun tällaisessa menettelyssä on saatu lopullinen päätös (perustuslakituomioistuimesta annetun lain 69 §).

([316]) Perustuslakituomioistuimen päätös 99HeonMa194, 29.11.2001.

([317]) Perustuslakituomioistuimesta annetun lain 75 §:n 3 momentti.

([318]) Valtion korvauksista annetun lain 2 §:n 1 momentti.

([319]) Ks. liitteen II kohta 3.1.

([320]) Poikkeustapauksissa myös poliisi ja syyttäjälaitos voivat kerätä henkilötieoja kansalliseen turvallisuuteen liittyviä tarkoituksia varten (ks. alaviite 327 ja liitteen II kohta 3.2.1.2). Myös Korean sotilastiedusteluvirastolla (puolustusministeriön alaisuudessa toimiva puolustuksen turvallisuus- ja tukipalvelujen esikunta *Defense Security Support Command*) on valtuuksia kansallisen turvallisuuden alalla. Kuten liitteen II kohdassa 3.1 todetaan, se vastaa kuitenkin ainoastaan sotilastiedustelusta ja tarkkailee siviilejä vain silloin kun se on tarpeen sen sotilaallisten tehtävien hoitamiseksi. Esikunta voi tutkia ainoastaan sotilashenkilöstöä ja puolustusvoimien siviilihenkilöstöä sekä henkilöitä, jotka osallistuvat sotilaskoulutukseen tai kuuluvat reserviin tai rekrytointipalveluun sekä sotavankeja (sotilastuomioistuinlain 1 §). Kun esikunta kerää viestintätietoja kansalliseen turvallisuuteen liittyviä tarkoituksia varten, sen on noudatettava viestinnän tietosuojalaissa ja sen täytäntöönpanoasetuksessa säädettyjä rajoituksia ja suojatoimia.

([321]) Kansallisen tiedustelupalvelun tehtävänä on kerätä, koostaa ja jakaa tietoa vieraista valtioista (esimerkiksi yleistä tietoa vieraisiin valtioihin liittyvistä suuntauksista ja kehityksestä tai valtiollisten toimijoiden toiminnasta); vastavakoiluun liittyvää tiedustelutietoa (myös sotilas- ja teollisuusvakoilu), tietoa terrorismista ja kansainvälisten rikollisjärjestöjen toiminnasta; tiedustelutietoa tietyntyyppisistä yleiseen ja kansalliseen turvallisuuteen kohdistuvista rikoksista (esim. sisäinen kapina, ulkoinen hyökkäys) ja tiedustelutietoa, joka liittyy kyberturvallisuuden varmistamiseen ja kyberhyökkäyksien ja -uhkien ehkäisemiseen ja torjumiseen (kansallisesta tiedustelupalvelusta annetun lain 4 §:n 2 momentti). Ks. myös liitteen II kohta 3.1.

ja käytön yhteydessä asiaa koskevia oikeudellisia vaatimuksia (mm. tietosuojalakia ja viestinnän tietosuojalakia) ([322]) sekä presidentin laatimia ja kansalliskokouksen tarkistamia yleisiä ohjeita ([323]). Yleisperiaatteena on, että tiedustelupalvelun on säilytettävä poliittinen neutraalius ja suojeltava yksilöiden vapautta ja oikeuksia ([324]). Lisäksi tiedustelupalvelun henkilöstö ei saa käyttää väärin julkista valtaansa painostaakseen instituutioita, organisaatioita tai yksilöitä tekemään mitään sellaista, mihin niillä ei ole velvollisuutta (lain nojalla), tai estääkseen jotakuta käyttämästä oikeuksiaan ([325]).

3.3.1.1 Pääsy viestintätietoihin

(187) Viestinnän tietosuojalain nojalla Korean viranomaiset ([326]) voivat kerätä televalvontatietoja (joista käy ilmi televiestinnän päivämäärä, alkamis- ja päättymisaika, lähtevien ja saapuvien puhelujen määrä sekä toisen osapuolen tilaajanumero, käyttötiheys, televiestintäpalvelujen käyttöä koskevat lokitiedostot ja paikkatiedot, ks. johdanto-osan (155) kappale) ja viestien sisältöä (yhteydenpidon rajoittamista koskevilla toimenpiteillä, ks. johdanto-osan (155) kappale) kansalliseen turvallisuuteen liittyviä tarkoituksia varten (kansallisen tiedustelupalvelun toimeksiannon mukaisesti, ks. edellä alaviite 322). Nämä valtuudet kattavat kahdentyyppisiä tietoja: 1) viestintä, jonka toinen osapuoli tai molemmat osapuolet ovat Korean kansalaisia ([327]); ja 2) viestintä, jonka osapuolena on a) Korean tasavallalle vihamielisiä maita, b) vieraiden valtioiden viranomaisia, ryhmiä tai kansalaisia, joiden epäillään osallistuvan Korean vastaiseen toimintaan ([328]), tai c) Korean niemimaalla toimivien ryhmien jäseniä, jotka eivät kuitenkaan ole Korean tasavallan suvereniteetin piirissä, ja niiden ulkomailla toimivia kattoryhmiä ([329]). EU:n yksilöiden viestintää, joka on siirretty unionista Korean tasavaltaan tämän päätöksen perusteella, voidaan sen vuoksi kerätä kansalliseen turvallisuuteen liittyviä tarkoituksia varten viestinnän tietosuojalain nojalla (johdanto-osan (188)–(192) kappaleessa esitettyjen edellytysten täyttyessä) vain jos viestintä tapahtuu EU:n yksilön ja Korean kansalaisen välillä, tai – jos viestintä tapahtuu yksinomaan muiden kuin Korean kansalaisten välillä – se kuuluu johonkin kolmesta edellä mainitusta tyypistä 2 a), b tai c.

(188) Kummassakin tapauksessa televalvontatietoja voidaan kerätä ainoastaan kansalliseen turvallisuuteen kohdistuvien uhkien ehkäisemiseksi ([330]), ja yhteydenpidon rajoittamista koskevia toimenpiteitä voidaan toteuttaa ainoastaan jos on olemassa kansalliseen turvallisuuteen kohdistuva vakava riski ja tietojen kerääminen on välttämätöntä sen ehkäisemiseksi ([331]). Lisäksi pääsy viestinnän sisältöön sallitaan vain viimesijaisena keinona, ja viestinnän yksityisyyden loukkaus on pyrittävä minimoimaan ([332]) sen varmistamiseksi, että se on oikeassa suhteessa tavoiteltuun kansallista turvallisuutta koskevaan tavoitteeseen. Sekä viestinnän sisällön että televalvontatietojen kerääminen saa kestää enintään neljä kuukautta, ja se on lopetettava välittömästi, jos asetettu tavoite saavutetaan aikaisemmin ([333]). Jos asiaankuuluvat edellytykset täyttyvät edelleen, keräämisaikaa voidaan jatkaa enintään neljällä kuukaudella, jos siihen saadaan ennakkohyväksyntä tuomioistuimelta (johdanto-osan (189) kappaleessa kuvattujen toimenpiteiden osalta) tai presidentiltä (johdanto-osan (190) kappaleessa kuvattujen toimenpiteiden osalta) ([334]).

(189) Televalvontatietojen ja viestinnän sisällön keräämiseen sovelletaan samoja menettelyllisiä suojatoimia ([335]). Jos ainakin yksi viestinnän osapuolista on Korean kansalainen, tiedusteluviraston on esitettävä kirjallinen pyyntö ylimmän syyttäjän virastolle, jonka puolestaan on haettava päätöstä ylemmän oikeusasteen tuomioistuimen

([322]) Ks. myös kansallisesta tiedustelupalvelusta annetun lain 14, 22 ja 23 §.
([323]) Kansallisesta tiedustelupalvelusta annetun lain 4 §:n 2 momentti.
([324]) Kansallisesta tiedustelupalvelusta annetun lain 3 §:n 1 momentti, 6 §:n 2 momentti sekä 11 ja 21 §. Ks. myös eturistiriitoja koskevat säännöt, erityisesti kansallisesta tiedustelupalvelusta annetun lain 10 ja 12 §.
([325]) Kansallisesta tiedustelupalvelusta annetun lain 13 §.
([326]) Tämä käsittää tiedusteluvirastot (esim. *National Intelligence Service* ja *Defense Security Support Command*) sekä poliisin/syyttäjänviraston.
([327]) Viestinnän tietosuojalain 7 §:n 1 momentin 1 kohta.
([328]) Kuten Korean hallitus selittää liitteen II alaviitteessä 244, tällä tarkoitetaan toimintaa, joka uhkaa kansakunnan olemassaoloa ja turvallisuutta, demokraattista järjestystä tai kansalaisten elämää ja vapautta.
([329]) Viestinnän tietosuojalain 7 §:n 1 momentin 2 kohta.
([330]) Viestinnän tietosuojalain 13-4 §.
([331]) Viestinnän tietosuojalain 7 §:n 1 momentti.
([332]) Viestinnän tietosuojalain 3 §:n 2 momentti. Lisäksi yhteydenpidon rajoittamista koskevat toimenpiteet on lopetettava heti kun ne eivät enää ole tarpeen, jotta voidaan varmistaa, että yksilön viestintäsalaisuuden loukkaus rajoitetaan mahdollisimman vähään (viestinnän tietosuojalain täytäntöönpanoasetuksen 2 §).
([333]) Viestinnän tietosuojalain 7 §:n 2 momentti.
([334]) Hakemus tarkkailun jatkamista koskevan hyväksynnän saamiseksi on esitettävä kirjallisesti, ja siinä on mainittava syyt, joiden vuoksi pidentämistä haetaan, ja toimitettava näyttöä (viestinnän tietosuojalain 7 §:n 2 momentti ja sen täytäntöönpanoasetuksen 5 §).
([335]) Ks. viestinnän tietosuojalain 13-4 §:n 2 momentti ja sen täytäntöönpanoasetuksen 37 §:n 4 momentti, joiden mukaan viestinnän sisällön keräämiseen sovellettavia menettelyjä sovelletaan myös televalvontatietojen keräämiseen. Ks. myös liitteen II kohta 3.2.1.1.1.

ylemmältä puheenjohtajalta (*senior Chief Justice of the High Court*) ([336]). Viestinnän tietosuojalaissa luetellaan tiedot, jotka on mainittava syyttäjälle esitettävässä pyynnössä, päätöstä koskevassa hakemuksessa ja itse päätöksessä. Näitä ovat erityisesti pyynnön perustelut, tärkeimmät epäilyksien taustalla olevat syyt ja näyttö sekä tiedot ehdotetun toimenpiteen tavoitteesta, kohteesta (eli kohdehenkilö(i)stä, soveltamisalasta ja kestosta) ([337]). Tietoja voidaan kerätä ilman päätöstä vain jos kyseessä on salahankkeeseen liittyvä toiminta, joka uhkaa kansallista turvallisuutta, eikä vallitsevan hätätilanteen vuoksi ole mahdollista noudattaa edellä mainittuja menettelyjä ([338]). Myös tässä tapauksessa päätöstä on kuitenkin haettava välittömästi toimenpiteen toteuttamisen jälkeen ([339]). Siksi viestinnän tietosuojalaissa määritellään selkeästi tämäntyyppisen keräämisen soveltamisala ja edellytykset ja säädetään niihin sovellettavista erityisistä (menettelyllisistä) suojatoimista (myös tuomioistuimen ennakkohyväksynnästä), jotta voidaan varmistaa, että tällaisten toimenpiteiden käyttö rajoitetaan siihen, mikä on välttämätöntä ja oikeasuhteista. Lisäksi vaatimus antaa yksityiskohtaisia tietoja sekä päätöstä koskevassa hakemuksessa että itse päätöksessä sulkee pois mielivaltaisen pääsyn mahdollisuuden.

(190) Kun kyseessä on muiden kuin Korean kansalaisten välinen viestintä, joka kuuluu johonkin johdanto-osan (187) kappaleessa mainituista kolmesta tyypistä, tietojen keräämiseksi on tehtävä hakemus kansallisen tiedustelupalvelun johtajalle, jonka on ehdotettujen toimenpiteiden asianmukaisuuden tarkistamisen jälkeen pyydettävä toimenpiteelle Korean tasavallan presidentin kirjallinen ennakkohyväksyntä ([340]). Tiedusteluviraston hakemuksessa on esitettävä samat yksityiskohtaiset tiedot kuin haettaessa tuomioistuimen päätöstä (ks. johdanto-osan (189) kappale). Näitä ovat erityisesti pyynnön perustelut, tärkeimmät epäilyksien taustalla olevat syyt ja todistusasiakirjat sekä tiedot ehdotettujen toimenpiteiden tavoitteesta, kohteesta (eli kohdehenkilö(i)stä, soveltamisalasta ja kestosta) ([341]). Hätätilanteissa ([342]) on saatava ennakkohyväksyntä ministeriltä, jonka alaisuuteen asianomainen tiedusteluvirasto kuuluu, mutta viraston on pyydettävä presidentin hyväksyntää välittömästi sen jälkeen kun hätätoimenpiteet on toteutettu ([343]). Myös silloin kun kerätään yksinomaan muiden kuin Korean kansalaisten välistä viestintää, viestinnän tietosuojalaissa rajoitetaan tällaisten toimenpiteiden käyttö siihen, mikä on tarpeen ja oikeasuhteista, määrittämällä selkeästi ne rajatut henkilöryhmät, joihin tällaisia toimenpiteitä voidaan soveltaa, ja vahvistamalla yksityiskohtaiset kriteerit, joiden täyttyminen tiedusteluvirastojen on osoitettava tietojen keräämistä koskevan hakemuksen perustelemiseksi. Myös tässä tapauksessa tämä sulkee pois mielivaltaisen pääsyn mahdollisuuden. Tällaisten toimenpiteiden osalta ei edellytetä riippumatonta ennakkohyväksyntää, mutta jälkikäteen tehtävästä riippumattomasta valvonnasta huolehtivat erityisesti tietosuojalautakunta ja ihmisoikeuskomissio (ks. esim. johdanto-osan (199)–(200) kappale).

(191) Viestinnän tietosuojalaissa säädetään lisäksi useista muista suojatoimista, jotka edistävät jälkikäteisvalvontaa ja helpottavat yksilön oikeussuojan saatavuutta. Ensinnäkin viestinnän tietosuojalaissa säädetään erilaisista tietojen kirjaamista ja raportointia koskevista vaatimuksista, joita sovelletaan aina kun mitä tahansa tietoja kerätään kansalliseen turvallisuuteen liittyviä tarkoituksia varten. Erityisesti silloin kun tiedusteluvirastot vaativat yksityisiä palveluntarjoajia tekemään yhteistyötä, niiden on esitettävä tuomioistuimen päätös / presidentin ennakkohyväksyntä tai jäljennös hätätilanteen sensuuria koskevan lausunnon kansilehdestä, joka yhteistyöhön pakotetun yksikön on säilytettävä tiedostoissaan ([344]). Silloin kun yksityiset palveluntarjoajat on velvoitettu yhteistyöhön, sekä

([336]) Viestinnän tietosuojalain 6 §:n 5 ja 8 momentti ja 7 §:n 1 momentin 1 ja 3 kohta yhdessä sen täytäntöönpanoasetuksen 7 §:n 3 ja 4 momentin kanssa.

([337]) Ks. viestinnän tietosuojalain 7 §:n 3 momentti ja 6 §:n 4 momentti (tiedusteluviraston esittämä pyyntö), viestinnän tietosuojalain täytäntöönpanoasetuksen 4 § (syyttäjän esittämä hakemus) ja viestinnän tietosuojalain 7 §:n 3 momentti ja 6 §:n 6 momentti (päätös).

([338]) Viestinnän tietosuojalain 8 §.

([339]) Viestinnän tietosuojalain 8 §:n 2 ja 8 momentti. Tietojen kerääminen on lopetettava välittömästi, jos tuomioistuimen hyväksyntää ei saada 36 tunnin kuluessa siitä kun toimenpiteet on toteutettu. Jos tarkkailu saadaan päätökseen lyhyessä ajassa, niin että tuomioistuimen hyväksyntää ei ole ehditty saada, toimivaltaisen syyttäjänviraston on lähetettävä toimivaltaisen tuomioistuimen puheenjohtajalle tiedusteluviraston laatima ilmoitus hätätilanteen toimenpiteen toteuttamisesta, jotta tämä voi tarkastaa tietojen keräämisen lainmukaisuuden (viestinnän tietosuojalain 8 §:n 5 ja 7 momentti). Ilmoituksessa on annettava tiedot tarkkailun tavoitteesta, kohteesta, soveltamisalasta, kestosta, toteuttamispaikasta ja -tavasta sekä perusteet, joiden vuoksi pyyntöä ei ole esitetty ennen toimenpiteen toteuttamista (viestinnän tietosuojalain 8 §:n 6 momentti). Yleensä ottaen tiedusteluvirastot voivat toteuttaa hätätoimenpiteitä vain ”hätätilanteen sensuuria/kuuntelua koskevan lausunnon” mukaisesti, ja niiden on pidettävä kirjaa tällaisista toimenpiteistä (viestinnän tietosuojalain 8 §:n 4 momentti).

([340]) Viestinnän tietosuojalain täytäntöönpanoasetuksen 8 §:n 1 ja 2 momentti.

([341]) Viestinnän tietosuojalain täytäntöönpanoasetuksen 8 §:n 3 momentti yhdessä lain 6 §:n 4 momentin kanssa.

([342]) Eli silloin kun toimenpiteen kohteena on salahankkeeseen liittyvä toiminta, joka uhkaa kansallista turvallisuutta, eikä ole aikaa pyytää presidentin hyväksyntää, ja hätätoimenpiteiden laiminlyönti voisi vaarantaa kansallisen turvallisuuden (viestinnän tietosuojalain 8 §:n 8 momentti).

([343]) Viestinnän tietosuojalain 8 §:n 9 momentti. Tietojen kerääminen on lopetettava välittömästi, jos hyväksyntää ei saada 36 tunnin kuluessa hakemuksen tekemisestä.

([344]) Viestinnän tietosuojalain 9 §:n 2 momentti ja sen täytäntöönpanoasetuksen 12 §. Ks. viestinnän tietosuojalain 13 §, jossa säädetään mahdollisuudesta velvoittaa postitoimistot ja televiestintäpalvelujen tarjoajat antamaan apua. Yksityiset palveluntarjoajat, joita vaaditaan luovuttamaan tietoja, voivat kieltäytyä siitä, jos päätöksessä/hyväksynnässä tai hätäsensuuria koskevassa lausunnossa viitataan väärään tunnisteeseen (esim. puhelinnumero kuuluu eri henkilölle kuin sille, joka on toimenpiteen kohteena). Palveluntarjoajat eivät missään tapauksessa saa paljastaa viestinnässä käytettyjä salasanoja (viestinnän tietosuojalain 9 §:n 4 momentti).

niiden että yhteistyötä vaativan viranomaisen on kirjattava ylös toimenpiteiden tarkoitus ja kohde sekä niiden täytäntöönpanopäivä ([345]). Tiedusteluvirastojen on lisäksi raportoitava keräämistään tiedoista ja tarkkailun tuloksesta kansallisen tiedustelupalvelun johtajalle ([346]).

(192) Toiseksi yksilöille on ilmoitettava siitä, että heidän tietojaan (sekä televalvontatietoja että viestinnän sisältöä) on kerätty kansalliseen turvallisuuteen liittyviä tarkoituksia varten, jos on kyse viestinnästä, jossa ainakin yksi osapuolista on Korean kansalainen ([347]). Ilmoitus on toimitettava kirjallisesti 30 päivän kuluessa keräämisen päättymisestä (myös silloin kun tiedot on saatu kiireellisen menettelyn mukaisesti), ja sitä voidaan lykätä vain jos ja ainoastaan niin kauan kuin ilmoittaminen vaarantaisi kansallisen turvallisuuden tai vahingoittaisi ihmisten henkeä ja fyysistä turvallisuutta ([348]). Tällaisesta ilmoituksesta riippumatta yksityishenkilöillä on oikeus käyttää erilaisia oikeussuojakeinoja, joita käsitellään lähemmin 3.3.4 kohdassa.

3.3.1.2 Terroristiepäiltyjen tietojen kerääminen

(193) Terrorismintorjuntalain mukaan kansallinen tiedustelupalvelu voi kerätä tietoja terrorismiepäillyistä ([349]) muissa laeissa säädettyjen rajoitusten ja suojatoimien mukaisesti ([350]). Kansallinen tiedustelupalvelu voi hankkia erityisesti viestintätietoja (viestinnän tietosuojalain perusteella) ja muita henkilötietoja (pyytämällä tietojen vapaaehtoista luovuttamista) ([351]). Viestintätietojen (joko viestinnän sisällön tai televalvontatietojen) keräämiseen sovelletaan 3.3.1.1 kohdassa kuvattuja rajoituksia ja suojatoimia, myös vaatimusta tuomioistuimen päätöksen hankkimisesta. Terrorismiepäiltyjen muuntyyppisten henkilötietojen vapaaehtoista luovuttamista koskevien pyyntöjen osalta kansallisen tiedustelupalvelun on noudatettava perustuslakiin ja tietosuojalakiin perustuvia tarpeellisuutta ja oikeasuhteisuutta koskevia vaatimuksia (ks. johdanto-osan (164) kappale) ([352]). Rekisterinpitäjät voivat noudattaa tällaisia pyyntöjä vapaaehtoisesti tietosuojalaissa säädettyjen edellytysten nojalla (esimerkiksi noudattaen tietojen minimointia koskevaa periaatetta ja rajoittamalla vaikutuksia rekisteröidyn yksityisyyteen) ([353]). Siinä tapauksessa niiden on noudatettava myös ilmoituksessa N:o 2021-5 säädettyä vaatimusta ilmoittaa tietojen luovuttamisesta asianomaiselle (ks. johdanto-osan (166) kappale).

([345]) Yhteydenpidon rajoittamista koskevien toimenpiteiden osalta tällaista kirjaa on pidettävä kolmen vuoden ajan, ks. viestinnän tietosuojalain 9 §:n 3 momentti ja sen täytäntöönpanoasetuksen 17 §:n 2 momentti. Televalvontatietojen osalta tiedusteluvirastojen on pidettävä kirjaa siitä, että tällaisia tietoja koskeva pyyntö on esitetty, ja talletettava myös kyseinen kirjallinen pyyntö ja tieto sen esittäneestä instituutiosta (viestinnän tietosuojalain 13 §:n 5 momentti ja 13-4 §:n 3 momentti). Televiestintäpalvelujen tarjoajien on säilytettävä nämä tiedot seitsemän vuoden ajan ja raportoitava tiede- ja tieto- ja viestintätekniikkaministeriölle kahdesti vuodessa siitä, kuinka usein tällaisia tietoja luovutetaan (viestinnän tietosuojalain 9 §:n 3 momentti yhdessä 13 §:n 7 momentin kanssa sekä sen täytäntöönpanoasetuksen 37 §:n 4 momentti ja 39 §).

([346]) Viestinnän tietosuojalain täytäntöönpanoasetuksen 18 §:n 3 momentti.

([347]) Viestinnän tietosuojalain 9-2 §:n 3 momentti ja 13-4 §. Ilmoituksessa on mainittava 1) se, että tietoja on kerätty, 2) täytäntöönpanosta vastaava elin ja 3) täytäntöönpanoaika.

([348]) Viestinnän tietosuojalain 9-2 §:n 4 momentti. Siinä tapauksessa ilmoitus on annettava 30 päivän kuluessa siitä kun lykkäämisen perusteet lakkaavat (ks. viestinnän tietosuojalain 13-4 §:n 2 momentti ja 9-2 §:n 6 momentti.

([349]) Tällä tarkoitetaan terroristiryhmän jäseniä (YK:n määritelmän mukaisesti, ks. terrorismintorjuntalain 2 §:n 2 momentti); henkilöitä, jotka edistävät ja levittävät terroristiryhmän aatteita tai taktiikkaa, keräävät tai myöntävät varoja terrorismin rahoittamiseksi tai osallistuvat muuhun terrorismin valmistelua ja siihen yllyttämistä sekä vehkeilyä ja propagandaa koskevaan toimintaan; tai henkilöitä, joiden voidaan hyvin perustein epäillä harjoittaneen tällaista toimintaa (terrorismintorjuntalain 2 §:n 3 momentti). ”Terrorismilla” tarkoitetaan terrorismintorjuntalain 2 §:n 1 momentissa olevan määritelmän mukaan toimintaa, jonka tarkoituksena on estää valtiota, paikallishallintoa tai ulkomaista hallitusta (myös kansainvälisiä järjestöjä) käyttämästä toimivaltaansa tai pakottaa ne toteuttamaan toimia ilman oikeudellista velvoitetta, tai uhata yleisöä. Tällainen toiminta voi tarkoittaa esimerkiksi henkilön tappamista, sieppaamista tai panttivangiksi ottamista; aluksen tai ilma-aluksen kaappaamista, tuhoamista tai vahingoittamista; biokemiallisten aseiden, räjähteiden tai tuliaseiden käyttöä kuoleman tai vakavan vamman tai vahingon aiheuttamiseksi; ja radioaktiivisten tai ydinaineiden väärinkäyttöä.

([350]) Terrorismintorjuntalain 9 §:n 1 ja 3 momentti.

([351]) Vaikka terrorismintorjuntalaissa viitataan myös mahdollisuuteen kerätä tietoja maahantulosta ja maasta poistumisesta maahanmuuttolain (*Immigration Act*) ja tullilain (*Customs Act*) nojalla, kyseisissä laeissa ei tällä hetkellä säädetä tällaisista valtuuksista (ks. liitteen II kohta 3.2.2.1). Tällaisia valtuuksia ei periaatteessa kuitenkaan sovellettaisi tämän päätöksen perusteella siirrettäviin tietoihin, vaan ne koskisivat Korean viranomaisten suoraan keräämiä tietoja (eikä pääsyä tietoihin, jotka on aiemmin siirretty unionista korealaisille rekisterinpitäjille). Lisäksi terrorismintorjuntalaissa todetaan, että rahoitustoimia koskevien tietojen keräämisessä sovellettava oikeusperusta on rahoitustoimia koskevasta raportoinnista annettu laki. Kyseisen lain nojalla hankittavat tiedot eivät kuitenkaan kuulu tämän päätöksen soveltamisalaan, kuten alaviitteessä 200 todetaan. Terrorismintorjuntalaissa säädetään myös, että kansallinen tiedustelupalvelu voi kerätä paikkatietoja ei-velvoittavien pyyntöjen avulla. Tällöin toimijat voivat luovuttaa paikkatietoja vapaaehtoisesti tietosuojalaissa säädetyin edellytyksin (ks. johdanto-osan (193) kappale ja paikkatiedoista annettu laki (*Location Information Act*)). Kuten myös alaviitteessä 17 todetaan, paikkatietoja ei siirrettäisi unionista korealaisille rekisterinpitäjille tämän päätöksen perusteella, vaan ne pikemminkin tuotettaisiin Koreassa.

([352]) Ks. liitteen II kohta 3.2.2.2.

([353]) Ks. tietosuojalain 58 §:n 4 momentti, jossa edellytetään, että henkilötietoja on käsiteltävä vain sen verran kuin on tarpeen aiotun tarkoituksen saavuttamiseksi, ja 3 §:n 6 momentti, jonka mukaan henkilötietoja on käsiteltävä siten, että voidaan minimoida yksilön yksityisyyden loukkaamisen mahdollisuus. Ks. myös tietosuojalain 59 §:n 2 ja 3 kohta, joiden mukaan rekisterinpitäjät eivät saa luovuttaa henkilötietoja kolmansille osapuolille ilman lupaa.

3.3.1.3 Tilaajatietojen vapaaehtoista luovuttamista koskevat pyynnöt

(194) Televiestintäyrityksiä koskevan lain mukaan televiestintäpalvelujen tarjoajat voivat luovuttaa tilaajatietoja vapaaehtoisesti (ks. johdanto-osan (163) kappale), jos jokin tiedusteluvirasto pyytää niitä kansalliseen turvallisuuteen kohdistuvan uhkan estämiseksi ([354]). Kun kansallinen tiedustelupalvelu esittää tällaisia pyyntöjä, sovelletaan samoja (perustuslakiin, tietosuojalakiin ja televiestintäyrityksiä koskevaan lakiin perustuvia) rajoituksia kuin lainvalvonnan alalla, ks. johdanto-osan (164) kappale ([355]). Televiestintäpalvelujen tarjoajien ei tarvitse noudattaa tällaisia pyyntöjä, ja ne voivat noudattaa niitä vain tietosuojalaissa säädetyin edellytyksin (esimerkiksi noudattaen tietojen minimointia koskevaa periaatetta ja rajoittamalla vaikutuksia rekisteröidyn yksityisyyteen, ks. myös johdanto-osa (193) kappale). Kirjanpidon ja asianomaiselle toimitettavan ilmoituksen osalta sovelletaan samoja vaatimuksia kuin lainvalvonnan alalla (ks. johdanto-osan (165) ja (166) kappale).

3.3.2 *Kerättyjen tietojen myöhempi käyttö*

(195) Korean viranomaisten kansalliseen turvallisuuteen liittyviä tarkoituksia varten keräämien henkilötietojen käsittelyyn sovelletaan tietosuojalaissa vahvistettuja periaatteita, jotka koskevat käyttötarkoituksen rajoittamista (3 §:n 1–2 momentti), käsittelyn lainmukaisuutta ja asianmukaisuutta (3 §:n 1 momentti), tietojen oikeasuhteisuutta/minimointia (3 §:n 1 ja 6 momentti ja 58 §), tietojen täsmällisyyttä (3 §:n 3 momentti), läpinäkyvyyttä (3 §:n 5 momentti) sekä turvallisuutta (58 §:n 4 momentti) ja säilytysajan rajoittamista (58 §:n 4 momentti) ([356]). Henkilötietoja voidaan luovuttaa kolmansille osapuolille (mukaan lukien kolmansiin maihin) ainoastaan jos noudatetaan näitä periaatteita (ja erityisesti käyttötarkoituksen rajoittamista ja tietojen minimointia), sen jälkeen kun on arvioitu tarpeellisuus- ja suhteellisuusperiaatteiden noudattaminen (perustuslain 37 §:n 2 momentti) ja otettu huomioon luovuttamisen vaikutus asianomaisten henkilöiden oikeuksiin (tietosuojalain 3 §:n 6 momentti).

(196) Viestinnän sisällön ja televalvontatietojen käyttöä rajoitetaan viestinnän tietosuojalaissa sallimalla kyseisten tietojen käyttö ainoastaan oikeudenkäyntimenettelyissä, jos viestintään liittyvä osapuoli vetoaa niihin vahingonkorvausvaatimuksessaan; käyttö voidaan sallia myös muiden lakien nojalla ([357]).

3.3.3 *Valvonta*

(197) Kansallisten turvallisuusviranomaisten toimintaa valvovat Koreassa useat eri elimet ([358]).

(198) Ensinnäkin terrorismintorjuntalaissa säädetään erityisistä terrorismintorjuntatoimien valvontamekanismista, joka koskee myös terrorismiepäiltyjen tietojen keräämistä. Johdon tasolla terrorismintorjuntatoimia valvoo terrorismintorjuntakomissio (*Counterterrorism Commission*) ([359]), jolle kansallisen tiedustelupalvelun johtajan on raportoitava terrorismiepäiltyjä koskevista tutkimuksista ja jäljitystoimista, joiden avulla kerätään terrorismintorjunnassa tarvittavaa tietoa tai aineistoa ([360]). Lisäksi ihmisoikeusvaltuutettu (*Human Rights Protection Officer*) valvoo erikseen, että terrorismintorjuntatoimissa noudatetaan perusoikeuksia ([361]). Terrorismintorjuntakomission puheenjohtaja nimittää ihmisoikeusvaltuutetun sellaisten henkilöiden joukosta, jotka täyttävät terrorismintorjuntalain täytäntöönpanoasetuksessa luetellut vaatimukset ([362]). Ihmisoikeusvaltuutetun toimikausi on kaksivuotinen, ja hänet voidaan erottaa tehtävistään vain erityisistä rajoitetuista ja hyvin perustelluista syistä ([363]). Ihmisoikeusvaltuutettu

([354]) Televiestintäyrityksiä koskevan lain 83 §:n 3 momentti.
([355]) Ks. myös liitteen II kohta 3.2.3.
([356]) Ks. liitteen II kohta 1.2.
([357]) Viestinnän tietosuojalain 5 §:n 1 ja 2 momentti, 12 § ja 13-5 §.
([358]) Ks. liitteen II kohta 3.3.
([359]) Terrorismintorjuntalain 5 §:n 3 momentti. Komission puheenjohtajana toimii pääministeri, ja siihen kuuluu useita ministereitä ja valtion virastojen johtajia, mm. ulkoministeri, oikeusministeri, puolustusministeri, sisäasiain- ja turvallisuusministeri, kansallisen tiedustelupalvelun johtaja ja kansallisen poliisiviraston päällikkö (terrorismintorjuntalain täytäntöönpanoasetuksen 3 §:n 1 momentti).
([360]) Terrorismintorjuntalain 9 §:n 4 momentti.
([361]) Terrorismintorjuntalain 7 §.
([362]) Edellytyksenä on vähintään 10 vuoden kokemus asianajajan tehtävistä tai asiantuntemus ihmisoikeusalalta ja vähintään 10 vuoden työskentely apulaisprofessorina tai ylemmässä tehtävässä tai ylempänä virkamiehenä valtion tai paikallishallinnon virastossa, tai vähintään 10 vuoden työkokemus ihmisoikeusalalta esimerkiksi valtiosta riippumattomassa järjestössä (terrorismintorjuntalain täytäntöönpanoasetuksen 7 §:n 1 momentti).
([363]) Esimerkiksi jos häntä vastaan on nostettu syyte hänen tehtäviinsä liittyvässä rikosasiassa luottamuksellisten tietojen paljastamisen vuoksi, tai pitkäaikaisen fyysisen tai psyykkisen toimintakyvyttömyyden vuoksi (terrorismintorjuntalain täytäntöönpanoasetuksen 7 §:n 3 momentti).

voi valvontatehtäväänsä hoitaessaan antaa yleisiä suosituksia ihmisoikeuksien suojelun parantamiseksi ([364]) ja erityisiä suosituksia korjaaviksi toimenpiteiksi, jos on todettu ihmisoikeusloukkaus ([365]). Viranomaisten on ilmoitettava ihmisoikeusvaltuutetulle sen suositusten perusteella toteutetuista jatkotoimista ([366]).

(199) Toiseksi myös tietosuojalautakunta valvoo, että kansalliset turvallisuusviranomaiset noudattavat tietosuojasääntöjä. Tämä tarkoittaa sekä sovellettavia tietosuojalain säännöksiä (ks. johdanto-osan (149) kappale) että henkilötietojen keräämiseen muiden lakien nojalla sovellettavia rajoituksia ja suojatoimia (viestinnän tietosuojalaki, terrorismintorjuntalaki ja televiestintäyrityksiä koskeva laki, ks. myös johdanto-osan (171) kappale) ([367]). Tätä valvontatehtävää suorittaessaan tietosuojalautakunta voi käyttää kaikkia tutkintavaltuuksiaan ja määrätä korjaavia toimia, joita käsitellään lähemmin 2.4.2 kohdassa.

(200) Kolmanneksi kansallisten turvallisuusviranomaisten toimintaan sovelletaan kansallisen ihmisoikeuskomission riippumatonta valvontaa johdanto-osan (172) kappaleessa kuvattujen menettelyjen mukaisesti ([368]).

(201) Neljänneksi valtion tilintarkastus- ja valvontaviranomaisen valvontatehtävä kattaa myös kansalliset turvallisuusviranomaiset, joskin kansallinen tiedustelupalvelu voi poikkeustapauksissa kieltäytyä antamasta määrättyjä tietoja tai aineistoja, esimerkiksi jos kyseessä on valtionsalaisuus, jonka julkistaminen aiheuttaisi kansalliselle turvallisuudelle vakavia seurauksia ([369]).

(202) Lopuksi todettakoon, että kansallisen tiedustelupalvelun toiminnan parlamentaarisesta valvonnasta vastaa kansalliskokous (erityisen tiedustelukomitean kautta) ([370]). Viestinnän tietosuojalaissa säädetään kansalliskokouksen erityisestä valvontatehtävästä, joka koskee yhteydenpidon rajoittamista koskevien toimenpiteiden käyttöä kansalliseen turvallisuuteen liittyviä tarkoituksia varten ([371]). Kansalliskokous voi erityisesti suorittaa salakuuntelulaitteiden tarkastuksia paikalla ja vaatia sekä kansallista tiedustelupalvelua että viestinnän sisältöä paljastaneita televiestintäpalvelujen tarjoajia antamaan asiasta selvityksen. Kansalliskokous voi myös harjoittaa yleistä valvontatehtäväänsä (johdanto-osan (174) kappaleessa kuvattujen menettelyjen mukaisesti). Kansallisesta tiedustelupalvelusta annetun lain mukaan tiedustelupalvelun johtajan on vastattava viipymättä, jos tiedustelukomitea pyytää raporttia jostakin tietystä asiasta ([372]). Tiettyjen erityisen arkaluonteisten tietojen käsittelystä on annettu erityiset säännöt. Käytännössä tiedustelupalvelun johtaja voi kieltäytyä vastaamasta tai todistamasta komitean edessä vain poikkeustapauksessa, eli jos pyyntö koskee sotilaallisia, diplomaattisia tai Pohjois-Koreaan liittyviä valtionsalaisuuksia, joiden julkistaminen voisi aiheuttaa vakavia seurauksia maan ”kansalliselle kohtalolle” ([373]). Tässä tapauksessa tiedustelukomitea voi pyytää selitystä pääministeriltä, ja jos sitä ei anneta 7 päivän kuluessa, vastaamisesta tai todistamisesta ei voida kieltäytyä.

3.3.4 *Oikeussuojakeinot*

(203) Korean järjestelmä tarjoaa myös kansallisen turvallisuuden alalla erilaisia (oikeudellisia) keinoja, joiden avulla yksilöt voivat saada apua ongelmatilanteisiin, myös mahdollisuuden saada vahingonkorvausta. Nämä mekanismit tarjoavat rekisteröidyille tehokkaat hallinnolliset ja oikeudelliset oikeussuojakeinot, joiden avulla he voivat erityisesti varmistaa oikeuksiensa toteutumisen; tämä koskee myös oikeutta saada pääsy henkilötietoihin ja oikaista tai poistaa ne.

(204) Ensinnäkin yksilöt voivat tietosuojalain 3 §:n 5 momentin ja 4 §:n 1, 3 ja 4 momentin nojalla käyttää oikeuttaan saada pääsy omiin tietoihinsa ja oikaista tai poistaa ne tai keskeyttää niiden käsittelyn myös suhteessa kansallisiin turvallisuusviranomaisiin. Ilmoituksessa N:o 2021-5 olevassa 6 kohdassa (liite I) selitetään tarkemmin, miten näitä oikeuksia sovelletaan, kun tietoja käsitellään kansalliseen turvallisuuteen liittyviä tarkoituksia varten. Kansallinen turvallisuusviranomainen voi muun muassa rajoittaa näiden oikeuksien käyttöä tai evätä sen vain siltä osin ja niin pitkäksi aikaa kuin se on tarpeen ja oikeasuhteista yleisen edun mukaisen tärkeän tavoitteen

([364]) Terrorismintorjuntalain täytäntöönpanoasetuksen 8 §:n 1 momentti.
([365]) Terrorismintorjuntalain täytäntöönpanoasetuksen 9 §:n 1 momentti. Ihmisoikeusvaltuutettu päättää suositusten antamisesta itsenäisesti, mutta hänen on raportoitava suosituksista terrorismintorjuntakomission puheenjohtajalle.
([366]) Terrorismintorjuntalain täytäntöönpanoasetuksen 9 §:n 2 momentti. Korean hallituksen virallisten lausuntojen mukaan ihmisoikeusvaltuutetun suositusten noudattamatta jättäminen vietäisiin terrorismintorjuntakomission ja siten pääministerin käsiteltäväksi. Toistaiseksi ei kuitenkaan ole ollut tapauksia, joissa ihmisoikeusvaltuutetun suosituksia ei olisi pantu täytäntöön (ks. liitteen II kohta 3.3.1).
([367]) Liitteen II kohta 3.3.4.
([368]) Ihmisoikeuskomissio on tutkinut viran puolesta erityisesti kansallisen tiedustelupalvelun toimintaa ja käsitellyt useita yksilövalituksia. Ks. esim. ihmisoikeuskomission vuosikertomus 2018, s. 128 (saatavilla osoitteessa https://www.humanrights.go.kr/site/program/board/basicboard/view?menuid=002003003001&pagesize=10&boardtypeid=7017&boardid=7604746) ja vuosikertomus 2019, s. 70 (saatavilla osoitteessahttps://www.humanrights.go.kr/site/program/board/basicboard/view?menuid=002003003001&pagesize=10&boardtypeid=7017&boardid=7606217).
([369]) Kansallisesta tiedustelupalvelusta annetun lain 13 §:n 1 momentti.
([370]) Kansalliskokouksesta annetun lain 36 § ja 37 §:n 1 momentin 15 kohta.
([371]) Viestinnän tietosuojalain 15 §.
([372]) Kansallisesta tiedustelupalvelusta annetun lain 15 §:n 2 momentti.
([373]) Kansallisesta tiedustelupalvelusta annetun lain 17 §:n 2 momentti. ”Valtionsalaisuuksilla” tarkoitetaan (turvaluokiteltuja) tosiseikkoja, tavaroita tai tietoa, joita ei saa luovuttaa millekään toiselle valtiolle tai organisaatiolle, jotta voidaan välttää kansalliseen turvallisuuteen kohdistuvat vakavat haitat, ja jotka ovat saatavilla vain rajoitetusti. Ks. kansallisesta tiedustelupalvelusta annetun lain 13 §:n 4 momentti.

suojelemiseksi (esimerkiksi siltä osin ja niin kauan kuin oikeuden myöntäminen vaarantaisi meneillään olevan tutkinnan tai uhkaisi kansallista turvallisuutta), tai kun oikeuden myöntäminen voisi vahingoittaa kolmannen osapuolen henkeä tai terveyttä. Tällaiseen rajoitukseen vetoaminen edellyttää sen vuoksi yksilön oikeuksien ja etujen tasapainottamista asiaa koskevan yleisen edun kanssa eikä se saa missään tapauksessa vaikuttaa oikeuden olennaiseen sisältöön (perustuslain 37 §:n 2 momentti). Jos pyyntö evätään tai sitä rajoitetaan, yksilölle on ilmoitettava syyt siihen viipymättä.

(205) Toiseksi yksilöt voivat käyttää erilaisia tietosuojalaissa säädettyjä oikeussuojakeinoja, jos jokin kansallinen turvallisuusviranomainen on käsitellyt heidän tietojaan tietosuojalain tai muissa laeissa henkilötietojen keräämiselle asetettujen rajoitusten ja suojatoimien vastaisesti (erityisesti viestinnän tietosuojalaki, ks. johdanto-osan (171) kappale) ([374]). Tätä oikeutta voidaan käyttää tekemällä valitus tietosuojalautakunnalle (esimerkiksi Korean internet- ja turvallisuusviraston ylläpitämän Privacy Call Centre -puhelinpalvelun kautta) ([375]). Jotta voitaisiin helpottaa oikeussuojan saatavuutta Korean kansallisia turvallisuusviranomaisia vastaan, EU:n yksilöt voivat tehdä valituksen Korean tietosuojalautakunnalle oman kansallisen tietosuojaviranomaisensa välityksellä ([376]). Siinä tapauksessa tietosuojalautakunta ilmoittaa yksilölle kansallisen tietosuojaviranomaisen välityksellä, kun tutkimus on päättynyt (ja mahdollisesti määrätyistä korjaavista toimenpiteistä). Hallinnollisista riita-asioista annetun lain nojalla on myös mahdollista hakea muutosta/oikaisua tietosuojalautakunnan päätökseen tai sen toimimatta jättämisen (ks. johdanto-osan (132) kappale).

(206) Kolmanneksi yksilöt voivat tehdä valituksen ihmisoikeusvaltuutetulle, jos he katsovat, että heidän oikeuttaan yksityisyyteen/tietosuojaan on loukattu terrorismintorjuntaan liittyvän toiminnan yhteydessä, (esimerkiksi terrorismintorjuntalain nojalla) ([377]). Ihmisoikeusvaltuutettu voi suosittaa korjaavia toimenpiteitä. Ihmisoikeusvaltuutettu käsittelee kaikki saamansa valitukset, vaikka valittaja ei pystyisi osoittamaan, että hänen oikeuksiaan todella on loukattu (esimerkiksi siksi, että kansallinen turvallisuusviranomainen on väitetysti kerännyt hänen tietojaan lainvastaisesti) ([378]). Kyseisen viranomaisen on ilmoitettava ihmisoikeusvaltuutetulle kaikista sen suositusten noudattamiseksi toteutetuista toimenpiteistä.

(207) Neljänneksi yksilöt voivat tehdä valituksen kansalliselle ihmisoikeuskomissiolle siitä, että kansalliset turvallisuusviranomaiset ovat keränneet heidän tietojaan, ja saada oikeussuojaa johdanto-osan (178) kappaleessa kuvatun menettelyn mukaisesti ([379]).

(208) Yksilöillä on käytettävissään erilaisia keinoja vedota tuomioistuimissa ([380]) 3.3.1 kohdassa kuvattuihin rajoituksiin ja suojatoimiin oikeussuojan saamiseksi. He voivat erityisesti riitauttaa kansallisten turvallisuusviranomaisten toiminnan lainmukaisuuden hallinnollisista riita-asioista annetun lain nojalla (johdanto-osan (181) kappaleessa kuvatun menettelyn tai perustuslakituomioistuimesta annetun lain mukaisesti (ks. johdanto-osan (182) kappale). He voivat myös saada vahingonkorvausta valtion korvauksista annetun lain perusteella (ks. lähemmin johdanto-osan (183) kappale).

4. PÄÄTELMÄT

(209) Komissio katsoo, että Korean tasavalta varmistaa – tietosuojalain, tietyillä sektoreilla sovellettavien erityissääntöjen (ks. analyysi 2 kohdassa) ja ilmoituksessa N:o 2021-5 (liite I) esitettyjen täydentävien suojatoimien ansiosta – Euroopan unionista siirrettyjen henkilötietojen suojan tason, joka vastaa olennaisilta osiltaan asetuksessa (EU) 2016/679 taattua suojan tasoa.

(210) Lisäksi komissio katsoo, että Korean lainsäädäntöön sisältyvät valvontamekanismit ja oikeussuojakeinot kokonaisuutena mahdollistavat sen, että Korean rekisterinpitäjien tekemät tietosuojasääntöjen rikkomiset voidaan tunnistaa ja niihin voidaan puuttua käytännössä, ja että ne myös tarjoavat rekisteröidylle oikeussuojakeinoja, joiden avulla hän voi saada pääsyn itseään koskeviin henkilötietoihin ja tarvittaessa oikaista tai poistaa ne.

([374]) Tietosuojalain 58 §:n 4 momentti ja 4 §:n 5 momentti. Ks. liitteen II kohta 3.4.2.
([375]) Tietosuojalain 62 § ja 63 §:n 2 momentti.
([376]) Ilmoitus N:o 2021-5, 6 kohta (liite I).
([377]) Terrorismintorjuntalain täytäntöönpanoasetuksen 8 §:n 1 momentin 2 kohta.
([378]) Ks. liitteen II kohta 3.4.1.
([379]) Ihmisoikeuskomissio saa säännöllisesti kansallista tiedustelupalvelua koskevia valituksia, ks. vuosikertomuksessa 2019 esitetyt luvut vuosina 2015–2019 vastaanotetuista valituksista, s. 70 (saatavilla osoitteessa https://www.humanrights.go.kr/site/program/board/basicboard/view?menuid=002003003001&pagesize=10&boardtypeid=7017&boardid=7606217).
([380]) Ks. liitteen II kohta 3.4.4.

(211) Korean oikeusjärjestystä koskevien käytettävissä olevien tietojen perusteella, mukaan lukien liitteessä II esitetyt Korean hallituksen lausunnot, vakuutukset ja sitoumukset, komissio katsoo, että Korean viranomaisten yleisen edun nimissä toteuttama puuttuminen erityisesti rikoslain valvontaan ja kansalliseen turvallisuuteen liittyvissä tarkoituksissa niiden yksilöiden perusoikeuksiin, joiden henkilötietoja siirretään Euroopan unionista Korean tasavaltaan, tulee rajatuksi siihen, mikä on ehdottoman välttämätöntä kyseessä olevan lainmukaisen tavoitteen saavuttamiseksi, ja että tällaista puuttumista vastaan on olemassa tehokas oikeussuoja.

(212) Sen vuoksi olisi tämän päätöksen päätelmien perusteella katsottava, että Korean tasavalta varmistaa asetuksen (EU) 2016/679 45 artiklassa tarkoitetun riittävän tietosuojan tason, sellaisena kuin sitä tulkitaan Euroopan unionin perusoikeuskirjan valossa, niille henkilötiedoille, joita siirretään Euroopan unionista Korean tietosuojalain soveltamisalaan kuuluville Korean tasavallan rekisterinpitäjille, lukuun ottamatta uskonnollisia organisaatioita siltä osin kuin ne käsittelevät henkilötietoja lähetystyöhön liittyviä tarkoituksia varten; poliittisia puolueita siltä osin kuin ne käsittelevät henkilötietoja ehdokasasettelua varten, ja rekisterinpitäjiä, jotka kuuluvat luottorekisterilain nojalla tehtävän henkilötietojen käsittelyn osalta rahoituspalvelukomission valvonnan piiriin, siltä osin kuin ne käsittelevät tällaisia tietoja.

5. TÄMÄN PÄÄTÖKSEN VAIKUTUKSET JA TIETOSUOJAVIRANOMAISTEN TOIMET

(213) Jäsenvaltioiden ja niiden elinten on toteutettava tarvittavat toimenpiteet unionin toimielinten antamien säädösten noudattamiseksi, sillä niiden oletetaan olevan lainmukaisia ja aiheuttavan siten oikeusvaikutuksia siihen asti, että ne perutaan, kumotaan kumoamiskanteen johdosta tai julistetaan pätemättömiksi ennakkoratkaisupyynnön tai lainvastaisuusväitteen perusteella.

(214) Näin ollen asetuksen (EU) 2016/679 45 artiklan 3 kohdan mukainen tietosuojan riittävyyttä koskeva komission päätös sitoo kaikkia elimiä jäsenvaltioissa, joille se on osoitettu, mukaan lukien niiden riippumattomat valvontaviranomaiset. Tällä päätöksellä mahdollistetaan erityisesti se, että tiedonsiirrot unionin rekisterinpitäjältä tai henkilötietojen käsittelijältä Korean tasavaltaan sijoittautuneille henkilötietojen käsittelijöille voidaan toteuttaa ilman eri hyväksyntää.

(215) Olisi kuitenkin muistettava, kuten asetuksen (EU) 2016/679 58 artiklan 5 kohdassa ja unionin tuomioistuimen asiassa Schrems antamassa tuomiossa ([381]) todetaan, että jos kansallinen tietosuojaviranomainen esimerkiksi valituksen käsittelyn yhteydessä asettaa kyseenalaiseksi sen, onko tietosuojan riittävyyttä koskeva komission päätös yksityisyydensuojaa ja tietosuojaa koskevan perusoikeuden mukainen, kansallisessa lainsäädännössä on säädettävä oikeussuojakeinoista, joiden avulla viranomainen voi esittää väitteensä kansallisessa tuomioistuimessa, jonka on tarvittaessa pyydettävä unionin tuomioistuimelta ennakkoratkaisua ([382]).

6. TÄMÄN PÄÄTÖKSEN SEURANTA JA TARKASTELU

(216) Tuomioistuimen oikeuskäytännön ([383]) mukaisesti ja kuten asetuksen (EU) 2016/679 45 artiklan 4 kohdassa todetaan, komission olisi tietosuojan riittävyyttä koskevan päätöksen hyväksymisen jälkeen jatkuvasti seurattava asiaa koskevaa kehitystä kolmannessa maassa. Näin komissio voi arvioida sitä, takaako kyseinen kolmas maa edelleen olennaisilta osin vastaavan suojan tason. Tällainen tarkastelu on joka tapauksessa tehtävä, kun komissio saa tietoja, jotka aiheuttavat perusteltuja epäilyksiä tältä osin.

(217) Komission olisi sen vuoksi seurattava jatkuvasti sitä, kuinka henkilötietojen käsittelyä koskeva lainsäädäntökehys ja käytännön toiminta, joita tässä päätöksessä arvioidaan, kehittyvät Korean tasavallassa, sekä sitä, noudattavatko Korean viranomaiset liitteeseen II sisältyviä lausuntoja, vakuutuksia ja sitoumuksia. Prosessin helpottamiseksi Korean viranomaisia kehotetaan ilmoittamaan viipymättä komissiolle kehityksestä, jolla on merkitystä tämän päätöksen kannalta ja joka koskee sitä, miten toiminnanharjoittajat ja viranomaiset käsittelevät henkilötietoja, ja sitä, mitä rajoituksia ja suojatoimia on asetettu viranomaisten pääsylle tietoihin.

([381]) Tuomio asiassa Schrems, 65 kohta.

([382]) Tuomio asiassa Schrems, 65 kohta. "Tässä yhteydessä kansallisen lainsäätäjän asiana on säätää oikeussuojakeinoista, joiden avulla asianomainen kansallinen valvontaviranomainen voi esittää perusteltuina pitämänsä perusteet kansallisissa tuomioistuimissa, jotta nämä voisivat, mikäli ne kyseisen viranomaisen tavoin epäilevät komission päätöksen pätevyyttä, pyytää ennakkoratkaisua päätöksen pätevyyden tutkimiseksi."

([383]) Tuomio asiassa Schrems, 76 kohta.

(218) Jotta komissio voisi harjoittaa tehokkaasti seurantatehtäväänsä, jäsenvaltioiden olisi lisäksi ilmoitettava komissiolle kaikista kansallisten tietosuojaviranomaisten toteuttamista asiaankuuluvista toimista, varsinkin siinä tapauksessa, että ne liittyvät EU:n rekisteröityjen esittämiin kysymyksiin tai valituksiin, jotka koskevat henkilötietojen siirtoa Euroopan unionista Korean tasavallan rekisterinpitäjille. Komissiolle olisi myös ilmoitettava havainnoista, joiden mukaan rikosten ehkäisystä, tutkinnasta, havaitsemisesta tai rikoksiin liittyvistä syytetoimista tai kansallisesta turvallisuudesta vastaavat Korean viranomaiset, mukaan lukien valvontaelimet, eivät varmista vaadittua suojan tasoa.

(219) Asetuksen (EU) 2016/679 45 artiklan 3 kohdan mukaisesti ([384]) ja ottaen huomioon sen, että Korean oikeusjärjestyksen tarjoaman suojan taso voi muuttua, komission olisi tämän päätöksen hyväksymisen jälkeen säännöllisin väliajoin tarkistettava, ovatko Korean tasavallan takaaman suojan tason riittävyyttä koskevat päätelmät edelleen asiasisällöltään ja oikeudellisesti perusteltuja.

(220) Sen vuoksi tätä päätöstä koskeva tarkastelu olisi tehtävä ensimmäisen kerran kolmen vuoden kuluessa sen voimaantulosta. Ensimmäisen tarkastelun jälkeen ja sen tuloksista riippuen komissio päättää tiiviissä yhteistyössä asetuksen (EU) 2016/679 93 artiklan 1 kohdan nojalla perustetun komitean kanssa siitä, onko kolmen vuoden jakso pidettävä voimassa. Myöhemmät tarkastelut olisi joka tapauksessa suoritettava vähintään joka neljäs vuosi ([385]). Tarkastelun olisi katettava kaikki tämän päätöksen toimivuuteen liittyvät näkökohdat ja erityisesti tämän päätöksen liitteessä I esitettyjen täydentävien suojatoimien soveltaminen, kiinnittäen erityistä huomiota suojatoimiin edelleen siirtämisen yhteydessä; asiaa koskevan oikeuskäytännön kehitys; säännöt pseudonymisoitujen tietojen käsittelystä tilastointia, tieteellistä tutkimusta ja yleisen edun mukaista arkistointia varten sekä tietosuojalain 28 §:n 7 momentissa säädettyjen poikkeusten soveltaminen; yksilön oikeuksien käytön tehokkuus, myös ennen äskettäistä tietosuojalautakunnan uudistamista, sekä näitä oikeuksia koskevien poikkeusten soveltaminen; tietosuojalaissa säädettyjen osittaisten vapautusten soveltaminen; sekä viranomaisten pääsyä tietoihin koskevat rajoitukset ja suojatoimet (ks. tämän päätöksen liite II), mukaan lukien yksilöiden tekemiä valituksia koskeva tietosuojalautakunnan yhteistyö EU:n tietosuojaviranomaisten kanssa. Tarkastelun tulisi kattaa myös valvonnan ja täytäntöönpanon tehokkuus sekä tietosuojalain osalta että rikoslain noudattamisen valvonnan ja kansallisen turvallisuuden alalla (erityisesti tietosuojalautakunnan ja kansallisen ihmisoikeuskomission toiminta).

(221) Tarkastelun suorittamiseksi komission olisi järjestettävä tietosuojalautakunnan kanssa kokous, johon osallistuisivat tarvittaessa muut Korean viranomaiset, jotka vastaavat viranomaisten pääsystä tietoihin, sekä asiaankuuluvat valvontaelimet. Euroopan tietosuojaneuvoston jäsenten edustajien olisi voitava osallistua kokoukseen. Tarkastelun yhteydessä komission olisi pyydettävä tietosuojalautakuntaa antamaan kattavat tiedot kaikista tietosuojan riittävyyttä koskevan päätelmän kannalta merkityksellisistä seikoista, mukaan lukien rajoituksista ja suojatoimista, jotka koskevat viranomaisten pääsyä tietoihin ([386]). Komission olisi myös pyydettävä selvityksiä kaikista sille toimitetuista tämän päätöksen kannalta merkityksellisistä tiedoista, mukaan lukien Korean viranomaisten tai muiden Koreassa olevien sidosryhmien, Euroopan tietosuojaneuvoston, yksittäisten tietosuojaviranomaisten, kansalaisyhteiskunnan ryhmien, tiedotusvälineiden tai muiden saatavilla olevien tietolähteiden julkiset raportit.

(222) Komission olisi laadittava tarkastelun perusteella julkinen kertomus, joka toimitetaan Euroopan parlamentille ja neuvostolle.

7. TÄMÄN PÄÄTÖKSEN SOVELTAMISEN KESKEYTTÄMINEN TAI PÄÄTÖKSEN KUMOAMINEN TAI MUUTTAMINEN

(223) Jos käytettävissä olevat tiedot, erityisesti tämän päätöksen seurannasta saatavat tiedot tai Korean tai jäsenvaltioiden viranomaisten toimittamat tiedot, osoittavat, että Korean tasavallan takaama tietosuojan taso ei mahdollisesti ole enää riittävä, komission olisi ilmoitettava viipymättä asiasta Korean toimivaltaisille viranomaisille ja vaadittava asianmukaisten toimenpiteiden toteuttamista tietyn kohtuullisen ajan kuluessa.

(224) Jos Korean toimivaltaiset viranomaiset eivät kyseisen määräajan päättyessä ole toteuttaneet näitä toimenpiteitä tai muutoin osoittaneet tyydyttävästi, että tämän päätöksen perustana on edelleen riittävä suojan taso, komissio aloittaa asetuksen (EU) 2016/679 93 artiklan 2 kohdassa tarkoitetun menettelyn tämän päätöksen soveltamisen keskeyttämiseksi tai sen kumoamiseksi osittain tai kokonaan.

(225) Vaihtoehtoisesti komissio aloittaa kyseisen menettelyn tämän päätöksen muuttamiseksi erityisesti soveltamalla tiedonsiirtoihin lisäehtoja tai rajoittamalla tietosuojan riittävyyttä koskevan päätelmän soveltamisalan vain sellaisiin tiedonsiirtoihin, joiden osalta riittävän tietosuojan jatkuvuus on varmistettu.

([384]) Asetuksen (EU) 2016/679 45 artiklan 3 kohdan mukaisesti ”täytäntöönpanosäädöksessä on säädettävä […] määräaikaistarkastelusta, jossa on otettava huomioon kaikki asiaan liittyvä kehitys kyseisessä kolmannessa maassa tai kansainvälisessä järjestössä.”

([385]) Asetuksen (EU) 2016/679 45 artiklan 3 kohdassa säädetään, että määräaikaistarkastelu on suoritettava vähintään joka neljäs vuosi. Ks. myös Euroopan tietosuojaneuvosto: *Tietosuojan riittävyyden viitearvot*, WP 254 rev. 01.

([386]) Ks. tämän päätöksen liite II.

(226) Komission olisi aloitettava keskeyttämis- tai kumoamismenettely erityisesti jos on viitteitä siitä, että tämän päätöksen nojalla henkilötietoja vastaanottavat toiminnanharjoittajat eivät noudata liitteessä I esitettyjä täydentäviä suojatoimia ja/tai että niitä ei ole pantu tehokkaasti täytäntöön tai että Korean viranomaiset eivät noudata tämän päätöksen liitteessä II olevia lausuntoja, vakuutuksia ja sitoumuksia.

(227) Komission olisi myös harkittava menettelyn aloittamista tämän päätöksen muuttamiseksi, sen soveltamisen keskeyttämiseksi tai sen kumoamiseksi, jos Korean toimivaltaiset viranomaiset eivät tarkastelun yhteydessä tai muutoin toimita tietoja tai selvityksiä, joita tarvitaan arvioitaessa Euroopan unionista Korean tasavaltaan siirrettyjen henkilötietojen suojan tasoa tai tämän päätöksen noudattamista. Tässä suhteessa komission olisi otettava huomioon se, missä määrin asiaa koskevia tietoja voidaan saada muista lähteistä.

(228) Asianmukaisesti perustelluissa kiireellisissä tapauksissa komissio käyttää mahdollisuutta hyväksyä asetuksen (EU) 2016/679 93 artiklan 3 kohdassa tarkoitettua menettelyä noudattaen välittömästi sovellettavia täytäntöönpanosäädöksiä tämän päätöksen soveltamisen keskeyttämiseksi tai päätöksen kumoamiseksi tai sen muuttamiseksi.

8. **LOPPUPÄÄTELMÄT**

(229) Euroopan tietosuojaneuvosto on julkaissut lausuntonsa ([387]), joka on otettu huomioon tätä päätöstä valmisteltaessa.

(230) Tässä päätöksessä säädetyt toimenpiteet ovat asetuksen (EU) 2016/679 93 artiklan 1 kohdalla perustetun komitean lausunnon mukaiset,

ON HYVÄKSYNYT TÄMÄN PÄÄTÖKSEN:

1 artikla

1. Asetuksen (EU) 2016/679 45 artiklaa sovellettaessa Korean tasavalta varmistaa Euroopan unionista Korean tasavallassa toimiville yksiköille siirrettävien henkilötietojen riittävän suojan tason silloin kun kyseisiin toiminnanharjoittajiin sovelletaan Korean tietosuojalakia, sellaisena kuin se on täydennettynä liitteessä I olevilla täydentävillä säännöillä, yhdessä liitteessä II olevien virallisten lausuntojen, vakuutusten ja sitoumusten kanssa.

2. Tämä päätös ei koske henkilötietoja, jotka on siirretty johonkin seuraavaan luokkaan kuuluville vastaanottajille, jos henkilötietojen käsittelyn tarkoitus kokonaisuudessaan tai osittain vastaa jotakin luetelluista tarkoituksista:

(a) uskonnolliset organisaatiot siltä osin kuin ne käsittelevät henkilötietoja lähetystyöhön liittyviä toimintojaan varten;

(b) poliittiset puolueet siltä osin kuin ne käsittelevät henkilötietoja ehdokasasettelun yhteydessä;

(c) yksiköt, jotka kuuluvat luottorekisterilain nojalla tehtävän henkilötietojen käsittelyn osalta rahoituspalvelukomission valvonnan piiriin, siltä osin kuin ne käsittelevät tällaisia tietoja.

2 artikla

Aina kun jäsenvaltioiden toimivaltaiset viranomaiset käyttävät asetuksen (EU) 2016/679 58 artiklan mukaisia toimivaltuuksiaan suojellakseen yksilöiden henkilötietoja tämän päätöksen 1 artiklan soveltamisalaan kuuluvien tiedonsiirtojen osalta, asianomaisen jäsenvaltion on ilmoitettava siitä komissiolle viipymättä.

3 artikla

1. Komissio seuraa jatkuvasti tämän päätöksen perustana olevan oikeudellisen kehyksen soveltamista, muun muassa niitä edellytyksiä, joiden nojalla tietoja siirretään edelleen, yksilön oikeuksia käytetään ja Korean viranomaisilla on pääsy tämän päätöksen nojalla siirrettyihin tietoihin, sen arvioimiseksi, takaako Korean tasavalta edelleen suojan riittävän tason 1 artiklassa tarkoitetussa merkityksessä.

([387]) Opinion 32/2021 regarding the European Commission Draft Implementing Decision pursuant to Regulation (EU) 2016/679 on the adequate protection of personal data in the Republic of Korea, saatavilla osoitteessa: https://edpb.europa.eu/our-work-tools/our-documents/opinion-art-70/opinion-322021-regarding-european-commission-draft_en.

2. Jäsenvaltiot ja komissio ilmoittavat toisilleen tapauksista, joissa Korean tietosuojalautakunta tai muu toimivaltainen viranomainen laiminlyö sen varmistamisen, että tämän päätöksen perustana olevaa oikeudellista kehystä noudatetaan.

3. Jäsenvaltiot ja komissio ilmoittavat toisilleen mahdollisista havainnoista, joiden mukaan Korean viranomaiset puuttuvat yksilöiden oikeuteen suojella henkilötietojaan suuremmassa määrin kuin on ehdottoman välttämätöntä tai joiden mukaan tällaista puuttumista vastaan ei ole olemassa tehokasta oikeudellista suojaa.

4. Kolmen vuoden kuluessa siitä päivästä, jona tämä päätös annetaan tiedoksi jäsenvaltioille, ja vähintään joka neljäs vuosi sen jälkeen komissio arvioi 1 artiklan 1 kohdassa tarkoitetun päätelmän kaikkien saatavilla olevien tietojen perusteella, mukaan lukien tiedot, jotka on saatu osana Korean viranomaisten kanssa tehtyä vuotuista tarkastelua.

5. Jos komissiolla on viitteitä siitä, että tietosuojan riittävää tasoa ei enää turvata, komissio ilmoittaa asiasta Korean toimivaltaisille viranomaisille. Se voi tarvittaessa päättää tämän päätöksen soveltamisen keskeyttämisestä tai päätöksen muuttamisesta tai kumoamisesta tai sen soveltamisalan rajoittamisesta asetuksen (EU) 2016/679 45 artiklan 5 kohdan mukaisesti, erityisesti jos on viitteitä siitä, että

(a) Euroopan unionista henkilötietoja tämän päätöksen mukaisesti vastaanottaneet Koreassa toimivat rekisterinpitäjät eivät noudata liitteessä I vahvistettuja täydentäviä suojatoimia tai että asiaa koskeva seuranta ja noudattamisen valvonta on riittämätöntä;

(b) Korean viranomaiset eivät noudata liitteeseen II sisältyviä lausuntoja, vakuutuksia ja sitoumuksia, mukaan lukien ehdot ja rajoitukset, jotka koskevat Korean viranomaisten lainvalvontaan ja kansalliseen turvallisuuteen liittyviä tarkoituksia varten suorittamaa tämän päätöksen nojalla siirrettyjen henkilötietojen keräämistä ja Korean viranomaisten pääsyä niihin.

Komissio voi myös hyväksyä tällaisia toimenpiteitä, jos Korean hallituksen yhteistyöhaluttomuus estää komissiota arvioimasta, takaako Korean tasavalta edelleen suojan riittävän tason.

4 artikla

Tämä päätös on osoitettu kaikille jäsenvaltioille.

Tehty Brysselissä 17 päivänä joulukuuta 2021.

Komission puolesta
Didier REYNDERS
Komission jäsen

LIITE I

TÄYDENTÄVÄT SÄÄNNÖT KOREAN TIETOSUOJALAIN TULKINNASTA JA SOVELTAMISESTA KOREAAN SIIRRETTYJEN HENKILÖTIETOJEN KÄSITTELYN YHTEYDESSÄ

Sisältö

I. **Tausta**

Korea ja Euroopan unioni, jäljempänä 'EU', ovat käyneet tietosuojan riittävyyttä koskevia keskusteluja, joiden tuloksena Euroopan komissio on katsonut, että Korea varmistaa yleisen tietosuoja-asetuksen 45 artiklassa tarkoitetun riittävän tietosuojan tason.

Korean tietosuojalautakunta (*Personal Information Protection Commission*) on tähän liittyen antanut tämän Korean tietosuojalain 5 §:ään (valtion velvollisuudet ym.) ja 14 §:ään (kansainvälinen yhteistyö) ([1]) perustuvan ilmoituksen (*Notification*) selventääkseen eräiden lain säännösten tulkintaa, soveltamista ja noudattamisen valvontaa, myös siltä osin kuin on kyse Koreaan tietosuojan riittävyyttä koskevan EU:n päätöksen nojalla siirrettävien henkilötietojen käsittelystä.

Edellä mainittu ilmoitus on toimivaltaisen hallintoviranomaisen antama hallintosääntö, jonka tarkoituksena on selventää tietosuojalain tulkintaan, soveltamiseen ja noudattamisen valvontaan liittyviä vaatimuksia Korean oikeusjärjestelmässä. Ilmoitus on rekisterinpitäjää oikeudellisesti sitova siinä mielessä, että sen rikkominen voidaan katsoa tietosuojalain asianomaisten säännösten rikkomiseksi. Jos yksilöiden oikeuksia ja etuja loukataan ilmoituksen rikkomisen seurauksena, asianomaisilla yksilöillä on lisäksi oikeus käyttää oikeussuojakeinoja Korean tietosuojalautakunnassa tai tuomioistuimessa.

Vastaavasti, jos rekisterinpitäjä, joka käsittelee Koreaan tietosuojan riittävyyttä koskevan EU:n päätöksen nojalla siirrettäviä henkilötietoja, ei toteuta ilmoituksen mukaisia toimenpiteitä, katsotaan että kyseessä on "merkittävä peruste katsoa, että on tapahtunut henkilötietoja koskeva tietoturvaloukkaus, jonka edellyttämien toimenpiteiden laiminlyönti aiheuttaisi todennäköisesti vaikeasti korjattavissa olevan vahingon" (tietosuojalain 64 §:n 1 ja 2 momentti). Tällaisissa tapauksissa tietosuojalautakunta tai asianomainen keskushallinnon virasto voi määrätä kyseisen rekisterinpitäjän toteuttamaan

([1]) Korean tietosuojalain 14 §:ssä säädetään Korean hallituksen toimivallasta vahvistaa toimintapolitiikkoja, joilla pyritään parantamaan henkilötietojen suojaa kansainvälisessä ympäristössä ja estämään rekisteröityjen oikeuksien loukkaaminen henkilötietojen rajatylittävien siirtojen yhteydessä.

esimerkiksi korjaavia toimenpiteitä kyseisessä säännöksessä annettujen valtuuksien mukaisesti, minkä lisäksi voidaan rikkomisen luonteesta riippuen määrätä asianmukaisia seuraamuksia (kuten rikosoikeudellinen seuraamus tai hallinnollinen sakko).

II. **Määritelmät**

Tässä säännöksessä käytetään seuraavia määritelmiä:

(i) laki: tietosuojalaki (*Personal Information Protection Act*), laki N:o 16930, sellaisena kuin se on muutettuna 4.2.2020 ja voimaan saatettuna 5.8.2020)

(ii) presidentin asetus: tietosuojalain täytäntöönpanoasetus (*Enforcement Decree of the Personal Information Protection Act*), täytäntöönpanoasetus N:o 30509, annettu 3.3.2020, (sillä muutetaan myös muita lakeja)

(iii) rekisteröity: yksilö, joka on käsiteltävien tietojen perusteella tunnistettavissa

(iv) rekisterinpitäjä: julkinen laitos, oikeushenkilö, organisaatio tai yksilö ym., joka käsittelee henkilötietoja suoraan tai välillisesti henkilötietorekisteriä varten osana toimintaansa;

(v) EU: EU (vuoden 2020 helmikuun lopussa 27 jäsenvaltiota ([2]): Belgia, Saksa, Ranska, Italia, Luxemburg, Alankomaat, Tanska, Irlanti, Kreikka, Portugali, Espanja, Itävalta, Suomi, Ruotsi, Kypros, Tšekki, Viro, Unkari, Latvia, Liettua, Malta, Puola, Slovakia, Slovenia, Romania, Bulgaria ja Kroatia) sekä EU:hun ETA-sopimuksen nojalla assosioituneet maat (Islanti, Liechtenstein, Norja).

(vi) yleinen tietosuoja-asetus: EU:n yleinen tietosuoja-asetus (asetus (EU) 2016/679)

(vii) tietosuojan tason riittävyyttä koskeva päätös: yleisen tietosuoja-asetuksen 45 artiklan 3 kohdan mukaan Euroopan komissio voi päättää, että kolmas maa tai kolmannen maan alue tai yksi tai useampi tietty sektori tai kansainvälinen järjestö tarjoaa riittävän tietosuojan tason.

III. **Täydentävät säännöt**

1. **Ilman tarkoitusta tapahtuvan henkilötietojen käytön ja luovuttamisen rajoittaminen (lain 3, 15 ja 18 §)**

<Tietosuojalaki

(Laki N:o 16930, sellaisena kuin se on osittain muutettuna 4.2.2020)>

3 § (Tietosuojaperiaatteet) (1) Rekisterinpitäjän on määriteltävä nimenomaisesti tarkoitus, jota varten henkilötietoja käsitellään; henkilötietoja on kerättävä lainmukaisesti ja asianmukaisesti vain sen verran kuin on tarpeen tätä tarkoitusta varten.

(2) Rekisterinpitäjän on käsiteltävä henkilötietoja käsittelytarkoituksen kannalta asianmukaisella tavalla eikä se saa käyttää tietoja muihin tarkoituksiin.

15 § (Henkilötietojen kerääminen ja käyttö) (1) Rekisterinpitäjä voi kerätä henkilötietoja missä tahansa seuraavissa olosuhteissa ja käyttää niitä keräämistarkoituksen puitteissa:

1. kun rekisteröity on antanut suostumuksensa;

2. kun laissa niin erikseen säädetään tai se on tarpeen lakisääteisten velvoitteiden noudattamiseksi;

3. kun se on tarpeen, jotta julkinen laitos voi suorittaa sille kuuluvat tehtävät lainkäyttövaltansa puitteissa laissa säädetyllä tavalla;

4. kun se on tarpeen rekisteröidyn kanssa tehdyn sopimuksen täytäntöönpanoa varten;

([2]) Siirtymäkauden loppuun saakka joukkoon kuuluu myös Yhdistynyt kuningaskunta, Ison-Britannian ja Pohjois-Irlannin yhdistyneen kuningaskunnan eroamisesta Euroopan unionista ja Euroopan atomienergiayhteisöstä tehdyn sopimuksen 126, 127 ja 132 artiklan mukaisesti (2019/C 384 I/01).

5. kun katsotaan, että on olemassa ilmeinen tarve suojella rekisteröidyn tai kolmannen osapuolen henkeä, terveyttä tai omaisuutta välittömältä vaaralta ja jos rekisteröity itse tai hänen laillinen edustajansa ei kykene ilmaisemaan tahtoaan tai ennakkosuostumusta ei ole mahdollista saada esimerkiksi siksi, että asianomaisen osoite ei ole tiedossa;

6. kun se on tarpeen rekisterinpitäjän oikeutetun edun saavuttamiseksi, jos kyseinen etu on selvästi rekisteröidyn oikeuksia tärkeämpi. Tällaisissa tapauksissa käsittely sallitaan vain siltä osin kuin se liittyy olennaisesti kyseiseen rekisterinpitäjän oikeutettuun etuun eikä ylitä kohtuullista soveltamisalaa.

18 § (Ilman tarkoitusta tapahtuvan käytön rajoittaminen ja henkilötietojen luovuttaminen) (1) Rekisterinpitäjä ei saa käyttää henkilötietoja 15 §:n 1 momentissa ja 39-3 §:n 1 ja 2 momentissa määriteltyä soveltamisalaa laajemmin eikä luovuttaa niitä kolmannelle osapuolelle muutoin kuin 17 §:n 1 ja 3 momentissa säädetyin edellytyksin.

(2) Sen estämättä, mitä (1) kohdassa säädetään, jos sovelletaan jotakin seuraavista alakohdista, rekisterinpitäjä voi käyttää tietoja tai luovuttaa niitä kolmansille osapuolille myös muihin tarkoituksiin, paitsi jos se todennäköisesti loukkaisi oikeudettomasti rekisteröidyn tai kolmannen osapuolen etua: edellyttäen, että tieto- ja viestintäpalvelujen tarjoajiin [joita tarkoitetaan tieto- ja viestintäverkon käytön ja tietosuojan edistämisestä annetun lain *(Act on Promotion of Information and Communications Network Utilization and Information Protection*) 2 §:n 1 momentin 3 kohdassa; jäljempänä sovelletaan samaa], jotka käsittelevät [em. lain 2 §:n 1 momentin 4 kohdassa tarkoitettujen; jäljempänä sovelletaan samaa] käyttäjien henkilötietoja, sovelletaan ainoastaan 1 ja 2 alakohtaa, kun taas 5–9 alakohtaa sovelletaan ainoastaan julkisiin laitoksiin:

1. kun rekisteröity on antanut täydentävän suostumuksensa;

2. kun laissa on muita erityissäännöksiä;

3. kun katsotaan, että on olemassa ilmeinen tarve suojella rekisteröidyn tai kolmannen osapuolen henkeä, terveyttä tai omaisuutta välittömältä vaaralta ja jos rekisteröity itse tai hänen laillinen edustajansa ei kykene ilmaisemaan tahtoaan tai ennakkosuostumusta ei ole mahdollista saada esimerkiksi siksi, että asianomaisen osoite ei ole tiedossa;

4. poistettu;<lailla N:o 16930, 4.2.2020>

5. kun rekisterinpitäjän on mahdotonta suorittaa toimivaltaansa kuuluvia, mihin tahansa lakiin perustuvia tehtäviään muutoin kuin käyttämällä henkilötietoja muuhun kuin aiottuun tarkoitukseen tai luovuttamalla ne kolmannelle osapuolelle; tällöin asia on saatettava tietosuojalautakunnan käsiteltäväksi, joka antaa siitä päätöksen;

6. kun on tarpeen luovuttaa henkilötietoja vieraan valtion viranomaisille tai kansainväliselle järjestölle jonkin (kansainvälisen) sopimuksen täytäntöönpanoa varten;

7. kun se on tarpeen rikoksen tutkimista tai syytteeseenpanoa varten;

8. kun se on tarpeen, jotta tuomioistuin voi jatkaa oikeudenkäyntiin liittyviä tehtäviään;

9. Kun se on tarpeen rangaistuksen, ehdonalaisen vapauden tai vankeusrangaistuksen täytäntöönpanoa varten.

poistettu: (3) ja (4) momentti

(5) Jos rekisterinpitäjä luovuttaa henkilötietoja kolmannelle osapuolelle muita kuin aiottuja tarkoituksia varten jossakin (2) kohdassa tarkoitetussa tapauksessa, sen on pyydettävä henkilötietojen vastaanottajaa rajoittamaan tietojen käyttötarkoitusta ja -tapaa ja muita tarvittavia seikkoja, tai laadittava tarvittavat suojatoimet henkilötietojen turvallisuuden varmistamiseksi. Pyynnön vastaanottajan on tällaisissa tapauksissa toteutettava tarvittavat toimenpiteet henkilötietojen turvallisuuden varmistamiseksi.

(i) Lain 3 §:n 1 ja 2 momentissa säädetään periaatteesta, jonka mukaan rekisterinpitäjän on kerättävä henkilötietoja vain sen verran kuin on tarpeen käsittelytarkoituksen toteuttamiseksi lainmukaisesti, ja jonka mukaan tietoja ei saa käyttää muihin kuin aiottuihin tarkoituksiin ([3]).

(ii) Tämän periaatteen mukaisesti lain 15 §:n 1 momentissa säädetään, että kun rekisterinpitäjä kerää henkilötietoja, niitä voidaan käyttää keräämistarkoitusta varten, ja 18 §:n 1 kohdassa säädetään, että henkilötietoja ei saa käyttää muuhun kuin keräämistarkoitukseen eikä luovuttaa kolmannelle osapuolelle.

([3]) Koska näissä säännöksissä vahvistetaan yleiset periaatteet, joita sovelletaan kaikkeen henkilötietojen käsittelyyn, myös silloin kun käsittelyä säännellään erikseen muilla säädöksillä, tässä kohdassa esitettyjä selvennyksiä sovelletaan myös silloin kun henkilötietoja käsitellään muiden lakien nojalla (ks. esim. luottotietolain (*Credit Information Act*) 15 §:n 1 momentti, jossa viitataan nimenomaisesti näihin säännöksiin).

(iii) Myös silloin kun henkilötietoja saa käyttää muuhun kuin aiottuun tarkoitukseen tai luovuttaa kolmannelle osapuolelle poikkeustapauksissa ([4]), joista säädetään lain 18 §:n 2 momentissa, on edellytettävä käyttötarkoituksen tai -tavan rajoittamista siten, että henkilötietoja voidaan käsitellä turvallisesti 5 kohdan mukaisesti, tai on toteutettava henkilötietojen turvallisuuden varmistamiseksi tarvittavat toimenpiteet.

(iv) Edellä mainittuja säännöksiä sovelletaan yhtäläisesti myös kaikkien sellaisten henkilötietojen käsittelyyn, jotka on vastaanotettu Korean lainkäyttöalueelle kolmannesta maasta, rekisteröityjen kansalaisuudesta riippumatta.

(v) Jos esimerkiksi EU:n rekisterinpitäjä siirtää henkilötietoja korealaiselle rekisterinpitäjälle tietosuojan tason riittävyyttä koskevan Euroopan komission päätöksen mukaisesti, katsotaan, että se tarkoitus, jota varten EU:n rekisterinpitäjä siirtää tiedot, on se tarkoitus, jota varten korealainen rekisterinpitäjä kerää tiedot, ja korealainen rekisterinpitäjä voi tällaisessa tapauksessa käsitellä tietoja tai luovuttaa niitä kolmannelle osapuolelle ainoastaan keräämistarkoitusta varten, paitsi jos on kyseessä jokin lain 18 §:n 2 kohdassa tarkoitettu poikkeustapaus.

2. **Henkilötietojen edelleen siirtämisen rajoittaminen (lain 17 §:n 3 ja 4 momentti ja 18 §)**

<Tietosuojalaki

(Laki N:o 16930, sellaisena kuin se on osittain muutettuna 4.2.2020)>

17 § (Henkilötietojen luovuttaminen) (1) poistettu

(2) Rekisterinpitäjän on ilmoitettava rekisteröidylle seuraavat seikat, kun se saa tämän suostumuksen 1 momentin 1 kohdan nojalla. Samaa sovelletaan, jos jotakin seuraavista muutetaan:

1. henkilötietojen vastaanottaja;

2. tarkoitus, jota varten henkilötietojen vastaanottaja käyttää kyseisiä tietoja;

3. yksityiskohtaiset tiedot luovutettavista henkilötiedoista;

4. kuinka kauan vastaanottaja säilyttää ja käyttää tietoja;

5. se, että rekisteröidyllä on oikeus evätä suostumuksensa, ja tästä mahdollisesti aiheutuvat haitat.

(3) Rekisterinpitäjän on ilmoitettava rekisteröidylle 2 kohdassa säädetyt seikat ja saatava rekisteröidyn suostumus henkilötietojen luovuttamiseen ulkomailla olevalle kolmannelle osapuolelle; Rekisterinpitäjä ei saa tehdä sopimusta henkilötietojen rajatylittävästä siirtämisestä tämän lain vastaisesti.

(4) Rekisterinpitäjä voi luovuttaa henkilötietoja ilman rekisteröidyn suostumusta, jos käsittelytarkoitus kohtuudella liittyy niihin tarkoituksiin, joita varten tiedot alun perin kerättiin, presidentin asetuksessa säädettyjen edellytysten mukaisesti, kun otetaan huomioon siitä rekisteröidylle mahdollisesti aiheutuvat haitat ja muun muassa se, onko toteutettu turvallisuuden varmistamiseksi tarvittavat toimenpiteet, kuten salaus.

※ Ks. 18 §:n osalta s. 3, 4 ja 5.

< **Tietosuojalain täytäntöönpanoasetus**

([Täytäntöönpanopäivä 5.2.2021.] [Presidentin asetus N:o 30892, 4.8.2020. (jolla muutetaan myös muita lakeja)])>

14-2 § (Henkilötietojen käyttöä/luovuttamista muuhun tarkoitukseen koskevat säännöt, ym.)

(1) Jos rekisterinpitäjä käyttää tai luovuttaa tietoja muuhun kuin lain 15 §:n 3 momentissa tai 17 §:n 4 momentissa säädettyyn tarkoitukseen, jäljempänä ”käyttö tai luovuttaminen muuhun tarkoitukseen”, ilman rekisteröidyn suostumusta, sen on otettava huomioon seuraavat seikat:

1. liittyykö tämä tarkoitus kohtuudella tietojen alkuperäiseen keräämistarkoitukseen;

2. onko henkilötietojen käyttö tai luovuttaminen muuhun tarkoitukseen ennakoitavissa niissä olosuhteissa, joissa henkilötiedot kerättiin, ja niiden käsittelykäytännöissä;

3. loukkaako henkilötietojen käyttö tai luovuttaminen muuhun tarkoitukseen oikeudettomasti rekisteröidyn etuja; ja

4. onko toteutettu turvallisuuden varmistamiseksi vaaditut toimenpiteet, kuten pseudonymisointi tai salaus.

([4]) Tieto- ja viestintäpalvelujen tarjoajiin sovelletaan ainoastaan 18 §:n 2 momentin 1 ja 2 kohdan säännöksiä. Vastaavasti 5–9 kohdan säännöksiä sovelletaan ainoastaan julkisiin laitoksiin.

(2) Rekisterinpitäjän on esitettävä etukäteen kriteerit, joiden mukaan 1 kohdan alakohdissa tarkoitettuja seikkoja arvioidaan, lain 30 §:n 1 momentissa tarkoitetussa tietosuojaselosteessa, ja lain 31 §:n 1 momentissa tarkoitetun tietosuojavastaavan on tarkistettava, että rekisterinpitäjä käyttää tai luovuttaa henkilötietoja asiaa koskevien sääntöjen mukaisesti.

(i) Jos rekisterinpitäjä luovuttaa henkilötietoja ulkomailla olevalle kolmannelle osapuolelle, sen on ilmoitettava rekisteröidyille etukäteen kaikista lain 17 §:n 2 momentissa tarkoitetuista seikoista ja saatava heidän suostumuksensa, 1 tai 2 momentin soveltamisalaan kuuluvia tapauksia lukuun ottamatta. Henkilötietojen rajatylittävästä siirtämisestä ei saa tehdä sopimuksia tämän lain vastaisesti.

(1) Jos henkilötietoja luovutetaan tarkoitukseen, joka ”liittyy kohtuullisesti” tietojen alkuperäiseen keräämistarkoitukseen lain 17 §:n 4 momentin mukaisesti. Tätä säännöstä voidaan kuitenkin soveltaa ainoastaan tapauksiin, joissa täytäntöönpanoasetuksen 14-2 §:ssä säädetyt henkilötietojen luovuttamista ja myöhempää käyttöä koskevat edellytykset täyttyvät. Rekisterinpitäjän on lisäksi otettava huomioon se, voiko henkilötietojen luovuttaminen aiheuttaa haittaa rekisteröidyille ja onko se toteuttanut tarvittavat toimenpiteet turvallisuuden varmistamiseksi, kuten salauksen.

(2) Jos henkilötietoja voidaan luovuttaa kolmannelle osapuolelle lain 18 §:n 2 momentissa mainituissa poikkeustapauksissa (ks. s. 3–5). Henkilötietoja ei kuitenkaan saa luovuttaa kolmannelle osapuolelle myöskään kyseisissä tapauksissa, jos luovuttaminen todennäköisesti loukkaisi oikeudettomasti rekisteröidyn tai kolmannen osapuolen etuja. Rekisterinpitäjän on lisäksi pyydettävä henkilötietojen vastaanottajaa rajoittamaan henkilötietojen käyttötarkoitusta tai -tapaa tai toteutettava tarvittavat toimenpiteet niin, että käsittely voidaan suorittaa turvallisesti.

(ii) Jos henkilötietoja luovutetaan ulkomailla olevalle kolmannelle osapuolelle, niihin ei välttämättä sovelleta samanlaista suojelun tasoa, jonka Korean tietosuojalaki tarjoaa, koska eri maissa sovelletaan erilaisia henkilötietojen suojaa koskevia järjestelmiä. Siksi katsotaan, että tällöin on kyse lain 17 §:n 4 momentissa tarkoitetuista ”tapauksista, joissa rekisteröidylle voi aiheutua haittoja” tai lain 18 §:n 2 momentissa ja sen täytäntöönpanoasetuksen 14-2 §:ssä tarkoitetuista ”tapauksista, joissa rekisteröidyn tai kolmannen osapuolen etuja loukataan oikeudettomasti” ([5]). Näissä säännöksissä asetettujen vaatimusten täyttämiseksi rekisterinpitäjän ja kolmannen osapuolen on nimenomaisesti varmistettava Korean tietosuojalain tasoinen suoja, muun muassa vahvistamalla oikeudellisesti sitovissa asiakirjoissa, kuten sopimuksissa, takeet siitä, että rekisteröity voi käyttää oikeuksiaan myös sen jälkeen kun henkilötiedot on siirretty ulkomaille.

3. **Tiedoista ilmoittaminen, jos henkilötietoja ei ole saatu rekisteröidyltä (lain 20 §)**

<Tietosuojalaki

(Laki N:o 16930, sellaisena kuin se on osittain muutettuna 4.2.2020)>

20 § (Ilmoitus henkilötietojen lähteestä ym., kun tiedot on kerätty kolmansilta osapuolilta) (1) Kun rekisterinpitäjä käsittelee henkilötietoja, jotka on kerätty kolmansilta osapuolilta, sen on viipymättä ilmoitettava rekisteröidylle tämän pyynnöstä seuraavat seikat:

1. lähde, josta henkilötiedot on kerätty;

2. henkilötietojen käsittelyn tarkoitus;

3. se, että rekisteröidyllä on oikeus vaatia henkilötietojen käsittelyn keskeyttämistä lain 37 §:n mukaisesti.

(2) Sen estämättä, mitä (1) kohdassa säädetään, kun rekisterinpitäjä, joka täyttää presidentin asetuksessa säädetyt vaatimukset, jotka koskevat muun muassa käsiteltävien henkilötietojen tyyppiä ja määrää sekä rekisterinpitäjän työntekijöiden ja liikevaihdon määrää, kerää henkilötietoja kolmansilta osapuolilta ja käsittelee niitä lain 17 §:n 1 momentin 1 kohdan mukaisesti, rekisterinpitäjän on ilmoitettava rekisteröidylle 1 kohdassa tarkoitetut seikat: edellyttäen, että tätä ei sovelleta silloin kun rekisterinpitäjän keräämät tiedot eivät sisällä lainkaan henkilötietoja, kuten yhteystietoja, joiden avulla ilmoitus rekisteröidylle voitaisiin tehdä.

([5]) Tietosuojalain 18 §:n 2 momentin 2 kohdan nojalla tätä sovelletaan myös silloin kun henkilötietoja luovutetaan ulkomailla oleville kolmansille osapuolille muiden lakien (kuten luottotietolain) säännösten nojalla.

(3) Tarvittavat säännöt, jotka koskevat 2 kohdassa tarkoitetun rekisteröidylle ilmoittamisen ajankohtaa, tapaa ja menettelyä, vahvistetaan presidentin asetuksessa.

(4) Edellä olevaa (1) kohtaa ja (2) kohdan päälauseketta ei sovelleta seuraavissa olosuhteissa: edellyttäen, että näin toimitaan vain silloin kun olosuhteet ovat selvästi tärkeämmät kuin tämän lain mukaiset rekisteröityjen oikeudet:

1. Kun henkilötiedot, joita ilmoitusvaatimus koskee, sisältyvät johonkin lain 32 §:n 2 momentin alakohdissa tarkoitettuun henkilötietorekisteriin;

2. Kun ilmoittaminen todennäköisesti vahingoittaisi toisen henkilön henkeä tai terveyttä tai aiheuttaisi oikeudettomasti vahinkoa toisen henkilön omaisuudelle ja muille eduille.

(i) Jos rekisterinpitäjä vastaanottaa henkilötietoja, jotka on siirretty EU:sta tietosuojan riittävyyttä koskevan päätöksen perusteella ([6]), sen on ilmoitettava rekisteröidylle (1)–(5) kohdassa mainitut tiedot viipymättä ja joka tapauksessa viimeistään kuukauden kuluttua siirrosta.

(1) Henkilötiedot siirtävien ja vastaanottavien henkilöiden nimi ja yhteystiedot.

(2) Siirrettävät henkilötiedot tai niiden ryhmät.

(3) Tietojen keräämis- ja käyttötarkoitus (tietojen viejä määrittää nämä tämän ilmoituksen 1 kohdan nojalla).

(4) Henkilötietojen säilytysaika.

(5) Tiedot rekisteröidyn oikeuksista henkilötietojen käsittelyn yhteydessä, oikeuksien käyttämistapa ja sovellettava menettely sekä oikeuksien käyttämisestä mahdollisesti aiheutuvat haitat.

(ii) Jos henkilötietojen rekisterinpitäjä luovuttaa henkilötietoja (i) Korean tasavallassa tai ulkomailla olevalle kolmannelle osapuolelle, sen on ilmoitettava rekisteröidylle (1)–(5) kohdassa mainitut tiedot ennen tietojen luovuttamista.

(1) Henkilötiedot luovuttavien ja vastaanottavien henkilöiden nimi ja yhteystiedot.

(2) Luovutettavat henkilötiedot tai niiden ryhmät.

(3) Maa, johon henkilötiedot luovutetaan, suunniteltu päivämäärä ja luovutustapa (vain silloin kun henkilötietoja luovutetaan ulkomailla olevalle kolmannelle osapuolelle).

(4) Henkilötietojen luovuttajan tarkoitus ja oikeusperusta, jonka perusteella tiedot luovutetaan.

(5) Tiedot rekisteröidyn oikeuksista henkilötietojen käsittelyn yhteydessä, oikeuksien käyttämistapa ja sovellettava menettely sekä oikeuksien käyttämisestä mahdollisesti aiheutuvat haitat.

(iii) Rekisterinpitäjän ei tarvitse soveltaa (i) tai (ii) alakohtaa (1)–(4) kohdassa mainituissa tapauksissa.

(1) Jos henkilötiedot, joista on ilmoitettava, sisältyvät johonkin lain 32 §:n 2 momentissa tarkoitettuun henkilötietorekisteriin, siltä osin kuin tällä säännöksellä suojatut edut ovat selvästi rekisteröidyn oikeuksia tärkeämpiä, ja vain niin kauan kuin ilmoittaminen uhkaisi kyseessä olevia etuja, esimerkiksi vaarantamalla meneillään olevan rikostutkinnan tai kansallisen turvallisuuden.

(2) Jos ja niin kauan kuin ilmoittaminen todennäköisesti vahingoittaisi toisen henkilön henkeä tai terveyttä tai loukkaisi oikeudettomasti toisen henkilön omistusoikeuksia, kun nämä oikeudet tai edut ovat selvästi rekisteröidyn oikeuksia tärkeämpiä.

(3) Jos rekisteröidyllä on jo tiedot, jotka rekisterinpitäjän on ilmoitettava (i) tai (ii) alakohdan nojalla.

(4) Jos rekisterinpitäjällä ei ole rekisteröidyn yhteystietoja tai jos ilmoittamisesta aiheutuisi kohtuutonta vaivaa, mukaan lukien tietosuojalain 3 §:ssä säädettyjen edellytysten mukaisen käsittelyn yhteydessä. Määritettäessä sitä, onko rekisteröityyn mahdollista ottaa yhteyttä tai aiheutuuko siitä kohtuutonta vaivaa, on otettava huomioon mahdollisuus tehdä yhteistyötä EU:ssa olevan tietojen viejän kanssa.

([6]) Jäljempänä (i), (ii) ja (iii) kohdassa lueteltuja velvoitteita sovelletaan myös silloin kun rekisterinpitäjä, joka vastaanottaa henkilötietoja EU:sta tietosuojan riittävyyttä koskevan päätöksen perusteella, käsittelee kyseisiä tietoja muiden lakien, kuten luottotietolain, nojalla.

4. **Pseudonymisoitujen tietojen käsittelyä koskevan erityispoikkeuksen soveltamisala (lain 28-2, 28-3, 28-4, 28-5, 28-6 ja 28-7 §, 3 § ja 58-2 §)**

<Tietosuojalaki

(Laki N:o 16930, sellaisena kuin se on osittain muutettuna 4.2.2020)>

III luku - Henkilötietojen käsittely

3 § - Pseudonymisoituja tietoja koskevat erityistapaukset

28-2 § (Pseudonymisoitujen tietojen käsittely) (1) Rekisterinpitäjä voi käsitellä pseudonymisoituja tietoja ilman rekisteröidyn suostumusta muun muassa tilastointia, tieteellistä tutkimusta tai yleisen edun mukaista arkistointia varten.

(2) Rekisterinpitäjä ei saa sisällyttää (1) kohdan mukaisesti kolmannelle osapuolelle luovutettaviin pseudonymisoituihin tietoihin tietoja, joita voidaan käyttää tietyn henkilön tunnistamiseen.

28-3 § (Pseudonymisoitujen tietojen yhdistämisen rajoittaminen) (1) Sen estämättä, mitä 28-2 §:ssä säädetään, eri rekisterinpitäjien tilastointia, tieteellistä tutkimusta tai yleisen edun mukaista arkistointia varten käsittelemien tietojen yhdistäminen on annettava tehtäväksi erikoistuneelle laitokselle, jonka tietosuojalautakunta tai asianomaisen keskushallinnon viraston päällikkö nimeää.

(2) Kun rekisterinpitäjä aikoo luovuttaa yhdistetyt tiedot ne yhdistäneen laitoksen ulkopuolelle, sen on saatava tähän lupa kyseisen laitoksen päälliköltä sen jälkeen kun tiedot on käsitelty pseudonymisoituun tai 58-2 §:ssä tarkoitettuun muotoon.

(3) Tarvittavat seikat, kuten (1) kohdassa tarkoitetut tietojen yhdistämisessä käytettävät menettelyt sekä säännöt ja menettelyt, joita sovelletaan erikoistuneiden laitosten johto- ja valvontahenkilöstön nimeämisessä tai nimeämisen peruuttamisessa, ja (2) kohdan nojalla tapahtuvaa vientiä ja hyväksymistä koskevat säännöt ja menettelyt vahvistetaan presidentin asetuksessa.

28-4 § (Velvoite toteuttaa pseudonymisoituja tietoja koskevia suojatoimia) (1) Rekisterinpitäjän on toteutettava pseudonymisoitujen tietojen käsittelyä varten tarvittavat tekniset, hallinnolliset ja fyysiset toimenpiteet (muun muassa säilyttämällä ja hallinnoimalla erikseen niitä tietoja, jotka ovat tarpeen pseudonymisoitujen tietojen palauttamiseksi alkuperäiseen tilaansa), jotta voidaan varmistaa presidentin asetuksessa tarkoitettu henkilötietojen turvallisuus ja estää niiden katoaminen, varastaminen, paljastaminen, väärentäminen, muuttaminen ja vahingoittuminen.

(2) Kun rekisterinpitäjä aikoo käsitellä pseudonymisoituja tietoja, sen on niiden hallinnointia varten pidettävä kirjaa presidentin asetuksessa säädetyistä seikoista, kuten tietojenkäsittelyn tarkoituksesta ja pseudonymisoidut tiedot vastaan ottavasta kolmannesta osapuolesta.

28-5 § (Pseudonymisoitujen tietojen käsittelyssä kielletyt toimet) (1) Pseudonymisoituja tietoja ei saa käsitellä yksittäisen henkilön tunnistamiseksi.

(2) Jos pseudonymisoitujen tietojen käsittelyn aikana syntyy tietoja, joiden avulla on mahdollista tunnistaa yksittäinen henkilö, rekisterinpitäjän on lopetettava tietojen käsittely ja haettava ja tuhottava kyseiset tiedot välittömästi.

28-6 § (Hallinnollisten lisämaksujen määrääminen pseudonymisoitujen tietojen käsittelyn vuoksi) (1) Tietosuojalautakunta voi määrätä rekisterinpitäjälle sakon, jonka määrä on enintään yksi kolmassadasosa rekisterinpitäjän liikevaihdosta, jos rekisterinpitäjä on käsitellyt tietoja 28-5 §:n (1) momentin vastaisesti yksittäisen henkilön tunnistamiseksi. Jos liikevaihtoa ei ole tai jos sitä on vaikea määrittää, rekisterinpitäjälle voidaan määrätä sakkoa enintään 400 miljoonaa wonia tai kolme sadasosaa sen pääomasta, sen mukaan kumpi näistä määristä on suurempi.

(2) 34-2 §:n 3–5 momenttia sovelletaan soveltuvin osin seikkoihin, joiden avulla hallinnolliset lisämaksut määritetään ja kerätään.

28-7 § (Soveltamisala) @20, 21 ja 27 pykälää, 34 §:n 1 momenttia, 35–37 §:ää sekä 39-3, 39-4 ja 39-6–39-8 pykälää ei sovelleta pseudonymisoituihin tietoihin.

I luku Yleiset säännökset

3 § (Tietosuojaperiaatteet) (1) Rekisterinpitäjän on määriteltävä nimenomaisesti tarkoitus, jota varten henkilötietoja käsitellään; henkilötietoja on kerättävä lainmukaisesti ja asianmukaisesti vain sen verran kuin on tarpeen tätä tarkoitusta varten.

(2) Rekisterinpitäjän on käsiteltävä henkilötietoja käsittelytarkoituksen kannalta asianmukaisella tavalla eikä se saa käyttää tietoja muihin tarkoituksiin.

(3) Rekisterinpitäjän on varmistettava, että henkilötiedot ovat täsmällisiä, täydellisiä ja ajantasaisia siltä osin kuin on tarpeen niiden tarkoitusten kannalta, joita varten tietoja käsitellään.

(4) Rekisterinpitäjän on hallinnoitava henkilötietoja turvallisesti ottaen huomioon muun muassa käsittelymenetelmät ja tietojen tyyppi sekä rekisteröidyn oikeuksien loukkaamisen mahdollisuus ja siihen liittyvien riskien vakavuus.

(5) Rekisterinpitäjän on julkistettava tietosuojaselosteensa ja muut henkilötietojen käsittelyyn liittyvät asiat; ja turvattava rekisteröidyn oikeudet, kuten oikeus tutustua omiin henkilötietoihinsa.

(6) Rekisterinpitäjän on käsiteltävä henkilötietoja niin, että voidaan minimoida mahdollisuus rekisteröidyn yksityisyyden loukkaamiseen.

(7) Jos henkilötietojen keräämisen tarkoitus on mahdollista saavuttaa käsittelemällä anonymisoituja tai pseudonymisoituja tietoja, rekisterinpitäjän on pyrittävä käsittelemään henkilötietoja anonymisoituina, jos se on mahdollista, tai pseudonymisoituina, jos käsittelytarkoitusta ei voida saavuttaa anonymisoitujen tietojen avulla.

(8) Rekisterinpitäjän on pyrittävä saamaan rekisteröidyn luottamus noudattamalla tietosuojalaissa ja muissa siihen liittyvissä säännöksissä säädettyjä velvollisuuksia ja vastuutehtäviä.

IX luku Täydentävät säännökset

58-2 § (Soveltamisesta vapauttaminen) Tätä lakia ei sovelleta tietoihin, joista ei voi enää tunnistaa yksittäistä henkilöä, kun ne yhdistetään muihin tietoihin, kun otetaan huomioon muun muassa tunnistamiseen kohtuudella tarvittava aika, kustannukset ja teknologia. <Tämä säännös on lisätty äskettäin lailla N:o16930, 4.2.2020>

(i) III luvun 3 jakso ”Pseudonymisoituja tietoja koskevat erityistapaukset” (28-2–28-7 §) mahdollistaa pseudonymisoitujen tietojen käsittelyn ilman rekisteröidyn suostumusta, kun käsittelyn tarkoituksena on esimerkiksi tilastointi, tieteellinen tutkimus tai yleisen edun mukainen arkistointi (28-2 §), kunhan noudatetaan asianmukaisia suojatoimia ja kieltoja rekisteröityjen oikeuksien suojaamiseksi (28-4 ja 28-5 §); sääntöjen rikkomisesta voidaan määrätä sakkoja (28-6 §), eikä eräitä tietosuojalaissa muuten säädettyjä suojatoimia sovelleta (28-7 §).

(ii) Näitä säännöksiä ei sovelleta silloin kun pseudonymisoituja tietoja käsitellään muita tarkoituksia kuin mm. tilastointia, tieteellistä tutkimusta tai yleisen edun mukaista arkistointia varten. Jos esimerkiksi EU:n kansalaisen henkilötiedot, jotka on siirretty Koreaan tietosuojan riittävyyttä koskevan Euroopan komission päätöksen nojalla, pseudonymisoidaan muuta tarkoitusta kuin tilastointia, tieteellistä tutkimusta tai yleisen edun mukaista arkistointia varten, III luvun 3 jakson erityissäännöksiä ei sovelleta ([7]).

(iii) Kun rekisterinpitäjä käsittelee pseudonymisoituja tietoja esimerkiksi tilastointia, tieteellistä tutkimusta tai yleisen edun mukaista arkistointia varten eikä pseudonymisoituja tietoja ole tuhottu sen jälkeen kun käsittelyn tarkoitus on saavutettu perustuslain 37 §:n ja tämän lain 3 §:n (Tietosuojaperiaatteet) mukaisesti, rekisterinpitäjän on anonymisoitava tiedot sen varmistamiseksi, että niistä ei yksinään tai muihin tietoihin yhdistettynä voida enää tunnistaa yksittäistä henkilöä, kun otetaan huomioon muun muassa tunnistamiseen kohtuudella tarvittava aika, kustannukset ja teknologia, tietosuojalain 58-2 §:n mukaisesti.

5. **Korjaavat toimenpiteet ym. (lain 64 §:n 1, 2 ja 4 momentti)**

<Tietosuojalaki

(Laki N:o 16930, sellaisena kuin se on osittain muutettuna 4.2.2020)>

64 § (Korjaavat toimenpiteet) (1) Jos tietosuojalautakunnan arvion mukaan on riittävät perusteet katsoa, että on tapahtunut tietoturvaloukkaus, ja toimenpiteiden toteuttamatta jättäminen todennäköisesti aiheuttaisi vaikeasti korjattavissa olevaa vahinkoa, se voi määrätä tämän lain rikkojan (pois lukien keskushallinnon virastot, paikallishallinto, kansalliskokous, tuomioistuin, perustuslakituomioistuin ja kansallinen vaalilautakunta) toteuttamaan jonkin seuraavista toimenpiteistä:

1. henkilötietoihin liittyvän rikkomisen keskeyttäminen;

2. henkilötietojen käsittelyn väliaikainen keskeyttäminen;

([7]) Vastaavasti luottotietolain 40-3 §:ää koskevaa poikkeusta sovelletaan ainoastaan silloin kun pseudonymisoituja luottotietoja käsitellään tilastointia, tieteellistä tutkimusta tai yleisen edun mukaista arkistointia varten.

3. muut toimenpiteet, jotka ovat tarpeen henkilötietojen suojaamiseksi ja tietoturvaloukkausten estämiseksi.

(2) Jos asianomaisen keskushallinnon viraston päällikkö arvioi, että on riittävät perusteet katsoa, että on tapahtunut tietoturvaloukkaus, ja toimenpiteiden toteuttamatta jättäminen todennäköisesti aiheuttaisi vaikeasti korjattavissa olevaa vahinkoa, hän voi määrätä rekisterinpitäjän toteuttamaan jonkin (1) kohdassa tarkoitetun toimenpiteen kyseisen keskushallinnon viraston toimivaltaa koskevien säännösten nojalla.

(4) Jos jokin keskushallinnon virasto, paikallishallinto, kansalliskokous, tuomioistuin, perustuslakituomioistuin tai kansallinen vaalilautakunta loukkaa tämän lain säännöksiä, tietosuojalautakunta voi suosittaa, että asianomaisen viraston ym. päällikkö toteuttaa jonkin (1) kohdassa tarkoitetun toimenpiteen. Tällaisen suosituksen saatuaan kyseisen viraston on noudatettava sitä, paitsi jos on kyse poikkeuksellisista olosuhteista.

(i) Ensinnäkin tuomioistuimen ennakkotapauksissa ([8]) ([9]) on tulkittu, että 'vaikeasti korjattavissa olevalla vahingolla' tarkoitetaan yksilön henkilökohtaisten oikeuksien tai yksityisyyden loukkaamista.

(ii) Näin ollen 64 §:n 1 ja 2 momentissa olevalla ilmaisulla 'on riittävät perusteet katsoa, että on tapahtunut tietoturvaloukkaus, ja toimenpiteiden toteuttamatta jättäminen todennäköisesti aiheuttaisi vaikeasti korjattavissa olevaa vahinkoa' tarkoitetaan tapauksia, joissa lain rikkomisen katsotaan todennäköisesti loukkaavan yksilön oikeuksia ja vapauksia hänen henkilötietojensa osalta. Tätä sovelletaan aina kun laissa säädettyjä henkilötietojen suojaamista koskevia periaatteita, oikeuksia ja velvollisuuksia rikotaan ([10]).

(iii) Tietosuojalain 64 §:n 4 momentin mukaan 'tämän lain rikkomisen' vuoksi toteutettavalla toimenpiteellä tarkoitetaan tietosuojalain rikkomisen vuoksi toteutettavaa toimenpidettä.

Keskushallinnon virasto ym. ovat oikeusvaltioperiaatteen noudattamiseen sitoutuneita viranomaisia, jotka eivät saa rikkoa mitään lakia. Niiden on toteutettava korjaavat toimenpiteet, kuten keskeytettävä toiminta, ja korvattava vahingot, jos lainvastainen teko on poikkeuksellisessa tapauksessa kuitenkin tapahtunut.

Näin ollen keskushallinnon viraston, joka havaitsee, että lakia on rikottu, on tietosuojalain 64 §:n 4 momentin nojalla toteutettava korjaavia toimenpiteitä myös ilman, että tietosuojalautakunnan tarvitsee puuttua asiaan.

Erityisesti silloin kun tietosuojalautakunta on suosittanut korjaavaa toimenpidettä, keskushallinnon virastolle on yleensä jo sen perusteella objektiivisesti selvää, että se on rikkonut lakia. Jotta virasto voisi tällaisessa tilanteessa perustella, miksi se ei katso tarpeelliseksi noudattaa tietosuojalautakunnan suositusta, sen on esitettävä selkeät perusteet osoittaakseen, ettei se ole rikkonut lakia. Suositusta on noudatettava, paitsi jos tietosuojalautakunta toteaa, että se ei todella ole tarpeen.

Tämän vuoksi tietosuojalain 64 §:n 4 momentissa tarkoitetut "poikkeukselliset olosuhteet" on rajattava tiukasti sellaisiin poikkeuksellisiin olosuhteisiin, joissa keskushallinnon virasto voi selkeiden perusteiden nojalla osoittaa, että "tätä lakia ei ole rikottu", kuten esimerkiksi "tapaukset, joissa on poikkeukselliset (oikeudellisiin tai tosiseikkoihin) perustuvat olosuhteet", jotka eivät olleet tietosuojalautakunnan tiedossa silloin kun se alun perin antoi suosituksensa, ja tietosuojalautakunta toteaa, että lakia ei ole rikottu.

6. **Korean tietosuojalain soveltaminen kansalliseen turvallisuuteen liittyviä tarkoituksia varten tapahtuvan henkilötietojen käsittelyn yhteydessä, mukaan lukien rikkomisten tutkiminen ja noudattamisen valvonta tietosuojalain mukaisesti (lain 7-8, 7-9 §, 58, 3, 4 ja 62 §)**

<Tietosuojalaki

(Laki N:o 16930, sellaisena kuin se on osittain muutettuna 4.2.2020)>

7-8 § (Tietosuojalautakunnan tehtävät) (1) Tietosuojalautakunta vastaa seuraavista tehtävistä: […]

3. rekisteröityjen oikeuksien loukkaamista koskevat tutkinnat ja niiden jatkotoimet;

4. henkilötietojen käsittelyä koskevien valitusten ja oikeussuojakeinojen käsittely ja henkilötietoja koskevien riita-asioiden sovittelu;

[…]

([8]) (Korkeimman oikeuden tuomio 97Da10215,10222, 26.1.1999). Jos syytettyä koskevat rikosoikeudelliset tosiseikat paljastetaan mediassa, siitä aiheutuu todennäköisesti sekä fyysistä että psyykkistä peruuttamatonta vahinkoa paitsi uhrille eli kantajalle, myös hänen läheisilleen, kuten perheenjäsenille.

([9]) (Soulin korkeimman oikeuden päätös 2006Na92006, 16.1.2008) Herjaavan artikkelinjulkaisemisesta aiheutuu todennäköisesti asianosaimelle henkilölle vakavaa peruuttamatonta vahinkoa.

([10]) Edellä ii kohdassa esitettyjä periaatteita sovelletaan myös luottotietolain 45-4 §:ään.

7-9 § (Asiat, jotka tietosuojalautakunta käsittelee ja ratkaisee) (1) Tietosuojalautakunta käsittelee ja ratkaisee seuraavat asiat: […]

5. Henkilötietojen suojaa koskevan lainsäädännön tulkintaan ja toimintaan liittyvät asiat;

[…]

58 § (Osittainen vapautus soveltamisesta) (1) III–VII lukua ei sovelleta seuraaviin henkilötietoihin:

1. henkilötiedot, jotka kerätään julkisten laitosten käsiteltäväksi tilastolain (*Statistics Act*) nojalla;

2. henkilötiedot, jotka kerätään tai joita pyydetään kansalliseen turvallisuuteen liittyvien tietojen analysointia varten;

3. henkilötiedot, joita käsitellään väliaikaisesti, kun se on tarpeen kiireellisissä tapauksissa esimerkiksi yleiseen turvallisuuteen ja kansanterveyteen liittyvistä syistä;

4. henkilötiedot, joita lehdistö, uskonnolliset organisaatiot tai poliittiset puolueet keräävät tai käyttävät omiin tarkoituksiinsa (journalistinen tai lähetystyöhön liittyvä toiminta ja puolueiden ehdokasasettelu).

[poistettu: (2) ja (3) momentti]

(4) Kun henkilötietoja käsitellään (1) kohdan nojalla, rekisterinpitäjän on käsiteltävä henkilötietoja vain sen verran kuin asianomaisen tarkoituksen saavuttamiseksi on tarpeen ja mahdollisimman lyhyen aikaa; lisäksi sen on toteutettava tarvittavat toimenpiteet (kuten tekniset, hallinnolliset ja fyysiset suojatoimet sekä toimenpiteet yksilöiden valitusten asianmukaista käsittelyä varten) turvallisen tiedonhallinnan ja asianmukaisen käsittelyn varmistamiseksi.

3 § (Tietosuojaperiaatteet) (1) Rekisterinpitäjän on määriteltävä nimenomaisesti tarkoitus, jota varten henkilötietoja käsitellään; henkilötietoja on kerättävä lainmukaisesti ja asianmukaisesti vain sen verran kuin on tarpeen tätä tarkoitusta varten.

(2) Rekisterinpitäjän on käsiteltävä henkilötietoja käsittelytarkoituksen kannalta asianmukaisella tavalla eikä se saa käyttää tietoja muihin tarkoituksiin.

(3) Rekisterinpitäjän on varmistettava, että henkilötiedot ovat täsmällisiä, täydellisiä ja ajantasaisia siltä osin kuin on tarpeen niiden tarkoitusten kannalta, joita varten tietoja käsitellään.

(4) Rekisterinpitäjän on hallinnoitava henkilötietoja turvallisesti ottaen huomioon muun muassa käsittelymenetelmät ja tietojen tyyppi sekä rekisteröidyn oikeuksien loukkaamisen mahdollisuus ja siihen liittyvien riskien vakavuus.

(5) Rekisterinpitäjän on julkistettava tietosuojaselosteensa ja muut henkilötietojen käsittelyyn liittyvät asiat; ja turvattava rekisteröidyn oikeudet, kuten oikeus tutustua omiin henkilötietoihinsa.

(6) Rekisterinpitäjän on käsiteltävä henkilötietoja niin, että voidaan minimoida mahdollisuus rekisteröidyn yksityisyyden loukkaamiseen.

(7) Jos henkilötietojen keräämisen tarkoitus on mahdollista saavuttaa käsittelemällä anonymisoituja tai pseudonymisoituja tietoja, rekisterinpitäjän on pyrittävä käsittelemään henkilötietoja anonymisoituina, jos se on mahdollista, tai pseudonymisoituina, jos käsittelytarkoitusta ei voida saavuttaa anonymisoitujen tietojen avulla.

(8) Rekisterinpitäjän on pyrittävä saamaan rekisteröidyn luottamus noudattamalla tietosuojalaissa ja muissa siihen liittyvissä säännöksissä säädettyjä velvollisuuksia ja vastuutehtäviä.

4 § (Rekisteröityjen oikeudet) Rekisteröidyllä on omien henkilötietojensa käsittelyn osalta seuraavat oikeudet:

1. oikeus saada tieto siitä, että hänen henkilötietojaan käsitellään;

2. oikeus päättää, suostuuko hän näiden henkilötietojen käsittelyyn, ja määrittää suostumuksen laajuus;

3. oikeus saada vahvistus sille, käsitelläänkö hänen henkilötietojaan, ja pääsyoikeus kyseisiin tietoihin (mukaan lukien oikeus saada jäljennös tiedoista; jäljempänä sovelletaan samaa);

4. oikeus keskeyttää tällaisten henkilötietojen käsittely ja pyytää tietojen oikaisemista, poistamista ja tuhoamista;

5. oikeus käyttää viipymättä ja oikeudenmukaisen menettelyn mukaisesti asianmukaisia oikeussuojakeinoja näiden henkilötietojen käsittelystä mahdollisesti aiheutuvien vahinkojen korjaamiseksi.

62 § (Oikeuksien loukkaamisesta ilmoittaminen) (1) Jokainen, jonka henkilötietoihin liittyviä oikeuksia tai etuja on loukattu rekisterinpitäjän suorittaman henkilötietojen käsittelyn yhteydessä, voi ilmoittaa asiasta tietosuojalautakunnalle.

(2) Tietosuojalautakunta voi nimetä erikoistuneen laitoksen, jonka tehtävänä on ottaa vastaan ja käsitellä tehokkaasti (1) kohdan nojalla tehdyt ilmoitukset, kuten presidentin asetuksessa säädetään. Tällaisissa tapauksissa erikoistuneen laitoksen on perustettava henkilötietoja koskevia tietoturvaloukkauksia käsittelevä puhelinpalvelu, jäljempänä 'Privacy Call Centre -puhelinpalvelu', ja vastattava se toiminnasta.

(3) Privacy Call Centre -puhelinpalvelu hoitaa seuraavia tehtäviä:

1. vastaanottaa ilmoituksia tietoturvaloukkauksista ja antaa neuvoja henkilötietojen käsittelystä;

2. tutkia turvapoikkeamia ja vahvistaa tarvittaessa, että sellainen on tapahtunut, ja kuulla osapuolten näkemyksiä;

3. tehtävät, jotka liittyvät 1 ja 2 alakohdissa mainittuihin tehtäviin.

(4) Tietosuojalautakunta voi tarvittaessa lähettää jäseniään virkamieslain (*State Public Officials Act*) 32-4 §:n 2 momentin nojalla nimettyyn erikoistuneeseen laitokseen varmistamaan, että 3 kohdan 2 alakohdassa tarkoitetut turvapoikkeamat tutkitaan ja vahvistetaan tehokkaasti.

(i) Henkilötietojen keräämistä kansalliseen turvallisuuteen liittyviä tarkoituksia varten säännellään erityislaeilla, joilla toimivaltaisille viranomaisille (esim. kansallinen tiedustelupalvelu) annetaan valtuudet kuunnella viestintää tai vaatia tietojen luovuttamista tietyin edellytyksin ja tiettyjä suojatoimia noudattaen, jäljempänä 'kansallista turvallisuutta koskevat lait'. Tällaisia kansallista turvallisuutta koskevia lakeja ovat muun muassa viestinnän tietosuojalaki (*Communications Privacy Protection Act*), yleistä turvallisuutta koskeva laki (ns. terrorismintorjuntalaki, *Act on Anti-Terrorism for the Protection of Citizens and Public Security*) ja televiestintäyrityksiä koskeva laki (*Telecommunications Business Act*). Lisäksi henkilötietojen keräämisessä ja myöhemmässä käsittelyssä on noudatettava tietosuojalain vaatimuksia. Tältä osin tietosuojalain 58 §:n 1 momentin 2 kohdassa säädetään, että sen III–VII lukua ei sovelleta henkilötietoihin, jotka kerätään tai joita pyydetään kansalliseen turvallisuuteen liittyvien tietojen analysointia varten. Näin ollen tätä osittaista poikkeusta sovelletaan silloin kun henkilötietoja käsitellään kansalliseen turvallisuuteen liittyviä tarkoituksia varten.

Toisaalta tällaiseen henkilötietojen käsittelyyn sovelletaan tietosuojalain I luvun (Yleiset säännökset), II luvun (Tietosuojapolitiikan laatiminen), VIII luvun (Tietoturvaloukkauksia koskeva ryhmäkanne), IX luvun (Täydentävät säännökset) ja X luvun (Seuraamukset) säännöksiä. Samoin sovelletaan tietosuojalain 3 §:ää (yleiset tietosuojaperiaatteet) ja 4 §:ää (rekisteröityjen oikeudet).

Lisäksi tietosuojalain 58 §:n 4 momentissa säädetään, että näitä tietoja on käsiteltävä vain sen verran kuin on tarpeen aiotun tarkoituksen saavuttamiseksi ja mahdollisimman lyhyen aikaa. Siinä myös edellytetään, että rekisterinpitäjä toteuttaa tarvittavat toimenpiteet turvallisen tiedonhallinnan ja asianmukaisen käsittelyn varmistamiseksi, kuten tekniset, hallinnolliset ja fyysiset suojatoimet sekä toimenpiteet yksilöiden valitusten asianmukaista käsittelyä varten.

Lisäksi sovelletaan tietosuojalautakunnan tehtäviä ja toimivaltaa koskevia säännöksiä (ml. tietosuojalain 60–65 §, joissa säädetään valitusten käsittelystä ja suositusten ja korjaavien toimenpiteiden hyväksymisestä) sekä hallinnollisia ja rikosoikeudellisia seuraamuksia koskevia säännöksiä (tietosuojalain 70 § ja sitä seuraavat pykälät). Tietosuojalain 7-8 §:n 1 momentin 3 ja 4 kohdan ja 7-9 §:n 1 momentin 5 kohdan mukaan nämä tutkintavaltuudet ja valtuudet määrätä korjaavia toimenpiteitä kattavat (myös valitusten käsittelyn yhteydessä) myös mahdolliset erityislakien säännösten rikkomiset. Näissä säännöksissä, joita sisältyy muun muassa kansallista turvallisuutta koskeviin lakeihin, säädetään henkilötietojen keräämistä koskevista rajoituksista ja suojatoimista. Kun otetaan huomioon tietosuojalain 3 §:n 1 momentissa säädetyt vaatimukset, joiden mukaan henkilötietojen keräämisen on tapahduttava lainmukaisesti ja asianmukaisesti, kyseessä on 63 ja 64 §:ssä tarkoitettu "tämän lain" rikkominen, minkä vuoksi tietosuojalautakunta voi suorittaa tutkintaa ja korjaavia toimenpiteitä ([11]). Näiden valtuuksien käyttö tietosuojalautakunnan toimesta täydentää, mutta ei korvaa kansallisesta ihmisoikeuskomissiosta annettuun lakiin (*Human Rights Commission Act*) perustuvia kansallisen ihmisoikeuskomission valtuuksia.

Tietosuojalain keskeisten periaatteiden, oikeuksien ja velvollisuuksien soveltaminen silloin kun henkilötietoja käsitellään kansalliseen turvallisuuteen liittyviä tarkoituksia varten perustuu perustuslaissa vahvistettuihin takeisiin, joilla suojataan yksilön oikeutta määrätä omista henkilötiedoistaan. Kuten perustuslakituomioistuin on todennut, tähän sisältyy yksilön oikeus ([12]) "päättää henkilökohtaisesti, kenelle tai kenen toimesta ja missä määrin hänen tietojaan luovutetaan tai käytetään. Kyseessä on perusoikeus ([13]), […], jonka tarkoituksena on suojata yksilön itsemääräämisoikeutta valtion toiminnan laajenemiseen ja tieto- ja viestintätekniikkaan liittyviltä riskeiltä". Kaikki tähän oikeuteen kohdistuvat rajoitukset, esimerkiksi silloin kun ne ovat tarpeen kansallisen turvallisuuden suojaamiseksi, edellyttävät sen vuoksi yksilön oikeuksien ja etujen tasapainottamista asiaa koskevan yleisen edun kanssa eivätkä ne saa missään tapauksessa vaikuttaa oikeuden olennaiseen sisältöön (perustuslain 37 §:n 2 momentti).

([11]) Tietosuojalain 64 §:ssä tarkoitettujen korjaavien toimenpiteiden osalta ks. edellä oleva 5 kohta.
([12]) Perustuslakituomioistuimen tuomio 99HunMa513, 2004HunMa190, 26.5.2005.
([13]) Perustuslakituomioistuimen tuomio 2003HunMa282, 21.7.2005.

Siksi rekisterinpitäjän (esim. kansallisen tiedustelupalvelun) on noudatettava muun muassa seuraavia vaatimuksia, kun se käsittelee henkilötietoja kansalliseen turvallisuuteen liittyviä tarkoituksia varten:

(1) Rekisterinpitäjän on täsmennettävä nimenomaisesti tarkoitukset, joita varten henkilötietoja käsitellään, ja kerättävä henkilötietoja lainmukaisesti ja asianmukaisesti vain sen verran kuin on tarpeen näitä tarkoituksia varten (tietosuojalain 3 §:n 1 momentti); rekisterinpitäjän on erityisesti kerättävä ja käsiteltävä henkilötietoja ainoastaan sellaisten velvoitteiden suorittamiseksi, jotka perustuvat asiaa koskeviin säännöksiin, kuten kansallisesta tiedustelupalvelusta annettuun lakiin;

(2) Henkilötietoja on käsiteltävä vain sen verran kuin on tarpeen aiotun tarkoituksen saavuttamiseksi ja mahdollisimman lyhyen aikaa (tietosuojalain 58 §:n 4 momentti); kun käsittelytarkoitus on saavutettu, rekisterinpitäjän on tuhottava henkilötiedot peruuttamattomasti, paitsi jos laissa nimenomaan annetaan valtuudet tietojen säilyttämiseen; siinä tapauksessa henkilötiedot on talletettava ja niitä on hallinnoitava erillään muista henkilötiedoista eikä niitä saa käyttää muuhun kuin asianomaisessa laissa täsmennettyyn tarkoitukseen, ja säilytysajan päätyttyä tiedot on tuhottava;

(3) Rekisterinpitäjän on käsiteltävä henkilötietoja käsittelytarkoituksen kannalta asianmukaisella tavalla eikä se saa käyttää tietoja muihin tarkoituksiin (tietosuojalain 3 §:n 2 momentti);

(4) Rekisterinpitäjän on varmistettava, että henkilötiedot ovat täsmällisiä, täydellisiä ja ajantasaisia siltä osin kuin on tarpeen niiden tarkoitusten kannalta, joita varten tietoja käsitellään (tietosuojalain 3 §:n 3 momentti);

(5) Rekisterinpitäjän on hallinnoitava henkilötietoja turvallisesti ottaen huomioon muun muassa käsittelymenetelmät ja tietojen tyyppi sekä rekisteröidyn oikeuksien loukkaamisen mahdollisuus ja siihen liittyvien riskien vakavuus (tietosuojalain 3 §:n 4 momentti);

(6) Rekisterinpitäjän on julkistettava tietosuojaselosteensa ja muut henkilötietojen käsittelyyn liittyvät asiat (tietosuojalain 3 §:n 5 momentti);

(7) Rekisterinpitäjän on käsiteltävä henkilötietoja niin, että voidaan minimoida rekisteröidyn yksityisyyden loukkaamisen mahdollisuus (tietosuojalain 3 §:n 6 momentti).

(ii) Tietosuojalain 58 §:n 4 momentin mukaan rekisterinpitäjän (esim. kansallisesta turvallisuudesta vastaava toimivaltainen viranomainen, kuten kansallinen tiedustelupalvelu) on toteutettava tarvittavat järjestelyt, kuten tekniset, hallinnolliset ja fyysiset suojatoimet, näiden periaatteiden noudattamisen ja henkilötietojen asianmukaisen käsittelyn varmistamiseksi. Tämä voi tarkoittaa esimerkiksi erityistoimenpiteitä, joilla varmistetaan henkilötietojen turvallisuus, kuten henkilötietoihin pääsyä koskevat rajoitukset ja valvonta, pääsylokit tai henkilötietojen käsittelyä koskevan erityiskoulutuksen antaminen työntekijöille.

Lisäksi rekisteröidyillä on tietosuojalain 3 §:n 5 momentin ja 4 §:n mukaisesti oltava seuraavat oikeudet, kun heidän henkilötietojaan käsitellään kansalliseen turvallisuuteen liittyviä tarkoituksia varten:

(1) Oikeus saada vahvistus siitä, että häntä koskevia henkilötietoja käsitellään tai että niitä ei käsitellä, ja oikeus saada tietoa käsittelystä ja pääsy kyseisiin henkilötietoihin, mukaan lukien jäljennös tiedoista (tietosuojalain 4 §:n 1 ja 3 momentti);

(2) Oikeus keskeyttää henkilötietojen käsittely ja pyytää niiden oikaisemista, poistamista ja tuhoamista (tietosuojalain 4 §:n 4 momentti).

(iii) Rekisteröity voi esittää pyynnön saada käyttää näitä oikeuksia joko suoraan rekisterinpitäjälle tai tietosuojalautakunnan välityksellä, tai valtuuttaa edustajansa tekemään niin. Kun rekisteröity esittää pyynnön, rekisterinpitäjän on myönnettävä oikeus viipymättä; se voi lykätä tai rajoittaa näiden oikeuksien käyttöä tai evätä sen, jos niin erikseen säädetään tai jos se on välttämätöntä muiden lakien noudattamiseksi, mutta vain siltä osin ja niin pitkäksi aikaa kuin se on tarpeen ja oikeasuhteista yleisen edun mukaisen tärkeän tavoitteen suojelemiseksi (esimerkiksi siltä osin ja niin kauan kuin oikeuden myöntäminen vaarantaisi meneillään olevan tutkinnan tai uhkaisi kansallista turvallisuutta), tai kun oikeuden myöntäminen voisi vahingoittaa kolmannen osapuolen henkeä tai terveyttä tai loukata oikeudettomasti kolmannen osapuolen omaisuutta ja muita etuja. Jos pyyntö evätään tai sitä rajoitetaan, rekisteröidylle on ilmoitettava syyt siihen viipymättä. Rekisterinpitäjän on laadittava menetelmä ja menettely, joiden avulla rekisteröidyt voivat esittää pyyntönsä, ja ilmoitettava niistä rekisteröidyille.

Lisäksi rekisteröidyillä on oltava oikeus asianmukaisiin oikeussuojakeinoihin tietosuojalain 58 §:n 4 momentin (vaatimus varmistaa, että rekisteröityjen valitukset käsitellään asianmukaisesti) ja 4 §:n 5 momentin (oikeus asianmukaisiin oikeussuojakeinoihin henkilötietojen käsittelystä mahdollisesti aiheutuvien vahinkojen korjaamiseksi) mukaisesti. Tähän sisältyy oikeus ilmoittaa väitetystä oikeuksien loukkauksesta tietoturvaloukkauksia käsittelevään puhelinpalveluun (tietosuojalain 62 §:n 3 momentin mukaisesti), oikeus tehdä valitus tietosuojalautakunnalle tietosuojalain 62 §:n nojalla mistä tahansa yksilön henkilötietoja koskevien oikeuksien tai etujen rikkomisesta ja oikeus hakea tuomioistuimessa muutosta tietosuojalautakunnan päätöksiin tai toimimatta jättämiseen hallinnollisista riita-asioista annetun lain nojalla (*Administrative Litigation Act*). Lisäksi rekisteröidyillä on oikeus saada oikeussuojaa tuomioistuimissa hallinnollisista riita-asioista annetun lain nojalla, jos jokin rekisterinpitäjän päätös tai toimimatta jättäminen (esim. henkilötietojen laiton kerääminen) on loukannut heidän oikeuksiaan tai etujaan, tai saada vahingonkorvaus valtion korvauksista annetun lain (*State Compensation Act*) mukaisesti. Nämä oikeussuojakeinot ovat käytettävissä myös silloin kun mahdollinen rikkominen koskee erityislakien säännöksiä (esim. kansallista turvallisuutta koskevien lakien säännöksiä, joissa säädetään henkilötietojen keräämistä koskevista rajoituksista ja suojatoimista) tai tietosuojalain säännöksiä.

EU:n yksilö voi tehdä valituksen Korean tietosuojalautakunnalle maansa kansallisen tietosuojaviranomaisen välityksellä, ja tietosuojalautakunta antaa ratkaisunsa tiedoksi kyseisen kansallisen tietosuojaviranomaisen kautta sen jälkeen kun se on tutkinut asian ja määrännyt tarvittaessa korjaavia toimenpiteitä.

LIITE II

18.5.2021

Vastaanottaja: Didier Reynders, oikeusasioista vastaava Euroopan komission jäsen

Arvoisa komissaari

Olen tyytyväinen Korean ja Euroopan komission rakentaviin keskusteluihin, joiden tarkoituksena on luoda puitteet henkilötietojen siirtämiselle EU:sta Koreaan.

Euroopan komission Korean hallitukselle esittämän pyynnön johdosta lähetän Teille oheisen asiakirjan, jossa esitetään yleiskatsaus oikeudelliseen kehykseen, jolla säännellään Korean viranomaisten pääsyä tietoihin.

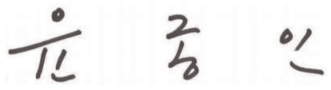
Asiakirja koskee Korean eri ministeriöitä ja virastoja (Korean tietosuojalautakunta, oikeusministeriö, kansallinen tiedustelupalvelu, kansallinen ihmisoikeuskomissio, kansallinen terrorismintorjuntakeskus ja kansallinen rahanpesun selvittelykeskus), ja kukin niistä on laatinut siitä asianomaisen osuuden oman toimivaltansa puitteissa. Jäljempänä luetellaan asiasta vastaavat ministeriöt ja virastot allekirjoituksineen.

Kaikki tätä asiakirjaa koskevat tiedustelut on toimitettava tietosuojalautakunnalle (*Personal Information Protection Commission*), joka koordinoi tarvittavat vastaukset asianomaisten ministeriöiden ja virastojen kanssa.

Toivon, että tästä asiakirjasta on hyötyä Euroopan komission päätöksenteossa.

Arvostan tähänastista suurta panostanne tämän asian edistämiseksi.

Kunnioittavasti

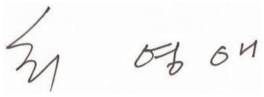


Yoon Jong In
Korean tietosuojalautakunnan puheenjohtaja

Tämän asiakirjan ovat laatineet tietosuojalautakunta sekä seuraavat ministeriöt ja virastot.

Park Jie Won
Kansallisen tiedustelupalvelun johtaja

Lee Jung Soo
Oikeusministeriön pääjohtaja



Choi Young Ae
Korean ihmisoikeuskomission puheenjohtaja

Kim Hyuck Soo
Kansallisen terrorismintorjuntakeskuksen johtaja

Kim, Jeong Kag
Korean rahanpesun selvittelykeskuksen jäsen

Oikeudellinen kehys Korean viranomaisten lainvalvontaan ja kansalliseen turvallisuuteen liittyvissä tarkoituksissa suorittamaa henkilötietojen keruuta ja käyttöä varten

Seuraavassa asiakirjassa tarkastellaan oikeudellista kehystä, jolla säännellään Korean viranomaisten lainvalvontaan ja kansalliseen turvallisuuteen liittyvissä tarkoituksissa suorittamaa henkilötietojen keruuta ja käyttöä, jäljempänä 'viranomaisten pääsy tietoihin', erityisesti käytettävissä olevien oikeusperustojen, sovellettavien ehtojen (rajoitukset) ja suojatoimien sekä riippumattoman valvonnan ja yksilöiden oikeussuojakeinojen osalta.

1. VIRANOMAISTEN PÄÄSYÄ TIETOIHIN KOSKEVAT YLEISET PERIAATTEET

1.1. Perustuslailliset puitteet

Korean tasavallan perustuslaissa säädetään yleisestä oikeudesta yksityisyyteen (17 §) ja erityisesti kirjesalaisuutta koskevasta oikeudesta (18 §). Valtion velvollisuutena on taata näiden perusoikeuksien toteutuminen ([1]). Perustuslain mukaan erityisesti perusoikeuksia ja -vapauksia voidaan rajoittaa ainoastaan lailla, silloin kun se on välttämätöntä kansallisen turvallisuuden, lain ja järjestyksen tai yleisen hyvinvoinnin turvaamiseksi ([2]). Silloin kun tällaisia rajoituksia sovelletaan, ne eivät kuitenkaan saa vaikuttaa vapauden tai oikeuden olennaiseen sisältöön ([3]). Korean tuomioistuimet ovat soveltaneet näitä säännöksiä asioissa, jotka koskevat viranomaisten puuttumista yksityisyydensuojaan. Korkein oikeus on muun muassa katsonut, että siviilien tarkkailu on loukannut yksityisyydensuojaa koskevaa perusoikeutta, ja korostanut, että "kansalaisilla on oikeus määrätä itse henkilötiedoistaan" ([4]). Toisessa asiassa perustuslakituomioistuin katsoi, että yksityisyys on perusoikeus, jolla suojataan kansalaisten yksityiselämää valtion puuttumiselta ja tarkkailulta ([5]).

Korean perustuslaissa taataan lisäksi, että ketään ei saa pidättää tai ottaa kiinni tai tehdä henkilöön kohdistuvaa etsintää eikä ketään saa kuulustella eikä keneltäkään saa takavarikoida omaisuutta muutoin kuin laissa säädetyin edellytyksin ([6]). Lisäksi etsinnän ja takavarikon suorittamista varten tarvitaan päätös, jonka tuomari voi antaa syyttäjän hakemuksesta, ja ne on suoritettava asianmukaista menettelyä noudattaen ([7]). Poikkeuksellisissa olosuhteissa, eli jos epäilty otetaan kiinni verekseltään (*flagrante delicto*), tai jos on olemassa vaara, että henkilö, jonka epäillään syyllistyneen rikokseen, josta voidaan määrätä vähintään kolme vuotta vankeutta, voi paeta tai hävittää todisteita, tutkintaviranomaiset voivat suorittaa etsinnän tai takavarikon ilman tuomioistuimen päätöstä; tällöin päätöstä on haettava jälkikäteen ([8]). Näitä yleisiä periaatteita täsmennetään edelleen erityislaeissa, jotka koskevat rikosprosessia ja viestinnän suojaamista (ks. jäljempänä yksityiskohtainen katsaus).

Ulkomaiden kansalaisten osalta perustuslaissa säädetään, että heidän asemansa taataan kansainvälisen oikeuden ja kansainvälisten sopimusten mukaisesti ([9]). Korea on osapuolena useissa kansainvälisissä sopimuksissa, joissa taataan oikeus yksityisyyteen, kuten kansalaisoikeuksia ja poliittisia oikeuksia koskeva kansainvälinen yleissopimus (17 §), yleissopimus vammaisten henkilöiden oikeuksista (22 §) ja yleissopimus lapsen oikeuksista (16 §). Lisäksi on huomattava, että vaikka perustuslaissa periaatteessa viitataan "*kansalaisiin*", perustuslakituomioistuin on todennut, että perusoikeudet koskevat myös ulkomaiden kansalaisia ([10]). Perustuslakituomioistuin on erityisesti katsonut, että ihmisarvon ja ihmisyyden suojelu sekä oikeus onnellisuuden tavoitteluun kuuluvat kaikille ihmisille eivätkä ainoastaan maan

([1]) Korean tasavallan perustuslain 10 §, vahvistettu 17 päivänä heinäkuuta 1948, jäljempänä 'perustuslaki'.
([2]) Perustuslain 37 §:n 2 momentti.
([3]) Perustuslain 37 §:n 2 momentti.
([4]) Korean korkeimman oikeuden päätös 96DA42789, 24.7.1998.
([5]) Perustuslakituomioistuimen päätös Ma51, 30.10.2003. Perustuslakituomioistuin katsoi vastaavasti päätöksessä 99Hun-Ma513 and 2004Hun-Ma190 (konsolidoitu), 26.5.2005, että "oikeudella määrätä omista henkilötiedoistaan tarkoitetaan rekisteröidyn oikeutta määrätä itse, milloin, kenelle tai kenen toimesta ja missä määrin hänen tietojaan luovutetaan tai käytetään. Vaikka sitä ei ole täsmennetty perustuslaissa, kyseessä on perusoikeus, jonka tarkoituksena on suojata yksilön itsemääräämisoikeutta valtion toiminnan laajenemiseen ja tieto- ja viestintätekniikkaan liittyviltä riskeiltä."
([6]) Perustuslain 12 §:n 1 momentti.
([7]) Perustuslain 16 § ja 12 §:n 3 momentti.
([8]) Perustuslain 12 §:n 3 momentti.
([9]) Perustuslain 6 §:n 2 momentti.
([10]) Perustuslakituomioistuimen päätös 93Hun-MA120, 29.12.1994. Ks. esimerkiksi perustuslakituomioistuimen päätös 2014Hun-Ma346 (31.5.2018), jossa tuomioistuin katsoi, että lentoasemalla pidätetyn Sudanin kansalaisen perustuslaillista oikeutta oikeusavustajaan oli loukattu. Toisessa asiassa perustuslakituomioistuin katsoi, että vapaus valita oma laillinen työpaikkansa liittyy läheisesti oikeuteen tavoitella onnellisuutta sekä ihmisarvoa koskevaan oikeuteen, minkä vuoksi se ei koske ainoastaan kansalaisia vaan voidaan taata myös Korean tasavallassa laillisesti työskenteleville ulkomaiden kansalaisille (perustuslakituomioistuimen päätös 2007Hun-Ma1083, 29.9.2011).

kansalaisille ([11]). Perustuslakituomioistuin on myös selventänyt, että oikeus määrätä omista tiedoistaan on perusoikeus, joka on johdettavissa oikeudesta ihmisarvoon, onnellisuuden tavoitteluun ja yksityiselämään ([12]). Vaikka oikeuskäytännössä ei ole tähän mennessä käsitelty erikseen muiden kuin Korean kansalaisten oikeutta yksityisyyteen, oikeusoppineet ovat laajalti sitä mieltä, että perustuslain 12-22 § (jossa säädetään sekä oikeudesta yksityisyyteen että henkilökohtaiseen vapauteen) koskee ”ihmisten oikeuksia”.

Perustuslaissa säädetään myös oikeudesta vaatia viranomaisilta oikeudenmukaista korvausta ([13]). Lisäksi jokaisella, jonka perustuslaillisia oikeuksia on loukattu julkisen vallan käytön seurauksena (tuomioistuinten tuomioita lukuun ottamatta), on perustuslakituomioistuimesta annetun lain nojalla oikeus tehdä perustuslakivalitus perustuslakituomioistuimeen ([14]).

1.2. **Yleiset tietosuojasäännöt**

Korean tasavallan yleistä tietosuojalakia (*Personal Information Protection Act*) sovelletaan sekä yksityiseen että julkiseen sektoriin. Tietosuojalaissa viitataan nimenomaisesti viranomaisten velvollisuuteen laatia politiikkatoimenpiteitä, joiden avulla voidaan estää ”henkilötietojen väärinkäyttö, epäasianmukainen tarkkailu ja seuraaminen jne. sekä taata ihmisarvo ja oikeus yksityisyyteen” ([15]).

Henkilötietojen käsittelyssä lainvalvontatarkoituksia varten sovelletaan kaikkia tietosuojalain vaatimuksia. Tämä tarkoittaa esimerkiksi sitä, että lainvalvontaviranomaisten on noudatettava lainmukaisen käsittelyn vaatimusta, eli ne voivat kerätä, käyttää tai luovuttaa henkilötietoja vain jonkin tietosuojalaissa (15-18 §) mainitun oikeusperustan nojalla. Lisäksi niiden on noudatettava periaatteita, jotka koskevat käyttötarkoituksen rajoittamista (3 §:n 1 ja 2 momentti), oikeasuhteisuutta / tietojen minimointia (3 §:n 1 ja 6 momentti), säilytysajan rajoittamista (21 §), tietoturvallisuutta ja tietoturvaloukkauksista ilmoittamista (3 §:n 4 momentti, 29 ja 34 §) sekä käsittelyn läpinäkyvyyttä (3 §:n 1 ja 5 momentti sekä 20, 30 ja 32 §). Arkaluonteisten tietojen osalta sovelletaan erityisiä suojatoimia (23 §). Lisäksi yksilöt voivat tietosuojalain 3 §:n 5 momentin ja 4 §:n sekä 35–39-2 §:n nojalla käyttää suhteessa lainvalvontaviranomaisiin oikeuttaan saada pääsy omiin tietoihinsa ja oikeutta oikaista ja poistaa ne tai keskeyttää niiden käsittely.

Vaikka tietosuojalakia sovelletaan kaikilta osin henkilötietojen käsittelyssä lainvalvontatarkoituksiin, siihen sisältyy poikkeus, joka koskee henkilötietojen käsittelyä kansalliseen turvallisuuteen liittyviä tarkoituksia varten. Tältä osin tietosuojalain 58 §:n 1 momentin 2 kohdassa säädetään, että lain 15–50 §:ää ei sovelleta henkilötietoihin, jotka kerätään tai joita pyydetään kansalliseen turvallisuuteen liittyvien tietojen analysointia varten ([16]). Toisaalta myös tällöin sovelletaan edelleen tietosuojalain I luvun (Yleiset säännökset), II luvun (Tietosuojapolitiikan laatiminen), VIII luvun (Tietoturvaloukkauksia koskeva ryhmäkanne), IX luvun (Täydentävät säännökset) ja X luvun (Seuraamukset) säännöksiä. Samoin sovelletaan tietosuojalain 3 §:ää (yleiset tietosuojaperiaatteet) ja 4 §:ää (rekisteröityjen oikeudet). Tämä tarkoittaa, että keskeiset periaatteet ja oikeudet taataan myös tällä alalla. Lisäksi tietosuojalain 58 §:n 4 momentissa säädetään, että näitä tietoja on käsiteltävä vain sen verran kuin on tarpeen aiotun tarkoituksen saavuttamiseksi ja mahdollisimman lyhyen aikaa. Siinä myös edellytetään, että rekisterinpitäjä toteuttaa tarvittavat toimenpiteet turvallisen tiedonhallinnan ja asianmukaisen käsittelyn varmistamiseksi, kuten tekniset, hallinnolliset ja fyysiset suojatoimet sekä toimenpiteet yksilöiden valitusten asianmukaista käsittelyä varten.

Korean tietosuojalautakunta (*Personal Information Protection Commission*) on antanut asiakirjassa *Notification No. 2021-1 on Supplementary rules for the interpretation and application of the Personal Information Protection Act*, jäljempänä ’ilmoitus N:o 2021-1’, täydentäviä sääntöjä tietosuojalain tulkinnasta ja soveltamisesta. Siinä täsmennetään myös tämän osittaisen poikkeuksen valossa sitä, miten tietosuojalakia sovelletaan, kun henkilötietoja käsitellään kansalliseen turvallisuuteen liittyviä tarkoituksia varten ([17]). Tämä koskee erityisesti yksilöiden oikeuksia (pääsy tietoihin ja oikeus oikaista ja poistaa ne tai keskeyttää niiden käsittely) ja niihin mahdollisesti kohdistuvien rajoitusten perusteita ja rajaamista. Ilmoituksen N:o 2021-1 mukaan tietosuojalain keskeisten periaatteiden, oikeuksien ja velvollisuuksien soveltaminen silloin kun henkilötietoja käsitellään kansalliseen turvallisuuteen liittyviä tarkoituksia varten perustuu perustuslaissa

([11]) Perustuslakituomioistuimen päätös 99HeonMa494, 29.11.2001.
([12]) Ks. esim. perustuslakituomioistuimen päätös 99HunMa513.
([13]) Perustuslain 29 §:n 1 momentti.
([14]) Perustuslakituomioistuimesta annetun lain 68 §:n 1 momentti.
([15]) Tietosuojalain 5 §:n 1 momentti.
([16]) Tietosuojalain 58 §:n 1 momentin 2 kohta.
([17]) Tietosuojalautakunnan asiakirja *Notification No. 2021-1 on Supplementary rules for the interpretation and application of the Personal Information Protection Act*, kohta III, 6.

vahvistettuihin takeisiin, joilla suojataan yksilön oikeutta määrätä omista henkilötiedoistaan. Kaikki tähän oikeuteen kohdistuvat rajoitukset, esimerkiksi silloin kun ne ovat tarpeen kansallisen turvallisuuden suojaamiseksi, edellyttävät sen vuoksi yksilön oikeuksien ja etujen tasapainottamista asiaa koskevan yleisen edun kanssa eivätkä ne saa missään tapauksessa vaikuttaa oikeuden olennaiseen sisältöön (perustuslain 37 §:ñn 2 momentti).

2. VIRANOMAISTEN PÄÄSY TIETOIHIN LAINVALVONTATARKOITUKSISSA

2.1. Toimivaltaiset lainvalvontaviranomaiset

Poliisi, syyttäjät ja tuomioistuimet voivat kerätä henkilötietoja lainvalvontatarkoituksiin rikosprosessilain (*Criminal Procedure Act*), viestinnän tietosuojalain (*Communications Privacy Protection Act*) ja televiestintäyrityksiä koskevan lain (*Telecommunications Business Act*) nojalla. Siltä osin kuin nämä valtuudet on annettu myös kansalliselle tiedustelupalvelulle sitä koskevalla lailla, sen on noudatettava edellä mainittuja lakeja ([18]). Tiettyjen rahoitustoimien raportoinnista ja käytöstä annettu laki (*Act on Reporting and Using Specified Financial Transaction Information*) tarjoaa oikeusperustan, jonka nojalla rahoituslaitokset voivat luovuttaa tietoja Korean rahanpesun selvittelykeskukselle, jäljempänä 'KOFIU', rahanpesun ja terrorismin rahoittamisen ehkäisemiseksi. Tämä erikoistunut virasto voi puolestaan luovuttaa tällaisia tietoja lainvalvontaviranomaisille. Luovutusvelvollisuus koskee kuitenkin ainoastaan niitä rekisterinpitäjiä, jotka käsittelevät henkilötietoja luottotietolain nojalla ja jotka kuuluvat rahoitusvalvontakomission valvonnan piiriin. Koska tällaisten rekisterinpitäjien suorittama henkilökohtaisten luottotietojen käsittely ei kuulu tietosuojan riittävyyttä koskevan päätöksen soveltamisalaan, tässä asiakirjassa ei esitellä tarkemmin rahoitustoimia koskevasta raportoinnista annetun lain nojalla sovellettavia rajoituksia ja suojatoimia.

2.2. Oikeusperustat ja rajoitukset

Rikosprosessilaissa (ks. kohta 2.2.1), viestinnän tietosuojalaissa (ks. kohta 2.2.2) ja televiestintäyrityksiä koskevassa laissa (ks. kohta 2.2.3) vahvistetaan sekä oikeusperustat henkilötietojen keräämiselle lainvalvontatarkoituksiin että sovellettavat rajoitukset ja suojatoimet.

2.2.1. *Etsinnät ja takavarikot*

2.2.1.1. Oikeusperusta

Syyttäjät ja ylemmät poliisivirkamiehet voivat tarkastaa esineitä, suorittaa henkilöön kohdistuvaa etsintää tai takavarikoida esineitä vain jos 1) asianomaisen henkilön epäillään syyllistyneen rikokseen (rikosepäilty), 2) se on tarpeen tutkinnan edistämiseksi ja 3) kyseisten esineiden tai henkilöiden katsotaan liittyvän tapaukseen ([19]). Myös tuomioistuimet voivat suorittaa etsintöjä ja takavarikoida mitä tahansa esineitä, joita voidaan käyttää todisteena tai mahdollisesti tuomita menetetyksi, kunhan kyseisten esineiden tai henkilöiden katsotaan liittyvän tiettyyn tapaukseen ([20]).

2.2.1.2. Rajoitukset ja suojatoimet

Yleisen velvoitteen nojalla syyttäjien ja poliisin virkamiesten on noudatettava rikosepäillyn ja kaikkien muidenkin asianomaisten henkilöiden ihmisoikeuksia ([21]). Lisäksi tutkinnan tavoitteen saavuttamiseksi voidaan käyttää pakkokeinoja vain jos niistä on säädetty nimenomaisesti rikosprosessilaissa ja vain sen verran kuin on välttämätöntä ([22]).

Poliisi ja syyttäjä voivat suorittaa etsintöjä, tarkastuksia ja takavarikkoja osana rikostutkintaa vain tuomioistuimen päätöksen perusteella ([23]). Kun viranomainen hakee tällaista päätöstä, sen on esitettävä todisteet, jotka osoittavat, miksi kyseistä henkilöä epäillään rikoksesta ja miksi etsintä, tarkastus tai takavarikko on tarpeen, ja että takavarikoitavaksi ehdotetut esineet ovat olemassa ([24]). Päätöksessä on täsmennettävä muun muassa rikosepäillyn nimi ja rikos, josta häntä epäillään; paikka, henkilö ja etsityt tai takavarikoitavat esineet; päätöksen antamispäivä; ja soveltamisaika ([25]). Myös silloin kun etsintä tai takavarikko on suoritettava osana meneillään olevaa oikeudenkäyntiä muutoin kuin julkisessa oikeudenistunnossa, niitä varten on saatava etukäteen tuomioistuimen päätös ([26]). Asianomaiselle ja hänen puolustusasianajajalleen ilmoitetaan etsinnästä tai takavarikosta etukäteen, ja he voivat olla läsnä kun päätös pannaan täytäntöön ([27]).

([18]) Ks. kansallisesta tiedustelupalvelusta annetun lain (laki N:o 12948) 3 §, jossa viitataan tiettyjä rikoksia, kuten kapinointia ja kansalliseen turvallisuuteen liittyviä rikoksia (kuten vakoilua) koskevaan rikostutkintaan. Tällöin olisi noudatettava rikosprosessilaissa säädettyjä etsintää ja takavarikkoa koskevia menettelyjä, kun taas viestinnän tietosuojalain nojalla säänneltäisiin viestintätietojen keräämistä (ks. osa 3, jossa tarkastellaan viestintätietoihin pääsyä kansalliseen turvallisuuteen liittyviä tarkoituksia varten).
([19]) Rikosprosessilain 215 §:n 1 ja 2 momentti.
([20]) Rikosprosessilain 106 §:n 1 momentti sekä 107 ja 109 §.
([21]) Rikosprosessilain 198 §:n 2 momentti.
([22]) Rikosprosessilain 199 §:n 1 momentti.
([23]) Rikosprosessilain 215 §:n 1 ja 2 momentti.
([24]) Rikosprosessista annetun asetuksen 108 §:n 1 momentti.
([25]) Rikosprosessilain 114 §:n 1 momentti yhdessä sen 219 §:n kanssa.
([26]) Rikosprosessilain 113 §.
([27]) Rikosprosessilain 121 ja 122 §.

Jos etsinnän tai takavarikon kohteena on tietokoneen kovalevy tai muu tallennusväline, periaatteessa takavarikko voi koskea ainoastaan tarvittavia tietoja (jotka kopioidaan tai tulostetaan) eikä koko tallennusvälinettä ([28]). Tallennusväline voidaan takavarikoida vain jos katsotaan, että tarvittavien tietojen tulostaminen tai kopioiminen erikseen olisi käytännössä mahdotonta tai että etsinnän tarkoituksen toteuttaminen muulla tavoin olisi käytännössä mahdotonta ([29]). Asianomaiselle on ilmoitettava takavarikosta viipymättä ([30]). Tähän ilmoitusvaatimukseen ei ole säädetty poikkeuksia rikosprosessilaissa.

Etsintöjä, tarkastuksia ja takavarikkoja voidaan suorittaa ilman päätöstä vain rajoitetuissa tilanteissa. Näin on ensinnäkin silloin kun päätöksen saaminen on mahdotonta siksi, että asia on hoidettava rikospaikalla kiireellisesti ([31]). Siinä tapauksessa päätös on kuitenkin pyydettävä jälkikäteen viipymättä ([32]). Toiseksi etsintöjä ja tarkastuksia voidaan suorittaa ilman päätöstä, kun rikosepäilty pidätetään tai otetaan kiinni rikospaikalla ([33]). Syyttäjä tai ylempi poliisivirkamies voi myös takavarikoida esineen ilman päätöstä, jos rikosepäilty tai kolmas henkilö on heittänyt sen pois tai luovuttaa sen vapaaehtoisesti ([34]).

Rikosprosessilain vastaisesti hankittu näyttö hylätään ([35]). Lisäksi rikoslaissa (*Criminal Act*) säädetään, että henkilön asunnon, vartioidun rakennuksen, rakennelman, auton, veneen, ilma-aluksen tai asuinhuoneen laittomasta etsinnästä voidaan määrätä vankeutta enintään kolme vuotta ([36]). Tätä säännöstä sovelletaan myös silloin kun esineitä, kuten tallennusvälineitä, takavarikoidaan laittoman etsinnän yhteydessä.

2.2.2. *Viestintätietojen kerääminen*

2.2.2.1. Oikeusperusta

Viestintätietojen keruuta säännellään erityisellä säädöksellä, viestinnän tietosuojalailla. Viestinnän tietosuojalaissa kielletään erityisesti viestien sensurointi, telekuuntelu, televalvontatietojen toimittaminen ja muiden henkilöiden välisen eijulkisen keskustelun tallentaminen tai kuunteleminen muutoin kuin rikosprosessilain, viestinnän tietosuojalain tai sotilastuomioistuinlain nojalla ([37]). Viestinnän tietosuojalaissa käytetty ilmaisu *"viestintä"* kattaa sekä tavallisen postin että televiestinnän ([38]). Viestinnän tietosuojalaissa erotetaan tältä osin toisistaan *"yhteydenpidon rajoittaminen"* ([39]) ja *"televalvontatietojen"* kerääminen.

Yhteydenpidon rajoittamisella tarkoitetaan sekä "sensuuria", eli perinteisen postilähetyksen sisällön haltuunottoa, että "telekuuntelua" eli televiestinnän sisällön välitöntä sieppaamista (hankkimista tai tallentamista) ([40]). Televalvontatiedoilla (*communication confirmation data*) tarkoitetaan televiestintään liittyviä teknisiä tietoja, joista käy ilmi televiestinnän päivämäärä, alkamis- ja päättymisaika, lähtevien ja saapuvien puhelujen määrä sekä toisen osapuolen tilaajanumero, käyttötiheys, televiestintäpalvelujen käyttöä koskevat lokitiedostot ja paikkatiedot (esimerkiksi tukiasema, josta signaalit on vastaanotettu) ([41]).

([28]) Rikosprosessilain 106 §:n 3 momentti.
([29]) Rikosprosessilain 106 §:n 3 momentti.
([30]) Rikosprosessilain 219 § yhdessä sen 106 §:n 4 momentin kanssa.
([31]) Rikosprosessilain 216 §:n 3 momentti.
([32]) Rikosprosessilain 216 §:n 3 momentti.
([33]) Rikosprosessilain 216 §:n 1 ja 2 momentti.
([34]) Rikosprosessilain 218 §. Henkilötietojen osalta tämä kattaa vain tilanteen, jossa asianomainen luovuttaa itse tietojaan vapaaehtoisesti. Jos kyse on rekisterinpitäjän hallussa olevista tiedoista, niiden hankinta edellyttää erityistä tietosuojalakiin sisältyvää oikeusperustaa. Vapaaehtoisesti luovutetut esineet hyväksytään todisteiksi oikeudenkäynnissä vain jos ei ole perusteltua epäilystä luovutuksen vapaaehtoisuudesta, mikä syyttäjän on osoitettava. Ks. korkeimman oikeuden päätös 2013Do11233, 10.3.2016.
([35]) Rikosprosessilain 308-2 §.
([36]) Rikoslain 321 §.
([37]) Viestinnän tietosuojalain 3 §. Sotilastuomioistuinlailla (*Military Court Act*) säännellään periaatteessa sotilashenkilöstöä koskevien tietojen keräämistä, ja sitä voidaan soveltaa siviilihenkilöihin vain rajoitetuissa tapauksissa (esim. jos sotilas- ja siviilihenkilöt tekevät rikoksen yhdessä, tai jos henkilö tekee rikoksen puolustusvoimia vastaan, menettely voidaan panna vireille sotilastuomioistuimessa, ks. lain 2 §). Etsintää ja takavarikkoa koskevat yleiset säännökset ovat samanlaiset kuin rikosprosessilaissa, ks. esim. sotilastuomioistuinlain 146–149 ja 153–156 §. Esimerkiksi postilähetys voidaan ottaa haltuun vain jos se on tarpeen tutkintaa varten ja sotilastuomioistuimen päätöksen nojalla. Siltä osin kuin on kyse sähköisen viestinnän keräämisestä, sovelletaan viestinnän tietosuojalaissa säädettyjä rajoituksia ja suojatoimia.
([38]) Viestinnän tietosuojalain 2 §:n 1 momentti: *"kaikenlaisten äänien, sanojen, symbolien tai kuvien lähettäminen ja vastaanottaminen langallisella tai langattomalla yhteydellä, kuitukaapelilla tai muulla sähkömagneettisella järjestelmällä, mukaan lukien puhelin, sähköposti, jäsenyyteen perustuva viestipalvelu, faksi ja kaukohakupalvelu"*.
([39]) Viestinnän tietosuojalain 2 §:n 7 momentti ja 3 §:n 2 momentti.
([40]) "Sensuurilla" tarkoitetaan 'viestin avaamista ilman asianomaisen suostumusta tai sen sisällön selvittämistä, tallentamista tai pidättämistä muulla tavoin' (viestinnän tietosuojalain 2 §:n 6 momentti). "Telekuuntelulla" tarkoitetaan 'televiestinnän sisällön hankkimista tai tallentamista kuuntelemalla tai lukemalla yhteisesti viestintään sisältyviä ääniä, sanoja, symboleita tai kuvia elektronisin ja mekaanisin laittein ilman asianomaisen suostumusta tai puuttumalla viestinnän lähettämiseen ja vastaanottamiseen' (viestinnän tietosuojalain 2 §:n 7 momentti).
([41]) Viestinnän tietosuojalain 2 §:n 11 momentti.

Viestinnän tietosuojalaissa säädetään molempien tietotyyppien keräämiseen sovellettavista rajoituksista ja suojatoimista. Monien vaatimusten osalta säädetään, että niiden laiminlyönti voi johtaa rikosoikeudellisiin seuraamuksiin ([42]).

2.2.2.2. Viestinnän sisällön keräämiseen sovellettavat rajoitukset ja suojatoimet (yhteydenpidon rajoittamista koskevat toimenpiteet)

Viestinnän sisällön kerääminen sallitaan vain täydentävänä keinona rikostutkinnan helpottamiseksi (eli viimesijaisena keinona), ja silloinkin on pyrittävä minimoimaan viestintäsalaisuuteen puuttuminen ([43]). Tämän yleisen periaatteen mukaisesti yhteydenpidon rajoittamista koskevia toimenpiteitä voidaan toteuttaa vain jos rikoksen estäminen, rikollisen pidättäminen tai todisteiden kerääminen olisi muutoin vaikeaa ([44]). Lainvalvontaviranomaisten on lopetettava viestinnän sisällön kerääminen heti kun jatkuvaa pääsyä näihin tietoihin ei enää katsota tarpeelliseksi, jotta voidaan varmistaa, että viestinnän yksityisyyttä loukataan mahdollisimman vähän ([45]).

Lisäksi yhteydenpidon rajoittamista voidaan käyttää vain jos on olemassa merkittävä syy epäillä, että suunnitteilla on tiettyjä viestinnän tietosuojalaissa erikseen lueteltuja vakavia rikoksia tai että sellaisia rikoksia on tehty. Tällaisia rikoksia ovat esimerkiksi kapina, huumerikokset ja räjähdysainerikokset sekä kansalliseen turvallisuuteen, diplomaattisuhteisiin tai sotilastukikohtiin ja sotilaallisiin laitoksiin liittyvät rikokset ([46]). Yhteydenpidon rajoittamisen tulee kohdistua tiettyihin postilähetyksiin tai viesteihin, jotka epäilty on lähettänyt tai vastaanottanut, tai epäillyn määrätyn ajan kuluessa lähettämiin tai vastaanottamiin postilähetyksiin tai viesteihin ([47]).

Myös silloin kun nämä vaatimukset täyttyisivät, sisällön keräämiseen vaaditaan tuomioistuimen päätös. Syyttäjä voi erityisesti pyytää tuomioistuinta antamaan luvan sisältötietojen keräämiseen henkilöltä, jota epäillään rikoksesta tai joka on tutkinnan kohteena ([48]). Myös poliisi voi pyytää tällaista lupaa syyttäjältä, joka vuorostaan pyytää tuomioistuinta tekemään asiaa koskevan päätöksen ([49]). Hakemus on tehtävä kirjallisesti ja siinä on mainittava tietyt seikat. Hakemuksessa on erityisesti kuvailtava 1) olennaiset syyt, joiden vuoksi on perusteltua epäillä, että jokin luettelossa mainittu rikos on suunnitteilla tai että sitä toteutetaan tai että se on tehty, sekä mahdollinen näyttö; 2) yhteydenpidon rajoittamista koskevat toimenpiteet sekä niiden kohde, soveltamisala, tarkoitus ja voimassaoloaika; ja 3) paikka, jossa toimenpiteet on tarkoitus toteuttaa, sekä toteuttamistapa ([50]).

Jos oikeudelliset vaatimukset täyttyvät, tuomioistuin voi antaa kirjallisen luvan toteuttaa yhteydenpidon rajoittamista koskevia toimenpiteitä epäillyn tai tutkinnan kohteena olevan henkilön osalta ([51]). Päätöksessä on täsmennettävä toimenpiteiden tyyppi sekä niiden kohde, soveltamisala, voimassaoloaika, toteuttamispaikka ja -tapa ([52]).

Yhteydenpidon rajoittamista koskevia toimenpiteitä saa toteuttaa enintään kahden kuukauden ajan ([53]). Jos toimenpiteiden tavoite saavutetaan aikaisemmin kyseisen ajan kuluessa, toimenpiteet on lopetettava välittömästi. Toisaalta jos vaaditut edellytykset täyttyvät edelleen, mainitun kahden kuukauden määräajan puitteissa on mahdollista hakea toimenpiteiden voimassaoloajan pidentämistä. Hakemuksessa on esitettävä näyttö, jonka nojalla toimenpiteiden jatkaminen vaikuttaa perustellulta ([54]). Pidennetty voimassaoloaika saa olla yhteensä enintään vuoden, tai kolme vuotta kun on kyse tietyistä erityisen vakavista rikoksista (esim. kapinaan, ulkomaiseen hyökkäykseen tai kansalliseen turvallisuuteen liittyvät rikokset) ([55]).

Lainvalvontaviranomaiset voivat vaatia televiestintäpalvelujen tarjoajia avustamaan toimenpiteiden toteuttamisessa esittämällä näille tuomioistuimen kirjallisen luvan ([56]). Televiestintäpalvelujen tarjoajien on tehtävä viranomaisten kanssa yhteistyötä ja säilytettävä saamansa lupa tiedostoissaan ([57]). Ne voivat kieltäytyä yhteistyöstä, jos tuomioistuimen kirjallisessa luvassa esitetyt kohdehenkilön tiedot (esimerkiksi puhelinnumero) ovat virheellisiä. Lisäksi ne eivät missään tapauksessa saa paljastaa televiestinnässä käytettäviä salasanoja ([58]).

([42]) Viestinnän tietosuojalain 16 ja 17 §. Tämä koskee esimerkiksi tietojen keräämistä ilman tuomioistuimen päätöstä, kirjanpidon laiminlyöntiä, keruun jatkamista myös sen jälkeen kun tilanne ei enää ole kiireellinen ja asianomaiselle tehtävän ilmoituksen laiminlyöntiä.
([43]) Viestinnän tietosuojalain 3 §:n 2 momentti.
([44]) Viestinnän tietosuojalain 5 §:n 1 momentti.
([45]) Viestinnän tietosuojalain täytäntöönpanoasetuksen 2 §.
([46]) Viestinnän tietosuojalain 5 §:n 1 momentti.
([47]) Viestinnän tietosuojalain 5 §:n 2 momentti.
([48]) Viestinnän tietosuojalain 6 §:n 1 momentti.
([49]) Viestinnän tietosuojalain 6 §:n 2 momentti.
([50]) Viestinnän tietosuojalain 6 §:n 4 momentti ja sen täytäntöönpanoasetuksen 4 §:n 1 momentti.
([51]) Viestinnän tietosuojalain 6 §:n 5 momentti ja 8 momentti.
([52]) Viestinnän tietosuojalain 6 §:n 6 momentti.
([53]) Viestinnän tietosuojalain 6 §:n 7 momentti.
([54]) Viestinnän tietosuojalain 6 §:n 7 momentti.
([55]) Viestinnän tietosuojalain 6 §:n 8 momentti.
([56]) Viestinnän tietosuojalain 9 §:n 2 momentti.
([57]) Viestinnän tietosuojalain 15-2 § ja sen täytäntöönpanoasetuksen 12 §.
([58]) Viestinnän tietosuojalain 9 §:n 4 momentti.

Kaikkien, jotka toteuttavat yhteydenpidon rajoittamista koskevia toimenpiteitä, tai joita vaaditaan tekemään sitä varten yhteistyötä, on pidettävä kirjaa toimenpiteiden tavoitteista, niiden toteuttamisesta, yhteistyöhön liittyvistä päivämääristä ja kohteesta ([59]). Myös tällaisia toimenpiteitä toteuttavien lainvalvontaviranomaisten on kirjattava ylös toimenpiteiden yksityiskohdat ja saavutetut tulokset ([60]). Poliisin on toimitettava nämä tiedot syyttäjälle tutkinnan päätteeksi annettavassa raportissa ([61]).

Kun syyttäjä nostaa syytteen asiassa, jossa on käytetty yhteydenpidon rajoittamista koskevia toimenpiteitä, tai päättää olla syyttämättä tai pidättämättä asianomaista henkilöä (eli kyseessä ei ole vain syytetoimien keskeyttäminen), syyttäjän on ilmoitettava asianomaiselle, että häneen on kohdistettu yhteydenpidon rajoittamista koskevia toimenpiteitä, ja toimenpiteiden toteuttaja ja toteuttamisaika. Ilmoitus on annettava 30 päivän kuluessa päätöksen tekemisestä ([62]). Ilmoittamista voidaan lykätä, jos se todennäköisesti aiheuttaisi vakavaa vaaraa kansalliselle turvallisuudelle tai häiritsisi yleistä turvallisuutta ja järjestystä tai jos se todennäköisesti aiheuttaisi aineellista vahinkoa muiden ihmisten hengelle ja terveydelle ([63]). Jos syyttäjä tai poliisi aikoo lykätä ilmoittamista, siihen on saatava piirisyyttäjänviraston päällikön lupa ([64]). Ilmoitus on annettava 30 päivän kuluessa siitä kun lykkäämisen perusteet lakkaavat olemasta ([65]).

Viestinnän tietosuojalaissa säädetään myös erityisestä menettelystä viestinnän sisällön keräämiseksi hätätilanteissa. Lainvalvontaviranomaiset voivat kerätä viestinnän sisältöä etenkin jos järjestäytyneen rikollisuuden tai muun vakavan rikoksen suunnittelu tai toteuttaminen uhkaa välittömästi aiheuttaa kuoleman tai vakavan vamman, eikä tilanteen kiireellisyyden vuoksi ole mahdollista noudattaa (edellä esitettyä) sääntöjenmukaista menettelyä ([66]). Tällaisessa hätätilanteessa poliisi tai syyttäjä voi toteuttaa yhteydenpidon rajoittamista koskevia toimenpiteitä ilman tuomioistuimen ennakkolupaa, mutta sitä on haettava välittömästi toimenpiteiden toteuttamisen jälkeen. Jos lainvalvontaviranomainen ei saa tuomioistuimen lupaa 36 tunnin kuluessa kiireellisten toimenpiteiden toteuttamisesta, tietojen kerääminen on lopetettava välittömästi ja kerätyt tiedot on yleensä tuhottava ([67]). Poliisit toteuttavat tällaisia kiireellisiä tarkkailutoimenpiteitä syyttäjän valvonnassa, tai jos syyttäjän ohjeita ei ole mahdollista saada etukäteen tilanteen kiireellisyyden takia, poliisin on saatava toimille syyttäjän hyväksyntä välittömästi sen jälkeen kun niiden toteuttaminen on aloitettu ([68]). Edellä kuvattuja asianomaiselle henkilölle ilmoittamista koskevia sääntöjä sovelletaan myös silloin kun viestinnän sisältöä on kerätty hätätilanteessa.

Hätätilanteessa tietojen keräämisen on aina tapahduttava ”hätätilanteen sensuuria/kuuntelua koskevan lausunnon” mukaisesti, ja tiedot keräävän viranomaisen on pidettävä kirjaa kaikista hätätoimenpiteistä ([69]). Tuomioistuimelle esitettävään hätätoimenpiteitä koskevaan hakemukseen on liitettävä asiakirja, jossa kuvataan yhteydenpidon rajoittamista koskevat toimenpiteet, niiden kohde ja tavoite, soveltamisala ja toteuttamisaika, -paikka ja -tapa ja selvitys siitä, miten toimenpiteet täyttävät viestinnän tietosuojalain 5 §:n 1 momentissa asetetut vaatimukset ([70]) sekä tarvittavat asiakirjatodisteet.

Jos hätätoimenpiteet saadaan päätökseen lyhyessä ajassa, niin että tuomioistuimen lupaa ei ehditä saada (esimerkiksi jos epäilty pidätetään välittömästi kuuntelun aloittamisen jälkeen, joka sen vuoksi lopetetaan), toimivaltaisen syyttäjänviraston päällikkö antaa toimivaltaiselle tuomioistuimelle tiedoksi ilmoituksen hätätoimenpiteen toteuttamisesta ([71]). Ilmoituksessa on esitettävä tietojen keräämisen tavoite, kohde, soveltamisala, kesto, toteuttamispaikka ja -tapa sekä perustelut sille, että tuomioistuimen lupaa ei ole pyydetty ([72]). Ilmoituksen perusteella vastaanottava tuomioistuin voi tutkia tietojen keräämisen lainmukaisuuden. Ilmoitus talletetaan hätätoimenpiteiden rekisteriin.

([59]) Viestinnän tietosuojalain 9 §:n 3 momentti.
([60]) Viestinnän tietosuojalain täytäntöönpanoasetuksen 18 §:n 1 momentti.
([61]) Viestinnän tietosuojalain täytäntöönpanoasetuksen 18 §:n 2 momentti.
([62]) Viestinnän tietosuojalain 9-2 §:n 1 momentti.
([63]) Viestinnän tietosuojalain 9-2 §:n 4 momentti.
([64]) Viestinnän tietosuojalain 9-2 §:n 5 momentti.
([65]) Viestinnän tietosuojalain 9-2 §:n 6 momentti.
([66]) Viestinnän tietosuojalain 8 §:n 1 momentti.
([67]) Viestinnän tietosuojalain 8 §:n 2 momentti.
([68]) Viestinnän tietosuojalain 8 §:n 3 momentti ja sen täytäntöönpanoasetuksen 16 §:n 3 momentti.
([69]) Viestinnän tietosuojalain 8 §:n 4 momentti.
([70]) Tällä tavoin osoitetaan, että on perusteltua epäillä, että suunnitteilla on tiettyjä vakavia rikoksia tai että niitä tehdään tai on tehty, ja rikoksen estäminen, rikollisen pidättäminen tai todisteiden kerääminen olisi muutoin vaikeaa.
([71]) Viestinnän tietosuojalain 8 §:n 5 momentti.
([72]) Viestinnän tietosuojalain 8 §:n 6 ja 7 momentti.

Yleisen vaatimuksen mukaan viestinnän sisältöä, joka on hankittu yhteydenpidon rajoittamista koskevien toimenpiteiden avulla viestinnän tietosuojalain nojalla, voidaan käyttää ainoastaan edellä mainittujen rikosten tutkinnassa, syytteeseenpanossa tai ehkäisemisessä, samoihin rikoksiin liittyvissä kurinpitomenettelyissä, viestinnän osapuolen esittämän vahingonkorvausvaatimuksen käsittelyssä tai jos tietojen käyttö sallitaan muissa laeissa ([73]).

Kun kerätään internetin kautta välitettyä televiestintää, sovelletaan erityisiä suojatoimia ([74]). Tällaisia tietoja saa käyttää ainoastaan viestinnän tietosuojalain 5 §:n 1 momentissa lueteltujen vakavien rikosten tutkinnassa. Tietojen säilyttämiseen on saatava lupa siltä tuomioistuimelta, joka hyväksyi yhteydenpidon rajoittamista koskevat toimenpiteet ([75]). Säilyttämislupaa koskevassa hakemuksessa on annettava tiedot yhteydenpidon rajoittamista koskevista toimenpiteistä, yhteenveto niiden tuloksista ja säilyttämisen perustelut (todistusasiakirjojen kanssa) sekä säilytettävä televiestintäaineisto ([76]). Jos säilyttämislupaa ei pyydetä, hankittu televiestintäaineisto on poistettava 14 päivän kuluessa siitä kun yhteydenpidon rajoittamista koskevat toimenpiteet ovat päättyneet ([77]). Jos hakemus hylätään, aineisto on poistettava 7 päivän kuluessa ([78]). Jos televiestintä poistetaan, siitä on toimitettava 7 päivän kuluessa raportti sille tuomioistuimelle, joka hyväksyi yhteydenpidon rajoittamista koskevat toimenpiteet. Raportissa esitetään poistamisen syyt sekä siihen liittyvät yksityiskohdat ja ajankohta.

Tietoja, jotka on saatu laittomasti yhteydenpidon rajoittamisen avulla, ei yleensä hyväksytä todisteeksi oikeudenkäynnissä tai kurinpitomenettelyssä ([79]). Viestinnän tietosuojalaissa kielletään myös yhteydenpidon rajoittamista koskevien toimenpiteiden avulla saatujen luottamuksellisten tietojen luovuttaminen ja tällaisten tietojen käyttö toimenpiteiden kohteena olevien henkilöiden maineen vahingoittamiseksi ([80]).

2.2.2.3. Televalvontatietojen keräämiseen sovellettavat rajoitukset ja suojatoimet

Lainvalvontaviranomaiset voivat viestinnän tietosuojalain nojalla vaatia televiestintäpalvelujen tarjoajia toimittamaan televalvontatietoja, jos se on tarpeen tutkintaa tai tuomion täytäntöönpanoa varten ([81]). Sisältötietojen keräämisestä poiketen televalvontatietojen keräämistä ei ole rajoitettu vain tiettyihin rikoksiin. Yhteinen vaatimus sekä sisältö- että televalvontatietojen keräämiselle on kuitenkin se, että siihen tarvitaan tuomioistuimen kirjallinen ennakkolupa, aiemmin kuvattujen edellytysten mukaisesti ([82]). Jos tämä ei ole mahdollista asian kiireellisyyden vuoksi, televalvontatietoja voidaan kuitenkin kerätä ilman tuomioistuimen lupaa. Tällöin lupaa on haettava välittömästi sen jälkeen kun tietoja on pyydetty, ja se on toimitettava asianomaiselle televiestintäpalvelujen tarjoajalle ([83]). Jos lupaa ei saada jälkikäteen, kerätyt tiedot on tuhottava ([84]).

Syyttäjien, poliisin ja tuomioistuinten on pidettävä kirjaa televalvontatietoja koskevista pyynnöistä ([85]). Lisäksi televiestintäpalvelujen tarjoajien on kahdesti vuodessa raportoitava televalvontatietojen luovuttamisesta tiede- ja tieto- ja viestintätekniikkaministeriölle (*Ministry of Science and ICT*) ja pidettävä siitä kirjaa 7 vuoden ajan tietojen luovuttamisesta ([86]).

Periaatteessa yksilöille on ilmoitettava siitä, että heiltä on kerätty televalvontatietoja ([87]). Ilmoittamisen ajankohta riippuu tutkinnan olosuhteista ([88]). Ilmoitus on annettava 30 päivän kuluessa siitä, kun on tehty syyttämis- tai syyttämättäjättämispäätös. Jos syytetoimet keskeytetään, ilmoitus on annettava 30 päivän kuluessa siitä, kun tällaisen päätöksen antamisesta on kulunut yksi vuosi. Ilmoitus on joka tapauksessa toimitettava 30 päivän kuluessa siitä, kun on kulunut yksi vuosi tietojen keräämisestä.

Ilmoittamista voidaan lykätä, jos se todennäköisesti 1) vaarantaisi kansallisen turvallisuuden tai yleisen turvallisuuden ja järjestyksen, 2) aiheuttaisi kuoleman tai ruumiinvamman, 3) estäisi oikeudenmukaisen oikeudenkäynnin toteutumisen

([73]) Viestinnän tietosuojalain 12 §.
([74]) Viestinnän tietosuojalain 12-2 §.
([75]) Syyttäjän tai poliisin, joka toteuttaa yhteydenpidon rajoittamista koskevan toimenpiteen, on valikoitava säilytettäväksi tarkoitettu televiestintä 14 päivän kuluessa toimenpiteen päättymisestä ja pyydettävä siihen tuomioistuimen hyväksyntä (jos kyseessä on poliisi, hakemus esitetään syyttäjälle, joka toimittaa sen edelleen tuomioistuimelle), ks. viestinnän tietosuojalain 12-2 §:n 1 ja 2 momentti.
([76]) Viestinnän tietosuojalain 12-2 §:n 3 momentti.
([77]) Viestinnän tietosuojalain 12-2 §:n 5 momentti.
([78]) Viestinnän tietosuojalain 12-2 §:n 5 momentti.
([79]) Viestinnän tietosuojalain 4 §.
([80]) Viestinnän tietosuojalain täytäntöönpanoasetuksen 11 §:n 2 momentti.
([81]) Viestinnän tietosuojalain 13 §:n 1 momentti.
([82]) Viestinnän tietosuojalain 13 ja 6 §.
([83]) Viestinnän tietosuojalain 13 §:n 2 momentti. Samoin kuin yhteydenpidon rajoittamista koskevien kiireellisten toimenpiteiden yhteydessä, on laadittava asiakirja tapauksen yksityiskohdista (epäilty, toteutettavat toimenpiteet, epäilty rikos ja asian kiireellisyys). Ks. viestinnän tietosuojalain täytäntöönpanoasetuksen 37 §:n 5 momentti.
([84]) Viestinnän tietosuojalain 13 §:n 3 momentti.
([85]) Viestinnän tietosuojalain 13 §:n 5 ja 6 momentti.
([86]) Viestinnän tietosuojalain 13 §:n 7 momentti.
([87]) Ks. viestinnän tietosuojalain 13-3 §:n 7 momentti yhdessä 9-2 §:n kanssa.
([88]) Viestinnän tietosuojalain 13-3 §:n 1 momentti.

(esimerkiksi siksi, että se johtaisi todisteiden hävittämiseen tai todistajien uhkailuun), tai 4) loukkaisi epäillyn, uhrien tai muiden tapaukseen liittyvien henkilöiden kunniaa tai heidän yksityisyyttään ([89]). Ilmoittamiseen jonkin edellä mainitun syyn perusteella tarvitaan toimivaltaisen piirisyyttäjänviraston päällikön lupa ([90]). Ilmoitus on annettava 30 päivän kuluessa siitä kun lykkäämisen perusteet lakkaavat olemasta ([91]).

Ilmoituksen saatuaan yksilöt voivat pyytää syyttäjältä tai poliisilta kirjallisesti perusteluja televalvontatietojensa keräämiseen ([92]). Syyttäjän tai poliisin on tällöin esitettävä perustelut kirjallisesti 30 päivän kuluessa pyynnön vastaanottamisesta, paitsi jos sovelletaan jotakin edellä mainittua ilmoituksen lykkäämistä koskevaa poikkeusta ([93]).

2.2.3. *Tietojen vapaaehtoinen luovuttaminen televiestintäpalvelujen tarjoajien toimesta*

Televiestintäyrityksiä koskevan lain 83 §:n 3 momentin mukaan televiestintäpalvelujen tarjoajat voivat vastata tuomioistuimen, syyttäjän tai tutkintaviraston johtajan esittämiin tietopyyntöihin (jotka liittyvät rikosoikeudenkäyntiin, -tutkintaan tai tuomion täytäntöönpanoon) luovuttamalla vapaaehtoisesti ”viestintätietoja”. Kyseisessä laissa ”viestintätiedoilla” tarkoitetaan käyttäjien nimeä, asukasrekisterinumeroa, osoitetta ja puhelinnumeroa, liittymän avaamis- tai sulkemispäivämäärää sekä käyttäjätunnusta (koodi, jonka avulla tietojärjestelmän tai viestintäverkon oikeutettu käyttäjä tunnistetaan) ([94]). Laissa säädettyjä tarkoituksia varten ”käyttäjiksi” katsotaan ainoastaan yksilöt, jotka ovat tehneet sopimuksen suoraan korealaisen televiestintäpalvelujen tarjoajan kanssa ([95]). Näin ollen tilanteet, joissa laissa tarkoitettuina käyttäjinä pidettäisiin sellaisia EU:n yksilöitä, joiden tiedot on siirretty Korean tasavaltaan, olisivat todennäköisesti hyvin rajallisia, koska nämä henkilöt eivät yleensä tekisi sopimuksia suoraan korealaisen televiestintäpalvelujen tarjoajan kanssa.

Televiestintäyrityksiä koskevan lain nojalla esitettävät viestintätietojen keräämistä koskevat pyynnöt on laadittava kirjallisesti, ja niissä on ilmoitettava perustelut, yhteys asianomaiseen käyttäjään ja pyydettyjen tietojen laajuus ([96]). Jos kirjallista pyyntöä ei voida toimittaa asian kiireellisyyden vuoksi, kirjallinen pyyntö on toimitettava heti kun kiireellisyyden syy lakkaa ([97]). Kun televiestintäpalvelujen tarjoajat noudattavat viestintätietojen luovuttamista koskevia pyyntöjä, niiden on pidettävä siitä kirjaa, ja kirjanpidossa on säilytettävä myös tähän liittyvä aineisto, kuten kirjalliset pyynnöt ([98]). Lisäksi televiestintäpalvelujen tarjoajien on kahdesti vuodessa raportoitava viestintätietojen luovuttamisesta tiede- ja tietoja viestintätekniikkaministeriölle ([99]).

Televiestintäpalvelujen tarjoajilla ei ole televiestintäyrityksiä koskevan lain nojalla velvollisuutta luovuttaa viestintätietoja. Siksi niiden on arvioitava jokaista pyyntöä erikseen tietosuojalain nojalla sovellettavien tietosuojavaatimusten perusteella. Televiestintäpalvelujen tarjoajan on otettava huomioon erityisesti rekisteröidyn edut, eikä tietoja saa luovuttaa, jos se todennäköisesti loukkaisi oikeudetta asianomaisen yksilön tai kolmannen osapuolen etuja ([100]). Lisäksi tietojen luovuttamisesta on ilmoitettava asianomaiselle henkilölle tietosuojalautakunnan antaman ilmoituksen N:o 2021-1 nojalla. Ilmoittamista voidaan lykätä poikkeuksellisissa tilanteissa, erityisesti jos ja niin kauan kuin se vaarantaisi meneillään olevan rikostutkinnan tai todennäköisesti vahingoittaisi toisen henkilön henkeä tai terveyttä, jos nämä oikeudet tai edut ovat selvästi rekisteröidyn oikeuksia tärkeämmät ([101]).

Korkein oikeus vahvisti vuonna 2016, että viestintätietojen luovuttaminen televiestintäpalvelujen tarjoajien toimesta vapaaehtoisesti, ilman televiestintäyrityksiä koskevan lain nojalla annettua päätöstä, ei itsessään loukkaa televiestintäpalvelun käyttäjän oikeutta määrätä omista tiedoistaan. Toisaalta korkein oikeus kuitenkin täsmensi, että kyseessä on tämän oikeuden loukkaaminen silloin kun on ilmeistä, että tietoja pyytänyt virasto on käyttänyt väärin toimivaltaansa pyytää viestintätietojen luovuttamista ja siten loukannut asianomaisen henkilön tai kolmannen osapuolen etuja ([102]). Yleensäkin kaikissa lainvalvontaviranomaisten esittämissä, tietojen vapaaehtoista luovuttamista koskevissa pyynnöissä on noudatettava Korean perustuslaissa vahvistettuja lainmukaisuuden, tarpeellisuuden ja oikeasuhteisuuden periaatteita (perustuslain 12 §:n 1 momentti ja 37 §:n 2 momentti).

([89]) Viestinnän tietosuojalain 13-3 §:n 2 momentti.
([90]) Viestinnän tietosuojalain 13-3 §:n 3 momentti.
([91]) Viestinnän tietosuojalain 13-3 §:n 4 momentti.
([92]) Viestinnän tietosuojalain 13-3 §:n 5 momentti.
([93]) Viestinnän tietosuojalain 13-3 §:n 6 momentti.
([94]) Televiestintäyrityksiä koskevan lain 83 §:n 3 momentti.
([95]) Televiestintäyrityksiä koskevan lain 2 §:n 9 momentti.
([96]) Televiestintäyrityksiä koskevan lain 83 §:n 4 momentti.
([97]) Televiestintäyrityksiä koskevan lain 83 §:n 4 momentti.
([98]) Televiestintäyrityksiä koskevan lain 83 §:n 5 momentti.
([99]) Televiestintäyrityksiä koskevan lain 83 §:n 6 momentti.
([100]) Tietosuojalain 18 §:n 2 momentti.
([101]) Tietosuojalautakunnan asiakirja *Notification No. 2021-1 on Supplementary rules for the interpretation and application of the Personal Information Protection Act*, kohta III, 2, iii.
([102]) Korkeimman oikeuden päätös 2012Da105482, 10.3.2016.

2.3. **Valvonta**

Lainvalvontaviranomaisten toimintaa valvotaan eri mekanismien avulla sekä sisäisten että ulkoisten elinten toimesta.

2.3.1. *Sisäinen tarkastus*

Julkisen sektorin tarkastuksista annetun lain mukaisesti viranomaisia kehotetaan perustamaan sisäinen tarkastuselin, jonka tehtävänä on muun muassa suorittaa laillisuusvalvontaa ([103]). Tällaisten tarkastuselinten johtajalle on taattava mahdollisimman laaja riippumattomuus ([104]). Hänet on erityisesti nimitettävä asianomaisen viranomaisen ulkopuolelta (kyseessä voi olla esimerkiksi entinen tuomari tai professori) 2–5 vuoden toimikaudeksi, ja hänet voidaan erottaa tehtävästä vain perustellusta syystä (esimerkiksi jos hän ei pysty hoitamaan tehtävää fyysisen tai psyykkisen toimintakyvyttömyyden vuoksi tai jos hän on joutunut kurinpitotoimien kohteeksi) ([105]). Tarkastajat nimitetään vastaavalla tavalla samassa laissa asetettujen edellytysten mukaisesti ([106]). Tarkastusraporteissa voidaan antaa suosituksia tai pyytää korvaus- tai oikaisupyyntöjä sekä esittää moitteita ja suosittaa tai vaatia kurinpitotoimia ([107]). Tarkastusraportit annetaan tiedoksi tarkastuksen kohteena olevan viranomaisen johtajalle sekä valtion tilintarkastus- ja valvontaviranomaiselle (ks. kohta 2.3.2) 60 päivän kuluessa tarkastuksen päättymisestä ([108]). Asianomaisen viranomaisen on toteutettava vaaditut toimenpiteet ja raportoitava tuloksista tilintarkastus- ja valvontaviranomaiselle ([109]). Lisäksi tarkastuksen tulokset yleensä julkaistaan ([110]). Sisäisen tarkastuksen estämisestä tai siitä kieltäytymisestä voidaan määrätä hallinnollisia sakkoja ([111]). Lainvalvonnan alalla edellä mainitun lainsäädännön noudattaminen edellyttää, että kansallisella poliisivirastolla on tarkastusjärjestelmä, jossa sisäiset tarkastukset käsitellään, mahdolliset ihmisoikeuksien loukkaukset mukaan lukien ([112]).

2.3.2. *Valtion tilintarkastus- ja valvontaviranomainen*

Valtion tilintarkastus- ja valvontaviranomainen (*Board of Audit and Inspection*, BAI) voi tarkastaa viranomaisten toiminnan ja antaa tarkastusten perusteella suosituksia tai pyytää kurinpitotoimia tai nostaa rikossyytteen ([113]). Se toimii virallisesti Korean tasavallan presidentin alaisuudessa, mutta hoitaa tehtäviään itsenäisesti ([114]). Lisäksi tilintarkastus- ja valvontaviranomaiselle on sen perustamissäädöksen nojalla myönnettävä mahdollisimman laaja riippumattomuus sen henkilöstön nimittämisen, erottamisen ja organisoinnin sekä talousarvion laatimisen suhteen ([115]). Tilintarkastus- ja valvontaviranomaisen johtajan nimittää presidentti kansalliskokouksen hyväksynnän saatuaan ([116]). Presidentti nimittää muut kuusi viranomaisen jäsentä (komissaarit) johtajan suosituksen perusteella neljän vuoden toimikaudeksi ([117]). Komissaarien (johtaja ml.) on täytettävä erityiset lakisääteiset pätevyysvaatimukset ([118]), ja heidät voidaan erottaa ainoastaan virkarikoksen perusteella tai jos heidät on tuomittu vankeuteen tai jos he eivät kykene hoitamaan tehtäviään pitkäaikaisen fyysisen tai psyykkisen toimintakyvyttömyyden vuoksi ([119]). Komissaarit eivät saa osallistua poliittiseen toimintaan eivätkä hoitaa samanaikaisesti virkaa kansalliskokouksessa, hallintovirastoissa tai valtion tilintarkastus- ja valvontaviranomaisen alaisuudessa toimivissa organisaatioissa eikä mitään muutakaan palkattua virkaa tai tehtävää ([120]).

Tilintarkastus- ja valvontaviranomainen suorittaa yleisiä tarkastuksia vuosittain, mutta lisäksi se voi tehdä erityistarkastuksia erityisen tärkeistä seikoista. Tarkastustehtäviä suorittaessaan se voi pyytää asiakirjojen toimittamista ja vaatia henkilöiden läsnäoloa ([121]). Tilintarkastus- ja valvontaviranomaisen tehtävänä on tarkastaa valtion tulot ja

([103]) Julkisen sektorin tarkastuksista annetun lain 3 ja 5 §.
([104]) Julkisen sektorin tarkastuksista annetun lain 7 §.
([105]) Julkisen sektorin tarkastuksista annetun lain 8-11 §.
([106]) Julkisen sektorin tarkastuksista annetun lain 16 § ja sitä seuraavat pykälät.
([107]) Julkisen sektorin tarkastuksista annetun lain 23 §:n 2 momentti.
([108]) Julkisen sektorin tarkastuksista annetun lain 23 §:n 1 momentti.
([109]) Julkisen sektorin tarkastuksista annetun lain 23 §:n 3 momentti.
([110]) Julkisen sektorin tarkastuksista annetun lain 26 §.
([111]) Julkisen sektorin tarkastuksista annetun lain 41 §.
([112]) Ks. erityisesti tilintarkastuksesta ja tarkastuksista vastaavan osaston (*Audit and Inspection Department*) jaostot: https://www.police.go.kr/eng/knpa/org/org01.jsp.
([113]) Valtion tilintarkastus- ja valvontaviranomaisesta annetun lain (*Act on the Board of Audit and Inspection*) 24 ja 31-35 §.
([114]) Valtion tilintarkastus- ja valvontaviranomaisesta annetun lain 2 §:n 1 momentti.
([115]) Valtion tilintarkastus- ja valvontaviranomaisesta annetun lain 2 §:n 2 momentti.
([116]) Valtion tilintarkastus- ja valvontaviranomaisesta annetun lain 4 §:n 1 momentti.
([117]) Valtion tilintarkastus- ja valvontaviranomaisesta annetun lain 5 §:n 1 momentti ja 6 §.
([118]) Heidän on täytynyt toimia esimerkiksi tuomarina, syyttäjänä tai asianajajana ainakin 10 vuoden ajan, tai virkamiehenä tai professorina tai ylemmässä tehtävässä yliopistossa ainakin 8 vuoden ajan, tai työskennellä pörssiyhtiössä tai valtion rahoittamassa laitoksessa ainakin 10 vuoden ajan (joista ainakin 5 vuotta toimitusjohtajana (*executive officer*)), ks. valtion tilintarkastus- ja valvontaviranomaisesta annetun lain 7 §.
([119]) Valtion tilintarkastus- ja valvontaviranomaisesta annetun lain 8 §.
([120]) Valtion tilintarkastus- ja valvontaviranomaisesta annetun lain 9 §.
([121]) Ks. esim. valtion tilintarkastus- ja valvontaviranomaisesta annetun lain 27 §.

menot ja yleisemmin myös valvoa viranomaisten velvollisuuksien täyttämistä julkishallinnon toiminnan parantamiseksi ([122]). Näin ollen sen tarkastustehtävä kattaa talousarvioon liittyvien näkökohtien lisäksi myös laillisuusvalvonnan.

2.3.3. *Kansalliskokous*

Kansalliskokous voi tutkia ja tarkastaa viranomaisten toimintaa ([123]). Tutkinnan tai tarkastuksen aikana se voi pyytää asiakirjojen luovuttamista ja vaatia todistajia tulemaan kuultavaksi ([124]). Väärän valan vannominen kansalliskokouksen tutkinnan yhteydessä voi johtaa rikosoikeudellisten seuraamusten määräämiseen (enintään 10 vuoden vankeusrangaistus) ([125]). Tarkastusten kulku ja tulokset voidaan julkistaa ([126]). Jos kansalliskokous havaitsee laitonta tai sääntöjenvastaista toimintaa, se voi vaatia kyseistä viranomaista toteuttamaan korjaavia toimenpiteitä, esimerkiksi myöntämään vahingonkorvausta, toteuttamaan kurinpitotoimia tai parantamaan sisäisiä menettelyjään ([127]). Viranomaisen on toimittava tällaisen kehotuksen saatuaan viipymättä ja raportoitava toimenpiteiden tuloksesta kansalliskokoukselle ([128]).

2.3.4. *Tietosuojalautakunta*

Korean tietosuojalautakunta valvoo lainvalvontaviranomaisten suorittamaa henkilötietojen käsittelyä tietosuojalain mukaisesti. Tietosuojalain 7-8 §:n 3 ja 4 momentin ja 7-9 §:n 5 momentin mukaan tietosuojalautakunnan valvonta kattaa myös henkilötietojen keräämistä koskevista rajoituksista ja suojatoimista annettujen sääntöjen mahdollisen rikkomisen, mukaan lukien erityislakeihin sisältyvät säännöt, joilla säännellään (sähköisen) todistusaineiston keräämistä lainvalvontatarkoituksia varten (ks. kohta 2.2). Kun otetaan huomioon tietosuojalain 3 §:n 1 momentissa säädetyt vaatimukset, joiden mukaan henkilötietojen keräämisen on tapahduttava lainmukaisesti ja asianmukaisesti, tällainen rikkominen kohdistuu aina myös tietosuojalakiin, minkä vuoksi tietosuojalautakunta voi suorittaa tutkintaa ja toteuttaa korjaavia toimenpiteitä ([129]).

Kun tietosuojalautakunta käyttää valvontavaltuuksiaan, sillä on pääsy kaikkiin merkityksellisiin tietoihin ([130]). Tietosuojalautakunta voi antaa lainvalvontaviranomaisille neuvontaa niiden käsittelytoimiin liittyvän henkilötietojen suojan tason parantamiseksi, määrätä korjaavia toimenpiteitä (esim. tietojenkäsittelyn keskeyttäminen tai tarvittavien toimien toteuttaminen henkilötietojen suojelemiseksi) tai kehottaa viranomaista toteuttamaan kurinpitotoimia ([131]). Eräiden tietosuojalain säännösten rikkomisesta voidaan määrätä myös rikosoikeudellisia seuraamuksia. Nämä säännökset koskevat esimerkiksi henkilötietojen laitonta käyttöä tai luovuttamista kolmansille osapuolille tai arkaluonteisten tietojen laitonta käsittelyä ([132]). Tältä osin tietosuojalautakunta voi saattaa asian toimivaltaisen tutkintaviranomaisen (kuten syyttäjän) käsiteltäväksi ([133]).

2.3.5. *Kansallinen ihmisoikeuskomissio*

Kansallinen ihmisoikeuskomissio (*National Human Rights Commission*, NHRC) on riippumaton elin, jonka tehtävänä on suojella ja edistää perusoikeuksia ([134]). Sillä on valtuudet tutkia ja korjata perustuslain 10–22 §:ään kohdistuvia rikkomisia, jotka koskevat muun muassa oikeutta yksityisyyteen ja kirjesalaisuutta. Kansallinen ihmisoikeuskomissio muodostuu 11 komissaarista, joista kansalliskokous nimittää neljä, presidentti neljä ja korkeimman oikeuden presidentti kolme ([135]). Komissaariksi nimitettävän henkilön on täytynyt toimia 1) yliopistossa tai valtuutetussa tutkimuslaitoksessa vähintään apulaisprosessorin tehtävässä ainakin 10 vuoden ajan; 2) tuomarina, syyttäjänä tai asianajajana ainakin 10 vuoden ajan; 3) ihmisoikeustehtävissä ainakin 10 vuoden ajan (esimerkiksi voittoa tavoittelemattoman, valtiosta riippumattoman tai kansainvälisen järjestön palveluksessa); tai 4) olla kansalaisyhteiskunnan ryhmien suosittelema ([136]). Presidentti nimittää komission puheenjohtajan komissaarien joukosta; nimitykselle

([122]) Valtion tilintarkastus- ja valvontaviranomaisesta annetun lain 20 ja 24 §.
([123]) Kansalliskokouksesta annetun lain (*National Assembly Act*) 128 § ja valtionhallinnon tarkastuksista ja tutkimuksista annetun lain (*Act on the Inspection and Investigation of State Administration*) 2, 3 ja 15 §. Tähän sisältyvät valtion toimintaa koskevat vuotuiset tarkastukset kokonaisuutena sekä yksittäisiä asioita koskevat tutkimukset.
([124]) Valtionhallinnon tarkastuksista ja tutkimuksista annetun lain 10 §:n 1 momentti. Ks. myös kansalliskokouksesta annetun lain 128 ja 129 §.
([125]) Todistajanlausunnoista, arvioinneista ym. kansalliskokouksessa annetun lain (*Act on Testimony, Appraisal, etc. before the National Assembly*) 14 §.
([126]) Valtionhallinnon tarkastuksista ja tutkimuksista annetun lain 12-2 §.
([127]) Valtionhallinnon tarkastuksista ja tutkimuksista annetun lain 16 §:n 2 momentti.
([128]) Valtionhallinnon tarkastuksista ja tutkimuksista annetun lain 16 §:n 3 momentti.
([129]) Tietosuojalautakunnan asiakirja *Notification No. 2021-1 on Supplementary rules for the interpretation and application of the Personal Information Protection Act*.
([130]) Tietosuojalain 63 §.
([131]) Viestinnän tietosuojalain 61 §:n 2 momentti, 65 §:n 1 ja 2 momentti sekä 64 §:n 4 momentti.
([132]) Tietosuojalain 70–74 §.
([133]) Tietosuojalain 65 §:n 1 momentti.
([134]) Ihmisoikeuskomissiosta annetun lain (*Human Rights Commission Act*) 1 §.
([135]) Ihmisoikeuskomissiosta annetun lain 5 §:n 1 ja 2 momentti.
([136]) Ihmisoikeuskomissiosta annetun lain 5 §:n 3 momentti.

on saatava kansalliskokouksen vahvistus ([137]). Komissaarit (ml. puheenjohtaja) nimitetään kolmen vuoden toimikaudeksi, joka voidaan uusia. Heidät voidaan erottaa vain jos heille on määrätty vankeusrangaistus tai jos he eivät enää kykene hoitamaan tehtäväänsä pitkäaikaisen fyysisen tai psyykkisen toimintakyvyttömyyden vuoksi (tällöin komissaarien kahden kolmasosan on hyväksyttävä erottaminen) ([138]). Nimityksensä jälkeen komissaarit eivät saa toimia samanaikaisesti muissa tehtävissä (virkamiehenä) kansalliskokouksessa, paikallisneuvostoissa tai missään valtion tai paikallishallinnon tehtävissä ([139]).

Ihmisoikeuskomissio voi käynnistää tutkinnan omasta aloitteestaan tai yksilön tekemän valituksen perusteella. Ihmisoikeuskomissio voi tutkinnan yhteydessä vaatia asiaa koskevien aineistojen luovuttamista, tehdä tarkastuksia ja kutsua yksilöitä kuultavaksi ([140]). Ihmisoikeuskomissiolla on valtuudet antaa tutkinnan perusteella suosituksia tiettyjen politiikkatoimien tai käytäntöjen parantamiseksi tai korjaamiseksi, ja se voi julkistaa nämä suositukset ([141]). Viranomaisten on esitettävä ihmisoikeuskomissiolle suunnitelma suositusten täytäntöönpanemiseksi 90 päivän kuluessa niiden vastaanottamisesta ([142]). Jos viranomainen ei noudata suosituksia, sen on ilmoitettava asiasta ihmisoikeuskomissiolle ([143]). Ihmisoikeuskomissio voi puolestaan ilmoittaa tästä kansalliskokoukselle ja/tai julkistaa asian. Yleensä viranomaiset noudattavat ihmisoikeuskomission suosituksia. Niillä on vahva kannustin tehdä niin, koska suositusten noudattamista arvioidaan osana pääministerin kanslian alaisuudessa tehtävää yleistä arviointia.

2.4. **Yksilölliset oikeussuojakeinot**

2.4.1. *Tietosuojalakiin sisältyvät oikeussuojakeinot*

Tietosuojalain mukaan yksilöillä on pääsyoikeus omiin henkilötietoihinsa, joita käsitellään lainvalvontatarkoituksia varten, ja oikeus oikaista tai poistaa ne ja keskeyttää niiden käsittely. Pääsyoikeutta voi pyytää joko suoraan asianomaiselta viranomaiselta tai välillisesti tietosuojalautakunnan kautta ([144]). Toimivaltainen viranomainen voi rajoittaa pääsyoikeutta tai evätä sen kokonaan vain jos niin säädetään laissa, tai jos oikeuden myöntäminen todennäköisesti vahingoittaisi kolmannen osapuolen henkeä tai terveyttä tai aiheuttaisi oikeudettomasti vahinkoa toisen henkilön omaisuudelle ja muille eduille (eli kun toisen henkilön edut olisivat pyynnön esittävän henkilön etuja tärkeämmät) ([145]). Jos pääsyoikeus evätään, yksilölle on ilmoitettava epäämisen syy ja annettava muutoksenhakua koskevat ohjeet ([146]). Vastaavasti pyyntö oikaista tai poistaa tiedot voidaan evätä, jos laissa niin säädetään, ja tällöin yksilölle on ilmoitettava epäämisen syy ja annettava mahdollisuus hakea päätökseen muutosta ([147]).

Yksilöt voivat käyttää tätä oikeutta tekemällä valituksen tietosuojalautakunnalle esimerkiksi Korean internet- ja turvallisuusviraston ylläpitämän Privacy Call Centre -puhelinpalvelun kautta ([148]). Lisäksi yksityishenkilö voi saada sovitteluapua henkilötietoihin liittyviä asioita käsittelevältä riitojenratkaisukomitealta ([149]). Nämä oikeussuojakeinot ovat käytettävissä myös silloin kun mahdollinen rikkominen koskee erityislakien säännöksiä (ks. kohta 2.2) tai tietosuojalain säännöksiä. Lisäksi yksilöt voivat hakea muutosta tietosuojalautakunnan päätöksiin tai toimimatta jättämiseen hallinnollisista riita-asioista annetun lain nojalla (ks. kohta 2.4.3).

([137]) Ihmisoikeuskomissiosta annetun lain 5 §:n 5 momentti.
([138]) Ihmisoikeuskomissiosta annetun lain 7 §:n 1 momentti ja 8 §.
([139]) Ihmisoikeuskomissiosta annetun lain 10 §.
([140]) Ihmisoikeuskomissiosta annetun lain 36 §. Lain 36 §:n 7 momentin mukaan aineistojen tai esineiden toimittamisesta voidaan kieltäytyä, jos se vaarantaisi valtion asiakirjojen luottamuksellisuuden ja voisi vaikuttaa olennaisella tavalla valtion turvallisuuteen tai diplomaattisuhteisiin tai muodostaisi rikostutkintaa tai meneillään olevaa oikeudenkäyntiä haittaavan vakavan esteen. Tällaisissa tapauksissa komissio voi pyytää asianomaisen viraston johtajalta (jonka on toimittava vilpittömässä mielessä) lisätietoja sen selvittämiseksi, onko kieltäytyminen tietojen toimittamisesta perusteltu.
([141]) Ihmisoikeuskomissiosta annetun lain 25 §:n 1 momentti.
([142]) Ihmisoikeuskomissiosta annetun lain 25 §:n 3 momentti.
([143]) Ihmisoikeuskomissiosta annetun lain 25 §:n 4 momentti.
([144]) Tietosuojalain 35 §:n 2 momentti.
([145]) Tietosuojalain 35 §:n 4 momentti.
([146]) Tietosuojalain täytäntöönpanoasetuksen 42 §:n 2 momentti.
([147]) Tietosuojalain 36 §:n 1 ja 2 momentti ja sen täytäntöönpanoasetuksen 43 §:n 3 momentti.
([148]) Tietosuojalain 62 §.
([149]) Tietosuojalain 40–50 § ja sen täytäntöönpanoasetuksen 48-2–57 §.

2.4.2. *Kansallisen ihmisoikeuskomission tarjoama oikeussuoja*

Kansallinen ihmisoikeuskomissio käsittelee yksilöiden (sekä korealaisten että ulkomaiden kansalaisten) tekemiä valituksia, jotka koskevat viranomaisten tekemiä ihmisoikeusloukkauksia ([150]). Yksilöille ei ole asetettu erityisiä vaatimuksia valituksen tekemiseksi kansalliselle ihmisoikeuskomissiolle ([151]). Tämä tarkoittaa, että ihmisoikeuskomissio ottaa valituksen käsiteltäväksi, vaikka asianomainen ei vielä tässä vaiheessa pystyisi osoittamaan, että hänen oikeuksiaan on todella loukattu. Kun on kyse henkilötietojen keräämisestä lainvalvontatarkoituksia varten, yksilön ei näin ollen tarvitse osoittaa, että Korean viranomaiset ovat tosiasiallisesti keränneet hänen henkilötietojaan, jotta ihmisoikeuskomissio ottaisi hänen valituksensa käsiteltäväksi. Yksilö voi myös pyytää valituksensa ratkaisemista sovittelussa ([152]).

Ihmisoikeuskomissio voi käyttää valituksen tutkinnassa tutkintavaltuuksiaan ja vaatia asiaa koskevien aineistojen luovuttamista, tehdä tarkastuksia ja kutsua yksilöitä kuultavaksi ([153]). Jos tutkinnassa käy ilmi, että asianomaisia säännöksiä on tosiaan rikottu, ihmisoikeuskomissio voi suosittaa korjaavia toimenpiteitä tai asiaa koskevan säännöksen, instituution, politiikkatoimen tai käytännön oikaisemista tai parantamista ([154]). Ehdotetut korjaavat toimenpiteet voivat koskea esimerkiksi sovittelua, ihmisoikeusloukkauksen lopettamista, vahingonkorvauksen suorittamista ja toimenpiteitä saman tai vastaavanlaisten loukkausten toistumisen estämiseksi ([155]). Jos henkilötietoja on kerätty sovellettavien sääntöjen vastaisesti, korjaaviin toimenpiteisiin voi sisältyä kerättyjen henkilötietojen tuhoaminen. Jos katsotaan, että rikkominen on erittäin todennäköisesti tapahtunut ja että sen jatkuminen aiheuttaisi vaikeasti korjattavissa olevaa vahinkoa, ihmisoikeuskomissio voi myös hyväksyä kiireellisiä korjaavia toimenpiteitä ([156]).

Vaikka ihmisoikeuskomissiolla ei ole valtuuksia antaa pakottavia päätöksiä, sen päätöksiin (esimerkiksi päätös olla jatkamatta valituksen tutkimista) ([157]) ja suosituksiin on mahdollista hakea muutosta Korean tuomioistuimissa hallinnollisista riita-asioista annetun lain nojalla (ks. kohta 2.4.3 jäljempänä) ([158]). Jos ihmisoikeuskomission havainnot osoittavat, että viranomainen on kerännyt henkilötietoja laittomasti, yksilö voisi vedota kyseistä viranomaista vastaan Korean tuomioistuimissa esimerkiksi riitauttamalla tietojen keräämisen hallinnollisista riita-asioista annetun lain nojalla, tekemällä perustuslakivalituksen perustuslakituomioistuimesta annetun lain nojalla tai vaatimalla vahingonkorvausta valtion korvauksista annetun lain nojalla (ks. kohta 2.4.3 jäljempänä).

2.4.3. *Oikeudellinen muutoksenhaku*

Yksilöt voivat vedota edellä kuvattuihin rajoituksiin ja suojatoimiin hakeakseen oikeussuojaa Korean tuomioistuimissa eri väylien kautta.

Ensinnäkin asianomainen henkilö (ja hänen avustajansa) voi rikosprosessilain mukaisesti olla läsnä, kun etsintä- tai takavarikkopäätös pannaan täytäntöön, ja hän voi myös vastustaa sitä täytäntöönpanohetkellä ([159]). Lisäksi rikosprosessilaissa säädetään nk. kvasi-valituksesta, mikä tarkoittaa, että yksilö voi pyytää toimivaltaista tuomioistuinta kumoamaan syyttäjän tai poliisin tekemän takavarikkopäätöksen tai muuttamaan sitä ([160]). Tämän mekanismin avulla yksilöt voivat riitauttaa takavarikointipäätöksen täytäntöönpanotoimet.

([150]) Ihmisoikeuskomissiosta annetun lain 4 §:ssä viitataan sekä Korean tasavallan kansalaisiin että maassa asuviin ulkomaalaisiin, mutta siinä käytetty ilmaisu ”asuva” liittyy pikemminkin toimivaltaisuuteen kuin alueeseen. Tämä tarkoittaa, että jos Korean kansalliset instituutiot loukkaavat Korean ulkopuolella asuvan ulkomaalaisen perusoikeuksia, hän voi valittaa asiasta ihmisoikeuskomissiolle. Ks. vastaava kysymys ihmisoikeuskomission sivustolla osiossa ”Usein kysyttyjä kysymyksiä”, saatavilla osoitteessa https://www.humanrights.go.kr/site/program/board/basicboard/list?boardtypeid=7025&menuid=002004005001&pagesize=10&currentpage=2. Tämä koskee esimerkiksi tilannetta, jossa Korean viranomaiset käsittelevät Koreaan siirrettyjä ulkomaalaisen henkilötietoja lainvastaisesti.

([151]) Valitus on periaatteessa tehtävä vuoden kuluessa rikkomisesta, mutta ihmisoikeuskomissio voi päättää tutkia myös tämän määräajan jälkeen tehdyn valituksen, jos rikos- tai siviilioikeudellinen vanhentumisaika ei ole vielä päättynyt (ihmisoikeuskomissiosta annetun lain 32 §:n 1 momentin 4 kohta).

([152]) Ihmisoikeuskomissiosta annetun lain 42 § ja sitä seuraavat pykälät.

([153]) Ihmisoikeuskomissiosta annetun lain 36 ja 37 §.

([154]) Ihmisoikeuskomissiosta annetun lain 44 §.

([155]) Ihmisoikeuskomissiosta annetun lain 42 §:n 4 momentti.

([156]) Ihmisoikeuskomissiosta annetun lain 48 §.

([157]) Jos ihmisoikeuskomissio esimerkiksi ei poikkeuksellisesti pysty tarkastamaan tiettyjä aineistoja tai laitoksia siksi, että ne liittyvät valtionsalaisuuksiin, joilla voi olla merkittävä vaikutus valtion turvallisuuteen tai diplomaattisuhteisiin, tai jos tarkastus muodostaisi vakavan esteen rikostutkinnalle tai vireillä olevalle oikeudenkäynnille (ks. alaviite 166), ja tämä estäisi ihmisoikeuskomissiota suorittamasta tutkimusta, joka on tarpeen vastaanotetun vetoomuksen sisällön arvioimiseksi, se ilmoittaa asianomaiselle henkilölle syyt valituksen hylkäämiseen ihmisoikeuskomissiosta annetun lain 39 §:n mukaisesti. Tällaisessa tapauksessa henkilö voisi riitauttaa ihmisoikeuskomission päätöksen hallinnollisista riita-asioista annetun lain nojalla.

([158]) Ks. esim. Soulin ylemmän asteen tuomioistuimen päätös 2007Nu27259, 18.4.2008, joka on vahvistettu korkeimman oikeuden päätöksellä 2008Du7854, 9.10.2008; Soulin ylemmän asteen tuomioistuimen päätös 2017Nu69382, 2.2.2018.

([159]) Rikosprosessilain 121 ja 219 §.

([160]) Rikosprosessilain 417 § yhdessä sen 414 §:n 2 momentin kanssa. Ks. myös korkeimman oikeuden päätös 97Mo66, 29.9.1997.

Yksilöt voivat myös vaatia vahingonkorvausta Korean tuomioistuimissa. Valtion korvauksista annetun lain perusteella yksilöt voivat vaatia korvausta vahingoista, joita virkamies on aiheuttanut suorittaessaan virkatehtäviään lainvastaisesti ([161]). Kyseisen lain nojalla tehtävä vaatimus käsitellään joko ns. korvausneuvostossa (*Compensation Council*) tai suoraan Korean tuomioistuimissa ([162]). Jos uhri on ulkomaalainen, valtion korvauksista annettua lakia sovelletaan, jos uhrin kansalaisuusmaa korvaa vastaavasti Korean kansalaisille aiheutuneet vahingot ([163]). Oikeuskäytännön mukaan tämä edellytys täyttyy, jos toisessa maassa sovellettavat korvauksen hakemista koskevat vaatimukset eivät ole ”selvästi epäsuhtaiset Korean ja toisen maan välillä” tai ”yleisesti tiukemmat kuin Korean asettamat vaatimukset, niin että niissä ei ole olennaisia eroja” ([164]). Valtion korvausvastuuta säännellään siviililailla (*Civil Act*), jonka nojalla valtion korvausvastuu kattaa myös muut kuin aineelliset vahingot (esimerkiksi henkisen kärsimyksen) ([165]).

Tietosuojasääntöjen rikkomisen osalta tietosuojalaissa säädetään täydentävästä oikeussuojakeinosta. Tietosuojalain 39 §:ssä säädetään, että jos rekisteröidylle aiheutuu vahinkoa tietosuojalain rikkomisen, hänen henkilötietojensa katoamisen, varastamisen, paljastamisen, väärentämisen, muuttamisen tai vahingoittumisen vuoksi, hän voi saada tällaisesta vahingosta korvauksen tuomioistuimessa. Valtion korvauksista annetussa laissa tarkoitetun kaltaista vastavuoroisuutta ei edellytetä.

Vahingonkorvauksen lisäksi hallintovirastojen toimien tai laiminlyöntien perusteella on mahdollista hakea muutosta hallinnollisessa menettelyssä hallinnollisista riita-asioista annetun lain nojalla. Kuka tahansa voi riitauttaa hallintoviraston päätöksen (eli tiettyä tapausta koskevan julkisen vallan käytön tai sen käytöstä kieltäytymisen) tai laiminlyönnin (pitkään jatkunut hallintoviraston oikeudellisen velvollisuuden laiminlyönti), minkä seurauksena lainvastainen päätös voidaan kumota tai sitä voidaan muuttaa tai se voidaan todeta pätemättömäksi (tämä tarkoittaa, että kyseisellä päätöksellä ei ole oikeusvaikutusta tai että sitä ei ole olemassa oikeusjärjestyksessä); myös laiminlyönti voidaan todeta lainvastaiseksi ([166]). Hallinnollinen päätös voidaan riitauttaa, jos se vaikuttaa suoraan kansalaisoikeuksiin ja -velvollisuuksiin ([167]). Tämä koskee myös toimenpiteitä, joiden nojalla henkilötietoja kerätään joko suoraan (esim. telekuuntelun avulla) tai (esim. palveluntarjoajalle esitetyn) luovutuspyynnön avulla.

Edellä mainittu vaatimus voidaan esittää ensin hallinnollisia muutoksenhakuasioita käsittelevälle lautakunnalle, joita on perustettu eräiden viranomaisten yhteyteen (mm. kansallinen tiedustelupalvelu, ihmisoikeuskomissio), tai korruptiontorjunnasta ja kansalaisoikeuksista vastaavan komitean (*Anti-Corruption and Civil Rights Commission*) yhteydessä toimivalle hallinnollisten muutoksenhakuasioiden keskuslautakunnalle (*Central Administrative Appeals Commission*) ([168]). Tällainen hallinnollinen muutoksenhaku on vaihtoehtoinen, epävirallisempi keino hakea muutosta viranomaisen määräykseen tai laiminlyöntiin. On myös mahdollista nostaa kanne suoraan korealaisessa tuomioistuimessa hallinnollisista riita-asioista annetun lain nojalla.

Päätöksen kumoamista/muuttamista voi hakea hallinnollisista riita-asioista annetun lain nojalla jokainen, jolla on siihen oikeudellinen intressi tai oikeus saada sen avulla oikeutensa palautetuksi, jos kyseinen päätös ei ole enää voimassa ([169]). Vastaavasti pätemättömäksi julistamista voi vaatia jokainen, jolla on siihen oikeudellinen intressi. Sen sijaan laiminlyönnin lainvastaiseksi toteamista voi vaatia jokainen, joka on pyytänyt laiminlyönnin kohteena olevaa päätöstä ja jolla on oikeudellinen intressi vaatia laiminlyönnin lainvastaisuuden toteamista ([170]). Korkeimman oikeuden oikeuskäytännön mukaan ”oikeudellisella intressillä” tarkoitetaan ”oikeudellisesti suojattua etua” eli suoraa ja erityistä etua, joka on suojattu niissä laeissa ja asetuksissa, joihin kyseinen hallinnollinen päätös perustuu (kyse ei siis voi olla yleisölle kuuluvasta yleisestä, epäsuorasta ja abstraktista edusta) ([171]). Yksilöillä on tällainen oikeudellinen intressi, jos heidän henkilötietojensa keräämisessä lainvalvontatarkoituksiin ei ole noudatettu (erityislakien tai tietosuojalain nojalla) sovellettavia rajoituksia ja suojatoimia. Hallinnollisista riita-asioista annetun lain nojalla annettu lainvoimainen tuomio sitoo asianosaisia ([172]).

Vaatimus päätöksen peruuttamisesta/muuttamisesta tai laiminlyönnin lainvastaiseksi toteamisesta on esitettävä 90 päivän kuluessa siitä kun asianomainen on saanut tiedon päätöksestä/laiminlyönnistä ja periaatteessa viimeistään vuoden

([161]) Valtion korvauksista annetun lain 2 §:n 1 momentti.
([162]) Valtion korvauksista annetun lain 9 ja 12 §. Lailla perustetaan piirineuvostot (*District Councils*, joiden puheenjohtajana toimii kyseisen alueen syyttäjänviraston apulaissyyttäjä), keskusneuvosto (*Central Council*, jonka puheenjohtajana toimii apulaisoikeusministeri) ja erityisneuvosto (*Special Council*, joka vastaa asevoimien sotilas- tai siviilihenkilöstön aiheuttamien vahinkojen korvaamisesta ja jonka puheenjohtajana toimii apulaispuolustusministeri). Vahingonkorvaushakemukset käsitellään pääsääntöisesti piirineuvostoissa, joiden on tietyissä olosuhteissa toimitettava tapaukset edelleen keskus- tai erityisneuvoston käsiteltäväksi, esimerkiksi jos korvaus ylittää tietyn määrän tai jos hakija pyytää asian uudelleenkäsittelyä. Jäsenet kaikkiin neuvostoihin nimittää oikeusministeri (mm. oikeusministeriön virkamiesten, oikeusvirkamiesten, juristien ja valtion korvauksiin perehtyneiden asiantuntijoiden joukosta) ja heihin sovelletaan erityisiä eturistiriitoja koskevia sääntöjä (ks. valtion korvauksista annetun lain täytäntöönpanoasetuksen 7 §).
([163]) Valtion korvauksista annetun lain 7 §.
([164]) Korkeimman oikeuden päätös 2013Da208388, 11.6.2015.
([165]) Ks. valtion korvauksista annetun lain 8 § sekä siviililain 751 §.
([166]) Hallinnollisista riita-asioista annetun lain 2 ja 4 §.
([167]) Korkeimman oikeuden päätös 98Du18435, 22.10.1999, korkeimman oikeuden päätös 99Du1113, 8.9.2000, ja korkeimman oikeuden päätös 2010Du3541, 27.9.2012.
([168]) Hallinnollisesta muutoksenhausta annetun lain 6 § ja hallinnollisista riita-asioista annetun lain 18 §:n 1 momentti.
([169]) Hallinnollisista riita-asioista annetun lain 12 §.
([170]) Hallinnollisista riita-asioista annetun lain 35 ja 36 §.
([171]) Korkeimman oikeuden päätös 2006Du330, 26.3.2006.
([172]) Hallinnollisista riita-asioista annetun lain 30 §:n 1 momentti.

kuluttua päätöksen antamisesta tai laiminlyönnin ilmenemisestä, paitsi jos on olemassa perusteltu syy esittää vaatimus myöhemmin ([173]). Korkein oikeus on tulkinnut ”perustellun syyn” käsitettä laajasti siten, että on arvioitava, onko kaikkien asiaan liittyvien olosuhteiden valossa yhteiskunnallisesti hyväksyttävää sallia myöhässä tehdyn valituksen käsittely ([174]). Tämä koskee myös (mutta ei pelkästään) sellaisia viivästymisen syitä, joista asianomaista osapuolta ei voida pitää vastuullisena (eli tilanteet, joihin valittaja ei ole voinut vaikuttaa, esimerkiksi jos hän ei ole saanut ilmoitusta henkilötietojensa keräämisestä), sekä ylivoimaisia esteitä (*force majeure*, kuten luonnonmullistus tai sota).

Yksilöt voivat myös tehdä perustuslakituomioistuimelle perustuslakivalituksen ([175]). Jokaisella, jonka perustuslaissa taattuja perusoikeuksia on loukattu julkisen vallan käytön tai käyttämättä jättämisen seurauksena (tuomioistuinten tuomioita lukuun ottamatta), on perustuslakituomioistuimesta annetun lain nojalla oikeus vaatia asian ratkaisemista perustuslakivalituksella. Ensin on kuitenkin käytettävä mahdolliset muut oikeussuojakeinot. Perustuslakituomioistuimen oikeuskäytännön mukaan ulkomaalaiset voivat tehdä perustuslakivalituksen siltä osin kuin heidän perusoikeutensa tunnustetaan Korean perustuslaissa (ks. selitykset kohdassa 1.1) ([176]). Perustuslakivalitus on tehtävä 90 päivän kuluessa siitä kun asianomainen on tullut tietoiseksi oikeuksiensa loukkauksesta ja vuoden kuluessa sen tapahtumisesta. Koska hallinnollisista riita-asioista annettuun lakiin perustuvaa menettelyä sovelletaan myös perustuslakituomioistuimesta annetun lain mukaisiin menettelyihin ([177]), valitus voidaan silti ottaa käsiteltäväksi, jos on olemassa ”perusteltu syy”, edellä kuvatun korkeimman oikeuden oikeuskäytännössä esitetyn tulkinnan mukaisesti.

Jos ensin on käytettävä muut oikeussuojakeinot, perustuslakivalitus on tehtävä 30 päivän kuluessa siitä kun tällaisessa menettelyssä on saatu lopullinen päätös ([178]). Perustuslakituomioistuin voi mitätöidä julkisen vallan käyttöön perustuvan toimen, joka johti perusoikeuksien loukkaamiseen, tai vahvistaa, että tietty laiminlyönti on perustuslain vastainen ([179]). Siinä tapauksessa toimivaltaisen viranomaisen on toteutettava tarvittavat toimenpiteet tuomioistuimen päätöksen noudattamiseksi.

3. VIRANOMAISTEN PÄÄSY TIETOIHIN KANSALLISEEN TURVALLISUUTEEN LIITTYVISSÄ TARKOITUKSISSA

3.1. Kansallisesta turvallisuudesta vastaavat toimivaltaiset lainvalvontaviranomaiset

Korean tasavallassa on kaksi tiedusteluvirastoa: kansallinen tiedustelupalvelu (*National Intelligence Service*, NIS) ja puolustuksen turvallisuus- ja tukipalvelujen esikunta (*Defense Security Support Command*, DSSC). Lisäksi myös poliisi ja syyttäjälaitos voivat kerätä henkilötietoja kansalliseen turvallisuuteen liittyviä tarkoituksia varten.

NIS on perustettu kansallisesta tiedustelupalvelusta annetulla lailla (*National Intelligence Service Act*), ja se toimii suoraan presidentin alaisuudessa ja valvonnassa ([180]). Sen tehtävänä on kerätä, koostaa ja jakaa erityisesti vieraita valtioita (ja Pohjois-Koreaa) koskevaa tietoa ([181]), vastavakoiluun liittyvää tiedustelutietoa (sotilas- ja teollisuusvakoilu mukaan lukien), tietoa terrorismista ja kansainvälisten rikollisjärjestöjen toiminnasta ja tietyntyyppisistä yleiseen ja kansalliseen turvallisuuteen kohdistuvista rikoksista (esim. maan sisäinen kapina, ulkoinen hyökkäys) ja tiedustelutietoa, joka liittyy kyberturvallisuuden varmistamiseen ja kyberhyökkäyksien ja -uhkien ehkäisemiseen ja torjuntaan ([182]). Kansallisesta tiedustelupalvelusta annetulla lailla perustetaan kyseinen tiedustelupalvelu ja vahvistetaan sen tehtävät, minkä lisäksi siinä esitetään sen toimintaa säätelevät yleiset periaatteet. Yleisperiaatteena on, että tiedustelupalvelun on säilytettävä poliittinen neutraalius ja suojeltava yksilöiden vapautta ja oikeuksia ([183]). Kansallisen tiedustelupalvelun johtajan tehtävänä on laatia yleiset suuntaviivat, joissa esitetään tiedustelupalvelun tehtäviä eli tietojen keruuta ja käyttöä koskevat periaatteet, soveltamisala ja menettelyt, ja hän raportoi niistä kansalliskokoukselle ([184]). Kansalliskokous (sen tiedusteluvaliokunta) voi vaatia suuntaviivojen korjaamista tai täydentämistä, jos se katsoo niiden olevan lainvastaisia tai perusteettomia. Tiedustelupalvelun johtaja ja henkilöstö eivät saa tehtäviään hoitaessaan käyttää väärin julkista valtaansa painostaakseen instituutioita, organisaatioita tai yksilöitä tekemään mitään sellaista, mihin niillä ei ole velvollisuutta, tai estääkseen jotakuta käyttämästä oikeuksiaan ([185]). Lisäksi tiedustelupalvelun on noudatettava viestinnän tietosuojalakia, paikkatiedoista annettua lakia (*Location Information Act*) ja rikosprosessilakia, kun se sensuroi viestejä, harjoittaa

([173]) Hallinnollisista riita-asioista annetun lain 20 §. Tätä määräaikaa sovelletaan myös laiminlyönnin lainvastaisuuden toteamista koskevaan vaatimukseen, ks. hallinnollisista riita-asioista annetun lain 38 §:n 2 momentti.
([174]) Korkeimman oikeuden päätös 90Nu6521, 28.6.1991.
([175]) Perustuslakituomioistuimesta annetun lain 68 §:n 1 momentti.
([176]) Perustuslakituomioistuimen päätös 99HeonMa194, 29.11.2001.
([177]) Perustuslakituomioistuimesta annetun lain 40 §.
([178]) Perustuslakituomioistuimesta annetun lain 69 §.
([179]) Perustuslakituomioistuimesta annetun lain 75 §:n 3 momentti.
([180]) Kansallisesta tiedustelupalvelusta annetun lain 2 § ja 4 §:n 2 momentti.
([181]) Tällä ei tarkoiteta yksilöitä koskevia tietoja, vaan yleistä tietoa vieraista valtioista (trendeistä ja kehityksestä) sekä kolmansien maiden valtiollisten toimijoiden toiminnasta.
([182]) Kansallisesta tiedustelupalvelusta annetun lain 3 §:n 1 momentti.
([183]) Lain 3 §:n 1 momentti, 6 §:n 2 momentti sekä 11 ja 21 §. Ks. myös eturistiriitoja koskevat säännöt, erityisesti lain 10 ja 12 §.
([184]) Kansallisesta tiedustelupalvelusta annetun lain 4 §:n 2 momentti.
([185]) Kansallisesta tiedustelupalvelusta annetun lain 13 §.

telekuuntelua, kerää paikka- tai televalvontatietoja tai tallentaa tai kuuntelee yksityistä viestintää ([186]). Toimivallan väärinkäytöstä tai tietojen keräämisestä näiden lakien vastaisesti voidaan määrätä rikosoikeudellisia seuraamuksia ([187]).

Puolustuksen turvallisuus- ja tukipalvelujen esikunta (*Defense Security Support Command*) on puolustusministeriön alaisuudessa toimiva sotilastiedusteluvirasto. Se vastaa turvallisuusasioista sotilasalalla, sotilasrikosten tutkinnasta (sotilastuomioistuimesta annetun lain (*Military Court Act*) mukaisesti) ja sotilastiedustelusta. Se ei yleensä harjoita siviilien tarkkailua, ellei se ole tarpeen sen sotilaallisten tehtävien hoitamiseksi. Esikunta voi tutkia ainoastaan sotilashenkilöstöä ja puolustusvoimien siviilihenkilöstöä sekä henkilöitä, jotka osallistuvat sotilaskoulutukseen tai kuuluvat reserviin tai rekrytointipalveluun sekä sotavankeja ([188]). Kun esikunta kerää viestintätietoja kansalliseen turvallisuuteen liittyviä tarkoituksia varten, sen on noudatettava viestinnän tietosuojalaissa ja sen täytäntöönpanoasetuksessa säädettyjä rajoituksia ja suojatoimia.

3.2. **Oikeusperustat ja rajoitukset**

Viestinnän tietosuojalaissa, terrorismintorjuntalaissa (*Act on Anti-Terrorism for the Protection of Citizens and Public Security*) ja televiestintäyrityksiä koskevassa laissa vahvistetaan oikeusperustat sekä sovellettavat rajoitukset ja suojatoimet, joiden nojalla henkilötietoja voidaan kerätä kansalliseen turvallisuuteen liittyviä tarkoituksia varten ([189]). Näillä rajoituksilla ja suojatoimilla, joita käsitellään tarkemmin jäljempänä, varmistetaan, että henkilötietojen kerääminen rajoittuu siihen, mikä on ehdottoman välttämätöntä oikeutetun tavoitteen saavuttamiseksi. Henkilötietoja ei saa kerätä laajamittaisesti tai kohdentamattomasti myöskään kansalliseen turvallisuuteen liittyviä tarkoituksia varten.

3.2.1. *Viestintätietojen kerääminen*

3.2.1.1. Viestintätietojen kerääminen tiedusteluvirastojen toimesta

3.2.1.1.1. Oikeusperusta

Viestinnän tietosuojalaissa annetaan tiedusteluvirastoille valtuudet kerätä viestintätietoja ja velvoitetaan viestintäpalvelujen tarjoajat tekemään yhteistyötä niiden kanssa ([190]). Kuten kohdassa 2.2.2.1 esitetään, viestinnän tietosuojalaissa erotetaan yhtäältä viestinnän sisällön kerääminen (eli ”yhteydenpidon rajoittamista koskevat toimenpiteet” kuten ”telekuuntelu” tai ”sensuuri” ([191])) ja toisaalta ”televalvontatietojen” kerääminen ([192]).

Näitä kahta eri tyyppiä edustavien tietojen keräämisen edellytykset eroavat toisistaan, mutta sovellettavat menettelyt ja suojatoimet ovat pitkälti samat ([193]). Televalvontatietoja (eli metatietoja) saa kerätä kansalliseen turvallisuuteen kohdistuvien uhkien ehkäisemiseksi ([194]). Yhteydenpidon rajoittamista koskevien toimenpiteiden toteuttamiseen (eli viestinnän sisällön keräämiseen) sovelletaan tiukempia edellytyksiä, sillä niitä voidaan toteuttaa ainoastaan jos on olemassa kansalliseen turvallisuuteen kohdistuva vakava vaara ja tietojen kerääminen on välttämätöntä sen ehkäisemiseksi ([195]). Lisäksi pääsy viestinnän sisältöön sallitaan vain viimesijaisena keinona kansallisen turvallisuuden varmistamiseksi, ja viestinnän yksityisyyden loukkaus on pyrittävä minimoimaan ([196]). Myös silloin kun toimenpiteisiin on saatu asianmukainen hyväksyntä/lupa, ne on lopetettava heti kun ne eivät enää ole tarpeen, jotta voidaan varmistaa, että yksilön viestintäsalaisuuden loukkaus rajoitetaan mahdollisimman vähään ([197]).

3.2.1.1.2. Viestintätietojen keräämiseen sovellettavat rajoitukset ja suojatoimet silloin kun ainakin yksi viestinnän osapuoli on Korean kansalainen

Kun viestinnän osapuolista ainakin yksi on Korean kansalainen, viestintätietoja (sekä sisältöä että metatietoja) saa kerätä ainoastaan ylemmän oikeusasteen tuomioistuimen (*High Court*) ylemmän puheenjohtajan

([186]) Kansallisesta tiedustelupalvelusta annetun lain 14 §.
([187]) Kansallisesta tiedustelupalvelusta annetun lain 22 ja 23 §.
([188]) Sotilastuomioistuimesta annetun lain 1 §.
([189]) Kansalliseen turvallisuuteen liittyvien rikosten tutkinnassa poliisin ja kansallisen tiedustelupalvelun on noudatettava rikosprosessilakia, kun taas sotilastiedustelupalvelun toimintaa säännellään sotilastuomioistuinlailla.
([190]) Viestinnän tietosuojalain 15-2 §.
([191]) Viestinnän tietosuojalain 2 §:n 6 ja 7 momentti.
([192]) Viestinnän tietosuojalain 2 §:n 11 momentti.
([193]) Ks. viestinnän tietosuojalain 13-4 §:n 2 momentti ja sen täytäntöönpanoasetuksen 37 §:n 4 momentti, joiden mukaan viestinnän sisällön keräämiseen sovellettavia menettelyjä sovelletaan soveltuvin osin myös televalvontatietojen keräämiseen.
([194]) Viestinnän tietosuojalain 13-4 §.
([195]) Viestinnän tietosuojalain 7 §:n 1 momentti.
([196]) Viestinnän tietosuojalain 3 §:n 2 momentti.
([197]) Viestinnän tietosuojalain täytäntöönpanoasetuksen 2 §.

luvalla ([198]). Asiaa koskeva tiedusteluviraston pyyntö on esitettävä kirjallisesti syyttäjälle tai ylemmän syyttäjän virastolle ([199]). Pyynnössä on ilmoitettava keräämisen syyt (esimerkiksi kansallista turvallisuutta uhkaava vakava vaara, tai että keruu on tarpeen kansalliseen turvallisuuteen kohdistuvien uhkien ehkäisemiseksi) ja perusteluna toimiva näyttö sekä pyyntöön liittyvät yksityiskohdat (eli keräämisen tavoitteet, kohteena oleva(t) yksilö(t), soveltamisala, keruuaika ja se, missä ja miten kerääminen on tarkoitus suorittaa) ([200]). Syyttäjä / ylemmän syyttäjän virasto pyytää puolestaan lupaa ylemmän oikeusasteen tuomioistuimen ylemmältä puheenjohtajalta ([201]). Puheenjohtaja voi antaa kirjallisen luvan vain jos hän katsoo hakemuksen olevan perusteltu; muussa tapauksessa pyyntö hylätään ([202]). Tietojenkeruuta koskevassa päätöksessä täsmennetään keräämisen tyyppi, tavoite, kohde, laajuus ja keräämisaika sekä se, missä ja miten kerääminen voidaan suorittaa ([203]).

Erityisiä sääntöjä sovelletaan silloin kun kyseessä on salahankkeeseen liittyvä toiminta, joka uhkaa kansallista turvallisuutta, eikä vallitsevan hätätilanteen vuoksi ole mahdollista noudattaa edellä mainittuja menettelyjä ([204]). Kun nämä edellytykset täyttyvät, tiedusteluvirastot voivat toteuttaa tarkkailutoimenpiteitä ilman tuomioistuimen ennakkohyväksyntää ([205]). Tiedusteluviraston on kuitenkin pyydettävä tuomioistuimen hyväksyntää heti kun hätätoimenpiteet on toteutettu. Jos hyväksyntää ei saada 36 tunnin kuluessa toimenpiteiden toteuttamisesta, ne on lopetettava välittömästi ([206]). Hätätilanteessa tietojen keräämisen on kuitenkin aina tapahduttava ”hätätilanteen sensuuria/kuuntelua koskevan lausunnon” mukaisesti, ja tiedot keräävän tiedusteluviraston on pidettävä kirjaa kaikista hätätoimenpiteistä ([207]).

Jos tarkkailu saadaan päätökseen lyhyessä ajassa, niin että tuomioistuimen hyväksyntää ei ole ehditty saada, toimivaltaisen syyttäjänviraston johtajan on lähetettävä toimivaltaisen tuomioistuimen puheenjohtajalle tiedusteluviraston laatima ilmoitus hätätilanteen toimenpiteen toteuttamisesta, joka pitää kirjaa hätätoimenpiteistä ([208]). Näin tuomioistuin voi tutkia tietojen keräämisen lainmukaisuuden.

3.2.1.1.3. Viestintätietojen keräämiseen sovellettavat rajoitukset ja suojatoimet silloin kun kaikki viestinnän osapuolet ovat muita kuin Korean kansalaisia

Jotta tiedusteluvirastot voisivat kerätä tietoja yksinomaan muiden kuin Korean kansalaisten välisestä viestinnästä, niiden on saatava etukäteen presidentin kirjallinen hyväksyntä ([209]). Tällaisia viestejä kerätään kansalliseen turvallisuuteen liittyviä tarkoituksia varten vain jos ne kuuluvat johonkin erikseen mainittuun ryhmään eli kun viestien lähettäjät tai vastaanottajat ovat Korean tasavallalle vihamielisten maiden virkamiehiä tai muita yksilöitä, tai vieraiden valtioiden elimiä, ryhmiä tai kansalaisia, joiden epäillään osallistuvan Korean-vastaiseen toimintaan ([210]), tai sellaisten Korean niemimaalla olevien ryhmien jäseniä, jotka eivät tosiasiallisesti kuulu Korean tasavallan suvereniteetin piiriin, tai tällaisten ryhmien vieraissa valtioissa toimivien kattoryhmien jäseniä ([211]). Jos taas yksi viestinnän osapuoli on Korean kansalainen ja toinen ei, vaaditaan tuomioistuimen hyväksyntä kohdassa 3.2.1.1.2 kuvatun menettelyn mukaisesti.

Tiedusteluviraston johtajan on esitettävä aiottuja toimenpiteitä koskeva suunnitelma kansallisen tiedustelupalvelun johtajalle ([212]). Tämä tarkistaa, että suunnitelma on asianmukainen, ja toimittaa sen sitten presidentin hyväksyttäväksi ([213]). Suunnitelmassa on esitettävä samat tiedot kuin silloin kun tuomioistuimelta haetaan lupaa kerätä Korean kansalaisten tietoja (ks. edellä) ([214]). Siinä on ilmoitettava erityisesti keräämisen syyt (esimerkiksi kansallista turvallisuutta uhkaava vakava vaara, tai että keruu on tarpeen kansalliseen turvallisuuteen kohdistuvien uhkien ehkäisemiseksi), tärkeimmät

([198]) Viestinnän tietosuojalain 7 §:n 1 momentin 1 kohta. Toimivaltainen tuomioistuin on jommankumman tai kummankin tarkkailukohteen koti- tai toimipaikan ylemmän oikeusasteen tuomioistuin.
([199]) Viestinnän tietosuojalain täytäntöönpanoasetuksen 7 §:n 3 momentti.
([200]) Viestinnän tietosuojalain 7 §:n 3 momentti ja 6 §:n 4 momentti.
([201]) Viestinnän tietosuojalain täytäntöönpanoasetuksen 7 §:n 4 momentti. Syyttäjän tuomioistuimelle esittämässä pyynnössä on esitettävä pääasialliset syyt epäilylle, ja jos pyyntö koskee samanaikaisesti useita lupia, niiden perustelut (ks. viestinnän tietosuojalain täytäntöönpanoasetuksen 4 §).
([202]) Viestinnän tietosuojalain 7 §:n 3 momentti sekä 6 §:n 5 ja 9 momentti.
([203]) Viestinnän tietosuojalain 7 §:n 3 momentti ja 6 §:n 6 momentti.
([204]) Viestinnän tietosuojalain 8 §.
([205]) Viestinnän tietosuojalain 8 §:n 1 momentti.
([206]) Viestinnän tietosuojalain 8 §:n 2 momentti.
([207]) Viestinnän tietosuojalain 8 §:n 4 momentti. Ks. edellä kohta 2.2.2.2 hätätoimenpiteet lainvalvonnan yhteydessä.
([208]) Viestinnän tietosuojalain 8 §:n 5 ja 7 momentti. Ilmoituksessa on annettava tiedot tarkkailutoimenpiteen tavoitteesta, kohteesta, soveltamisalasta, kestosta, toteuttamispaikasta ja -tavasta sekä perusteet, joiden vuoksi pyyntöä ei ole esitetty ennen toimenpiteen toteuttamista (viestinnän tietosuojalain 8 §:n 6 momentti).
([209]) Viestinnän tietosuojalain 7 §:n 1 momentin 2 kohta.
([210]) Tällä tarkoitetaan toimintaa, joka uhkaa kansakunnan olemassaoloa ja turvallisuutta, demokraattista järjestystä tai kansalaisten elämää ja vapautta.
([211]) Jos taas yksi osapuoli on viestinnän tietosuojalain 7 §:n 1 momentin 2 kohdassa tarkoitettu henkilö ja toinen osapuoli tuntematon tai määrittämätön, sovelletaan 7 §:n 1 momentin 2 kohdassa kuvattua menettelyä.
([212]) Viestinnän tietosuojalain täytäntöönpanoasetuksen 8 §:n 1 momentti. Kansallisen tiedustelupalvelun johtajan nimittää presidentti kansalliskokouksen hyväksynnän jälkeen (kansallisesta tiedustelupalvelusta annetun lain 7 §).
([213]) Viestinnän tietosuojalain täytäntöönpanoasetuksen 8 §:n 2 momentti.
([214]) Viestinnän tietosuojalain täytäntöönpanoasetuksen 8 §:n 3 momentti yhdessä lain 6 §:n 4 momentin kanssa.

epäilynaiheet ja perusteluna toimiva näyttö sekä pyyntöön liittyvät yksityiskohdat (eli keräämisen tavoitteet, kohteena oleva(t) yksilö(t), soveltamisala, keruuaika ja se, missä ja miten kerääminen on tarkoitus suorittaa). Jos samanaikaisesti haetaan useita lupia, on esitettävä niiden kaikkien tarkoitus ja perustelut ([215]).

Hätätilanteissa ([216]) on saatava ennakkohyväksyntä ministeriltä, jonka alaisuuteen asianomainen tiedusteluvirasto kuuluu. Tällöin tiedusteluviraston on pyydettävä presidentin hyväksyntää välittömästi hätätoimenpiteiden toteuttamisen jälkeen. Jos hyväksyntää ei saada 36 tunnin kuluessa hakemuksen tekemisestä, tietojen kerääminen on lopetettava välittömästi ([217]). Tällaisissa tapauksissa kerätyt tiedot on aina tuhottava.

3.2.1.1.4. Yleiset rajoitukset ja suojatoimet

Erityisesti silloin kun tiedusteluvirastot vaativat yksityisiä palveluntarjoajia tekemään yhteistyötä, niiden on esitettävä tuomioistuimen päätös / presidentin ennakkohyväksyntä tai jäljennös hätätilanteen sensuuria koskevan lausunnon kansilehdestä, joka yhteistyöhön pakotetun yksikön on säilytettävä tiedostoissaan ([218]). Yksiköt, joita vaaditaan luovuttamaan tietoja tiedusteluvirastoille viestinnän tietosuojalain nojalla, voivat kieltäytyä siitä, jos hyväksynnässä tai hätäsensuuria koskevassa lausunnossa viitataan väärään tunnisteeseen (esim. puhelinnumero kuuluu eri henkilölle kuin sille, joka on toimenpiteen kohteena). Televiestinnässä käytettäviä salasanoja ei saa paljastaa missään tapauksessa ([219]).

Tiedusteluvirastot voivat uskoa yhteydenpitoa rajoittavien toimenpiteiden toteuttamisen tai telekuuntelutietojen keräämisen postitoimistolle tai televiestintäpalvelujen tarjoajalle (nämä on määritelty televiestintäyrityksiä koskevassa laissa) ([220]). Sekä asianomaisen tiedusteluviraston että yhteistyöpyynnön vastaanottavan palveluntarjoajan on pidettävä rekisteriä, josta käy ilmi toimenpidepyyntöjen tarkoitus, niiden täytäntöönpanon tai yhteistyön ajankohta sekä toimenpiteiden kohde (esim. posti, puhelin, sähköposti) kolmen vuoden ajan ([221]). Televalvontatietoja toimittavien palveluntarjoajien on säilytettävä seitsemän vuoden ajan tieto siitä, kuinka usein tällaisia tietoja kerätään, ja raportoitava siitä tiedeja tieto- ja viestintätekniikkaministeriölle kahdesti vuodessa ([222]).

Tiedusteluvirastojen on raportoitava keräämistään tiedoista ja tarkkailutoimien tuloksesta kansallisen tiedustelupalvelun johtajalle ([223]). Televalvontatietojen osalta tiedusteluelinten on pidettävä kirjaa siitä, että tällaisia tietoja koskeva pyyntö on esitetty, ja talletettava myös kyseinen kirjallinen pyyntö ja tieto sen esittäneestä instituutiosta ([224]).

Sekä viestinnän sisällön että televalvontatietojen kerääminen saa kestää enintään neljä kuukautta, ja se on lopetettava välittömästi, jos asetettu tavoite saavutetaan aikaisemmin ([225]). Jos lupaedellytykset ovat edelleen voimassa, määräaikaa voidaan jatkaa enintään neljällä kuukaudella tuomioistuimen tai presidentin luvalla. Hakemus tarkkailutoimenpiteiden jatkamista koskevan hyväksynnän saamiseksi on esitettävä kirjallisesti, ja siinä on mainittava syyt, joiden vuoksi pidentämistä haetaan ja toimitettava näyttöä ([226]).

Keräämisen oikeusperustasta riippuen yksilöille yleensä ilmoitetaan heidän viestiensä keräämisestä. Riippumatta siitä, kerätäänkö viestinnän sisältöä vai televalvontatietoja ja onko tiedot saatu tavanomaisessa menettelyssä vai hätätilanteessa, tiedusteluviraston johtajan on ilmoitettava asianomaiselle tällaisesta tarkkailutoimenpiteestä kirjallisesti 30 päivän kuluessa siitä kun tarkkailu on päättynyt ([227]). Ilmoituksessa on mainittava 1) se, että tietoja on kerätty,

([215]) Viestinnän tietosuojalain täytäntöönpanoasetuksen 8 §:n 3 momentti ja 4 §.
([216]) Eli silloin kun toimenpiteen kohteena on salahankkeeseen liittyvä toiminta, joka uhkaa kansallista turvallisuutta, eikä ole aikaa pyytää presidentin hyväksyntää, ja hätätoimenpiteiden laiminlyönti voisi vaarantaa kansallisen turvallisuuden (viestinnän tietosuojalain 8 §:n 8 momentti).
([217]) Viestinnän tietosuojalain 8 §:n 9 momentti.
([218]) Viestinnän tietosuojalain 9 §:n 2 momentti ja sen täytäntöönpanoasetuksen 12 §.
([219]) Viestinnän tietosuojalain 9 §:n 4 momentti.
([220]) Viestinnän tietosuojalain täytäntöönpanoasetuksen 13 §.
([221]) Viestinnän tietosuojalain 9 §:n 3 momentti ja sen täytäntöönpanoasetuksen 17 §:n 2 momentti. Tätä määräaikaa ei sovelleta televalvontatietoihin (ks. viestinnän tietosuojalain täytäntöönpanoasetuksen 39 §).
([222]) Viestinnän tietosuojalain 13 §:n 7 momentti ja sen täytäntöönpanoasetuksen 39 §.
([223]) Viestinnän tietosuojalain täytäntöönpanoasetuksen 18 §:n 3 momentti.
([224]) Viestinnän tietosuojalain 13 §:n 5 momentti ja 13-4 §:n 3 momentti.
([225]) Viestinnän tietosuojalain 7 §:n 2 momentti.
([226]) Viestinnän tietosuojalain 7 §:n 2 momentti ja sen täytäntöönpanoasetuksen 5 §.
([227]) Viestinnän tietosuojalain 9-2 §:n 3 momentti. Viestinnän tietosuojalain 13-4 §:n mukaisesti tämä koskee sekä viestinnän sisällön että televalvontatietojen keräämistä.

2) täytäntöönpanosta vastaava virasto ja 3) täytäntöönpanoaika. Ilmoittamista voidaan kuitenkin lykätä, jos se vaarantaisi kansallisen turvallisuuden tai uhkaisi ihmisten henkeä ja fyysistä turvallisuutta ([228]). Ilmoitus on tehtävä 30 päivän kuluessa siitä kun lykkäyksen syyt ovat lakanneet olemasta ([229]).

Ilmoitusvelvollisuutta sovelletaan kuitenkin tietojen keräämiseen vain silloin kun ainakin yksi osapuolista on Korean kansalainen. Näin ollen muille kuin Korean kansalaisille ilmoitetaan vain jos kerääminen kohdistuu heidän viestintäänsä Korean kansalaisten kanssa. Ilmoitusvelvollisuutta ei siis ole silloin kun viestintä tapahtuu yksinomaan muiden kuin Korean kansalaisten kesken.

Viestinnän sisältöä ja televalvontatietoja, jotka on hankittu tarkkailun avulla viestinnän tietosuojalain nojalla, voidaan käyttää ainoastaan 1) tiettyjen rikosten tutkinnassa, syytteeseenpanossa tai ehkäisemisessä, 2) kurinpitomenettelyissä, 3) oikeudenkäynnissä, kun viestinnän osapuoli vetoaa niihin vahingonkorvauksen saamiseksi, tai 4) jos tietojen käyttö sallitaan muissa laeissa ([230]).

3.2.1.2. Viestintätietojen kerääminen poliisin/syyttäjien toimesta kansalliseen turvallisuuteen liittyviä tarkoituksia varten

Poliisi/syyttäjä voi kerätä viestintätietoja (sekä sisältöä että televalvontatietoja) kansalliseen turvallisuuteen liittyviä tarkoituksia varten samoin edellytyksin kuin ne, joita käsitellään kohdassa 3.2.1.1. Hätätilanteissa ([231]) sovellettava menettely on edellä kuvattu menettely, jota sovelletaan viestinnän sisällön keräämiseen lainvalvontatarkoituksia varten hätätilanteissa (ks. viestinnän tietosuojalain 8 §).

3.2.2. *Terroristiepäiltyjen tietojen kerääminen*

3.2.2.1. Oikeusperusta

Terrorismintorjuntalaissa annetaan kansallisen tiedustelupalvelun johtajalle valtuudet kerätä tietoja terroristiepäillyistä ([232]). *"Terroristiepäillyllä"* tarkoitetaan terroristiryhmän jäsentä ([233]), henkilöä, joka on tukenut terroristiryhmää (edistämällä ja levittämällä sen aatteita tai taktiikkaa), kerännyt tai antanut varoja terrorismiin ([234]), tai osallistunut muuhun toimintaan, jolla valmistellaan tai edistetään terrorismia tai vehkeillään ja yllytetään siihen, tai henkilöä, jonka voidaan perustellusti epäillä harjoittaneen tällaista toimintaa ([235]). Pääsääntönä on, että terrorismintorjuntalain täytäntöönpanosta vastaavien viranomaisten on kunnioitettava Korean perustuslaissa vahvistettuja perusoikeuksia ([236]).

Terrorismintorjuntalaissa itsessään ei säädetä terrorismiepäiltyjen tietojen keräämisen yhteydessä sovellettavista erityisistä valtuuksista, rajoituksista tai suojatoimista, vaan siinä viitataan muissa säädöksissä vahvistettuihin menettelyihin. Terrorismintorjuntalain nojalla kansallisen tiedustelupalvelun johtaja voi ensinnäkin kerätä 1) tietoa maahantulosta Korean tasavaltaan ja maasta lähdöstä, 2) tietoa rahoitustoimista ja 3) viestintätietoja. Riippuen siitä, minkätyyppisiä tietoja hankitaan, asiaa koskevat menettelyvaatimukset on vahvistettu maahanmuuttolaissa (*Immigration Act*), tullilaissa (*Customs Act*), rahoitustoimia koskevasta raportoinnista annetussa laissa tai viestinnän tietosuojalaissa ([237]). Maahantuloa ja maastalähtöä koskevien tietojen keräämisen osalta terrorismintorjuntalaissa viitataan maahanmuuttolaissa ja tullilaissa säädettyihin menettelyihin. Näissä laeissa ei kuitenkaan tällä hetkellä säädetä tällaisista toimivaltuuksista. Viestintätietojen

([228]) Viestinnän tietosuojalain 9-2 §:n 4 momentti.
([229]) Viestinnän tietosuojalain 13-4 §:n 2 momentti ja 9-2 §:n 6 momentti.
([230]) Viestinnän tietosuojalain 5 §:n 1 ja 2 momentti sekä 12 ja 13-5 §.
([231]) Eli silloin kun toimenpiteen kohteena on salahankkeeseen liittyvä toiminta, joka uhkaa kansallista turvallisuutta, eikä ole mahdollista soveltaa tavanomaista hyväksymismenettelyä (viestinnän tietosuojalain 8 §:n 1 momentti).
([232]) Terrorismintorjuntalain 9 §.
([233]) *"Terroristiryhmällä"* tarkoitetaan ryhmää, jonka Yhdistyneet kansakunnat on nimennyt terroristiryhmäksi (terrorismintorjuntalain 2 §:n 2 momentti).
([234]) "Terrorismilla" tarkoitetaan terrorismintorjuntalain 2 §:n 1 momentissa esitetyn määritelmän mukaan toimintaa, jonka tarkoituksena on estää valtiota, paikallishallintoa tai vieraan valtion hallitusta (myös kansainvälisiä järjestöjä) käyttämästä toimivaltaansa tai pakottaa ne toteuttamaan toimia ilman oikeudellista velvoitetta, tai uhata yleisöä. Tämä tarkoittaa muun muassa a) henkilön surmaamista tai hengenvaaran aiheuttamista ruumiinvamman seurauksena taikka henkilön pidättämistä, eristämistä, sieppaamista tai panttivangiksi ottamista; b) tietyntyyppistä ilma-alukseen kohdistuvaa toimintaa (esim. pudottaminen, sieppaaminen tai ilmassa olevan aluksen vahingoittaminen); c) tietyntyyppistä alukseen kohdistuvaa toimintaa (esim. toiminnassa olevan aluksen tai meriliikenteen rakenteen haltuunotto, tuhoaminen tai vahingoittaminen siinä määrin, että sen turvallisuus vaarantuu, mukaan lukien toiminnassa olevan aluksen tai meriliikenteen rakenteen lastin vahingoittaminen); d) biokemiallisten aseiden, räjähteiden tai tuliaseiden tai laitteiden sijoittamista, laukaisemista tai käyttämistä millä tahansa muulla tavoin kuoleman, vakavan vamman tai vakavan aineellisen vahingon aiheuttamiseksi tai tällaisen vaikutuksen aiheuttamista tietyntyyppisillä ajoneuvoilla tai laitoksilla (esim. junat, raitiovaunut, moottoriajoneuvot, yleiset puistot ja asemat sekä sähkö- ja kaasulaitokset ja televiestintäpalveluja tarjoavat laitokset); e) tietyntyyppistä toimintaa, joka liittyy ydinmateriaaleihin ja radioaktiivisiin aineisiin tai ydinlaitoksiin (esim. hengenvaaran tai ruumiinvamman aiheuttaminen ja omaisuuden vahingoittaminen tai yleisen turvallisuuden häiritseminen muulla tavoin tuhoamalla ydinreaktori tai käsittelemällä radioaktiivisia aineita väärin).
([235]) Terrorismintorjuntalain 2 §:n 3 momentti.
([236]) Terrorismintorjuntalain 3 §:n 3 momentti.
([237]) Terrorismintorjuntalain 9 §:n 1 momentti.

ja rahoitustoimia koskevien tietojen keräämisen osalta terrorismintorjuntalaissa viitataan viestinnän tietosuojalaissa säädettyihin rajoituksiin ja suojatoimiin (joita täsmennetään jäljempänä) sekä rahoitustoimia koskevasta raportoinnista annettuun lakiin (joka ei ole merkityksellinen tietosuojan riittävyyttä koskevan arvioinnin kannalta, kuten kohdassa 2.1 selitetään).

Lisäksi terrorismintorjuntalain 9 §:n 3 momentissa täsmennetään, että kansallisen tiedustelupalvelun johtaja voi pyytää terroristiepäillyn henkilötietoja rekisterinpitäjältä ([238]) tai paikkatietoja tällaisten tietojen toimittajalta ([239]). Tämä mahdollisuus rajoittuu vapaaehtoisiin luovuttamispyyntöihin, joihin henkilötietojen rekisterinpitäjien ja paikkatietojen toimittajien ei tarvitse vastata, ja joihin ne voivat joka tapauksessa vastata ainoastaan tietosuojalain ja paikkatiedoista annetun lain mukaisesti (ks. kohta 3.2.2.2 jäljempänä).

3.2.2.2. Tietojen vapaaehtoiseen luovuttamiseen tietosuojalain ja paikkatiedoista annetun lain nojalla sovellettavat rajoitukset ja suojatoimet

Terrorismintorjuntalain nojalla esitettävät vapaaehtoista yhteistyötä koskevat pyynnöt on rajoitettava terroristiepäiltyjä koskeviin tietoihin (ks. kohta 3.2.2.1 edellä). Kaikissa tällaisissa kansallisen tiedustelupalvelun pyynnöissä on noudatettava Korean perustuslaissa vahvistettuja lainmukaisuuden, tarpeellisuuden ja oikeasuhteisuuden periaatteita (12 §:n 1 momentti ja 37 §:n 2 momentti) ([240]) sekä henkilötietojen keräämistä koskevia tietosuojalain vaatimuksia (3 §:n 1 momentti, ks. kohta 1.2 edellä). Kansallisesta tiedustelupalvelusta annetussa laissa täsmennetään lisäksi, että tiedustelupalvelu ei saa tehtäviään hoitaessaan käyttää väärin julkista valtaansa painostaakseen instituutioita, organisaatioita tai yksilöitä tekemään mitään sellaista, mihin niillä ei ole velvollisuutta, tai estääkseen jotakuta käyttämästä oikeuksiaan ([241]). Tämän kiellon rikkomisesta voidaan määrätä rikosoikeudellisia seuraamuksia ([242]).

Henkilötietojen rekisterinpitäjät ja paikkatietojen toimittajat, jotka saavat kansalliselta tiedustelupalvelulta pyyntöjä terrorismintorjuntalain perusteella, eivät ole velvollisia noudattamaan niitä. Ne voivat tehdä niin vapaaehtoisesti, mutta ainoastaan tietosuojalain ja paikkatiedoista annetun lain mukaisesti. Tietosuojalain noudattamisen osalta rekisterinpitäjän on otettava huomioon erityisesti rekisteröidyn edut, eikä tietoja saa luovuttaa, jos se todennäköisesti loukkaisi oikeudetta asianomaisen yksilön tai kolmannen osapuolen etuja ([243]). Lisäksi tietojen luovuttamisesta on ilmoitettava asianomaiselle henkilölle tietosuojalautakunnan antaman ilmoituksen N:o 2021-1 nojalla. Ilmoittamista voidaan lykätä poikkeuksellisissa tilanteissa, erityisesti jos ja niin kauan kuin se vaarantaisi meneillään olevan rikostutkinnan tai todennäköisesti vahingoittaisi toisen henkilön henkeä tai terveyttä, jos nämä oikeudet tai edut ovat selvästi rekisteröidyn oikeuksia tärkeämmät ([244]).

3.2.2.3. Viestinnän tietosuojalain mukaiset rajoitukset ja suojatoimet

Terrorismintorjuntalain mukaan tiedusteluvirastot voivat kerätä viestintätietoja (sekä sisältöä että televalvontatietoja) vain jos se on tarpeen terrorismintorjuntatoimien vuoksi eli terrorismin ehkäisemiseksi ja torjumiseksi. Viestinnän tietosuojalain menettelyjä, joita käsitellään kohdassa 3.2.1, sovelletaan viestintätietojen keräämiseen terrorismintorjuntaa varten.

3.2.3. *Tietojen vapaaehtoinen luovuttaminen televiestintäpalvelujen tarjoajien toimesta*

Televiestintäyrityksiä koskevan lain mukaan televiestintäpalvelujen tarjoajat voivat luovuttaa ”viestintätietoja” vapaaehtoisesti, jos jokin tiedusteluvirasto pyytää niitä kansalliseen turvallisuuteen kohdistuvan uhkan estämiseksi ([245]). Kaikissa tällaisissa pyynnöissä on noudatettava Korean perustuslaissa vahvistettuja lainmukaisuuden, tarpeellisuuden ja oikeasuhteisuuden periaatteita (12 §:n 1 momentti ja 37 §:n 2 momentti) ([246]) sekä henkilötietojen keräämistä koskevia tietosuojalain vaatimuksia (3 §:n 1 momentti, ks. kohta 1.2 edellä). Lisäksi sovelletaan samoja rajoituksia ja suojatoimia kuin silloin kun tietoja luovutetaan vapaaehtoisesti lainvalvontatarkoituksia varten (ks. kohta 2.2.3) ([247]).

([238]) Tietosuojalain 2 §:ssä olevan määritelmän mukaisesti julkinen laitos, oikeushenkilö, organisaatio tai henkilö ym., joka käsittelee henkilötietoja henkilötietorekisterissä suoraan tai välillisesti virallisia tarkoituksia tai liiketoimintaa varten.

([239]) Paikkatiedoista annetun lain 5 §:ssä olevan määritelmän mukaisesti jokainen, joka on saanut Korean viestintäpalvelukomissiolta (*Korea Communications Commission*) luvan harjoittaa paikkatietoja koskevaa liiketoimintaa.

([240]) Ks. myös terrorismintorjuntalain 3 §:n 2 ja 3 momentti.

([241]) Kansallisesta tiedustelupalvelusta annetun lain 11 §:n 1 momentti.

([242]) Kansallisesta tiedustelupalvelusta annetun lain 19 §.

([243]) Tietosuojalain 18 §:n 2 momentti.

([244]) Tietosuojalautakunnan asiakirja *Notification No. 2021-1 on Supplementary rules for the interpretation and application of the Personal Information Protection Act*, kohta III, 2, iii.

([245]) Televiestintäyrityksiä koskevan lain 83 §:n 3 momentti.

([246]) Ks. myös terrorismintorjuntalain 3 §:n 2 ja 3 momentti.

([247]) Pyyntö on esitettävä kirjallisesti, ja siinä on esitettävä pyynnön syyt sekä yhteys asianomaiseen käyttäjään ja pyydettyjen tietojen laajuus. Televiestintäpalvelujen tarjoajien on pidettävä pyynnöistä kirjaa ja raportoitava niistä tiede- ja tieto- ja viestintätekniikkaministeriölle kahdesti vuodessa.

Televiestintäpalvelujen tarjoajan ei ole pakko noudattaa pyyntöä, mutta se voi tehdä niin vapaaehtoisesti ja ainoastaan tietosuojalain mukaisesti. Tältä osin televiestintäpalvelujen tarjoajiin sovelletaan myös asianomaiselle ilmoittamisen osalta samoja velvoitteita kuin silloin kun ne saavat vastaavia pyyntöjä lainvalvontaviranomaisilta, ks. lähemmin kohta 2.2.3.

3.3. **Valvonta**

Korean tiedusteluvirastojen toimintaa valvovat eri elimet. Puolustuksen turvallisuus- ja tukipalvelujen esikuntaa valvoo kansallinen puolustusministeriö sisäisen tarkastuksen täytäntöönpanosta annetun ministeriön ohjeen (*Directive on Implementation of Internal Audit*) nojalla. Kansallisen tiedustelupalvelun toimintaa valvovat toimeenpanoelimet, kansalliskokous ja muut riippumattomat elimet, kuten jäljempänä tarkemmin selitetään.

3.3.1. *Ihmisoikeusvaltuutettu*

Kun tiedusteluvirastot keräävät tietoja terroristiepäillyistä, terrorismintorjuntalaissa säädetään terrorismintorjuntakomission (*Counterterrorism Commission*) ja ihmisoikeusvaltuutetun (*Human Rights Protection Officer*) valvonnasta ([248]).

Terrorismintorjuntakomission tehtäviin kuuluu muun muassa laatia terrorismintorjuntaa koskevia politiikkatoimia ja valvoa niiden toteuttamista sekä eri toimivaltaisten viranomaisten toimintaa terrorismintorjunnan alalla ([249]). Komission puheenjohtajana toimii pääministeri, ja siihen kuuluu useita ministereitä ja valtion virastojen johtajia, mm. ulkoministeri, oikeusministeri, puolustusministeri, sisäasiain- ja turvallisuusministeri, kansallisen tiedustelupalvelun johtaja ja kansallisen poliisiviraston päällikkö sekä rahoituspalvelukomission puheenjohtaja ([250]). Kun kansallisen tiedustelupalvelun johtaja suorittaa terrorismintorjuntaan liittyviä tutkintatoimia ja tarkkailee terroristiepäiltyjä terrorismintorjunnassa tarvittavien tietojen tai aineistojen keräämistä varten, hänen on raportoitava toimista terrorismintorjuntakomission puheenjohtajalle (eli pääministerille) ([251]).

Terrorismintorjuntalailla on myös perustettu ihmisoikeusvaltuutetun tehtävä yksilön oikeuksien suojaamiseksi terrorismintorjuntatoimista johtuvilta loukkauksilta ([252]). Terrorismintorjuntakomission puheenjohtaja nimittää ihmisoikeusvaltuutetun sellaisten henkilöiden joukosta, jotka täyttävät terrorismintorjuntalain täytäntöönpanoasetuksessa luetellut pätevyysvaatimukset (edellytyksenä on vähintään 10 vuoden kokemus asianajajan tehtävistä tai asiantuntemus ihmisoikeusalalta ja vähintään 10 vuoden työskentely apulaisprofessorina tai ylemmässä tehtävässä tai työskentely ylempänä virkamiehenä valtion tai paikallishallinnon virastossa, tai vähintään 10 vuoden työkokemus ihmisoikeusalalta esimerkiksi valtiosta riippumattomassa järjestössä ([253]). Ihmisoikeusvaltuutetun toimikausi on kaksi vuotta (se voidaan uusia), ja hänet voidaan erottaa tehtävästä vain erityisistä rajoitetuista ja perustelluista syistä, esimerkiksi jos häntä vastaan nostetaan syyte hänen tehtäviinsä liittyvässä rikosasiassa tai jos hän paljastaa luottamuksellisia tietoja tai pitkäaikaisen fyysisen tai psyykkisen toimintakyvyttömyyden vuoksi ([254]).

Ihmisoikeusvaltuutetulla on valtuudet antaa suosituksia ihmisoikeuksien suojelun parantamiseksi terrorismintorjuntaan osallistuvissa virastoissa ja käsitellä kansalaisvetoomuksia (ks. kohta 3.4.3) ([255]). Jos voidaan kohtuudella osoittaa virkamiehen syyllistyneen ihmisoikeuksien loukkaukseen virkatehtäviensä hoitamisessa, ihmisoikeusvaltuutettu voi suosittaa asianomaisen viraston johtajalle tällaisen loukkauksen korjaamista ([256]). Viraston on puolestaan ilmoitettava ihmisoikeusvaltuutetulle tällaisen suosituksen perusteella toteutetuista toimista ([257]). Jos virasto ei pane ihmisoikeusvaltuutetun suositusta täytäntöön, asia voidaan viedä terrorismintorjuntakomission ja sen puheenjohtajan eli pääministerin käsiteltäväksi. Toistaiseksi ei ole ollut tapauksia, joissa ihmisoikeusvaltuutetun suosituksia ei olisi pantu täytäntöön.

3.3.2. *Kansalliskokous*

Kuten kohdassa 2.3.2 esitetään, kansalliskokous voi tutkia ja tarkastaa viranomaisten toimintaa ja pyytää tässä yhteydessä luovuttamaan asiakirjoja ja vaatia todistajia tulemaan kuultavaksi. Kansallisen tiedustelupalvelun toimivaltaan

([248]) Terrorismintorjuntalain 7 §.
([249]) Terrorismintorjuntalain 5 §:n 3 momentti.
([250]) Terrorismintorjuntalain täytäntöönpanoasetuksen 3 §:n 1 momentti.
([251]) Terrorismintorjuntalain 9 §:n 4 momentti.
([252]) Terrorismintorjuntalain 7 §.
([253]) Terrorismintorjuntalain täytäntöönpanoasetuksen 7 §:n 1 momentti.
([254]) Terrorismintorjuntalain täytäntöönpanoasetuksen 7 §:n 3 momentti.
([255]) Terrorismintorjuntalain täytäntöönpanoasetuksen 8 §:n 1 momentti.
([256]) Terrorismintorjuntalain täytäntöönpanoasetuksen 9 §:n 1 momentti. Ihmisoikeusvaltuutettu päättää suositusten antamisesta itsenäisesti, mutta hänen on raportoitava suosituksista terrorismintorjuntakomission puheenjohtajalle.
([257]) Terrorismintorjuntalain täytäntöönpanoasetuksen 9 §:n 2 momentti.

kuuluvissa asioissa tästä parlamentaarisesta valvonnasta vastaa kansalliskokouksen tiedusteluvaliokunta (*Intelligence Committee of the National Assembly*) ([258]). Kansallisen tiedustelupalvelun johtaja, joka valvoo viraston tehtävien hoitamista, raportoi tiedusteluvaliokunnalle (ja presidentille) ([259]). Tiedusteluvaliokunta voi myös itse pyytää raporttia jostakin tietystä kysymyksestä, ja kansallisen tiedustelupalvelun johtajan on vastattava pyyntöön viipymättä ([260]). Tiedustelupalvelun johtaja voi kieltäytyä vastaamasta tai todistamasta valiokunnan edessä vain jos pyyntö koskee sotilaallisia, diplomaattisia tai Pohjois-Koreaan liittyviä valtionsalaisuuksia, joiden julkistaminen voisi aiheuttaa vakavia seurauksia maan kansalliselle kohtalolle ([261]). Tässä tapauksessa tiedusteluvaliokunta voi pyytää selitystä pääministeriltä. Jos selitystä ei anneta 7 päivän kuluessa, vastaamisesta tai todistamisesta ei voida kieltäytyä.

Jos kansalliskokous havaitsee laitonta tai sääntöjenvastaista toimintaa, se voi vaatia kyseistä viranomaista toteuttamaan korjaavia toimenpiteitä, esimerkiksi myöntämään vahingonkorvausta, toteuttamaan kurinpitotoimia tai parantamaan sisäisiä menettelyjään ([262]). Viranomaisen on toimittava tällaisen kehotuksen saatuaan viipymättä ja raportoitava toimenpiteiden tuloksesta kansalliskokoukselle. Viestinnän tietosuojalaissa säännellään erityisesti yhteydenpitoa rajoittaviin toimenpiteisiin (eli viestinnän sisällön keräämiseen) sovellettavaa parlamentaarista valvontaa ([263]). Kansalliskokous voi pyytää tiedusteluvirastojen päälliköiltä raporttia kaikista tällaisista toimenpiteistä. Lisäksi se voi suorittaa salakuuntelulaitteiden tarkastuksia paikalla. Niiden tiedusteluvirastojen, jotka ovat keränneet viestinnän sisältöä kansalliseen turvallisuuteen liittyviä tarkoituksia varten, sekä tällaisia tietoja luovuttaneiden televiestintäpalvelujen tarjoajien on myös annettava kansalliskokoukselle pyynnöstä raportti näistä toimista.

3.3.3. *Valtion tilintarkastus- ja valvontaviranomainen*

Valtion tilintarkastus- ja valvontaviranomainen toteuttaa tiedusteluvirastoihin nähden samoja valvontatehtäviä kuin lainvalvonnan alalla (ks. kohta 2.3.2) ([264]).

3.3.4. *Tietosuojalautakunta*

Kun tietoja käsitellään kansalliseen turvallisuuteen liittyviä tarkoituksia varten, tietosuojalautakunta suorittaa täydentävää valvontaa, joka kattaa myös tietojen keräämisen. Kuten kohdassa 1.2 tarkemmin selitetään, tämä valvonta kattaa tietosuojalain 3 §:ssä ja 58 §:n 4 momentissa esitetyt yleiset periaatteet ja velvoitteet sekä 4 §:ssä taattujen yksilön oikeuksien käyttämisen. Tietosuojalain 7-8 §:n 3 ja 4 momentin ja 7-9 §:n 5 momentin mukaan tietosuojalautakunnan valvonta kattaa myös rikkomiset, jotka kohdistuvat erityislaeissa, kuten viestinnän tietosuojalaissa, terrorismintorjuntalaissa ja televiestintäyrityksiä koskevassa laissa annettuihin, henkilötietojen keräämiseen sovellettavia rajoituksia ja suojatoimia koskeviin sääntöihin. Kun otetaan huomioon tietosuojalain 3 §:n 1 momentissa säädetyt vaatimukset, joiden mukaan henkilötietojen keräämisen on tapahduttava lainmukaisesti ja asianmukaisesti, mainittujen erityislakien rikkominen merkitsee samalla tietosuojalain rikkomista. Tietosuojalautakunnalla on näin ollen valtuudet tutkia ([265]) rikkomisia, jotka koskevat lakeja, joilla säännellään pääsyä tietoihin kansalliseen turvallisuuteen liittyviä tarkoituksia varten, sekä tietosuojalakiin sisältyviä käsittelysääntöjä. Lisäksi se voi antaa ohjeita toimien parantamiseksi, määrätä korjaavia toimenpiteitä ja suosittaa kurinpitotoimia sekä saattaa mahdolliset rikokset toimivaltaisten tutkintaviranomaisten käsiteltäväksi ([266]).

3.3.5. *Kansallinen ihmisoikeuskomissio*

Kansallisen ihmisoikeuskomission valvonta koskee tiedusteluvirastoja samalla tavoin kuin muita valtion viranomaisia (ks. kohta 2.3.2).

3.4. **Yksilölliset oikeussuojakeinot**

3.4.1. *Ihmisoikeusvaltuutetun tarjoama oikeussuoja*

Kun henkilötietoja kerätään terrorismintorjuntatoimien yhteydessä, terrorismintorjuntakomission alaisuudessa toimiva ihmisoikeusvaltuutettu tarjoaa erityistä oikeussuojaa. Ihmisoikeusvaltuutettu käsittelee kansalaisvetoomuksia, jotka koskevat terrorismintorjuntatoimiin liittyviä ihmisoikeusloukkauksia ([267]). Hän voi suosittaa korjaavia toimia, ja asianomaisen viraston on raportoitava hänelle niiden toteuttamisesta. Yksilöille ei ole asetettu erityisiä vaatimuksia valituksen tekemiseksi ihmisoikeusvaltuutetulle. Tämä tarkoittaa, että ihmisoikeusvaltuutettu ottaa valituksen käsiteltäväksi, vaikka asianomainen henkilö ei vielä tässä vaiheessa pystyisi osoittamaan, että hänen oikeuksiaan on todella loukattu.

([258]) Kansalliskokouksesta annetun lain 36 § ja 37 §:n 1 momentin 16 kohta.
([259]) Kansallisesta tiedustelupalvelusta annetun lain 18 §.
([260]) Kansallisesta tiedustelupalvelusta annetun lain 15 §:n 2 momentti.
([261]) Kansallisesta tiedustelupalvelusta annetun lain 17 §:n 2 momentti. ”Valtionsalaisuuksilla ”tarkoitetaan *”valtionsalaisuuksiksi luokiteltuja tosiseikkoja, tavaroita tai tietoa, joihin pääsy on rajattu ja joita ei saa luovuttaa millekään toiselle maalle tai organisaatiolle, jotta voidaan välttää kansalliseen turvallisuuteen kohdistuvat vakavat haitat*”, ks. kansallisesta tiedustelupalvelusta annetun lain 13 §:n 4 momentti.
([262]) Valtionhallinnon tarkastuksista ja tutkimuksista annetun lain 16 §:n 2 momentti.
([263]) Viestinnän tietosuojalain 15 §.
([264]) Samoin kuin kansalliskokouksen tiedusteluvaliokunnan osalta, kansallisen tiedustelupalvelun johtaja voi kieltäytyä vastaamasta tilintarkastus- ja valvontavirastolle ainoastaan jos asia koskee valtionsalaisuuksia, joiden julkistamisella voisi olla vakavia seurauksia kansallisen turvallisuuden kannalta (kansallisesta tiedustelupalvelusta annetun lain 13 §:n 1 momentti).
([265]) Tietosuojalain 63 §.
([266]) Tietosuojalain 61 §:n 2 momentti, 65 §:n 1 ja 2 momentti sekä 64 §:n 4 momentti.
([267]) Terrorismintorjuntalain täytäntöönpanoasetuksen 8 §:n 1 momentin 2 kohta.

3.4.2. *Tietosuojalakiin perustuvat oikeussuojakeinot*

Tietosuojalain mukaan yksilöillä on pääsyoikeus omiin henkilötietoihinsa, joita käsitellään kansalliseen turvallisuuteen liittyviä tarkoituksia varten, ja oikeus oikaista tai poistaa ne ja keskeyttää niiden käsittely ([268]). Näiden oikeuksien käyttöä koskevat pyynnöt voidaan toimittaa joko suoraan asianomaiselle tiedusteluvirastolle tai välillisesti tietosuojalautakunnan kautta. Tiedusteluvirasto voi lykätä tai rajoittaa näiden oikeuksien käyttöä tai evätä sen vain siltä osin ja niin pitkäksi aikaa kuin se on tarpeen ja oikeasuhteista yleisen edun mukaisen tärkeän tavoitteen suojelemiseksi (esimerkiksi siltä osin ja niin kauan kuin oikeuden myöntäminen vaarantaisi meneillään olevan tutkinnan tai uhkaisi kansallista turvallisuutta), tai kun oikeuden myöntäminen voisi vahingoittaa kolmannen osapuolen henkeä tai terveyttä. Jos pyyntö evätään tai sitä rajoitetaan, yksilölle on ilmoitettava syyt siihen viipymättä.

Lisäksi yksilöillä on oikeus asianmukaisiin oikeussuojakeinoihin tietosuojalain 58 §:n 4 momentin (vaatimus varmistaa, että rekisteröityjen valitukset käsitellään asianmukaisesti) ja 4 §:n 5 momentin (oikeus asianmukaisiin oikeussuojakeinoihin henkilötietojen käsittelystä mahdollisesti aiheutuvien vahinkojen korjaamiseksi) mukaisesti. Tähän sisältyy oikeus ilmoittaa väitetystä rikkomisesta Korean internet- ja turvallisuusviraston ylläpitämään Privacy Call Centre -puhelinpalveluun ja tehdä valitus tietosuojalautakunnalle ([269]). Nämä oikeussuojakeinot ovat käytettävissä myös silloin kun mahdollinen rikkominen koskee erityislakien säännöksiä (esim. kansallista turvallisuutta koskevien lakien säännöksiä, joissa säädetään henkilötietojen keräämistä koskevista rajoituksista ja suojatoimista) tai tietosuojalain säännöksiä. Kuten ilmoituksessa N:o 2021-1 todetaan, EU:n yksilöt voivat tehdä valituksen Korean tietosuojalautakunnalle oman kansallisen tietosuojaviranomaisensa välityksellä. Siinä tapauksessa tietosuojalautakunta ilmoittaa yksilölle samaa tietä (kansallisen tietosuojaviranomaisen tai Euroopan tietosuojaneuvoston välityksellä), kun tutkimus on päättynyt (ja mahdollisesti määrätyistä korjaavista toimenpiteistä). Tietosuojalautakunnan päätöksiin tai toimimatta jättämiseen voi hakea muutosta Korean tuomioistuimissa hallinnollisista riita-asioista annetun lain nojalla.

3.4.3. *Kansallisen ihmisoikeuskomission tarjoama oikeussuoja*

Kansallisen ihmisoikeuskomission tarjoama oikeussuoja koskee tiedusteluvirastoja samalla tavoin kuin muita valtion viranomaisia (ks. kohta 2.4.2).

3.4.4. *Oikeussuoja tuomioistuimissa*

Samoin kuin lainvalvontaviranomaisten toimien suhteen, yksilöt voivat hakea eri kanavia käyttäen oikeussuojaa tiedusteluvirastoja vastaan, jos he katsovat näiden rikkoneen edellä mainittuja rajoituksia ja suojatoimia.

Yksilöt voivat ensinnäkin vaatia vahingonkorvausta valtion korvauksista annetun lain nojalla. Vahingonkorvausta on myönnetty esimerkiksi tapauksessa, jossa puolustuksen tukipalvelujen esikunnan (puolustuksen turvallisuus- ja tukipalvelujen esikunnan edeltäjä) katsottiin suorittaneen tarkkailua laittomasti ([270]).

Toiseksi yksilöt voivat riitauttaa hallintoviranomaisten ja myös tiedusteluvirastojen päätökset ja laiminlyönnit hallinnollisista riita-asioista annetun lain nojalla ([271]).

Lisäksi yksilöt voivat tehdä tiedusteluviraston toimenpiteistä perustuslakivalituksen perustuslakituomioistuimelle perustuslakituomioistuimesta annetun lain nojalla.

([268]) Tietosuojalain 3 §:n 5 momentti ja 4 §:n 1, 3 ja 4 momentti.
([269]) Tietosuojalain 62 § ja 63 §:n 2 momentti.
([270]) Korkeimman oikeuden päätös 96Da42789, 24.7.1998.
([271]) Hallinnollisista riita-asioista annetun lain 3 ja 4 §.

ISSN 1977-0812 (sähköinen julkaisu)
ISSN 1725-261X (painettu julkaisu)

Euroopan unionin julkaisutoimisto
L-2985 Luxemburg
LUXEMBURG

FI