II

(Nezakonodavni akti)

ODLUKE

PROVEDBENA ODLUKA KOMISIJE (EU) 2022/254

od 17. prosinca 2021.

u skladu s Uredbom (EU) 2016/679 Europskog parlamenta i Vijeća o primjerenosti zaštite osobnih podataka u Republici Koreji na temelju Zakona o zaštiti osobnih informacija

(priopćeno pod brojem dokumenta C(2021) 9316)

(Tekst značajan za EGP)

EUROPSKA KOMISIJA,

uzimajući u obzir Ugovor o funkcioniranju Europske unije,

uzimajući u obzir Uredbu (EU) 2016/679 Europskog parlamenta i Vijeća od 27. travnja 2016. o zaštiti pojedinaca u vezi s obradom osobnih podataka i o slobodnom kretanju takvih podataka te o stavljanju izvan snage Direktive 95/46/EZ (Opća uredba o zaštiti podataka) ([1]), a posebno njezin članak 45. stavak 3.,

budući da:

1. UVOD

(1) Uredbom (EU) 2016/679 utvrđuju se pravila za prijenos osobnih podataka od voditelja obrade ili izvršitelja obrade u Uniji trećim zemljama i međunarodnim organizacijama, u mjeri u kojoj je takav prijenos obuhvaćen njezinim područjem primjene. Pravila o međunarodnim prijenosima podataka utvrđena su u poglavlju V. (članci od 44. do 50.) te uredbe. Iako je protok osobnih podataka u zemlje izvan Europske unije i iz njih bitan za proširenje prekogranične trgovine i međunarodne suradnje, razina zaštite osobnih podataka u Uniji ne smije se ugroziti prijenosima trećim zemljama ([2]).

(2) U skladu s člankom 45. stavkom 3. Uredbe (EU) 2016/679 Komisija može provedbenim aktom odlučiti da treća zemlja, područje, ili jedan ili više određenih sektora unutar treće zemlje, ili međunarodna organizacija osigurava primjerenu razinu zaštite. Pod tim uvjetom prijenosi osobnih podataka trećoj zemlji mogu se obavljati bez potrebe za bilo kakvim dodatnim odobrenjem, kako je predviđeno u članku 45. stavku 1. i uvodnoj izjavi 103. Uredbe (EU) 2016/679.

(3) Kako je navedeno u članku 45. stavku 2. Uredbe (EU) 2016/679, donošenje odluke o primjerenosti mora se temeljiti na sveobuhvatnoj analizi pravnog poretka treće zemlje, koja obuhvaća i pravila koja se primjenjuju na uvoznike podataka i ograničenja i zaštitne mjere u pogledu pristupa tijela javne vlasti osobnim podacima. Komisija u procjeni mora utvrditi jamči li predmetna treća zemlja razinu zaštite koja je „u načelu istovjetna" onoj koja je osigurana u Europskoj uniji (uvodna izjava 104. Uredbe (EU) 2016/679). Je li to tako ocjenjuje se s obzirom na zakonodavstvo Unije, ponajprije Uredbu (EU) 2016/679, te sudsku praksu Suda Europske unije ([3]).

([1]) SL L 119, 4.5.2016., str. 1.
([2]) Vidjeti uvodnu izjavu 101. Uredbe (EU) 2016/679.
([3]) Vidjeti nedavni predmet C-311/18, Facebook Ireland i Schrems (*Schrems II*), ECLI:EU:C:2020:559.

(4) Kako je pojasnio Sud Europske unije, to ne zahtijeva utvrđivanje potpuno istovjetne razine zaštite ([4]). Naime, pravna sredstva kojima se predmetna treća zemlja koristi za zaštitu osobnih podataka mogu se razlikovati od onih koja se primjenjuju u Uniji, pod uvjetom da se u praksi pokažu djelotvornima za osiguravanje primjerene razine zaštite ([5]). Prema tome, standard primjerenosti ne podrazumijeva doslovno ponavljanje pravila Unije. Umjesto toga ispituje se pruža li predmetni strani sustav kao cjelina potrebnu razinu zaštite podataka sadržajem prava na privatnost i njihovom djelotvornom provedbom, nadzorom i ostvarivanjem ([6]). Smjernice o tome daju se i u referentnom dokumentu o primjerenosti Europskog odbora za zaštitu podataka, u kojem se nastoji dodatno pojasniti taj standard ([7]).

(5) Komisija je pomno proučila korejsko pravo i praksu. Na temelju nalaza iznesenih u uvodnim izjavama od 8. do 208. Komisija zaključuje da Koreja osigurava primjerenu razinu zaštite osobnih podataka koji se prenose od voditelja obrade ili izvršitelja obrade u Uniji ([8]) subjektima (npr. fizičke ili pravne osobe, organizacije, javne institucije) u Koreji obuhvaćenima područjem primjene Zakona o zaštiti osobnih informacija (Zakon br. 10465 od 29. ožujka 2011., kako je zadnje izmijenjen Zakonom br. 16930 od 4. veljače 2020.). To uključuje voditelje obrade i izvršitelje obrade (takozvane „vanjske izvršitelje" ([9])) u smislu Uredbe (EU) 2016/679. Zaključak o primjerenosti ne obuhvaća obradu osobnih podataka koju provode vjerske organizacije za misionarske aktivnosti i političke stranke za imenovanje kandidata ili obrade osobnih kreditnih informacija u skladu sa Zakonom o kreditnim informacijama koju provode voditelji obrade koji podliježu nadzoru Povjerenstva za financijske usluge.

(6) U tom se zaključku u obzir uzimaju i dodatne zaštitne mjere utvrđene u Obavijesti br. 2021-5 (Prilog I.) i službenim izjavama, jamstvima i obvezama koje je korejska vlada uputila Komisiji (Prilog II.).

(7) Ova Odluka znači da za prijenose osobnih informacija voditeljima obrade i izvršiteljima obrade u Republici Koreji nisu potrebna daljnja odobrenja. Ona ne utječe na izravnu primjenu Uredbe (EU) 2016/679 na takve subjekte ako su ispunjeni uvjeti utvrđeni u njezinu članku 3., koji se odnose na teritorijalno područje primjene te uredbe.

2. PRAVILA KOJA SE PRIMJENJUJU NA OBRADU OSOBNIH PODATAKA

2.1. Okvir za zaštitu podataka u Republici Koreji

(8) Pravni sustav kojim se uređuje privatnost i zaštita podataka u Koreji počiva na korejskom Ustavu proglašenom 17. srpnja 1948. Iako pravo na zaštitu osobnih podataka nije izričito navedeno u Ustavu, ono je ipak priznato kao osnovno pravo, koje proizlazi iz ustavnih prava na ljudsko dostojanstvo i težnju sreći (članak 10.), privatni život (članak 17.) i privatnost komunikacija (članak 18.). To su potvrdili i Vrhovni sud ([10]) i Ustavni sud ([11]). Temeljna prava i slobode (uključujući pravo na privatnost) smiju se ograničiti samo zakonom, ako je to potrebno radi nacionalne sigurnosti ili održavanja javnog reda za dobrobit građana te to ne smije utjecati na bit predmetnog prava ili predmetne slobode (članak 37. stavak 2.).

([4]) Predmet C-362/14, Maximilian Schrems protiv Data Protection Commissioner (*Schrems*), ECLI:EU:C:2015:650, točka 73.
([5]) Presuda u predmetu *Schrems*, točka 74.
([6]) Vidjeti Komunikaciju Komisije Europskom parlamentu i Vijeću, Razmjena i zaštita osobnih podataka u globaliziranom svijetu, COM(2017) 7 od 10. siječnja 2017., odjeljak 3.1., str. 6.–7.
([7]) Europski odbor za zaštitu podataka, Referentni dokument o primjerenosti, WP 254 rev.01. dostupan na adresi: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=614108
([8]) Ova je Odluka značajna za EGP. U Sporazumu o Europskom gospodarskom prostoru (Sporazum o EGP-u) predviđeno je proširenje unutarnjeg tržišta Europske unije na tri države EGP-a: Island, Lihtenštajn i Norvešku. Odluku Zajedničkog odbora (JCD) o uključivanju Uredbe (EU) 2016/679 u Prilog XI. Sporazumu o EGP-u donio je Zajednički odbor EGP-a 6. srpnja 2018. te je stupila na snagu 20. srpnja 2018. Uredba je stoga obuhvaćena tim sporazumom. Za potrebe ove Odluke upućivanja na EU i države članice EU-a trebalo bi stoga tumačiti tako da ona obuhvaćaju i države EGP-a.
([9]) Vidjeti odjeljak 2.2.3. ove Odluke.
([10]) Vidjeti, primjerice, Odluku Vrhovnog suda 2014Da77970 od 15. listopada 2015. (sažetak na engleskom jeziku dostupan je na poveznici *Lawmaker's disclosure of teachers' trade union members case* (predmet koji se odnosi na otkrivanje članova sindikata učitelja od strane zakonodavca) na adresi https://www.privacy.go.kr/eng/enforcement_01.do) i sudsku praksu navedenu u njoj, uključujući Odluku 2012Da49933 od 24. srpnja 2014.
([11]) Vidjeti posebice Odluku Ustavnog suda 99Hun-ma513 od 26. svibnja 2005. (sažetak na engleskom jeziku dostupan je na adresi http://www.koreanlii.or.kr/w/index.php/99Hun-Ma513?ckattempt=2) i Odluku 2014JHun-ma449 2013 Hun-Ba68 (pročišćeni tekst) od 23. prosinca 2015. (sažetak na engleskom jeziku dostupan je na poveznici *Change of resident registration number case* (predmet o promjeni registracijskog broja rezidenta) na adresi https://www.privacy.go.kr/eng/enforcement_01.do).

(9) Iako se u Ustavu na raznim mjestima upućuje na prava korejskih građana, Ustavni sud presudio je da i strani državljani imaju osnovna prava ([12]). Sud je konkretno utvrdio da su zaštita dostojanstva i vrijednosti osobe kao ljudskog bića te pravo na težnju sreći prava svakog ljudskog bića, a ne samo građana ([13]). Nadalje, prema službenim izjavama korejske vlade ([14]), općenito se priznaje da su u člancima od 12. do 22. Ustava (koji uključuju prava na privatnost) propisana osnovna ljudska prava ([15]). Iako zasad ne postoji nikakva sudska praksa koja se posebno odnosi na pravo na privatnost stranih državljana, taj se zaključak potkrepljuje činjenicom da se to pravo temelji na zaštiti ljudskog dostojanstva i težnji sreći ([16]).

(10) Nadalje, Koreja je donijela niz zakona u području zaštite podataka u kojima se predviđaju zaštitne mjere za sve pojedince, bez obzira na njihovo državljanstvo ([17]). Za potrebe ove Odluke mjerodavni su sljedeći zakoni:

— Zakon o zaštiti osobnih informacija (PIPA),

— Zakon o upotrebi i zaštiti kreditnih informacija ([18]),

— Zakon o zaštiti privatnosti komunikacija.

(11) U PIPA-i propisuje se opći pravni okvir za zaštitu podataka u Republici Koreji. Dopunjen je dekretom o izvršavanju (Predsjednički dekret br. 23169 od 29. rujna 2011., koji je zadnji put izmijenjen Predsjedničkim dekretom br. 30892 od 4. kolovoza 2020.) (Dekret o izvršavanju PIPA-e), koji je, kao i PIPA, pravno obvezujući i izvršiv.

(12) Nadalje, regulatornim „obavijestima" koje donosi Povjerenstvo za zaštitu osobnih informacija (PIPC) propisuju se dodatna pravila o tumačenju i primjeni PIPA-e. Na temelju članka 5. (Obveze države) i članka 14. (Međunarodna suradnja) PIPA-e, PIPC je donio Obavijest br. 2021-5 od 1. rujna 2020. (kako je izmijenjena Obaviješću br. 2021-1 od 21. siječnja 2021. i Obaviješću br. 2021-5 od 16. studenoga 2021., Obavijest br. 2021-5) o tumačenju, primjeni i izvršavanju određenih odredaba PIPA-e. U toj se obavijesti daju pojašnjenja koja se primjenjuju na svaku obradu osobnih podataka na temelju PIPA-e te se propisuju dodatne zaštitne mjere za osobne podatke koji se prenose u Koreju na temelju ove Odluke. Obavijest je pravno obvezujuća za voditelje obrade osobnih informacija te je mogu izvršavati i PIPC i sudovi ([19]). Kršenje pravila utvrđenih u Obavijesti podrazumijeva kršenje odgovarajućih odredaba PIPA-e koje se tim pravilima dopunjuju. Stoga se sadržaj tih dodatnih zaštitnih mjera analizira u okviru ocjene odgovarajućih članaka PIPA-e. Naposljetku, dodatne smjernice o PIPA-i i njezinu dekretu o izvršavanju, na kojima se temelji način na koji PIPC primjenjuje i izvršava pravila o zaštiti podataka, navedene su u Priručniku o PIPA-i i smjernicama o PIPA-i koje je donio PIPC ([20]).

([12]) Odluka Ustavnog suda 93 Hun-MA120 od 29. prosinca 1994.

([13]) Odluka Ustavnog suda 99HeonMa494 od 29. studenoga 2001.

([14]) Vidjeti odjeljak 1.1. Priloga II.

([15]) Vidjeti i članak 1. Zakona o zaštiti osobnih informacija, u kojem se izričito navode „slobode i prava pojedinaca". Točnije, u njemu se navodi da je svrha tog zakona „propisati odredbe o obradi i zaštiti osobnih informacije u svrhu zaštite slobode i prava pojedinaca i daljnjeg ostvarivanja dostojanstva i vrijednosti pojedinaca". Slično tomu, u članku 5. stavku 1. Zakona o zaštiti osobnih informacija utvrđuje se odgovornost države da „osmisli politike radi sprečavanja štetnih posljedica prikupljanja podataka u nepredviđene svrhe, zloupotrebe i pogrešne upotrebe osobnih informacija, neselektivnog nadzora i praćenja itd. te unapređivanja dostojanstva ljudskih bića i privatnosti pojedinaca".

([16]) Nadalje, u članku 6. stavku 2. Ustava propisuje se da je status stranih državljana zajamčen kako je propisano međunarodnim pravom i ugovorima. Koreja je potpisnica više međunarodnih sporazuma kojima se jamči pravo na privatnost, kao što su Međunarodni pakt o građanskim i političkim pravima (članak 17.), Konvencija o pravima osoba s invaliditetom (članak 22.) i Konvencija o pravima djeteta (članak 16.).

([17]) To uključuje pravila koja su relevantna za zaštitu osobnih podataka, ali se ne primjenjuju u situacijama u kojima se osobni podaci prikupljaju u Uniji i prenose u Koreju na temelju Uredbe (EU) 2016/679, primjerice, u Zakonu o zaštiti, upotrebi i drugome u vezi s informacijama o lokaciji.

([18]) Svrha je tog zakona poticati dobro poslovanje s kreditnim informacijama tako da se promiče učinkovita upotreba kreditnih informacija i sustavno upravljanje njima te štiti privatnost od pogrešne upotrebe i zloupotrebe kreditnih informacija (članak 1. Zakona).

([19]) Na primjer, korejski sudovi donijeli su odluku o usklađenosti s regulatornim obavijestima u nizu slučajeva, među ostalim tako što su korejske voditelje obrade smatrali odgovornima za kršenja obavijesti (vidjeti npr. Odluku Vrhovnog suda 2018Da219406 od 25. listopada 2018., u kojoj je Sud naložio voditelju obrade da plati naknadu pojedincima za pretrpljenu štetu zbog kršenja „Obavijesti o standardu za mjere za sigurnost osobnih informacija"; vidjeti i Odluku Vrhovnog suda 2018Da219352 od 25. listopada 2018.; Odluku Vrhovnog suda 2011Da24555 od 16. svibnja 2016.; Odluku Središnjeg okružnog suda u Seoulu 2014Gahap511956 od 13. listopada 2016.; Odluku Središnjeg okružnog suda u Seoulu 2009Gahap43176 od 26. siječnja 2010.).

([20]) Članak 12. stavak 1. PIPA-e.

(13) Osim toga, u Zakonu o upotrebi i zaštiti kreditnih informacija („CIA”) utvrđuju se posebna pravila koja se primjenjuju i na „obične” komercijalne subjekte i na specijalizirane subjekte u financijskom sektoru ako obrađuju osobne kreditne informacije, to jest informacije koje su potrebne da bi se utvrdila kreditna sposobnost stranaka u financijskim ili komercijalnim transakcijama. To ponajprije uključuje ime, podatke za kontakt, financijske transakcije, kreditni rejting, status osiguranja ili saldo zajma ako se te informacije upotrebljavaju za utvrđivanje kreditne sposobnosti pojedinca ([21]). Međutim, ako se te informacije upotrebljavaju u druge svrhe (kao što su ljudski resursi), PIPA se primjenjuje u cijelosti. Kad je riječ o posebnim odredbama o zaštiti podataka iz CIA-e, usklađenost s njima djelomično nadzire PIPC (za komercijalne organizacije vidjeti članak 45-3. CIA-e), a djelomično Povjerenstvo za financijske usluge ([22]) (za financijski sektor, uključujući agencije za kreditni rejting, banke, osiguravajuća društva, uzajamne štedionice, specijalizirana kreditna društva, društva za usluge financijskog ulaganja, društva za financiranje vrijednosnih papira, kreditne unije itd. vidjeti članak 45. stavak 1. CIA-e u vezi s člankom 36-2. Dekreta o izvršavanju CIA-e i člankom 38. Zakona o Povjerenstvu za financijske usluge). S obzirom na to, područje primjene ove Odluke ograničeno je na komercijalne subjekte koji podliježu nadzoru PIPC-a ([23]). Posebna pravila iz CIA-e koja se primjenjuju u tom kontekstu (opća pravila iz PIPA-e primjenjuju se ako ne postoje posebna pravila) opisana su u odjeljku 2.3.11.

2.2. **Materijalno i osobno područje primjene PIPA-e**

(14) Osim ako nije drukčije predviđeno drugim zakonima, zaštita osobnih podataka uređena je PIPA-om (članak 6.). Materijalno i osobno područje njezine primjene određuje se prema utvrđenim pojmovima „osobne informacije”, „obrada” i „voditelj obrade osobnih informacija”.

2.2.1. *Definicija osobnih podataka*

(15) U članku 2. stavku 1. PIPA-e osobne informacije definiraju se kao informacije koje se odnose na žive pojedince i kojima se identitet pojedinca utvrđuje izravno, na primjer po njegovu imenu, registracijskom broju rezidenta ili slici, ili neizravno, to jest ako se samim informacijama ne može utvrditi identitet pojedinca, ali se one mogu lako kombinirati s drugim informacijama. Pitanje mogu li se informacije „lako” kombinirati ovisi o tome je li takvo kombiniranje u razumnoj mjeri vjerojatno, uzimajući u obzir mogućnost dobivanja drugih informacija te vrijeme, trošak i tehnologiju koji su potrebni da bi se utvrdio identitet pojedinca.

(16) Osim toga, pseudonimizirane informacije – tj. informacije kojima se identitet određenog pojedinca ne može utvrditi, a da se one pritom ne koriste ili kombiniraju s dodatnim informacijama kako bi se vratile u svoje izvorno stanje – smatraju se osobnim podacima na temelju PIPA-e (članak 2. stavak 1. točka (c) PIPA-e). Međutim, informacije koje su potpuno „anonimizirane” isključene su iz područja primjene PIPA-e (članak 58-2. PIPA-e). To je slučaj s informacijama kojima se ne može utvrditi identitet određenog pojedinca, čak i ako se kombiniraju s drugim informacijama, uzimajući u obzir vrijeme, trošak i tehnologiju koji su u razumnoj mjeri potrebni za utvrđivanje identiteta.

(17) To odgovara materijalnom području primjene Uredbe (EU) 2016/679 i pojmovima „osobni podaci”, „pseudonimizacija” ([24]) i „anonimizirane informacije” ([25]).

([21]) Članak 2. stavak 1. CIA-e.

([22]) Povjerenstvo za financijske usluge je korejsko nadzorno tijelo za financijski sektor i u tom svojstvu izvršava i odredbe iz CIA-e.

([23]) Ako bi se to u budućnosti promijenilo, npr. proširenjem nadležnosti PIPC-a na sve obrade osobnih kreditnih informacija na temelju CIA-e, mogla bi se razmotriti izmjena odluke o primjerenosti kako bi se njome obuhvatili i subjekti koji trenutačno podliježu nadzoru Povjerenstva za financijske usluge.

([24]) U PIPA-i se pod pojmom „pseudonimizirana obrada” smatra obrada primjenom metoda kao što su djelomično brisanje osobnih podataka ili djelomično ili potpuno zamjenjivanje osobnih podataka tako da se identitet nijednog određenog pojedinca ne može utvrditi bez dodatnih informacija (članak 2. stavak 1-2. PIPA-e). To odgovara definiciji pseudonimizacije iz članka 4. točke 5. Uredbe (EU) 2016/679, u kojoj se navodi da je to „obrada osobnih podataka na način da se osobni podaci više ne mogu pripisati određenom ispitaniku bez uporabe dodatnih informacija, pod uvjetom da se takve dodatne informacije drže odvojeno te da podliježu tehničkim i organizacijskim mjerama kako bi se osiguralo da se osobni podaci ne mogu pripisati pojedincu čiji je identitet utvrđen ili se može utvrditi”.

([25]) Konkretno, u uvodnoj izjavi 26. Uredbe (EU) 2016/679 pojašnjava se da se ta uredba ne primjenjuje na anonimizirane informacije, tj. informacije koje se ne odnose na pojedinca čiji je identitet utvrđen ili se može utvrditi. To ovisi o svim sredstvima koja voditelj obrade ili bilo koja druga osoba mogu po svemu sudeći upotrijebiti u svrhu izravnog ili neizravnog utvrđivanja identiteta pojedinca. Kako bi se utvrdilo je li po svemu sudeći izgledno da se upotrebljavaju takva sredstva, u obzir se moraju uzeti svi objektivni čimbenici, kao što su troškovi i vrijeme potrebno za utvrđivanje identiteta, uzimajući u obzir i tehnologiju dostupnu u vrijeme obrade i tehnološki razvoj.

2.2.2. *Definicija obrade*

(18) Pojam „obrada" široko je definiran u PIPA-i tako da obuhvaća „prikupljanje, generiranje, povezivanje, kombiniranje, snimanje, pohranjivanje, zadržavanje, obradu s dodanom vrijednošću, uređivanje, pronalaženje, izdavanje, ispravljanje, oporavak, upotrebu, prosljeđivanje i otkrivanje, uništavanje osobnih informacija i druge slične aktivnosti" ([26]). Iako se u određenim odredbama PIPE-e navode samo posebne vrste obrade, kao što su „upotreba", „prosljeđivanje" ili „prikupljanje" ([27]), pojam „upotreba" tumači se tako da uključuje svaku vrstu obrade koja nije „prikupljanje" ni „prosljeđivanje" (trećim stranama). Stoga se tim širokim tumačenjem pojma „upotreba" osigurava da ne postoje nikakvi nedostaci u zaštiti s obzirom na posebne aktivnosti obrade. Pojam obrade stoga odgovara istom pojmu iz Uredbe (EU) 2016/679.

2.2.3. *Voditelj obrade osobnih informacija i „vanjski izvršitelj"*

(19) PIPA se primjenjuje na „voditelje obrade osobnih informacija" (voditelj obrade). Slično kao i u Uredbi (EU) 2016/679, to uključuje sve javne institucije, pravne osobe, organizacije ili pojedince koji izravno ili neizravno obrađuju osobne podatke radi upravljanja datotekama s osobnim podacima u okviru svojih aktivnosti ([28]). U tom kontekstu pojam „datoteka s osobnim informacijama" znači svaki „skup ili skupovi osobnih informacija koji su sustavno složeni ili organizirani na temelju određenog pravila radi lakog pristupa osobnim informacijama" (članak 2. stavak 4. PIPA-e) ([29]). Voditelj obrade interno je obvezan osposobiti osobe koje su uključene u obradu pod njegovim vodstvom, kao što su službenici trgovačkog društva ili zaposlenici, te izvršavati odgovarajuću kontrolu i nadzor (članak 28. stavak 1. PIPA-e).

(20) Posebne se obveze primjenjuju kad voditelj obrade („naručitelj") eksternalizira obradu osobnih podataka trećoj strani („vanjski izvršitelj"). U prvom redu, eksternalizacija mora biti uređena pravno obvezujućim dogovorom (što je obično ugovor) ([30]) u kojem se utvrđuju opseg eksternaliziranog posla, svrha obrade, tehničke i upravljačke zaštitne mjere koje se trebaju primjenjivati, nadzor koji vrši voditelj obrade, odgovornost (kao što je naknada za štete prouzročene kršenjem ugovornih obveza) te ograničenja povezana s bilo kakvom podobradom ([31]) (članak 26. stavci 1. i 2. PIPA-e u vezi s člankom 28. stavkom 1. Dekreta o izvršavanju) ([32]).

(21) Osim toga, voditelj obrade mora objavljivati, i stalno ažurirati, pojedinosti o eksternaliziranom poslu i identitetu vanjskog izvršitelja ili, ako se eksternalizirana obrada odnosi na aktivnosti izravne prodaje, izravno obavijestiti pojedince o relevantnim informacijama (članak 26. stavci 2. i 3. PIPA-e u vezi s člankom 28. stavcima od 2. do 5. Dekreta o izvršavanju) ([33]).

(22) Nadalje, u skladu s člankom 26. stavkom 4. PIPA-e u vezi s člankom 28. stavkom 6. Dekreta o izvršavanju, voditelj obrade obvezan je „educirati" vanjskog izvršitelja o potrebnim sigurnosnim mjerama i nadzirati (među ostalim, provođenjem inspekcijskih pregleda) poštuje li vanjski izvršitelj sve obveze voditelja obrade na temelju PIPA-e ([34]) te na temelju ugovora o eksternalizaciji. Ako vanjski izvršitelj prouzroči štetu zbog kršenja PIPA-e, njegove radnje ili nedjelovanje pripisat će se voditelju obrade za potrebe utvrđivanja odgovornosti kao kad je riječ o zaposleniku (članak 26. stavak 6. PIPA-e).

([26]) Članak 2. stavak 2. PIPA-e.

([27]) Primjerice, u člancima od 15. do 19. PIPA-e navodi se samo prikupljanje, upotreba i prosljeđivanje osobnih informacija.

([28]) Članak 2. stavak 5. PIPA-e. Javne institucije u smislu PIPA-e uključuju sve središnje upravne odjele ili agencije i tijela povezana s njima, tijela lokalne vlasti, škole i javna poduzeća u koja ulažu tijela lokalne vlasti, upravna tijela Nacionalne skupštine i pravosudna tijela (uključujući Ustavni sud) (članak 2. stavak 6. PIPA-e u vezi s člankom 2. Dekreta o izvršavanju PIPA-e).

([29]) To odgovara materijalnom području primjene Uredbe (EU) 2016/679. U skladu s člankom 2. stavkom 1. Uredbe (EU) 2016/679, ta uredba primjenjuje se na „obradu osobnih podataka koja se u cijelosti ili djelomično obavlja automatizirano te na neautomatiziranu obradu osobnih podataka koji čine dio sustava pohrane ili su namijenjeni biti dio sustava pohrane". U članku 4. točki 6. Uredbe (EU) 2016/679 pojam „sustav pohrane" definira se kao „svaki strukturirani skup osobnih podataka dostupnih prema posebnim kriterijima". U skladu s time, u uvodnoj izjavi 15. objašnjava se da bi se zaštita pojedinaca trebala primjenjivati na „obradu osobnih podataka automatiziranim sredstvima, kao i na ručnu obradu, ako su osobni podaci pohranjeni ili ih se namjerava pohraniti u sustav pohrane. Dokumenti ili skupovi dokumenata, kao i njihove naslovne stranice, koji nisu strukturirani prema posebnim mjerilima ne bi trebali biti obuhvaćeni područjem primjene ove Uredbe".

([30]) Vidjeti u Priručniku o PIPA-i poglavlje III., odjeljak 2. o članku 26. (str. 203.–212.), u kojem se objašnjava da se članak 26. stavak 1. PIPA-e odnosi na obvezujuće dogovore, kao što su ugovori ili slični dogovori.

([31]) U skladu s člankom 26. stavkom 5. PIPA-e izvršitelju obrade zabranjeno je upotrebljavati bilo kakve osobne informacije izvan opsega eksternaliziranog posla ili prosljeđivati osobne informacije trećoj strani. Nepoštovanje tog zahtjeva može za posljedicu imati kaznene sankcije u skladu s člankom 71. točkom 2. PIPA-e.

([32]) Nepoštovanje tog zahtjeva može dovesti do izricanja novčane kazne, vidjeti članak 75. stavak 4. točku 4. PIPA-e.

([33]) Nepoštovanje tog zahtjeva može dovesti do izricanja novčane kazne, vidjeti članak 75. stavak 2. točku 1. i članak 75. stavak 4. točku 5. PIPA-e.

([34]) Vidjeti i članak 26. stavak 7. PIPA-e, u skladu s kojim se članci od 15. do 25., od 27. do 31., od 33. do 38. i članak 50. primjenjuju *mutatis mutandis* na izvršitelja obrade.

(23) Stoga, iako se u PIPA-i ne koriste različiti pojmovi za „voditelje obrade" i „izvršitelje obrade", pravilima o eksternalizaciji propisuju se u načelu istovjetne obveze i zaštitne mjere kao i one kojima se uređuje odnos između voditelja obrade i izvršitelja obrade na temelju Uredbe (EU) 2016/679.

2.2.4. *Posebne odredbe za pružatelje informacijskih i komunikacijskih usluga*

(24) Iako se PIPA primjenjuje na obradu osobnih podataka koju obavljaju svi voditelji obrade, određene odredbe sadržavaju posebna pravila (kao *lex specialis*) za obradu osobnih podataka „korisnika" koju obavljaju „pružatelji informacijskih i komunikacijskih usluga" ([35]). Pojam „korisnici" obuhvaća pojedince koji koriste informacijske i komunikacijske usluge (članak 2. stavak 1. točka 4. Zakona o promicanju upotrebe informacijskih i komunikacijskih mreža i zaštiti podataka – Zakon o mrežama). To zahtijeva da pojedinac ili izravno koristi telekomunikacijske usluge koje pruža korejski telekomunikacijski operater ili da koristi informacijske usluge ([36]) koje komercijalno (tj. u svrhu ostvarivanja dobiti) pruža subjekt koji se pak oslanja na usluge telekomunikacijskog operatera licenciranog/registriranog u Koreji ([37]). U oba slučaja posebne odredbe PIPA-e obvezuju onog subjekta koji izravno pruža internetsku uslugu pojedincu (tj. korisniku).

(25) Međutim, zaključak o primjerenosti odnosi se isključivo na razinu zaštite osobnih podataka koji se prenose od voditelja obrade/izvršitelja obrade iz Unije subjektu u trećoj zemlji (u ovom slučaju: u Republici Koreji). U potonjem će scenariju pojedinci u Uniji obično imati izravan odnos samo s „izvoznikom podataka" u Uniji, a ne s korejskim pružateljem informacijskih i komunikacijskih usluga ([38]). Stoga će se posebne odredbe PIPA-e koje se odnose na osobne podatke korisnika informacijskih i komunikacijskih usluga eventualno primjenjivati samo u ograničenim situacijama na osobne podatke koji se prenose na temelju ove Odluke.

2.2.5. *Izuzeće od određenih odredaba PIPA-e*

(26) Člankom 58. stavkom 1. PIPA-e isključuje se primjena dijela PIPA-e (tj. članaka od 15. do 57.) u pogledu četiri kategorije obrade podataka ([39]). Točnije, ne primjenjuju se dijelovi PIPA-e koji se odnose na posebne osnove za obradu, određene obveze u pogledu zaštite podataka, detaljna pravila za ostvarivanje prava pojedinaca te pravila kojima se uređuje rješavanje sporova koje provodi Odbor za posredovanje u sporovima o osobnim informacijama. Ostale osnovne odredbe PIPA-e i dalje se primjenjuju, naročito opće odredbe o načelima zaštite podataka (članak 3. PIPA-e) – uključujući, primjerice, načela zakonitosti, navođenja svrhe i ograničavanja svrhe, smanjenja količine podataka, točnosti i sigurnosti podataka – i prava pojedinaca (na pristup, ispravak, brisanje i suspenziju – vidjeti članak 4. PIPA-e). Osim toga, člankom 58. stavkom 4. PIPA-e uvode se posebne obveze u vezi s tim aktivnostima obrade, to jest u pogledu smanjenja količine podataka, ograničene pohrane podataka, sigurnosnih mjera i rješavanja pritužbi ([40]). Stoga pojedinci i dalje mogu podnijeti pritužbu PIPC-u ako se ta načela i obveze ne bi poštovali, a on je u tom slučaju ovlašten poduzimati mjere izvršenja.

([35]) Vidjeti naročito članak 18. stavak 2. i poglavlje VI. PIPA-e.

([36]) Informacijske usluge sastoje se od pružanja informacija i usluga posredovanja u pružanju informacija.

([37]) Vidjeti članak 2. stavak 1. točku 3. (u vezi s člankom 2. stavkom 1. točkama 2. i 4.) Zakona o mrežama i članak 2. stavke 6. i 8. Zakona o telekomunikacijama.

([38]) Ako bi korejski pružatelji informacijskih i komunikacijskih usluga imali izravan odnos s pojedincima u EU-u (pružanjem internetskih usluga), to bi moglo dovesti do izravne primjene Uredbe (EU) 2016/679, u skladu s njezinim člankom 3. stavkom 2. točkom (a).

([39]) U članku 58. stavku 2. PIPA-e predviđa se i da se članak 15., članak 22., članak 27. stavci 1. i 2., članak 34. i članak 37. ne primjenjuju na osobne informacije koje se obrađuju uređajima za obradu vizualnih podataka koji su postavljeni i rade na otvorenim mjestima. Budući da se ta odredba odnosi na primjenu videonadzora unutar Koreje, tj. na izravno prikupljanje osobnih informacija od pojedinaca u Koreji, nije relevantna za potrebe ove Odluke, koja obuhvaća prijenose osobnih podataka od voditelja obrade/izvršitelja obrade iz EU-a subjektima u Koreji. Osim toga, u skladu s člankom 58. stavkom 3. PIPA-e, članak 15. (prikupljanje i upotreba osobnih informacija), članak 30. (obveza donošenja javne politike zaštite privatnosti) i članak 31. (obveza imenovanja službenika za zaštitu privatnosti) ne primjenjuju se na osobne informacije koje se obrađuju u svrhu djelovanja skupina ili udruženja namijenjenih prijateljstvu (npr. hobistički klubovi). Budući da se takve skupine smatraju privatnima po prirodi i nisu povezane s profesionalnom ili komercijalnom djelatnošću, ne zahtijeva se nikakva posebna pravna osnova (kao što je privola predmetnih pojedinaca) za prikupljanje i upotrebu informacija tih pojedinaca u tom kontekstu. Međutim, i dalje se primjenjuju sve ostale odredbe PIPA-e (npr. smanjenje količine podataka, ograničavanje svrhe, zakonitost obrade, sigurnost i prava pojedinaca). Nadalje, to se izuzeće ne primjenjuje ni na koju obradu osobnih informacija čija svrha nadilazi osnivanje društvene skupine.

([40]) Točnije, člankom 58. stavkom 4. PIPA-e propisuje se obveza prema kojoj se osobne informacije moraju obrađivati u najmanjoj mjeri koja je potrebna da bi se ostvarila predviđena svrha i tijekom minimalnog razdoblja te se moraju poduzeti potrebne mjere za sigurno upravljanje takvim osobnim informacijama i njihovu prikladnu obradu. Potonje uključuje tehničke, upravljačke i fizičke zaštitne mjere te mjere za osiguravanje pravilnog postupanja s pritužbama pojedinaca.

(27) Prvo, djelomično izuzeće obuhvaća osobne podatke prikupljene u skladu sa Zakonom o statističkim podacima radi obrade koju vrše javne institucije. Prema pojašnjenjima dobivenima od korejske vlade, osobni podaci obrađeni u tom kontekstu obično se odnose na korejske državljane i mogu samo iznimno uključivati informacije o strancima, ponajprije u pogledu statističkih podataka o ulasku na državni teritorij i odlasku iz njega ili o stranim ulaganjima. Međutim, čak i u tim situacijama takve podatke obično ne prenose voditelji obrade/izvršitelji obrade iz Unije, već ih radije izravno prikupljaju tijela javne vlasti u Koreji ([41]). Nadalje, slično onomu što je predviđeno u uvodnoj izjavi 162. Uredbe (EU) 2016/679, na obradu podataka u skladu sa Zakonom o statističkim podacima primjenjuje se nekoliko uvjeta i zaštitnih mjera. Konkretno, Zakonom o statističkim podacima uvode se posebne obveze, kao što je osiguravanje točnosti, dosljednosti i nepristranosti; jamčenje povjerljivosti podataka o pojedincima; zaštita informacija o sudionicima statističkih istraživanja, među ostalim i kako bi se spriječilo da se takve informacije upotrebljavaju u bilo koje druge svrhe osim prikupljanja statističkih podataka i kako bi se članovi osoblja podvrgnuli zahtjevima čuvanja povjerljivosti ([42]). Tijela javne vlasti koja obrađuju statističke podatke također moraju poštovati, među ostalim, načela smanjenja količine podataka, ograničavanja svrhe i sigurnosti (članak 3. i članak 58. stavak 4. PIPA-e) te pojedincima omogućiti ostvarivanje njihovih prava (pristupa, ispravka, brisanja i suspenzije, vidjeti članak 4. PIPA-e). Naposljetku, podaci se moraju obrađivati u anonimiziranom ili pseudonimiziranom obliku ako je na taj način moguće ispuniti svrhu obrade (članak 3. stavak 7. PIPA-e).

(28) Drugo, članak 58. stavak 1. PIPA-e odnosi se na osobne podatke prikupljene ili zatražene radi analize informacija povezanih s nacionalnom sigurnošću. Područje primjene i posljedice tog djelomičnog izuzeća podrobnije su opisani u uvodnoj izjavi 149.

(29) Treće, djelomično izuzeće primjenjuje se na privremenu obradu osobnih podataka ako je to hitno potrebno radi javne zaštite i sigurnosti, uključujući javno zdravlje. PIPC tu kategoriju tumači strogo i, prema primljenim informacijama, nikad nije upotrijebljena. Ona se primjenjuje samo u izvanrednim situacijama u kojima je potrebno hitno djelovanje, primjerice, radi praćenja uzročnika zaraze ili spašavanja i pomaganja žrtvama prirodnih katastrofa ([43]). Čak i u tim situacijama djelomično izuzeće obuhvaća samo obradu osobnih podataka u ograničenom razdoblju provedbe takvih radnji. Situacije u kojima bi se to moglo primjenjivati na prijenose podataka obuhvaćene ovom Odlukom još su više ograničene, uzimajući u obzir malu vjerojatnost da bi osobni podaci koji se prenose iz Unije korejskim subjektima bili takve vrste da bi njihova naknadna obrada mogla postati „hitno potrebna” za takve izvanredne situacije.

(30) Naposljetku, djelomično izuzeće primjenjuje se na osobne podatke koje prikupljaju ili upotrebljavaju mediji, vjerske organizacije u svrhu misionarskih aktivnosti i političke stranke u svrhu imenovanja kandidata. Izuzeće se primjenjuje samo ako osobne podatke obrađuju mediji, vjerske organizacije ili političke stranke u te posebne svrhe (tj. novinarske aktivnosti, misionarski rad i imenovanje političkih kandidata). Ako ti subjekti osobne podatke obrađuju u druge svrhe, kao što su upravljanje ljudskim resursima ili unutarnji administrativni poslovi, PIPA se primjenjuje u cijelosti.

(31) Kad je riječ o obradi osobnih podataka koju vrše mediji u svrhu novinarskih aktivnosti, postizanje ravnoteže između slobode izražavanja i drugih prava (uključujući pravo na privatnost) propisano je Zakonom o arbitraži i korektivnim mjerama itd. za štetu prouzročenu medijskim izvješćivanjem (Zakon o medijima) ([44]). Konkretno,

([41]) S obzirom na to, člankom 33. Zakona o statističkim podacima od javnih institucija zahtijeva se da štite informacije o sudionicima statističkih istraživanja, među ostalim i kako bi se spriječilo da se takve informacije upotrebljavaju u bilo koje druge svrhe osim prikupljanja statističkih podataka.

([42]) Članak 2. stavci 2. i 3., članak 30. stavak 2., članak 33. i članak 34. Zakona o statističkim podacima.

([43]) Priručnik o PIPA-i, odjeljak o članku 58.

([44]) Primjerice, u članku 4. Zakona o medijima propisuje se da medijska izvješća moraju biti nepristrana i objektivna i u javnom interesu te se u njima moraju poštovati ljudsko dostojanstvo i vrijednost i ne smiju se klevetati druge osobe niti narušavati njihova prava, javni moral ili društvena etika.

člankom 5. Zakona o medijima predviđa se da mediji (tj. bilo koja radiodifuzijska organizacija, novine, časopis ili internetske novine), bilo koji internetski servis za vijesti ili internetska multimedijska radiodifuzijska organizacija ne smiju povrijediti privatnost pojedinaca. Ako se povreda privatnosti ipak dogodi, mora se u najkraćem ispraviti u skladu s posebnim postupcima utvrđenima u tom zakonu. S obzirom na to, Zakonom o medijima daju se brojna prava pojedincima koji su pretrpjeli štetu zbog medijskih izvješća, kao što su pravo na objavu ispravka netočne izjave, pravo na ispravak objavom izjave kojom se proturječi medijskom izvješću ili objavom dodatnog izvješća (ako se medijsko izvješće odnosi na tvrdnje o počinjenju kaznenog djela za koje je pojedinac poslije oslobođen optužbi) ([45]). Zahtjeve pojedinaca mogu riješiti same medijske kuće (preko službenika za pritužbe) ([46]) ili se one mogu riješiti mirenjem ili arbitražom (pred specijaliziranim Povjerenstvom za medijsku arbitražu) ([47]) ili pred sudovima. Pojedinci mogu dobiti i naknadu štete ako pretrpe novčanu štetu, povredu osobnog prava ili bilo kakvu drugu duševnu bol zbog nezakonitog postupka medija (koji se može počiniti s namjerom ili iz nehaja) ([48]). Mediji su na temelju tog zakona oslobođeni od odgovornosti u mjeri u kojoj medijsko izvješće kojim se narušavaju prava pojedinca nije u suprotnosti s društvenim vrijednostima te je objavljeno uz suglasnost predmetnog pojedinca ili u javnom interesu (i postoje dostatne osnove da bi se smatralo da to izvješće odgovara istini) ([49]).

(32) Dok obrada osobnih podataka koju vrše mediji u svrhu novinarskih aktivnosti podliježe posebnim zaštitnim mjerama koje proizlaze iz Zakona o medijima, nema takvih dodatnih zaštitnih mjera kojima bi se utvrdila primjena izuzeća za aktivnosti obrade koje vrše vjerske organizacije i političke stranke na način koji bi bio usporediv s člancima 85., 89. i 91. Uredbe (EU) 2016/679. Komisija stoga smatra da je iz područja primjene ove Odluke primjereno isključiti vjerske organizacije, u mjeri u kojoj obrađuju osobne podatke u svrhe svojih misionarskih aktivnosti, i političke stranke, u mjeri u kojoj obrađuju osobne podatke u kontekstu imenovanja kandidata.

2.3. **Zaštitne mjere, prava i obveze**

2.3.1. *Zakonitost i poštenost obrade*

(33) Osobni podaci trebali bi se obrađivati zakonito i pošteno.

(34) To je načelo utvrđeno člankom 3. stavcima 1. i 2. PIPA-e i potvrđeno člankom 59. PIPA-e, kojim se zabranjuje obrada osobnih podataka „prijevarom, neprikladnim ili nepravednim sredstvima”, „bez pravnog ovlaštenja” ili „izvan okvira propisnog ovlaštenja” ([50]). Ta opća načela zakonite obrade razrađuju se u člancima od 15. do 19. PIPA-e, u kojima se utvrđuju različite pravne osnove za obradu (prikupljanje, upotrebu i prosljeđivanje trećim stranama), uključujući okolnosti u kojima to može dovesti do promjene svrhe (članak 18. PIPA-e).

([45]) Članci od 15. do 17. Zakona o medijima.

([46]) Svaka medijska kuća mora imati vlastita službenika za pritužbe radi sprečavanja i ispravljanja bilo koje štete koju su prouzročili mediji (npr. davanjem preporuka o ispravcima medijskih izvješća koja su netočna ili kojima se nanosi šteta ugledu drugih), članak 6. Zakona o medijima.

([47]) Povjerenstvo se sastoji od 40 do 90 povjerenika za arbitražu, koje imenuje ministar kulture, sporta i turizma iz redova sudaca, odvjetnika, osoba s najmanje 10 godina radnog iskustva u području prikupljanja vijesti i izvješćivanja o vijestima ili drugih osoba sa stručnim znanjem povezanim s medijima. Povjerenici za arbitražu ne mogu istodobno biti javni dužnosnici, članovi političkih stranaka ili novinari. U skladu s člankom 8. Zakona o medijima povjerenici za arbitražu moraju svoje dužnosti izvršavati neovisno i ne smiju se usmjeravati niti primati upute u vezi s tim dužnostima. Nadalje, postoje posebna pravila za sprečavanje sukoba interesa, npr. izuzimanjem pojedinih povjerenika iz rješavanja pojedinih predmeta u kojima su stranke njihov bračni drug ili rođaci (članak 10. Zakona o medijima). Povjerenstvo sporove može rješavati mirenjem ili arbitražom, ali može i određivati preporuke za ispravljanje povreda (odjeljak 5. Zakona o medijima).

([48]) Članak 30. Zakona o medijima.

([49]) Članak 5. Zakona o medijima.

([50]) Člankom 59. PIPA-e zabranjuje se svakoj osobi „koja obrađuje ili je ikad obrađivala osobne informacije” da „pribavi osobne informacije ili dobije privolu za obradu osobnih informacija prijevarom, neprikladnim ili nepravednim sredstvima”, „da otkrije osobne informacije pribavljene u okviru poslovne djelatnosti ili da ih proslijedi za upotrebu bilo kojoj trećoj strani bez ovlaštenja” ili da „ošteti, uništi, izmijeni, krivotvori ili otkrije osobne informacije druge osobe bez pravnog ovlaštenja ili izvan okvira propisnog ovlaštenja”. Kršenje te zabrane može dovesti do kaznenih sankcija, vidjeti članak 71. stavke 5. i 6. i članak 72. stavak 2. PIPA-e. Člankom 70. stavkom 2. PIPA-e usto se omogućuje izricanje kaznene sankcije za pribavljanje osobnih informacija koje obrađuju treće strane prijevarom ili drugim nepravednim sredstvima ili metodama ili za prosljeđivanje tih informacija trećoj strani u svrhe ostvarivanja dobiti ili nepravedne svrhe te za pomaganje u takvom postupanju ili dogovaranje takvog postupanja.

(35) U skladu s člankom 15. stavkom 1. PIPA-e voditelj obrade smije samo prikupljati osobne podatke (u okviru svrhe prikupljanja) na temelju ograničenog broja pravnih osnova. Te su osnove: 1. privola ispitanika ([51]) (točka 1.); 2. ako je to nužno radi izvršenja i provedbe ugovora s ispitanikom (točka 4.); 3. posebno ovlaštenje koje proizlazi iz zakona ili ako je to nužno radi poštovanja pravnih obveza (točka 2.); ako je to nužno ([52]) da bi javna institucija mogla izvršavati zadaće iz svoje nadležnosti kako je propisano zakonom; 4. ako se to smatra očito nužnim za zaštitu života te zdravstvenih ili imovinskih interesa ispitanika ili treće strane od neposredne opasnosti (samo ako ispitanik nije u mogućnosti izraziti svoju namjeru ili se prethodna privola ne može pribaviti) (točka 5.); 5. ako je to nužno za ostvarenje „opravdanog interesa" voditelja obrade, pod uvjetom da takav interes „nedvojbeno ima prednost" pred interesima ispitanika (i to samo ako postoji „znatna povezanost" obrade s tim legitimnim interesom i ako ona ne prelazi ono što je razumno) (točka 6.) ([53]). Te osnove za obradu u načelu su istovjetne osnovama utvrđenima u članku 6. Uredbe (EU) 2016/679, uključujući osnovu „opravdanog interesa" koja je istovjetna osnovi „legitimnog interesa" iz članka 6. stavka 1. točke (f) Uredbe (EU) 2016/679.

(36) Nakon što su prikupljeni, osobni podaci smiju se koristiti u okviru svrhe prikupljanja (članak 15. stavak 1. PIPA-e) ili „u okviru koji je razumno povezan" sa svrhom prikupljanja, uzimajući u obzir moguće negativne posljedice prouzročene ispitaniku i pod uvjetom da su donesene potrebne sigurnosne mjere (npr. enkripcija) (članak 15. stavak 3. PIPA-e). Kako bi se utvrdilo je li svrha upotrebe „razumno povezana" s prvotnom svrhom prikupljanja, u Dekretu o izvršavanju propisuju se posebni kriteriji koji su slični onima iz članka 6. stavka 4. Uredbe (EU) 2016/679. Konkretno, mora postojati znatna relevantnost u odnosu na prvotnu svrhu; dodatna upotreba mora biti predvidljiva (primjerice, s obzirom na okolnosti u kojima su informacije prikupljene); i, ako je moguće, podaci moraju biti pseudonimizirani ([54]). Posebni kriteriji koje voditelj obrade primjenjuje u toj ocjeni moraju se unaprijed iznijeti u politici zaštite privatnosti ([55]). Nadalje, od službenika za zaštitu privatnosti (vidjeti uvodnu izjavu 94.) posebno se zahtijeva da preispita odvija li se daljnja upotreba unutar tih parametara.

([51]) Privola se mora dati dobrovoljno, mora biti utemeljena i izričita te se mora izraziti na jedan od nekoliko načina koji su unaprijed utvrđeni zakonom. U svakom slučaju, privola se ne smije dobiti prijevarom te neprikladnim ili na drugi način nepravednim sredstvima (članak 59. stavak 1. PIPA-e). Prvo, u skladu s člankom 4. točkom 2. PIPA-e, ispitanici imaju pravo odlučiti „hoće li dati privolu" i „odabrati opseg te privole" te ih o tome treba obavijestiti (članak 15. stavak 2., članak 16. stavci 2. i 3., članak 17. stavak 2. i članak 18. stavak 3. PIPA-e). Članak 22. stavak 5. sadržava dodatnu zaštitnu mjeru prema kojoj se voditelju obrade zabranjuje da uskrati isporuku robe ili pružanje usluga ako bi se time narušilo pravo pojedinca na slobodan izbor oko davanja privole. To uključuje situacije u kojima je samo za određene vrste obrade potrebna privola (dok se ostale temelje na ugovoru) te obuhvaća i daljnju obradu osobnih podataka prikupljenih u kontekstu isporuke robe ili pružanja usluga. Drugo, u skladu s člankom 15. stavkom 2., člankom 17. stavcima 2. i 3. i člankom 18. stavkom 3. PIPA-e, voditelj obrade mora pri traženju privole obavijestiti ispitanika o „pojedinostima" predmetnih osobnih podataka (npr. da je riječ o osjetljivim podacima, vidjeti članak 17. stavak 2. točku 2. podtočku (a) Dekreta o izvršavanju PIPA-e), svrsi obrade, razdoblju pohrane i svakom primatelju tih podataka. Svaki takav zahtjev mora se iznijeti „na izričito prepoznatljiv način" kojim se pitanja za koja je potrebna privola razlikuju od ostalih pitanja (članak 22. stavci od 1. do 4. PIPA-e). Treće, u članku 17. stavku 1. točkama od 1. do 6. Dekreta o izvršavanju PIPA-e propisuju se posebne metode kojima voditelj obrade mora dobiti privolu, kao što su pisana privola s potpisom ispitanika ili privola dana (povratnom) e-porukom. Iako se PIPA-om pojedincima ne daje opće pravo na povlačenje privole, oni imaju pravo na suspenziju obrade podataka koji se na njih odnose, a kad se to pravo ostvari, prekida se obrada i brišu se podaci (vidjeti uvodnu izjavu 78. o pravu na suspenziju).

([52]) Prema informacijama dobivenima od PIPC-a, javne institucije smiju se pozivati na tu osnovu samo ako je obrada osobnih informacija neizbježna, tj. mora biti nemoguće ili neopravdano teško za instituciju da obavlja svoje funkcije bez obrade tih podataka.

([53]) Člankom 39-3. PIPA-e uvode se posebne (strože) obveze za pružatelje informacijskih i komunikacijskih usluga u vezi s prikupljanjem i upotrebom osobnih informacija njihovih korisnika. Konkretno, zahtijeva se da pružatelj usluga pribavi privolu korisnika nakon što ga obavijesti o svrsi prikupljanja/upotrebe, kategorijama osobnih informacija koje će se prikupljati i razdoblju tijekom kojeg će se informacije obrađivati (članak 39-3. stavak 1. PIPA-e). Isto vrijedi i ako se bilo koji od tih aspekata promijeni. Nepribavljanje privole za prikupljanje informacija podliježe kaznenim sankcijama (članak 71. stavak 4-5. PIPA-e). Iznimno, pružatelji informacijskih i komunikacijskih usluga mogu prikupljati i upotrebljavati osobne informacije korisnika bez pribavljanja njihove prethodne privole. To je slučaj 1. kad je izrazito teško dobiti uobičajenu privolu za osobne informacije koje su potrebne za izvršenje ugovora kojim se uređuje pružanje informacijskih i komunikacijskih usluga zbog gospodarskih i tehnoloških razloga (npr. kad se osobni podaci neizbježno stvaraju u postupku izvršenja ugovora, primjerice, informacije o naplati računa, evidencije pristupa i evidencije o plaćanju); 2. ako je to potrebno za obračun naknada nakon pružanja informacijskih i komunikacijskih usluga; ili 3. ako je to dopušteno drugim zakonima (primjerice, u članku 21. stavku 1. točki 6. Zakona o zaštiti potrošača u području elektroničke trgovini predviđa se da poslovni subjekti smiju prikupljati osobne informacije o zakonskim skrbnicima maloljetnika kako bi potvrdili da je dobivena valjana privola u ime maloljetnika) (članak 39-3. stavak 2. PIPA-e). U svim slučajevima pružatelji informacijskih i komunikacijskih usluga ne smiju odbiti pružati usluge samo zbog toga što korisnik nije dao više osobnih informacija od onoga što je minimalno potrebno (tj. informacije koje su nužne za obavljanje bitnih elemenata predmetne usluge), vidjeti članak 39-3. stavak 3. PIPA-e.

([54]) Vidjeti članak 14-2. Dekreta o izvršavanju PIPA-e.

([55]) Članak 14-2. stavak 2. Dekreta o izvršavanju PIPA-e.

(37) Slična (ali nešto stroža) pravila primjenjuju se na prosljeđivanje podataka trećoj strani. U skladu s člankom 17. stavkom 1. PIPA-e prosljeđivanje osobnih podataka trećoj strani dopušteno je na temelju privole ([56]) ili, u okviru svrhe prikupljanja, ako su te informacije prikupljene na temelju jedne od pravnih osnova iz članka 15. stavka 1. točaka 2., 3. i 5. PIPA-e. Time se ponajprije isključuje bilo kakvo otkrivanje na temelju „opravdanog interesa" voditelja obrade. Osim toga, člankom 17. stavkom 4. PIPA-e prosljeđivanje trećim stranama dopušta se „u okviru koji je razumno povezan" sa svrhom prikupljanja, uzimajući ponovno u obzir moguće negativne posljedice prouzročene ispitaniku i pod uvjetom da su donesene potrebne sigurnosne mjere (kao što je enkripcija). Kako bi se ocijenilo je li prosljeđivanje u okviru koji je razumno povezan sa svrhom prikupljanja, u obzir se moraju uzeti isti čimbenici kao i oni opisani u uvodnoj izjavi 36. te se primjenjuju iste zaštitne mjere (tj. s obzirom na transparentnost u okviru politike zaštite privatnosti i sudjelovanje službenika za zaštitu privatnosti).

(38) Ako korejski voditelj obrade podataka primi osobne podatke iz Unije, to se smatra „prikupljanjem" u smislu članka 15. PIPA-e. U Obavijesti br. 2021-5 (odjeljak I. Priloga I. ovoj Odluci) pojašnjava se da svrha u koju je predmetni subjekt iz EU-a prenio podatke čini svrhu prikupljanja za korejskog voditelja obrade podataka. Stoga se od korejskih voditelja obrade podataka koji su primili osobne podatke iz Unije u načelu zahtijeva da te informacije obrađuju u okviru svrhe prijenosa, u skladu s člankom 17. PIPA-e.

(39) Posebna ograničenja primjenjuju se ako voditelj obrade želi te osobne podatke upotrebljavati ili ih proslijediti trećoj strani u svrhu koja se razlikuje od svrhe prikupljanja ([57]). U skladu s člankom 18. stavkom 2. PIPA-e privatni voditelj obrade iznimno ([58]) smije osobne podatke upotrebljavati ili ih prosljeđivati trećoj strani u drugu svrhu: 1. na temelju dodatne (to jest zasebne) privole ispitanika; 2. ako je to predviđeno posebnim zakonskim odredbama; ili 3. ako je to očito nužno za zaštitu života te zdravstvenih ili imovinskih interesa ispitanika ili treće strane od neposredne opasnosti (samo ako ispitanik nije u mogućnosti izraziti svoju namjeru, a prethodna privola ne može se pribaviti) ([59]).

(40) U određenim situacijama i javne institucije smiju osobne podatke upotrebljavati ili ih prosljeđivati trećoj strani u drugu svrhu. To uključuje slučajeve u kojima bi inače javnim institucijama bilo nemoguće izvršavati svoje zakonske dužnosti kako su propisane zakonodavstvom, pri čemu takvi slučajevi podliježu odobrenju PIPC-a. Osim toga, javne institucije smiju osobne podatke prosljeđivati drugom tijelu ili sudu ako je to potrebno za istragu i kazneni progon kaznenih djela ili za podizanje optužnice; ako je to potrebno sudu radi izvršavanja njegovih funkcija povezanih sa sudskim postupcima koji su u tijeku; ili ako je to potrebno za izvršenje kaznene sankcije, rješenja o probaciji ili naloga o pritvoru ([60]). Javne institucije smiju osobne podatke proslijediti i stranoj vladi ili međunarodnoj organizaciji kako bi ispunile pravnu obvezu koja proizlazi iz ugovora ili međunarodne konvencije, a u tom slučaju moraju poštovati i zahtjeve za prekogranične prijenose podataka (vidjeti uvodnu izjavu 90.).

(41) Stoga su načela zakonitosti i poštenosti obrade provedena u korejskom pravnom okviru na načelno istovjetan način kao i u Uredbi (EU) 2016/679, dopuštanjem obrade samo na temelju legitimnih i jasno utvrđenih osnova. Nadalje, u svim navedenim slučajevima obrada je dopuštena samo ako se njome vjerojatno neće „nepravedno povrijediti" interesi ispitanika ili treće strane, što zahtijeva uravnoteženje interesa. Osim toga, u članku 18. stavku 5. PIPA-e propisuju se dodatne zaštitne mjere kad voditelj obrade prosljeđuje osobne podatke trećoj strani, što može uključivati zahtjev da se ograniči svrha i metoda upotrebe ili da se uvedu posebne sigurnosne mjere. Od treće se strane pak traži da provede zatražene mjere.

([56]) Kršenja članka 17. stavka 1. točke 1. PIPA-e mogu dovesti do izricanja kaznenih sankcija (članak 71. stavak 1. PIPA-e).

([57]) „Predviđena svrha" je svrha u koju su informacije prikupljene. Primjerice, kad se informacije prikupljaju na temelju privole predmetnog pojedinca, predviđena svrha je svrha priopćena pojedincu u skladu s člankom 15. stavkom 2. PIPA-e.

([58]) Usp. članak 18. stavak 1. PIPA-e. Kršenja članka 18. stavaka 1. i 2. mogu dovesti do izricanja kaznenih sankcija (članak 71. stavak 2. PIPA-e).

([59]) Pružatelji informacijskih i komunikacijskih usluga smiju osobne informacije upotrebljavati ili ih prosljeđivati trećoj strani u svrhu koja se razlikuje od prvotne svrhe samo na temelju osnova navedenih u članku 18. stavku 2. točkama 1. i 2. PIPA-e (tj. ako je pribavljena dodatna privola ili ako postoje posebne odredbe u zakonodavstvu). Vidjeti članak 18. stavak 2. PIPA-e.

([60]) Osim kad je obrada potrebna za istragu kaznenih djela, podizanje optužnice i kazneni progon, od javnih institucija koje osobne informacije upotrebljavaju ili ih prosljeđuju trećoj strani u svrhu koja se razlikuje od svrhe prikupljanja (primjerice, ako je to posebno dopušteno zakonom ili potrebno radi izvršenja ugovora) zahtijeva se da objave pravnu osnovu za obradu, svrhu obrade i opseg obrade na svojim internetskim stranicama ili u službenom listu te da vode evidenciju o tome (članak 18. stavak 4. PIPA-e s člankom 15. Dekreta o izvršavanju PIPA-e).

(42) Naposljetku, člankom 28-2. PIPA-e dopušta se (daljnja) obrada pseudonimiziranih informacija bez privole predmetnog pojedinca u svrhu prikupljanja statističkih podataka, provođenja znanstvenih istraživanja ([61]) i arhiviranja u javnom interesu, što podliježe posebnim zaštitnim mjerama. Stoga se u PIPA-a, slično kao i u Uredbi (EU) 2016/679 ([62]), olakšava (daljnja) obrada osobnih podataka u takve svrhe unutar okvira u kojem su predviđene odgovarajuće zaštitne mjere za zaštitu prava pojedinaca. Umjesto oslanjanja na pseudonimizaciju kao moguću zaštitnu mjeru, u PIPA-i se ona uvodi kao preduvjet za provođenje određenih aktivnosti obrade u svrhe prikupljanja statističkih podataka, provođenja znanstvenih istraživanja i arhiviranja u javnom interesu (kako bi ti podaci mogli obrađivati bez privole ili kako bi se mogli kombinirati različiti skupovi podataka).

(43) Nadalje, PIPA-om se uvodi niz posebnih zaštitnih mjera, ponajprije u obliku potrebnih tehničkih i organizacijskih mjera, vođenja evidencije, ograničenja razmjene podataka i otklanjanja mogućih rizika povezanih s ponovnom identifikacijom. Kombiniranjem raznih zaštitnih mjera opisanih u uvodnim izjavama od 44. do 48. osigurava se da obrada osobnih podataka u tom kontekstu podliježe u načelu istovjetnim zaštitama u usporedbi s onima koje bi se zahtijevale u skladu s Uredbom (EU) 2016/679.

(44) Prvo i najvažnije, člankom 28-5. stavkom 1. PIPA-e zabranjuje se obrada pseudonimiziranih informacija u svrhu utvrđivanja identiteta određenog pojedinca. Ako bi pri obradi pseudonimiziranih informacija ipak došlo do generiranja informacija kojima bi se mogao utvrditi identitet određenog pojedinca, voditelj obrade mora odmah suspendirati obradu i uništiti takve informacije (članak 28-5. stavak 2. PIPA-e). Nepoštovanje tih odredaba podliježe upravnim novčanim kaznama i čini kazneno djelo ([63]). To znači da je, čak i u onim situacijama u kojima bi bilo *praktički* moguće ponovno identificirati pojedinca, takva ponovna identifikacija *zakonski* zabranjena.

(45) Drugo, pri (daljnjoj) obradi pseudonimiziranih informacija u takve svrhe od voditelja obrade zahtijeva se da uvede posebne tehnološke, upravljačke i fizičke mjere kako bi se osigurala sigurnost informacija (uključujući zasebno pohranjivanje informacija koje su potrebne za vraćanje pseudonimiziranih informacija u njihovo izvorno stanje i zasebno upravljanje tim informacijama) ([64]). Osim toga, mora se voditi evidencija o pseudonimiziranim informacijama koje se obrađuju, svrsi obrade, povijesti upotrebe i svakom primatelju koji je treća strana (članak 29-5. stavak 2. Dekreta o izvršavanju PIPA-e).

(46) Treće i konačno, u PIPA-i se predviđaju posebne zaštitne mjere za sprečavanje utvrđivanja identiteta pojedinaca od strane trećih strana u slučaju razmjene informacija. Konkretno, kad prosljeđuju pseudonimizirane informacije trećoj strani u svrhu prikupljanja statističkih podataka, provođenja znanstvenih istraživanja ili arhiviranja u javnom interesu, voditelji obrade ne smiju uključiti informacije koje bi se mogle upotrijebiti za utvrđivanje identiteta određenog pojedinca (članak 28-2. stavak 2. PIPA-e) ([65]).

(47) Konkretnije, iako se PIPA-om dopušta kombiniranje pseudonimiziranih informacija (koje obrađuju različiti voditelji obrade) u svrhu prikupljanja statističkih podataka, provođenja znanstvenih istraživanja ili arhiviranja u javnom interesu, ta je ovlast pridržana specijaliziranim institucijama koje imaju posebne sigurnosne kapacitete (članak 28-3. stavak 1. PIPA-e) ([66]). Pri podnošenju zahtjeva za kombiniranje pseudonimiziranih podataka voditelj

([61]) Znanstveno istraživanje definira se u članku 2. stavku 8. PIPA-e kao „istraživanje u kojem se primjenjuju znanstvene metode, a to obuhvaća, primjerice, tehnološki razvoj i demonstracijske aktivnosti, temeljna istraživanja, primijenjena istraživanja i istraživanja koja se financiraju iz privatnih izvora". Te kategorije odgovaraju kategorijama utvrđenima u uvodnoj izjavi 159. Uredbe (EU) 2016/679.

([62]) Vidjeti članak 5. stavak 1. točku (b) i članak 89. stavke 1. i 2. te uvodne izjave 50. i 157. Uredbe (EU) 2016/679.

([63]) Vidjeti članak 28-6. stavak 1., članak 71. stavak 4-3., i članak 75. stavak 2. točku 4-4. PIPA-e.

([64]) Članak 28-4. PIPA-e i članak 29-5. Dekreta o izvršavanju PIPA-e. Nepoštovanje tih obveza podliježe upravnim i kaznenim sankcijama, vidjeti članak 73. stavak 1. i članak 75. stavak 2. točku 6. PIPA-e.

([65]) Kršenja tih zahtjeva mogu dovesti do izricanja kaznenih sankcija (članak 71. stavak 2. PIPA-e). PIPC je odmah započeo s provođenjem tih novih pravila, npr. u svojoj odluci od 28. travnja 2021., kojom je izrekao novčanu kaznu i odredio korektivne mjere trgovačkom društvu koje, među ostalim kršenjima PIPA-e, nije poštovalo zahtjev iz članka 28-2. stavka 2. PIPA-e, vidjeti na adresi https://www.pipc.go.kr/np/cop/bbs/selectBoardArticle.do?bbsId=BS074&mCode=C020010000&nttId=7298&fbclid=IwAR3SKcMQi6G5pR9k4I7j6GNXtc8aBVDOwcURevvvzQtYI7AS40UKYXoOXo8.

([66]) Kako bi se određeni subjekt imenovao takvom specijaliziranom institucijom („stručna agencija za kombiniranje podataka"), mora se podnijeti zahtjev PIPC-u zajedno s popratnim dokumentima u kojima se detaljno navode, među ostalim, objekti i oprema koji postoje za sigurno kombiniranje pseudonimiziranih podataka i u kojima se potvrđuje da podnositelj zahtjeva zapošljava najmanje tri člana osoblja koji su zaposleni na puno radno vrijeme i imaju kvalifikacije ili iskustvo u području zaštite osobnih podataka (članak 29-2. stavci 1. i 2. Dekreta o izvršavanju PIPA-e). Detaljni zahtjevi, npr. oni koji se odnose na kvalifikacije osoblja, dostupne kapacitete, sigurnosne mjere, interne politike i postupke, te financijski zahtjevi utvrđeni su u Obavijesti PIPC-a 2020-9 o kombiniranju i prijenosu pseudonimiziranih informacija (Prilog I.). PIPC može opozvati (nakon saslušanja) imenovanje stručnom agencijom za kombiniranje podataka ako za to postoje određeni razlozi, npr. ako agencija više ne ispunjava sigurnosne standarde potrebne za imenovanje ili ako je u kontekstu kombiniranja podataka došlo do povrede podataka (članak 29-2. stavci 5. i 6. Dekreta o izvršavanju PIPA-e). PIPC mora objaviti svako imenovanje (ili opoziv imenovanja) stručne agencije za kombiniranje podataka (članak 29-2. stavak 7. Dekreta o izvršavanju PIPA-e).

obrade mora dostaviti dokumentaciju o, među ostalim, podacima koje treba kombinirati, svrsi kombiniranja te predloženim sigurnosnim mjerama za obradu kombiniranih podataka ([67]). Kako bi se omogućilo kombiniranje, voditelj obrade mora poslati podatke koje treba kombinirati specijaliziranoj instituciji i dostaviti „ključ za kombiniranje" (tj. informacije koje su upotrijebljene za pseudonimizaciju) Korejskoj agenciji za internet i sigurnost ([68]). Ta agencija generira „podatke za povezivanje ključeva za kombiniranje" (koji omogućuju povezivanje ključeva za kombiniranje različitih podnositelja zahtjeva radi provođenja kombiniranja tih skupova podataka) i dostavlja ih specijaliziranoj instituciji ([69]).

(48) Voditelj obrade koji traži kombiniranje informacija smije analizirati te kombinirane informacije u prostorima specijalizirane institucije u kojima se primjenjuju posebne tehničke, fizičke i administrativne sigurnosne mjere (članak 29-3. Dekreta o izvršavanju PIPA-e). Voditelji obrade koji su dali skup podataka za to kombiniranje smiju kombinirane podatke izvesti iz specijalizirane institucije tek nakon njihove daljnje pseudonimizacije ili anonimizacije i uz odobrenje te institucije (članak 28-3. stavak 2. PIPA-e) ([70]). Pri razmatranju toga da da odobrenje institucija će ocijeniti povezanost kombiniranih podataka i svrhe obrade te je li za upotrebu tih podataka izrađen poseban sigurnosni plan ([71]). Izvoz kombiniranih informacija izvan institucije neće se dopustiti ako te informacije sadržavaju podatke koji bi omogućili utvrđivanje identiteta pojedinca ([72]). Naposljetku, kombiniranje i prijenos pseudonimiziranih podataka koje obavlja specijalizirana institucija nadzire PIPC (članak 29-4. stavak 3. Dekreta o izvršavanju PIPA-e).

2.3.2. *Obrada posebnih kategorija osobnih podataka*

(49) Trebale bi postojati posebne zaštitne mjere ako se obrađuju „posebne kategorije" podataka.

(50) PIPA sadržava posebna pravila o obradi osjetljivih podataka ([73]), koji se definiraju kao osobni podaci kojima se otkrivaju informacije o ideologiji, uvjerenjima, primanju u članstvo sindikata ili političke stranke ili prestanku tog članstva, političkim stajalištima, zdravstvenom stanju i spolnom životu pojedinca te druge osobne informacije za koje je vjerojatno da bi „znatno" ugrozile privatnost ispitanika i koje su predsjedničkim dekretom propisane kao osjetljive ([74]). Prema pojašnjenjima dobivenima od PIPC-a, pojam spolni život tumači se tako da obuhvaća i spolnu orijentaciju ili sklonosti ([75]). Nadalje, člankom 18. Dekreta o izvršavanju u opseg pojma osjetljivih podataka dodaju se dodatne kategorije, ponajprije informacije o DNK-u pribavljene genetskim testiranjem i podaci koji čine kaznenu evidenciju. Nedavnom izmjenom Dekreta o izvršavanju PIPA-e dodatno je proširen pojam osjetljivih podataka uključivanjem i osobnih podataka koji otkrivaju rasno ili etničko podrijetlo i biometrijske informacije ([76]). Nakon te izmjene pojam osjetljivih podataka na temelju PIPA-e u načelu je istovjetan pojmu osjetljivih podataka iz članka 9. Uredbe (EU) 2016/679.

(51) U skladu s člankom 23. stavkom 1. PIPA-e i slično onomu što je predviđeno člankom 9. stavkom 1. Uredbe (EU) 2016/679, obrada osjetljivih podataka općenito je zabranjena, osim ako se primjenjuje jedna od navedenih iznimaka ([77]). Tim iznimkama obrada se ograničava na slučajeve u kojima voditelj obrade obavijesti ispitanika

([67]) Članak 8. stavci 1. i 2. Obavijesti 2020-9 o kombiniranju i prijenosu pseudonimiziranih informacija.
([68]) Članak 2. stavci 3. i 6. i članak 9. stavak 1. Obavijesti 2020-9 o kombiniranju i prijenosu pseudonimiziranih informacija.
([69]) Članak 2. stavak 4. i članak 9. stavci 2. i 3. Obavijesti 2020-9 o kombiniranju i prijenosu pseudonimiziranih informacija. Specijalizirana institucija mora nakon kombiniranja podataka odmah uništiti podatke za povezivanje ključeva za kombiniranje (članak 9. stavak 4. Obavijesti).
([70]) Kršenja zahtjeva za kombiniranje skupova podataka mogu dovesti do izricanja kaznenih sankcija (članak 71. stavak 4-2. PIPA-e). Vidjeti i članak 29-2. stavak 4. Dekreta o izvršavanju PIPA-e.
([71]) Postupak za odobrenje prijenosa kombiniranih podataka utvrđen je u članku 11. Obavijesti 2020-9 o kombiniranju i prijenosu pseudonimiziranih informacija. Ponajprije, specijalizirana institucija mora osnovati „odbor za preispitivanje prijenosa", koji se sastoji od članova s opsežnim znanjem i iskustvom u području zaštite podataka.
([72]) Članak 29-2. stavak 4. Dekreta o izvršavanju PIPA-e i članak 11. Obavijesti br. 2020-9.
([73]) Potrebu za osiguravanjem posebnih zaštita za obradu osjetljivih podataka, kao što su osobni podaci koji se odnose na zdravlje ili spolno ponašanje, potvrdio je i korejski Ustavni sud, vidjeti Odluku Ustavnog suda HunMa 1139 od 31. svibnja 2007.
([74]) Članak 23. stavak 1. PIPA-e.
([75]) Vidjeti i Priručnik o PIPA-i, poglavlje III. odjeljak 2. o članku 23. (str. 157.–164).
([76]) To jest, osobne informacije dobivene posebnom tehničkom obradom podataka povezanih s fizičkim obilježjima, fiziološkim obilježjima ili obilježjima ponašanja pojedinca u svrhu jedinstvene identifikaciju tog pojedinca.
([77]) Nepoštovanje tih zahtjeva može dovesti do sankcija u skladu s člankom 71. točkom 3. PIPA-e.

u skladu s člancima 15. i 17. PIPA-e i pribavi zasebnu privolu (tj. privolu zasebnu od privole za obradu ostalih osobnih podataka) ili ako se obrada zahtijeva ili je dopuštena zakonom. Osim toga, tijela javne vlasti mogu biometrijske informacije, informacije o DNK-u dobivene genetskim testiranjem, osobne informacije koje otkrivaju rasno ili etničko podrijetlo i podatke koji čine kaznenu evidenciju obrađivati na temelju onih osnova koje su dostupne isključivo njima (primjerice, ako je to potrebno za istrage kaznenih djela ili sudu za vođenje predmeta) ([78]). Stoga su pravne osnove koje su dostupne za obradu osjetljivih podataka ograničenije nego osnove za druge vrste osobnih podataka te su u korejskom pravu čak i restriktivnije od osnova na temelju članka 9. stavka 2. Uredbe (EU) 2016/679.

(52) Nadalje, u članku 23. stavku 2. PIPA-e – nepoštovanje te odredbe može dovesti do sankcija ([79]) – naglašava se naročita važnost osiguravanja prikladne sigurnosti pri postupanju s osjetljivim podacima kako „ne bi došlo do gubitka, krađe, otkrivanja, krivotvorenja, izmjene ili oštećenja" tih podataka. Iako je to opći zahtjev na temelju članka 29. PIPA-e, u članku 3. stavku 4. pojašnjava se da se razina sigurnosti mora prilagoditi vrsti osobnih podataka koji se obrađuju, što znači da se u obzir moraju uzeti posebni rizici povezani s obradom osjetljivih podataka. Nadalje, obrada podataka mora se uvijek provoditi „tako da se mogućnost povrede privatnosti ispitanika svede na najmanju mjeru" i po mogućnosti „anonimizacijom" (članak 3. stavci 6. i 7. PIPA-e). Ti zahtjevi naročito su relevantni ako se obrada odnosi na osjetljive podatke.

2.3.3. *Ograničavanje svrhe*

(53) Osobni podaci trebali bi se prikupljati u određenu svrhu i na način koji nije nesukladan svrsi obrade.

(54) To načelo osigurava se člankom 3. stavcima 1. i 2. PIPA-e, prema kojima voditelj obrade mora „izričito navesti" svrhu obrade, osobne podatke obrađivati na prikladan način potreban za tu svrhu i ne smije ih upotrebljavati izvan te svrhe. Opće načelo ograničavanja svrhe potvrđuje se i u članku 15. stavku 1., članku 18. stavku 1., članku 19. i – za izvršitelje obrade (takozvane „vanjske izvršitelje") – u članku 26. stavku 1. točki 1. i članku 26. stavcima 5. i 7. PIPA-e. Konkretno, osobni podaci smiju se u načelu upotrebljavati i prosljeđivati trećim stranama samo u okviru svrhe u koju su prikupljeni (članak 15. stavak 1. i članak 17. stavak 1. točka 2.). Obrada u sukladnu svrhu, tj. „u okviru koji je razumno povezan s prvotnom svrhom prikupljanja" može se provoditi samo ako ne utječe negativno na predmetne ispitanike i ako su donesene potrebne sigurnosne mjere (kao što je enkripcija) (članak 15. stavak 3. i članak 17. stavak 4. PIPA-e). Kako bi se utvrdilo provodi li se daljnja obrada u sukladnu svrhu, u Dekretu o izvršavanju PIPA-e navode se posebni kriteriji koji su slični onima predviđenima člankom 6. stavkom 4. Uredbe (EU) 2016/679, vidjeti uvodnu izjavu 36.

(55) Kako je objašnjeno u uvodnoj izjavi 38., svrha prikupljanja u slučaju korejskih voditelja obrade koji primaju osobne podatke iz Unije svrha je u koju su ti podaci preneseni. Mogućnost da voditelj obrade promijeni svrhu dopuštena je samo iznimno, u određenim (navedenim) slučajevima (članak 18. stavak 2. točke od 1. do 3. PIPA-e, vidjeti i uvodnu izjavu 39.). U mjeri u kojoj je promjena svrhe dopuštena zakonom, u tim se zakonima mora poštovati temeljno pravo na privatnost i zaštitu podataka, kao i načela nužnosti i proporcionalnosti iz korejskog Ustava. Nadalje, člankom 18. stavcima 2. i 5. PIPA-e predviđaju se dodatne zaštitne mjere, ponajprije zahtjev da se takvom promjenom svrhe ne smiju „nepravedno povrijediti interesi ispitanika" pa je stoga uvijek nužno uravnoteženje interesa. Time se osigurava razina zaštite koja je u načelu istovjetna onoj na temelju članka 5. stavka 1. točke (b) i članka 6. u vezi s uvodnom izjavom 50. Uredbe (EU) 2016/679.

2.3.4. *Točnost i smanjenje količine podataka*

(56) Osobni podaci trebali bi biti točni i, prema potrebi, ažurirani. Trebali bi biti i primjereni, relevantni i ograničeni na ono što je nužno u odnosu na svrhe u koje se obrađuju.

([78]) U članku 18. Dekreta o izvršavanju PIPA-e propisuje se da su kategorije podataka koje su tamo navedene isključene od odredbe iz članka 23. stavka 1. Zakona ako ih obrađuje javna institucija u skladu s člankom 18. stavkom 2. točkama od 5. do 9. PIPA-e.

([79]) Vidjeti članak 73. točku 1. i članak 75. stavak 2. točku 6. PIPA-e.

(57) Načelo točnosti na sličan je način potvrđeno u članku 3. stavku 3. PIPA-e, u kojem se zahtijeva da osobni podaci budu „točni, potpuni i ažurirani u mjeri u kojoj je to nužno u odnosu na svrhe" u koje se ti podaci obrađuju. Smanjenje količine podataka zahtijeva se na temelju članka 3. stavaka 1. i 6. i članka 16. stavka 1. PIPA-e, u kojima se propisuje da voditelj obrade (samo) prikuplja osobne podatke „u najmanjoj mjeri koja je potrebna " za predviđenu svrhu te je na njemu teret dokazivanja u tom pogledu. Ako je svrhu prikupljanja moguće ostvariti obradom informacija u anonimiziranom obliku, voditelji obrade trebali bi to nastojati učiniti (članak 3. stavak 7. PIPA-e).

2.3.5. *Ograničenje pohrane*

(58) Osobni podaci u načelu se ne bi trebali čuvati duže nego što je nužno za svrhe u koje se obrađuju.

(59) Načelo ograničenja pohrane na sličan je način propisano člankom 21. stavkom 1. PIPA-e ([80]), u kojem se od voditelja obrade zahtijeva da bez odgode „uništi" ([81]) osobne podatke nakon ostvarenja svrhe obrade ili nakon isteka razdoblja pohrane (ovisno o tome što nastupi ranije), osim ako se daljnja pohrana zahtijeva zakonom ([82]). U potonjem se slučaju relevantni osobni podaci „pohranjuju i njima se upravlja zasebno od drugih osobnih informacija" (članak 21. stavak 3. PIPA-e).

(60) Članak 21. stavak 1. PIPA-e ne primjenjuje se kad se pseudonimizirani podaci obrađuju u statističke svrhe, svrhe znanstvenog istraživanja ili svrhe arhiviranja u javnom interesu ([83]). Kako bi se i u tom slučaju osiguralo poštovanje načela ograničene pohrane podataka, u Obavijesti 2021-5 od voditelja obrade zahtijeva se da te informacije anonimiziraju u skladu s člankom 58-2. PIPA-e ako ti podaci nisu uništeni nakon ostvarenja određene svrhe obrade ([84]).

2.3.6. *Sigurnost podataka*

(61) Osobni podaci trebali bi se obrađivati tako da se jamči njihova sigurnost, uključujući zaštitu od neovlaštene ili nezakonite obrade te od slučajnog gubitka, uništenja ili oštećenja. U tu bi svrhu poslovni subjekti trebali poduzeti odgovarajuće tehničke ili organizacijske mjere za zaštitu osobnih podataka od mogućih prijetnji. Te bi mjere trebalo procijeniti uzimajući u obzir najsuvremeniju tehnologiju, povezane troškove i prirodu, opseg, kontekst i svrhe obrade te rizike za prava pojedinaca.

(62) Slično načelo sigurnosti utvrđeno je u članku 3. stavku 4. PIPA-e, u kojem se od voditelja obrade zahtijeva da „upravljaju osobnim informacijama na siguran način u skladu s metodama obrade, vrstom i drugim obilježjima osobnih informacija, uzimajući u obzir mogućnost povrede prava ispitanika i ozbiljnost relevantnih rizika". Nadalje, voditelj obrade „obrađuje osobne informacije tako da se mogućnost povrede privatnosti ispitanika svede na najmanju mjeru" i u tom kontekstu nastoji, po mogućnosti, obrađivati osobne podatke u anonimiziranom ili pseudonimiziranom obliku (članak 3. stavci 6. i 7. PIPA-e).

(63) Ti opći zahtjevi dodatno se razrađuju u članku 29. PIPA-e, prema kojem svaki voditelj obrade „poduzima tehničke, upravljačke i fizičke mjere, kao što su izrada plana unutarnjeg upravljanja i čuvanje evidencije prijava itd., koje su potrebne za jamčenje sigurnosti kako je propisano Predsjedničkim dekretom da ne bi

([80]) Članak 8. (u vezi s člankom 8-2. Dekreta o izvršavanju), članak 11. (u vezi s člankom 12. stavkom 2. Dekreta o izvršavanju).
([81]) O metodama za uništavanje osobnih informacija vidjeti članak 16. Dekreta o izvršavanju PIPA-e. U članku 21. stavku 2. PIPA-e pojašnjava se da to uključuje „mjere koje su nužne za sprečavanje oporavljanja i obnavljanja".
([82]) Nepoštovanje tih zahtjeva može dovesti do kaznenih sankcija (članak 73. stavak 1-2. PIPA-e). Člankom 39-6. PIPA-e uvodi se dodatan zahtjev pružateljima informacijskih i komunikacijskih usluga da izbrišu osobne informacije korisnika koji nisu koristili ponuđene informacijske i komunikacijske usluge barem godinu dana (osim ako se daljnja pohrana zahtijeva zakonom ili na zahtjev pojedinca). Pojedinci se moraju obavijestiti o namjeri brisanja njihovih informacija 30 dana prije isteka tog roka od godine dana (članak 39-6. stavak 2. PIPA-e i članak 48-5. stavak 3. Dekreta o izvršavanju PIPA-e). Ako se daljnja pohrana zahtijeva zakonom, pohranjeni podaci moraju se pohraniti zasebno od ostalih informacija korisnika i smiju se upotrebljavati ili otkrivati jedino u skladu s tim zakonom (članak 48-5. stavci 1. i 2. Dekreta o izvršavanju PIPA-e).
([83]) Članak 28-7. PIPA-e.
([84]) Obavijest 2021-5 (Prilog I.), odjeljak 4.

došlo do gubitka, krađe, otkrivanja, krivotvorenja, izmjene ili oštećenja osobnih informacija". U članku 30. stavku 1. Dekreta o izvršavanju PIPA-e te se mjere pobliže određuju tako što se navodi sljedeće: 1. izrada i provedba plana unutarnjeg upravljanja za sigurnu obradu osobnih podataka, 2. kontrole i ograničenja pristupa, 3. uvođenje tehnologije za enkripciju radi sigurne pohrane i prijenosa osobnih podataka, 4. evidencija prijava, 5. sigurnosni programi i 6. fizičke mjere kao što su sustav za sigurnu pohranu i zaključavanje ([85]).

(64) Osim toga, u slučaju povrede podataka primjenjuju se posebne obveze (članak 34. PIPA-e u vezi s člancima 39. i 40. Dekreta o izvršavanju PIPA-e) ([86]). Konkretno, od voditelja obrade zahtijeva se da bez odgode obavijesti ispitanike čiji su podaci povrijeđeni o pojedinostima povrede ([87]), što uključuje informacije o (obveznim) protumjerama koje je voditelj obrade poduzeo i o tome što ispitanici mogu poduzeti kako bi se rizik od štete sveo na najmanju mjeru (članak 34. stavci 1. i 2. PIPA-e) ([88]). Ako se povreda podataka odnosi na najmanje 1 000 ispitanika, voditelj obrade dužan je, bez odgode, o povredi podataka i protumjerama izvijestiti i PIPC i Korejsku agenciju za internet i sigurnost, koji mogu pružiti tehničku pomoć (članak 34. stavak 3. PIPA-e u vezi s člankom 39. Dekreta o izvršavanju PIPA-e). Voditelji obrade odgovaraju za štetu nastalu zbog povreda podataka, u skladu s odredbama Građanskog zakona o deliktnoj odgovornosti za štetu (vidjeti i odjeljak 2.5. o pravnoj zaštiti) ([89]).

(65) Voditelju obrade pri ispunjavanju njegovih obveza u pogledu sigurnosti mora pomagati službenik za zaštitu privatnosti, čije zadaće uključuju, među ostalim, osmišljavanje sustava unutarnje kontrole „radi sprečavanja otkrivanja, zloupotrebe i pogrešne upotrebe osobnih informacija" (članak 31. stavak 2. točka 4. PIPA-e). Nadalje, voditelj obrade dužan je provoditi „primjerenu kontrolu i nadzor" nad članovima svojeg osoblja koji obrađuju osobne podatke, među ostalim i s obzirom na sigurno upravljanje tim podacima; to uključuje potrebno osposobljavanje („edukaciju") zaposlenika (članak 28. stavci 1. i 2. PIPA-e). Naposljetku, u slučaju podobrade, voditelj obrade mora uvesti zahtjeve „vanjskom izvršitelju", među ostalim u pogledu sigurnog upravljanja osobnim podacima („tehničke i upravljačke zaštitne mjere"), i mora nadzirati način provedbe tih mjera inspekcijskim pregledima (članak 26. stavci 1. i 4. PIPA-e u vezi s člankom 28. stavkom 1. točkama 3. i 4. i člankom 28. stavkom 6. Dekreta o izvršavanju PIPA-e).

2.3.7. *Transparentnost*

(66) Ispitanike bi trebalo obavijestiti o glavnim obilježjima obrade njihovih osobnih podataka.

([85]) Kad je riječ o obradi osobnih podataka koju provode pružatelji informacijskih i komunikacijskih usluga, u članku 39-5. PIPA-e izričito se propisuje da se broj osoba koje postupaju s osobnim informacijama mora svesti na najmanju moguću mjeru. Nadalje, pružatelji informacijskih i komunikacijskih usluga dužni su osigurati da se osobne informacije korisnika ne otkriju javnosti putem informacijskih i komunikacijskih mreža (članak 39-10. stavak 1. PIPA-e). Na zahtjev PIPC-a otkrivene informacije moraju se izbrisati ili im se mora onemogućiti pristup (članak 39-10. stavak 2. PIPA-e). Općenitije, pružatelji informacijskih i komunikacijskih usluga (i treće strane koje prime osobne podatke korisnika) podliježu dodatnim sigurnosnim obvezama navedenima u članku 48-2. Dekreta o izvršavanju PIPA-e, npr. izrada i provedba plana unutarnjeg upravljanja u odnosu na sigurnosne mjere, mjere za osiguranje kontrole pristupa, enkripcija, upotreba softvera za otkrivanje zlonamjernih računalnih programa itd.

([86]) Osim toga, postoji opća zabrana oštećivanja, uništavanja, izmjene, krivotvorenja ili otkrivanja osobnih informacija bez pravnog ovlaštenja, vidjeti članak 59. točku 3. PIPA-e.

([87]) Zahtjev za obavješćivanje pojedinca ne primjenjuje se ako je do povrede podataka došlo u vezi sa pseudonimiziranim informacijama koje se obrađuju u svrhu prikupljanja statističkih podataka, provođenja znanstvenih istraživanja ili arhiviranja u javnom interesu (članak 28-7. PIPA-e, u kojem se predviđa izuzeće od članka 34. stavka 1. i članka 39-4. PIPA-e). Kako bi osigurao obavješćivanje pojedinaca, predmetni voditelj obrade trebao bi utvrditi njihov identitet iz pseudonimiziranog skupa podataka, što je izričito zabranjeno člankom 28-5. PIPA-e. Međutim, i dalje se primjenjuje zahtjev za opće obavješćivanje (PIPC-a) o povredi podataka.

([88]) Zahtjevi za obavješćivanje, uključujući vrijeme u kojem je to potrebno učiniti i mogućnost obavješćivanja „u fazama", dodatno su utvrđeni u članku 40. Dekreta o izvršavanju PIPA-e. Stroža se pravila primjenjuju na pružatelje informacijskih i komunikacijskih usluga, od kojih se zahtijeva da ispitanika i PIPC obavijeste u roku od 24 sata nakon što su saznali da su osobne informacije izgubljene, ukradene ili neovlašteno otkrivene (članak 39-4. stavak 1. PIPA-e). Ta obavijest mora uključivati pojedinosti o osobnim informacijama koje su neovlašteno otkrivene, točnom vremenu kad se to dogodilo, mjerama koje korisnik može poduzeti, mjerama odgovora na povredu koje je donio pružatelj usluga i kontaktnim podacima odjela kojem korisnik može uputiti svoja pitanja (članak 39-4. stavak 1. točke od 1. do 5. PIPA-e). Ako postoji opravdan razlog, npr. nepostojanje kontaktnih podataka korisnika, mogu se primijeniti drugi načini obavješćivanja, npr. javno objavljivanje te informacije na internetskim stranicama (članak 39-4. stavak 1. PIPA-e u vezi s člankom 48-4. stavkom 4. i dalje Dekreta o izvršavanju PIPA-e). U tom se slučaju o tim razlozima mora obavijestiti PIPC (članak 34-4. stavak 3. PIPA-e).

([89]) Vidjeti npr. odluke Vrhovnog suda 2011Da59834, 2011Da59858 i 2011Da59841 od 26. prosinca 2012. Sažetak na engleskom jeziku dostupan je na: http://library.scourt.go.kr/SCLIB_data/decision/9-69%202012.12.26.2011Da59834.htm.

(67) To se u korejskom sustavu osigurava na različite načine. Osim prava na obavješćivanje u skladu s člankom 4. točkom 1. PIPA-e (opće obavješćivanje) i člankom 20. stavkom 1. PIPA-e (za osobne podatke prikupljene od trećih strana) te prava na pristup u skladu s člankom 35. PIPA-e, PIPA uključuje i opći zahtjev transparentnosti u pogledu svrhe obrade (članak 3. stavak 1. PIPA-e) te posebne zahtjeve transparentnosti ako se obrada temelji na privoli (članak 15. stavak 2., članak 17. stavak 2. i članak 18. stavak 3. PIPA-e) ([90]). Nadalje, člankom 20. stavkom 2. PIPA-e od određenih se voditelja obrade – onih kod kojih obrada premašuje određene pragove ([91]) – zahtijeva da ispitanika čije su osobne podatke primili od treće strane obavijeste o izvoru informacija, svrsi obrade i njegovu pravu da zatraži suspenziju obrade, osim ako se takvo obavješćivanje pokaže nemogućim zbog nepostojanja bilo kakvih kontaktnih informacija. Iznimke se primjenjuju na određene datoteke s osobnim podacima koje drže tijela javne vlasti, ponajprije datoteke koje sadržavaju podatke koji se obrađuju u svrhe nacionalne sigurnosti, drugih naročito važnih („ozbiljnih”) nacionalnih interesa ili kaznenog progona, ili ako bi se obavješćivanjem vjerojatno ugrozio život ili zdravlje druge osobe ili nepravedno nanijela šteta imovini i drugim interesima druge osobe, ali samo ako predmetni javni ili privatni interesi „nedvojbeno imaju prednost” pred pravima predmetnih ispitanika (članak 20. stavak 4. PIPA-e). To zahtijeva uravnoteženje interesa.

(68) Osim toga, u članku 3. stavku 5. PIPA-e propisuje se da voditelji obrade moraju javno objaviti svoju politiku zaštite privatnosti (i druga pitanja povezana s obradom osobnih podataka). Taj se zahtjev dodatno razrađuje u članku 30. PIPA-e u vezi s člankom 31. Dekreta o izvršavanju PIPA-e. U skladu s tim odredbama politika zaštite privatnosti mora, među ostalim, uključivati sljedeća pitanja: 1. vrste osobnih podataka koji se obrađuju, 2. svrhu obrade, 3 razdoblje pohrane, 4. proslјeđuju li se osobni podaci trećoj strani ([92]), 5. provodi li se ikakva podobrada, 6. informacije o pravima ispitanika i kako se mogu ostvariti te 7. kontaktne informacije (uključujući ime službenika za zaštitu privatnosti ili podatke o unutarnjem odjelu odgovornom za osiguravanje poštovanja pravila o zaštiti podataka i rješavanje pritužbi). Politika zaštite privatnosti mora se objaviti tako da je ispitanici „mogu lako uočiti” (članak 30. stavak 2. PIPA-e) ([93]) i mora se stalno ažurirati (članak 31. stavak 2. Dekreta o izvršavanju PIPA-e).

(69) Javne institucije podliježu dodatnoj obvezi da pri PIPC-u registriraju ponajprije sljedeće informacije: 1. ime javne institucije. 2. osnove za obradu datoteka s osobnim podacima i svrhe te obrade, 3. pojedinosti o osobnim podacima koji se bilježe, 4. metodu obrade, 5. razdoblje pohrane, 6. broj ispitanika čiji se osobni podaci pohranjuju, 7. odjel zadužen za rješavanje zahtjeva ispitanika i 8. primatelje osobnih podataka ako se podaci rutinski ili učestalo proslјeđuju (članak 32. stavak 1. PIPA-e) ([94]). PIPC objavljuje registrirane datoteke s osobnim podacima, a javne institucije moraju u svojoj politici zaštite privatnosti navesti i upućivanja na njih (članak 30. stavak 1. i članak 32. stavak 4. PIPA-e).

(70) Kako bi se povećala transparentnost za ispitanike iz Unije čiji se osobni podaci prenose u Koreju na temelju ove Odluke, u odjeljku 3. točkama i. i ii. Obavijesti 2021-5 (Prilog I.) uvode se dodatni zahtjevi transparentnosti. Prvo, kad primaju osobne podatke iz Unije na temelju ove Odluke, korejski voditelji obrade moraju obavijestiti predmetne ispitanike bez neopravdane odgode (a u svakom slučaju najkasnije mjesec dana od prijenosa) o imenima i kontaktnim podacima subjekata koji prenose i primaju te informacije, prenesenim osobnim podacima

([90]) Konkretno, kad se osobne informacije obrađuju uz privolu pojedinca, voditelj obrade mora ga obavijestiti o svrsi obrade, pojedinostima o informacijama koje će se obrađivati, primatelju tih informacija, razdoblju tijekom kojeg se informacije pohranjuju i upotrebljavaju te o tome da pojedinac ima pravo uskratiti privolu (i svim negativnim posljedicama koje bi mogle iz toga proizaći).

([91]) U skladu s člankom 15-2. stavkom 1. Dekreta o izvršavanju PIPA-e, to se odnosi na voditelje obrade koji obrađuju osjetljive informacije od najmanje 50 000 ispitanika ili „obične” osobne informacije od najmanje milijun ispitanika. U članku 15-2. stavku 2. Dekreta o izvršavanju PIPA-e utvrđuju se metode i vrijeme obavješćivanja, a u članku 15-2. stavku 3. propisuje se zahtjev za čuvanje određenih evidencija o tome. Osim toga, posebna pravila primjenjuju se na određene kategorije pružatelja informacijskih i komunikacijskih usluga (one koji su u prethodnoj godini ostvarili prihode od prodaje u iznosu od najmanje 10 milijardi vona ili one koji su u posljednja tri mjeseca prethodne godine pohranjivali osobne podatke/upravljali osobnim podacima od prosječno najmanje milijun korisnika dnevno), od kojih se zahtijeva da redovito obavješćuju korisnike o povijesti upotrebe njihovih osobnih informacija, osim ako se to pokaže nemogućim zbog nepostojanja nikakvih kontaktnih informacija (članak 39-8. PIPA-e i članak 48-6. Dekreta o izvršavanju PIPA-e).

([92]) Prema informacijama dobivenima od korejske vlade, to uključuje obvezu da se u politici zaštite privatnosti pojedinačno navedu ti primatelji.

([93]) Drugi načini objave utvrđeni su u članku 31. stavku 3. Dekreta o izvršavanju PIPA-e.

([94]) Zahtjev za registriranje ne primjenjuje se na određene vrste datoteka s osobnim informacijama, primjerice na one u kojima se bilježe informacije povezane s nacionalnom sigurnošću, diplomatskim tajnama, kaznenim istragama, kaznenim progonom, kažnjavanjem, istragama kaznenih djela koja se odnose na oporezivanje, ili na datoteke koji se isključivo odnose na unutarnje informacije o radnom učinku (članak 32. stavak 2. PIPA-e).

(ili kategorijama osobnih podataka), svrsi u koju ih korejski voditelj obrade prikuplja, razdoblju pohrane i pravima koja imaju na temelju PIPA-e. Drugo, kad se osobni podaci primljeni iz Unije na temelju ove Odluke prosljeđuju trećim stranama, ispitanici se moraju obavijestiti, među ostalim, o primatelju, osobnim podacima ili kategorijama osobnih podataka koji će se proslijediti, zemlji u koju se ti podaci prosljeđuju (prema potrebi) te pravima koja imaju na temelju PIPA-e ([95]). Tako se Obaviješću osigurava da pojedinci iz EU-a i dalje budu obaviješteni o konkretnim voditeljima obrade koji obrađuju njihove informacije te da mogu ostvariti svoja prava u odnosu na relevantne subjekte.

(71) U odjeljku 3. točki iii. Obavijesti (Prilog I.) dopuštaju se određena ograničena i uvjetovana izuzeća od tih dodatnih obveza u pogledu transparentnosti koja su u načelu istovjetna izuzećima predviđenima Uredbom (EU) 2016/679. Konkretno, obavješćivanje ispitanika iz Unije ne zahtijeva se: 1. ako i onoliko dugo koliko je potrebno ograničiti obavješćivanje zbog određenih razloga od javnog interesa (primjerice, ako se informacije obrađuju u svrhe nacionalne sigurnosti ili kaznenih istraga koje su u tijeku), pod uvjetom da taj javni interes nedvojbeno ima prednost pred pravima ispitanika; 2. ako ispitanik već ima te informacije; 3. ako i dokle god bi se obavješćivanjem vjerojatno ugrozio život ili zdravlje tog pojedinca ili druge osobe ili nepravedno povrijedili imovinski interesi druge osobe ako ta prava ili interesi nedvojbeno imaju prednost pred pravima ispitanika; ili 4. ako ne postoje kontaktne informacije za predmetne pojedince ili bi bilo potrebno uložiti nerazmjeran napor da bi se oni obavijestili. Pri određivanju toga je li moguće stupiti u kontakt s ispitanikom ili uključuje li to prekomjeran napor uzet će se u obzir mogućnost suradnje s izvoznikom podataka u Uniju.

(72) Stoga se pravilima iz uvodnih izjava od 67. do 71. osigurava u načelu istovjetna razina zaštite s obzirom na transparentnost kao i ona koja se predviđa na temelju Uredbe (EU) 2016/679.

2.3.8. *Prava pojedinaca*

(73) Ispitanici bi trebali imati određena prava koja se mogu ostvariti u odnosu na voditelja obrade ili izvršitelja obrade, osobito pravo na pristup podacima, pravo na ispravak, pravo na prigovor na obradu i pravo na brisanje podataka. Istodobno, ta prava mogu podlijegati ograničenjima u mjeri u kojoj su ona nužna i proporcionalna kako bi se zaštitili važni ciljevi od općeg javnog interesa.

(74) U skladu s člankom 3. stavkom 5. PIPA-e voditelj obrade dužan je jamčiti ispitaniku prava navedena u članku 4. PIPA-e i dodatno razrađena u člancima od 35. do 37., članku 39. i članku 39-2. PIPA-e.

(75) Prvo, pojedinci imaju prava na informacije i pristup. Ako je voditelj obrade osobne podatke prikupio od treće strane – što će uvijek biti slučaj kad se podaci prenose iz Unije – ispitanici općenito imaju pravo na dobivanje informacija o 1. „izvoru" prikupljenih osobnih podataka (tj. o prenositelju), 2. svrsi obrade i 3. činjenici da ispitanik ima pravo zatražiti suspenziju obrade (članak 20. stavak 1. PIPA-e). Pritom se primjenjuju ograničena izuzeća, to jest ako bi se takvim obavješćivanjem vjerojatno ugrozio život ili zdravlje druge osobe ili „nepravedno nanijela šteta imovini i drugim interesima" druge osobe, ali samo ako ti interesi trećih strana „nedvojbeno imaju prednost" pred pravima ispitanika (članak 20. stavak 4. točka 2. PIPA-e).

(76) Osim toga, člankom 35. stavcima 1. i 3. PIPA-e u vezi s člankom 41. stavkom 4. Dekreta o izvršavanju PIPA-e ispitanicima se daje pravo na pristup vlastitim osobnim informacijama ([96]). Pravo na pristup obuhvaća potvrdu obrade, informacije o vrsti podataka koji se obrađuju, svrsi obrade, razdoblju pohrane, kao i svakom otkrivanju podataka trećoj strani te davanje preslike osobnih informacija koje se obrađuju (članak 4. točka 3. PIPA-e

([95]) Obavijest 2021-5, odjeljak 3. točka ii. (Prilog I.).

([96]) U skladu s člankom 35. stavkom 3. PIPA-e u vezi s člankom 42. stavkom 2. Dekreta o izvršavanju PIPA-e voditelj obrade može odgoditi davanje pristupa zbog „valjanog razloga" (tj. na temelju opravdanih razloga, npr. ako je potrebno više vremena da bi se procijenilo može li se pristup odobriti), ali mora obavijestiti ispitanika o tom opravdanju u roku od 10 dana i dati mu informacije o načinu podnošenja žalbe na tu odluku; čim razlog za odgodu prestane postojati, pristup se mora odobriti.

u vezi s člankom 41. stavkom 1. Dekreta o izvršavanju PIPA-e) ([97]). Pristup se može ograničiti (djelomičan pristup) ([98]) ili uskratiti samo ako je to predviđeno zakonom ([99]), ako bi se time vjerojatno ugrozio život ili zdravlje treće strane ili neopravdano povrijedila imovina i ostali interesi druge osobe (članak 35. stavak 4. PIPA-e) ([100]). Potonje podrazumijeva da bi trebalo postići ravnotežu između, s jedne strane, ustavom zaštićenih prava i sloboda pojedinca i, s druge strane, ustavom zaštićenih prava i sloboda drugih osoba. Ako se pristup ograniči ili uskrati, voditelj obrade mora obavijestiti ispitanika o razlozima za to i o načinu podnošenja žalbe na tu odluku (članak 41. stavak 5. i članak 42. stavak 2. Dekreta o izvršavanju PIPA-e).

(77) Drugo, ispitanici imaju pravo na ispravak ili brisanje ([101]) svojih osobnih podataka, „osim ako je drugim zakonima posebno predviđeno drukčije" (članak 36. stavci 1. i 2. PIPA-e) ([102]). Po zaprimanju zahtjeva voditelj obrade mora istražiti to pitanje bez odgode, poduzeti potrebne mjere ([103]) i obavijestiti ispitanika o tome u roku od 10 dana; ako se zahtjev ne može odobriti, taj zahtjev za obavješćivanje odnosi se na razloge za uskraćivanje pristupa i način podnošenja žalbe (vidjeti članak 36. stavak 4. PIPA-e u vezi s člankom 43. stavkom 3. Dekreta o izvršavanju PIPA-e) ([104]).

(78) Naposljetku, ispitanici imaju pravo na suspenziju obrade njihovih osobnih podataka, bez odgode ([105]), osim ako se primjenjuje jedna od navedenih iznimaka (članak 37. stavci 1. i 2. PIPA-e) ([106]). Voditelj obrade smije odbiti taj zahtjev 1. ako je to posebno dopušteno zakonom ili nužno („neizbježno") radi ispunjenja pravnih obveza, 2. ako bi se suspenzijom vjerojatno ugrozio život ili tijelo treće strane ili neopravdano povrijedila imovina i ostali interesi druge osobe, 3. ako bi javnoj instituciji bez obrade tih informacija bilo nemoguće obavljati svoju funkciju kako je propisano zakonom, ili 4. ako ispitanik izričito ne raskine temeljni ugovor s voditeljem obrade iako bi bilo neizvedivo izvršiti taj ugovor bez takve obrade podataka. U tom slučaju voditelj obrade mora, bez odgode, obavijestiti ispitanika o razlozima za odbijanje zahtjeva i načinu podnošenja žalbe (članak 37. stavak 2. PIPA-e u vezi s člankom 44. stavkom 2. Dekreta o izvršavanju PIPA-e). U skladu s člankom 37. stavkom 4. PIPA-e voditelj obrade pri ispunjavanju zahtjeva za suspenziju mora, bez odgode, „poduzeti potrebne mjere, uključujući uništenje relevantnih osobnih informacija" ([107]).

(79) Pravo na suspenziju primjenjuje se i ako se osobni podaci upotrebljavaju u svrhe izravne prodaje, tj. radi promicanja robe ili usluga ili nagovaranja na njihovu kupnju. Nadalje, za takvu daljnju obradu općenito je potrebna posebna (dodatna) privola ispitanika (vidjeti članak 15. stavak 1. točku 1. i članak 17. stavak 2. točku 1. PIPA-e) ([108]). Voditelj obrade pri traženju te privole mora ispitanika naročito obavijestiti, na „izričito

([97]) Pristup osobnim informacijama koje obrađuje javna institucija može se dobiti izravno od institucije ili neizravno podnošenjem zahtjeva PIPC-u, koji je dužan bez odgode proslijediti taj zahtjev (članak 35. stavak 2. PIPA-e i članak 41. stavak 3. Dekreta o izvršavanju PIPA-e).

([98]) U skladu s člankom 42. stavkom 1. Dekreta o izvršavanju PIPA-e voditelj obrade obvezan je odobriti djelomičan pristup ako barem dio informacija nije obuhvaćen razlozima za odbijanje.

([99]) Tim se zakonom mora poštovati temeljno pravo na privatnost i zaštitu podataka, kao i načela nužnosti i proporcionalnosti iz korejskog Ustava.

([100]) Osim toga, javne institucije mogu odbiti odobriti pristup ako bi to prouzročilo ozbiljne poteškoće u obavljanju određenih funkcija, uključujući revizije koje su u tijeku ili uvođenje, naplatu ili povrat poreza (članak 35. stavak 4. PIPA-e).

([101]) U tom slučaju voditelj obrade mora poduzeti mjere kojima se sprečava oporavljanje osobnih informacija, vidjeti članak 36. stavak 3. PIPA-e.

([102]) Ti zakoni moraju ispunjavati zahtjeve iz Ustava prema kojima se temeljno pravo smije ograničiti samo kad je to nužno radi nacionalne sigurnosti ili čuvanja javnog reda i mira za opću dobrobit te ne smiju utjecati na bit slobode ili prava (članak 37. stavak 2. Ustava).

([103]) U članku 43. stavku 2. Dekreta o izvršavanju PIPA-e predviđa se poseban postupak ako voditelj obrade obrađuje datoteke s osobnim informacijama koje mu je proslijedio drugi voditelj obrade.

([104]) Nepoduzimanje potrebnih mjera za ispravljanje ili brisanje osobnih informacija te daljnja upotreba tih informacija ili njihovo prosljeđivanje trećoj strani mogu dovesti do kaznenih sankcija (članak 73. stavak 2. PIPA-e).

([105]) U skladu s člankom 44. stavkom 2. Dekreta o izvršavanju PIPA-e voditelj obrade dužan je obavijestiti ispitanika o tome da je propisno suspendirao obradu u roku od 10 dana od zaprimanja zahtjeva.

([106]) Kad je riječ o javnim institucijama, pravo na suspenziju obrade može se ostvariti u odnosu na informacije koje se nalaze u registriranim datotekama s osobnim informacijama (članak 37. u vezi s člankom 32. PIPA-e). Takva registracija ne zahtijeva se u ograničenom broju situacija, npr. kad se datoteke s osobnim informacijama odnose na nacionalnu sigurnost, kaznene istrage, diplomatske odnose itd. (članak 32. stavak 2. PIPA-e).

([107]) Ako se obrada ne suspendira, to može dovesti do kaznenih sankcija (članak 73. stavak 3. PIPA-e).

([108]) Odbor za posredovanje u sporovima (vidjeti uvodnu izjavu 133.) odlučivao je u nekoliko predmeta u kojima su se pojedinci žalili na upotrebu njihovih podataka u svrhe izravne prodaje bez njihove privole, zbog čega je, primjerice, relevantni voditelj obrade morao platiti naknadu i izbrisati osobne podatke (vidjeti npr. Odbor za posredovanje u sporovima 20R10-024(2020.11.18), 20R08-015(2020,8,28), 20R07-031(2020.9.1)).

uočljiv način”, o namjeri upotrebe tih podataka u svrhe izravne prodaje – tj. tome da bi ga se moglo kontaktirati radi promicanja robe ili usluga ili nagovaranja na njihovu kupnju (članak 22. stavci 2. i 4. PIPA-e u vezi s člankom 17. stavkom 2. točkom 1. Dekreta o izvršavanju PIPA-e).

(80) Kako bi se olakšalo ostvarivanje prava pojedinaca, voditelj obrade mora uspostaviti posebne postupke za to i objaviti ih (članak 38. stavak 4. PIPA-e) ([109]). To uključuje postupke za ulaganje prigovora na odbijanje zahtjeva (članak 38. stavak 5. PIPA-e). Voditelj obrade mora osigurati da je postupak za ostvarivanje prava „lako razumljiv ispitanicima” i da nije zahtjevniji od postupka za prikupljanje osobnih podataka; to uključuje i obvezu navođenja informacija o tom postupku na internetskim stranicama voditelja obrade (članak 41. stavak 2., članak 43. stavak 1. i članak 44. stavak 1. Dekreta o izvršavanju PIPA-e) ([110]). Pojedinci mogu ovlastiti zastupnika na podnošenje tog zahtjeva (članak 38. stavak 1. PIPA-e u vezi s člankom 45. Dekreta o izvršavanju PIPA-e). Iako voditelj obrade ima pravo naplatiti naknadu (i poštarinu, u slučaju zahtjeva da se kopije osobnih podataka dostave poštom), taj se iznos mora odrediti „u okviru stvarnih troškova potrebnih za obradu [zahtjeva]”; nikakva naknada (ni poštarina) ne smije se naplatiti ako je voditelj obrade prouzročio zahtjev (članak 38. stavak 3. PIPA-e u vezi s člankom 47. Dekreta o izvršavanju PIPA-e).

(81) PIPA i Dekret o izvršavanju PIPA-e ne sadržavaju opće odredbe koje bi se odnosile na pitanje odluka koje utječu na ispitanika i koje se isključivo temelje na automatiziranoj obradi osobnih podataka. Međutim, kad je riječ o osobnim podacima koji su prikupljeni u Uniji, svaku odluku koja se temelji na automatiziranoj obradi obično donosi voditelj obrade u Uniji (koji ima izravan odnos s predmetnim ispitanikom) te ona stoga podliježe Uredbi (EU) 2016/679 ([111]). To uključuje scenarije prijenosa u kojima obradu vrši strani (na primjer, korejski) poslovni subjekt koji djeluje kao posrednik (izvršitelj obrade) u ime voditelja obrade u Uniji (ili kao podizvršitelj obrade koji djeluje u ime izvršitelja obrade iz Unije nakon što je podatke dobio od voditelja obrade u Uniji koji ih je prikupio) koji onda na temelju toga donosi odluku. Stoga nije vjerojatno da će nepostojanje posebnih pravila za automatizirano donošenje odluka u PIPA-i utjecati na razinu zaštite osobnih podataka koji se prenose na temelju ove Odluke.

(82) Iznimno, odredbe o transparentnosti na zahtjev (članak 20.) i pravima pojedinaca (članci od 35. do 37.), kao i zahtjev za obavješćivanje pojedinaca koji se odnosi na pružatelje informacijskih i komunikacijskih usluga (članak 39-8. PIPA-e), ne primjenjuju se u odnosu na pseudonimizirane informacije ako se one obrađuju u svrhu prikupljanja statističkih podataka, provođenja znanstvenih istraživanja ili arhiviranja u javnom interesu (članak 28-7. PIPA-e) ([112]). U skladu s pristupom iz članka 11. stavka 2. (u vezi s uvodnom izjavom 57.) Uredbe (EU) 2016/679, to se opravdava činjenicom da bi voditelj obrade, kako bi osigurao transparentnost ili dodijelio pojedinačna prava, morao utvrditi jesu li (i, ako jesu, koji su) podaci povezani s pojedincem koji podnosi zahtjev, što je izričito zabranjeno PIPA-om (članak 28-5. stavak 1. PIPA-e). Osim toga, ako takva ponovna identifikacija podrazumijeva poništavanje pseudonimizacije cijelog (pseudonimiziranog) skupa podataka, osobne informacije svih drugih predmetnih pojedinaca bile bi izložene povećanim rizicima. Dok se u Uredbi (EU) 2016/679 upućuje na situacije u kojima je ponovna identifikacija praktički nemoguća, u PIPA-i se primjenjuje stroži pristup tako što se izričito zabranjuje ponovna identifikacija u svim situacijama u kojima se obrađuju pseudonimizirane informacije.

(83) Korejski sustav, kako je opisano u uvodnim izjavama od 74. do 82., stoga sadržava pravila o pravima ispitanika kojima se osigurava razina zaštite koja je u načelu istovjetna onoj na temelju Uredbe (EU) 2016/679.

([109]) Vidjeti i članak 30. stavak 1. točku 5. PIPA-e o politici zaštite privatnosti, koja, među ostalim, mora sadržavati informacije o pravima koja pojedinac ima i načinu njihova ostvarivanja.

([110]) Vidjeti i članak 39-7. stavak 2. PIPA-e u pogledu pružatelja informacijskih i komunikacijskih usluga.

([111]) Suprotno tome, u iznimnom slučaju kad korejski poslovni subjekt ima izravan odnos s ispitanikom iz EU-a, to je obično posljedica toga što se ciljano usmjerio na tog pojedinca u Europskoj uniji ponudom robe ili usluga ili praćenjem njegova ponašanja. U tom će scenariju sam korejski poslovni subjekt biti obuhvaćen područjem primjene Uredbe (EU) 2016/679 (članak 3. stavak 2.) te se mora izravno pridržavati prava EU-a o zaštiti podataka.

([112]) Vidjeti i Obavijest 2021-5, u kojoj se potvrđuje da se odjeljak III. PIPA-e (uključujući članak 28-7.) primjenjuje samo kad se pseudonimizirane informacije obrađuju u svrhe provođenja znanstvenih istraživanja, prikupljanja statističkih podataka ili arhiviranja u javnom interesu, vidjeti odjeljak 4. Priloga I. ovoj Odluci.

2.3.9. *Daljnji prijenosi*

(84) Razina zaštite osobnih podataka koji se prenose iz Unije voditeljima obrade u Republici Koreji ne smije se ugroziti daljnjim prijenosom tih podataka primateljima u trećim zemljama.

(85) Sa stajališta korejskog voditelja obrade takvi „daljnji prijenosi" čine međunarodne prijenose iz Republike Koreje. S obzirom na to, u PIPA-i se razlikuju eksternalizacija obrade vanjskom izvršitelju (tj. izvršitelju obrade) i prosljeđivanje osobnih podataka trećim stranama ([113]).

(86) Prvo, kad se obrada osobnih podataka eksternalizira subjektu koji se nalazi u trećoj zemlji, korejski voditelj obrade mora osigurati poštovanje odredaba PIPA-e o eksternalizaciji (članak 26. PIPA-e). To uključuje uvođenje pravno obvezujućeg instrumenta kojim se, među ostalim, obrada koju provodi vanjski izvršitelj ograničava na svrhu eksternaliziranog posla, uvode tehničke i upravljačke zaštitne mjere i ograničava podobrada (vidjeti članak 26. stavak 1. PIPA-e) te objavljivanje informacija o eksternaliziranom poslu. Osim toga, voditelj obrade obvezan je „educirati" vanjskog izvršitelja o potrebnim sigurnosnim mjerama i nadzirati (među ostalim, provođenjem inspekcijskih pregleda) poštovanje svih obveza voditelja obrade na temelju PIPA-e ([114]) te ugovora o eksternalizaciji.

(87) Ako vanjski izvršitelj prouzroči štetu obradom osobnih podataka suprotno odredbama PIPA-e, to će se pripisati voditelju obrade za potrebe utvrđivanja odgovornosti, kao što bi to bilo i da su štetu prouzročili zaposlenici voditelja obrade (članak 26. stavak 6. PIPA-e). Korejski voditelj obrade stoga je i dalje odgovoran za osobne podatke koji su eksternalizirani i mora osigurati da inozemni izvršitelj obrade obrađuje te informacije u skladu s PIPA-om. Ako vanjski izvršitelj obrađuje informacije suprotno odredbama PIPA-e, korejski voditelj obrade može se smatrati odgovornim za nepoštovanje svoje obveze da osigura poštovanje PIPA-e, primjerice, svojim nadzorom rada vanjskog izvršitelja. Zaštitnim mjerama uključenima u ugovor o eksternalizaciji i odgovornošću korejskog voditelja obrade za postupke vanjskog izvršitelja osigurava se kontinuitet zaštite kad se obrada osobnih podataka eksternalizira subjektu izvan Koreje.

(88) Drugo, korejski voditelji obrade smiju osobne podatke prosljeđivati trećim stranama koje se nalaze izvan Koreje. Iako PIPA sadržava niz zakonskih osnova na temelju kojih se općenito dopušta prosljeđivanje trećim stranama, ako se treća strana nalazi izvan Koreje, voditelj obrade u načelu ([115]) mora pribaviti privolu ispitanika ([116]) nakon što ga obavijesti o 1. vrsti osobnih podataka, 2. primatelju osobnih podataka, 3. svrsi prijenosa u smislu svrhe obrade koju će obavljati primatelj, 4. razdoblju pohrane za obradu koju će obavljati primatelj te o 5. činjenici da ispitanik može uskratiti privolu (članak 17. stavci 2. i 3. PIPA-e). U Obavijesti 2021-5, u njezinu odjeljku o transparentnosti (vidjeti uvodnu izjavu 70.), zahtijeva se da se pojedinci obavijeste o trećoj zemlji u koju će se njihovi podaci prosljeđivati. Time se osigurava da ispitanici iz Unije mogu donijeti potpuno utemeljenu odluku o davanju privole na prosljeđivanje u inozemstvo. Nadalje, voditelj obrade ne smije sklopiti ugovor s primateljem koji je treća strana suprotno odredbama PIPA-e, što znači da taj ugovor ne smije sadržavati obveze koje bi bile u suprotnosti sa zahtjevima koji su PIPA-om uvedeni voditelju obrade ([117]).

([113]) Na pružatelje informacijskih i komunikacijskih usluga primjenjuju se posebna pravila. U skladu s člankom 39-12. PIPA-e, pružatelji informacijskih i komunikacijskih usluga moraju u načelu pribaviti privolu korisnika za svaki prijenos osobnih informacija u inozemstvo. Ako se osobne informacije prenose u okviru eksternalizacije postupaka obrade, među ostalim i radi pohrane, privola nije potrebna ako su predmetni pojedinci unaprijed obaviješteni, izravno ili putem javne obavijesti kojoj se može lako pristupiti, o 1. pojedinostima informacija koje će se prenijeti, 2. zemlji u koju će se informacije prenijeti (te o datumu i metodi prijenosa), 3. imenu primatelja i 4. svrsi u koju će primatelj te informacije upotrebljavati i pohranjivati (članak 39-12. stavak 3. PIPA-e). Osim toga, u tom će se slučaju primjenjivati opći zahtjevi za eksternalizaciju. Za svaki pojedini prijenos moraju se uvesti posebne zaštitne mjere u pogledu sigurnosti, rješavanja pritužbi i sporova, kao i druge mjere potrebne za zaštitu informacija korisnika (članak 48-10. Dekreta o izvršavanju PIPA-e).

([114]) Vidjeti i članak 26. stavak 7. PIPA-e, u skladu s kojim se članci od 15. do 25., od 27. do 31., od 33. do 38. i članak 50. primjenjuju *mutatis mutandis* na izvršitelja obrade.

([115]) Ako pružatelji informacijskih i komunikacijskih usluga prosljeđuju osobne informacije korisnika trećim stranama, za to je uvijek potrebna privola korisnika (članak 39-12. stavak 2. PIPA-e).

([116]) Kako je detaljnije objašnjeno u bilješci 51., da bi takva privola bila valjana, mora se dati dobrovoljno, mora biti utemeljena i izričita.

([117]) Vidjeti i članak 39-12. stavak 1. PIPA-e u pogledu pružatelja informacijskih i komunikacijskih usluga.

(89) Osobni podaci smiju se prosljeđivati trećim stranama (u inozemstvu) bez privole pojedinca ako je svrha otkrivanja „u okviru koji je razumno povezan" s prvotnom svrhom prikupljanja (članak 17. stavak 4. PIPA-e, vidjeti uvodnu izjavu 36.). Međutim, pri odlučivanju o tome hoće li otkriti osobne podatke u „povezanu" svrhu voditelj obrade mora voditi računa o tome uzrokuju li se otkrivanjem negativne posljedice za ispitanika i jesu li poduzete potrebne sigurnosne mjere (kao što je enkripcija). Budući da treća zemlja u koju se osobni podaci prenose možda ne pruža zaštite slične onima predviđenima na temelju PIPA-e, u odjeljku 2. Obavijesti 2021-5 potvrđuje se da se takve negativne posljedice mogu pojaviti i da se mogu izbjeći jedino ako korejski voditelj obrade i inozemni primatelj, pravno obvezujućim instrumentom (kao što je ugovor), osiguraju razinu zaštite koja je istovjetna onoj iz PIPA-e, među ostalim i u pogledu prava ispitanika.

(90) Posebna se pravila primjenjuju na „nenamjensko" otkrivanje, tj. prosljeđivanje podataka trećoj strani u novu (nepovezanu) svrhu, koje se može provesti samo na temelju jedne od osnova iz članka 18. stavka 2. PIPA-e, kako je opisano u uvodnoj izjavi 39. Međutim, čak i pod tim uvjetima prosljeđivanje trećim stranama isključeno je ako će se njime vjerojatno „nepravedno povrijediti" interesi ispitanika ili treće strane, što zahtijeva uravnoteženje interesa. Osim toga, u skladu s člankom 18. stavkom 5. PIPA-e voditelj obrade mora primjenjivati dodatne zaštite mjere, što može uključivati zahtjev prema trećoj strani da ograniči svrhu i metodu obrade ili da uvede posebne sigurnosne mjere. Ponovno, s obzirom na to da treća zemlja u koju se osobni podaci prenose možda ne pruža zaštite slične onima predviđenima na temelju PIPA-e, u odjeljku 2. Obavijesti 2021-5 potvrđuje se da se takva „nepravedna povreda" interesa pojedinca ili treće strane može pojaviti i izbjeći jedino ako korejski voditelj obrade i inozemni primatelj, pravno obvezujućim instrumentom (kao što je ugovor), osiguraju razinu zaštite koja je istovjetna onoj iz PIPA-e, među ostalim i u pogledu prava ispitanika.

(91) Stoga se pravilima iz uvodnih izjava od 86. do 90. osigurava kontinuitet zaštite u slučaju daljnjeg prijenosa osobnih podataka („vanjskom izvršitelju" ili trećoj strani) iz Republike Koreje na način koji je u načelu istovjetan onomu što se predviđa Uredbom (EU) 2016/679.

2.3.10. *Odgovornost*

(92) Na temelju načela odgovornosti subjekti koji obrađuju podatke moraju uvesti odgovarajuće tehničke i organizacijske mjere kako bi djelotvorno ispunili svoje obveze u pogledu zaštite podataka te mogli dokazati da su ispunjene, prije svega nadležnom nadzornom tijelu.

(93) U skladu s člankom 3. stavcima 6. i 8. PIPA-e voditelj obrade mora osobne podatke obrađivati „tako da se mogućnost povrede privatnosti ispitanika svede na najmanju mjeru" te mora nastojati zadobiti povjerenje ispitanika tako da poštuje i izvršava zadaće i odgovornosti predviđene PIPA-om i drugim povezanim zakonima. To uključuje izradu plana unutarnjeg upravljanja (članak 29. PIPA-e) te uspostavljanje prikladnog osposobljavanja i nadzora osoblja (članak 28. PIPA-e).

(94) Kao sredstvo za osiguranje odgovornosti, člankom 31. PIPA-e u vezi s člankom 32. Dekreta o izvršavanju PIPA-e uvodi se obveza za voditelje obrade da imenuju službenika za zaštitu privatnosti koji „sveobuhvatno preuzima odgovornost za obradu osobnih informacija". Konkretno, taj službenik za zaštitu privatnosti zadužen je za obavljanje sljedećih funkcija: 1. izrada i provedba plana zaštite osobnih podataka i izrada politike zaštite privatnosti, 2. provođenje redovitih anketa o stanju i praksama obrade osobnih podataka radi otklanjanja bilo kakvih nedostataka, 3. rješavanje pritužbi i pitanja povezanih s naknadom radi ispravljanja štete, 4. uspostavljanje sustava unutarnje kontrole radi sprečavanja otkrivanja, zloupotrebe ili pogrešne upotrebe osobnih podataka, 5. pripremanje i provedba programa edukacije, 6. zaštita i kontroliranje datoteka s osobnim podacima te upravljanje njima i 7. uništavanje osobnih podataka nakon što se ostvari svrha obrade ili istekne razdoblje pohrane. U obavljanju tih dužnosti službenik za zaštitu privatnosti može provjeravati stanje obrade osobnih podataka i povezanih sustava te zatražiti informacije o njima (članak 31. stavak 3. PIPA-e). Ako službenik za zaštitu privatnosti sazna za bilo koju povredu PIPA-e ili drugih relevantnih zakona o zaštiti podataka, dužan je odmah poduzeti korektivne mjere i, prema potrebi, prijaviti te mjere upravi („čelniku") voditelja obrade (članak 31. stavak 4. PIPA-e). U skladu s člankom 31. stavkom 5. PIPA-e, službenik za zaštitu privatnosti ne smije snositi nikakve neopravdane negativne posljedice zbog obavljanja svojih funkcija.

(95) Osim toga, voditelji obrade moraju proaktivno nastojati provesti procjenu učinka na privatnost ako postupanje s datotekama s osobnim podacima uključuje rizik za privatnost (članak 33. stavak 8. PIPA-e). Na temelju članka 33. stavaka 1. i 2. PIPA-e u vezi s člancima 35., 36. i 38. Dekreta o izvršavanju PIPA-e relevantni čimbenici u procjeni rizika za prava ispitanika bit će, primjerice, vrsta i priroda podataka koji se obrađuju (a naročito to je li riječ o osjetljivim informacijama), količina podataka, razdoblje pohrane i vjerojatnost da će doći do povreda podataka. Svrha je procjene učinka na privatnost osigurati da se analiziraju čimbenici rizika za privatnost te sve sigurnosne ili druge protumjere te utvrditi elemente koje treba poboljšati (vidjeti članak 33. stavak 1. PIPA-e u vezi s člankom 38. Dekreta o izvršavanju PIPA-e).

(96) Javne institucije imaju obvezu provođenja procjene učinka kad obrađuju određene datoteke s osobnim podacima za koje postoji veći rizik od mogućih povreda privatnosti (članak 33. stavak 1. PIPA-e). U skladu s člankom 35. Dekreta o izvršavanju PIPA-e, takve su datoteke, među ostalim, datoteke koje sadržavaju osjetljive informacije o najmanje 50 000 ispitanika, datoteke koje se mogu povezati s drugim datotekama, pa će, zahvaljujući tom povezivanju, sadržavati informacije o najmanje 500 000 ispitanika, ili datoteke koje sadržavaju informacije o najmanje milijun ispitanika. Rezultat procjene učinka koju je provela javna institucija mora se priopćiti PIPC-u (članak 33. stavak 1. PIPA-e), koji može dati svoje mišljenje (članak 33. stavak 3. PIPA-e).

(97) Naposljetku, u članku 13. PIPA-e predviđa se da PIPC utvrđuje politike potrebne za promicanje i podupiranje „samoregulirajućih aktivnosti zaštite podataka" koje provode voditelji obrade, među ostalim, edukacijom o zaštiti podataka, promicanjem i podupiranjem organizacija koje se bave zaštitom podataka i pomaganjem voditeljima obrade pri utvrđivanju i provođenju samoregulirajućih pravila. Nadalje, PIPC uvodi i olakšava primjenu sustava oznaka za privatnost na internetu. U vezi s time, u članku 32-2. PIPA-e u vezi s člancima od 34-2. do 34-8. Dekreta o izvršavanju PIPA-e predviđa se mogućnost izdavanja certifikata kojim se potvrđuje da su sustavi voditelja obrade za obradu i zaštitu osobnih podataka usklađeni sa zahtjevima iz PIPA-e. U skladu s tim pravilima certifikat ([118]) se može izdati (na razdoblje od tri godine) ako voditelj obrade ispunjava kriterije za certificiranje koje je utvrdio PIPC, uključujući uvođenje upravljačkih, tehničkih i fizičkih zaštitnih mjera za zaštitu osobnih podataka ([119]). Kako bi se očuvala djelotvornost certifikata, PIPC mora barem jednom godišnje ispitati sustave voditelja obrade relevantne za taj certifikat, a to može dovesti do oduzimanja certifikata (članak 32. stavak 4. PIPA-e u vezi s člankom 34-5. Dekreta o izvršavanju PIPA-e; takozvano „daljnje praćenje").

(98) Stoga se načelo odgovornosti u korejskom okviru provodi tako da se osigurava razina zaštite koja je u načelu istovjetna onoj na temelju Uredbe (EU) 2016/679, među ostalim i predviđanjem različitih mehanizama za osiguravanje i dokazivanje usklađenosti s PIPA-om.

2.3.11. *Posebna pravila za obradu osobnih kreditnih informacija*

(99) Kako je opisano u uvodnoj izjavi 13., u CIA-i se utvrđuju posebna pravila za obradu osobnih kreditnih informacija koju provode komercijalni subjekti. Stoga komercijalni subjekti pri obradi osobnih kreditnih informacija moraju poštovati opće zahtjeve iz PIPA-e, osim ako CIA sadržava konkretnija pravila. To će primjerice biti slučaj kad ti subjekti obrađuju informacije povezane s kreditnom karticom ili bankovnim računom u kontekstu komercijalne transakcije s pojedincem. Budući da je CIA sektorsko zakonodavstvo za obradu kreditnih informacija (i osobnih i neosobnih), njome se uvode ne samo posebne zaštitne mjere za zaštitu podataka (primjerice, u pogledu transparentnosti i sigurnosti) već se i općenitije uređuju posebne okolnosti u kojima se osobne kreditne informacije mogu obrađivati. To se ponajprije odražava u detaljnim zahtjevima za upotrebu podataka, prosljeđivanje podataka trećoj strani i pohranjivanje tih podataka.

(100) Kao i PIPA-a, CIA-a sadržava načelo zakonitosti i proporcionalnosti. Prvo, kao opći zahtjev, člankom 15.stavkom 1. CIA-e dopušta se samo prikupljanje osobnih kreditnih informacija razumnim i poštenim sredstvima, i to u najmanjoj mjeri koja je nužna za ostvarenje određene svrhe, u skladu s člankom 3. stavcima 1. i 2. PIPA-e. Drugo, CIA-om se posebno uređuje zakonitost obrade osobnih kreditnih informacija, ograničavanjem njihova prikupljanja, upotrebe i prosljeđivanja trećoj strani te općenitim vezivanjem tih aktivnosti obrade za zahtjev za dobivanje privole predmetne osobe.

([118]) Osim toga, ako voditelj obrade namjerava navoditi ili promicati taj certifikat u svojim poslovnim aktivnostima, može koristiti oznaku za zaštitu osobnih informacija koju je uveo PIPC. Vidjeti članak 34-7. Dekreta o izvršavanju PIPA-e.

([119]) Od studenoga 2018. razvijen je „sustav za upravljanje osobnim informacijama i informacijskom sigurnošću" (engl. *Personal Information & Information Security Management System* – ISMS-P), kojim se certificira da voditelji obrade u radu primjenjuju sveobuhvatan sustav upravljanja.

(101) Osobne kreditne informacije smiju se prikupljati na temelju jedne od osnova predviđenih PIPA-om ili na temelju posebnih osnova utvrđenih u CIA-i. Budući da se člankom 45. Uredbe (EU) 2016/679 pretpostavlja da prijenos osobnih podataka provodi voditelj obrade ili izvršitelj obrade u Uniji, ali njime nije obuhvaćeno izravno prikupljanje podataka (primjerice, od pojedinca ili s internetskih stranica) koje provodi voditelj obrade u Koreji, za ovu su Odluku relevantne jedino privola i osnove dostupne na temelju PIPA-e. Te osnove uključuju ponajprije scenarije u kojima je prijenos nužan radi izvršenja ugovora s pojedincem ili za legitimne interese korejskog voditelja obrade (članak 15. stavak 1. točke 4. i 6. PIPA-e) ([120]).

(102) Nakon što su prikupljene, osobne kreditne informacije smiju se upotrebljavati 1. u prvotnu svrhu u koju ih je pojedinac (izravno) dao ([121]); 2. u svrhu koja je u skladu s prvotnom svrhom prikupljanja ([122]); 3. radi utvrđivanja treba li uspostaviti ili nastaviti komercijalni odnos koji je zatražio pojedinac ([123]); 4. u svrhu prikupljanja statističkih podataka, provođenja istraživanja ili arhiviranja u javnom interesu ([124]) ako su informacije pseudonimizirane ([125]); 5. ako se pribavi dodatna privola ili 6. u skladu sa zakonom.

(103) Ako komercijalni subjekt namjerava otkriti osobne kreditne informacije trećoj strani, mora pribaviti privolu pojedinca ([126]) nakon što ga obavijesti o primatelju tih podataka, svrsi u koju će primatelj obrađivati podatke, pojedinostima o podacima koji će se proslijediti, razdoblju tijekom kojeg će primatelj pohranjivati podatke i pravu na odbijanje davanja privole (članak 32. stavak 1. CIA-e i članak 28. stavak 2. Dekreta o izvršavanju CIA-e) ([127]). Taj zahtjev dobivanja privole ne primjenjuje se u određenim situacijama, to jest ako osobne kreditne informacije otkrivaju ([128]): 1. vanjskom izvršitelju u svrhe eksternalizacije ([129]); 2. trećoj strani u slučaju poslovnog prijenosa, podjele ili spajanja; 3. u svrhu prikupljanja statističkih podataka, provođenja istraživanja ili arhiviranja u javnom interesu ako su informacije pseudonimizirane; 4. u svrhu koja je u skladu s prvotnom svrhom prikupljanja; 5. trećoj strani koja te informacije upotrebljava radi naplate duga pojedinca ([130]); 6. radi ispunjavanja

([120]) CIA sadržava i druge pravne osnove za prikupljanje, tj. ako se to zahtijeva zakonom, ako je informacije javno objavila javna institucija u skladu sa zakonodavstvom o slobodi informiranja ili ako su informacije dostupne na društvenoj mreži. Kako bi se komercijalni subjekt mogao pozvati na posljednju navedenu osnovu, mora moći pokazati da se prikupljanje i dalje provodi u okviru privole ispitanika, na temelju razumnog („objektivnog") tumačenja i uzimajući u obzir prirodu podataka, namjeru i svrhu njihova objavljivanja na društvenoj mreži, toga je li svrha prikupljanja „izrazito relevantna" za tu svrhu itd. (članak 13. Dekreta o izvršavanju CIA-e). Međutim, kako je objašnjeno u uvodnoj izjavi 101., te osnove neće u načelu biti relevantne u scenariju prijenosa.

([121]) Primjerice, kad se kreditne informacije generiraju/daju u kontekstu komercijalne transakcije s pojedincem. Međutim, na tu se osnovu nije moguće pozivati za upotrebu osobnih kreditnih informacija u svrhe izravne prodaje (vidjeti članak 33. stavak 1. točku 3. CIA-e).

([122]) Kako bi se utvrdilo je li svrha upotrebe u skladu s prvotnom svrhom prikupljanja, u obzir se moraju uzeti sljedeći čimbenici: 1. odnos između te dvije svrhe („relevantnost"); 2. način na koji su te informacije prikupljene; 3. učinak te upotrebe na pojedinca; i 4. jesu li provedene prikladne sigurnosne mjere, kao što je pseudonimizacija (usp. članak 32. stavak 6. točku 9-4. CIA-e).

([123]) Primjerice, voditelj obrade možda mora uzeti u obzir osobne kreditne informacije koje je dobio od pojedinca kako bi odlučio hoće li produljiti rok otplate zajma tom pojedincu.

([124]) Članak 33. CIA-e, u vezi s člankom 32. stavkom 6. točkama 9-2., 9-4. i 10. CIA-e.

([125]) Pseudonimizacija se definira u članku 2. stavku 15. CIA-e kao obrada osobnih kreditnih informacija tako da se identitet pojedinaca više ne može utvrditi na temelju tih informacija, već samo u kombinaciji s dodatnim informacijama. Iako CIA sadržava posebne zaštitne mjere za obradu pseudonimiziranih informacija u svrhu prikupljanja statističkih podataka, provođenja istraživanja i arhiviranja u javnom interesu (članak 40-2. CIA-e), ta se pravila ne primjenjuju na komercijalne organizacije. Umjesto toga, te organizacije i dalje podliježu posebnim zahtjevima iz odjeljka III. PIPA-e, kako je opisano u uvodnim izjavama od 42. do 48. Nadalje, člankom 40-3. CIA-e obrada pseudonimiziranih kreditnih informacija – ako se provodi u svrhe prikupljanja statističkih podataka, provođenja znanstvenih istraživanja ili arhiviranja u javnom interesu – izuzima se od zahtjeva o transparentnosti i pravima pojedinaca, slično izuzeću iz članka 28-7. PIPA-e i podložno zaštitnim mjerama iz odjeljka III. PIPA-e, kako je detaljnije opisano u uvodnim izjavama od 42. do 48.

([126]) To se ne primjenjuje ako se informacije prosljeđuju trećoj strani radi održavanja točnosti i ažuriranosti osobnih kreditnih informacija, sve dok prosljeđivanje ostaje u okviru prvotne svrhe obrade (članak 32. stavak 1. CIA-e). To se može dogoditi, primjerice, ako se ažurirane informacije prosljeđuju agenciji za kreditni rejting kako bi se osigurala točnost njezinih evidencija.

([127]) Ako pružanje navedenih informacija nije praktično, može biti dovoljno da se pojedinac radi dobivanja potrebnih informacija uputi na treću stranu koja je primatelj.

([128]) Budući da se CIA-om ne uređuju posebno otkrivanja osobnih kreditnih informacija u inozemstvo, pri takvim otkrivanjima moraju se poštovati zaštitne mjere za daljnje prijenose koje su uvedene odjeljkom 2. Obavijesti br. 2021-5.

([129]) Eksternalizacija obrade osobnih kreditnih informacija smije se provoditi samo na temelju pisanog ugovora i u skladu sa zahtjevima iz članka 26. stavaka od 1. do 3. i stavka 5. PIPA-e, kako je opisano u uvodnoj izjavi 20. (članak 17. CIA-e i članak 14. Dekreta o izvršavanju CIA-e). Vanjski izvršitelj ne smije te informacije upotrebljavati izvan okvira eksternaliziranih zadaća, a naručitelj eksternalizacije mora uvesti posebne sigurnosne zahtjeve (npr. o enkripciji) i educirati vanjskog izvršitelja o načinu sprečavanja gubitka, krađe, otkrivanja, izmjene ili narušavanja pouzdanosti kreditnih informacija.

([130]) Vidjeti i članak 28. stavak 10. točke 1., 2. i 6. Dekreta o izvršavanju CIA-e.

sudskog naloga; 7. tužitelju/službeniku pravosudne policije u izvanrednoj situaciji kad je život pojedinca u opasnosti ili se očekuje da će pojedinac pretrpjeti tjelesnu ozljedu, a nema vremena za izdavanje sudskog naloga ([131]); 8. nadležnim poreznim tijelima radi poštovanja poreznih propisa; ili 9. u skladu s drugim zakonima. U slučaju otkrivanja na temelju jedne od tih osnova, ispitanik se o tome mora unaprijed obavijestiti (članak 32. stavak 7. CIA-e).

(104) CIA-om se posebno uređuje i trajanje obrade osobnih kreditnih informacija na temelju jedne od tih osnova za upotrebu ili prosljeđivanje trećoj strani nakon prestanka komercijalnog odnosa s pojedincem ([132]). Smiju se zadržati jedino informacije koje su bile potrebne za uspostavljanje ili održavanje tog odnosa, što podliježe dodatnim zaštitnim mjerama (informacije se moraju čuvati zasebno od kreditnih informacija koje se odnose na pojedince s kojima je komercijalni odnos još traje, moraju biti zaštićene posebnim sigurnosnim mjerama i dostupne jedino ovlaštenim osobama) ([133]). Svi ostali podaci moraju se izbrisati (članak 17-2. stavak 1. točka 2. Dekreta o izvršavanju CIA-e). Za utvrđivanje toga koji su podaci bili potrebni za komercijalni odnos u obzir se moraju uzeti različiti čimbenici, među ostalim pitanje bi li bilo moguće uspostaviti taj odnos bez tih podataka i odnose li se ti podaci izravno na robu koja se isporučuje ili usluge koje se pružaju pojedincu (članak 17-2. stavak 2. Dekreta o izvršavanju CIA-e).

(105) Čak i ako se osobne kreditne informacije smiju u načelu zadržati i nakon prestanka komercijalnog odnosa, moraju se izbrisati u roku od tri mjeseca nakon ostvarenja daljnje svrhe obrade ([134]) ili, u svakom slučaju, nakon pet godina (članak 20-2. CIA-e). U ograničenom broju okolnosti osobne kreditne informacije smiju se čuvati dulje od pet godina, ponajprije ako je to nužno radi poštovanja pravne obveze; ako je to nužno radi ključnih interesa povezanih sa životom, zdravljem ili imovinom pojedinca; radi arhiviranja pseudonimiziranih informacija (koje su se upotrebljavale u svrhe provođenja znanstvenih istraživanja, prikupljanja statističkih podataka ili arhiviranja u javnom interesu); ili za potrebe osiguranja (osobito za potrebe plaćanja povezanih s osiguranjem ili radi sprečavanja prijevara povezanih s osiguranjem) ([135]). U tim iznimnim slučajevima primjenjuju se posebne zaštitne mjere (kao što su obavješćivanje pojedinca o daljnjoj upotrebi, odvajanje zadržanih informacija od informacija koje se odnose na pojedince s kojima komercijalni odnos još traje i ograničavanje prava na pristup, vidjeti članak 17-2. stavke 1. i 2. Dekreta o izvršavanju CIA-e).

(106) U CIA-i se dodatno utvrđuju načela točnosti i kvalitete podataka tako što se zahtijeva da se osobne kreditne informacije moraju „registrirati i mijenjati" te se njima mora „upravljati" tako da se osigura njihova točnost i ažuriranost (članak 18. stavak 1. CIA-e i članak 15. stavak 3. Dekreta o izvršavanju CIA-e) ([136]). Kad se kreditne informacije prosljeđuju određenim drugim subjektima (kao što su agencije za kreditni rejting), od komercijalnih subjekata posebno se zahtijeva i da provjere njihovu točnost kako bi primatelj registrirao i upravljao samo točnim informacijama (članak 15. stavak 1. Dekreta o izvršavanju CIA-e u vezi s člankom 18. stavkom 1. CIA-e). Općenitije, CIA-om se zahtijeva da se za osobne kreditne informacije vode evidencije o njihovu prikupljanju, upotrebi, prosljeđivanju trećim stranama i uništavanju (članak 20. stavak 2. CIA-e) ([137]).

(107) Nadalje, obrada osobnih kreditnih informacija podliježe posebnim zahtjevima u pogledu sigurnosti podataka. CIA-om se ponajprije zahtijeva uvođenje tehnoloških, fizičkih i organizacijskih mjera radi sprečavanja nezakonitog pristupa računalnim sustavima, izmjene ili uništavanja podataka koji se obrađuju ili bilo kojeg drugog rizika za te podatke (što se ostvaruje, primjerice, kontrolama pristupa, vidjeti članak 19. CIA-e i članak 16. Dekreta o izvršavanju CIA-e). Osim toga, kad se osobne kreditne informacije razmjenjuju s trećom stranom, potrebno je sklopiti sporazum u kojem se utvrđuju posebne sigurnosne mjere (članak 19. stavak 2. CIA-e). Ako dođe do povrede osobnih kreditnih informacija, mjere za svođenje štete na minimum moraju se provesti bez odgode te se moraju obavijestiti predmetni pojedinci (članak 39-4. stavci 1. i 2. CIA-e). Osim toga, o obavijesti poslanoj pojedincima i provedenim mjerama mora se obavijestiti PIPC (članak 39-4. stavak 4. CIA-e).

([131]) U tom se slučaju nalog mora zatražiti bez odgode. Ako se nalog ne izda u roku od 36 sati, primljeni podaci moraju se izbrisati bez odgode (članak 32. stavak 6. točka 6. CIA-e).

([132]) Primjerice, zbog toga što je jedna stranka ostvarila svoje pravo na raskid ugovora itd. nakon ispunjenja ugovornih obveza, vidjeti članak 17-2. stavak 5. Dekreta o izvršavanju CIA-e.

([133]) Članak 20-2. stavak 1. CIA-e i članak 17-2. stavak 1. točka 1. Dekreta o izvršavanju CIA-e.

([134]) Kod tog se roka uzima u obzir to da se brisanje često neće moći izvršiti odmah, već su obično potrebni određeni koraci (npr. izdvajanje podataka koje treba izbrisati od ostalih podataka i provođenje brisanja tako da ono ne utječe na stabilnost informacijskih sustava) za čiju je provedbu potrebno određeno vrijeme.

([135]) Članak 20-2. stavak 2. CIA-e.

([136]) U članku 18. stavku 2. CIA-e i članku 15. stavku 4. Dekreta o izvršavanju CIA-e propisuju se konkretnija pravila u pogledu tog zahtjeva o vođenju evidencije, npr. za evidencije o informacijama koje mogu imati negativne posljedice za pojedinca, kao što su informacije o kašnjenjima u plaćanju i stečaju.

([137]) Kad je riječ o mehanizmima za odgovornost, u CIA-i se zahtijeva da određene organizacije (npr. zadruge i javna trgovačka društva, vidjeti članak 21. stavak 2. Dekreta o izvršavanju CIA-e) imenuju „službenika/upravitelja za kreditne informacije" koji je zadužen za praćenje usklađenosti s CIA-om i koji obavlja zadaće „službenika za zaštitu privatnosti" u skladu s PIPA-om (članak 20. stavci 3. i 4. CIA-e).

(108) CIA-om se uvode i posebne obveze u pogledu transparentnosti pri pribavljanju privole za upotrebu ili prosljeđivanje osobnih kreditnih informacija (članak 32. stavak 4. i članak 34-2. CIA-e te članak 30-3. Dekreta o izvršavanju CIA-e) te, općenitije, prije prosljeđivanja informacija trećoj strani (članak 32. stavak 7. CIA-e) ([138]). Osim toga, pojedinci imaju pravo na zahtjev dobiti informacije o upotrebi i prosljeđivanju njihovih kreditnih informacija trećim stranama za razdoblje od tri godine koje prethodi zahtjevu (uključujući svrhu i datume te upotrebe/tog prosljeđivanja) ([139]).

(109) Na temelju CIA-e pojedinci imaju i pravo na pristup svojim osobnim kreditnim informacijama (članak 38. stavak 1. CIA-e) i na ispravak netočnih podataka (članak 38. stavci 2. i 3. CIA-e) ([140]). Nadalje, osim općeg prava na brisanje na temelju PIPA-e (vidjeti uvodnu izjavu 77.), CIA-om se predviđa posebno pravo na brisanje osobnih kreditnih informacija koje su zadržane nakon isteka razdoblja pohrane navedenog u uvodnoj izjavi 104., tj. pet godina (za osobne kreditne informacije koje su bile potrebne za uspostavljanje ili održavanje komercijalnog odnosa) ili tri mjeseca (za ostale vrste osobnih kreditnih informacija) ([141]). Zahtjev za brisanje može se iznimno odbiti ako je daljnja pohrana potrebna u okolnostima opisanima u uvodnoj izjavi 105. Ako pojedinac zatraži brisanje, ali se primjenjuje jedna od iznimaka, na predmetne kreditne informacije moraju se primijeniti posebne zaštitne mjere (članak 38-3. stavak 3. CIA-e i članak 33-3. Dekreta o izvršavanju CIA-e). Primjerice, informacije se moraju čuvati zasebno od ostalih informacija, smije im pristupati jedino ovlaštena osoba i na njih se moraju primijeniti posebne sigurnosne mjere.

(110) Osim prava navedenih u uvodnoj izjavi 109., CIA-om se pojedincima jamči pravo da od voditelja obrade zatraže da ih prestane kontaktirati u svrhe izravne prodaje (članak 37. stavak 2. CIA-e) i pravo na prenosivost podataka. Kad je riječ o potonjem, CIA-om se pojedincima omogućuje da zatraže prijenos njihovih osobnih kreditnih informacija njima samima ili određenim trećim stranama (kao što su financijske institucije i agencije za kreditni rejting). Osobne kreditne informacije moraju se obrađivati i prosljeđivati trećim stranama u obliku koji omogućuje obradu tih informacija uređajem za obradu informacija (kao što je računalo).

(111) Stoga, u mjeri u kojoj CIA sadržava posebna pravila u odnosu na PIPA-u, Komisija smatra da se i tim pravilima osigurava razina zaštite koja je u načelu istovjetna onoj na temelju Uredbe (EU) 2016/679.

2.4. **Nadzor i izvršavanje**

(112) Kako bi se u praksi osigurala primjerena razina zaštite podataka, trebalo bi uspostaviti neovisno nadzorno tijelo s ovlastima za praćenje i provedbu usklađenosti s pravilima o zaštiti podataka. To bi tijelo pri obavljanju svojih dužnosti i izvršavanju svojih ovlasti trebalo djelovati potpuno neovisno i nepristrano.

2.4.1. *Neovisni nadzor*

(113) U Republici Koreji neovisno tijelo nadležno za praćenje i izvršavanje PIPA-e je PIPC. PIPC se sastoji od predsjednika, potpredsjednika i sedam povjerenika. Predsjednika i potpredsjednika imenuje predsjednik države na preporuku premijera. Dva povjerenika imenuje predsjednik države na preporuku predsjednika PIPC-a, a pet na preporuku Nacionalne skupštine (dva na preporuku političke stranke kojoj pripada predsjednik države, a tri na preporuku ostalih političkih stranaka (članak 7-2. stavak 2. PIPA-e), što pomaže u suzbijanju pristranosti u

([138]) To uključuje opći zahtjev za obavješćivanje (članak 32. stavak 7. CIA-e) i posebnu obvezu o transparentnosti ako se informacije na temelju kojih se može utvrditi kreditna sposobnost pojedinca prosljeđuju određenim subjektima, kao što su agencije za kreditni rejting i agencije za prikupljanje kreditnih informacija (članak 35-3. CIA-e i članak 30-3. Dekreta o izvršavanju CIA-e), ili ako se komercijalni transakcijski odnos odbije ili raskine na temelju osobnih kreditnih informacija dobivenih od treće strane (članak 36. CIA-e i članak 31. Dekreta o izvršavanju CIA-e).

([139]) Članak 35. CIA-e. Određene komercijalne organizacije, npr. zadruge i javna trgovačka društva (članak 21. stavak 2. Dekreta o izvršavanju CIA-e) podliježu dodatnim zahtjevima transparentnosti prema kojima, primjerice, moraju objaviti određene informacije (članak 31. CIA-e) i obavijestiti pojedince o mogućim negativnim posljedicama za njihov kreditni rejting ako obavljaju financijske transakcije povezane s kreditnim rizicima (članak 35-2. CIA-e).

([140]) Kad je riječ o uvjetima i iznimkama od prava na pristup i ispravak, primjenjuju se pravila iz PIPA-e (opisana u uvodnim izjavama 76. i 77.). Osim toga, daljnji modaliteti utvrđeni su u članku 38. stavcima od 4. do 8. CIA-e i članku 33. Dekreta o izvršavanju CIA-e. Konkretno, komercijalni subjekt koji je ispravio ili izbrisao netočne kreditne informacije mora o tome obavijestiti pojedinca. Osim toga, mora se obavijestiti svaka treća strana kojoj su te informacije otkrivene u prethodnih šest mjeseci te se o tome mora obavijestiti predmetni pojedinac. Ako pojedinac nije zadovoljan načinom na koji je zahtjev za ispravak riješen, može podnijeti zahtjev PIPC-u, koji provjerava postupke voditelja obrade i može odrediti korektivne mjere.

([141]) Članak 38-3. CIA-e.

postupku imenovanja) ([142]). Taj je postupak u skladu sa zahtjevima koji se primjenjuju na imenovanje članova tijela za zaštitu podataka u Uniji (članak 53. stavak 1. Uredbe (EU) 2016/679). Nadalje, svi povjerenici moraju se suzdržavati od svih poslovnih djelatnosti koje donose zaradu, političkih aktivnosti i od obnašanja dužnosti u javnoj upravi ili Nacionalnoj skupštini (članak 7-6. i članak 7-7. stavak 1. točka 3. PIPA-e) ([143]). Na sve povjerenike primjenjuju se posebna pravila prema kojima ne smiju sudjelovati u raspravama u slučaju mogućeg sukoba interesa (članak 7-11. PIPA-e). PIPC-u u radu pomaže tajništvo (članak 7-13.) i on može osnivati potpovjerenstva (koja se sastoje od triju povjerenika) za rješavanje manjih povreda i učestalih pitanja (članak 7-12. PIPA-e).

(114) Svaki član PIPC-a imenuje se na mandat od tri godine i može se još jednom ponovno imenovati (članak 7-4. stavak 1. PIPA-e). Povjerenici se mogu razriješiti dužnosti samo u određenim okolnostima, to jest ako više ne mogu obavljati svoje dužnosti zbog dugotrajnog mentalnog ili tjelesnog invaliditeta, ako su prekršili zakon ili ako je ispunjena jedna od osnova za zabranu obavljanja dužnosti ([144]) (članak 7-5. PIPA-e). Time im se daje institucionalna zaštita pri izvršavanju njihovih funkcija.

(115) Općenitije, člankom 7. stavkom 1. PIPA-e izričito se jamči neovisnost PIPC-a, a člankom 7-5. stavkom 2. PIPA-e od povjerenika se zahtijeva da svoje dužnosti obavljaju neovisno, u skladu sa zakonom i svojom savješću ([145]). Opisanim institucionalnim i postupovnim zaštitnim mjerama, među ostalim i s obzirom na imenovanje i razrješenje članova PIPC-a, osigurava se da PIPC djeluje potpuno neovisno i bez vanjskog utjecaja ili uputa. Nadalje, PIPC kao središnja upravna agencija svake godine predlaže vlastiti proračun (koji preispituje Ministarstvo financija kao dio ukupnog nacionalnog proračuna prije nego što ga prihvati Nacionalna skupština) te je zadužen za upravljanje vlastitim osobljem. PIPC trenutačno ima proračun od oko 35 milijuna EUR i zapošljava 154 člana osoblja (uključujući 40 zaposlenika specijaliziranih za informacijsku i komunikacijsku tehnologiju, 32 zaposlenika zadužena za istrage i 40 pravnih stručnjaka).

(116) Zadaće i ovlasti PIPC-a uglavnom su predviđene u člancima 7-8. i 7-9. te u člancima od 61. do 66. PIPA-e ([146]). Zadaće PIPC-a u prvom redu uključuju davanje savjeta o zakonima i drugim propisima koji se odnose na zaštitu podataka, izradu politika i smjernica o zaštiti podataka, provođenje istraga o povredama prava pojedinaca, rješavanje pritužbi i posredovanje u sporovima, provedbu usklađenosti s PIPA-om, osiguravanje edukacije i promicanja u području zaštite podataka te razmjenu i suradnju s tijelima za zaštitu podataka iz trećih zemalja ([147]).

(117) Na temelju članka 68. PIPA-e u vezi s člankom 62. Dekreta o izvršavanju PIPA-e određene zadaće PIPC-a delegirane su Korejskoj agenciji za internet i sigurnost, a to su: 1. edukacija i odnosi s javnošću, 2. osposobljavanje specijalista i izrada kriterija za procjene učinka na privatnost, 3. rješavanje zahtjeva za imenovanje takozvane institucije za procjenu učinka na privatnost, 4. rješavanje zahtjeva za neizravan pristup osobnim podacima koje drže tijela javne vlasti (članak 35. stavak 2. PIPA-e) i 5. zadaća traženja materijala i provođenja inspekcijskih pregleda u pogledu pritužbi primljenih preko takozvanog Pozivnog centra za zaštitu privatnosti. U

([142]) Kao povjerenici PIPC-a mogu se imenovati samo osobe koje ispunjavaju sljedeće kriterije: viši javni službenici zaduženi za pitanja povezana s osobnim informacijama; bivši suci, javni tužitelji ili odvjetnici s barem deset godina radnog iskustva u tom svojstvu; bivši rukovoditelji s iskustvom u području zaštite podataka koji su radili kao rukovoditelji u javnoj instituciji ili organizaciji više od tri godine ili koje je ta institucija ili organizacija preporučila; i bivši izvanredni profesori sa stručnim znanjem u području zaštite podataka koji su barem pet godina radili kao profesori u akademskoj instituciji (članak 7-2. PIPA-e).

([143]) Vidjeti i članak 4-2. Dekreta o izvršavanju PIPA-e.

([144]) Vidjeti članak 7-7. PIPA-e, prema kojem osobe koje nemaju korejsko državljanstvo i članovi političkih stranaka ne mogu postati članovima PIPC-a. Isto se odnosi i na osobe kojima su izrečene određene vrste kaznenih sankcija, koje su u prethodnih pet godina razriješene dužnosti u okviru stegovnog postupka itd. (članak 7-7. PIPA-e u vezi s člankom 33. Zakona o javnim dužnosnicima).

([145]) Iako se u članku 7. stavku 2. PIPA-e upućuje na opću ovlast premijera na temelju članka 18. Zakona o organizaciji vlade da suspendira ili poništi – uz odobrenje predsjednika države – bilo koju nezakonitu ili nepravednu odluku središnje upravne agencije, takva ovlast ne postoji u odnosu na istražne i provedbene ovlasti PIPC-a (vidjeti članak 7. stavak 2. točke 1. i 2. PIPA-e). Prema objašnjenjima dobivenima od korejske vlade, svrha je članka 18. Zakona o organizaciji vlade premijeru omogućiti da djeluje u izvanrednim okolnostima, npr. kako bi posredovao u slučaju neslaganja između vladinih agencija. Međutim, premijer nikad nije iskoristio tu ovlast otkad je ta odredba donesena 1963.

([146]) Kad je to potrebno za obavljanje zadaća u skladu s člankom 7-9. stavkom 1. PIPA-e, PIPC može zatražiti mišljenja relevantnih javnih dužnosnika, stručnjaka u području zaštite podataka, organizacija civilnog društva i relevantnih poslovnih subjekata. Osim toga, PIPC može zatražiti relevantne materijale, izdavati preporuke za poboljšanje i inspekcijskim pregledima provjeravati provode li se te preporuke (članak 7-9. stavci od 2. do 5. PIPA-e).

([147]) Vidjeti i članak 9. PIPA-e (trogodišnji glavni plan za zaštitu osobnih informacija), članak 12. PIPA-e (standardne smjernice za zaštitu osobnih informacija) i članak 13. PIPA-e (politike za promicanje i podupiranje samoreguliranja).

kontekstu rješavanja pritužbi primljenih preko Pozivnog centra za zaštitu privatnosti Korejska agencija za internet i sigurnost, ako utvrdi da je došlo do kršenja zakona, prosljeđuje taj predmet PIPC-u ili tužiteljstvu. Mogućnost podnošenja pritužbe Pozivnom centru za zaštitu privatnosti ne sprečava pojedince da izravno podnesu pritužbu PIPC-u ili da mu se obrate ako smatraju da Korejska agencija za internet i sigurnost nije na zadovoljavajući način riješila njihovu pritužbu.

2.4.2. *Izvršavanje, uključujući sankcije*

(118) Kako bi se osigurala usklađenost s PIPA-om, zakonodavac je PIPC-u dodijelio i istražne i provedbene ovlasti, u rasponu od izdavanja preporuka do izricanja upravnih novčanih kazni. Te su ovlasti dodatno dopunjene režimom kaznenih sankcija.

(119) Kad je riječ o istražnim ovlastima, ako se sumnja na kršenje PIPA-e ili je to kršenje prijavljeno, ili ako je to potrebno radi zaštite prava ispitanika od kršenja tih prava, PIPC može provoditi inspekcijske preglede na licu mjesta i zatražiti sve relevantne materijale (kao što su predmeti i dokumenti) od voditelja obrade osobnih podataka (članak 63. PIPA-e u vezi s člankom 60. Dekreta o izvršavanju PIPA-e) ([148]).

(120) Kad je riječ o izvršavanju, PIPC na temelju članka 61. stavka 2. PIPA-e može davati savjete voditeljima obrade podataka o tome kako poboljšati razinu zaštite osobnih podataka za određene aktivnosti obrade. Voditelji obrade podataka moraju u dobroj vjeri nastojati provesti te savjete i od njih se traži da o ishodu obavijeste PIPC. Nadalje, ako postoje opravdani razlozi za vjerovati da je došlo do kršenja PIPA-e i da bi, ako se ne poduzmu mjere, vjerojatno nastala šteta koju je teško popraviti, PIPC može uvesti korektivne mjere (članak 64. stavak 1. PIPA-e) ([149]). U odjeljku 5. Obavijesti 2021-5 (Prilog I.) pojašnjava se, s obvezujućim učinkom, da su ti uvjeti ispunjeni u pogledu kršenja bilo koje odredbe iz PIPA-e kojom se štite prava na privatnost pojedinaca u odnosu na osobne informacije ([150]). Mjere koje je PIPC ovlašten poduzimati uključuju naređivanje prestanka ponašanja koje uzrokuje kršenje, privremenu suspenziju obrade podataka ili bilo koje druge potrebne mjere. Nepoštovanje korektivne mjere može dovesti do sankcije u obliku novčane kazne u najvišem iznosu od 50 milijuna vona (članak 75. stavak 2. točka 13. PIPA-e).

(121) Kad je riječ o određenim tijelima javne vlasti (kao što su Nacionalna skupština, središnje upravne agencije, tijela lokalne vlasti i sudovi), u članku 64. stavku 4. PIPA-e predviđa se da PIPC može „preporučiti" bilo koju od korektivnih mjera navedenih u uvodnoj izjavi 120. i da ta tijela moraju postupiti u skladu s tom preporukom, osim u izvanrednim okolnostima. Prema odjeljku 5. Obavijesti 2021-5 to se odnosi na izvanredne činjenične ili pravne okolnosti za koje PIPC nije znao kad je dao svoju preporuku. Predmetno javno tijelo može se pozvati na takve izvanredne okolnosti samo ako jasno pokaže da nije došlo ni do kakve povrede, a PIPC utvrdi da zaista nije došlo do povrede. U suprotnome, javno tijelo mora poštovati preporuku PIPC-a i „poduzeti korektivnu mjeru, među ostalim odmah prestati s određenom radnjom, i nadoknaditi štetu u iznimnom slučaju u kojem je ipak počinjena nezakonita radnja".

(122) PIPC može i od drugih upravnih agencija s posebnom nadležnošću u skladu sa sektorskim zakonodavstvom (npr. zdravstvo, obrazovanje) zatražiti da same ili zajedno s PIPC-om provedu istragu o povredama privatnosti (na koje se sumnja), koje su počinili voditelji obrade koji djeluju u tim sektorima u njihovoj nadležnosti te da uvedu korektivne mjere (članak 63. stavci od 4. do 5. PIPA-a). U tom slučaju PIPC utvrđuje osnove, predmet i opseg istrage ([151]). Relevantna upravna agencija mora PIPC-u dostaviti plan inspekcijskog pregleda i obavijestiti ga o rezultatima inspekcijskog pregleda. PIPC može preporučiti poduzimanje konkretne korektivne mjere koju relevantna agencija mora nastojati provesti. U svakom slučaju, tim se zahtjevom ne ograničava nadležnost PIPC-a za provođenje vlastite istrage ili izricanje sankcija.

([148]) PIPC usto može ulaziti u poslovne prostore voditelja obrade kako bi pregledao stanje poslovnih operacija, evidencije, dokumenata itd. (članak 63. stavak 2. PIPA-e). Vidjeti i članak 45-3. CIA-e i članak 36-4. Dekreta o izvršavanju CIA-e s obzirom na ovlasti PIPC-a na temelju tog zakona.

([149]) Vidjeti i članak 45-4. CIA-e s obzirom na ovlasti PIPC-a na temelju CIA-e.

([150]) U odjeljku 5. Obavijesti navodi se da „opravdana osnova na temelju koje se smatra da je došlo do povrede u vezi s osobnim informacijama, a nepoduzimanje mjera vjerojatno će uzrokovati štetu koju je teško popraviti u smislu članka 64. stavaka 1. i 2. PIPA-e, odnosi se na povredu bilo kojeg od načela, prava i dužnosti uključenih u zakon radi zaštite prava pojedinaca u vezi s osobnim informacijama". Isto vrijedi i za ovlasti PIPC-a na temelju članka 45-4. CIA-e.

([151]) Članak 60. Dekreta o izvršavanju PIPA-a.

(123) Osim svojih korektivnih ovlasti, PIPC može izricati upravne novčane kazne u iznosu od 10 do 50 milijuna vona za povrede raznih zahtjeva iz PIPA-e (članak 75. PIPA-e) ([152]). Među ostalim, to uključuje nepoštovanje zahtjeva o zakonitosti obrade, nepoduzimanje potrebnih sigurnosnih mjera, neobavješćivanje ispitanika u slučaju povrede podataka, nepoštovanje zahtjeva o podobradi, neutvrđivanje i neobjavljivanje politike zaštite privatnosti, neimenovanje službenika za zaštitu privatnosti ili nepostupanje na temelju zahtjeva ispitanika koji ostvaruje svoja prava pojedinca te određene postupovne povrede (nesuradnja tijekom istrage). U slučaju da isti voditelj obrade prekrši više odredaba PIPA-e, za svako se kršenje može izreći novčana kazna, a pri određivanju visine novčane kazne uzet će se u obzir broj pogođenih pojedinaca.

(124) Nadalje, ako postoje opravdani razlozi za sumnju na povredu PIPA-e ili bilo kojih drugih „zakona koji se odnose na zaštitu podataka", PIPC može podnijeti kaznenu prijavu nadležnoj istražnoj agenciji (kao što je javno tužiteljstvo, vidjeti članak 65. stavak 1. PIPA-e). Osim toga, PIPC može savjetovati voditelju obrade da poduzme stegovne mjere protiv odgovorne osobe (uključujući odgovornog rukovoditelja, vidjeti članak 65. stavak 2. PIPA-e). Nakon primanja tog savjeta voditelj obrade mora postupiti u skladu s njim ([153]) i u pisanom obliku obavijestiti PIPC o rezultatima (članak 65. PIPA-e u vezi s člankom 58. Dekreta o izvršavanju PIPA-e).

(125) Kad je riječ o savjetu u skladu s člankom 61., korektivnim mjerama u skladu s člankom 64., optužnom prijedlogu ili savjetu o stegovnim mjerama u skladu s člankom 65. i izricanju upravnih novčanih kazni u skladu s člankom 75. PIPA-e, PIPC može objaviti činjenice – tj. povredu, subjekta koji je prekršio zakon i uvedene mjere – tako da ih objavi na svojim internetskim stranicama ili u glavnim nacionalnim dnevnim novinama (članak 66. PIPA-e u vezi s člankom 61. stavkom 1. Dekreta o izvršavanju PIPA-e) ([154]).

(126) Na kraju, ispunjavanje zahtjeva o zaštiti podataka iz PIPA-e (te drugih „zakona koji se odnose na zaštitu podataka") podupire se režimom kaznenih sankcija. S obzirom na to, članci od 70. do 73. PIPA-e sadržavaju odredbe o sankcijama koje mogu dovesti do izricanja novčane kazne (u iznosu od 20 do 100 milijuna vona) ili kazne zatvora (s najvišom kaznom koja se kreće u rasponu od dvije do deset godina). Relevantne povrede uključuju, među ostalima, upotrebu osobnih podataka ili prosljeđivanje tih podataka trećoj strani bez potrebne privole, obradu osjetljivih informacija suprotno zabrani iz članka 23. stavka 1. PIPA-e, nepoštovanje primjenjivih zahtjeva o sigurnosti s posljedicom gubitka, krađe, otkrivanja, krivotvorenja, izmjene ili oštećivanja osobnih podataka, nepoduzimanje potrebnih mjera za ispravak ili brisanje osobnih podataka ili suspendiranje obrade tih podataka ili nezakonit prijenos osobnih podataka u treću zemlju ([155]). U skladu s člankom 74. PIPA-e, u svakom od tih slučajeva odgovoran je zaposlenik, agent ili predstavnik voditelja obrade te sam voditelj obrade ([156]).

(127) Osim kaznenih sankcija propisanih PIPA-om, pogrešna upotreba osobnih podataka može činiti i kazneno djelo na temelju Kaznenog zakona. To se osobito odnosi na povredu tajnosti pisama, dokumenata ili elektroničkih evidencija (članak 316.), otkrivanje informacija koje podliježu obvezi čuvanja profesionalne tajne (članak 317.), prijevaru upotrebom računala (članak 347-2.) te pronevjeru i zloupotrebu povjerenja (članak 355.).

(128) Stoga se u korejskom sustavu kombiniraju različite vrste sankcija, od korektivnih mjera i upravnih novčanih kazni do kaznenih sankcija, koje vjerojatno imaju naročito velik učinak odvraćanja na voditelje obrade i osobe koje postupaju s podacima. PIPC je počeo koristiti svoje ovlasti odmah nakon što je osnovan 2020. Iz godišnjeg

([152]) Nadalje, ako sustavi za obradu i zaštitu osobnih informacija kojima upravlja voditelj obrade imaju certifikat da su u skladu s PIPA-om, ali kriteriji certificiranja u skladu s člankom 34-2. stavkom 1. Dekreta o izvršavanju PIPA-e zapravo nisu ispunjeni, ili u slučaju ozbiljne povrede bilo kojeg „zakona koji se odnosi na zaštitu [osobnih] informacija", PIPC može oduzeti taj certifikat (članak 32-2. stavci 3. i 5. PIPA-e). PIPC je dužan obavijestiti voditelja obrade o tom oduzimanju certifikata i to proglasiti ili objaviti na svojim internetskim stranicama ili u službenom listu (članak 34-4. Dekreta o izvršavanju PIPA-e). Upravne novčane kazne (članak 52. CIA-e) i kaznene sankcije (članak 50. CIA-e) predviđene su i za povrede CIA-e.

([153]) U skladu s člankom 58. stavkom 2. Dekreta o izvršavanju PIPA-e, ako zbog posebnih okolnosti postupanje u skladu s tim savjetom postane „neizvedivo", voditelj obrade mora PIPC-u dostaviti obrazloženo opravdanje.

([154]) Pri odlučivanju o objavi PIPC uzima u obzir sadržaj i težinu povrede, njezino trajanje i učestalost te njezine posljedice (razmjere štete). Predmetni se subjekti o tome obavještava i omogućuje mu se da iznese svoju obranu. Vidjeti članak 61. stavke 2. i 3. Dekreta o izvršavanju PIPA-e.

([155]) Vidjeti članak 71. točku 2. u vezi s člankom 18. stavkom 1. PIPA-e (nepoštovanje uvjeta iz članka 17. stavka 3. PIPA-e, na koje se upućuje u članku 18. stavku 1). Vidjeti i članak 75. stavak 2. točku 1. u vezi s člankom 17. stavkom 2. PIPA-e (nedavanje potrebnih informacija predmetnom pojedincu u skladu s člankom 17. stavkom 2. PIPA-e, na koji se upućuje u članku 17. stavku 3.).

([156]) Nadalje, člankom 74-2. PIPA-e dopušta se zapljena sveg novca, robe ili drugih oblika zarade koji su stečeni kao posljedica povrede ili, ako zapljena nije moguća, „uzimanje" sve nezakonito ostvarene koristi.

izvješća PIPC-a za 2021. proizlazi da je PIPC već izdao niz preporuka, upravnih novčanih kazni i korektivnih naloga javnom sektoru (oko 34 javna tijela) i privatnim subjektima (oko 140 poduzeća) ([157]). Među najvažnijim slučajevima, u prosincu 2020. jednom poduzeću je izrečena novčana kazna od 6,7 milijardi vona zbog povrede različitih odredaba PIPA-e (uključujući zahtjeve o sigurnosti, zahtjeve o privoli za prosljeđivanje trećim stranama i zahtjeve transparentnosti) ([158]), a u travnju 2021. izrečena je novčana kazna od 103,3 milijuna vona jednom poduzeću koje se bavi tehnologijom umjetne inteligencije (zbog povrede, među ostalim odredbama, pravila o zakonitosti obrade, posebice u vezi s privolom, i pravila o obradi pseudonimiziranih informacija) ([159]). U kolovozu 2021. PIPC je dovršio još jednu istragu povezanu s djelatnostima triju poduzeća, čiji je rezultat bio uvođenje korektivnih mjera i izricanje novčanih kazni u iznosu do 6,47 milijardi vona (među ostalim zbog neobavješćivanja pojedinaca o otkrivanju osobnih podataka trećim stranama, uključujući prijenose trećim zemljama) ([160]). Osim toga, već i prije nedavne reforme Južna Koreja imala je dobre rezultate u izvršavanju, pri čemu su nadležna tijela koristila sve raspoložive mjere izvršenja, uključujući upravne novčane kazne, korektivne mjere te „objavljivanje imena i javno sramoćenje”, koje su primijenjene na mnoge voditelje obrade, uključujući pružatelje komunikacijskih usluga (Korejsko povjerenstvo za komunikacije) te komercijalne subjekte, financijske institucije, tijela javne vlasti, sveučilišta i bolnice (Ministarstvo unutarnjih poslova i sigurnosti) ([161]). Komisija na temelju toga zaključuje da korejski sustav u praksi osigurava djelotvorno provođenje pravila o zaštiti podataka, čime se jamči razina zaštite koja je u načelu istovjetna onoj na temelju Uredbe (EU) 2016/679.

2.5. **Pravna zaštita**

(129) Kako bi se osigurala primjerena zaštita, a naročito ostvarivanje prava pojedinca, ispitaniku bi trebalo pružiti djelotvornu upravnu i sudsku zaštitu, uključujući naknadu štete.

(130) Korejski sustav pruža pojedincima razne mehanizme za djelotvorno ostvarivanje njihovih prava i dobivanje (sudske) pravne zaštite.

(131) Kao prvi korak, pojedinci koji smatraju da su njihova prava na zaštitu podataka ili interesi povezani sa zaštitom podataka prekršeni mogu se obratiti odgovarajućem voditelju obrade. U skladu s člankom 30. stavkom 1. točkom 5. PIPA-e politika voditelja obrade o zaštiti privatnosti mora, među ostalim, sadržavati informacije o pravima ispitanika i načinu njihova ostvarivanja. Nadalje, u njoj se moraju navesti kontaktne informacije – kao što su ime i telefonski broj službenika za zaštitu privatnosti ili odjela odgovornog za zaštitu podataka – kako bi se omogućilo podnošenje pritužbi. Unutar organizacije voditelja obrade službenik za zaštitu privatnosti zadužen je za rješavanje pritužbi, donošenje korektivnih mjera u slučaju povrede privatnosti i naknadu radi ispravljanja štete (članak 31. stavak 2. točka 3. i članak 31. stavak 4. PIPA-e). Potonje je relevantno, primjerice, u slučaju povrede podataka jer voditelj obrade mora obavijestiti ispitanika o kontaktnim točkama za prijavljivanje, među ostalim, bilo kakve štete (članak 34. stavak 1. točka 5. PIPA-e).

(132) Osim toga, u PIPA-i se pojedincima nudi nekoliko mogućnosti za pravnu zaštitu protiv voditelja obrade. Prvo, svaki pojedinac koji smatra da mu je voditelj obrade povrijedio prava na zaštitu podataka ili interese povezane sa zaštitom podataka može prijaviti takvu povredu izravno PIPC-u i/ili jednoj od specijaliziranih institucija koje je PIPC imenovao za primanje i rješavanje pritužbi; to uključuje Korejsku agenciju za internet i sigurnost, koja u tu svrhu vodi pozivni centar za osobne informacije (takozvani „Pozivni centar za zaštitu privatnosti”) (članak 62. stavci 1. i 2. PIPA-e u vezi s člankom 59. Dekreta o izvršavanju PIPA-e). Pozivni centar za zaštitu privatnosti

([157]) Vidjeti godišnje izvješće PIPC-a za 2021., str. 50.–55. (dostupno samo na korejskom jeziku) na adresi https://www.pipc.go.kr/np/cop/bbs/selectBoardArticle.do?bbsId=BS074&mCode=C020010000&nttId=7511#LINK

([158]) Vidjeti na adresi (dostupno samo na korejskom jeziku) https://www.pipc.go.kr/np/cop/bbs/selectBoardArticle.do?bbsId=BS074&mCode=C020010000&nttId=6954#LINK

([159]) Vidjeti na adresi (dostupno samo na korejskom jeziku) https://www.pipc.go.kr/np/cop/bbs/selectBoardArticle.do?bbsId=BS074&mCode=C020010000&nttId=7298&fbclid=IwAR3SKcMQi6G5pR9k4I7j6GNXtc8aBVDOwcURevvvzQtYI7AS40UKYXoOXo8

([160]) Vidjeti na adresi (dostupno samo na korejskom jeziku): https://www.pipc.go.kr/np/cop/bbs/selectBoardArticle.do?bbsId=BS074&mCode=C020010000&nttId=7497#LINK

([161]) Vidjeti npr. godišnje izvješće za 2020. na adresi (dostupno samo na korejskom jeziku) https://www.pipc.go.kr/np/cop/bbs/selectBoardList.do?bbsId=BS079&mCode=D070020000 i primjere navedene na engleskom jeziku na adresi https://www.privacy.go.kr/eng/enforcement_02.do.

istražuje i utvrđuje povrede, pruža savjetovanje u vezi s obradom osobnih podataka (članak 62. stavak 3. PIPA-e) i može prijaviti povrede PIPC-u (ali ne može sam poduzeti mjere izvršenja). Pozivni centar za zaštitu privatnosti prima brojne pritužbe/zahtjeve (npr. 177 457 u 2020., 159 255 u 2019. i 164 497 u 2018.) ([162]). Prema informacijama dobivenima od PIPC-a, sam je PIPC od kolovoza 2020. do kolovoza 2021. primio oko 1 000 pritužbi. PIPC može u odgovoru na pritužbu dati savjet za poboljšanja, izricanje korektivnih mjera, podnošenje „optužnog prijedloga" nadležnoj istražnoj agenciji (uključujući javno tužiteljstvo) ili izdavanje prijedloga o stegovnim mjerama (vidjeti članke 61., 64. i 65. PIPA-e). Odluke PIPC-a (kao što su odbijanje rješavanja pritužbe ili odbijanje zbog neosnovanosti pritužbe) mogu se osporavati na temelju Zakona o upravnim sporovima ([163]).

(133) Drugo, u skladu s člancima od 40. do 50. PIPA-e u vezi s člancima od 48-14. do 57. Dekreta o izvršavanju PIPA-e, ispitanici mogu podnijeti zahtjeve takozvanom „Odboru za posredovanje u sporovima", koji se sastoji od predstavnika koje je imenovao predsjednik PIPC-a iz redova članova Službe viših rukovoditelja PIPC-a i pojedinaca imenovanih na temelju njihova iskustva u području zaštite podataka koji pripadaju određenim prihvatljivim skupinama (vidjeti članak 40. stavke 2., 3. i 7. PIPA-e i članak 48-14. Dekreta o izvršavanju PIPA-e) ([164]). Mogućnost posredovanja pred Odborom za posredovanje u sporovima pruža alternativni način za dobivanje pravne zaštite, ali ne ograničava pravo pojedinca da se umjesto toga obrati PIPC-u ili sudovima. Kako bi ispitao predmet, Odbor može zatražiti od stranaka u sporu da dostave potrebne materijale i/ili pozovu relevantne svjedoke da dođu svjedočiti pred Odborom (članak 45. PIPA-e). Nakon što se pitanje razjasni, Odbor sastavlja nacrt pravorijeka o posredovanju ([165]), s kojim se mora složiti većina članova Odbora. Nacrt pravorijeka o posredovanju može uključivati suspendiranje povrede, potrebne pravne lijekove (uključujući povrat u prijašnje stanje ili naknadu štete) te sve mjere koje su potrebne za sprečavanje ponavljanja istih ili sličnih povreda (članak 47. stavak 1. PIPA-e). Ako se obje stranke slože s pravorijekom o posredovanju, on će imati isti učinak kao i sudska nagodba (članak 47. stavak 5. PIPA-e). Nijedna od stranaka ne sprečava se u pokretanju sudske tužbe dok je posredovanje u tijeku, a u tom će se slučaju posredovanje obustaviti (vidjeti članak 48. stavak 2. PIPA-e) ([166]). Godišnji brojčani podaci koje izdaje PIPC pokazuju da pojedinci redovito koriste postupak pred Odborom za posredovanje u sporovima, što često ima uspješan ishod. Na primjer, Odbor je 2020. obradio 126 predmeta, od kojih je 89 riješeno pred Odborom (u 77 predmeta stranke su postigle dogovor prije završetka posredovanja, a u 12 predmeta stranke su prihvatile prijedlog za posredovanje), te je stopa posredovanja bila 70,6 % ([167]). Nadalje, Odbor je 2019. obradio 139 predmeta, od kojih su 92 riješena, te je stopa mirenja bila 62,2 %.

(134) Nadalje, ako štetu pretrpi najmanje 50 pojedinaca ili ako su njihova prava na zaštitu podataka povrijeđena na isti ili sličan način kao posljedica istog incidenta/iste vrste incidenta ([168]), ispitanik ili organizacija za zaštitu podataka mogu u ime takve skupine pojedinaca podnijeti zahtjev za posredovanje u kolektivnom sporu; drugi ispitanici mogu podnijeti zahtjev da se priključe tom posredovanju, koje će Odbor za posredovanje u sporovima javno najaviti (članak 49. stavci od 1. do 3. PIPA-e u vezi s člancima od 52. do 54. Dekreta o izvršavanju PIPA-e) ([169]). Odbor za posredovanje u sporovima može kao reprezentativnu stranku odabrati najmanje jednu osobu koja

([162]) Vidjeti godišnje izvješće PIPC-a za 2021., str. 174. Te su se pritužbe 2020. odnosile, primjerice, na prikupljanje podataka bez privole, nepoštovanje obveza transparentnosti, povrede PIPA-e od strane izvršitelja obrade, nedovoljne sigurnosne mjere, neodgovaranje na zahtjeve ispitanika i općenita pitanja.

([163]) Konkretno, pojedinci mogu podnijeti žalbu na izvršavanje ili odbijanje izvršavanja javne ovlasti od strane upravne agencije (članak 2. stavak 1. točka 1. i članak 3. točka 1. Zakona o upravnim sporovima). Detaljnije informacije o postupovnim aspektima, uključujući zahtjeve o dopuštenosti, navode se u uvodnoj izjavi 181.

([164]) Svi članovi imaju fiksni mandat i mogu se razriješiti dužnosti samo zbog opravdanog razloga (vidjeti članak 40. stavak 5. i članak 41. PIPA-e). Nadalje, članak 42. PIPA-e sadržava zaštitne mjere za sprečavanje sukoba interesa.

([165]) Vidjeti članak 44. PIPA-e. Osim toga, Odbor može predložiti nacrt nagodbe i preporučiti nagodbu bez posredovanja (vidjeti članak 46. PIPA-e).

([166]) Nadalje, Odbor može odbiti posredovanje ako smatra da ne bi bilo primjereno posredovati u sporu s obzirom na njegovu prirodu ili zbog toga što je zahtjev za posredovanje podnesen u nepoštenu svrhu (članak 48. PIPA-e).

([167]) Vidjeti godišnje izvješće PIPC-a za 2021., str. 179.–180. Ti su se predmeti, među ostalim, odnosili na povrede obveze dobivanja privole za prikupljanje podataka, načela ograničavanja svrhe i prava ispitanika.

([168]) Vidjeti članak 49. stavak 1. PIPA-e, prema kojem ispitanici moraju pretrpjeti štetu ili povredu svojih prava „na jednak ili sličan način", i članak 52. točku 2. Dekreta o izvršavanju PIPA-e u kojoj se propisuje zahtjev da „[g]lavna pitanja incidenta moraju činjenično ili pravno biti ista".

([169]) Štoviše, koristi od pravorijeka o posredovanju u kolektivnom sporu koji je prihvatio voditelj obrade mogu imati čak i osobe koje nisu stranke tako što Odbor za posredovanje u sporovima može savjetovati voditelju obrade da izradi i dostavi plan naknade štete koji obuhvaća (i) njih (članak 49. stavak 5. PIPA-e).

najprikladnije predstavlja zajednički interes (članak 49. stavak 4. PIPA-e). Ako voditelj obrade odbije posredovanje u kolektivnom sporu ili ne prihvati pravorijek o posredovanju, određene organizacije ([170]) mogu podnijeti zajedničku tužbu radi rješavanja problema povrede (članci od 51. do 57. PIPA-e).

(135) Treće, u slučaju povrede privatnosti kojom je prouzročena „šteta" pojedincu, ispitanik ima pravo na prikladnu pravnu zaštitu u okviru „brzog i poštenog postupka" (članak 4. točka 5. u vezi s člankom 39. PIPA-e) ([171]). Voditelj obrade može se osloboditi optužbi tako da dokaže da ne postoji krivnja („protupravna namjera" ili nehaj). Ako ispitanik pretrpi štetu kao posljedicu gubitka, krađe, otkrivanja, krivotvorenja, izmjene ili oštećenja njegovih osobnih podataka, sud može dodijeliti iznos naknade koji je do tri puta veći od stvarne štete, uzimajući u obzir brojne čimbenike (članak 39. stavci 3. i 4. PIPA-e). Alternativno, ispitanik može tražiti „razuman iznos" naknade koji ne premašuje iznos od 3 milijuna vona (članak 39-2. stavci 1. i 2. PIPA-e). Nadalje, u skladu s Građanskim zakonom, naknada štete može se tražiti od svake osobe „koja prouzroči gubitke ili nanese štetu drugoj osobi nezakonitom radnjom, iz namjere ili nehaja" ([172]) ili od osobe „koja je nanijela štetu osobi, povrijedila slobodu ili ugled druge osobe ili uzrokovala bilo kakvu duševnu patnju drugoj osobi" ([173]). Takvu deliktnu odgovornost za štetu koja proizlazi iz povrede pravila o zaštiti podataka potvrdio je Vrhovni sud ([174]). Ako je šteta prouzročena nezakonitim postupanjem javnih tijela, zahtjev za naknadu štete može se usto podnijeti na temelju Zakona o naknadi štete od države ([175]). Zahtjev na temelju Zakona o naknadi štete od države može se podnijeti specijaliziranom „Vijeću za naknadu" ili izravno korejskim sudovima ([176]). Odgovornost države za štetu obuhvaća i nematerijalnu štetu (kao što je duševna patnja) ([177]). Ako je žrtva strani državljanin, Zakon o naknadi štete od države primjenjuje se pod uvjetom da zemlja podrijetla tog državljanina jednako tako osigurava naknadu štete od države za korejske državljane ([178]).

(136) Četvrto, Vrhovni sud potvrdio je da pojedinci imaju pravo tražiti izdavanje naloga o privremenom prekidu povreda njihovih prava koja imaju na temelju Ustava, uključujući pravo na zaštitu osobnih podataka ([179]). Sudovi u tom kontekstu mogu, primjerice, narediti voditeljima obrade da suspendiraju ili prestanu provoditi bilo koju nezakonitu aktivnost. Osim toga, prava na zaštitu podataka, uključujući prava zaštićena PIPA-om, mogu se prisilno izvršavati građanskopravnim tužbama. Tu horizontalnu primjenu ustavnopravne zaštite privatnosti na odnose između privatnih stranaka potvrdio je Vrhovni sud ([180]).

([170]) To jest, skupine potrošača ili neprofitne nevladine organizacije određene veličine u smislu broja članova koje kao svoj cilj djelovanja navode zaštitu podataka (iako u potonjem slučaju postoji dodatni zahtjev prema kojem zahtjev za pokretanje zajedničke tužbe mora podnijeti barem 100 ispitanika koji su doživjeli istu (vrstu) povrede). Vidjeti članak 51. PIPA-e.

([171]) U člancima od 43. do 43-3. CIA-e isto se tako propisuje odgovornost za naknadu štete koja proizlazi iz povreda tog zakona.

([172]) Članak 750. Građanskog zakona.

([173]) Članak 751. stavak 1. Građanskog zakona.

([174]) Vidjeti, primjerice, Odluku Vrhovnog suda 2015Da251539, 251546, 251553, 251560, 251577 od 30. svibnja 2018. Osim toga, Vrhovni sud potvrdio je da povrede podataka mogu dovesti do dodjele naknade štete na temelju Građanskog zakona, vidjeti Odluku Vrhovnog suda 2011Da59834, 59858, 59841 od 26. prosinca 2012. (sažetak na engleskom jeziku dostupan je na http://library.scourt.go.kr/SCLIB_data/decision/9-69%202012.12.26.2011Da59834.htm). U tom je predmetu Vrhovni sud pojasnio da je, kako bi se ocijenilo je li pojedinac pretrpio duševnu bol za koju se može tražiti naknada štete, u obzir potrebno uzeti nekoliko čimbenika, kao što su vrsta i obilježja neovlašteno odanih informacija, mogućnost utvrđivanja identiteta pojedinca koja je posljedica povrede, mogućnost da treće strane pristupe tim podacima, mjera u kojoj su osobne informacije raširene, je li to dovelo do bilo kakvih dodatnih povreda prava pojedinca, kako se osobnim informacijama upravljalo i kako su one bile zaštićene itd.

([175]) Na temelju Zakona o naknadi štete od države pojedinci mogu podnijeti zahtjev za naknadu štete koju su nanijeli javni službenici pri izvršenju službenih dužnosti u suprotnosti sa zakonom (članak 2. stavak 1. Zakona).

([176]) Članci 9. i 12. Zakona o naknadi štete od države. Zakonom se osnivaju okružna vijeća (kojima predsjeda zamjenik tužitelja u pripadajućem uredu tužitelja), Središnje vijeće (kojim predsjeda zamjenik ministra pravosuđa) i Posebno vijeće (koje je zaduženo za zahtjeve za naknadu štete koju su nanijeli vojno osoblje ili civilni zaposlenici vojske, a kojim predsjeda zamjenik ministra nacionalne obrane). Zahtjeve za naknadu u načelu obrađuju okružna vijeća, no ona u određenim okolnostima moraju proslijediti predmete Središnjem ili Posebnom vijeću, primjerice ako naknada premašuje određeni iznos ili ako pojedinac podnese zahtjev za ponovno razmatranje. Sva se vijeća sastoje od članova koje je imenovao ministar pravosuđa (npr. iz redova javnih službenika Ministarstva pravosuđa, pravosudnih službenika, odvjetnika i osoba koje imaju stručno znanje u vezi s naknadom štete od države) i podliježu posebnim pravilima o sukobu interesa (vidjeti članak 7. Dekreta o izvršavanju Zakona o naknadi štete od države).

([177]) Vidjeti članak 8. Zakona o naknadi štete od države (u kojem se upućuje na Građanski zakon) te članak 751. Građanskog zakona.

([178]) Članak 7. Zakona o naknadi štete od države.

([179]) Odluka Vrhovnog suda 93Da40614 od 12. travnja 1996. i Odluka 2008Da42430 od 2. rujna 2011. (sažetak na engleskom jeziku dostupan je na https://www.scourt.go.kr/eng/supreme/decisions/NewDecisionsView.work?seq=696&pageIndex=1&mode=6&searchWord=).

([180]) Vidjeti, primjerice, Odluku Vrhovnog suda 2008Da42430 od 2. rujna 2011. (sažetak na engleskom jeziku dostupan je na https://www.scourt.go.kr/eng/supreme/decisions/NewDecisionsView.work?seq=696&pageIndex=1&mode=6&searchWord=).

(137) Na kraju, pojedinci mogu podnijeti kaznenu prijavu u skladu sa Zakonom o kaznenom postupku (članak 223.) javnom tužitelju ili službeniku pravosudne policije ([181]).

(138) Stoga korejski sustav pruža razne mogućnosti za dobivanje pravne zaštite, od lako dostupnih i jeftinih mogućnosti (primjerice, stupanjem u kontakt s Pozivnim centrom za zaštitu privatnosti ili (kolektivnim) posredovanjem), preko upravnih mogućnosti za pravnu zaštitu (pred PIPC-om) do sudskih mogućnosti za pravnu zaštitu, među ostalim i s mogućnošću dobivanja naknade štete.

3. **PRISTUP TIJELA JAVNE VLASTI U REPUBLICI KOREJI OSOBNIM PODACIMA PRENESENIMA IZ EUROPSKE UNIJE I NJIHOVA UPOTREBA TIH PODATAKA**

(139) Komisija je ocijenila i ograničenja i zaštitne mjere, uključujući mehanizme za nadzor i pravnu zaštitu pojedinaca dostupne u korejskom pravu kad je riječ o prikupljanju i naknadnoj upotrebi osobnih podataka koje korejska tijela javne vlasti prenose voditeljima obrade u Koreji u javnom interesu, osobito za potrebe kaznenog progona i nacionalne sigurnosti (pristup vlade). U tom je pogledu korejska vlada Komisiji dostavila službene izjave, jamstva i obveze potpisane na najvišoj ministarskoj razini i razini agencija, koje se nalaze u Prilogu II. ovoj Odluci.

(140) Pri ocjenjivanju toga ispunjavaju li uvjeti pod kojima je omogućen pristup vlade podacima prenesenima u Koreju na temelju ove Odluke test „načelne istovjetnosti" u skladu s člankom 45. stavkom 1. Uredbe (EU) 2016/679, kako je tumači Sud Europske unije s obzirom na Povelju o temeljnim pravima, Komisija je posebno uzela u obzir kriterije u nastavku.

(141) Prvo, svako ograničenje prava na zaštitu osobnih podataka mora biti predviđeno zakonom, a u samoj se pravnoj osnovi kojom se dopušta zadiranje u takvo pravo mora definirati doseg ograničenja ostvarivanja predmetnog prava ([182]).

(142) Drugo, da bi se ispunio zahtjev proporcionalnosti, prema kojem se odstupanja od zaštite osobnih podataka i ograničenja te zaštite u demokratskom društvu moraju primjenjivati samo ako je to nužno za ostvarenje specifičnih ciljeva od općeg interesa koji su jednakovrijedni onima koje priznaje Unija, u predmetnom propisu treće zemlje kojim se dopušta zadiranje u to pravo moraju biti utvrđena jasna i precizna pravila o dosegu i primjeni predmetnih mjera i moraju se uvesti minimalne zaštitne mjere tako da osobe čiji su podaci preneseni raspolažu dostatnim jamstvima koja omogućuju djelotvornu zaštitu njihovih osobnih podataka od rizika zloupotrebe ([183]). U propisu se osobito mora navesti u kojim se okolnostima i pod kojim uvjetima može donijeti mjera koja omogućuje obradu tih podataka ([184]), a ispunjenje takvih zahtjeva mora se podvrgnuti neovisnom nadzoru ([185]).

(143) Treće, taj propis i zahtjevi iz njega moraju biti pravno obvezujući na temelju domaćeg prava. To se prije svega odnosi na tijela predmetne treće zemlje, ali ti pravni zahtjevi moraju biti izvršivi pred sudovima i protiv tih tijela ([186]). Točnije, ispitanici moraju imati mogućnost pokretanja tužbe pred neovisnim i nepristranim sudom radi pristupa svojim osobnim podacima ili ispravka ili brisanja tih podataka ([187]).

3.1. **Opći pravni okvir**

(144) Ograničenja i zaštitne mjere koji se primjenjuju na prikupljanje i naknadnu upotrebu osobnih podataka od strane korejskih tijela javne vlasti proizlaze iz sveobuhvatnog ustavnog okvira, posebnih zakona kojima se uređuju aktivnosti tih tijela u područjima kaznenog progona i nacionalne sigurnosti te pravila koja se posebno primjenjuju na obradu osobnih podataka.

([181]) Kako je objašnjeno u uvodnoj izjavi 127., pogrešna upotreba podataka može činiti kazneno djelo na temelju Kaznenog zakona.

([182]) Vidjeti predmet *Schrems II*, točke 174. i 175. te navedenu sudsku praksu. Kad je riječ o pristupu tijela javne vlasti država članica, vidjeti i predmet C-623/17, *Privacy International*, ECLI:EU:C:2020:790, točku 65. i spojene predmete C-511/18, C-512/18 i C-520/18, *La Quadrature du Net i dr.*, ECLI:EU:C:2020:791, točku 175.

([183]) Vidjeti predmet *Schrems II*, točke 176. i 181. te navedenu sudsku praksu. Kad je riječ o pristupu tijela javne vlasti država članica, vidjeti i predmet *Privacy International*, točku 68. i predmet *La Quadrature du Net i dr.*, točku 132.

([184]) Vidjeti predmet *Schrems II*, točku 176. Kad je riječ o pristupu tijela javne vlasti država članica, vidjeti i predmet *Privacy International*, točku 68. i predmet *La Quadrature du Net i dr.*, točku 132.

([185]) Vidjeti predmet *Schrems II*, točku 179.

([186]) Vidjeti predmet Schrems II, točke 181. i 182.

([187]) Vidjeti predmet Schrems I, točku 95., i predmet Schrems II, točku 194. Sud Europske unije u tom je pogledu posebno istaknuo da poštovanje članka 47. Povelje o temeljnim pravima, u kojem se jamči pravo na djelotvoran pravni lijek pred neovisnim i nepristranim sudom, „pridonosi razini zaštite koja se zahtijeva u okviru Unije [i to poštovanje] mora utvrditi Komisija prije nego što donese odluku o primjerenosti na temelju članka 45. stavka 1. [Uredbe (EU) 2016/679]" (*Schrems II*, točka 186.).

(145) Prvo, pristup korejskih tijela javne vlasti osobnim podacima uređuje se općim načelima zakonitosti, nužnosti i proporcionalnosti koja proizlaze iz korejskog Ustava ([188]). Konkretnije, temeljna prava i slobode (uključujući pravo na privatnost i pravo na privatnost korespondencije) ([189]) smiju se ograničiti samo zakonom i ako je to potrebno radi nacionalne sigurnosti ili održavanja javnog reda za dobrobit građana. Ta ograničenja ne smiju utjecati na bit predmetnog prava ili predmetne slobode. Kad je posebno riječ o pretragama i zapljenama, Ustavom se propisuje da se one mogu provoditi jedino u skladu sa zakonom, na temelju naloga koji izdaje sudac i u skladu s odgovarajućim postupkom ([190]). Na kraju, pojedinci se mogu pozivati na svoja prava i slobode pred Ustavnim sudom ako smatraju da su im tijela javne vlasti u izvršavanju svojih ovlasti povrijedila ta prava i slobode ([191]). Slično tomu, pojedinci koji su pretrpjeli štetu zbog nezakonitog postupanja javnog službenika tijekom obavljanja njegovih službenih dužnosti imaju pravo tražiti pravednu naknadu štete ([192]).

(146) Drugo, kako je detaljnije opisano u odjeljcima 3.2.1. i 3.3.1., opća načela navedena u uvodnoj izjavi 145. odražavaju se i u posebnim zakonima kojima se uređuju ovlasti tijela kaznenog progona i tijela za nacionalnu sigurnost. Na primjer, kad je riječ o kaznenim istragama, u Zakonu o kaznenom postupku (CPA) propisuje se da se prisilne mjere smiju poduzimati samo ako je to izričito predviđeno CPA-om i u najmanjoj mjeri potrebnoj za ostvarenje svrhe istrage ([193]). Slično tomu, u članku 3. Zakona o zaštiti privatnosti komunikacija (CPPA) zabranjuje se pristup privatnim komunikacijama osim na temelju zakona i podložno ograničenjima i zaštitnim mjerama utvrđenima u zakonu. U području nacionalne sigurnosti Zakonom o Nacionalnoj obavještajnoj službi (Zakon o NIS-u) propisuje se da svaki pristup komunikacijama ili informacijama o lokaciji mora biti u skladu sa zakonom te da zloupotreba ovlasti i kršenja zakona podliježu kaznenim sankcijama ([194]).

(147) Treće, obrada osobnih podataka koju provode tijela javne vlasti, među ostalim i za potrebe kaznenog progona i nacionalne sigurnosti, podliježe pravilima o zaštiti podataka u skladu s PIPA-om ([195]). Kao opće načelo, člankom 5. stavkom 1. PIPA-e od tijela javne vlasti zahtijeva se da izrade politike za sprečavanje „zloupotrebe i pogrešne upotrebe osobnih informacija, neselektivnog nadzora i praćenja itd. te za unapređenje dostojanstva ljudskih bića i privatnosti pojedinaca”. Osim toga, svaki voditelj obrade mora osobne podatke obrađivati tako da se mogućnost povrede privatnosti ispitanika svede na najmanju mjeru (članak 3. stavak 6. PIPA-e).

(148) Svi zahtjevi iz PIPA-e, kako su detaljno opisano u odjeljku 2., primjenjuju se na obradu osobnih podataka za potrebe kaznenog progona. To uključuje temeljna načela (kao što su zakonitost i poštenost, ograničavanje svrhe, točnost, smanjenje količine podataka, ograničenje pohrane, sigurnost i transparentnost), obveze (primjerice, u vezi s obavješćivanjem o povredi podataka i osjetljivim podacima) i prava (na dobivanje pristupa, ispravak, brisanje i suspenziju).

(149) Iako obrada osobnih podataka za potrebe nacionalne sigurnosti podliježe ograničenjem skupu odredaba iz PIPA-e, na nju se primjenjuju temeljna načela te pravila o nadzoru, izvršavanju i pravnoj zaštiti ([196]). Konkretnije, u člancima 3. i 4. PIPA-e utvrđuju se opća načela zaštite podataka (zakonitost i poštenost, ograničavanje svrhe, točnost, smanjenje količine podataka, sigurnost i transparentnost) i prava pojedinaca (pravo pojedinca da bude obaviješten, pravo na pristup te prava na ispravak, brisanje i suspenziju) ([197]). U članku 4. stavku 5. PIPA-e pojedincima se usto daje i pravo na prikladnu pravnu zaštitu za svaku štetu koja proizlazi iz obrade njihovih osobnih podataka u okviru brzog i poštenog postupka. To je dopunjeno konkretnijim obvezama prema kojima se

([188]) Vidjeti Prilog II., odjeljak 1.1.
([189]) Članak 37. stavak 2. Ustava.
([190]) Članak 16. i članak 12. stavak 3. Ustava. U članku 12. stavku 3. Ustava nadalje se utvrđuju iznimne okolnosti u kojima se pretrage i zapljene mogu provoditi bez naloga (iako se i dalje zahtijeva naknadni nalog), tj. ako je počinitelj uhvaćen pri samom počinjenju djela (*in flagrante delicto*) ili, za kaznena djela za koja je predviđena kazna zatvora od najmanje tri godine, ako postoji opasnost da će dokazi biti uništeni ili da će osumnjičenik nestati.
([191]) Članak 68. stavak 1. Zakona o Ustavnom sudu.
([192]) Članak 29. stavak 1. Ustava.
([193]) Članak 199. stavak 1. CPA-a. Općenitije, pri izvršavanju svojih ovlasti na temelju CPA-a tijela javne vlasti moraju poštovati temeljna prava osumnjičenika za kaznena djela i svih drugih predmetnih osoba (članak 198. stavak 2. CPA-a).
([194]) Članak 14. Zakona o NIS-u.
([195]) Vidjeti Prilog II., odjeljak 1.2.
([196]) Članak 58. stavak 1. točka 2. PIPA-e. Vidjeti i odjeljak 6. Obavijesti br. 2021-5 (Prilog I.). To izuzeće od određenih odredaba PIPA-e primjenjuje se samo kad se osobni podaci obrađuju „za potrebe nacionalne sigurnosti”. Nakon što stanje nacionalne sigurnosti koje opravdava obradu podataka završi, više se ne može pozivati na izuzeće i primjenjuju se svi zahtjevi PIPA-e.
([197]) Ta prava smiju se ograničiti samo ako je to predviđeno zakonom, i to u mjeri i onoliko dugo koliko je to nužno i proporcionalno radi zaštite važnog cilja od javnog interesa, ili ako bi se izvršavanjem prava mogao ugroziti život ili zdravlje treće strane ili uzrokovati neopravdana povreda imovine i drugih interesa treće strane. Vidjeti odjeljak 6. Obavijesti br. 2021-5.

osobni podaci moraju obrađivati samo u najmanjoj mjeri koja je potrebna za ostvarenje predviđene svrhe i tijekom minimalnog razdoblja, moraju se uvesti potrebne mjere za osiguranje sigurnog upravljanja podacima i prikladne obrade (kao što su tehničke, upravljačke i fizičke zaštitne mjere) te se moraju uvesti mjere za prikladno rješavanje pojedinačnih pritužbi ([198]). Na kraju, opća načela zakonitosti, nužnosti i proporcionalnosti iz korejskog Ustava (vidjeti uvodnu izjavu 145.) primjenjuju se i na obradu osobnih podataka za potrebe nacionalne sigurnosti.

(150) Na ta opća ograničenja i zaštitne mjere pojedinci se mogu pozivati pred neovisnim nadzornim tijelima (npr. PIPC i/ili Nacionalno povjerenstvo za ljudska prava, vidjeti uvodne izjave 177. i 178.) i sudovima (vidjeti uvodne izjave od 179. do 183.) kako bi dobili pravnu zaštitu.

3.2. **Pristup korejskih tijela javne vlasti podacima i njihova upotreba za potrebe kaznenog progona**

(151) Pravom Republike Koreje uvode se brojna ograničenja pristupa osobnim podacima i njihove upotrebe za potrebe kaznenog progona te se predviđaju mehanizmi nadzora i pravne zaštite koji su u skladu sa zahtjevima iz uvodnih izjava od 141. do 143. ove Odluke. Uvjeti pod kojima je takav pristup moguć i zaštitne mjere koje se primjenjuju na upotrebu tih ovlasti detaljno se ocjenjuju u odjeljcima u nastavku.

3.2.1. *Pravne osnove, ograničenja i zaštitne mjere*

(152) Osobne podatke koje obrađuju korejski voditelji obrade, a koji bi se prenosili iz Unije na temelju ove Odluke ([199]) mogla bi prikupljati korejska tijela za potrebe kaznenog progona u kontekstu pretrage ili zapljene (na temelju CPA-a), pristupanjem informacijama o komunikaciji (na temelju CPPA-a) ili pribavljanjem podataka o pretplatnicima putem zahtjevâ za dobrovoljno otkrivanje (na temelju Zakona o telekomunikacijama, TBA) ([200]).

3.2.1.1. Pretrage i zapljene

(153) CPA-om se predviđa da se pretraga ili zapljena smije provoditi samo ako se osoba sumnjiči za kazneno djela, ako je to potrebno za istragu i ako se utvrdi povezanost između istrage i osobe koju treba pretražiti ili predmeta koji treba pregledati ili zaplijeniti ([201]). Nadalje, pretraga ili zapljena (kao i bilo koja prisilna mjera) smiju se dopustiti/provoditi samo u najmanjoj potrebnoj mjeri ([202]). Ako se pretraga odnosi na računalni disk ili drugi medij za pohranu podataka, u načelu se zapljenjuju samo potrebni podaci (kopirani ili ispisani), a ne cijeli medij ([203]). Potonji se smije zaplijeniti samo ako se smatra gotovo nemogućim zasebno ispisati ili kopirati potrebne podatke ili ako se smatra da je gotovo neizvedivo na drugi način ostvariti svrhu pretrage ([204]). Stoga se CPA-om propisuju jasna i precizna pravila o opsegu i primjeni tih mjera, čime se osigurava da će zadiranje u prava pojedinaca u slučaju pretrage ili zapljene biti ograničeno na ono što je nužno za određenu kaznenu istragu i proporcionalno predviđenoj svrsi.

([198]) Članak 58. stavak 4. PIPA-e.

([199]) Vidjeti Prilog II., odjeljak 2.1. U službenoj izjavi korejske vlade (odjeljak 2.1. Priloga II.) navodi se i mogućnost prikupljanja informacija o financijskim transakcijama za potrebe sprečavanja pranja novca i financiranja terorizma na temelju Zakona o prijavljivanju i upotrebi određenih informacija o financijskim transakcijama (ARUSFTI). Međutim, ARUSFTI-jem se samo uvode obveze otkrivanja za voditelje obrade koji obrađuju osobne kreditne informacije u skladu s CIA-om i podliježu nadzoru FSC-a (vidjeti uvodnu izjavu 13.). Budući da je obrada osobnih kreditnih informacija koju provode takvi voditelji obrade isključena iz područja primjene ove Odluke, ARUSFTI nije relevantan za ovu ocjenu.

([200]) U članku 3. CPPA-a navodi se i Zakon o vojnim sudovima kao moguća pravna osnova za prikupljanje podataka o komunikacijama. Međutim, tim zakonom uređuje se prikupljanje informacija o vojnom osoblju i može se primijeniti na civile samo u ograničenom broju slučajeva (npr. ako vojno osoblje i civili zajedno počine kazneno djelo ili ako pojedinac počini kazneno djelo protiv vojske, postupak se može pokrenuti pred vojnim sudom, vidjeti članak 2. Zakona o vojnim sudovima). U svakom slučaju, njime se propisuju opće odredbe kojima se uređuju pretrage i zapljene i koje su slične odredbama iz CPA-a (vidjeti npr. članke od 146. do 149. i članke od 153. do 156. Zakona o vojnim sudovima) te se njime predviđa, primjerice, da se obična pošta može prikupljati samo ako je to potrebno za istragu i na temelju naloga Vojnog suda. Ako bi se elektroničke komunikacije prikupljale na temelju tog zakona, primjenjivala bi se ograničenja i zaštitne mjere iz CPPA-a. Vidjeti Prilog II., odjeljak 2.2.2. i bilješku 50.

([201]) Članak 215. stavci 1. i 2. CPA-a. Vidjeti i članak 106. stavak 1., članak 107. i članak 109. CPA-a, u kojima se predviđa da sudovi smiju provoditi pretrage i zapljene sve dok se predmeti ili osobe u pitanju smatraju povezanima s određenim slučajem. Vidjeti Prilog II., odjeljak 2.2.1.2.

([202]) Članak 199. stavak 1. CPA-a.

([203]) Članak 106. stavak 3. CPA-a.

([204]) Članak 106. stavak 3. CPA-a.

(154) Kad je riječ o postupovnim zaštitnim mjerama, CPA-om se zahtijeva da se za provođenje pretrage ili zapljene mora dobiti nalog suda ([205]). Pretraga ili zapljena bez naloga samo je iznimno dopuštena, to jest u hitnim okolnostima ([206]), na licu mjesta u trenutku uhićenja ili zadržavanja osumnjičenika za kazneno djelo ([207]) ili ako su osumnjičenik za kazneno djelo ili treća osoba (odnosno, kad je riječ o osobnim podacima, sam predmetni pojedinac) odbacili ili dobrovoljno predali predmet ([208]). Nezakonite pretrage i zapljene podliježu kaznenim sankcijama ([209]) te se svi dokazi prikupljeni suprotno odredbama CPA-a smatraju nedopuštenima ([210]). Naposljetku, predmetni pojedinci moraju se uvijek bez odgode obavijestiti o pretrazi ili zapljeni (uključujući zapljenu njihovih podataka) ([211]), čime će se pak olakšati ostvarivanje njihovih materijalnih prava i prava na pravnu zaštitu (vidjeti naročito mogućnost osporavanja izvršenja naloga za zapljenu, vidjeti uvodnu izjavu 180.).

3.2.1.2. Pristup informacijama o komunikaciji

(155) Na temelju CPPA-a korejska tijela kaznenog progona mogu poduzimati dvije vrste mjera ([212]): s jedne strane, prikupljanje „podataka o potvrdi komunikacije” ([213]), što uključuje datum telekomunikacija, njihovo vrijeme početka i završetka, broj odlaznih i dolaznih poziva te pretplatnički broj druge strane, učestalost upotrebe, zapisnike o upotrebi telekomunikacijskih usluga i informacije o lokaciji (na primjer s odašiljača na kojima su signali primljeni); i, s druge strane, „mjere ograničavanja komunikacije”, koje obuhvaćaju i prikupljanje sadržaja tradicionalne pošte i izravno presretanje sadržaja telekomunikacija ([214]).

(156) Podacima o potvrdi komunikacije smije se pristupiti samo kad je to potrebno radi vođenja kaznene istrage ili izvršenja kazne ([215]), na temelju naloga koji je izdao sud ([216]). S obzirom na to, u CPPA-u se zahtijeva da se detaljne informacije navedu i u zahtjevu za nalog (npr. o razlozima za zahtjev, odnos s ciljem/pretplatnikom i potrebnim podacima) i u samom nalogu (npr. o svrsi, cilju i opsegu mjere) ([217]). Prikupljanje bez naloga smije se provoditi samo ako zbog hitnosti nije moguće dobiti dopuštenje suda, a u tom se slučaju nalog mora ishoditi i o

([205]) Članak 215. stavci 1. i 2. i članak 113. CPA-a. Pri podnošenju zahtjeva za izdavanje naloga predmetno tijelo mora podnijeti materijale kojima se dokazuje da postoji osnova za sumnju da je pojedinac počinio kazneno djelo, da je pretraga, inspekcijski pregled ili zapljena potrebna i da predmeti koje je potrebno zaplijeniti postoje (članak 108. stavak 1. Uredbe o kaznenom postupku). U samom nalogu moraju se navesti, među ostalim, imena osumnjičenika i kazneno djelo; mjesto, osoba ili predmeti koje je potrebno pretražiti ili zaplijeniti; datum izdavanja; i razdoblje valjanosti (članak 114. stavak 1. u vezi s člankom 219. CPA-a). Vidjeti Prilog II., odjeljak 2.2.1.2.

([206]) To jest, ako je nemoguće ishoditi nalog zbog hitnosti na mjestu počinjenja kaznenog djela (članak 216. stavak 3. CPA-a), a u tom se slučaju nalog i dalje mora ishoditi naknadno bez odgode (članak 216. stavak 3. CPA-a).

([207]) Članak 216. stavci 1. i 2. CPA-a.

([208]) Članak 218. CPA-a. Nadalje, kako je objašnjeno u odjeljku 2.2.1.2. Priloga II., dobrovoljno predani predmeti mogu se prihvatiti kao dokaz u sudskom postupku samo ako ne postoji opravdana sumnja u vezi s dobrovoljnom prirodom otkrivanja, što treba dokazati tužitelj.

([209]) Članak 321. Kaznenog zakona.

([210]) Članak 308-2. CPA-a. Osim toga, pojedinac (i njegov odvjetnik) mogu biti prisutni kad se nalog za pretragu ili zapljenu izvršava te stoga mogu uložiti i prigovor u trenutku izvršenja tog naloga (članci 121. i 219. CPA-a).

([211]) Članci 121. i 122. CPA-a (u vezi s pretragama) i članak 219. u vezi s člankom 106. stavkom 4. CPA-a (u vezi sa zapljenama).

([212]) Vidjeti i Prilog II., odjeljak 2.2.2.1. Takve se mjere mogu poduzimati uz pomoć telekomunikacijskih operatera koju su oni prisiljeni pružiti nakon što im se uruči pisano dopuštenje dobiveno od suda (članak 9. stavak 2. CPPA-a), koje operateri moraju čuvati (članak 15-2. CPPA-a i članak 12. Dekreta o izvršavanju CPPA-a). Telekomunikacijski operateri mogu odbiti surađivati ako informacije o ciljanom pojedincu, kako su navedene u pisanom dopuštenju suda (na primjer telefonski broj pojedinca), nisu točne te im je u svim okolnostima zabranjeno otkrivati lozinke za telekomunikacije (članak 9. stavak 4. CPPA-a).

([213]) Članak 2. točka 11. CPPA-a.

([214]) Vidjeti članak 2. točku 6. CPPA-a, koji se odnosi na „cenzuru” (otvaranje pošte bez privole predmetne stranke ili pribavljanje informacija o njezinu sadržaju ili snimanje ili uskraćivanje njezina sadržaja na druge načine) i članak 2. točku 7. CPPA-a, koja se odnosi na „prisluškivanje” (pribavljanje ili snimanje sadržaja telekomunikacija slušanjem ili zajedničkim čitanjem zvukova, riječi, simbola ili slika u komunikacijama s pomoću elektroničkih ili mehaničkih uređaja bez privole predmetne stranke ili ometanje njihova prijenosa i primitka).

([215]) Članak 13. stavak 1. CPPA-a. Vidjeti i Prilog II., odjeljak 2.2.2.3. Osim toga, podaci o praćenju lokacije u stvarnom vremenu i podaci o potvrdi komunikacije koji se odnose na određenu baznu stanicu smiju se prikupljati samo za istrage teških kaznenih djela ili ako bi inače bilo teško spriječiti počinjenje kaznenog djela ili prikupiti dokaze (članak 13. stavak 2. CPPA). To odražava potrebu da se, u skladu s načelom proporcionalnosti, osiguraju dodatne zaštitne mjere kad je riječ o mjerama kojima se naročito zadire u privatnost.

([216]) Članci 13. i 6. CPPA-a.

([217]) Vidjeti članak 13. stavke 3. i 9. u vezi s člankom 6. stavcima 4. i 6. CPPA-a.

njemu se mora obavijestiti pružatelj telekomunikacijskih usluga odmah nakon što se zatraže podaci ([218]). Ako sud odbija dati naknadno dopuštenje, prikupljene informacije moraju se uništiti ([219]).

(157) Kad je riječ o dodatnim zaštitnim mjerama s obzirom na prikupljanje podataka o potvrdi komunikacije, CPPA-om se uvode posebni zahtjevi o vođenju evidencije i transparentnosti ([220]). Konkretno, i tijela kaznenog progona ([221]) i pružatelji telekomunikacijskih usluga ([222]) moraju voditi evidencije o podnesenim zahtjevima i izvršenim otkrivanjima. Osim toga, tijela kaznenog progona moraju u načelu obavijestiti pojedince o tome da su prikupljeni njihovi podaci o potvrdi komunikacije ([223]). To obavješćivanje smije se odgoditi samo u iznimnim okolnostima, na temelju odobrenja direktora nadležnog ureda okružnog javnog tužitelja ([224]). To odobrenje može se dati samo ako je vjerojatno da će se obavješćivanjem 1. ugroziti nacionalna sigurnost, javna sigurnost i javni red, 2. prouzročiti smrt ili tjelesne ozljede, 3. onemogućiti pravedan sudski postupak (na primjer, dovesti do uništenja dokaza ili prijetnje svjedocima) ili 4. dovesti do klevete osumnjičenika, žrtava ili drugih osoba povezanih s predmetom ili zadiranja u njihovu privatnost. U tim se slučajevima obavijest mora dati u roku od 30 dana nakon što osnove za odgodu prestanu postojati ([225]). Nakon obavješćivanja pojedinci imaju pravo dobiti informacije o razlozima za prikupljanje njihovih podataka ([226]).

(158) Stroža pravila primjenjuju se na mjere ograničavanja komunikacije, koje se smiju primjenjivati samo ako postoji opravdan razlog za sumnju da se određena teška kaznena djela navedena u CPPA-u planiraju, čine ili da su počinjena ([227]). Nadalje, mjere ograničavanja komunikacije smiju se poduzimati samo kao krajnja mjera i ako je teško na drugi način spriječiti počinjenje kaznenog djela, uhititi počinitelja ili prikupiti dokaze ([228]). Moraju se obustaviti čim prestanu biti potrebne kako bi se osiguralo da povreda privatnosti komunikacija bude što ograničenija ([229]). Informacije koje su nezakonito pribavljene primjenom mjera ograničavanja komunikacije ne priznaju se kao dokaz u sudskom ili stegovnom postupku ([230]).

(159) Kad je riječ o postupovnim zaštitnim mjerama, CPPA-om se zahtijeva da se za provođenje mjera ograničavanja komunikacije mora ishoditi sudski nalog ([231]). Osim toga, CPPA-om se zahtijeva da zahtjev za nalog i sam nalog sadržavaju detaljne informacije ([232]), među ostalim o obrazloženju zahtjeva te komunikacijama koje treba prikupiti (koje moraju biti komunikacije osumnjičenika pod istragom) ([233]). Takve se mjere smiju poduzimati bez naloga jedino u slučaju neminovne prijetnje organiziranog kriminala ili ako je neminovno drugo teško kazneno djelo koje može izravno dovesti do smrti ili teških ozljeda, a riječ je o izvanrednoj situaciji u kojoj

([218]) Članak 13. stavak 2. CPPA-a.
([219]) Članak 13. stavak 3. CPPA-a.
([220]) Vidjeti Prilog II., odjeljak 2.2.2.3.
([221]) Članak 13. stavci 5. i 6. CPPA-a.
([222]) Članak 13. stavak 7. CPPA-a. Nadalje, pružatelji telekomunikacijskih usluga moraju dvaput godišnje izvješćivati Ministarstvo znanosti i IKT-a o otkrivanju podataka o potvrdi komunikacije.
([223]) Vidjeti članak 13-3. stavak 7. u vezi s člankom 9-2. CPPA-a. Konkretno, pojedinci se moraju obavijestiti u roku od 30 dana od donošenja odluke o tome hoće li se provoditi kazneni progon ili u roku od 30 dana od isteka godine dana od donošenja odluke o suspendiranju optužnice (iako se obavijest u svakom slučaju mora dati u roku od 30 dana od isteka godine dana od prikupljanja informacija), vidjeti članak 13-3. stavak 1. CPPA-a.
([224]) Članak 13-3. stavci 2. i 3. CPPA-a.
([225]) Članak 13-3. stavak 4. CPPA-a.
([226]) Članak 13-3. stavak 5. CPPA-a. Na zahtjev pojedinca tužitelj ili službenik pravosudne policije mora pisanim putem navesti te razloge u roku od 30 dana nakon zaprimanja zahtjeva, osim ako se primjenjuje jedno od izuzeća za odgodu obavijesti (članak 13-3. stavak 6. CPPA-a).
([227]) Primjerice, pobuna, kaznena djela povezana s drogama ili kaznena djela koja uključuju eksplozive, kao i kaznena djela povezana s nacionalnom sigurnošću, diplomatskim odnosima ili vojnim bazama i objektima, vidjeti članak 5. stavak 1. CPPA-a. Vidjeti i Prilog II., odjeljak 2.2.2.2.
([228]) Članak 3. stavak 2. i članak 5. stavak 1. CPPA-a.
([229]) Članak 2. Dekreta o izvršavanju CPPA-a.
([230]) Članak 4. CPPA-a.
([231]) Članak 6. stavci 1. i 2. i stavci 5. i 6. CPPA-a.
([232]) U zahtjevu za nalog moraju se opisati 1. opravdani razlozi zbog kojih se (na prvi pogled) sumnja da se jedno od navedenih kaznenih djela planira, čini ili da je počinjeno, kao i svi materijali kojima se to potkrepljuje; 2. mjere ograničavanja komunikacije te njihov cilj, opseg, svrha i razdoblje valjanosti; i 3. mjesto na kojem bi se te mjere trebale izvršavati i način izvršavanja (članak 6. stavak 4. CPPA-a i članak 4. stavak 1. Dekreta o izvršavanju CPPA-a). U samom se nalogu moraju navesti mjere te njihov cilj, opseg, razdoblje valjanosti, mjesto izvršenja i način izvršenja (članak 6. stavak 6. CPPA-a).
([233]) Cilj mjere ograničavanja komunikacije mora biti određena pošta ili telekomunikacije koje osumnjičenik šalje ili prima ili pošta ili telekomunikacije koje osumnjičenik šalje ili prima u određenom razdoblju (članak 5. stavak 2. CPPA-a).

nije moguće provesti redovni postupak ([234]). Međutim, u tom se slučaju zahtjev za nalog mora podnijeti odmah nakon poduzimanja mjere ([235]). Mjere ograničavanja komunikacije smiju se provoditi u razdoblju od najviše dva mjeseca ([236]) i mogu se produljiti samo odobrenjem suda ako su uvjeti za njihovo provođenje i dalje ispunjeni ([237]). To produljeno razdoblje ne smije ukupno trajati više od godine dana ili tri godine za određena naročito teška kaznena djela (kao što su kaznena djela povezana s pobunom, stranom agresijom i nacionalnom sigurnošću) ([238]).

(160) Kao i za prikupljanje podataka o potvrdi komunikacije, CPPA-om se od pružatelja telekomunikacijskih usluga ([239]) i tijela kaznenog progona ([240]) zahtijeva da vode evidencije izvršavanja mjera ograničavanja komunikacije i predviđa obveza obavješćivanja predmetnog pojedinca, što se prema potrebi iznimno može odgoditi na temelju važnog javnog interesa ([241]).

(161) Naposljetku, nepoštovanje pojedinih ograničenja i zaštitnih mjera iz CPPA-a (uključujući, primjerice, obveze ishođenja naloga, vođenja evidencije i obavješćivanja pojedinca), i u vezi s prikupljanjem podataka o potvrdi komunikacije i u vezi s primjenom mjera ograničavanja komunikacije, podliježe kaznenim sankcijama ([242]).

(162) Stoga su ovlasti tijela kaznenog progona za prikupljanje podataka o komunikacijama na temelju CPPA-a (i sadržaja komunikacija i podataka o potvrdi komunikacije) ograničene jasnim i preciznim pravilima te podliježu brojnim zaštitnim mjerama. Tim zaštitnim mjerama ponajprije se jamči nadzor nad izvršavanjem tih mjera, i *ex ante* (prethodnim sudskim odobrenjem) i *ex post* (zahtjevima o vođenju evidencije i obavješćivanju), te se olakšava pristup pojedinaca djelotvornim pravnim lijekovima (time što se osigurava da su obaviješteni o prikupljanju njihovih podataka).

3.2.1.3. Zahtjevi za dobrovoljno otkrivanje podataka o pretplatnicima

(163) Osim oslanjanja na prisilne mjere opisane u uvodnim izjavama od 153. do 162., korejska tijela kaznenog progona mogu od pružatelja telekomunikacijskih usluga zatražiti da na dobrovoljnoj osnovi otkriju „podatke o komunikacijama” radi potpore u kaznenom postupku, istrazi ili izvršenju kazne (članak 83. stavak 3. TBA-a). Ta mogućnost postoji samo za ograničene skupove podataka, tj. ime, registracijski broj rezidenta, adresu i telefonski broj korisnika, datume kad su se korisnici pretplatili ili okončali pretplatu te korisničke identifikacijske kodove (tj. kodove koji služe za identifikaciju stvarnog korisnika računalnih sustava ili komunikacijskih mreža) ([243]). Budući da se „korisnicima” smatraju samo pojedinci koji izravno ugovaraju usluge kod korejskog pružatelja telekomunikacijskih usluga ([244]), pojedinci iz EU-a čiji su podaci preneseni u Republiku Koreju neće obično biti obuhvaćeni tom kategorijom ([245]).

(164) Na takva dobrovoljna otkrivanja primjenjuju se različita ograničenja, i s obzirom na izvršavanje ovlasti od strane tijela kaznenog progona i s obzirom na odgovor telekomunikacijskog operatera. Kao opći zahtjev, tijela kaznenog progona moraju postupati u skladu s ustavnim načelima nužnosti i proporcionalnosti (članak 12. stavak 1. i članak 37. stavak 2. Ustava), među ostalim i kad traže otkrivanje informacija na dobrovoljnoj osnovi. Osim toga, moraju poštovati PIPA-u, prije svega prikupljanjem samo minimalnih osobnih podataka, u mjeri potrebnoj za

([234]) Članak 8. stavak 1. CPPA-a. Međutim, prikupljanje informacija u izvanrednim situacijama mora se uvijek odvijati u skladu s „izjavom o hitnoj cenzuri/prisluškivanju”, a tijelo koje provodi prikupljanje mora voditi registar svih izvanrednih mjera (članak 8. stavak 4. CPPA-a).

([235]) Prikupljanje se mora odmah prekinuti ako tijelo kaznenog progona ne uspije ishoditi dopuštenje suda u roku od 36 sati (članak 8. stavak 2. CPPA-a), a u tom će se slučaju, kako je objašnjeno u odjeljku 2.2.2.2. Priloga II., prikupljene informacije u načelu uništiti. Sud se mora obavijestiti i ako su izvanredne mjere provedene u tako kratkom roku da je potreba za dopuštenjem postala bespredmetna (npr. ako se osumnjičenik uhiti odmah nakon početka presretanja, vidjeti članak 8. stavak 5. CPPA-a). U tom se slučaju sudu moraju navesti informacije o svrsi, cilju, opsegu, razdoblju, mjestu izvršenja i metodi prikupljanja te razlozi za nepodnošenje zahtjeva za dopuštenje suda (članak 8. stavci 6. i 7. CPPA-a).

([236]) Članak 6. stavak 7. CPPA-a. Ako se svrha mjera ostvari u kraćem roku, one se moraju odmah obustaviti.

([237]) Članak 6. stavci 7. i 8. CPPA-a.

([238]) Članak 6. stavak 8. CPPA-a.

([239]) Članak 9. stavak 3. CPPA-a.

([240]) Članak 18. stavak 1. Dekreta o izvršavanju CPPA-a.

([241]) Konkretno, tužitelj mora obavijestiti pojedinca u roku od 30 dana od podizanja optužnice ili izdavanja odluke o nepodizanju optužnice ili neuhićenju (članak 9-2. stavak 1. CPPA-a). To se obavješćivanje može odgoditi uz odobrenje čelnika ureda okružnog javnog tužitelja ako bi se njime vjerojatno ozbiljno ugrozila nacionalna sigurnost ili narušila javna sigurnost i red ili ako bi se njime vjerojatno prouzročila znatna šteta životima i zdravlju drugih (članak 9-2. stavci od 4. do 6. CPPA-a).

([242]) Članci 16. i 17 CPPA-a.

([243]) Članak 83. stavak 3. TBA-a. Vidjeti i Prilog II., odjeljak 2.2.3.

([244]) Članak 2. stavak 9. TBA-a.

([245]) Vidjeti i Prilog II., odjeljak 2.2.3.

ostvarenje legitimne svrhe i tako da se učinak na privatnost pojedinaca svede na najmanju mjeru (članak 3. stavci 1. i 6. PIPA-e). Konkretnije, zahtjevi za pribavljanje podataka o komunikacijama na temelju TBA-a moraju se podnijeti u pisanom obliku i u njima se moraju navesti razlozi za zahtjev, poveznica na relevantnog korisnika i opseg traženih podataka ([246]).

(165) Pružatelji telekomunikacijskih usluga nisu obvezni postupiti po takvim zahtjevima i smiju to činiti samo u skladu s PIPA-om. To konkretno znači da moraju uzeti u obzir različite predmetne interese i da ne smiju otkrivati podatke ako bi se time vjerojatno nepošteno povrijedili interesi pojedinca ili treće strane ([247]). To bi na primjer bio slučaj ako je očito da je tijelo koje je uputilo zahtjev zloupotrijebilo svoje ovlasti ([248]). Telekomunikacijski operateri moraju čuvati evidencije o otkrivanjima na temelju TBA-a i dvaput godišnje izvješćivati ministra znanosti i IKT-a ([249]).

(166) Osim toga, u skladu s odjeljkom 3. Obavijesti br. 2021-5 (Prilog I.), pružatelji telekomunikacijskih usluga u načelu moraju obavijestiti predmetnog pojedinca kad dobrovoljno postupe po zahtjevu ([250]). Time će se pak pojedincu omogućiti da ostvari svoja prava i, ako da su njegovi podaci otkriveni nezakonito, dobije pravnu zaštitu, ili protiv voditelja obrade (primjerice, zbog otkrivanja podataka suprotno odredbama PIPA-e ili zbog postupanja po zahtjevu koji je očito bio neproporcionalan) ili protiv tijela kaznenog progona (primjerice, zbog postupanja izvan okvira onoga što je nužno i proporcionalno ili zbog nepoštovanja postupovnih zahtjeva iz TBA-a).

3.2.2. *Daljnja upotreba prikupljenih informacija*

(167) Obrada osobnih podataka koje prikupljaju korejska tijela kaznenog progona podliježe svim zahtjevima iz PIPA-e, među ostalim u pogledu ograničavanja svrhe (članak 3. stavci 1. i 2. PIPA-e), zakonitosti upotrebe i prosljeđivanja trećim stranama (članci 15., 17. i 18. PIPA-e), međunarodnih prijenosa (članci 17. i 18. PIPA-e u vezi s odjeljkom 2. Obavijesti 2021-5) ([251]), proporcionalnosti/smanjenja količine podataka (članak 3. stavci 1. i 6. PIPA-e) i ograničenja pohrane (članak 21. PIPA-e) ([252]).

(168) Kad je riječ o sadržaju komunikacija koji je pribavljen izvršenjem mjera ograničavanja komunikacije, njegova se moguća upotreba CPPA-om izričito ograničava na istragu, kazneni progon ili sprečavanje teških kaznenih djela ([253]), stegovne postupke za ista kaznena djela, postupke o zahtjevima za naknadu štete koje je podnijela stranka uključena u komunikaciju ili ako je to izričito dopušteno drugim zakonima ([254]). Nadalje, prikupljeni sadržaj telekomunikacija prenesenih internetom smije se zadržati samo uz odobrenje suda koji je dopustio mjere ograničavanja komunikacije ([255]), kako bi se upotrijebio za potrebe istrage, kaznenog progona ili sprečavanja teških kaznenih djela ([256]). Općenitije, CPPA-om se zabranjuje otkrivanje povjerljivih informacija pribavljenih primjenom mjera ograničavanja komunikacije i upotreba tih informacija u svrhu narušavanja ugleda osoba koje su bile cilj tih mjera ([257]).

3.2.3. *Nadzor*

(169) U Koreji aktivnosti tijela kaznenog progona nadziru različita tijela ([258]).

([246]) Članak 83. stavak 4. TBA-a. Ako zbog hitnosti nije moguće dostaviti pisani zahtjev, on se mora dostaviti čim nestane razlog za hitnost (članak 83. stavak 4. TBA-a).
([247]) Članak 18. stavak 2. PIPA-e.
([248]) Odluka Vrhovnog suda br. 2012Da105482 od 10. ožujka 2016. O toj odluci Vrhovnog suda vidjeti i Prilog II., odjeljak 2.2.3.
([249]) Članak 83. stavci 5. i 6. TBA-a.
([250]) Taj zahtjev podliježe ograničenim i uvjetovanim izuzećima, osobito ako i onoliko dugo koliko bi se tim obavješćivanjem ugrozila kaznena istraga u tijeku ili ako je vjerojatno da bi se time ugrozio život ili zdravlje druge osobe čija prava ili interesi nedvojbeno imaju prednost pred pravima ispitanika. Vidjeti odjeljak 3. točku iii. podtočku 1. Obavijesti.
([251]) Konkretno, korejska tijela javne vlasti moraju s pomoću pravno obvezujućeg instrumenta osigurati razinu zaštite istovjetnu PIPA-i, vidjeti i uvodnu izjavu 90.
([252]) Vidjeti i Prilog II., odjeljak 1.2.
([253]) Vidjeti uvodnu izjavu 158.
([254]) Članak 12. CPPA-a. Vidjeti Prilog II., odjeljak 2.2.2.2.
([255]) Tužitelj ili policijski službenik koji izvršava mjere ograničavanja komunikacije mora odabrati koje će se telekomunikacije zadržati u roku od 14 dana nakon završetka mjera i zatražiti odobrenje suda (ako je riječ o policijskom službeniku, zahtjev se mora uputiti tužitelju, koji zatim podnosi zahtjev sudu); vidjeti članak 12-2. stavke 1. i 2. CPPA-a.
([256]) Zahtjev za to dopuštenje mora sadržavati informacije o mjerama ograničavanja komunikacije, sažetak rezultata mjera, razloge za pohranu (zajedno s popratnim materijalima) i telekomunikacije koje se trebaju pohraniti (članak 12-2. stavak 3. CPPA-a). Ako se zahtjev ne podnese, pribavljeni podaci moraju se izbrisati u roku od 14 dana od završetka mjere ograničavanja komunikacije (članak 12-2. stavak 5. CPPA-a), a ako se zahtjev odbije, u roku od sedam dana (članak 12-2. stavak 5. CPPA-a). U oba se slučaja u roku od sedam dana sudu koji je dopustio prikupljanje mora podnijeti izvješće o brisanju.
([257]) Članak 11. stavak 2. Dekreta o izvršavanju CPPA-a.
([258]) Vidjeti Prilog II., odjeljak 2.3.

(170) Prvo, policija podliježe unutarnjem nadzoru glavnog inspektora ([259]), koji provodi provjeru zakonitosti, među ostalim u vezi s mogućim povredama ljudskih prava. Uloga glavnog inspektora uvedena je radi provedbe Zakona o revizijama u javnom sektoru, kojim se potiče osnivanje tijela za samoreviziju i utvrđuju posebni zahtjevi o njihovu sastavu i zadaćama. Točnije, tim se zakonom zahtijeva da se voditelj tijela za samoreviziju imenuje iz redova osoba izvan relevantnog tijela (kao što su bivši suci i profesori) na razdoblje od dvije do pet godina ([260]), da se on može razriješiti dužnosti samo zbog opravdanih razloga (na primjer ako ne može izvršavati svoje dužnosti zbog zdravstvenih razloga ili ako su na njega primijenjene stegovne mjere) ([261]) te mu se jamči neovisnost u najvećoj mogućoj mjeri ([262]). Ometanje samorevizije podliježe upravnim novčanim kaznama ([263]). Izvješća o reviziji (koja mogu uključivati preporuke, zahtjeve za stegovni postupak, naknadu štete ili ispravak) priopćuju se čelniku relevantnog javnog tijela, Revizijskom i inspekcijskom odboru (BAI) ([264]) i općenito se javno objavljuju ([265]). O rezultatima provedbe izvješća mora se obavijestiti i BAI ([266]) (vidjeti uvodnu izjavu 173. o nadzornoj ulozi i ovlastima BAI-ja).

(171) Drugo, PIPC nadzire usklađenost obrade podataka koju provode tijela kaznenog progona s PIPA-om i drugim zakonima kojima se štiti privatnost pojedinaca, uključujući zakone kojima se uređuje prikupljanje (elektroničkih) dokaza za potrebe kaznenog progona, kako je opisano u odjeljku 3.2.1. ([267]) Konkretno, s obzirom na to da nadzor PIPC-a obuhvaća i zakonitost i poštenost prikupljanja i obrade podataka (članak 3. stavak 1. PIPA-e), koje će biti povrijeđene ako se osobnim podacima pristupa i ako ih se upotrebljava suprotno tim zakonima ([268]), PIPC ujedno može i istraživati i provoditi usklađenost s ograničenjima i zaštitnim mjerama opisanima u odjeljku 3.2.1. ([269]) Pri izvršavanju nadzorne uloge PIPC može koristiti sve svoje istražne i korektivne ovlast, kako je detaljno opisano u odjeljku 2.4.2. Već i prije nedavne reforme PIPA-e (tj. u svojoj prethodnoj nadzornoj ulozi za javni sektor) PIPC je proveo nekoliko aktivnosti nadzora obrade osobnih podataka koju su provodila tijela kaznenog progona, npr. u kontekstu ispitivanja osumnjičenika (predmet br. 2013-16 od 26. kolovoza 2013.), u vezi s obavješćivanjem pojedinaca o izricanju upravnih novčanih kazni (predmet br. 2015-02-04 od 26. siječnja 2015.), o razmjeni podataka s drugim tijelima (predmet br. 2018-15-146 od 9. srpnja 2018., predmet br. 2018-25-308 od 10. prosinca 2018. i predmet br. 2019-02-015 od 29. siječnja 2019.), o prikupljanju otisaka prstiju ili fotografija (predmet br. 2019-17-273 od 9. rujna 2019.), o korištenju bespilotnih letjelica (predmet br. 2020-01-004 od 13. siječnja 2020.). PIPC je u tim predmetima istraživao poštovanje pojedinih odredaba PIPA-e (npr. zakonitost obrade, načela ograničavanja svrhe i smanjenja količine podataka), ali i relevantnih odredaba iz drugih zakon kao što je Zakon o kaznenom postupku, te je, prema potrebi, izdao preporuke kako bi se obrada uskladila sa zahtjevima o zaštiti podataka.

(172) Treće, neovisni nadzor osigurava Nacionalno povjerenstvo za ljudska prava (NHRC) ([270]), koje može istraživati povrede prava na privatnost i prava na privatnost korespondencije u okviru svojeg općeg mandata zaštite temeljnih prava iz članaka od 10. do 22. Ustava. NHRC se sastoji od 11 povjerenika koji moraju ispunjavati posebne uvjete ([271]), a imenuje ih predsjednik države u skladu s postupcima utvrđenima zakonom. Točnije, četiri povjerenika imenuju se na prijedlog Nacionalne skupštine, četiri na prijedlog predsjednika države i tri na prijedlog predsjednika Vrhovnog suda ([272]). Predsjednika NHRC-a imenuje predsjednik države među povjerenicima i mora ga potvrditi Nacionalna skupština ([273]). Povjerenici (uključujući predsjednika) imenuju se na mandat od tri godine

([259]) Vidjeti Prilog II., odjeljak 2.3.1. Vidjeti i https://www.police.go.kr/eng/knpa/org/org01.jsp.
([260]) Slično tomu, revizori se imenuju na temelju posebnih uvjeta utvrđenih Zakonom, vidjeti članak 16. i dalje Zakona o revizijama u javnom sektoru.
([261]) Članci od 8. do 11. Zakona o revizijama u javnom sektoru.
([262]) Članak 7. Zakona o revizijama u javnom sektoru.
([263]) Članak 41. Zakona o revizijama u javnom sektoru.
([264]) Članak 23. stavak 1. Zakona o revizijama u javnom sektoru.
([265]) Članak 26. Zakona o revizijama u javnom sektoru.
([266]) Članak 23. stavak 3. Zakona o revizijama u javnom sektoru.
([267]) Vidjeti članak 7-8. stavke 3. i 4. i članak 7-9. stavak 5. PIPA-e.
([268]) Vidjeti Obavijest PIPC-a br. 2021-5, odjeljak 6. (Prilog I.).
([269]) Vidjeti i Prilog II., odjeljak 2.3.4.
([270]) Članak 1. Zakona o Povjerenstvu za ljudska prava (Zakon o NHRC-u).
([271]) Kako bi bio imenovan, povjerenik mora ispunjavati jedan od sljedećih uvjeta: 1. mora najmanje deset godina raditi na sveučilištu ili u ovlaštenom istraživačkom institutu barem kao izvanredni profesor; 2. mora najmanje deset godina obnašati dužnost suca, tužitelja ili odvjetnika; 3. mora najmanje deset godina sudjelovati u aktivnostima povezanima s ljudskim pravima (npr. u okviru neprofitne, nevladine organizacije ili međunarodne organizacije); ili 4. moraju ga preporučiti udruge civilnog društva (članak 5. stavak 3. Zakona o NHRC-u). Nadalje, nakon što se imenuju, povjerenicima je zabranjeno istodobno obnašati dužnost u Nacionalnoj skupštini, lokalnim vijećima ili u bilo kojem državnom tijelu ili tijelu lokalne vlasti (kao javni dužnosnik); vidjeti članak 10. Zakona o NHRC-u.
([272]) Članak 5. stavci 1. i 2. Zakona o NHRC-u.
([273]) Članak 5. stavak 5. Zakona o NHRC-u.

s mogućnošću produljenja i mogu se razriješiti dužnosti samo ako su osuđeni na kaznu zatvora ili ako više nisu u stanju izvršavati svoje dužnosti zbog dugotrajnih fizičkih ili mentalnih poteškoća (a u tom se slučaju dvije trećine povjerenika moraju složiti s razrješenjem) ([274]). U okviru svoje istrage NHRC može zatražiti dostavljanje relevantnih materijala, provoditi inspekcijske preglede i pozivati pojedince da svjedoče ([275]). Kad je riječ o njegovim korektivnim ovlastima, NHRC može izdavati (javne) preporuke za poboljšanje ili ispravljanje određenih politika i praksi, na koje tijela javne vlasti moraju odgovoriti prijedlogom plana za provedbu preporuka ([276]). Ako predmetno tijelo ne provede preporuke, mora o tome obavijestiti NHRC ([277]), koji o tome može izvijestiti Nacionalnu skupštinu i/ili to javno objaviti. Prema službenoj izjavi korejske vlade (odjeljak 2.3.5. Priloga II.) korejska tijela općenito poštuju preporuke NHRC-a i imaju velik poticaj za to s obzirom na to da se provedba tih preporuka ocjenjivala u okviru opće, stalne evaluacije koja se provodi pod nadležnošću ureda premijera. Godišnji brojčani podaci o aktivnostima NHRC-a pokazuju da on aktivno nadzire aktivnosti tijela kaznenog progona, na temelju zahtjeva pojedinaca ili istragama koje pokreće po službenoj dužnosti ([278]).

(173) Četvrto, opći nadzor zakonitosti aktivnosti tijela javne vlasti provodi BAI, koji pregledava prihode i rashode države, ali, općenitije, nadzire i ispunjavanje dužnosti tijela javne vlasti kako bi se poboljšalo funkcioniranje javne uprave ([279]). BAI službeno djeluje pod nadležnošću predsjednika Republike Koreje, ali zadržava neovisan status u odnosu na svoje dužnosti ([280]). Usto, potpuno je neovisan u pogledu imenovanja, razrješenja i organiziranja svojeg osoblja i sastavljanja svojeg proračuna ([281]). BAI se sastoji od predsjednika (kojeg imenuje predsjednik države uz suglasnost Nacionalne skupštine) ([282]) i šest povjerenika (koje imenuje predsjednik države na preporuku predsjednika BAI-ja) ([283]), koji moraju ispunjavati određene uvjete propisane zakonom ([284]) i mogu se razriješiti dužnosti samo u slučaju opoziva, osude na kaznu zatvora ili nemogućnosti izvršavanja svojih dužnosti zbog dugotrajnih mentalnih ili fizičkih poteškoća ([285]). BAI svake godine provodi opću reviziju, ali može provoditi i posebne revizije o pitanjima od posebnog interesa. Pri obavljanju revizije ili inspekcijskog pregleda BAI može zatražiti dostavljanje dokumenata i pojavljivanje pojedinaca pred njim ([286]). BAI može izdavati preporuke, zatražiti pokretanje stegovnih mjera ili podnositi kaznene prijave ([287]).

(174) Naposljetku, Nacionalna skupština provodi parlamentarni nadzor nad tijelima javne vlasti istragama i inspekcijskim pregledima ([288]) njihovih aktivnosti ([289]). Može zatražiti otkrivanje dokumenata, prisiliti svjedoke na svjedočenje ([290]), preporučiti poduzimanje korektivnih mjera (ako zaključi da je bilo nezakonitih ili neprikladnih

([274]) Članak 7. stavak 1. i članak 8. Zakona o NHRC-u.

([275]) Članak 36. Zakona o NHRC-u. U skladu s člankom 6. stavkom 7. Zakona podnošenje materijala ili predmeta može se odbiti ako bi se time dovela u pitanje državna povjerljivost koja bi mogla imati znatne posljedice na državnu sigurnost ili diplomatske odnose ili bi to činilo ozbiljnu prepreku u kaznenoj istrazi ili sudskom postupku u tijeku. U takvim slučajevima NHRC može prema potrebi zatražiti dodatne informacije od čelnika relevantne agencije (koji taj zahtjev mora ispuniti u dobroj vjeri) kako bi se omogućilo da se preispita je li odbijanje dostavljanja informacija opravdano.

([276]) Članak 25. stavci 1. i 3. Zakona o NHRC-u.

([277]) Članak 25. stavak 4. Zakona o NHRC-u.

([278]) Primjerice, u razdoblju od 2015. do 2019. NHRC je godišnje zaprimio od 1 380 do 1 699 zahtjeva protiv tijelâ kaznenog progona i obradio podjednako visok broj tih zahtjeva (npr. 2018. obradio je 1 546 pritužbi protiv policije, a 2019. 1 249 pritužbi); osim toga, proveo je i nekoliko istraga po službenoj dužnosti, kako je detaljnije opisano u godišnjem izvješću NHRC-a za 2018. (dostupno na https://www.humanrights.go.kr/site/program/board/basicboard/view?menuid=002003003001&pagesize=10&boardtypeid=7017&boardid=7602641) i godišnjem izvješću za 2019. (dostupno na https://www.humanrights.go.kr/site/program/board/basicboard/view?menuid=002003003001&pagesize=10&boardtypeid=7017&boardid=7606217).

([279]) Članci 20. i 24. Zakona o Revizijskom i inspekcijskom odboru (Zakon o BAI-ju). Vidjeti Prilog II., odjeljak 2.3.2.

([280]) Članak 2. stavak 1. Zakona o BAI-ju.

([281]) Članak 2. stavak 2. Zakona o BAI-ju.

([282]) Članak 4. stavak 1. Zakona o BAI-ju.

([283]) Članak 5. stavak 1. i članak 6. Zakona o BAI-ju.

([284]) Na primjer, moraju imati najmanje deset godina staža na položaju suca, javnog tužitelja ili odvjetnika, najmanje osam godina rada kao javni službenici ili kao profesori (ili osobe na višem položaju) na sveučilištu ili najmanje deset godina rada u poduzeću uvrštenom na burzu ili instituciji u koju ulaže država (od čega najmanje pet godina na položaju izvršnog direktora); vidjeti članak 7. Zakona o BAI-ju. Osim toga, povjerenicima je zabranjeno sudjelovati u političkim aktivnostima i istodobno obnašati dužnosti u Nacionalnoj skupštini, upravnim agencijama, organizacijama u kojima BAI provodi reviziju i inspekcijski pregled ili biti na bilo kojoj drugoj plaćenoj dužnosti ili položaju (članak 9. Zakona o BAI-ju).

([285]) Članak 8. Zakona o BAI-ju.

([286]) Vidjeti npr. članak 27. Zakona o BAI-ju.

([287]) Članak 24. i članci od 31. do 35. Zakona o BAI-ju.

([288]) Članak 128. Zakona o Nacionalnoj skupštini te članci 2., 3. i 15. Zakona o inspekcijskom pregledu i istrazi državne uprave. To uključuje godišnje inspekcijske preglede vladinih poslova u cjelini, ali i istrage posebnih pitanja.

([289]) Vidjeti Prilog, odjeljak 2.2.3.

([290]) Članak 10. stavak 1. Zakona o inspekcijskom pregledu i istrazi državne uprave. Vidjeti i članke 128. i 129. Zakona o Nacionalnoj skupštini.

aktivnosti) ([291]) i javno objavljivati rezultate svojih nalaza ([292]). Ako Nacionalna skupština zatraži poduzimanje korektivnih mjera – koje mogu, primjerice, uključivati isplatu naknade štete, poduzimanje stegovnih mjera ili poboljšanje internih postupaka – predmetno javno tijelo mora djelovati bez odgode i izvijestiti Nacionalnu skupštinu o ishodu ([293]).

3.2.4. *Pravna zaštita*

(175) Korejski sustav pruža razne mogućnosti za dobivanje (sudske) pravne zaštite, uključujući naknadu za štetu.

(176) Prvo, pojedinci na temelju PIPA-e imaju pravo na pristup, ispravak, brisanje i suspenziju u odnosu na osobne podatke koje obrađuju tijela kaznenog progona ([294]).

(177) Drugo, pojedinci mogu koristiti razne mehanizme pravne zaštite koji se pružaju na temelju PIPA-e ako je tijelo kaznenog progona obrađivalo njihove podatke suprotno odredbama PIPA-e ili kršeći ograničenja i zaštitne mjere iz drugih zakona kojima se uređuje prikupljanje osobnih podataka (tj. iz CPA-a ili CPPA-a, vidjeti uvodnu izjavu 171.). Pojedinci u prvom redu mogu podnijeti pritužbu PIPC-u (među ostalim preko Pozivnog centra za zaštitu privatnosti, kojim upravlja Korejska agencija za internet i sigurnost ([295])) ili Odboru za posredovanje u sporovima o osobnim informacijama ([296]). Na te mogućnosti pravne zaštite ne primjenjuju se daljnji zahtjevi o dopuštenosti. Nadalje, na temelju Zakona o upravnim sporovima pojedinci se mogu žaliti na odluke ili nepostupanje PIPC-a ili ih osporavati (vidjeti uvodnu izjavu 132.).

(178) Treće, svaki pojedinac ([297]) može podnijeti pritužbu NHRC-u o povredi prava na privatnost i zaštitu podataka koju je počinilo korejsko tijelo kaznenog progona. NHRC može preporučiti ispravak ili poboljšanje bilo kojeg relevantnog propisa, institucije, politike ili prakse ([298]) ili provedbu pravnih lijekova kao što su posredovanje ([299]), prestanak povrede ljudskih prava, nadoknada štete i mjere za sprečavanje ponavljanja istih ili sličnih povreda ([300]). Prema službenoj izjavi korejske vlade (odjeljak 2.4.2. Priloga II.), to može uključivati i brisanje nezakonito prikupljenih osobnih podataka. Iako nema ovlast izdavanja obvezujućih odluka, NHRC pruža neformalniju, jeftinu i lako dostupnu mogućnost pravne zaštite, ponajprije zbog toga što se, kako je objašnjeno u odjeljku 2.4.2. Priloga II., pred NHRC-om ne zahtijeva činjenično dokazivanje štete da bi se pritužba istražila ([301]). Time se osigurava da se pritužbe pojedinaca u vezi s prikupljanjem njihovih podataka mogu istražiti čak i ako pojedinac nije u mogućnosti dokazati da su njegovi podaci stvarno prikupljeni (npr. zato što još nije obaviješten). Godišnje izvješće o aktivnostima NHRC-a pokazuje da pojedinci u praksi koriste i tu mogućnost kako bi osporili aktivnosti tijela kaznenog progona, među ostalim i u pogledu postupanja s osobnim podacima ([302]). Ako pojedinac nije zadovoljan ishodom postupka pred NHRC-om, može osporavati odluke (kao što je odluka da se istraga pritužbe

([291]) Članak 16. stavak 2. Zakona o inspekcijskom pregledu i istrazi državne uprave.
([292]) Članak 12-2. Zakona o inspekcijskom pregledu i istrazi državne uprave.
([293]) Članak 16. stavak 3. Zakona o inspekcijskom pregledu i istrazi državne uprave.
([294]) To se pravo može ostvariti izravno u odnosu na nadležno tijelo ili neizravno preko PIPC-a (članak 35. stavak 2. PIPA-e). Kako je detaljnije opisano u uvodnim izjavama od 76. do 78., iznimke od tih prava primjenjivat će se samo kad je to potrebno radi zaštite važnih (javnih) interesa.
([295]) Članak 62. PIPA-e.
([296]) Članci od 40. do 50. PIPA-e i članci od 48-2. do 57. Dekreta o izvršavanju PIPA-e. Vidjeti i Prilog II., odjeljak 2.4.1.
([297]) Kako je objašnjeno u odjeljku 2.4.2. Priloga II., iako se u članku 4. Zakona o NHRC-u upućuje na građane i strane državljane koji borave u Republici Koreji, pojam „boravak" odnosi se na nadležnost, a ne na državno područje. Stoga, ako nacionalne institucije unutar Koreje povrijede temeljna prava stranog državljanina izvan Koreje, taj pojedinac može podnijeti pritužbu NHRC-u. To bi bio slučaj ako bi korejska javna tijela nezakonito pristupila osobnim podacima stranog državljanina koji su preneseni u Koreju. Vidjeti naročito objašnjenja navedena na stranici https://www.humanrights.go.kr/site/program/board/basicboard/list?boardtypeid=7025&menuid=002004005001&pagesize=10&currentpage=2.
([298]) Članak 44. Zakona o NHRC-u.
([299]) Pojedinac može i zatražiti rješavanje pritužbe posredovanjem, vidjeti članak 42. i dalje Zakona o NHRC-u.
([300]) Članak 42. stavak 4. Zakona o NHRC-u. Nadalje, NHRC može donijeti hitne mjere pomoći ako se zanemari povreda koja je u tijeku i kojom će se vjerojatno uzrokovati šteta koju će biti teško popraviti; vidjeti članak 48. Zakona o NHRC-u.
([301]) Pritužba se u načelu mora podnijeti unutar godine dana od povrede, ali NHRC može i dalje odlučiti istražiti pritužbu koja je podnesena nakon isteka tog roka ako nije nastupila zastara na temelju kaznenog ili građanskog prava (članak 32. stavak 1. točka 4. Zakona o NHRC-u).
([302]) Na primjer, NHRC je u prošlosti rješavao pritužbe i izdavao preporuke u vezi s nezakonitim zapljenama i kršenjem zahtjeva da se pojedinci moraju obavijestiti o zapljeni (vidjeti stranice 80 i 91 u godišnjem izvješću NHRC-a za 2018., koje je dostupno na https://www.humanrights.go.kr/site/program/board/basicboard/view?menuid=002003003001&pagesize=10&boardtypeid=7017&boardid=7604746) te u vezi s nezakonitom obradom osobnih informacija koju su provodili policija, tužiteljstvo i sudovi (vidjeti stranice 157 i 158 u godišnjem izvješću NHRC-a za 2017., koje je dostupno na https://www.humanrights.go.kr/site/program/board/basicboard/view?menuid=002003003001&pagesize=10&boardtypeid=7017&boardid=7603308, i stranicu 76 u godišnjem izvješću NHRC-a za 2019., koje je dostupno na https://www.humanrights.go.kr/site/program/board/basicboard/view?menuid=002003003001&pagesize=10&boardtypeid=7017&boardid=7606217).

ne nastavi ([303])) i preporuke NHRC-a pred korejskim sudovima na temelju Zakona o upravnim sporovima (vidjeti uvodnu izjavu 181.) ([304]). Nadalje, postupak pred NHRC-om može dodatno olakšati pristup sudovima, s obzirom na to da bi pojedinac mogao tražiti daljnju pravnu zaštitu protiv javnog tijela koje je nezakonito obrađivalo njegove podatke na temelju nalaza NHRC-a, u skladu s postupcima opisanima u uvodnim izjavama od 181. do 183.

(179) Konačno, dostupni su razni sudski pravni lijekovi, kojima se pojedincima omogućuje da se pozivaju na ograničenja i zaštitne mjere opisane u odjeljku 3.2.1. radi dobivanja pravne zaštite ([305]).

(180) Kad je riječ o zapljenama (uključujući zapljene podataka), CPA-om se predviđa mogućnost ulaganja prigovora na izvršenje naloga ili osporavanja izvršenja naloga „kvazi-pritužbom", to jest upućivanjem nadležnom sudu zahtjeva za poništenje ili izmjenu odluke koju je donio tužitelj ili policijski službenik ([306]).

(181) Općenitije govoreći, pojedinci mogu osporavati djelovanja ([307]) ili propuste ([308]) tijela javne vlasti (uključujući tijela kaznenog progona) na temelju Zakona o upravnim sporovima ([309]). Upravno djelovanje smatra se „osporivom odlukom" ako izravno utječe na građanska prava i dužnosti ([310]), što je, kako je potvrdila korejska vlada (odjeljak 2.4.3. Priloga II.), slučaj s mjerama za prikupljanje osobnih podataka, bez obzira na to provode li se one izravno (primjerice, presretanjem komunikacija), obvezujućim zahtjevima za otkrivanje (primjerice, zahtjevima upućenima pružatelju usluge) ili zahtjevima za dobrovoljnu suradnju. Da bi pritužba na temelju Zakona o upravnim sporovima bila dopuštena, pojedinac mora imati pravni interes za podnošenje zahtjeva ([311]). Prema sudskoj praksi Vrhovnog suda „pravni interes" tumači se kao „pravno zaštićeni interes", tj. izravan i konkretan interes zaštićen zakonima i propisima na kojima se temelje upravne odluke (to znači da taj interes ne može biti opći, neizravan i apstraktan interes javnosti) ([312]). Pojedinci imaju takav pravni interes u slučaju svakog kršenja ograničenja i zaštitnih mjera koji se primjenjuju na prikupljanje njihovih osobnih podataka za potrebe kaznenog progona (na temelju posebnih zakona ili PIPA-e). Na temelju Zakona o upravnim sporovima sud može odlučiti poništiti ili izmijeniti nezakonitu odluku, izdati proglašenje ništavosti (tj. proglašenje da odluka nema pravni učinak ili da je pravno nepostojeća) ili izdati proglašenje propusta nezakonitim ([313]). Pravomoćna presuda na temelju Zakona o upravnim sporovima obvezujuća je za stranke ([314]).

([303]) Na primjer, ako NHRC iznimno ne može pregledati određene materijale ili objekte jer su povezani s državnim tajnama koje bi mogle imati znatne posljedice na državnu sigurnost ili diplomatske odnose ili ako bi inspekcijski pregled činio ozbiljnu prepreku u kaznenoj istrazi ili sudskom postupku u tijeku i ako to sprečava NHRC da provodi istragu potrebnu za ocjenu utemeljenosti zaprimljenog zahtjeva, obavijestit će pojedinca o razlozima zbog kojih je pritužba odbijena u skladu s člankom 39. Zakona o NHRC-u. U tom bi slučaju pojedinac mogao osporiti odluku NHRC-a na temelju Zakona o upravnim sporovima.

([304]) Vidjeti npr. Odluku Visokog suda u Seoulu 2007Nu27259 od 18. travnja 2008., koja je potvrđena u Odluci Vrhovnog suda 2008Du7854 od 9. listopada 2008., i Odluku Visokog suda u Seoulu 2017Nu69382 od 2. veljače 2018.

([305]) Vidjeti Prilog II., odjeljak 2.4.3.

([306]) Članak 417. CPA-a u vezi s člankom 414. stavkom 2. CPA-a. Vidjeti i Odluku Vrhovnog suda br. 97Mo66 od 29. rujna 1997.

([307]) U Zakonu o upravnim sporovima navodi se pojam „odluka", tj. izvršavanje ili odbijanje izvršavanja javne ovlasti u određenom slučaju.

([308]) Prema Zakonu o upravnim sporovima pod tim se pojmom podrazumijeva situacija u kojoj upravna agencija dulje vrijeme ne donese određenu odluku iako je pravno obvezna učiniti to.

([309]) Upravno osporavanje može se, kao neformalnija mogućnost za dobivanje pravne zaštite, najprije pokrenuti pred povjerenstvima za upravne žalbe osnovanima u okviru određenih tijela javne vlasti (npr. NIS ili NHRC) ili pred Središnjim povjerenstvom za upravne žalbe osnovanim u okviru Povjerenstva za borbu protiv korupcije i civilna prava (članak 6. Zakona o upravnim žalbama i članak 18. stavak 1. Zakona o upravnim sporovima). Međutim, zahtjev se može podnijeti i izravno korejskim sudovima na temelju Zakona o upravnim sporovima.

([310]) Odluka Vrhovnog suda 98Du18435 od 22. listopada 1999., Odluka Vrhovnog suda 99Du1113 od 8. rujna 2000. i Odluka Vrhovnog suda 2010Du3541 od 27. rujna 2012.

([311]) Članci 12., 35. i 36. Zakona o upravnim sporovima. Osim toga, zahtjev za poništenje/izmjenu odluke i zahtjev za potvrdu nezakonitosti propusta moraju se podnijeti u roku od 90 dana od datuma na koji pojedinac sazna za odluku/propust, a u načelu najkasnije godinu dana od datuma izdavanja odluke ili datuma kad se dogodio propust, osim ako postoje opravdani razlozi (članak 20. i članak 38. stavak 2. Zakona o upravnim sporovima). Vrhovni sud široko tumači pojam „opravdani razlozi" i zahtijeva procjenu toga je li društveno prihvatljivo dopustiti zakašnjelo podnošenje pritužbe uzimajući u obzir sve okolnosti predmeta (Odluka Vrhovnog suda 90Nu6521 od 28. lipnja 1991.). Kako je to potvrdila korejska vlada u odjeljku 2.4.3. Priloga II., to uključuje (među ostalim) razloge za odgodu za koje se predmetna stranka ne može smatrati odgovornom (tj. situacije koje su izvan kontrole podnositelja pritužbe, na primjer ako nije bio obaviješten o prikupljanju njegovih osobnih informacija) ili višu silu (npr. prirodne katastrofe ili rat).

([312]) Odluka Vrhovnog suda br. 2006Du330 od 26. ožujka 2006.

([313]) Članci 2. i 4. Zakona o upravnim sporovima.

([314]) Članak 30. stavak 1. Zakona o upravnim sporovima.

(182) Osim osporavanja postupaka vlade upravnim sporom pojedinci mogu podnijeti i ustavnu tužbu Ustavnom sudu o bilo kojoj povredi njihovih temeljnih prava zbog izvršavanja ili neizvršavanja državnih ovlasti (ne uključujući sudske presude) ([315]). Najprije treba iskoristiti druge pravne lijekove ako su dostupni. Prema sudskoj praksi Ustavnog suda strani državljani mogu podnijeti ustavnu tužbu ako su njihova osnovna prava priznata korejskim Ustavom (vidjeti objašnjenja u odjeljku 1.1.) ([316]). Ustavni sud može proglasiti nevažećim izvršavanje državnih ovlasti koje je prouzročilo povredu ili potvrditi da je određeno nečinjenje protuustavno ([317]). U tom se slučaju od relevantnog tijela zahtijeva da poduzme mjere radi usklađivanja s odlukom Suda.

(183) Nadalje, pojedinci mogu pred korejskim sudovima ishoditi naknadu za štetu. To prije svega uključuje mogućnost traženja naknade štete za povrede PIPA-e koje su počinila tijela kaznenog progona, u skladu s člankom 39. (vidjeti i uvodnu izjavu 135.). Općenitije govoreći, na temelju Zakona o naknadi štete od države pojedinci mogu podnijeti zahtjev za naknadu štete koju su nanijeli javni službenici pri izvršenju svojih službenih dužnosti u suprotnosti sa zakonom (vidjeti i uvodnu izjavu 135.) ([318]).

(184) Mehanizmima opisanima u uvodnim izjavama od 176. do 183. ispitanicima se osiguravaju djelotvorni upravni i sudski pravni lijekovi, što im prije svega omogućuje da ostvaruju svoja prava, uključujući pravo na pristup svojim osobnim podacima te ispravak ili brisanje tih podataka.

3.3. **Pristup korejskih tijela javne vlasti podacima i njihova upotreba za potrebe nacionalne sigurnosti**

(185) Pravo Republike Koreje sadržava brojna ograničenja i zaštitne mjere u pogledu pristupa osobnim podacima i njihove upotrebe za potrebe nacionalne sigurnosti te se njime predviđaju mehanizmi nadzora i pravne zaštite koji su u skladu sa zahtjevima iz uvodnih izjava od 141. do 143. ove Odluke. Uvjeti pod kojima je takav pristup moguć i zaštitne mjere koje se primjenjuju na upotrebu tih ovlasti detaljno se ocjenjuju u odjeljcima u nastavku.

3.3.1. *Pravne osnove, ograničenja i zaštitne mjere*

(186) U Republici Koreji osobnim podacima smije se pristupati za potrebe nacionalne sigurnosti na temelju CPPA-a, TBA-a i Zakona o borbi protiv terorizma radi zaštite građana i javne sigurnosti (Zakon o borbi protiv terorizma) ([319]). Glavno tijelo ([320]) s nadležnostima u području nacionalne sigurnosti je Nacionalna obavještajna služba (NIS) ([321]). Prikupljanje i upotreba osobnih podataka koje provodi NIS moraju biti u skladu s relevantnim

([315]) Članak 68. stavak 1. Zakona o Ustavnom sudu. Ustavne tužbe moraju se podnijeti u roku od 90 dana od trenutka kad je pojedinac saznao za povredu i u roku od godine dana od njezina počinjenja. Kako je objašnjeno i u odjeljku 2.4.3. Priloga II., s obzirom na to da se postupak iz Zakona o upravnim sporovima primjenjuje na sporove na temelju Zakona o Ustavnom sudu u skladu s člankom 40. Zakona o Ustavnom sudu, pritužba će i dalje biti dopuštena ako postoje „opravdani razlozi" prema tumačenju iz sudske prakse Vrhovnog suda opisane u bilješci 312. Ako se najprije moraju iskoristiti drugi pravni lijekovi, ustavna tužba mora se podnijeti u roku od 30 dana od pravomoćne odluke o takvom pravnom lijeku (članak 69. Zakona o Ustavnom sudu).

([316]) Odluka Ustavnog suda br. 99HeonMa194 od 29. studenoga 2001.

([317]) Članak 75. stavak 3. Zakona o Ustavnom sudu.

([318]) Članak 2. stavak 1. Zakona o naknadi štete od države.

([319]) Vidjeti Prilog II., odjeljak 3.1.

([320]) Iznimno, policija i tužiteljstvo isto tako mogu prikupljati osobne informacije za potrebe nacionalne sigurnosti (vidjeti bilješku 327. i Prilog II., odjeljak 3.2.1.2.). Osim toga, ovlasti u području nacionalne sigurnosti ima i korejska vojna obavještajna agencija (Sigurnosno-obrambeno zapovjedništvo za podršku, koje je osnovano u okviru Ministarstva obrane). Međutim, kako je objašnjeno u odjeljku 3.1. Priloga II., ona je nadležna samo za vojni obavještajni rad, a nadzor nad civilima provodi samo ako je to potrebno za izvršavanje njezinih vojnih funkcija. Konkretno, smije provoditi istrage samo nad vojnim osobljem, civilnim zaposlenicima vojske, osobama u vojnoj obuci, osobama u vojnoj pričuvi ili službi novačenja i ratnim zarobljenicima (članak 1. Zakona o vojnim sudovima). Pri prikupljanju informacija o komunikaciji za potrebe nacionalne sigurnosti Sigurnosno-obrambeno zapovjedništvo za podršku podliježe ograničenjima i zaštitnim mjerama utvrđenima u CPPA-u i njegovu dekretu o izvršavanju.

([321]) NIS ima zadaću prikupljati, kompilirati i distribuirati informacije o stranim državama (tj. opće informacije o trendovima i kretanjima u odnosu na strane države ili o aktivnostima državnih subjekata); obavještajne podatke povezane sa suzbijanjem špijunaže (uključujući vojnu i industrijsku špijunažu), terorizma i aktivnosti međunarodnih zločinačkih udruženja; obavještajne podatke o određenim vrstama kaznenih djela usmjerenih protiv javne i nacionalne sigurnosti (npr. unutarnje pobune, strana agresija) i obavještajne podatke povezane sa zadaćom osiguravanja kibersigurnosti i sprečavanja ili suzbijanja kibernapada i prijetnji (članak 4. stavak 2. Zakona o NIS-u). Vidjeti i Prilog II., odjeljak 3.1.

pravnim zahtjevima (uključujući PIPA-u i CPPA) ([322]) te općim smjernicama koje izrađuje predsjednik države i preispituje Nacionalna skupština ([323]). NIS u pravilu mora ostati politički neutralan te štititi slobodu i prava pojedinaca ([324]). Osim toga, osoblje NIS-a ne smije zloupotrebljavati svoje službene ovlasti kako bi prisililo bilo koju instituciju, organizaciju ili pojedinca da učine nešto što nisu obvezni činiti (na temelju zakona) niti smije sprečavati bilo koju osobu u ostvarivanju svojih prava ([325]).

3.3.1.1. Pristup informacijama o komunikaciji

(187) Na temelju CPPA-a korejska tijela javne vlasti ([326]) smiju prikupljati podatke o potvrdi komunikacije (tj. datum telekomunikacija, njihovo vrijeme početka i završetka, broj odlaznih i dolaznih poziva te pretplatnički broj druge strane, učestalost upotrebe, zapisnike o upotrebi telekomunikacijskih usluga i informacije o lokaciji; vidjeti uvodnu izjavu 155.) i sadržaj komunikacija (primjenom mjera ograničavanja komunikacije; vidjeti uvodnu izjavu 155.) za potrebe nacionalne sigurnosti (kako je utvrđeno zadaćama NIS-a, vidjeti bilješku 322.). Te ovlasti obuhvaćaju dvije vrste informacija: 1. komunikacije u kojima su jedan ili oba sudionika korejski državljani ([327]); i 2. komunikacije (a) država koje su neprijatelji Republike Koreje, (b) stranih agencija, skupina ili državljana koje se sumnjiči za sudjelovanje u aktivnostima protiv Koreje ([328]) ili (c) članova skupina koje djeluju na Korejskom poluotoku, ali u stvarnosti nisu pod suverenom vlašću Republike Koreje i njihovih krovnih skupina koje se nalaze u stranim državama ([329]). Stoga se komunikacije pojedinaca iz EU-a koje su prenesene iz Unije u Republiku Koreju na temelju ove Odluke smiju za potrebe nacionalne sigurnosti prikupljati samo na temelju CPPA-a (pod uvjetima navedenima u uvodnim izjavama od 188. do 192.) ako je riječ o komunikacijama između pojedinca iz EU-a i korejskog državljanina ili ako se odnose na komunikacije isključivo između osoba koje nemaju korejsko državljanstvo te ako su obuhvaćene nekom od triju prethodno navedenih kategorija 2.a, 2.b i 2.c.

(188) U oba scenarija prikupljanje podataka o potvrdi komunikacije smije se provoditi samo u svrhu sprečavanja prijetnji nacionalnoj sigurnosti ([330]), a mjere ograničavanja komunikacije smiju se poduzimati samo ako postoji ozbiljan rizik za nacionalnu sigurnost te je prikupljanje podataka neophodno za njegovo sprečavanje ([331]). Osim toga, pristupanje sadržaju komunikacija dopušteno je samo kao krajnja mjera te se povreda privatnosti komunikacija mora nastojati svesti na najmanju mjeru ([332]), čime se osigurava da ta mjera ostane proporcionalna cilju nacionalne sigurnosti koji se nastoji ostvariti. Prikupljanje sadržaja komunikacija i podataka o potvrdi komunikacije smije trajati najviše četiri mjeseca i mora se odmah prekinuti ako se predviđeni cilj ostvari ranije ([333]). Ako relevantni uvjeti i dalje budu ispunjeni, to se razdoblje može produljiti za najviše četiri mjeseca, uz prethodno dopuštenje suda (za mjere opisane u uvodnoj izjavi 189.) ili predsjednika države (za mjere opisane u uvodnoj izjavi 190.) ([334]).

(189) Iste postupovne zaštitne mjere primjenjuju se na prikupljanje podataka o potvrdi komunikacije i sadržaja komunikacija ([335]). Konkretno, ako je barem jedan od pojedinaca uključenih u komunikaciju korejski državljanin, obavještajna agencija mora podnijeti pisani zahtjev uredu višeg javnog tužitelja, koji pak mora podnijeti

([322]) Vidjeti i članke 14., 22. i 23. Zakona o NIS-u.
([323]) Članak 4. stavak 2. Zakona o NIS-u.
([324]) Članak 3. stavak 1., članak 6. stavak 2., članak 11. i članak 21. Zakona o NIS-u. Vidjeti i pravila o sukobu interesa, osobito članke 10. i 12. Zakona o NIS-u.
([325]) Članak 13. Zakona o NIS-u.
([326]) To uključuje obavještajne agencije (tj. NIS i Sigurnosno-obrambeno zapovjedništvo za podršku) i policiju/tužiteljstvo.
([327]) Članak 7. stavak 1. točka 1. CPPA-a.
([328]) Kako je objasnila korejska vlada u bilješci 244. Priloga II., to se odnosi na aktivnosti kojima se ugrožavaju postojanje i sigurnost države, demokratski poredak ili život i sloboda građana.
([329]) Članak 7. stavak 1. točka 2. CPPA-a.
([330]) Članak 13-4. CPPA-a.
([331]) Članak 7. stavak 1. CPPA-a.
([332]) Članak 3. stavak 2. CPPA-a. Osim toga, mjere ograničavanja komunikacije moraju se prekinuti odmah nakon što prestanu biti nužne, čime se osigurava da svaka povreda komunikacijskih tajni pojedinca bude svedena na najmanju mjeru (članak 2. Dekreta o izvršavanju CPPA-a).
([333]) Članak 7. stavak 2. CPPA-a.
([334]) Zahtjev za dobivanje odobrenja za produljenje mjera nadzora mora se uputiti u pisanom obliku te se moraju navesti razlozi za traženje produljenja i priložiti popratni materijali (članak 7. stavak 2. CPPA-a i članak 5. Dekreta o izvršavanju CPPA-a).
([335]) Vidjeti članak 13-4. stavak 2. CPPA-a i članak 37. stavak 4. Dekreta o izvršavanju CPPA-a, prema kojima se postupci primjenjivi na prikupljanje sadržaja komunikacija primjenjuju i na prikupljanje podataka o potvrdi komunikacije. Vidjeti i Prilog II., odjeljak 3.2.1.1.1.

zahtjev za nalog višem predsjedniku Visokog suda ([336]). U CPPA-u se navode informacije koje se moraju navesti u zahtjevu tužitelju, zahtjevu za nalog i samom nalogu, a one konkretno uključuju obrazloženje zahtjeva i glavne osnove za sumnju, popratne materijale te informacije o svrsi, cilju (tj. ciljanim pojedincima), opsegu i trajanju predložene mjere ([337]). Prikupljanje bez naloga smije se provoditi samo ako postoji zavjera koja čini prijetnju nacionalnoj sigurnosti i izvanredna situacija zbog koje nije moguće provesti navedene postupke ([338]). Međutim, i u tom se slučaju zahtjev za nalog mora podnijeti odmah nakon poduzimanja mjere ([339]). Stoga se CPPA-om jasno utvrđuju opseg i uvjeti tih vrsta prikupljanja te se oni uvjetuju primjenom određenih (postupovnih) zaštitnih mjera (uključujući prethodno sudsko odobrenje), čime se osigurava da primjena tih mjera prikupljanja bude ograničena na ono što je nužno i proporcionalno. Nadalje, zahtjevom o navođenju detaljnih informacija i u zahtjevu za nalog i u samom nalogu isključuje se mogućnost neselektivnog pristupa.

(190) Za komunikacije između osoba koje nisu korejski državljani, a koje su obuhvaćene nekom od triju posebnih kategorija navedenih u uvodnoj izjavi 187., mora se podnijeti zahtjev direktoru NIS-a, koji, nakon što provjeri prikladnost predloženih mjera, mora zatražiti prethodno pisano odobrenje Predsjednika Republike Koreje ([340]). Zahtjev koji sastavlja obavještajna agencija mora uključivati iste detaljne informacije kao i zahtjev za sudski nalog (vidjeti uvodnu izjavu 189.), a ponajprije obrazloženje zahtjeva i glavne osnove za sumnju, popratne materijale te informacije o svrhama, ciljanim pojedincima, opsegu i trajanju predloženih mjera ([341]). U izvanrednim situacijama ([342]) mora se ishoditi prethodno odobrenje ministra u čijoj je nadležnosti relevantna obavještajna agencija, iako ta obavještajna agencija mora zatražiti odobrenje predsjednika odmah nakon poduzimanja hitnih mjera ([343]). Stoga se, isto u pogledu prikupljanja komunikacija između isključivo osoba koje nisu korejski državljani, CPPA-om ograničava primjena tih mjera na ono što je nužno i proporcionalno, jasnim sužavanjem ograničenih kategorija pojedinaca na koje se takve mjere smiju primjenjivati i utvrđivanjem detaljnih kriterija za koje obavještajne agencije moraju dokazati da su ispunjeni kako bi opravdale zahtjev za prikupljanje informacija. Nadalje, time se još jednom isključuje mogućnost neselektivnog pristupa. Iako se za takve mjere ne traži prethodno neovisno odobrenje, osigurava se naknadni neovisni nadzor, koji ponajprije provode PIPC i NHRC (vidjeti na primjer uvodne izjave 199. i 200.).

(191) CPPA-om se nadalje uvodi nekoliko dodatnih zaštitnih mjera kojima se pridonosi naknadnom nadzoru i olakšava pojedincima pristup djelotvornim pravnim lijekovima. Prvo, u pogledu bilo koje vrste prikupljanja za potrebe nacionalne sigurnosti, CPPA-om se predviđaju razni zahtjevi o vođenju evidencije i izvješćivanju. Konkretno, kad se zahtijeva suradnja privatnih subjekata, obavještajne agencije moraju predočiti sudski nalog/dopuštenje predsjednika ili presliku naslovnice izjave o hitnoj cenzuri, što subjekt koji se prisiljava na suradnju mora čuvati u svojim evidencijama ([344]). Kad su privatni subjekti prisiljeni na suradnju, i javno tijelo koje zahtijeva suradnju

([336]) Članak 6. stavci 5. i 8., članak 7. stavak 1. točka 1. i članak 7. stavak 3. CPPA-a u vezi s člankom 7. stavcima 3. i 4. Dekreta o izvršavanju CPPA-a.

([337]) Vidjeti članak 7. stavak 3. i članak 6. stavak 4. CPPA-a (za zahtjev obavještajne agencije), članak 4. Dekreta o izvršavanju CPPA-a (za zahtjev tužitelja) te članak 7. stavak 3. i članak 6. stavak 6. CPPA-a (za nalog).

([338]) Članak 8. CPPA-a.

([339]) Članak 8. stavci 2. i 8. CPPA-a. Prikupljanje se mora odmah prekinuti ako se dopuštenje suda ne ishodi u roku od 36 sati od trenutka poduzimanja mjera. Ako se nadzor dovrši u kratkom roku, čime dopuštenje suda postaje bespredmetno, čelnik nadležnog ureda višeg javnog tužitelja mora čelniku nadležnog suda poslati obavijest o hitnoj mjeri koju je sastavila obavještajna agencija, na temelju koje sud može preispitati zakonitost prikupljanja (članak 8. stavci 5. i 7. CPPA-a). U toj se obavijesti moraju navesti svrha, cilj, opseg, razdoblje, mjesto izvršenja i metoda nadzora te razlozi zbog kojih zahtjev nije podnesen prije poduzimanja mjere (članak 8. stavak 6. CPPA-a). Općenitije govoreći, obavještajne agencije smiju hitne mjere poduzimati samo u skladu s „izjavom o hitnoj cenzuri/prisluškivanju” te moraju o njima voditi evidencije (članak 8. stavak 4. CPPA-a).

([340]) Članak 8. stavci 1. i 2. Dekreta o izvršavanju CPPA-a.

([341]) Članak 8. stavak 3. Dekreta o izvršavanju CPPA-a u vezi s člankom 6. stavkom 4. CPPA-a.

([342]) To jest u slučajevima u kojima je cilj mjere zavjera koja čini prijetnju nacionalnoj sigurnosti, ako nema dovoljno vremena za dobivanje odobrenja predsjednika i ako nepoduzimanje hitnih mjera može narušiti nacionalnu sigurnost (članak 8. stavak 8. CPPA-a).

([343]) Članak 8. stavak 9. CPPA-a. Prikupljanje se mora odmah prekinuti ako se dopuštenje ne ishodi u roku od 36 sati od trenutka podnošenja zahtjeva za dopuštenje.

([344]) Članak 9. stavak 2. CPPA-a i članak 12. Dekreta o izvršavanju CPPA-a. Vidjeti članak 13. Dekreta o izvršavanju CPPA-a o mogućnosti da se poštanski uredi i pružatelji telekomunikacijskih usluga prisile na pružanje pomoći. Privatni subjekti od kojih se zatraži otkrivanje informacija mogu odbiti to učiniti ako se nalog/odobrenje ili izjava o hitnoj cenzuri odnose na pogrešan identifikator (npr. telefonski broj koji pripada nekoj drugoj osobi, a ne utvrđenom pojedincu). U svakom slučaju zabranjeno im je otkrivati lozinke za komunikacije (članak 9. stavak 4. CPPA-a).

i relevantni subjekt moraju čuvati evidencije o svrsi i predmetu mjera te o datumu izvršenja ([345]). Osim toga, obavještajne agencije moraju izvješćivati direktora NIS-a o informacijama koje su prikupile i ishodu aktivnosti nadzora ([346]).

(192) Drugo, pojedinci se moraju obavijestiti o prikupljanju njihovih podataka (podataka o potvrdi komunikacije ili sadržaja komunikacija) za potrebe nacionalne sigurnosti ako se to odnosi na komunikacije u kojima je barem jedan od sudionika korejski državljanin ([347]). Ta se obavijest mora dostaviti u pisanom obliku u roku od 30 dana od datuma na koji je prikupljanje završilo (među ostalim i ako su podaci pribavljeni u skladu s izvanrednim postupkom) te se može odgoditi ako i onoliko dugo koliko bi se njome dovela u pitanje nacionalna sigurnost ili ugrozio život i fizička sigurnost građana ([348]). Bez obzira na tu obavijest, pojedinci mogu dobiti pravnu zaštitu na više načina, kako je detaljnije objašnjeno u odjeljku 3.3.4.

3.3.1.2. Prikupljanje informacija o osumnjičenicima za terorizam

(193) U Zakonu o borbi protiv terorizma predviđa se da NIS smije prikupljati podatke o osumnjičenicima za terorizam ([349]) u skladu s ograničenjima i zaštitnim mjerama utvrđenima u drugim zakonima ([350]). Konkretno, NIS smije pribavljati podatke o komunikacijama (na temelju CPPA-a) i druge osobne informacije (zahtjevom za dobrovoljno otkrivanje) ([351]). Kad je riječ o prikupljanju informacija o komunikacijama (tj. sadržaja komunikacija ili podataka o potvrdi komunikacije), primjenjuju se ograničenja i zaštitne mjere opisane u odjeljku 3.3.1.1., uključujući zahtjev za ishođenje naloga koji je odobrio sud. Kad je riječ o zahtjevima za dobrovoljno otkrivanju drugih vrsta osobnih podataka o osumnjičenicima za terorizam, NIS mora poštovati zahtjeve na temelju Ustava i PIPA-e o nužnosti i proporcionalnosti (vidjeti uvodnu izjavu 164.) ([352]). Voditelji obrade koji prime takve zahtjeve mogu postupiti sukladno njima na dobrovoljnoj osnovi pod uvjetima utvrđenima u PIPA-i (na primjer, u skladu s načelom smanjenja količine podataka i ograničavanjem učinka na privatnost pojedinca) ([353]). U tom slučaju moraju ispuniti i zahtjev za obavješćivanje predmetnog pojedinca koji proizlazi iz Obavijesti br. 2021-5 (vidjeti uvodnu izjavu 166.).

([345]) Za mjere ograničavanja komunikacije te se evidencije moraju čuvati tri godine; vidjeti članak 9. stavak 3. CPPA-a i članak 17. stavak 2. Dekreta o izvršavanju CPPA-a. Kad je riječ o podacima o potvrdi komunikacije, obavještajne agencije moraju čuvati evidencije o činjenici da je zahtjev za takve podatke upućen te o samom pisanom zahtjevu i instituciji koja se pozvala na njega (članak 13. stavak 5. i članak 13-4. stavak 3. CPPA-a). Pružatelji telekomunikacijskih usluga moraju čuvati evidencije sedam godina i dvaput godišnje izvješćivati ministra znanosti i IKT-a o učestalosti tih otkrivanja (članak 9. stavak 3. CPPA-a u vezi s člankom 13. stavkom 7. CPPA-a te člankom 37. stavkom 4. i člankom 39. Dekreta o izvršavanju CPPA-a).

([346]) Članak 18. stavak 3. Dekreta o izvršavanju CPPA-a.

([347]) Članak 9-2. stavak 3. i članak 13-4. CPPA-a. Obavijest mora uključivati 1. činjenicu da su informacije prikupljene, 2. agenciju koja je izvršila prikupljanje informacija i 3. razdoblje izvršenja.

([348]) Članak 9-2. stavak 4. CPPA-a. U tom se slučaju obavijest mora dati u roku od 30 dana nakon što osnova za odgodu prestane postojati; vidjeti članak 13-4. stavak 2. i članak 9-2. stavak 6. CPPA-a.

([349]) To jest, o članovima terorističke skupine (kako su je proglasili Ujedinjeni narodi; vidjeti članak 2. točku 2. Zakona o borbi protiv terorizma); osobama koje promiču i šire ideje ili taktike terorističke skupine, prikupljaju ili pridonose sredstva za terorizam ili sudjeluju u drugim aktivnostima pripreme, zavjere, propagiranja ili poticanja terorizma; ili osobama za koje se na temelju valjanih razloga sumnja da su se bavile takvim aktivnostima (članak 2. točka 3. Zakona o borbi protiv terorizma). „Terorizam" se definira u članku 2. točki 1. Zakona o borbi protiv terorizma kao postupanje čija je svrha narušiti izvršavanje ovlasti države, lokalne vlasti ili strane vlade (uključujući međunarodne organizacije) ili u svrhu njihova primoravanja na djelovanja na koja nisu pravno obvezna ili u svrhu prijetnje javnosti. Takvo postupanje može uključivati, primjerice, ubojstvo, otmicu ili uzimanje taoca; otmicu/preuzimanje, uništavanje ili oštećivanje broda ili zrakoplova; upotrebu biokemijskog, eksplozivnog ili zapaljivog oružja s namjerom uzrokovanja smrti, ozbiljne ozljede ili štete; i zloupotrebu nuklearnih ili radioaktivnih materijala.

([350]) Članak 9. stavci 1. i 3. Zakona o borbi protiv terorizma.

([351]) Iako se u Zakonu o borbi protiv terorizma upućuje i na mogućnost prikupljanja informacija o ulasku u Republiku Koreju i odlasku iz nje na temelju Zakona o imigraciji i Carinskog zakona, u tim se zakonima trenutačno ne predviđa takvo ovlaštenje (vidjeti odjeljak 3.2.2.1. Priloga II.). U svakom slučaju, oni se u načelu ne bi primjenjivali na podatke prenesene na temelju ove Odluke jer bi se obično odnosili na informacije koje bi izravno prikupljala korejska tijela (a ne na pristup podacima koji su prethodno preneseni iz Unije korejskim voditeljima obrade). Osim toga, u Zakonu o borbi protiv terorizma navodi se ARUSFTI kao pravna osnova za prikupljanje informacija o financijskim transakcijama. Međutim, kako je objašnjeno u bilješci 200., vrste podataka koje bi se mogle pribavljati na temelju tog zakona nisu obuhvaćene područjem primjene ove Odluke. Naposljetku, u Zakonu o borbi protiv terorizma predviđa se i da NIS smije prikupljati informacije o lokaciji putem neobvezujućih zahtjeva, a u tom bi slučaju pružatelji informacija o lokaciji mogli dobrovoljno otkriti takve informacije pod uvjetima utvrđenima u PIPA-i (kako je opisano u uvodnoj izjavi 193.) i Zakonu o informacijama o lokaciji. Međutim, kako je objašnjeno i u bilješci 17., informacije o lokaciji ne bi se prenosile iz Unije korejskim voditeljima obrade na temelju ove Odluke, već bi se umjesto toga generirale unutar Koreje.

([352]) Vidjeti Prilog II., odjeljak 3.2.2.2.

([353]) Vidjeti članak 58. stavak 4. PIPA-e, u kojem se zahtijeva da se osobne informacije obrađuju u najmanjoj mjeri koja je potrebna za predviđenu svrhu, i članak 3. stavak 6. PIPA-e, u kojem se propisuje da se osobne informacije moraju obrađivati tako da se mogućnost povrede privatnosti pojedinca svede na najmanju mjeru. Vidjeti i članak 59. točke 2. i 3. PIPA-e, u skladu s kojima se voditeljima obrade zabranjuje neovlašteno otkrivanje osobnih informacija trećim stranama.

3.3.1.3. Zahtjevi za dobrovoljno otkrivanje podataka o pretplatnicima

(194) Na temelju TBA-a pružatelji telekomunikacijskih usluga mogu dobrovoljno otkriti podatke o pretplatnicima (vidjeti uvodnu izjavu 163.) na zahtjev obavještajne agencije koja namjerava prikupljati takve informacije kako bi se spriječila prijetnja nacionalnoj sigurnosti ([354]). Kad je riječ o takvim zahtjevima koje upućuje NIS, primjenjuju se ista ograničenja (koja proizlaze iz Ustava, PIPA-e i TBA-a) kao i u području kaznenog progona, kako je navedeno u uvodnoj izjavi 164. ([355]). Pružatelji telekomunikacijskih usluga nisu dužni postupiti sukladno tim zahtjevima, a mogu to učiniti samo pod uvjetima utvrđenima u PIPA-i (prije svega u skladu s načelom smanjenja količine podataka i ograničavanjem učinka na privatnost pojedinca, vidjeti i uvodnu izjavu 193.). Primjenjuju se isti zahtjevi u vezi s vođenjem evidencija i obavješćivanjem predmetnog pojedinca kao i u području kaznenog progona (vidjeti uvodne izjave 165. i 166.).

3.3.2. *Daljnja upotreba prikupljenih informacija*

(195) Obrada osobnih podataka koje prikupljaju korejska tijela za potrebe nacionalne sigurnosti podliježe načelima ograničavanja svrhe (članak 3. stavci 1. i 2. PIPA-e), zakonitosti i poštenosti obrade (članak 3. stavak 1. PIPA-e), proporcionalnosti/smanjenja količine podataka (članak 3. stavci 1. i 6. i članak 58. PIPA-e), točnosti (članak 3. stavak 3. PIPA-e), transparentnosti (članak 3. stavak 5. PIPA-e), sigurnosti (članak 58. stavak 4. PIPA-e) i ograničenja pohrane (članak 58. stavak 4. PIPA-e) ([356]). Moguće otkrivanje osobnih podataka trećim stranama (uključujući treće zemlje) moguće je samo u skladu s tim načelima (posebice načelima ograničavanja svrhe i smanjenja količine podataka), nakon što se ocijeni usklađenost s načelima nužnosti i proporcionalnosti (članak 37. stavak 2. Ustava) i uzimajući u obzir učinak na prava dotičnih pojedinaca (članak 3. stavak 6. PIPA-e).

(196) Kad je riječ o sadržaju komunikacija i podacima o potvrdi komunikacije, upotreba tih podataka CPPA-om se dodatno ograničava na sudske postupke u kojima se stranka koja je povezana s komunikacijom oslanja na njih pri traženju naknade štete ili na upotrebe koje su dopuštene na temelju drugih zakona ([357]).

3.3.3. *Nadzor*

(197) Aktivnosti korejskih tijela za nacionalnu sigurnost nadziru različita tijela ([358]).

(198) Prvo, u Zakonu o borbi protiv terorizma predviđaju se posebni mehanizmi nadzora za aktivnosti suzbijanja terorizma, uključujući prikupljanje podataka o osumnjičenicima za terorizam. Konkretno, na razini rukovodstva, aktivnosti suzbijanja terorizma nadzire Povjerenstvo za borbu protiv terorizma ([359]), koje je direktor NIS-a dužan izvješćivati o istragama i praćenju osumnjičenika za terorizam radi prikupljanja informacija ili materijala potrebnih za aktivnosti suzbijanja terorizma ([360]). Osim toga, službenik za zaštitu ljudskih prava („HRPO”) posebno nadzire usklađenost aktivnosti suzbijanja terorizma s temeljnim pravima ([361]). HRPO-a imenuje predsjednik Povjerenstva za borbu protiv terorizma iz redova osoba koje ispunjavaju posebne uvjete navedene u Dekretu o izvršavanju Zakona o borbi protiv terorizma ([362]) na mandat od dvije godine (koji se može obnoviti) te se on može razriješiti dužnosti samo na temelju određene, ograničene osnove i zbog valjanih razloga ([363]). U

([354]) Članak 83. stavak 3. TBA-a.
([355]) Vidjeti i Prilog II., odjeljak 3.2.3.
([356]) Vidjeti Prilog II., odjeljak 1.2.
([357]) Članak 5. stavci 1. i 2., članak 12. i članak 13-5. CPPA-a.
([358]) Vidjeti Prilog II., odjeljak 3.3.
([359]) Članak 5. stavak 3. Zakona o borbi protiv terorizma. Povjerenstvom predsjedava premijer, a sastoji se od nekoliko ministara i čelnika vladinih agencija, kao što su ministar vanjskih poslova, ministar pravosuđa, ministar nacionalne obrane, ministar unutarnjih poslova i sigurnosti, direktor NIS-a i glavni načelnik Nacionalne policijske agencije (članak 3. stavak 1. Dekreta o izvršavanju Zakona o borbi protiv terorizma).
([360]) Članak 9. stavak 4. Zakona o borbi protiv terorizma.
([361]) Članak 7. Zakona o borbi protiv terorizma.
([362]) To jest, svatko tko ima barem deset godina radnog iskustva kao odvjetnik ili stručno znanje u području ljudskih prava i barem deset godina radi ili je radio kao izvanredni profesor (ili više zvanje) ili tko je obnašao dužnost višeg javnog službenika u državnim agencijama ili lokalnim vlastima ili ima najmanje deset godina radnog iskustva u području ljudskih prava (npr. u nevladinoj organizaciji) (članak 7. stavak 1. Dekreta o izvršavanju Zakona o borbi protiv terorizma).
([363]) Na primjer, ako je protiv njega podignuta optužnica u kaznenom predmetu povezanom s njegovim dužnostima, ako otkriva povjerljive informacije ili zbog dugotrajne mentalne ili fizičke nesposobnosti (članak 7. stavak 3. Dekreta o izvršavanju Zakona o borbi protiv terorizma).

okviru izvršavanja svoje nadzorne funkcije HRPO može izdavati opće preporuke za poboljšanje zaštite ljudskih prava ([364]) i posebne preporuke za korektivne mjere ako se utvrdi povreda ljudskih prava ([365]). Tijela javne vlasti dužna su obavješćivati HRPO-a o daljnjim mjerama poduzetima na temelju njegovih preporuka ([366]).

(199) Drugo, PIPC nadzire usklađenost tijela za nacionalnu sigurnost s pravilima o zaštiti podataka, što uključuje i primjenjive odredbe PIPA-e (vidjeti uvodnu izjavu 149.) i ograničenja i zaštitne mjere koje se primjenjuju na prikupljanje osobnih podataka na temelju drugih zakona (CPPA, Zakon o borbi protiv terorizma i TBA; vidjeti i uvodnu izjavu 171.) ([367]). Pri izvršavanju svoje nadzorne uloge PIPC može koristiti sve svoje istražne i korektivne ovlasti, kako je detaljno opisano u odjeljku 2.4.2.

(200) Treće, aktivnosti tijela za nacionalnu sigurnost podliježu neovisnom nadzoru NHRC-a, u skladu s postupcima opisanima u uvodnoj izjavi 172. ([368]).

(201) Četvrto, nadzornom funkcijom BAI-ja obuhvaćena su i tijela za nacionalnu sigurnost, iako NIS može, u iznimnim okolnostima, odbiti dostaviti određene informacije ili materijale, tj. ako su oni državne tajne te bi upoznatost javnosti s njima mogla imati ozbiljne posljedice na nacionalnu sigurnost ([369]).

(202) Naposljetku, parlamentarni nadzor nad aktivnostima NIS-a provodi Nacionalna skupština (preko specijaliziranog Obavještajnog odbora) ([370]). CPPA-om se utvrđuje posebna nadzorna uloga Nacionalne skupštine u vezi s primjenom mjera ograničavanja komunikacije za potrebe nacionalne sigurnosti ([371]). Konkretno, Nacionalna skupština može provoditi inspekcijske preglede opreme za prisluškivanje na licu mjesta te zahtijevati i od NIS-a i od telekomunikacijskih operatera koji su otkrili sadržaj komunikacija da podnesu izvješće o tome. Nacionalna skupština može obavljati i svoje opće nadzorne funkcije (u skladu s postupcima opisanima u uvodnoj izjavi 174.). U Zakonu o NIS-u od direktora NIS-a zahtijeva se da bez odgode odgovori Obavještajnom odboru kad on zatraži izvješće o nekom određenom pitanju ([372]), pri čemu postoje posebna pravila za određene naročito osjetljive informacije. Konkretno, direktor NIS-a može odbiti odgovoriti Obavještajnom odboru ili odbiti svjedočiti pred njime samo u iznimnim okolnostima, tj. ako se zahtjev odnosi na državne tajne u pogledu vojske, diplomatskih pitanja ili pitanja povezanih sa Sjevernom Korejom te bi upoznatost javnosti s njima mogla imati ozbiljne posljedice na sudbinu države ([373]). U tom slučaju Obavještajni odbor može zatražiti objašnjenje od premijera, a ako se nikakvo objašnjenje ne dostavi u roku od sedam dana, odgovor ili svjedočenje ne može se odbiti.

3.3.4. *Pravna zaštita*

(203) Korejski sustav i u području nacionalne sigurnosti pruža razne mogućnosti za dobivanje (sudske) pravne zaštite, uključujući naknadu za štetu. Tim mehanizmima ispitanicima se osiguravaju djelotvorni upravni i sudski pravni lijekovi, što im prije svega omogućuje da ostvaruju svoja prava, uključujući pravo na pristup svojim osobnim podacima te ispravak ili brisanje tih podataka.

(204) Prvo, u skladu s člankom 3. stavkom 5. i člankom 4. stavcima 1., 3. i 4. PIPA-e, pojedinci mogu ostvariti svoja prava na pristup, ispravak, brisanje i suspenziju u pogledu tijela za nacionalnu sigurnost. U odjeljku 6. Obavijesti br. 2021-5 (Prilog I. ovoj Odluci) dodatno se pojašnjava kako se ta prava primjenjuju u kontekstu obrade

([364]) Članak 8. stavak 1. Dekreta o izvršavanju Zakona o borbi protiv terorizma.
([365]) Članak 9. stavak 1. Dekreta o izvršavanju Zakona o borbi protiv terorizma. HRPO samostalno odlučuje o donošenju preporuka, no obvezan je o njima izvijestiti predsjednika Povjerenstva za borbu protiv terorizma.
([366]) Članak 9. stavak 2. Dekreta o izvršavanju Zakona o borbi protiv terorizma. Prema službenoj izjavi korejske vlade, ako se preporuka HRPO-a ne bi provela, taj bi se slučaj proslijedio Povjerenstvu za borbu protiv terorizma, koje uključuje premijera, no dosad nije bilo slučajeva u kojima preporuke HRPO-a nisu provedene (vidjeti odjeljak 3.3.1. Priloga II.).
([367]) Prilog II., odjeljak 3.3.4.
([368]) Kad je konkretno riječ o NIS-u, NHRC je u prošlosti provodio istrage po službenoj dužnosti i obradio brojne pritužbe pojedinaca. Vidjeti npr. stranicu 128 u godišnjem izvješću NHRC-a za 2018. (dostupno na https://www.humanrights.go.kr/site/program/board/basicboard/view?menuid=002003003001&pagesize=10&boardtypeid=7017&boardid=7604746) i stranicu 70 u godišnjem izvješću NHRC-a za 2019. (dostupno na https://www.humanrights.go.kr/site/program/board/basicboard/view?menuid=002003003001&pagesize=10&boardtypeid=7017&boardid=7606217).
([369]) Članak 13. stavak 1. Zakona o NIS-u.
([370]) Članak 36. i članak 37. stavak 1. točka 15. Zakona o Nacionalnoj skupštini.
([371]) Članak 15. CPPA-a.
([372]) Članak 15. stavak 2. Zakona o NIS-u.
([373]) Članak 17. stavak 2. Zakona o NIS-u. „Državne tajne" definiraju su kao (klasificirane) činjenice, proizvodi ili znanje koji se ne smiju otkrivati nijednoj drugoj državi ni organizaciji kako bi se izbjegle bilo kakve ozbiljne negativne posljedice na nacionalnu sigurnost i kojima je dopušten samo ograničen pristup. Vidjeti članak 13. stavak 4. Zakona o NIS-u.

podataka za potrebe nacionalne sigurnosti. Prije svega, tijelo za nacionalnu sigurnost smije ograničiti ili odbiti ostvarivanje prava samo u mjeri i onoliko dugo koliko je to nužno i proporcionalno za zaštitu važnog cilja od javnog interesa (na primjer u mjeri i onoliko dugo koliko bi se izvršavanjem prava ugrozila istraga u tijeku ili nacionalna sigurnost) ili ako bi se izvršavanjem prava mogao ugroziti život ili zdravlje treće strane. Da bi se primijenilo takvo ograničenje potrebno je stoga uravnotežiti prava i interese pojedinca s relevantnim javnim interesom te ono ni u kojem slučaju ne smije utjecati na bit tog prava (članak 37. stavak 2. Ustava). Ako se zahtjev odbije ili ograniči, pojedinac se mora bez odgode obavijestiti o razlozima za to.

(205) Drugo, pojedinci imaju pravo na dobivanje pravne zaštite na temelju PIPA-e ako je tijelo za nacionalnu sigurnost obrađivalo njihove podatke suprotno odredbama PIPA-e ili kršeći ograničenja i zaštitne mjere iz drugih zakona kojima se uređuje prikupljanje osobnih podataka (naročito iz CPPA-a, vidjeti uvodnu izjavu 171.) ([374]). To se pravo može ostvariti pritužbom PIPC-u (među ostalim preko Pozivnog centra za zaštitu privatnosti, kojim upravlja Korejska agencija za internet i sigurnost) ([375]). Nadalje, kako bi se olakšao jednostavniji pristup pravnoj zaštiti protiv korejskih tijela za nacionalnu sigurnost, pojedinci iz EU-a mogu podnijeti pritužbu PIPC-u preko svojeg nacionalnog tijela za zaštitu podataka ([376]). U tom će slučaju PIPC obavijestiti pojedinca preko nacionalnog tijela za zaštitu podataka nakon zaključenja istrage (prema potrebi uključujući informacije o izrečenim korektivnim mjerama). Nadalje, na temelju Zakona o upravnim sporovima pojedinci se mogu žaliti na odluke ili nepostupanje PIPC-a ili ih osporavati (vidjeti uvodnu izjavu 132.).

(206) Treće, pojedinci mogu podnijeti pritužbu HRPO-u o povredi njihova prava na privatnost/zaštitu podataka u kontekstu aktivnosti suzbijanja terorizma (tj. u skladu sa Zakonom o borbi protiv terorizma) ([377]), koji može predložiti korektivne mjere. Budući da za postupak pred HRPO-om nema zahtjeva o dopuštenosti, pritužba će se obraditi čak i ako predmetni pojedinac ne može dokazati da su mu zapravo povrijeđena prava (na primjer zbog toga što je tijelo za nacionalnu sigurnost navodno nezakonito prikupljalo njegove podatke) ([378]). Relevantno tijelo mora obavijestiti HRPO-a o svim mjerama koje su poduzete kako bi se provele njegove preporuke.

(207) Četvrto, pojedinci mogu podnijeti pritužbu NHRC-u o prikupljanju njihovih podataka koje su provodila tijela za nacionalnu sigurnost i dobiti pravnu zaštitu u skladu s postupkom opisanim u uvodnoj izjavi 178. ([379]).

(208) Konačno, dostupni su razni sudski pravni lijekovi ([380]) kojima se pojedincima omogućuje da se pozivaju na ograničenja i zaštitne mjere opisane u odjeljku 3.3.1. radi dobivanja pravne zaštite. U prvom redu, pojedinci mogu zakonitost postupaka tijela za nacionalnu sigurnost osporavati na temelju Zakona o upravnim sporovima (u skladu s postupkom opisanim u uvodnoj izjavi 181.) ili Zakona o Ustavnom sudu (vidjeti uvodnu izjavu 182.). Osim toga, mogu dobiti naknadu štete na temelju Zakona o naknadi štete od države (kako je detaljnije opisano u uvodnoj izjavi 183.).

4. **ZAKLJUČAK**

(209) Komisija smatra da Republika Koreja – PIPA-om, posebnim pravilima koja se primjenjuju na određene sektore (kako su analizirana u odjeljku 2.) i dodatnim zaštitnim mjerama predviđenima u Obavijesti br. 2021-5 (Prilog I.) – za osobne podatke koji se prenose iz Europske unije osigurava razinu zaštite koja je u načelu istovjetna onoj koja se jamči Uredbom (EU) 2016/679.

(210) Nadalje, Komisija smatra da, u cjelini, nadzorni mehanizmi i mogućnosti za pravnu zaštitu u korejskom pravu omogućuju da se u praksi utvrde i otklone povrede pravila o zaštiti podataka koje su počinili voditelji obrade u Koreji te ispitaniku pružaju pravne lijekove za dobivanje pristupa njegovim osobnim podacima i, konačno, za ispravak ili brisanje takvih podataka.

([374]) Članak 58. stavak 4. i članak 4. stavak 5. PIPA-e. Vidjeti Prilog II., odjeljak 3.4.2.
([375]) Članak 62. i članak 63. stavak 2. PIPA-e.
([376]) Obavijest br. 2021-5 (odjeljak 6., Prilog I.).
([377]) Članak 8. stavak 1. točka 2. Dekreta o izvršavanju Zakona o borbi protiv terorizma.
([378]) Vidjeti Prilog II., odjeljak 3.4.1.
([379]) Na primjer, NHRC redovito dobiva pritužbe protiv Nacionalne obavještajne službe, vidjeti podatke o broju pritužbi zaprimljenih u razdoblju od 2015. do 2019. na stranici 70 u godišnjem izvješću NHRC-a za 2019. (dostupno na https://www.humanrights.go.kr/site/program/board/basicboard/view?menuid=002003003001&pagesize=10&boardtypeid=7017&boardid=7606217).
([380]) Vidjeti Prilog II., odjeljak 3.4.4.

(211) Naposljetku, na temelju dostupnih informacija o korejskom pravnom poretku, uključujući izjave, jamstva i obveze korejske vlade iz Priloga II., Komisija smatra da će se svako zadiranje u temeljna prava pojedinaca čiji se osobni podaci prenose iz Europske unije u Republiku Koreju, a koje vrše korejska tijela javne vlasti u javnom interesu, posebno za potrebe kaznenog progona i nacionalne sigurnosti, ograničiti na ono što je strogo nužno za ostvarivanje predmetnog legitimnog cilja te da postoji djelotvorna pravna zaštita od takvog zadiranja.

(212) Stoga bi s obzirom na nalaze iz ove Odluke trebalo odlučiti da Republika Koreja osigurava primjerenu razinu zaštite u smislu članka 45. Uredbe (EU) 2016/679, kako je protumačen s obzirom na Povelju Europske unije o temeljnim pravima, za osobne podatke koji se prenose iz Europske unije u Republiku Koreju voditeljima obrade osobnih podataka u Republici Koreji koji podliježu PIPA-i, uz iznimku vjerskih organizacija, u mjeri u kojoj obrađuju osobne podatke u svrhe svojih misionarskih aktivnosti, političkih stranaka, u mjeri u kojoj obrađuju osobne podatke u kontekstu imenovanja kandidata, i voditelja obrade koji podliježu nadzoru Povjerenstva za financijske usluge za obradu osobnih kreditnih informacija u skladu sa Zakonom o kreditnim informacijama, u mjeri u kojoj obrađuju takve informacije.

5. **UČINCI OVE ODLUKE I AKTIVNOSTI TIJELA ZA ZAŠTITU PODATAKA**

(213) Države članice i njihova tijela dužni su poduzeti mjere potrebne za usklađivanje s aktima institucija Unije jer se potonji smatraju zakonitima i proizvode pravne učinke do njihova povlačenja, poništenja u postupku za poništenje ili proglašavanja nevažećima nakon zahtjeva za prethodnu odluku ili tužbenog zahtjeva za proglašenje nezakonitosti.

(214) Stoga je odluka Komisije o primjerenosti donesena u skladu s člankom 45. stavkom 3. Uredbe (EU) 2016/679 obvezujuća za sva tijela država članica kojima je upućena, uključujući njihova neovisna nadzorna tijela. Konkretno, za prijenos od voditelja obrade ili izvršitelja obrade u Europskoj uniji voditeljima obrade u Republici Koreji nisu potrebna daljnja odobrenja.

(215) Trebalo bi podsjetiti da, u skladu s člankom 58. stavkom 5. Uredbe (EU) 2016/679 i kako je objašnjeno u presudi Suda Europske unije u predmetu *Schrems* ([381]), ako nacionalno tijelo za zaštitu podataka, među ostalim nakon što je zaprimilo pritužbu, ima sumnje u pogledu spojivosti odluke Komisije o primjerenosti s temeljnim pravima pojedinca na privatnost i zaštitu podataka, nacionalnim pravom mora biti predviđen pravni lijek za iznošenje tih prigovora pred nacionalnim sudom od kojeg se može tražiti da Sudu Europske unije uputi zahtjev za prethodnu odluku ([382]).

6. **PRAĆENJE I PREISPITIVANJE OVE ODLUKE**

(216) U skladu sa sudskom praksom Suda Europske unije ([383]), a kako je potvrđeno u članku 45. stavku 4. Uredbe (EU) 2016/679, Komisija bi nakon donošenja odluke o primjerenosti trebala kontinuirano pratiti relevantne događaje u trećoj zemlji kako bi ocijenila osigurava li ta treća zemlja i dalje u načelu istovjetnu razinu zaštite. Takva provjera potrebna je, u svakom slučaju, kad Komisija dobije informacije na temelju kojih može opravdano posumnjati u to.

(217) Stoga bi Komisija trebala kontinuirano pratiti situaciju u Republici Koreji u pravnom okviru i stvarnoj praksi za obradu osobnih podataka kako je ocijenjeno u ovoj Odluci, među ostalim poštuju li korejska tijela izjave, jamstva i obveze iz Priloga II. Kako bi se taj proces olakšao, korejska se tijela pozivaju da bez odgode obavijeste Komisiju o svim znatnim promjenama koje su relevantne za ovu Odluku kad je riječ o obradi osobnih podataka koju vrše poslovni subjekti i tijela javne vlasti te o ograničenjima i zaštitnim mjerama primjenjivima na pristup tijela javne vlasti osobnim podacima.

([381]) Presuda u predmetu *Schrems*, točka 65.

([382]) Presuda u predmetu *Schrems*, točka 65.: „U tom je pogledu nacionalni zakonodavac dužan predvidjeti pravna sredstva koja nacionalnom nadzornom tijelu omogućuju isticanje prigovora pred nacionalnim sudovima koje smatra osnovanima, kako bi ti sudovi mogli, u slučaju da dijele sumnje tog tijela u vezi s valjanošću Komisijine odluke, uputiti zahtjev za prethodnu odluku radi ispitivanja valjanosti te odluke."

([383]) Presuda u predmetu *Schrems*, točka 76.

(218) Nadalje, kako bi Komisija mogla djelotvorno obavljati svoju funkciju praćenja, države članice trebale bi je obavješćivati o svim relevantnim mjerama koje poduzimaju nacionalna tijela za zaštitu podataka, naročito u pogledu upita ili pritužbi ispitanika iz EU-a o prijenosu osobnih podataka iz Europske unije voditeljima obrade podataka u Republici Koreji. Komisiju bi trebalo obavijestiti i o svakoj naznaci da mjere korejskih tijela javne vlasti odgovornih za sprečavanje, istragu, otkrivanje ili progon kaznenih djela ili za nacionalnu sigurnost, uključujući nadzorna tijela, ne osiguravaju potrebnu razinu zaštite.

(219) U skladu s člankom 45. stavkom 3. Uredbe (EU) 2016/679 ([384]) i s obzirom na činjenicu da se razina zaštite koju pruža korejski pravni poredak može promijeniti, Komisija bi nakon donošenja ove Odluke trebala periodično preispitivati jesu li nalazi koji se odnose na primjerenost razine zaštite koju je osigurala Republika Koreja još uvijek činjenično i pravno opravdani.

(220) U tu bi svrhu ovu Odluku trebalo prvi put preispitati u roku od tri godine od njezina stupanja na snagu. Nakon prvog preispitivanja i ovisno o njegovu ishodu Komisija će u bliskoj suradnji s Odborom osnovanim na temelju članka 93. stavka 1. Uredbe (EU) 2016/679 odlučiti je li potrebno zadržati trogodišnji ciklus. U svakom slučaju, sljedeća preispitivanja trebala bi se provesti najmanje svake četiri godine ([385]). To bi preispitivanje trebalo obuhvatiti sve aspekte funkcioniranja ove Odluke, a posebno primjenu dodatnih zaštitnih mjera iz Priloga I. ovoj Odluci, pri čemu bi posebnu pozornost trebalo posvetiti zaštiti koja se pruža u slučaju daljnjeg prijenosa; razvoj relevantne sudske prakse; pravila o obradi pseudonimiziranih informacija u svrhe prikupljanja statističkih podataka, provođenja znanstvenih istraživanja i arhiviranja u javnom interesu, kao i primjene iznimki iz članka 28. stavka 7. PIPA-e; djelotvornost ostvarivanja prava pojedinaca, među ostalim i pred nedavno reformiranim PIPC-om, i primjenu iznimaka od tih prava; primjenu djelomičnih izuzeća iz PIPA-e; te ograničenja i zaštitne mjere u vezi s pristupom vlade (kako je navedeno u Prilogu II. ovoj Odluci), uključujući suradnju PIPC-a s tijelima za zaštitu podataka iz EU-a u području pritužbi pojedinaca. Trebalo bi obuhvatiti i djelotvornost nadzora i izvršavanja u pogledu PIPA-e i u području kaznenog progona i nacionalne sigurnosti (ponajprije nadzora i izvršavanja koje obavljaju PIPC i NHRC).

(221) Za provedbu preispitivanja Komisija bi se trebala sastati s PIPC-om, prema potrebi zajedno s drugim korejskim tijelima odgovornima za pristup vlade, uključujući relevantna nadzorna tijela. Sudjelovanje na tom sastanku trebalo bi biti otvoreno za predstavnike članova Europskog odbora za zaštitu podataka. U okviru preispitivanja Komisija bi trebala zatražiti od PIPC-a da dostavi sveobuhvatne informacije o svim aspektima relevantnima za zaključak o primjerenosti, među ostalim o ograničenjima i zaštitnim mjerama u pogledu pristupa vlade ([386]). Komisija bi trebala i zatražiti objašnjenja svih informacija relevantnih za ovu Odluku koje je zaprimila, uključujući javna izvješća korejskih tijela ili drugih dionika u Koreji, Europskog odbora za zaštitu podataka, pojedinačnih tijela za zaštitu podataka, skupina civilnog društva te medijska izvješća ili informacije iz bilo kojih drugih dostupnih izvora.

(222) Na temelju preispitivanja Komisija bi trebala sastaviti javno izvješće koje podnosi Europskom parlamentu i Vijeću.

7. SUSPENZIJA, STAVLJANJE IZVAN SNAGE ILI IZMJENA OVE ODLUKE

(223) Ako dostupne informacije, naročito one dobivene praćenjem primjene ove Odluke ili one koje dostavljaju korejska tijela ili tijela država članica, pokažu da razina zaštite koju pruža Republika Koreja možda više nije primjerena, Komisija bi o tome trebala bez odgode obavijestiti nadležna korejska tijela i zatražiti poduzimanje odgovarajućih mjera u određenom, razumnom roku.

(224) Ako nakon isteka navedenog roka nadležna korejska tijela ne poduzmu te mjere ili na drugi zadovoljavajući način ne dokažu da se ova Odluka i dalje temelji na primjerenoj razini zaštite, Komisija će pokrenuti postupak iz članka 93. stavka 2. Uredbe (EU) 2016/679 radi djelomične ili potpune suspenzije ili stavljanja izvan snage ove Odluke.

(225) Alternativno, Komisija će pokrenuti taj postupak radi izmjene Odluke, ponajprije utvrđivanjem dodatnih uvjeta za prijenose podataka ili ograničavanjem područja primjene zaključka o primjerenosti samo na prijenose podataka za koje se i dalje osigurava primjerena razina zaštite.

([384]) U skladu s člankom 45. stavkom 3. Uredbe (EU) 2016/679 „[u] provedbenom aktu predviđa se mehanizam za periodično preispitivanje, […] kojim će se uzeti u obzir svi relevantni događaji u toj trećoj zemlji ili međunarodnoj organizaciji".

([385]) Člankom 45. stavkom 3. Uredbe (EU) 2016/679 predviđa se da se periodično preispitivanje mora provoditi „najmanje svake četiri godine". Vidjeti i Europski odbor za zaštitu podataka, Referentni dokument o primjerenosti, WP 254 rev.01.

([386]) Vidjeti Prilog II. ovoj Odluci.

(226) Konkretno, Komisija bi trebala pokrenuti postupak suspenzije ili stavljanja izvan snage u slučaju naznaka da poslovni subjekti koji primaju osobne podatke na temelju ove Odluke ne poštuju dodatne zaštitne mjere iz Priloga I. i/ili da njihovo izvršavanje provedba nije djelotvorno osigurano, ili ako korejska tijela ne postupaju u skladu s izjavama, jamstvima i obvezama iz Priloga II. ovoj Odluci.

(227) Komisija bi trebala razmotriti i pokretanje postupka koji vodi do izmjene, suspenzije ili stavljanja izvan snage ove Odluke ako, u kontekstu preispitivanja ili na drugi način, nadležna korejska tijela ne dostave informacije ili pojašnjenja koja su potrebna za ocjenu razine zaštite osobnih podataka koji se prenose iz Europske unije u Republiku Koreju ili usklađenosti s ovom Odlukom. S obzirom na to Komisija bi trebala uzeti u obzir opseg u kojem se relevantne informacije mogu dobiti iz drugih izvora.

(228) Zbog valjano utemeljenih krajnje hitnih razloga Komisija će iskoristiti mogućnost donošenja, u skladu s postupkom iz članka 93. stavka 3. Uredbe (EU) 2016/679, odmah primjenjivih provedbenih akata o suspenziji, stavljanju izvan snage ili izmjeni Odluke.

8. **ZAVRŠNA RAZMATRANJA**

(229) Europski odbor za zaštitu podataka objavio je svoje mišljenje ([387]), koje je uzeto u obzir pri izradi ove Odluke.

(230) Mjere predviđene ovom Odlukom u skladu su s mišljenjem Odbora osnovanog na temelju članka 93. stavka 1. Uredbe (EU) 2016/679,

DONIJELA JE OVU ODLUKU:

Članak 1.

1. Za potrebe članka 45. Uredbe (EU) 2016/679 Republika Koreja osigurava primjerenu razinu zaštite osobnih podataka koji se iz Europske unije prenose subjektima u Republici Koreji koji podliježu Zakonu o zaštiti osobnih informacija, kako je dopunjen dodatnim zaštitnim mjerama iz Priloga I. te službenim izjavama, jamstvima i obvezama iz Priloga II.

2. Ova Odluka ne odnosi se na osobne podatke koji se prenose primateljima iz jedne od sljedećih kategorija, u mjeri u kojoj svrha obrade osobnih podataka odgovara, djelomično ili u potpunosti, jednoj od svrha navedenih u njima, a to su:

(a) vjerske zajednice, u mjeri u kojoj obrađuju osobne podatke za svoje misionarske aktivnosti;

(b) političke stranke, u mjeri u kojoj obrađuju osobne podatke u kontekstu imenovanja kandidata;

(c) subjekti koji podliježu nadzoru Povjerenstva za financijske usluge za obradu osobnih kreditnih informacija u skladu sa Zakonom o kreditnim informacijama, u mjeri u kojoj obrađuju takve informacije.

Članak 2.

Kad god nadležna tijela u državama članicama, radi zaštite pojedinaca u vezi s obradom njihovih osobnih podataka, izvršavaju svoje ovlasti u skladu s člankom 58. Uredbe (EU) 2016/679 u pogledu prijenosa podataka koji su obuhvaćeni područjem primjene navedenim u članku 1. ove Odluke, predmetna država članica o tome bez odgode obavješćuje Komisiju.

Članak 3.

1. Komisija kontinuirano prati primjenu pravnog okvira na kojem se temelji ova Odluka, uključujući uvjete pod kojima se odvijaju daljnji prijenosi, ostvaruju prava pojedinaca i korejska tijela javne vlasti imaju pristup podacima koji se prenose na temelju ove Odluke, kako bi ocijenila osigurava li Republika Koreja i dalje primjerenu razinu zaštite u smislu članka 1.

([387]) Mišljenje 32/2021 o Nacrtu provedbene odluke Europske komisije u skladu s Uredbom (EU) 2016/679 o primjerenosti zaštite osobnih podataka u Republici Koreji, dostupno na sljedećoj poveznici: https://edpb.europa.eu/our-work-tools/our-documents/opinion-art-70/opinion-322021-regarding-european-commission-draft_en.

2. Države članice i Komisija međusobno se obavješćuju o slučajevima u kojima Povjerenstvo za zaštitu osobnih informacija ili bilo koje drugo nadležno tijelo u Koreji ne osigura poštovanje pravnog okvira na kojem se temelji ova Odluka.

3. Države članice i Komisija međusobno se obavješćuju o bilo kakvim naznakama da zadiranje korejskih tijela javne vlasti u pravo pojedinaca na zaštitu njihovih osobnih podataka prelazi ono što je nužno ili da ne postoji djelotvorna pravna zaštita od takvog zadiranja.

4. Nakon tri godine od dana kad su države članice obaviještene o ovoj Odluci, a potom najmanje svake četiri godine, Komisija ocjenjuje zaključak iz članka 1. stavka 1. na temelju svih dostupnih informacija, među ostalim na temelju informacija primljenih u okviru preispitivanja provedenog s relevantnim korejskim tijelima.

5. Ako Komisija ima saznanja da primjerena razina zaštite više nije osigurana, o tome obavješćuje nadležna korejska tijela. Ako je potrebno, može odlučiti suspendirati, izmijeniti ili staviti izvan snage ovu Odluku, ili ograničiti njezino područje primjene, u skladu s člankom 45. stavkom 5. Uredbe (EU) 2016/679, posebno ako ima saznanja da:

(a) voditelji obrade u Koreji koji su primili osobne podatke iz Europske unije na temelju ove Odluke ne poštuju dodatne zaštitne mjere iz Priloga I. ili nadzor i izvršavanje u tom pogledu nisu dostatni;

(b) korejska tijela javne vlasti ne poštuju izjave, jamstva i obveze iz Priloga II., među ostalim u pogledu uvjeta i ograničenja za prikupljanje osobnih podataka prenesenih na temelju ove Odluke i pristup korejskih tijela javne vlasti tim podacima za potrebe kaznenog progona ili nacionalne sigurnosti.

Komisija može donijeti takve mjere i ako zbog nesuradnje korejske vlade ne može utvrditi osigurava li Republika Koreja i dalje primjerenu razinu zaštite.

Članak 4.

Ova je Odluka upućena državama članicama.

Sastavljeno u Bruxellesu 17. prosinca 2021.

Za Komisiju
Didier REYNDERS
Član Komisije

PRILOG I.

DOPUNSKA PRAVILA ZA TUMAČENJE I PRIMJENU ZAKONA O ZAŠTITI OSOBNIH INFORMACIJA U VEZI S OBRADOM OSOBNIH PODATAKA KOJI SE PRENOSE U KOREJU

Sadržaj

I. Kratak prikaz

Koreja i Europska unija (dalje u tekstu „EU”) sudjelovale su u raspravama o primjerenosti, na temelju kojih je Europska komisija utvrdila da Koreja jamči primjerenu razinu zaštite osobnih podataka u skladu s člankom 45. Opće uredbe o zaštiti podataka.

U tom je kontekstu Povjerenstvo za zaštitu osobnih informacija donijelo ovu Obavijest na temelju članka 5. (Obveze države i slično) i članka 14. (Međunarodna suradnja) ([1]) Zakona o zaštiti osobnih informacija kako bi se razjasnilo tumačenje, primjena i izvršavanje određenih odredaba Zakona, među ostalim u vezi s obradom osobnih podataka koji se prenose u Koreju na temelju odluke EU-a o primjerenosti.

Budući da ova Obavijest ima status upravnog propisa koji nadležna upravna agencija uvodi i najavljuje kako bi se razjasnili standardi za tumačenje, primjenu i izvršenje Zakona o zaštiti osobnih informacija u korejskom pravnom sustavu, pravno je obvezujuća za voditelja obrade osobnih informacija u smislu da se svako kršenje ove Obavijesti može smatrati kršenjem relevantnih odredaba PIPA-e. Usto, ako zbog kršenja ove Obavijesti dolazi do povrede osobnih prava i interesa, predmetni pojedinci imaju pravo tražiti pravnu zaštitu od Povjerenstva za zaštitu osobnih informacija ili suda.

Prema tome, ako voditelj obrade osobnih informacija koji obrađuje osobne informacije prenesene u Koreju u skladu s odlukom EU-a o primjerenosti ne poduzme mjere u skladu s ovom Obavijesti, smatrat će se da „postoji opravdana osnova na temelju koje se smatra da je došlo do povrede u vezi s osobnim informacijama, a nepoduzimanje mjera vjerojatno će uzrokovati štetu koju je teško popraviti” na temelju članka 64. stavaka 1. i 2. Zakona. U takvim slučajevima Povjerenstvo za zaštitu osobnih informacija ili povezane središnje upravne agencije mogu naložiti

([1]) Člankom 14. Zakona o zaštiti osobnih informacija propisuje se ovlast korejske Vlade da uvodi politike za poboljšanje razine zaštite osobnih informacija u međunarodnom okruženju i da sprečava povrede prava ispitanika zbog prekograničnog prijenosa osobnih informacija.

predmetnom voditelju obrade osobnih informacija da poduzme korektivne mjere i slično u skladu s ovlastima dodijeljenima na temelju te odredbe, a može se, ovisno o konkretnoj povredi prava, izreći i odgovarajuća kazna (sankcije, upravne novčane kazne itd.).

II. **Definicije pojmova**

U ovim se odredbama upotrebljavaju sljedeće definicije pojmova:

i. Zakon: Zakon o zaštiti osobnih informacija (Zakon br. 16930, koji je izmijenjen 4. veljače 2020. i koji je stupio na snagu 5. kolovoza 2020.);

ii. Predsjednički dekret: Dekret o izvršavanju Zakona o zaštiti osobnih informacija (Predsjednički dekret br. 30509 od 3. ožujka 2020., kojim se mijenjaju drugi zakoni);

iii. ispitanik: pojedinac čiji se identitet može utvrditi na temelju informacija koje se obrađuju i koji postaje predmet tih informacija;

iv. voditelj obrade osobnih informacija: javna institucija, pravna osoba, organizacija, pojedinac itd. koji izravno ili neizravno obrađuje osobne informacije u okviru svojih aktivnosti;

v. EU: EU (od kraja veljače 2020. 27 država članica ([2]), uključujući Belgiju, Njemačku, Francusku, Italiju, Luksemburg, Nizozemsku, Dansku, Irsku, Grčku, Portugal, Španjolsku, Austriju, Finsku, Švedsku, Cipar, Češku, Estoniju, Mađarsku, Latviju, Litvu, Maltu, Poljsku, Slovačku, Sloveniju, Rumunjsku, Bugarsku i Hrvatsku) te države povezane s EU-om na temelju Sporazuma o Europskom gospodarskom prostoru (Island, Lihtenštajn i Norveška);

vi. Opća uredba o zaštiti podataka: opći zakonodavni akt EU-a o zaštiti osobnih informacija (Uredba (EU) 2016/679);

vii. odluka o primjerenosti: u skladu s člankom 45. stavkom 3. Opće uredbe o zaštiti podataka Europska komisija odlučila je da treća zemlja, državno područje treće zemlje, jedno ili više područja ili međunarodna organizacija jamči primjerenu razinu zaštite osobnih informacija.

III. **Dopunska pravila**

1. **Ograničenje nenamjenske upotrebe i pružanja osobnih informacija (članci 3., 15. i 18. Zakona)**

<Zakon o zaštiti osobnih informacija

(Zakon br. 16930, djelomično izmijenjen 4. veljače 2020.)>

Članak 3. (Načela za zaštitu osobnih informacija) 1. Voditelj obrade osobnih informacija mora izričito navesti svrhe obrade osobnih informacija i prikupljati osobne informacije zakonito, pošteno i u najmanjoj mjeri koja je potrebna za takve svrhe.

2. Voditelj obrade osobnih informacija obrađuje osobne informacije na prikladan način potreban za svrhe u koje se te informacije obrađuju i ne smije ih upotrebljavati izvan takvih svrha.

Članak 15. (Prikupljanje i upotreba osobnih informacija) 1. Voditelj obrade osobnih informacija može prikupljati osobne informacije u bilo kojoj od sljedećih okolnosti i upotrebljavati ih u okviru svrhe prikupljanja:

1. ako se od ispitanika pribavi privola;

2. ako u zakonodavstvu postoje posebne odredbe ili je to neizbježno kako bi se poštovale pravne obveze;

3. ako je to neizbježno da bi javna institucija mogla obnašati svoje zadaće u okviru svoje nadležnosti kako je utvrđeno propisima i slično;

4. ako je to neophodno radi izvršenja i provedbe ugovora s ispitanikom;

([2]) Do kraja prijelaznog razdoblja to uključuje i Ujedinjenu Kraljevinu, kako je predviđeno člancima 126., 127. i 132. Sporazuma o povlačenju Ujedinjene Kraljevine Velike Britanije i Sjeverne Irske iz Europske unije i Europske zajednice za atomsku energiju (2019/C 384 I/01).

5. ako se to smatra očito nužnim za zaštitu života te zdravstvenih ili imovinskih interesa ispitanika ili treće strane od neposredne opasnosti ako ispitanik ili njegov zakonski zastupnik nije u mogućnosti izraziti namjeru ili se prethodna privola ne može pribaviti zbog nepoznate adrese itd.;

6. ako je to potrebno za ostvarenje opravdanog interesa voditelja obrade osobnih informacija, pod uvjetom da takav interes nedvojbeno ima prednost pred pravima ispitanika. U takvim se slučajevima obrada dopušta samo u mjeri u kojoj je znatno povezana s opravdanim interesom voditelja obrade osobnih informacija i ako ne prelazi razuman okvir.

Članak 18. (Ograničenje nenamjenske upotrebe i pružanja osobnih informacija) 1. Voditelj obrade osobnih informacija ne smije upotrebljavati osobne informacije izvan okvira predviđenog člankom 15. stavkom 1. i člankom 39-3. stavcima 1. i 2. ili ih pružati bilo kojoj trećoj strani izvan okvira predviđenog člankom 17. stavcima 1. i 3.

2. Neovisno o stavku 1., ako se primjenjuje bilo koji od sljedećih podstavaka, voditelj obrade osobnih informacija može upotrebljavati osobne informacije ili ih pružati trećoj strani u druge svrhe, osim ako je vjerojatno da bi se time nepravedno povrijedili interesi ispitanika ili treće strane; pod uvjetom da pružatelji informacijskih i komunikacijskih usluga [kako je utvrđeno u članku 2. stavku 1. točki 3. Zakona o promicanju upotrebe informacijskih i komunikacijskih mreža, zaštiti informacija i sličnome; isto se primjenjuje i dalje u tekstu] koji obrađuju osobne informacije korisnika [kako je utvrđeno u članku 2. stavku 1. točki 4. Zakona o promicanju upotrebe informacijskih i komunikacijskih mreža, zaštiti informacija i sličnome; isto se primjenjuje i dalje u tekstu] podliježu samo podstavcima 1. i 2., a da se podstavci od 5. do 9. primjenjuju samo na javne institucije:

1. ako se od ispitanika pribavi dodatna privola;

2. ako postoje druge posebne odredbe u zakonodavstvu;

3. ako se to smatra očito nužnim za zaštitu života te zdravstvenih ili imovinskih interesa ispitanika ili treće strane od neposredne opasnosti ako ispitanik ili njegov zakonski zastupnik nije u mogućnosti izraziti namjeru ili se prethodna privola ne može pribaviti zbog nepoznate adrese;

4. izbrisano; <Zakonom br. 16930, 4. veljače 2020.>

5. ako institucija ne može obavljati zadaće u svojoj nadležnosti kako je predviđeno bilo kojim zakonom, osim ako voditelj obrade osobnih informacija upotrebljava osobne informacija u svrhu koja nije predviđena ili ako ih pruži trećoj strani, što podliježe razmatranju i odluci Povjerenstva;

6. ako je potrebno pružati osobne informacije stranoj vladi ili međunarodnoj organizaciji radi provedbe ugovora ili druge međunarodne konvencije;

7. ako je to potrebno za istragu kaznenog djela, podizanje optužnice i kazneni progon;

8. ako je to potrebno sudu radi izvršavanja zadaća povezanih sa sudskim postupkom;

9. ako je to potrebno za izvršenje kazne, uvjetne kazne i zadržavanja.

Izostavljeni su stavci 3. i 4.

5. Ako voditelj obrade osobnih informacija pruža osobne informacije trećoj strani u svrhu koja nije predviđena bilo kojim slučajem navedenim u stavku 2., voditelj obrade osobnih informacija mora zatražiti od primatelja osobnih informacija da ograniči svrhu i metodu upotrebe i druga potrebna pitanja ili da pripremi potrebne zaštitne mjere kako bi se osigurala sigurnost osobnih informacija. U takvim slučajevima osoba kojoj je upućen takav zahtjev poduzima potrebne mjere za osiguranje sigurnosti osobnih informacija.

i. U članku 3. stavcima 1. i 2. Zakona propisuje se načelo prema kojem voditelj obrade osobnih informacija mora prikupiti samo minimalne osobne informacije koje su potrebne za pravno i zakonito izvršavanje svrhe obrade osobnih informacija te prema kojem ih ne bi trebao upotrebljavati u svrhe koje nisu predviđene ([3]).

ii. Prema tom načelu, u članku 15. stavku 1. Zakona propisuje se da ako voditelj obrade osobnih informacija prikuplja osobne informacije, te se informacije mogu upotrebljavati u okviru svrhe prikupljanja, a člankom 18. stavkom 1. propisuje se da se osobne informacije ne bi trebale upotrebljavati izvan svrhe prikupljanja niti pružati trećoj strani.

([3]) Budući da se ovim odredbama utvrđuju opća načela koja se primjenjuju na svaku obradu osobnih informacija, među ostalim ako je takva obrada posebno uređena drugim zakonima, pojašnjenja u ovom odjeljku primjenjuju se i ako se osobni podaci obrađuju na temelju drugih zakona (vidjeti npr. članak 15. stavak 1. Zakona o kreditnim informacijama, u kojem se izričito upućuje na ove odredbe).

iii. Isto tako, čak i ako se osobne informacije mogu upotrebljavati u svrhe koje nisu predviđene ili se pružati trećoj strani u iznimnim slučajevima ([4]) opisanima u podstavcima članka 18. stavka 2. Zakona, mora se zatražiti da se svrha ili metoda upotrebe ograniči kako bi se osobne informacije mogle obrađivati na siguran način u skladu sa stavkom 5. ili da se poduzmu mjere potrebne za osiguranje sigurnosti osobnih informacija.

iv. Navedene odredbe primjenjuju se i na obradu svih osobnih informacija primljenih u području pravne nadležnosti Koreje iz treće zemlje, neovisno o državljanstvu ispitanika.

v. Primjerice, ako voditelj obrade osobnih informacija u EU-u prenosi osobne informacije korejskom voditelju obrade osobnih informacija u skladu s odlukom o primjerenosti Europske komisije, svrha u koju voditelj obrade osobnih informacija u EU-u prenosi osobne informacije smatra se svrhom u koju korejski voditelj obrade osobnih informacija prikuplja osobne informacije te u takvim slučajevima korejski voditelj obrade može upotrebljavati te informacije ili ih pružati trećoj strani samo u okviru svrhe prikupljanja, osim u iznimnim slučajevima opisanima u podstavcima članka 18. stavka 2. Zakona.

2. **Ograničenje daljnjeg prijenosa osobnih podataka (članak 17. stavci 3. i 4. te članak 18. Zakona)**

<Zakon o zaštiti osobnih informacija

(Zakon br. 16930, djelomično izmijenjen 4. veljače 2020.)>

Članak 17. (Pružanje osobnih informacija) 1. izostavljeno

2. Nakon što pribavi privolu na temelju stavka 1. točke 1., voditelj obrade osobnih informacija obavješćuje ispitanika o sljedećim stavkama. To se primjenjuje i ako se izmijeni bilo koje od sljedećeg:

1. primatelj osobnih informacija;

2. svrha u koju primatelj osobnih informacija upotrebljava takve informacije;

3. pojedinosti osobnih informacija koje je potrebno pružiti;

4. razdoblje tijekom kojeg primatelj pohranjuje i upotrebljava osobne informacije;

5. činjenica da ispitanik ima pravo odbiti dati privolu i negativne posljedice, ako postoje, koje proizlaze iz odbijanja davanja privole.

3. Voditelj obrade osobnih informacija obavještava ispitanika o stavkama navedenima u stavku 2. i pribavlja od njega privolu za pružanje osobnih informacija trećoj strani u inozemstvu te ne smije sklopiti ugovor o prekograničnom prijenosu osobnih informacija kojim se krši ovaj Zakon.

4. Voditelj obrade osobnih informacija može pružati osobne informacije bez privole ispitanika u okviru koji je razumno povezan sa svrhama u koje su se osobne informacije prvotno prikupljale u skladu s odredbama propisanima Predsjedničkim dekretom, uzimajući u obzir jesu li ispitaniku uzorkovane negativne posljedice, jesu li poduzete mjere potrebne za osiguranje sigurnosti, kao što je enkripcija itd.

※ Vidjeti više o članku 18. na 3., 4. i 5. stranici.

<Dekret o izvršavanju Zakona o zaštiti osobnih informacija

([Datum stupanja na snagu 5. veljače 2021.] [Predsjednički dekret br. 30892, 4. kolovoza 2020., kojim se mijenjaju drugi zakoni])>

Članak 14-2. (Standardi za dodatnu upotrebu/pružanje osobnih informacija i slično)

1. Ako voditelj obrade osobnih informacija upotrebljava ili pruža osobne informacije (dalje u tekstu „dodatna upotreba ili pružanje osobnih informacija") bez privole ispitanika, u skladu s člankom 15. stavkom 3. ili člankom 17. stavkom 4. Zakona, voditelj obrade osobnih informacija razmatra sljedeća pitanja:

1. je li to razumno povezano s prvotnom svrhom u koju su osobne informacije prikupljene;

2. može li se dodatna upotreba ili pružanje osobnih informacija predvidjeti u kontekstu okolnosti pod kojima su osobne informacije prikupljene i prakse obrade;

3. dovodi li dodatna upotreba ili pružanje osobnih informacija do nepravedne povrede interesa ispitanika; i

4. jesu li poduzete potrebne mjere za osiguranje sigurnosti, kao što su pseudonimizacija ili enkripcija.

([4]) Pružatelji informacijskih i komunikacijskih usluga podliježu samo članku 18. stavku 2. podstavcima 1. i 2. Podstavci od 5. do 9. primjenjuju se samo na javne institucije.

2. Voditelj obrade osobnih informacija mora unaprijed navesti kriterije za procjenu stavki iz podstavaka stavka 1. u politici zaštite privatnosti na temelju članka 30. stavka 1. Zakona, a službenik za zaštitu privatnosti na temelju članka 31. stavka 1. Zakona provjerava upotrebljava li ili pruža li voditelj obrade osobnih informacija dodatne osobne informacije u skladu s relevantnim standardima.

i. Ako voditelj obrade osobnih informacija pruža osobne informacije trećoj strani u inozemstvu, mora unaprijed obavijestiti ispitanike o svim stavkama opisanima u članku 17. stavku 2. Zakona i pribaviti njihovu privolu, osim u slučajevima iz podtočke 1. ili 2. Ne bi trebalo sklopiti nikakav ugovor o prekograničnom pružanju osobnih podataka kojim se krši Zakon.

(1) Ako se osobne informacije pružaju u okviru koji je razumno povezan s prvotnom svrhom prikupljanja u skladu s člankom 17. stavkom 4. Zakona. Međutim, ta se odredba može primijeniti samo u ograničenim slučajevima ako su ispunjeni standardi za dodatnu upotrebu i pružanje osobnih informacija propisani člankom 14-2. Dekreta o izvršavanju. Usto, voditelj obrade osobnih informacija mora razmotriti može li pružanje osobnih informacija uzrokovati negativne posljedice za ispitanike i je li poduzeo potrebne mjere za osiguranje sigurnosti, kao što je enkripcija.

(2) Ako se osobne informacije mogu pružati trećoj strani u iznimnim slučajevima navedenima u članku 18. stavku 2. Zakona (vidjeti stranice od 3. do 5.). Međutim, čak i u takvim slučajevima, ako je vjerojatno da će se pružanjem takvih osobnih informacija nepravedno povrijediti interesi ispitanika ili treće strane, osobne informacije ne mogu se pružiti trećoj strani. Nadalje, pružatelj osobnih informacija mora zatražiti od primatelja osobnih informacija da ograniči svrhu ili metodu upotrebe osobnih informacija ili da poduzme mjere potrebne za osiguranje njihove sigurnosti kako bi se te informacije mogle obrađivati na siguran način.

ii. Ako se osobne informacije pružaju trećoj strani u inozemstvu, možda neće primiti istu razinu zaštite zajamčenu korejskim Zakonom o zaštiti osobnih informacija zbog razlika u sustavima zaštite osobnih informacija među državama. U skladu s tim, takvi će se slučajevi smatrati „slučajevima u kojima se ispitaniku mogu uzrokovati negativne posljedice" navedenima u članku 17. stavku 4. Zakona ili „slučajevima u kojima dolazi do nepravedne povrede interesa ispitanika ili treće strane" navedenima u članku 18. stavku 2. i članku 14-2. Dekreta o izvršavanju tog zakona ([5]). Kako bi se ispunili zahtjevi tih odredaba, voditelj obrade osobnih informacija i treća strana stoga moraju izričito osigurati razinu zaštite koja je jednaka Zakonu, uključujući jamstvo da će ispitanik moći ostvariti svoja prava u zakonski obvezujućim dokumentima kao što su ugovori, čak i nakon što se osobne informacije prenesu u inozemstvo.

3. **Obavješćivanje o podacima ako osobni podaci nisu dobiveni od ispitanika (članak 20. Zakona)**

<Zakon o zaštiti osobnih informacija

(Zakon br. 16930, djelomično izmijenjen 4. veljače 2020.)>

Članak 20. (Obavješćivanje o izvorima i slično za osobne informacije prikupljene od trećih strana) 1. Ako voditelj obrade osobnih informacija obrađuje osobne informacije prikupljene od trećih strana, mora odmah obavijestiti ispitanika o sljedećem na njegov zahtjev:

1. izvoru prikupljenih osobnih informacija;

2. svrsi obrade osobnih informacija;

3. pravu ispitanika da zatraži suspenziju obrade osobnih informacija, kako je propisano člankom 37.

2. Neovisno o stavku 1., ako voditelj obrade osobnih informacija koji zadovoljava kriterije propisane Predsjedničkim dekretom, uzimajući u obzir vrste i količine obrađenih osobnih informacija, broj zaposlenika, količinu prodaje itd., prikuplja osobne informacije od trećih strana i obrađuje ih na temelju članka 17. stavka 1. točke 1., taj voditelj obrade obavještava ispitanika o stavkama iz stavka 1.; pod uvjetom da se to ne primjenjuje ako informacije koje je prikupio voditelj obrade osobnih informacija ne sadržavaju nikakve osobne informacije, kao što su informacije za kontakt, s pomoću kojih se može obavijestiti ispitanika.

([5]) Na temelju članka 18. stavka 2. točke 2. PIPA-e to se primjenjuje i ako se osobne informacije otkrivaju trećim stranama u inozemstvu na temelju odredaba drugih zakona (kao što je npr. Zakon o kreditnim informacijama).

3. Potrebne stavke povezane s vremenom, metodom i postupkom obavješćivanja ispitanika na temelju glavne rečenice stavka 2. propisuju se Predsjedničkim dekretom.

4. Stavak 1. i glavna odredba stavka 2. ne primjenjuju se na sljedeće okolnosti; pod uvjetom da je to slučaj samo ako to nedvojbeno ima prednost pred pravima ispitanikâ na temelju ovog Zakona:

1. ako su osobne informacije koje podliježu zahtjevu za obavješćivanje uključene u datoteke s osobnim informacijama iz bilo kojeg podstavka članka 32. stavka 2.;

2. ako bi se takvim obavješćivanjem vjerojatno ugrozio život ili zdravlje bilo koje druge osobe ili nepravedno nanijela šteta imovini i drugim interesima bilo koje druge osobe.

i. Ako voditelj obrade osobnih informacija primi osobne informacije prenesene iz EU-a na temelju odluke o primjerenosti ([6]), mora obavijestiti ispitanika o sljedećim informacijama iz podtočaka od 1. do 5. bez nepotrebne odgode, a u svakom slučaju najkasnije mjesec dana od prijenosa:

(1) imenu i informacijama za kontakt osoba koje prenose i primaju osobne informacije;

(2) stavkama ili kategorijama prenesenih osobnih informacija;

(3) svrsi prikupljanja i upotrebe osobnih informacija (kako je odredio izvoznik podataka na temelju točke 1. ove Obavijesti);

(4) razdoblju pohrane osobnih informacija;

(5) informacijama o pravima ispitanika u vezi s obradom osobnih informacija, metodom i postupkom ostvarivanja prava i svim negativnim posljedicama ako ih njihovo ostvarenje uzrokuje.

ii. Isto tako, ako voditelj obrade osobnih informacija pruža osobne informacije iz točke i. trećoj strani u Republici Koreji ili inozemstvu, mora obavijestiti ispitanika o informacijama iz podtočaka od 1. do 5. prije pružanja osobnih informacija:

(1) imenu i informacijama za kontakt osoba koje pružaju i primaju osobne informacije;

(2) stavkama ili kategorijama pruženih osobnih informacija;

(3) državi u koju se pružaju osobne informacije, predviđenom datumu i metodi pružanja (ograničeno na slučajeve u kojima se osobne informacije pružaju trećoj strani u inozemstvu);

(4) svrsi pružatelja osobnih informacija i pravnoj osnovi za pružanje osobnih informacija;

(5) informacijama o pravima ispitanika u vezi s obradom osobnih informacija, metodom i postupkom ostvarivanja prava i svim negativnim posljedicama ako ih njihovo ostvarenje uzrokuje.

iii. Voditelj obrade osobnih informacija ne smije primijeniti točku i. ili ii. u sljedećim slučajevima iz podtočaka od 1. do 4.:

(1) ako su osobne informacije o kojima je potrebno obavijestiti uključene u bilo koju od datoteka s osobnim informacijama navedenih u članku 32. stavku 2. Zakona, pod uvjetom da interesi zaštićeni ovom odredbom očito imaju prednost pred pravima ispitanika i samo onoliko dugo koliko bi se obavješćivanjem ugrozilo ostvarenje predmetnih interesa, primjerice ako bi se ugrozile kaznene istrage u tijeku ili nacionalna sigurnost;

(2) ako i dok bi se obavješćivanjem vjerojatno ugrozio život ili zdravlje druge osobe ili nepravedno povrijedili imovinski interesi druge osobe ako ta prava ili interesi nedvojbeno imaju prednost pred pravima ispitanika;

(3) ako ispitanik već ima informacije o kojima voditelj obrade osobnih informacija mora obavješćivati u skladu s točkom i. ili ii.;

(4) ako voditelj obrade osobnih informacija nema informacije za kontakt ispitanika ili ako stupanje u kontakt s ispitanikom uključuje prekomjeran napor, među ostalim u kontekstu obrade prema uvjetima utvrđenima u odjeljku 3. PIPA-e. Pri određivanju toga je li moguće stupiti u kontakt s ispitanikom ili uključuje li to prekomjeran napor, trebalo bi uzeti u obzir mogućnost suradnje s izvoznikom podataka u EU-u.

([6]) Obveze iz točaka i., ii. i iii. primjenjuju se i kad voditelj obrade koji prima osobne informacije iz EU-a na temelju odluke o primjerenosti obrađuje takve informacije na temelju drugih zakona, primjerice Zakona o kreditnim informacijama.

4. **Područje primjene posebnog izuzeća od obrade pseudonimiziranih informacija (članci 28-2., 28-3., 28-4., 28-5., 28-6. i 28-7., članak 3. i članak 58-2. Zakona)**

<Zakon o zaštiti osobnih informacija

(Zakon br. 16930, djelomično izmijenjen 4. veljače 2020.)>

Poglavlje III. Obrada osobnih informacija

ODJELJAK 3. Posebni slučajevi povezani sa pseudonimiziranim podacima

Članak 28-2. (Obrada pseudonimiziranih podataka) 1. Voditelj obrade osobnih informacija može obrađivati pseudonimizirane informacije bez privole ispitanikâ u statističke svrhe, svrhe znanstvenog istraživanja, svrhe arhiviranja u javnom interesu i slično.

2. Pri pružanju pseudonimiziranih informacija trećoj strani u skladu sa stavkom 1. voditelj obrade osobnih informacija ne smije uključiti informacije koje bi se mogle iskoristiti za utvrđivanje identiteta određene osobe.

Članak 28-3. (Ograničenje kombiniranja pseudonimiziranih podataka) 1. Neovisno o članku 28-2., kombiniranje pseudonimiziranih informacija koje obrađuju različiti voditelji obrade osobnih informacija u statističke svrhe, radi znanstvenog istraživanja i čuvanje evidencija u javnom interesu itd., mora provoditi specijalizirana institucija koju imenuje Povjerenstvo za zaštitu ili čelnik povezane središnje upravne agencije.

2. Voditelj obrade osobnih informacija koji namjerava prenijeti kombinirane informacije izvan organizacije koja ih je kombinirala mora dobiti odobrenje čelnika specijalizirane institucije nakon pseudonimizacije informacija ili njihova pretvaranja u oblik iz članka 58-2.

3. Potrebne stavke propisuju se Predsjedničkim dekretom, uključujući postupke i metode kombiniranja na temelju stavka 1., standarde i postupke za imenovanje ili poništavanje imenovanja specijalizirane institucije, upravljanje i nadzor te standarde i postupke izvoza i odobrenja na temelju stavka 2.

Članak 28-4. (Obveza poduzimanja sigurnosnih mjera za pseudonimizirane podatke) 1. Pri obradi pseudonimiziranih informacija voditelj obrade osobnih informacija poduzima tehničke, organizacijske i fizičke mjere, kao što su zasebna pohrana i upravljanje dodatnim informacijama potrebnima za vraćanje u izvorno stanje, koje bi mogle biti potrebne za osiguranje sigurnosti kako je propisano Predsjedničkim dekretom da ne bi došlo do gubitka, krađe, otkrivanja, krivotvorenja, izmjene ili oštećenja osobnih informacija.

2. Voditelj obrade osobnih informacija koji namjerava obrađivati pseudonimizirane informacije sastavlja i čuva evidencije povezane sa stavkama propisanima Predsjedničkim dekretom, uključujući svrhu obrade pseudonimiziranih informacija, i povezane s trećom stranom kojoj se pružaju pseudonimizirane informacije radi upravljanja obradom pseudonimiziranih informacija.

Članak 28-5. (Zabranjene radnje u obradi pseudonimiziranih informacija) 1. Nitko ne smije obrađivati pseudonimizirane informacije u svrhu utvrđivanja identiteta određene osobe.

2. Ako se tijekom obrade pseudonimiziranih informacija generiraju informacije kojima se otkriva identitet određene osobe, voditelj obrade osobnih informacija prestaje s obradom tih informacija te ih odmah pronalazi i uništava.

Članak 28-6. (Izricanje dodatnih upravnih naknada za obradu pseudonimiziranih informacija) 1. Povjerenstvo može izreći novčanu kaznu u iznosu manjem od tristotog dijela ukupne prodaje voditelju obrade podataka koji je obrađivao podatke u svrhu utvrđivanja identiteta određene osobe u suprotnosti s člankom 28-5. stavkom 1.; pod uvjetom da se, ako nije bilo prodaje ili postoje poteškoće pri izračunavanju prihoda od prodaje, voditelju obrade podataka može izreći kazna od najviše 400 milijuna vona ili tristotog dijela kapitalnog iznosa, ovisno o tome što je veće.

2. Članak 34-2. stavci od 3. do 5. primjenjuju se *mutatis mutandis* na stavke potrebne za izricanje i prikupljanje dodatnih upravnih naknada.

Članak 28-7. (Područje primjene) Članci 20., 21., 27., članak 34. stavak 1., članci od 35. do 37., članci 39-3. i 39-4. te članci od 39-6. do 39-8. ne primjenjuju se na pseudonimizirane informacije.

Poglavlje I. Opće odredbe

Članak 3. (Načela za zaštitu osobnih informacija) 1. Voditelj obrade osobnih informacija mora izričito navesti svrhe obrade osobnih informacija i prikupljati osobne informacije zakonito, pošteno i u najmanjoj mjeri koja je potrebna za takve svrhe.

2. Voditelj obrade osobnih informacija obrađuje osobne informacije na prikladan način potreban za svrhe u koje se te informacije obrađuju i ne smije ih upotrebljavati izvan takvih svrha.

3. Voditelj obrade osobnih informacija osigurava da su osobne informacije točne, potpune i ažurne u mjeri u kojoj je to potrebno za svrhe u koje se osobne informacije obrađuju.

4. Voditelj obrade osobnih informacija upravlja osobnim informacijama na siguran način u skladu s metodama obrade, vrstom i drugim obilježjima osobnih informacija, uzimajući u obzir mogućnost povrede prava ispitanika i ozbiljnost relevantnih rizika.

5. Voditelj obrade osobnih informacija objavljuje svoju politiku zaštite privatnosti i druga pitanja povezana s obradom osobnih informacija te jamči prava ispitanika, kao što je pravo na pristup vlastitim osobnim informacijama.

6. Voditelj obrade osobnih informacija obrađuje osobne informacije tako da se mogućnost povrede privatnosti ispitanika svede na najmanju mjeru.

7. Ako je i dalje moguće ostvariti svrhe prikupljanja osobnih informacija obradom anonimiziranih ili pseudonimiziranih osobnih informacija, voditelj obrade osobnih informacija nastoji obrađivati osobne informacije anonimizacijom, ako je moguća, ili pseudonimizacijom ako nije moguće ostvariti svrhe prikupljanja osobnih informacija anonimizacijom.

8. Voditelj obrade osobnih informacija nastoji zadobiti povjerenje ispitanika tako da poštuje i izvršava zadaće i odgovornosti predviđene Zakonom i drugim povezanim propisima.

Poglavlje IX. Dopunske odredbe

Članak 58-2. (Izuzeće od primjene) Ovaj se Zakon ne primjenjuje na informacije kojima se, kad se kombiniraju s drugim informacijama, više ne može utvrditi identitet određenog pojedinca, uzimajući u obzir u razumnoj mjeri vrijeme, trošak, tehnologiju itd. <ovaj je članak dodan Zakonom br. 16930, 4. veljače 2020.>

i. Poglavljem III., odjeljkom 3. „Posebni slučajevi povezani sa pseudonimiziranim podacima" (članci od 28-2. do 28-7.) omogućuje se obrada pseudonimiziranih informacija bez privole ispitanika u svrhu prikupljanja statističkih podataka, znanstvenog istraživanja, čuvanja javne evidencije itd. (članak 28-2.), no u takvim su slučajevima obavezne prikladne zaštitne mjere i zabrane potrebne za zaštitu prava ispitanika (članci 28-4. i 28-5.), počiniteljima se mogu izreći dodatne kaznene naknade (članak 28-6.), a ne primjenjuju se određene zaštitne mjere koje su inače dostupne na temelju PIPA-e (članak 28-7.).

ii. Te se odredbe ne primjenjuju u slučajevima u kojima se pseudonimizirane informacije obrađuju u svrhe koje nisu prikupljanje statističkih podataka, znanstveno istraživanje, čuvanje javne evidencije itd. Primjerice, ako su osobne informacije pojedinca u EU-u koje su prenesene u Koreju na temelju odluke o primjerenosti Europske komisije pseudonimizirane u svrhe koje nisu prikupljanje statističkih podataka, znanstveno istraživanje, čuvanje javne evidencije itd., ne primjenjuju se posebne odredbe iz poglavlja III. odjeljka 3. ([7])

iii. Ako voditelj obrade osobnih informacija obrađuje pseudonimizirane informacije u svrhu prikupljanja statističkih podataka, znanstvenog istraživanja i čuvanja javne evidencije itd. te ako pseudonimizirane informacije nisu uništene nakon što se ostvari konkretna svrha obrade u skladu s člankom 37. Ustava i člankom 3. (Načela za zaštitu osobnih informacija) Zakona, voditelj obrade mora anonimizirati informacije kako bi se osiguralo da se njima više ne može utvrditi identitet određene osobe samostalno ili u kombinaciji s drugim informacijama, uzimajući u obzir u razumnoj mjeri vrijeme, trošak, tehnologiju itd. u skladu s člankom 58-2. PIPA-e.

5. **Korektivne mjere i drugo (članak 64. stavci 1., 2. i 4. Zakona)**

<Zakon o zaštiti osobnih informacija

(Zakon br. 16930, djelomično izmijenjen 4. veljače 2020.)>

Članak 64. (Korektivne mjere) 1. Ako Povjerenstvo za zaštitu utvrdi da postoji opravdana osnova na temelju koje se smatra da je došlo do povrede u vezi s osobnim informacijama, a nepoduzimanje mjera vjerojatno će uzrokovati štetu koju je teško popraviti, može naložiti subjektu koji je prekršio ovaj Zakon (uključujući središnje upravne agencije, lokalnu vlast, Nacionalnu skupštinu, Sud, Ustavni sud i Nacionalno izborno povjerenstvo) da poduzme bilo koju od sljedećih mjera:

1. suspenziju povrede povezane s osobnim informacijama;

2. privremenu suspenziju obrade osobnih informacija;

([7]) Slično tome, izuzeće iz članka 40-3. Zakona o kreditnim informacijama primjenjuje se samo na obradu pseudonimiziranih kreditnih informacija u svrhe prikupljanja statističkih podataka, znanstvenog istraživanja i čuvanja javne evidencije.

3. druge mjere potrebne za zaštitu osobnih informacija i sprečavanje povrede osobnih informacija.

2. Ako čelnik povezane središnje upravne agencije smatra da postoji opravdana osnova na temelju koje se smatra da je došlo do povrede u vezi s osobnim informacijama, a nepoduzimanje mjera vjerojatno će uzrokovati štetu koju je teško popraviti, može naložiti voditelju obrade osobnih informacija da poduzme bilo koju od mjera predviđenih stavkom 1. na temelju propisâ pod nadležnošću takve povezane središnje upravne agencije.

4. Ako središnja upravna agencija, lokalna vlast, Nacionalna skupština, Sud, Ustavni sud ili Nacionalno izborno povjerenstvo prekrši ovaj Zakon, Povjerenstvo za zaštitu može preporučiti čelniku relevantne agencije da poduzme bilo koju od mjera predviđenih stavkom 1. U takvim slučajevima agencija po zaprimanju preporuke mora postupiti u skladu s njome, osim ako postoje izvanredne okolnosti.

i. Prvo, u sudskim presedanima ([8]), ([9]) „šteta koju je teško popraviti" tumači se kao slučaj u kojem bi se narušila osobna prava ili privatnost pojedinca.

ii. U skladu s tim, dio „opravdana osnova na temelju koje se smatra da je došlo do povrede u vezi s osobnim informacijama, a nepoduzimanje mjera vjerojatno će uzrokovati štetu koju je teško popraviti" propisan člankom 64. stavcima 1. i 2. odnosi se na slučajeve u kojima se smatra da će se kršenjem zakona vjerojatno povrijediti prava i sloboda pojedinaca u vezi s osobnim informacijama. To se primjenjuje kad se god prekrše bilo koja načela, prava i obveze koji su uključeni u zakonodavstvo radi zaštite osobnih informacija ([10]).

iii. U skladu s člankom 64. stavkom 4. Zakona o zaštiti osobnih informacija riječ je o mjeri u vezi s „kršenjem ovog Zakona", tj. radnji protiv kršenja PIPA-e.

Središnja upravna agencija ili slično tijelo, kao javno tijelo obvezno vladavinom prava, ne smije prekršiti nijedan zakon i obvezno je poduzeti korektivnu mjeru, među ostalim odmah prestati s određenom radnjom, i nadoknaditi štetu u iznimnom slučaju u kojem je ipak počinjena nezakonita radnja.

U skladu s tim, čak i bez intervencije Povjerenstva za zaštitu u skladu s člankom 64. stavkom 4. PIPA-e, središnja upravna agencija ili slično tijelo mora poduzeti korektivnu mjeru protiv prekršaja ako postane svjesno bilo kakvog kršenja zakona.

Posebice, ako je Povjerenstvo za zaštitu preporučilo korektivnu mjeru, središnjoj upravnoj agenciji ili sličnom tijelu obično će objektivno biti jasno da je prekršilo zakon. Stoga, kako bi opravdala zašto smatra da ne bi trebala postupati prema preporuci Povjerenstva za zaštitu, središnja upravna agencija ili slično tijelo mora predstaviti jasnu osnovu na temelju koje može dokazati da nije prekršen zakon. Osim ako Povjerenstvo za zaštitu utvrdi da do toga ipak nije došlo, preporuka se mora poštovati.

S obzirom na navedeno, „izvanredne okolnosti" iz članka 64. stavka 4. Zakona o zaštiti osobnih informacija moraju se strogo ograničiti na izvanredne okolnosti u kojima postoji jasna osnova na temelju koje središnje upravne agencije ili slična tijela mogu dokazati da „Zakon u biti nije prekršen", kao što su „slučajevi u kojima postoje izvanredne (činjenične ili pravne) okolnosti" za koje Povjerenstvo za zaštitu nije znalo kad je prvotno dalo svoju preporuku i to povjerenstvo utvrdi da zapravo nije došlo do prekršaja.

6. **Primjena PIPA-e na obradu osobnih podataka u svrhu nacionalne sigurnosti, uključujući istragu kršenja i izvršenje u skladu s PIPA-om (članci 7-8., 7-9., 58., 3., 4. i 62. PIPA-e)**

<Zakon o zaštiti osobnih informacija

(Zakon br. 16930, djelomično izmijenjen 4. veljače 2020.)>

Članak 7-8. (Djelovanje Povjerenstva za zaštitu) 1. Povjerenstvo za zaštitu zaduženo je za sljedeće: […]

3. pitanja povezana s istragom povrede prava ispitanikâ i odluke koje iz toga proizlaze;

4. rješavanje pritužbi ili provedbu postupaka za popravljanje štete u vezi s obradom osobnih informacija i posredovanje u sporovima o osobnim informacijama;

[…]

([8]) (Presuda Vrhovnog suda br. 97Da10215,10222 od 26. siječnja 1999.) Ako se kriminalne činjenice optuženika otkriju putem medija, vjerojatno je da će nanijeti nepopravljivu mentalnu i fizičku štetu ne samo žrtvi, tj. tužitelju, već i osobama bliskima toj osobi, uključujući obitelji.

([9]) (Presuda Visokog suda u Seoulu br. 2006Na92006 od 16. siječnja 2008.) Ako se objavi klevetnički članak, vjerojatno će uzrokovati ozbiljnu nepopravljivu štetu uključenoj osobi.

([10]) Ista načela kakva su utvrđena točkom ii. primjenjuju se na članak 45-4. Zakona o kreditnim informacijama.

Članak 7-9. (Pitanja koja razmatra i o kojima odlučuje Povjerenstvo za zaštitu) 1. Povjerenstvo za zaštitu razmatra sljedeća pitanja i odlučuje o njima: […]

5. pitanja o tumačenju i primjeni prava povezana sa zaštitom osobnih informacija;

[…]

Članak 58. (Djelomično izuzeće od primjene) 1. Poglavlja od III. do VII. ne primjenjuju se na sljedeće osobne informacije:

1. osobne informacije prikupljene na temelju Zakona o statističkim podacima radi obrade koju vrše javne institucije;

2. osobne informacije prikupljene ili zatražene radi analize informacija povezanih s nacionalnom sigurnošću;

3. osobne informacije koje se privremeno obrađuju ako je to hitno potrebno radi javne zaštite i sigurnosti, javnog zdravlja itd.;

4. osobne informacije koje mediji prikupljaju ili upotrebljavaju u vlastite svrhe izvješćivanja, koje vjerske organizacije prikupljaju ili upotrebljavaju u misionarskim aktivnostima i koje političke stranke prikupljaju i upotrebljavaju radi imenovanja kandidata.

[Izostavljeni su stavci 2. i 3.]

4. Kad je riječ o obradi osobnih informacija na temelju stavka 1., voditelj obrade osobnih informacija obrađuje osobne informacije u najmanjoj mjeri koja je potrebna za predviđenu svrhu tijekom minimalnog razdoblja, a isto tako poduzima potrebne mjere, kao što su tehničke, upravljačke i fizičke zaštitne mjere, rješavanje pojedinačnih pritužbi i druge potrebne mjere za sigurno upravljanje i prikladnu obradu takvih osobnih informacija.

Članak 3. (Načela za zaštitu osobnih informacija) 1. Voditelj obrade osobnih informacija mora izričito navesti svrhe obrade osobnih informacija i prikupljati osobne informacije zakonito, pošteno i u najmanjoj mjeri koja je potrebna za takve svrhe.

2. Voditelj obrade osobnih informacija obrađuje osobne informacije na prikladan način potreban za svrhe u koje se te informacije obrađuju i ne smije ih upotrebljavati izvan takvih svrha.

3. Voditelj obrade osobnih informacija osigurava da su osobne informacije točne, potpune i ažurne u mjeri u kojoj je to potrebno za svrhe u koje se osobne informacije obrađuju.

4. Voditelj obrade osobnih informacija upravlja osobnim informacijama na siguran način u skladu s metodama obrade, vrstom i drugim obilježjima osobnih informacija, uzimajući u obzir mogućnost povrede prava ispitanika i ozbiljnost relevantnih rizika.

5. Voditelj obrade osobnih informacija objavljuje svoju politiku zaštite privatnosti i druga pitanja povezana s obradom osobnih informacija te jamči prava ispitanika, kao što je pravo na pristup vlastitim osobnim informacijama.

6. Voditelj obrade osobnih informacija obrađuje osobne informacije tako da se mogućnost povrede privatnosti ispitanika svede na najmanju mjeru.

7. Ako je i dalje moguće ostvariti svrhe prikupljanja osobnih informacija obradom anonimiziranih ili pseudonimiziranih osobnih informacija, voditelj obrade osobnih informacija nastoji obrađivati osobne informacije anonimizacijom, ako je moguća, ili pseudonimizacijom ako nije moguće ostvariti svrhe prikupljanja osobnih informacija anonimizacijom.

8. Voditelj obrade osobnih informacija nastoji zadobiti povjerenje ispitanika tako da poštuje i izvršava zadaće i odgovornosti predviđene Zakonom i drugim povezanim propisima.

Članak 4. (Prava ispitanika) Ispitanik ima sljedeća prava u vezi s obradom svojih osobnih informacija:

1. pravo da bude informiran o obradi takvih osobnih informacija;

2. pravo odlučiti hoće li dati privolu i opseg te privole u vezi s obradom takvih osobnih informacija;

3. pravo provjeriti obrađuju li se osobne informacije i zatražiti pristup takvim osobnim informacijama (uključujući pružanje kopija; to se primjenjuje i na sljedeće odredbe);

4. pravo suspendirati obradu takvih osobnih informacija i zatražiti njihov ispravak, brisanje i uništenje;

5. pravo na prikladnu pravnu zaštitu za svaku štetu koja proizlazi iz obrade takvih osobnih informacija u okviru brzog i poštenog postupka.

Članak 62. (Izvješćivanje o povredama) 1. Svatko tko pretrpi povredu prava ili interesa u vezi sa svojim osobnim informacijama dok voditelj obrade osobnih informacija obrađuje osobne informacije može izvijestiti Povjerenstvo za zaštitu o takvoj povredi.

2. Povjerenstvo za zaštitu može imenovati specijaliziranu instituciju kako bi se učinkovito zaprimala i obrađivala izvješća o zahtjevima na temelju stavka 1., kako je propisano Predsjedničkim dekretom. U takvim slučajevima specijalizirana institucija uspostavlja i upravlja pozivnim centrom za povrede osobnih informacija (dalje u tekstu „Pozivni centar za zaštitu privatnosti").

3. Pozivni centar za zaštitu privatnosti izvršava sljedeće zadaće:

1. zaprimanje izvješća o zahtjevima i savjetovanje u vezi s obradom osobnih informacija;

2. istragu i potvrdu incidenata te saslušavanje mišljenja uključenih stranaka;

3. zadaće povezane sa stavcima 1. i 2.

4. Povjerenstvo za zaštitu može, prema potrebi, poslati svojeg javnog službenika u specijaliziranu instituciju imenovanu na temelju stavka 2. u skladu s člankom 32-4. Zakona o državnim javnim službenicima kako bi se učinkovito istražili i potvrdili incidenti na temelju stavka 3. točke 2.

i. Prikupljanje osobnih informacija u svrhu nacionalne sigurnosti uređeno je posebnim zakonima kojima se nadležna tijela (npr. Nacionalna obavještajna služba) ovlašćuju da presreću komunikacije i zatraže otkrivanje u određenim uvjetima i uz zaštitne mjere (dalje u tekstu „zakoni o nacionalnoj sigurnosti"). Takvi zakoni o nacionalnoj sigurnosti uključuju primjerice Zakon o zaštiti privatnosti komunikacija, Zakon o borbi protiv terorizma radi zaštite građana i javne sigurnosti ili Zakon o telekomunikacijama. Osim toga, prikupljanje i daljnja obrada osobnih informacija moraju biti u skladu sa zahtjevima PIPA-e. U tom se kontekstu člankom 58. stavkom 1. točkom 2. PIPA-e propisuje da se poglavlja od III. do VII. ne primjenjuju na osobne informacije prikupljene ili zatražene radi analize informacija povezanih s nacionalnom sigurnošću. Stoga se to djelomično izuzeće primjenjuje na obradu osobnih informacija u svrhu nacionalne sigurnosti.

Istodobno, poglavlje I. (Opće odredbe), poglavlje II. (Uspostava politika o zaštiti osobnih informacija i drugo), poglavlje VIII. (Zajednička tužba u vezi s povredom podataka), poglavlje IX. (Dopunske odredbe) i poglavlje X. (Odredbe o sankcijama) PIPA-e primjenjuju se na obradu takvih osobnih informacija. To uključuje opća načela zaštite podataka utvrđena u članku 3. (Načela za zaštitu osobnih informacija) i pojedinačna prava zajamčena člankom 4. PIPA-e (Prava ispitanika).

Usto, člankom 58. stavkom 4. PIPA-e propisuje se da se takve informacije moraju obrađivati u najmanjoj mjeri koja je potrebna za predviđenu svrhu i tijekom minimalnog razdoblja; od voditelja obrade osobnih informacija zahtijeva se i da uvede potrebne mjere za osiguranje sigurnog upravljanja podacima i prikladne obrade, kao što su tehničke, upravljačke i fizičke zaštitne mjere te mjere za prikladno rješavanje pojedinačnih pritužbi.

Na kraju, primjenjuju se odredbe kojima se uređuju zadaće i ovlasti PIPC-a (uključujući članke od 60. do 65. PIPA-e o rješavanju pritužbi i donošenju preporuka i korektivnih mjera) te odredbe o upravnim i kaznenim sankcijama (članak 70. i dalje PIPA-e). U skladu s člankom 7-8. stavkom 1. točkama 3. i 4. te člankom 7-9. stavkom 1. točkom 5. PIPA-e, te istražne i korektivne ovlasti, među ostalim kad se izvršavaju u kontekstu rješavanja pritužbi, obuhvaćaju i moguće povrede pravila iz određenih zakona u kojima se utvrđuju ograničenja i zaštitne mjere za prikupljanje osobnih informacija, kao što su zakoni o nacionalnoj sigurnosti. S obzirom na zahtjeve iz članka 3. stavka 1. PIPA-e za zakonito i pošteno prikupljanje osobnih informacija, svaka takva povreda ujedno je i kršenje „ovog Zakona" u smislu članaka 63. i 64., čime se PIPC-u dopušta da provodi istragu i poduzme korektivne mjere ([11]). Izvršavanje tih ovlasti PIPC-a dopunjuje, ali ne zamjenjuje ovlasti Nacionalnog povjerenstva za ljudska prava na temelju Zakona o povjerenstvu za ljudska prava.

Primjena temeljnih načela, prava i obveza PIPA-e na obradu osobnih informacija u svrhu nacionalne sigurnosti odražava jamstva predviđena Ustavom za zaštitu prava pojedinca da upravlja vlastitim osobnim informacijama. Kako je priznao Ustavni sud, to uključuje pravo osobe ([12]) „da sama odluči o tome kad će se njezine informacije otkrivati ili upotrebljavati, tko će to činiti ili za koga će se to činiti te u kojoj mjeri. To je osnovno pravo ([13]), […], koje postoji kako bi se osobna sloboda odlučivanja zaštitila od rizika uzorkovanog proširenjem državnih funkcija i informacijsko-komunikacijskim tehnologijama." Svako ograničenje tog prava, primjerice ako je to potrebno za zaštitu nacionalne sigurnosti, zahtijeva uravnoteženje prava i interesa pojedinca i relevantnog javnog interesa te ne smije utjecati na bit tog prava (članak 37. stavak 2. Ustava).

([11]) Vidjeti i odjeljak 5. u vezi s korektivnim mjerama na temelju članka 64.
([12]) Presuda Ustavnog suda, 99HunMa513, 2004HunMa190, od 26. svibnja 2005.
([13]) Presuda Ustavnog suda, 2003HunMa282, od 21. srpnja 2005.

Stoga pri obradi osobnih informacija za potrebe nacionalne sigurnosti voditelj obrade (npr. NIS) mora, među ostalim:

1. izričito navesti svrhe u koje se osobne informacije obrađuju te prikupljati osobne informacije zakonito, pošteno i u najmanjoj mjeri koja je potrebna za takve svrhe (članak 3. stavak 1. PIPA-e); točnije, prikuplja i dodatno obrađuje osobne informacije u svrhu izvršavanja zadaća na temelju relevantnih propisa, kao što je Zakon o Nacionalnoj obavještajnoj službi;

2. obrađivati osobne informacije u najmanjoj mjeri i tijekom minimalnog razdoblja koji su potrebni za predviđenu svrhu (članak 58. stavak 4. PIPA-e); nakon ispunjenja svrhe obrade, voditelj obrade nepovratno uništava osobne informacije, osim ako se daljnja pohrana izričito zahtijeva propisom, a u tom se slučaju relevantne osobne informacije pohranjuju i njima se upravlja zasebno od drugih osobnih informacija te se ne smiju upotrebljavati ni u koju drugu svrhu osim one koja je utvrđena propisom i uništavaju se na kraju razdoblja pohrane;

3. obrađivati osobne informacije na prikladan način potreban za svrhe u koje se te informacije obrađuju i ne smije ih upotrebljavati izvan takvih svrha (članak 3. stavak 2. PIPA-e);

4. osigurati da su osobne informacije točne, potpune i ažurne u mjeri u kojoj je to potrebno za svrhe u koje se osobne informacije obrađuju (članak 3. stavak 3. PIPA-e);

5. upravljati osobnim informacijama na siguran način u skladu s metodama obrade, vrstom i drugim obilježjima osobnih informacija, uzimajući u obzir mogućnost povrede prava ispitanika i ozbiljnost relevantnih rizika (članak 3. stavak 4. PIPA-e);

6. objaviti svoju politiku zaštite privatnosti i druga pitanja povezana s obradom osobnih informacija (članak 3. stavak 5. PIPA-e);

7. obrađivati osobne informacije tako da se mogućnost povrede privatnosti ispitanika svede na najmanju mjeru (članak 3. stavak 6. PIPA-e).

ii. U skladu s člankom 58. stavkom 4. PIPA-e voditelj obrade (npr. tijela nadležna za nacionalnu sigurnost kao što je NIS) poduzima potrebne mjere, kao što su uvođenje tehničkih, upravljačkih i fizičkih zaštitnih mjera, kako bi se osigurale usklađenost s tim načelima i prikladna obrada osobnih informacija. Primjerice, to može uključivati posebne mjere za osiguranje sigurnosti osobnih informacija, kao što su ograničenja pristupa osobnim informacijama, kontrole pristupa, zapisnici, osiguravanje posebnog osposobljavanja o postupanju s osobnim informacijama za zaposlenike itd.

Usto, u skladu s člankom 3. stavkom 5. i člankom 4. PIPA-e ispitanici među ostalim imaju sljedeća prava u vezi s osobnim informacijama koje se obrađuju u svrhu nacionalne sigurnosti:

1. pravo na dobivanje potvrde o tome obrađuju li se njihove osobne informacije, dobivanje informacija o obradi te pravo na pristup tim informacijama, uključujući pružanje kopija (članak 4. stavci 1. i 3. PIPA-e);

2. pravo na suspenziju obrade te na ispravak, brisanje i uništenje osobnih informacija (članak 4. stavak 4. PIPA-e).

iii. Ispitanik može podnijeti zahtjev za ostvarivanje tih prava izravno voditelju obrade ili neizravno preko Povjerenstva za zaštitu te može ovlastiti svojeg predstavnika da to učini. Ako ispitanik podnese zahtjev, voditelj obrade izvršava to pravo bez odgode; no može i odgoditi, ograničiti ili odbiti to pravo ako je to izričito predviđeno drugim propisima ili ako je to neizbježno radi usklađenosti s njima u mjeri i onoliko dugo koliko je to potrebno i razmjerno za zaštitu važnog cilja od javnog interesa (primjerice u mjeri i onoliko dugo koliko bi se izvršavanjem prava ugrozila istraga u tijeku ili nacionalna sigurnost) ili ako bi se izvršavanjem prava mogao ugroziti život ili zdravlje treće strane ili uzrokovati neopravdana povreda imovine i drugih interesa treće strane. Ako se zahtjev odbije ili ograniči, voditelj obrade bez odgode obavještava ispitanika o razlozima za to. Voditelj obrade priprema metodu i postupak kojim će se ispitanicima omogućiti da podnose zahtjeve i objavljuje ih kako bi ispitanici mogli o njima biti obaviješteni.

Nadalje, u skladu s člankom 58. stavkom 4. PIPA-e (zahtjev da se osigura prikladno rješavanje pojedinačnih pritužbi) i člankom 4. stavkom 5. PIPA-e (pravo na prikladnu pravnu zaštitu za svaku štetu koja proizlazi iz obrade osobnih informacija u okviru brzog i poštenog postupka), ispitanici imaju pravo na dobivanje pravne zaštite. To uključuje pravo prijaviti navodno kršenje Centru za prijavljivanje povreda osobnih informacija (u skladu s člankom 62. stavkom 3. PIPA-e), podnijeti pritužbu PIPC-u na temelju članka 62. PIPA-e o bilo kakvom kršenju u vezi s pravima ili interesima povezanima s osobnim informacijama pojedinca i dobiti sudsku zaštitu u pogledu odluka ili nedjelovanja PIPC-a na temelju Zakona o upravnim sporovima. Osim toga, ispitanici mogu dobiti sudsku zaštitu na temelju Zakona o upravnim sporovima ako je došlo do povrede njihovih prava ili interesa zbog odluke ili propusta voditelja obrade (npr. nezakonito prikupljanje osobnih podataka) ili primiti naknadu za štetu u skladu sa Zakonom o naknadi od države. Te su mogućnosti za pravnu zaštitu dostupne u slučaju mogućih povreda pravila iz određenih zakona u kojima se utvrđuju ograničenja i zaštitne mjere za prikupljanje osobnih informacija, kao što su zakoni o nacionalnoj sigurnosti, i PIPA-e.

Pojedinac iz EU-a može podnijeti pritužbu PIPC-u preko svojeg nacionalnog tijela za zaštitu podataka, a PIPC će obavijestiti pojedinca preko nacionalnog tijela za zaštitu podataka nakon zaključenja istrage i korektivne mjere (prema potrebi).

PRILOG II.

18. svibnja 2021.

Njegova Ekscelencija Didier Reynders, povjerenik Europske komisije za pravosuđe

Vaša Ekscelencijo,

pozdravljam konstruktivne razgovore između Koreje i Europske komisije čiji je cilj stvaranje okvira za prijenos osobnih podataka iz EU-a u Koreju.

Na zahtjev Europske komisije upućen vladi Koreje, dostavljam Vam priloženi dokument u kojem se daje pregled pravnog okvira u vezi s pristupom korejske vlade informacijama.

Dokument se odnosi na brojna ministarstva i agencije vlade Koreje, a kad je riječ o sadržaju dokumenta, relevantna ministarstva i agencije (Povjerenstvo za zaštitu osobnih informacija, Ministarstvo pravosuđa, Nacionalna obavještajna služba, Korejsko nacionalno povjerenstvo za ljudska prava, Nacionalni centar za borbu protiv terorizma, Korejska financijsko-obavještajna jedinica) odgovorni su za dijelove u okviru njihovih nadležnosti. U nastavku su navedena relevantna ministarstva i agencije s priloženim potpisima.

Povjerenstvo za zaštitu osobnih informacija prihvaća sve upite povezane s ovim dokumentom te će koordinirati potrebne odgovore među relevantnim ministarstvima i agencijama.

Nadam se da će ovaj dokument pomoći u donošenju odluka Europske komisije.

Cijenim Vaš izniman doprinos u vezi s ovim pitanjem.

S poštovanjem,

Yoon Jong In
Predsjednik Povjerenstva za zaštitu osobnih informacija

Ovaj dokument sastavili su Povjerenstvo za zaštitu osobnih informacija i sljedeća relevantna ministarstva i agencije.

Park Jie Won
Predsjednik (direktor) Nacionalne obavještajne službe

Lee Jung Soo
Glavni direktor Ministarstva pravosuđa

Choi Young Ae
Predsjednica Korejskog nacionalnog povjerenstva za ljudska prava

Kim Hyuck Soo
Direktor Nacionalnog centra za borbu protiv terorizma

Kim Jeong Kag
Povjerenik Korejske financijsko-obavještajne jedinice

Pravni okvir za prikupljanje i upotrebu osobnih podataka koje vrše korejska javna tijela u svrhu kaznenog progona i nacionalne sigurnosti

U sljedećem se dokumentu daje pregled pravnog okvira za prikupljanje i upotrebu osobnih podataka koje vrše korejska javna tijela u svrhu kaznenog progona i nacionalne sigurnosti (dalje u tekstu „pristup vlade"), posebno u pogledu dostupnih pravnih osnova, primjenjivih uvjeta (ograničenja) i zaštitnih mjera, kao i neovisnih mogućnosti nadzora i pojedinačnih mogućnosti pravne zaštite.

1. OPĆA PRAVNA NAČELA RELEVANTNA ZA PRISTUP VLADE

1.1. Ustavni okvir

U Ustavu Republike Koreje općenito se utvrđuje pravo na privatnost (članak 17.), a posebice pravo na privatnost korespondencije (članak 18.). Država je dužna zajamčiti ta temeljna prava ([1]). U Ustavu se nadalje propisuje da se prava i slobode građana mogu ograničiti samo zakonom i ako je to potrebno radi nacionalne sigurnosti ili održavanja javnog poretka za dobrobit građana ([2]). Čak i ako se nametnu takva ograničenja, njima se ne smije narušiti bit slobode ili prava ([3]). Korejski sudovi primjenjivali su te odredbe u predmetima koji su se odnosili na zadiranje vlade u privatnost. Primjerice, Vrhovni sud utvrdio je da se praćenjem građana krši temeljno pravo na privatnost i istaknuo je da građani imaju „pravo na samoodređenje u pogledu osobnih informacija" ([4]). U drugom je predmetu Ustavni sud presudio da je privatnost temeljno pravo kojim se pruža zaštita od državne intervencije i praćenja u privatnom životu građana ([5]).

Ustavom Koreje jamči se i da se nijednu osobu neće uhititi, zadržati, pretražiti, ispitivati ili da se njezino vlasništvo neće zaplijeniti osim kako je predviđeno zakonom ([6]). Nadalje, pretrage i zapljene mogu se vršiti samo na temelju naloga koji izdaje sudac na zahtjev tužitelja u skladu s odgovarajućim postupkom ([7]). U iznimnim okolnostima, tj. ako je osumnjičenik za kazneno djelo uhićen pri počinjenju kaznenog djela (*flagrante delicto*) ili ako postoji rizik da bi osoba osumnjičena za kazneno djelo kažnjivo zatvorom u trajanju od tri godine ili više mogla pobjeći ili uništiti dokaze, istražna tijela mogu izvršiti pretragu ili zapljenu bez naloga, a u tom slučaju moraju naknadno zatražiti nalog ([8]). Ta su opća načela dodatno objašnjena u posebnim zakonima koji se odnose na kazneni postupak i zaštitu komunikacija (vidjeti detaljan pregled u nastavku).

Kad je riječ o stranim državljanima, Ustavom se propisuje da je njihov status zajamčen kako je utvrđeno međunarodnim pravom i ugovorima ([9]). Koreja je potpisnica više međunarodnih sporazuma kojima se jamče prava na privatnost, kao što su Međunarodni pakt o građanskim i političkim pravima (članak 17.), Konvencija o pravima osoba s invaliditetom (članak 22.) i Konvencija o pravima djeteta (članak 16.). Osim toga, iako se Ustav u načelu odnosi na prava „građana", Ustavni sud presudio je da i strani državljani imaju osnovna prava ([10]). Sud je konkretno utvrdio da su zaštita dostojanstva i vrijednosti osobe kao ljudskog bića te pravo na težnju sreći prava bilo kojeg ljudskog bića, a ne samo

([1]) Članak 10. Ustava Republike Koreje, proglašenog 17. srpnja 1948. (dalje u tekstu „Ustav").
([2]) Članak 37. stavak 2. Ustava.
([3]) Članak 37. stavak 2. Ustava.
([4]) Odluka Vrhovnog suda Koreje br. 96DA42789, 24. srpnja 1998.
([5]) Odluka Ustavnog suda br. 2002Hun-Ma51, 30. listopada 2003. Slično tome, u odlukama br. 99Hun-Ma513 i 2004Hun-Ma190 (konsolidirane) od 26. svibnja 2005. Ustavni sud pojasnio je da je „pravo na upravljanje vlastitim osobnim informacijama pravo osobe na koju se informacije odnose da sama odluči o tome kad će se njezine informacije otkrivati ili upotrebljavati, tko će to činiti ili kome će se otkrivati te u kojoj mjeri. Iako nije navedeno u Ustavu, to je osnovno pravo koje postoji kako bi se osobna sloboda odlučivanja zaštitila od rizika uzorkovanog proširenjem državnih funkcija i informacijsko-komunikacijskim tehnologijama."
([6]) Članak 12. stavak 1. prva rečenica Ustava.
([7]) Članak 16. i članak 12. stavak 3. Ustava.
([8]) Članak 12. stavak 3. Ustava.
([9]) Članak 6. stavak 2. Ustava.
([10]) Odluka Ustavnog suda br. 93Hun-MA120, 29. prosinca 1994. Vidjeti i primjerice Odluku Ustavnog suda br. 2014Hun-Ma346 (31. svibnja 2018.), u kojoj je Sud utvrdio da je sudanskom državljaninu koji je zadržan u zračnoj luci povrijeđeno ustavno pravo na primanje pomoći pravnog zastupnika. U drugom je predmetu Ustavni sud utvrdio da je sloboda odabira zakonskog radnog mjesta blisko povezana s pravom na ostvarivanje sreće, ljudsko dostojanstvo i vrijednost te stoga nije rezervirana samo za građane, već se može zajamčiti i stranim državljanima koji su zakonito zaposleni u Republici Koreji (Odluka Ustavnog suda br. 2007Hun-Ma1083, 29. rujna 2011.).

građana ([11]). Sud je pojasnio i da se pravo na upravljanje vlastitim informacijama smatra osnovnim pravom, utemeljenim na pravu na dostojanstvo i ostvarivanje sreće te pravu na privatni život ([12]). Stoga se, iako se sudska praksa dosad nije izričito bavila pravom na privatnost stranih državljana, stručnjaci općenito slažu da se člancima od 12. do 22. Ustava (koji uključuju pravo na privatnost i osobnu slobodu) utvrđuju „prava ljudskih bića".

U konačnici, Ustavom je predviđeno i pravo na zahtijevanje poštene naknade od javnih tijela ([13]). Nadalje, na temelju Zakona o Ustavnom sudu svaka osoba čija se temeljna prava zajamčena Ustavom povrijede izvršavanjem državnih ovlasti (ne uključujući sudske presude) može uložiti ustavnu žalbu pri Ustavnom sudu ([14]).

1.2. **Opća pravila o zaštiti podataka**

Opći zakon o zaštiti podataka u Republici Koreji, Zakon o zaštiti osobnih informacija (dalje u tekstu „PIPA"), primjenjuje se i na privatni i na javni sektor. Kad je riječ o javnim tijelima, u PIPA-i se izričito upućuje na obvezu osmišljavanja politika kako bi se spriječila „zlouporaba i pogrešna upotreba osobnih informacija, neselektivan nadzor i praćenje itd. te da bi se unaprijedilo dostojanstvo ljudskih bića i privatnost pojedinaca." ([15])

Obrada osobnih podataka u svrhu kaznenog progona podliježe svim zahtjevima iz PIPA-e. To primjerice znači da tijela kaznenog progona moraju postupati u skladu s obvezama zakonite obrade, tj. moraju se oslanjati na jednu od pravnih osnova navedenih u PIPA-i za prikupljanje, upotrebu ili pružanje osobnih informacija (članci od 15. do 18. PIPA-e), kao i na načela ograničavanja svrhe (članak 3. stavci 1. i 2. PIPA-e), proporcionalnosti/smanjenja količine podataka (članak 3. stavci 1. i 6. PIPA-e), ograničene pohrane podataka (članak 21. PIPA-e), sigurnosti podataka, uključujući izvješćivanje o povredi osobnih podataka (članak 3. stavak 4. te članci 29. i 34. PIPA-e) i transparentnosti (članak 3. stavci 1. i 5. te članci 20., 30. i 32. PIPA-e). Za osjetljive informacije primjenjuju se posebne zaštitne mjere (članak 23. PIPA-e). Štoviše, u skladu s člankom 3. stavkom 5. i člankom 4. PIPA-e, kao i njezinim člancima od 35. do 39-2., pojedinci mogu ostvariti svoja prava na pristup, ispravak, brisanje i suspenziju u pogledu tijelâ kaznenog progona.

Iako se PIPA stoga u potpunosti primjenjuje na obradu osobnih podataka u svrhu kaznenog progona, u njoj se nalazi i izuzeće ako se osobni podaci obrađuju u svrhu nacionalne sigurnosti. U skladu s člankom 58. stavkom 1. točkom 2. PIPA-e, članci od 15. do 50. tog zakona ne primjenjuju se na osobne informacije prikupljene ili zatražene radi analize informacija povezanih s nacionalnom sigurnošću ([16]). Međutim, poglavlje I. (Opće odredbe), poglavlje II. (Uspostava politika o zaštiti osobnih informacija i drugo), poglavlje VIII. (Zajednička tužba u vezi s povredom podataka), poglavlje IX. (Dopunske odredbe) i poglavlje X. (Odredbe o sankcijama) PIPA-e i dalje se primjenjuju. To uključuje opća načela zaštite podataka utvrđena u članku 3. (Načela za zaštitu osobnih informacija) i pojedinačna prava zajamčena člankom 4. PIPA-e (Prava ispitanika). To znači da su i u tom području zajamčena glavna načela i prava. Usto, člankom 58. stavkom 4. PIPA-e propisuje se da se takve informacije moraju obrađivati u najmanjoj mjeri koja je potrebna za predviđenu svrhu i tijekom minimalnog razdoblja; od voditelja obrade osobnih informacija zahtijeva se i da uvede potrebne mjere za osiguranje sigurnog upravljanja podacima i prikladne obrade, kao što su tehničke, upravljačke i fizičke zaštitne mjere te mjere za prikladno rješavanje pojedinačnih pritužbi.

U Obavijesti br. 2021-1 o dopunskim pravilima za tumačenje i primjenu Zakona o zaštiti osobnih informacija, Povjerenstvo za zaštitu osobnih informacija (dalje u tekstu „PIPC") dodatno je razjasnilo kako se PIPA primjenjuje na obradu osobnih podataka u svrhu nacionalne sigurnosti u kontekstu tog djelomičnog izuzeća ([17]). To naročito uključuje prava pojedinaca (pristup, ispravak, suspenzija i brisanje) te osnovu i ograničenja za moguće ograničavanje tih prava. U skladu s Obavijesti, primjena temeljnih načela, prava i obveza PIPA-e na obradu osobnih podataka u svrhu nacionalne sigurnosti odražava jamstva predviđena Ustavom za zaštitu prava pojedinca da upravlja vlastitim osobnim informacijama. Svako

([11]) Odluka Ustavnog suda br. 99HeonMa494, 29. studenoga 2001.
([12]) Vidjeti primjerice Odluku Ustavnog suda br. 99HunMa513.
([13]) Članak 29. stavak 1. Ustava.
([14]) Članak 68. stavak 1. Zakona o Ustavnom sudu.
([15]) Članak 5. stavak 1. PIPA-e.
([16]) Članak 58. stavak 1. točka 2. PIPA-e.
([17]) Obavijest PIPC-a br. 2021-1 o dopunskim pravilima za tumačenje i primjenu Zakona o zaštiti osobnih informacija, odjeljak III., dio 6.

ograničenje tog prava, primjerice ako je to potrebno za zaštitu nacionalne sigurnosti, zahtijeva uravnoteženje prava i interesa pojedinca i relevantnog javnog interesa te ne smije utjecati na bit tog prava (članak 37. stavak 2. Ustava).

2. PRISTUP VLADE U SVRHU KAZNENOG PROGONA

2.1. Nadležna javna tijela u području kaznenog progona

Na temelju Zakona o kaznenom postupku (dalje u tekstu „CPA”), Zakona o zaštiti privatnosti komunikacija (dalje u tekstu „CPPA”) i Zakona o telekomunikacijama (dalje u tekstu „TBA”) policija, tužitelji i sudovi mogu prikupljati osobne podatke u svrhu kaznenog progona. U mjeri u kojoj se Zakonom o Nacionalnoj obavještajnoj službi takve ovlasti dodjeljuju i Nacionalnoj obavještajnoj službi (dalje u tekstu „NIS”), ona mora postupati u skladu s navedenim zakonima ([18]). Na kraju, Zakon o prijavljivanju i upotrebi određenih informacija o financijskim transakcijama (dalje u tekstu „ARUSFTI”) financijskim institucijama pruža pravnu osnovu za otkrivanje informacija Korejskoj financijsko-obavještajnoj jedinici (dalje u tekstu „KOFIU”) u svrhu sprečavanja pranja novca i financiranja terorizma. Ta specijalizirana agencija može pružiti takve informacije tijelima kaznenog progona. Međutim, te se obveze otkrivanja primjenjuju samo na voditelje obrade podataka koji obrađuju osobne kreditne informacije u skladu sa Zakonom o kreditnim informacijama i podliježu nadzoru Povjerenstva za financijske usluge. Budući da je obrada osobnih kreditnih informacija od strane takvih voditelja isključena iz područja primjene odluke o primjerenosti, ograničenja i zaštitne mjere koji se primjenjuju na temelju ARUSFTI-ja nisu detaljnije opisani u ovom dokumentu.

2.2. Pravna osnova i ograničenja

CPA (vidjeti odjeljak 2.2.1.), CPPA (vidjeti odjeljak 2.2.2.) i Zakon o telekomunikacijama (vidjeti odjeljak 2.2.3.) pružaju pravnu osnovu za prikupljanje osobnih informacija u svrhu kaznenog progona i njima se utvrđuju primjenjiva ograničenja i zaštitne mjere.

2.2.1. *Pretrage i zapljene*

2.2.1.1. Pravna osnova

Tužitelji i viši službenici pravosudne policije mogu pregledavati predmete, pretraživati osobe ili zapljenjivati predmete samo 1. ako se osoba sumnjiči za kazneno djelo (osumnjičenik za kazneno djelo), 2. ako je to potrebno za istragu i 3. ako se smatra da su predmeti koje je potrebno pregledati, osobe koje je potrebno pretražiti i bilo koji zaplijenjeni predmeti povezani sa slučajem ([19]). Isto tako, sudovi mogu provoditi pretrage i zaplijeniti sve predmete koji se trebaju upotrijebiti kao dokazi ili oduzeti dokle se god takvi predmeti ili osobe smatraju povezanima s određenim slučajem ([20]).

2.2.1.2. Ograničenja i zaštitne mjere

Tužitelji i službenici pravosudne policije općenito moraju poštovati ljudska prava osumnjičenika za kazneno djelo i svake druge uključene osobe ([21]). Usto, prisilne mjere za ostvarenje svrhe istrage mogu se poduzeti samo ako je to izričito navedeno u CPA-u i u najmanjoj potrebnoj mjeri ([22]).

Pretrage, inspekcijski pregledi ili zapljene koje provode policijski službenici ili tužitelji u sklopu kaznene istrage mogu se vršiti samo na temelju sudskog naloga ([23]). Tijelo koje zahtijeva nalog mora podnijeti materijale kojima se dokazuje da postoji osnova za sumnju da je pojedinac počinio kazneno djelo, da je pretraga, inspekcijski pregled ili zapljena potrebna i da predmeti koje je potrebno zaplijeniti postoje ([24]). Kad je riječ o nalogu, on među ostalim elementima mora uključivati imena osumnjičenika i kazneno djelo; mjesto, osobu ili predmete koje je potrebno pretražiti ili zaplijeniti; datum izdavanja i razdoblje valjanosti ([25]). Slično tome, ako se u sklopu sudskih postupaka u tijeku provode pretrage i zapljene koje nisu u okviru javne rasprave, potrebno je prethodno ishoditi sudski nalog ([26]). Predmetni pojedinac i njegovo vijeće za obranu unaprijed se obavještavaju o pretrazi ili zapljeni te mogu biti prisutni pri izvršavanju naloga ([27]).

([18]) Vidjeti članak 3. Zakona o NIS-u (Zakon br. 12948), koji se odnosi na kaznene istrage određenih kaznenih djela, kao što su pobuna, ustanak i kaznena djela povezana s nacionalnom sigurnošću (npr. špijunaža). U takvim bi se slučajevima primjenjivali postupci iz CPA-a povezani s pretragama i zapljenama, a CPPA-om bi se uređivalo prikupljanje podataka o komunikaciji (vidjeti dio 3. o odredbama koje se odnose na pristup komunikacijama u svrhu nacionalne sigurnosti).
([19]) Članak 215. stavci 1. i 2. CPA-a.
([20]) Članak 106. stavak 1. te članci 107. i 109. CPA-a.
([21]) Članak 198. stavak 2. CPA-a.
([22]) Članak 199. stavak 1. CPA-a.
([23]) Članak 215. stavci 1. i 2. CPA-a.
([24]) Članak 108. stavak 1. Uredbe o kaznenom postupku.
([25]) Članak 114. stavak 1. CPA-a u vezi s člankom 219. CPA-a.
([26]) Članak 113. CPA-a.
([27]) Članci 121. i 122. CPA-a.

Pri provedbi pretraga ili zapljena te ako je predmet koji je potrebno pretražiti računalni disk ili drugi medij za pohranu podataka, u načelu se zapljenjuju samo podaci (kopirani ili ispisani) umjesto cijelog medija ([28]). Sam medij za pohranu podataka može se zaplijeniti samo ako se smatra gotovo nemogućim ispisati ili zasebno kopirati potrebne podatke ili ako se smatra da je gotovo neizvedivo na drugi način ostvariti svrhu pretrage ([29]). Predmetni pojedinac mora se bez odgode obavijestiti o zapljeni ([30]). U CPA-u se ne predviđaju iznimke od tog zahtjeva za obavješćivanje.

Pretrage, inspekcijski pregledi i zapljene bez naloga mogu se provoditi samo u ograničenim situacijama. Prvo, to je slučaj ako je nemoguće ishoditi nalog zbog hitnosti na mjestu počinjenja kaznenog djela ([31]). Međutim, zatim se mora bez odgode ishoditi nalog ([32]). Drugo, pretrage i inspekcijski pregledi bez naloga mogu se odvijati na licu mjesta ako je osumnjičenik uhićen ili zadržan ([33]). Na kraju, tužitelj ili viši službenik pravosudne policije može zaplijeniti predmet bez naloga ako je osumnjičenik za kazneno djelo ili treća osoba odbacila predmet ili ako je dobrovoljno predan ([34]).

Dokazi koji se prikupe suprotno odredbama CPA-a neće se smatrati dopustivima ([35]). Štoviše, u Kaznenom zakonu propisano je da su nezakonite pretrage osoba ili njihovih boravišta, čuvanih zgrada, konstrukcija, automobila, brodova, zrakoplova ili soba kažnjive kaznom zatvora u trajanju od najviše tri godine ([36]). Stoga se ta odredba primjenjuje i na predmete, kao što su uređaji za pohranu podataka, koji se zaplijene za vrijeme nezakonite pretrage.

2.2.2. *Prikupljanje informacija o komunikaciji*

2.2.2.1. Pravna osnova

Prikupljanje informacija o komunikaciji uređeno je posebnim zakonom, tj. CPPA-om. CPPA-om se posebice za svakoga propisuje zabrana cenzure bilo kakve pošte, prisluškivanja bilo kakvih telekomunikacija, pružanja podataka o potvrdi komunikacije ili snimanja ili slušanja bilo kojeg razgovora među drugima koji nije javan, osim na temelju CPA-a, CPPA-a ili Zakona o vojnim sudovima ([37]). Pojam „komunikacija" u značenju CPPA-a obuhvaća i običnu poštu i telekomunikacije ([38]). U tom se kontekstu u CPPA-u razlikuju „mjere ograničavanja komunikacije" ([39]) i prikupljanje „podataka o potvrdi komunikacije".

Pojam „mjere ograničavanja komunikacije" obuhvaća „cenzuru", tj. prikupljanje sadržaja tradicionalne pošte, te „prisluškivanje", tj. izravno presretanje (pribavljanje ili snimanje) sadržaja telekomunikacija ([40]). Pojam „podaci o potvrdi komunikacije" obuhvaća „podatke o evidenciji telekomunikacija", što uključuje datum telekomunikacija, njihovo vrijeme početka i završetka, broj odlaznih i dolaznih poziva te pretplatnički broj druge strane, učestalost upotrebe, zapisnike o upotrebi telekomunikacijskih usluga i informacije o lokaciji (npr. od odašiljača na kojima su primjeni signali) ([41]).

([28]) Članak 106. stavak 3. CPA-a.
([29]) Članak 106. stavak 3. CPA-a.
([30]) Članak 219. CPA-a u vezi s člankom 106. stavkom 4. CPA-a.
([31]) Članak 216. stavak 3. CPA-a.
([32]) Članak 216. stavak 3. CPA-a.
([33]) Članak 216. stavci 1. i 2. CPA-a.
([34]) Članak 218. CPA-a. Kad je riječ osobnim informacijama, to obuhvaća samo situaciju u kojoj predmetni pojedinac sam dobrovoljno preda predmet, a ne voditelj obrade osobnih informacija koji posjeduje takve informacije (što bi zahtijevalo posebnu pravnu osnovu na temelju Zakona o zaštiti osobnih informacija). Dobrovoljno predani predmeti mogu se prihvatiti kao dokaz u sudskim postupcima samo ako ne postoji opravdana sumnja u vezi s dobrovoljnom prirodom otkrivanja, što treba dokazati tužitelj. Vidjeti Odluku Vrhovnog suda br. 2013Do11233, 10. ožujka 2016.
([35]) Članak 308-2. CPA-a.
([36]) Članak 321. Kaznenog zakona.
([37]) Članak 3. CPPA-a. Zakonom o vojnim sudovima u pravilu se uređuje prikupljanje informacija o vojnom osoblju i može se primijeniti na civile samo u ograničenom broju slučajeva (npr. ako vojno osoblje i civili zajedno čine kazneno djelo ili ako pojedinac počini kazneno djelo protiv vojske, postupak se može pokrenuti pri vojnom sudu, vidjeti članak 2. Zakona o vojnim sudovima). Opće odredbe kojima se uređuju pretrage i zapljene slične su CPA-u, vidjeti npr. članke od 146. do 149. i članke od 153. do 156. Zakona o vojnim sudovima. Primjerice, obična pošta može se prikupljati samo ako je to potrebno za istragu i na temelju naloga Vojnog suda. Ako se prikupljaju elektroničke komunikacije, primjenjuju se ograničenja i zaštitne mjere iz CPPA-a.
([38]) Članak 2. stavak 1. CPPA-a, tj. „prijenos ili prijam svih vrsta zvukova, riječi, simbola ili slika telegrafom, bežično, kabelima od optičkih vlakana ili drugim elektromagnetskim sustavom, uključujući telefon, e-poštu, člansku informacijsku uslugu, telefaks i radijsko dojavljivanje".
([39]) Članak 2. stavak 7. i članak 3. stavak 2. CPPA-a.
([40]) „Cenzura" se definira kao „otvaranje pošte bez privole predmetne stranke ili pribavljanje informacija o njezinu sadržaju ili snimanje ili uskraćivanje njezina sadržaja na druge načine" (članak 2. točka 6. CPPA-a). „Prisluškivanje" znači „stjecanje ili snimanje sadržaja telekomunikacija slušanjem ili zajedničkim čitanjem zvukova, riječi, simbola ili slika u komunikacijama s pomoću elektroničkih ili mehaničkih uređaja bez privole predmetne stranke ili ometanje njihova prijenosa i primitka" (članak 2. točka 7. CPPA-a).
([41]) Članak 2. točka 11. CPPA-a.

U CPPA-u se utvrđuju ograničenja i zaštitne mjere za prikupljanje obiju vrsta podataka, a nepoštovanje nekih od tih zahtjeva dovodi do kaznenih sankcija ([42]).

2.2.2.2. Ograničenja i zaštitne mjere koji se primjenjuju na prikupljanje sadržaja komunikacija (mjere ograničavanja komunikacije)

Prikupljanje sadržaja komunikacija može se provoditi samo kao dodatno sredstvo za olakšavanje kaznene istrage (tj. krajnja mjera) i potrebno se pobrinuti da se zadiranje u komunikacijske tajne građana svede na najmanju mjeru ([43]). U skladu s tim općim načelom, mjere ograničavanja komunikacije mogu se iskoristiti samo ako je teško na drugi način spriječiti počinjenje kaznenog djela, uhititi počinitelja ili prikupiti dokaze ([44]). Tijela kaznenog progona koja prikupljaju sadržaj komunikacija moraju odmah prestati s prikupljanjem nakon što se daljnji pristup više ne smatra potrebnim, čime se osigurava da je povreda privatnosti komunikacija što ograničenija ([45]).

Nadalje, mjere ograničavanja komunikacije mogu se upotrebljavati samo ako postoji opravdan razlog za sumnju da se određena teška kaznena djela navedena u CPPA-u planiraju, čine ili da su počinjena. To uključuje kaznena djela kao što su pobuna, kaznena djela povezana s drogama ili kaznena djela koja uključuju eksplozive te kaznena djela povezana s nacionalnom sigurnosti, diplomatskim odnosima ili vojnim bazama i objektima ([46]). Cilj mjere ograničavanja komunikacije mora biti određena pošta ili telekomunikacije koje osumnjičenik šalje ili prima ili pošta ili telekomunikacije koje osumnjičenik šalje ili prima u određenom razdoblju ([47]).

Čak i ako su ti zahtjevi ispunjeni, podaci o sadržaju mogu se prikupljati samo na temelju sudskog naloga. Tužitelj naročito može zatražiti od suda dozvolu za prikupljanje podataka o sadržaju u vezi s osumnjičenikom ili osobom pod istragom ([48]). Slično tome, službenik pravosudne policije može podnijeti zahtjev za ovlaštenje tužitelju, koji pak može zatražiti nalog od suda ([49]). Zahtjev za nalog mora biti u pisanom obliku i sadržavati određene elemente. U njemu se naročito moraju utvrditi 1. opravdani razlozi zbog kojih se sumnja da je jedno od navedenih kaznenih djela planirano, da se čini ili da je počinjeno te svi materijali kojima se uspostavlja predmet s jasnim dokazima sumnje, 2. mjere ograničavanja komunikacije uz njihov cilj, opseg, svrhu i razdoblje valjanosti te 3. mjesto na kojem bi se te mjere trebale izvršavati i način izvršavanja ([50]).

Ako su pravni zahtjevi ispunjeni, sud može dati pisano dopuštenje za provedbu mjera ograničavanja komunikacije u vezi s osumnjičenikom ili osobom pod istragom ([51]). U tom se nalogu utvrđuju vrste mjera, njihov cilj, opseg, razdoblje valjanosti te mjesto i način izvršenja ([52]).

Mjere ograničavanja komunikacije mogu se provoditi samo dva mjeseca ([53]). Ako se njihova svrha ostvari u kraćem roku, moraju se odmah obustaviti. Međutim, ako su potrebni uvjeti i dalje ispunjeni, u tom roku od dva mjeseca može se podnijeti zahtjev za produljenje razdoblja valjanosti mjera ograničavanja komunikacije. Takav zahtjev mora uključivati materijale kojima se uspostavlja predmet s jasnim dokazima za produljenje mjera ([54]). Produljeno razdoblje ne smije ukupno trajati više od godine dana ili tri godine za određena naročito teška kaznena djela (npr. kaznena djela povezana s pobunom, stranom agresijom, nacionalnom sigurnošću itd.) ([55]).

Tijela kaznenog progona mogu zahtijevati pomoć komunikacijskih operatera tako da im pruže pisano dopuštenje suda ([56]). Komunikacijski operateri moraju surađivati i čuvati primljeno dopuštenje u svojim evidencijama ([57]). Mogu odbiti surađivati ako informacije o ciljanom pojedincu, kako su navedene u pisanom dopuštenju suda (primjerice telefonski broj pojedinca), nisu točne. Međutim, u svim im je okolnostima zabranjeno otkrivati lozinke za telekomunikacije ([58]).

([42]) Članci 16. i 17. CPPA-a. To se primjenjuje primjerice na prikupljanje, nevođenje evidencije, nastavak prikupljanja ako izvanredna situacija više ne postoji ili neobavješćivanje predmetnog pojedinca.
([43]) Članak 3. točka 2. CPPA-a.
([44]) Članak 5. točka 1. CPPA-a.
([45]) Članak 2. Dekreta o izvršavanju CPPA-a.
([46]) Članak 5. točka 1. CPPA-a.
([47]) Članak 5. točka 2. CPPA-a.
([48]) Članak 6. točka 1. CPPA-a.
([49]) Članak 6. točka 2. CPPA-a.
([50]) Članak 6. stavak 4. CPPA-a i članak 4. stavak 1. Dekreta o izvršavanju CPPA-a.
([51]) Članak 6. stavak 5. i članak 6. stavak 8. CPPA-a.
([52]) Članak 6. točka 6. CPPA-a.
([53]) Članak 6. točka 7. CPPA-a.
([54]) Članak 6. točka 7. CPPA-a.
([55]) Članak 6. točka 8. CPPA-a.
([56]) Članak 9. točka 2. CPPA-a.
([57]) Članak 15-2. CPPA-a i članak 12. Dekreta o izvršavanju CPPA-a.
([58]) Članak 9. točka 4. CPPA-a.

Svatko tko izvršava mjere ograničavanja komunikacije ili od koga se zatraži suradnja mora čuvati evidencije u kojima se navode ciljevi mjera, njihovo izvršenje, datum suradnje i cilj ([59]). Evidencije moraju čuvati i tijela kaznenog progona koja provode mjere ograničavanja komunikacije, a u njima se moraju navesti pojedinosti i ishodi ([60]). Službenici pravosudne policije moraju navesti te informacije u izvješću tužitelju pri zaključenju istrage ([61]).

Ako tužitelj podigne optužnicu u vezi s predmetom u kojem su se upotrebljavale mjere ograničavanja komunikacije ili izda odluku o nepodizanju optužnice ili neuhićenju predmetnog pojedinca (tj. nije riječ samo o prekidu kaznenog progona), tužitelj mora obavijestiti pojedinca koji je predmet mjera ograničavanja komunikacije o činjenici da su takve mjere izvršene, izvršnoj agenciji i razdoblju izvršavanja. Takva se obavijest mora pružiti u pisanom obliku u roku od 30 dana od odluke ([62]). Ta se obavijest može odgoditi ako je vjerojatno da će se njome ozbiljno ugroziti nacionalna sigurnost ili narušiti javna sigurnost i red ili ako je vjerojatno da će prouzročiti znatnu štetu životima i zdravlju drugih ([63]). Ako se obavijest namjerava odgoditi, tužitelj ili službenik pravosudne policije mora dobiti odobrenje od čelnika ureda okružnog javnog tužitelja ([64]). Nakon što osnova za odgodu prestane postojati, obavijest se mora pružiti u roku od 30 dana od tog trenutka ([65]).

U CPPA-u se utvrđuje i poseban postupak prikupljanja sadržaja komunikacija u izvanrednim situacijama. Tijela kaznenog progona naročito mogu prikupljati sadržaj komunikacija ako je neminovno planiranje ili izvršenje organiziranog kriminala ili drugog teškog kaznenog djela koje može izravno dovesti do smrti ili ozbiljnih ozljeda, a postoji izvanredna situacija u kojoj nije moguće provesti uobičajeni postupak (kako je prethodno navedeno) ([66]). U takvoj izvanrednoj situaciji policijski službenik ili tužitelj može uvesti mjere ograničavanja komunikacije bez prethodnog dopuštenja suda, ali mora odmah nakon njihova izvršenja zatražiti dopuštenje suda. Ako tijelo kaznenog progona ne uspije ishoditi dopuštenje suda u roku od 36 sati od izvršenja hitnih mjera, prikupljanje se mora odmah prekinuti, a nakon toga se prikupljene informacije obično uništavaju ([67]). Policijski službenici koji vrše hitan nadzor čine to pod kontrolom tužitelja ili, ako ne mogu unaprijed primiti upute tužitelja zato što je potrebno hitno djelovati, policija mora dobiti odobrenje tužitelja odmah nakon što počne s izvršenjem ([68]). Pravila o obavješćivanju pojedinca kako su prethodno opisana primjenjuju se i na prikupljanje sadržaja komunikacija u izvanrednim situacijama.

Prikupljanje informacija u izvanrednim situacijama mora se uvijek odvijati u skladu s „izjavom o hitnoj cenzuri/prisluškivanju”, a tijelo koje prikuplja informacije mora voditi registar svih izvanrednih mjera ([69]). Zahtjev sudu za davanje dopuštenja za izvanredne mjere mora biti popraćen pisanim dokumentom u kojem se navode potrebne mjere ograničavanja komunikacije, cilj, predmet, opseg, razdoblje, mjesto izvršenja, metoda i objašnjenje na koji su način relevantne mjere ograničavanja komunikacije u skladu s odredbama članka 5. stavka 1. CPPA-a ([70]), zajedno s popratnim dokumentima.

Ako se izvanredne mjere provedu u kratkom roku, čime dopuštenje suda postaje bespredmetno (npr. ako se osumnjičenik uhiti odmah nakon početka presretanja, koje se zbog toga i zaustavlja), čelnik nadležnog ureda javnog tužitelja dostavlja obavijest o izvanrednim mjerama nadležnom sudu ([71]). U obavijesti se moraju navesti svrha, cilj, opseg, razdoblje, mjesto izvršenja i metoda prikupljanja te razlozi za nepodnošenje zahtjeva za dopuštenje suda ([72]). Ta obavijest omogućuje sudu koji je zaprima da preispita zakonitost prikupljanja i mora se unijeti u registar obavijesti o izvanrednim mjerama.

([59]) Članak 9. točka 3. CPPA-a.
([60]) Članak 18. stavak 1. Dekreta o izvršavanju CPPA-a.
([61]) Članak 18. stavak 2. Dekreta o izvršavanju CPPA-a.
([62]) Članak 9-2. stavak 1. CPPA-a.
([63]) Članak 9-2. stavak 4. CPPA-a.
([64]) Članak 9-2. stavak 5. CPPA-a.
([65]) Članak 9-2. stavak 6. CPPA-a.
([66]) Članak 8. točka 1. CPPA-a.
([67]) Članak 8. točka 2. CPPA-a.
([68]) Članak 8. stavak 3. CPPA-a i članak 16. stavak 3. Dekreta o izvršavanju CPPA-a.
([69]) Članak 8. točka 4. CPPA-a.
([70]) To jest da postoji opravdan razlog za sumnju da se određena teška kaznena djela planiraju ili čine ili da su počinjena, a nije izvedivo na drugi način spriječiti počinjenje kaznenog djela, uhititi počinitelja ili prikupiti dokaze.
([71]) Članak 8. točka 5. CPPA-a.
([72]) Članak 8. stavci 6. i 7. CPPA-a.

Sadržaj komunikacija pribavljen mjerama ograničavanja komunikacije na temelju CPPA-a u pravilu se može upotrijebiti samo za istragu, kazneni progon ili sprečavanje određenih prethodno navedenih kaznenih djela, u stegovnim postupcima za ista kaznena djela, u zahtjevu za naknadu štete koji upućuje stranka u tim komunikacijama ili ako je to dopušteno drugim zakonodavstvom ([73]).

Ako se prikupljaju telekomunikacije koje se prenose internetom, primjenjuju se posebne zaštitne mjere ([74]). Takve se informacije mogu upotrebljavati samo za istragu teških kaznenih djela navedenih u članku 5. stavku 1. CPPA-a. Za pohranu informacija potrebno je dobiti odobrenje od suda koji je dopustio mjere ograničavanja komunikacije ([75]). Zahtjev za pohranu mora sadržavati informacije o mjerama ograničavanja komunikacije, sažetak rezultata mjera, razloge za pohranu (zajedno s popratnim materijalima) i telekomunikacije koje se trebaju pohraniti ([76]). Ako se ne podnese takav zahtjev, pribavljene telekomunikacije moraju se izbrisati u roku od 14 dana nakon završetka mjera ograničavanja komunikacije ([77]). Ako se zahtjev odbije, telekomunikacije se moraju uništiti u roku od sedam dana ([78]). Ako se telekomunikacije izbrišu, potrebno je u roku od sedam dana podnijeti izvješće sudu koji je dopustio mjere ograničavanja komunikacije u kojem se navode razlozi za brisanje te pojedinosti i vrijeme kad je to učinjeno.

Općenitije govoreći, ako su informacije nezakonito pribavljene s pomoću mjera ograničavanja komunikacije, neće se priznati kao dokaz u sudskim ili stegovnim postupcima ([79]). Usto, CPPA-om se svakoj osobi koja provodi mjere ograničavanja komunikacije zabranjuje otkrivanje povjerljivih informacija pribavljenih za vrijeme provedbe takvih mjera i upotrebljavanje pribavljenih informacija u svrhu narušavanja ugleda osoba koje su cilj tih mjera ([80]).

2.2.2.3. Ograničenja i zaštitne mjere koji se primjenjuju na prikupljanje informacija o potvrdi komunikacije

Tijela kaznenog progona mogu na temelju CPPA-a zatražiti od telekomunikacijskih operatera da pruže podatke o potvrdi komunikacije ako je to potrebno za istragu ili izvršenje kazne ([81]). Za razliku od prikupljanja podataka o sadržaju, mogućnost prikupljanja podataka o potvrdi komunikacije nije ograničena na određena kaznena djela. Međutim, kao i za podatke o sadržaju, prikupljanje podataka o potvrdi komunikacije zahtijeva prethodno pisano odobrenje suda, podložno istim uvjetima kakvi su prethodno opisani ([82]). Ako zbog hitnosti nije moguće dobiti dopuštenje suda, podaci o potvrdi komunikacije mogu se prikupiti bez naloga, a u tom se slučaju dopuštenje mora ishoditi odmah nakon što se zatraže podaci te se o njemu mora obavijestiti pružatelj telekomunikacijskih usluga ([83]). Ako se ne dobije naknadno dopuštenje, prikupljene informacije moraju se uništiti ([84]).

Tužitelji, službenici pravosudne policije i sudovi moraju voditi evidencije o zahtjevima za podatke o potvrdi komunikacije ([85]). Osim toga, pružatelji telekomunikacijskih usluga moraju dvaput godišnje izvješćivati ministra znanosti i IKT-a o otkrivanju podataka o potvrdi komunikacije i moraju čuvati evidencije o tome sedam godina od datuma otkrivanja podataka ([86]).

Pojedinci se u načelu obavješćuju o tome da su prikupljeni podaci o potvrdi komunikacije ([87]). Vrijeme takve obavijesti ovisi o okolnostima istrage ([88]). Nakon što se donese odluka o tome hoće li se provoditi kazneni progon, obavijest je potrebno dati u roku od 30 dana. Međutim, ako se optužnica suspendira, obavijest se mora pružiti u roku od 30 dana godinu dana nakon donošenja takve odluke. Obavijest se u svakom slučaju mora pružiti u roku od 30 dana godinu dana nakon prikupljanja informacija.

Obavijest se može odgoditi ako je vjerojatno da će se njome 1. ugroziti nacionalna sigurnost, javna sigurnost i red, 2. prouzročiti smrt ili tjelesne ozljede, 3. onemogućiti pravedni sudski postupci (npr. dovesti do uništenja dokaza ili prijetnje svjedocima) ili 4. dovesti do klevete osumnjičenika, žrtve ili drugih osoba koje su povezane s predmetom ili

([73]) Članak 12. CPPA-a.
([74]) Članak 12-2. CPPA-a.
([75]) Tužitelj ili policijski službenik koji izvršava mjere ograničavanja komunikacije mora odabrati koje će se telekomunikacije zadržati u roku od 14 dana nakon završetka mjera i zatražiti odobrenje suda (ako je riječ o policijskom službeniku, zahtjev se mora uputiti tužitelju, koji zatim podnosi zahtjev sudu); vidjeti članak 12-2. stavke 1. i 2. CPPA-a.
([76]) Članak 12-2. stavak 3. CPPA-a.
([77]) Članak 12-2. stavak 5. CPPA-a.
([78]) Članak 12-2. stavak 5. CPPA-a.
([79]) Članak 4. CPPA-a.
([80]) Članak 11. stavak 2. Dekreta o izvršavanju CPPA-a.
([81]) Članak 13. točka 1. CPPA-a.
([82]) Članci 13. i 6. CPPA-a.
([83]) Članak 13. točka 2. CPPA-a. Kao i kad je riječ o hitnim mjerama ograničavanja komunikacije, potrebno je sastaviti dokument u kojem se navode pojedinosti o predmetu (osumnjičenik, mjere koje se trebaju poduzeti, kazneno djelo na koje se sumnja i hitnost). Vidjeti članak 37. stavak 5. Dekreta o izvršavanju CPPA-a.
([84]) Članak 13. točka 3. CPPA-a.
([85]) Članak 13. stavci 5. i 6. CPPA-a.
([86]) Članak 13. točka 7. CPPA-a.
([87]) Vidjeti članak 13-3. stavak 7. u vezi s člankom 9-2. CPPA-a.
([88]) Članak 13-3. stavak 1. CPPA-a.

ako će se zadirati u njihovu privatnost ([89]). Obavješćivanje na jednoj od navedenih osnova zahtijeva odobrenje direktora nadležnog ureda okružnog javnog tužitelja ([90]). Nakon što osnova za odgodu prestane postojati, obavijest se mora pružiti u roku od 30 dana od tog trenutka ([91]).

Obaviješteni pojedinci mogu podnijeti pisani zahtjev tužitelju ili službeniku pravosudne policije u vezi s razlozima za prikupljanje podataka o potvrdi komunikacije ([92]). U tom slučaju tužitelj ili službenik pravosudne policije moraju pisanim putem pružiti te razloge u roku od 30 dana nakon zaprimanja zahtjeva, osim ako se primjenjuje jedna od navedenih osnova (izuzeća za odgodu obavijesti) ([93]).

2.2.3. *Dobrovoljno otkrivanje telekomunikacijskih operatera*

Člankom 83. stavkom 3. TBA-a telekomunikacijskim se operaterima omogućuje da dobrovoljno postupaju u skladu sa zahtjevom (koji se podnosi radi potpore u kaznenom postupku, istrazi ili izvršenju kazne) suda, tužitelja ili čelnika istražne agencije za otkrivanje „podataka o komunikacijama”. U kontekstu TBA-a „podaci o komunikacijama” obuhvaćaju ime, registracijski broj rezidenta, adresu i telefonski broj korisnika, datume kad su se korisnici pretplatili ili kad su okončali pretplatu te korisničke identifikacijske kodove (tj. kodove koji služe za identifikaciju stvarnog korisnika računalnih sustava ili komunikacijskih mreža) ([94]). Za potrebe TBA-a korisnicima se smatraju samo pojedinci koji izravno ugovaraju usluge kod korejskog pružatelja telekomunikacijskih usluga ([95]). Stoga će situacije u kojima će se pojedinci iz EU-a čiji su podaci preneseni u Republiku Koreju smatrati korisnicima u okviru TBA-a biti veoma ograničene s obzirom na to da takvi pojedinci obično ne sklapaju izravan ugovor s korejskim telekomunikacijskim operaterom.

Zahtjevi za pružanje podataka o komunikacijama na temelju TBA-a moraju se podnijeti u pisanom obliku i u njima se moraju navesti razlozi za zahtjev, poveznica na relevantnog korisnika i opseg traženih podataka ([96]). Ako zbog hitnosti nije moguće pružiti pisani zahtjev, pisani zahtjev mora se pružiti čim nestane razlog za hitnost ([97]). Telekomunikacijski operateri koji postupaju u skladu sa zahtjevima za otkrivanje podataka o komunikacijama moraju čuvati knjige s evidencijama u kojima se naznačuje da su pruženi podaci o komunikacijama, kao i povezane materijale, kao što je pisani zahtjev ([98]). Nadalje, telekomunikacijski operateri moraju dvaput godišnje izvješćivati ministra znanosti i IKT-a o pružanju podataka o komunikacijama ([99]).

Telekomunikacijski operateri nisu obvezni postupati prema zahtjevima za otkrivanje podataka o komunikacijama na temelju TBA-a. Stoga operater treba procijeniti svaki zahtjev u skladu s primjenjivim zahtjevima za zaštitu podataka na temelju PIPA-e. Telekomunikacijski operater mora posebice uzeti u obzir interese ispitanika i ne smije otkrivati informacije ako bi se time vjerojatno nepošteno povrijedili interesi pojedinca ili treće strane ([100]). Usto, u skladu s Obavijesti br. 2021-1 o dopunskim pravilima za tumačenje i primjenu Zakona o zaštiti osobnih informacija, predmetni pojedinac mora se obavijestiti o otkrivanju. U iznimnim situacijama takva se obavijest može odgoditi, posebice ako i onoliko dugo koliko bi se njome ugrozila kaznena istraga u tijeku ili ako je vjerojatno da bi se ugrozio život ili zdravlje druge osobe čija prava ili interesi nedvojbeno imaju prednost pred pravima ispitanika ([101]).

Vrhovni sud potvrdio je 2016. da se dobrovoljnim pružanjem podataka o komunikacijama koje vrše telekomunikacijski operateri bez naloga na temelju TBA-a ne krše prava korisnika telekomunikacijske usluge na samoodređenje u pogledu informacija. Sud je ujedno razjasnio da bi se to smatralo kršenjem ako bi bilo nedvojbeno očito da je agencija koja upućuje zahtjev zlouporabila svoju ovlast da zatraži otkrivanje podataka o komunikacijama, čime bi povrijedila interese predmetnog pojedinca ili treće strane ([102]). Općenitije govoreći, svaki zahtjev za dobrovoljno otkrivanje koji uputi tijelo kaznenog progona mora biti u skladu s načelima zakonitosti, nužnosti i proporcionalnosti prema Ustavu Koreje (članak 12. stavak 1. i članak 37. stavak 2.).

([89]) Članak 13-3. stavak 2. CPPA-a.
([90]) Članak 13-3. stavak 3. CPPA-a.
([91]) Članak 13-3. stavak 4. CPPA-a.
([92]) Članak 13-3. stavak 5. CPPA-a.
([93]) Članak 13-3. stavak 6. CPPA-a.
([94]) Članak 83. stavak 3. TBA-a.
([95]) Članak 2. stavak 9. TBA-a.
([96]) Članak 83. stavak 4. TBA-a.
([97]) Članak 83. stavak 4. TBA-a.
([98]) Članak 83. stavak 5. TBA-a.
([99]) Članak 83. stavak 6. TBA-a.
([100]) Članak 18. stavak 2. PIPA-e.
([101]) Obavijest PIPC-a br. 2021-1 o dopunskim pravilima za tumačenje i primjenu Zakona o zaštiti osobnih informacija, odjeljak III., dio 2., točka iii.
([102]) Odluka Vrhovnog suda br. 2012Da105482 od 10. ožujka 2016.

2.3. **Nadzor**

Postoje različiti mehanizmi za nadzor tijelâ kaznenog progona, a može se provoditi interno ili ga mogu provoditi vanjska tijela.

2.3.1. *Samorevizija*

U skladu sa Zakonom o revizijama u javnom sektoru, javna tijela potiču se na to da uspostave unutarnje tijelo za samoreviziju, koje bi, među ostalim, bilo odgovorno za provjeru zakonitosti ([103]). Voditeljima takvih revizijskih tijela mora se u najvećoj mogućoj mjeri zajamčiti neovisnost ([104]). Točnije, oni se imenuju izvan relevantnog tijela (npr. bivši suci, profesori) na razdoblje od dvije do pet godina i mogu se razriješiti dužnosti samo zbog opravdanih razloga (npr. ako ne mogu izvršavati dužnosti zbog mentalnih ili fizičkih problema ili ako podliježu stegovnim mjerama) ([105]). Usto, revizori se imenuju na temelju posebnih uvjeta utvrđenih u Zakonu ([106]). Revizorska izvješća mogu uključivati preporuke ili zahtjeve za naknadu ili ispravak te opomene i preporuke ili zahtjeve za stegovne mjere ([107]). Oni se u roku od 60 dana od završetka revizije priopćavaju čelniku javnog tijela u kojem se provodi revizija te Revizijskom i inspekcijskom odboru (vidjeti odjeljak 2.3.2.) ([108]). Predmetno tijelo mora provesti potrebne mjere te izvijestiti Revizijski i inspekcijski odbor o rezultatima ([109]). Osim toga, rezultati revizije obično su javno dostupni ([110]). Odbijanje ili ometanje samorevizije podložno je upravnim novčanim kaznama ([111]). U području kaznenog progona, radi usklađenosti s navedenim zakonodavstvom Nacionalna policijska agencija upotrebljava sustav glavnog inspektora za provedbu unutarnjih revizija, među ostalim u vezi s mogućim povredama ljudskih prava ([112]).

2.3.2. *Revizijski i inspekcijski odbor*

Revizijski i inspekcijski odbor (dalje u tekstu „BAI”) može provoditi inspekcijski pregled aktivnosti javnih tijela i, na osnovu takvih pregleda, izdati preporuke, zahtijevati stegovne mjere ili podnijeti kaznenu pritužbu ([113]). BAI je uspostavio predsjednik Republike Koreje, ali zadržava neovisan status u odnosu na svoje zadaće ([114]). Usto, Zakonom kojim se uspostavlja BAI zahtijeva se da taj odbor bude u najvećoj mjeri neovisan u pogledu imenovanja, razrješenja i organizacije svojeg osoblja i sastavljanja svojeg proračuna ([115]). Predsjednika BAI-ja imenuje predsjednik države uz pristanak Nacionalne skupštine ([116]). Preostalih šest povjerenika imenuje predsjednik države na preporuku predsjednika BAI-ja na mandat od četiri godine ([117]). Povjerenici (uključujući predsjednika) moraju zadovoljavati određene zakonom propisane kvalifikacije ([118]) i mogu se razriješiti dužnosti samo u slučaju smjene, osude na kaznu zatvora ili nemogućnosti izvršavanja zadaća zbog dugotrajnih mentalnih ili fizičkih poteškoća ([119]). Nadalje, povjerenicima je zabranjeno sudjelovati u političkim aktivnostima i istodobno obnašati dužnosti u Nacionalnoj skupštini, upravnim agencijama, organizacijama u kojima BAI provodi reviziju ili inspekcijski pregled ili biti na bilo kojoj drugoj plaćenoj dužnosti ili položaju ([120]).

BAI svake godine provodi opću reviziju, ali može provoditi i posebne revizije o pitanjima od posebnog interesa. BAI može za vrijeme inspekcijskog pregleda zatražiti podnošenje dokumenata i prisutnost određenih osoba ([121]). Taj odbor u sklopu revizije pregledava prihode i rashode države, ali nadzire i općenitu usklađenost sa zadaćama javnih tijela i javnih

([103]) Članci 3. i 5. Zakona o revizijama u javnom sektoru.
([104]) Članak 7. Zakona o revizijama u javnom sektoru.
([105]) Članci od 8. do 11. Zakona o revizijama u javnom sektoru.
([106]) Članak 16. i dalje Zakona o revizijama u javnom sektoru.
([107]) Članak 23. stavak 2. Zakona o revizijama u javnom sektoru.
([108]) Članak 23. stavak 1. Zakona o revizijama u javnom sektoru.
([109]) Članak 23. stavak 3. Zakona o revizijama u javnom sektoru.
([110]) Članak 26. Zakona o revizijama u javnom sektoru.
([111]) Članak 41. Zakona o revizijama u javnom sektoru.
([112]) Vidjeti osobito odjele u nadležnosti glavnog direktora za reviziju i inspekcijski pregled: https://www.police.go.kr/eng/knpa/org/org01.jsp
([113]) Članak 24. i članci od 31. do 35. Zakona o Revizijskom i inspekcijskom odboru (dalje u tekstu „Zakon o BAI-ju”).
([114]) Članak 2. stavak 1. Zakona o BAI-ju.
([115]) Članak 2. stavak 2. Zakona o BAI-ju.
([116]) Članak 4. stavak 1. Zakona o BAI-ju.
([117]) Članak 5. stavak 1. i članak 6. Zakona o BAI-ju.
([118]) Na primjer, najmanje deset godina obnašanja dužnosti suca, javnog tužitelja ili odvjetnika, najmanje osam godina rada kao javni službenik ili profesor ili na višem položaju u sveučilištu ili najmanje deset godina rada u poduzeću uvrštenom na burzu ili instituciji u koju ulaže država (a od toga najmanje pet godina treba biti na položaju izvršnog direktora); vidjeti članak 7. BAI-ja.
([119]) Članak 8. Zakona o BAI-ju.
([120]) Članak 9. Zakona o BAI-ju.
([121]) Vidjeti npr. članak 27. Zakona o BAI-ju.

službenika kako bi se poboljšalo funkcioniranje javne uprave ([122]). Stoga njegov nadzor nije ograničen na proračunske aspekte, već uključuje i provjeru zakonitosti.

2.3.3. *Nacionalna skupština*

Nacionalna skupština može provoditi istragu i inspekcijske preglede javnih tijela ([123]). Za vrijeme istrage ili inspekcijskog pregleda Nacionalna skupština može zahtijevati otkrivanje dokumenata i zatražiti od pojedinaca da svjedoče ([124]). Svako lažno svjedočenje za vrijeme istrage Nacionalne skupštine podliježe kaznenim sankcijama (kazna zatvora do deset godina) ([125]). Proces i rezultati inspekcijskih pregleda mogu se objaviti ([126]). Ako Nacionalna skupština utvrdi nezakonite ili neprikladne aktivnosti, može od predmetnog javnog tijela zatražiti da poduzme korektivne mjere, uključujući isplatu naknade, poduzimanje stegovnih mjera i poboljšanje internih postupaka ([127]). To tijelo nakon takvog zahtjeva mora djelovati bez odgode i izvijestiti Nacionalnu skupštinu o ishodu ([128]).

2.3.4. *Povjerenstvo za zaštitu osobnih informacija*

Povjerenstvo za zaštitu osobnih informacija (dalje u tekstu „PIPC") nadzire obradu osobnih informacija koju vrše tijela kaznenog progona u skladu s PIPA-om. Usto, u skladu s člankom 7-8. stavcima 3. i 4. te člankom 7-9. stavkom 5. PIPA-e nadzor PIPC-a obuhvaća i moguće kršenje pravila o ograničenjima i zaštitnim mjerama u pogledu prikupljanja osobnih informacija, uključujući onih iz posebnih zakona kojima se uređuje prikupljanje (elektroničkih) dokaza u svrhe kaznenog progona (vidjeti odjeljak 2.2.). S obzirom na zahtjeve iz članka 3. stavka 1. PIPA-e za zakonito i pošteno prikupljanje osobnih informacija, svaka takva povreda ujedno je i kršenje PIPA-e, čime se PIPC-u dopušta da provodi istragu i poduzme korektivne mjere ([129]).

PIPC pri izvršavanju svoje nadzorne funkcije ima pristup svim relevantnim informacijama ([130]). Može savjetovati tijela kaznenog progona kako bi se poboljšala njihova razina zaštite osobnih informacija u okviru njihovih aktivnosti obrade, izreći korektivne mjere (npr. suspendirati obradu podataka ili poduzeti potrebne mjere za zaštitu osobnih informacija) ili savjetovati tijelo da poduzme stegovne mjere ([131]). Na kraju, predviđene su kaznene sankcije za određene vrste kršenja PIPA-e, kao što je nezakonita upotreba ili otkrivanje osobnih informacija trećim stranama ili nezakonita obrada osjetljivih informacija ([132]). PIPC u tom kontekstu može uputiti predmet nadležnoj istražnoj agenciji (uključujući tužitelja) ([133]).

2.3.5. *Nacionalno povjerenstvo za ljudska prava*

Nacionalno povjerenstvo za ljudska prava (dalje u tekstu „NHRC") je neovisno tijelo zaduženo za zaštitu i promicanje temeljnih prava ([134]) te ima ovlast istraživati i ispravljati kršenja članaka od 10. do 22. Ustava, koji uključuju pravo na privatnost i privatnost korespondencije. NHRC se sastoji od 11 povjerenika, koje imenuju Nacionalna skupština (četiri), predsjednik (četiri) i predsjednik Vrhovnog suda (tri) ([135]). Kako bi bio imenovan, povjerenik mora 1. najmanje deset godina raditi na sveučilištu ili u ovlaštenom istraživačkom institutu barem kao izvanredni profesor, 2. najmanje deset godina obnašati dužnost suca, tužitelja ili odvjetnika, 3. najmanje deset godina sudjelovati u aktivnostima povezanima s ljudskim pravima (npr. u okviru neprofitne, nevladine organizacije ili međunarodne organizacije) ili 4. moraju ga preporučiti udruge civilnog društva ([136]). Predsjednika NHRC-a imenuje predsjednik države među povjerenicima i

([122]) Članci 20. i 24. Zakona o BAI-ju.
([123]) Članak 128. Zakona o Nacionalnoj skupštini te članci 2., 3. i 15. Zakona o inspekcijskom pregledu i istrazi državne uprave. To uključuje godišnje inspekcijske preglede vladinih poslova u cjelini i istrage posebnih pitanja.
([124]) Članak 10. stavak 1. Zakona o inspekcijskom pregledu i istrazi državne uprave. Vidjeti i članke 128. i 129. Zakona o Nacionalnoj skupštini.
([125]) Članak 14. Zakona o svjedočenju, procjeni i drugome pred Nacionalnom skupštinom.
([126]) Članak 12-2. Zakona o inspekcijskom pregledu i istrazi državne uprave.
([127]) Članak 16. stavak 2. Zakona o inspekcijskom pregledu i istrazi državne uprave.
([128]) Članak 16. stavak 3. Zakona o inspekcijskom pregledu i istrazi državne uprave.
([129]) Vidjeti Obavijest PIPC-a br. 2021-1 o dopunskim pravilima za tumačenje i primjenu Zakona o zaštiti osobnih informacija.
([130]) Članak 63. PIPA-e.
([131]) Članak 61. stavak 2., članak 65. stavak 1., članak 65. stavak 2. i članak 64. stavak 4. PIPA-e.
([132]) Članci od 70. do 74. PIPA-e.
([133]) Članak 65. stavak 1. PIPA-e.
([134]) Članak 1. Zakona o Povjerenstvu za ljudska prava (dalje u tekstu „Zakon o NHRC-u").
([135]) Članak 5. stavci 1. i 2. Zakona o NHRC-u.
([136]) Članak 5. stavak 3. Zakona o NHRC-u.

mora ga potvrditi Nacionalna skupština ([137]). Povjerenici (uključujući predsjednika) imenuju se na mandat od tri godine s mogućnošću produljenja i mogu se razriješiti dužnosti samo ako su osuđeni na kaznu zatvora ili ako više nisu u stanju izvršavati svoje zadaće zbog dugotrajnih fizičkih ili mentalnih poteškoća (a u tom se slučaju dvije trećine povjerenika moraju složiti s razrješenjem) ([138]). Povjerenicima NHRC-a zabranjeno je istodobno obnašati dužnost u Nacionalnoj skupštini, lokalnim vijećima ili u bilo kojem državnom tijelu ili tijelu lokalne vlasti (kao javni službenik) ([139]).

NHRC može pokrenuti istragu na vlastitu inicijativu ili na temelju zahtjeva pojedinca. U sklopu svoje istrage može zahtijevati podnošenje relevantnih materijala, provoditi inspekcijske preglede i pozivati pojedince da svjedoče ([140]). Nakon istrage može izdati preporuke za poboljšanje ili ispravljanje određenih politika i praksi te ih objaviti ([141]). Javna tijela moraju obavijestiti NHRC o planu provedbe takvih preporuka u roku od 90 dana nakon što ih zaprime ([142]). Međutim, ako se preporuke ne provedu, predmetno tijelo o tome mora obavijestiti Odbor ([143]). NHRC pak o tome može izvijestiti Nacionalnu skupštinu i/ili to objaviti. Javna tijela općenito poštuju preporuke NHRC-a i imaju velik poticaj za to s obzirom na to da se njihova provedba procjenjivala u sklopu opće ocjene koju je provodio Ured za koordinaciju vladinih politika pod nadležnošću ureda premijera.

2.4. **Pravna zaštita pojedinaca**

2.4.1. *Mehanizmi pravne zaštite dostupni na temelju PIPA-e*

Pojedinci mogu ostvariti svoja prava na pristup, ispravak, brisanje i suspenziju na temelju PIPA-e u odnosu na osobne informacije koje obrađuju tijela kaznenog progona. Pristup se može zatražiti izravno od relevantnog tijela ili neizravno preko PIPC-a ([144]). Nadležno tijelo može ograničiti ili odbiti pristup samo ako je to predviđeno zakonom, ako bi se time vjerojatno ugrozio život ili zdravlje treće strane ili ako bi to vjerojatno dovelo do neopravdane povrede imovine i ostalih interesa druge osobe (tj. ako bi interesi druge osobe prevagnuli nad interesima pojedinca koji upućuje zahtjev) ([145]). Ako se odbije zahtjev za pristup, potrebno je obavijestiti pojedinca o razlozima za to i o načinu podnošenja žalbe ([146]). Slično tome, zahtjev za ispravljanje ili brisanje može se odbiti ako je to predviđeno drugim zakonima, a u tom se slučaju pojedinac mora obavijestiti o razlozima za to i mogućnosti podnošenja žalbe ([147]).

Kad je riječ o pravnoj zaštiti, pojedinci mogu podnijeti pritužbu PIPC-u, među ostalim preko Pozivnog centra za zaštitu privatnosti, kojim upravlja Korejska agencija za internet i sigurnost ([148]). Osim toga, pojedincu se može osigurati posredovanje Odbora za posredovanje u sporovima o osobnim informacijama ([149]). Te su mogućnosti za pravnu zaštitu dostupne u slučaju mogućih povreda pravila iz određenih zakona u kojima se utvrđuju ograničenja i zaštitne mjere za prikupljanje osobnih informacija (odjeljak 2.2.) i PIPA-e. Usto, pojedinci mogu osporiti odluke ili nedjelovanje PIPC-a na temelju Zakona o upravnim sporovima (vidjeti odjeljak 2.4.3.).

([137]) Članak 5. stavak 5. Zakona o NHRC-u.
([138]) Članak 7. stavak 1. i članak 8. Zakona o NHRC-u.
([139]) Članak 10. Zakona o NHRC-u.
([140]) Članak 36. Zakona o NHRC-u. U skladu s člankom 36. stavkom 7. Zakona podnošenje materijala ili predmeta može se odbiti ako bi se time dovela u pitanje državna povjerljivost koja bi mogla imati znatan učinak na državnu sigurnost ili diplomatske odnose ili bi ono činilo ozbiljnu prepreku u kaznenoj istrazi ili sudskom postupku u tijeku. U takvim slučajevima Odbor može prema potrebi zahtijevati dodatne informacije od čelnika relevantne agencije (koji mora postupati u skladu s tim u dobroj vjeri) kako bi se preispitalo je li odbijanje pružanja informacija opravdano.
([141]) Članak 25. stavak 1. Zakona o NHRC-u.
([142]) Članak 25. stavak 3. Zakona o NHRC-u.
([143]) Članak 25. stavak 4. Zakona o NHRC-u.
([144]) Članak 35. stavak 2. PIPA-e.
([145]) Članak 35. stavak 4. PIPA-e.
([146]) Članak 42. stavak 2. Dekreta o izvršavanju PIPA-e.
([147]) Članak 36. stavci 1. i 2. PIPA-e i članak 43. stavak 3. Dekreta o izvršavanju PIPA-e.
([148]) Članak 62. PIPA-e.
([149]) Članci od 40. do 50. PIPA-e i članci od 48-2. do 57. Dekreta o izvršavanju PIPA-e.

2.4.2. *Pravna zaštita pri Nacionalnom povjerenstvu za ljudska prava*

NHRC rješava pritužbe pojedinaca (i korejskih i stranih državljana) povezane s povredama ljudskih prava koje su počinila javna tijela ([150]). Pojedinci ne podliježu nijednom zahtjevu da bi podnijeli pritužbu NHRC-u ([151]). Stoga će NHRC obraditi pritužbu čak i ako predmetni pojedinac ne može činjenično dokazati povredu u fazi ispitivanja dopuštenosti. U kontekstu prikupljanja osobnih podataka u svrhu kaznenog progona, od pojedinca se stoga ne bi zahtijevalo da dokaže da su korejska javna tijela zbilja pristupila njegovim osobnim informacijama kako bi pritužba bila prihvatljiva pri NHRC-u. Pojedinac može i zatražiti rješavanje pritužbe posredovanjem ([152]).

Kako bi istražio pritužbu, NHRC može iskoristiti svoje istražne ovlasti, među ostalim tako da zahtijeva podnošenje relevantnih materijala, provodi inspekcijske preglede i poziva pojedince da svjedoče ([153]). Ako se u istrazi otkrije da je došlo do kršenja relevantnih zakona, NHRC može preporučiti provedbu pravnih lijekova ili ispravak ili poboljšanje bilo kojeg relevantnog propisa, institucije, politike ili prakse ([154]). Predloženi pravni lijekovi mogu uključivati posredovanje, prestanak povrede ljudskih prava, nadoknadu štete i mjere za sprečavanje budućih istih ili sličnih povreda ([155]). Mjere za popravljanje štete u slučaju nezakonitog prikupljanja osobnih informacija prema primjenjivim pravilima mogu uključivati brisanje prikupljenih osobnih informacija. Ako se smatra vrlo vjerojatnim da je povreda i dalje u tijeku te ako se smatra vjerojatnim da će se, ako se ne poduzmu mjere, uzrokovati šteta koju je teško popraviti, NHRC može donijeti hitne mjere pomoći ([156]).

Ako NHRC nema ovlasti nametanja obveze, njegove odluke (npr. odluka da se istraga pritužbe ne nastavi) ([157]) i preporuke mogu se osporiti pri korejskim sudovima na temelju Zakona o upravnim sporovima (vidjeti odjeljak 2.4.3.) ([158]). Usto, ako nalazi NHRC-a pokažu da je javno tijelo nezakonito prikupljalo osobne podatke, pojedinac bi mogao tražiti dodatnu pravnu zaštitu pri korejskim sudovima protiv tog javnog tijela, npr. osporavanjem prikupljanja na temelju Zakona o upravnim sporovima, podnošenjem ustavne žalbe na temelju Zakona o Ustavnom sudu ili traženjem naknade štete na temelju Zakona o naknadi od države (vidjeti odjeljak 2.4.3.).

2.4.3. *Sudska zaštita*

Pojedinci se mogu pozvati na ograničenja i zaštitne mjere iz prethodnih odjeljaka kako bi na više načina primili pravnu zaštitu pri korejskim sudovima.

Prvo, u skladu s CPA-om predmetni pojedinac i njegov pravni savjetnik mogu biti prisutni kad se nalog za pretragu ili zapljenu izvršava te stoga mogu uložiti prigovor u vrijeme izvršenja tog naloga ([159]). Usto, CPA-om se predviđa mehanizam tzv. „kvazi-pritužbe”, koji pojedincima omogućuje da od nadležnog suda zatraže da poništi ili izmijeni odluku koju je donio tužitelj ili policijski službenik u vezi sa zapljenom ([160]). Time se pojedincima omogućuje da ospore mjere poduzete za izvršenje naloga za zapljenu.

([150]) Iako se u članku 4. Zakona o NHRC-u upućuje na građane i strane državljane koji borave u Republici Koreji, pojam „boravka” odnosi se na nadležnost umjesto na državno područje. Stoga, ako nacionalne institucije unutar Koreje povrijede temeljna prava stranog državljanina izvan Koreje, taj pojedinac može podnijeti pritužbu NHRC-u. Vidjeti primjerice pitanje o tome na stranici NHRC-a s najčešćim pitanjima, dostupnoj na https://www.humanrights.go.kr/site/program/board/basicboard/list?boardtypeid=7025&menuid=002004005001&pagesize=10&currentpage=2. To bi bio slučaj ako bi korejska javna tijela nezakonito pristupila osobnim podacima stranog državljanina koji su preneseni u Koreju.

([151]) Pritužba se u načelu mora podnijeti unutar godine dana od povrede, ali NHRC može i dalje odlučiti istražiti pritužbu koja je podnesena nakon isteka tog roka ako nije nastupila zastara na temelju kaznenog ili građanskog prava (članak 32. stavak 1. točka 4. Zakona o NHRC-u).

([152]) Članak 42. i dalje Zakona o NHRC-u.

([153]) Članci 36. i 37. Zakona o NHRC-u.

([154]) Članak 44. Zakona o NHRC-u.

([155]) Članak 42. stavak 4. Zakona o NHRC-u.

([156]) Članak 48. Zakona o NHRC-u.

([157]) Na primjer, ako NHRC iznimno ne može pregledati određene materijale ili objekte jer su povezani s državnim tajnama koje bi mogle imati znatne posljedice na državnu sigurnost ili diplomatske odnose ili ako bi inspekcijski pregled činio ozbiljnu prepreku u kaznenoj istrazi ili sudskom postupku u tijeku (vidjeti bilješku 166.) i ako to sprečava NHRC da provodi istragu potrebnu za procjenu utemeljenosti zaprimljenog zahtjeva, obavijestit će pojedinca o razlozima zbog kojih je pritužba odbijena u skladu s člankom 39. Zakona o NHRC-u. U tom bi slučaju pojedinac mogao osporiti odluku NHRC-a na temelju Zakona o upravnim sporovima.

([158]) Vidjeti npr. Odluku Visokog suda u Seoulu 2007Nu27259 od 18. travnja 2008., koja je potvrđena u Odluci Vrhovnog suda 2008Du7854 od 9. listopada 2008.; Odluku Visokog suda u Seoulu 2017Nu69382 od 2. veljače 2018.

([159]) Članci 121. i 219. CPA-a.

([160]) Članak 417. CPA-a u vezi s člankom 414. stavkom 2. CPA-a. Vidjeti i Odluku Vrhovnog suda br. 97Mo66 od 29. rujna 1997.

Nadalje, pojedinci mogu pred korejskim sudovima ishoditi naknadu za štetu. Na temelju Zakona o naknadi od države pojedinci mogu podnijeti zahtjev za naknadu štete koju su nanijeli javni službenici pri izvršenju službenih dužnosti u suprotnosti sa zakonom ([161]). Zahtjev na temelju Zakona o naknadi štete od države može se podnijeti specijaliziranom „Vijeću za naknadu" ili izravno korejskim sudovima ([162]). Ako je žrtva strani državljanin, Zakon o naknadi od države primjenjuje se pod uvjetom da zemlja podrijetla tog državljanina jednako tako osigurava naknadu od države za korejske državljane ([163]). Prema sudskoj praksi taj je uvjet ispunjen ako zahtjevi za traženje naknade u drugoj državi „nisu znatno neuravnoteženi između Koreje i druge države" i ako „nisu općenito stroži od onih koje je odredila Koreja te ako među njima nema materijalnih i sadržajnih razlika" ([164]). Građanskim zakonom uređuje se odgovornost države za naknadu, a ta odgovornost stoga obuhvaća i štetu koja nije povezana s imovinom (npr. mentalna patnja) ([165]).

Kad je riječ o kršenjima pravila o zaštiti podataka, PIPA-om se predviđa dodatan pravni lijek. U skladu s člankom 39. PIPA-e svaki pojedinac koji pretrpi štetu zbog kršenja PIPA-e ili gubitka, krađe, otkrivanja, krivotvorenja, izmjene ili oštećenja svojih osobnih informacija može pri sudovima ishoditi naknadu štete. Ne postoji sličan zahtjev za recipročnost kao na temelju Zakona o naknadi od države.

Uz naknadu štete moguće je na temelju Zakona o upravnim sporovima dobiti i upravnu pravnu zaštitu protiv djelovanja ili propusta upravnih agencija. Svaki pojedinac može osporiti odluku (tj. izvršavanje ili odbijanje izvršavanja javne ovlasti u određenom slučaju) ili propust (ako upravna agencija dulje vrijeme ne donese određenu odluku iako je pravno obvezna učiniti to), što može dovesti do poništenja/izmjene nezakonite odluke, proglašenja ništavosti (tj. proglašenje da odluka nema pravni učinak ili da je pravno nepostojeća) ili proglašenja propusta nezakonitim ([166]). Kako bi se upravna odluka mogla osporiti, mora izravno utjecati na građanska prava i dužnosti ([167]). To uključuje mjere za prikupljanje osobnih podataka, neovisno o tome čini li se to izravno (npr. presretanjem komunikacija) ili zahtjevom za otkrivanje (npr. pružatelju usluge).

Navedeni zahtjevi mogu se najprije iznijeti pred povjerenstvima za upravne žalbe uspostavljenima u okviru određenih javnih tijela (npr. NIS ili NHRC) ili pred Središnjim povjerenstvom za upravne žalbe uspostavljenim u okviru Povjerenstva za borbu protiv korupcije i civilna prava ([168]). Takvom se upravnom žalbom pruža alternativna i neformalnija mogućnost za osporavanje odluke ili propusta javnog tijela. Međutim, zahtjevi se mogu iznijeti i izravno pri korejskim sudovima na temelju Zakona o upravnim sporovima.

Zahtjev za poništenje/izmjenu odluke na temelju Zakona o upravnim sporovima može podnijeti bilo koja osoba koja ima pravni interes tražiti poništenje/izmjenu ili da se poništenjem/izmjenom obnove njezina prava ako odluka više nema učinak ([169]). Slično tome, spor za potvrdu ništavosti može pokrenuti osoba u čijem je pravnom interesu takva potvrda, a spor za potvrdu nezakonitosti propusta može pokrenuti svaka osoba koja je podnijela zahtjev za odluku i u čijem je pravnom interesu tražiti potvrdu nezakonitosti takvog propusta ([170]). U sudskoj praksi Vrhovnog suda „pravni interes" tumači se kao „pravno zaštićeni interes", tj. izravan i konkretan interes zaštićen zakonodavstvom i propisima na kojima se temelje upravne odluke (tj. ne opći, neizravan i apstraktan interes javnosti) ([171]). Pojedinci stoga imaju pravni interes u slučaju svakog kršenja ograničenja i zaštitnih mjera u vezi s prikupljanjem njihovih osobnih podataka u svrhu kaznenog progona (na temelju određenih zakona ili PIPA-e). Pravomoćna presuda na temelju Zakona o upravnim sporovima obvezujuća je za stranke ([172]).

Zahtjev za poništenje/izmjenu odluke i zahtjev za potvrdu nezakonitosti propusta moraju se podnijeti u roku od 90 dana od datuma na koji pojedinac dozna za odluku/propust, a u načelu ne više od godine dana od datuma izdavanja

([161]) Članak 2. stavak 1. Zakona o naknadi od države.

([162]) Članci 9. i 12. Zakona o naknadi štete od države. Zakonom se uspostavljaju okružna vijeća (kojima predsjeda zamjenik tužitelja u pripadajućem uredu tužitelja), Središnje vijeće (kojim predsjeda zamjenik ministra pravosuđa) i Posebno vijeće (kojim predsjeda zamjenik ministra nacionalne obrane i koje je zaduženo za zahtjeve za naknadu štete koju je nanijelo vojno osoblje ili civilni zaposlenici vojske). Zahtjeve za naknadu u načelu obrađuju okružna vijeća, no ona u određenim okolnostima moraju proslijediti predmete Središnjem ili Posebnom vijeću, primjerice ako naknada premašuje određeni iznos ili ako pojedinac podnese zahtjev za ponovno razmatranje. Sva se vijeća sastoje od članova koje je imenovao ministar pravosuđa (npr. među javnim službenicima Ministarstva pravosuđa, pravosudnim službenicima, odvjetnicima i osobama koje imaju stručno znanje u vezi s naknadom od države) i podliježu posebnim pravilima o sukobu interesa (vidjeti članak 7. Dekreta o izvršavanju Zakona o naknadi od države).

([163]) Članak 7. Zakona o naknadi od države.

([164]) Odluka Vrhovnog suda br. 2013Da208388 od 11. lipnja 2015.

([165]) Vidjeti članak 8. Zakona o naknadi od države i članak 751. Građanskog zakona.

([166]) Članci 2. i 4. Zakona o upravnim sporovima.

([167]) Odluka Vrhovnog suda 98Du18435 od 22. listopada 1999., Odluka Vrhovnog suda 99Du1113 od 8. rujna 2000. i Odluka Vrhovnog suda 2010Du3541 od 27. rujna 2012.

([168]) Članak 6. Zakona o upravnim žalbama i članak 18. stavak 1. Zakona o upravnim sporovima.

([169]) Članak 12. Zakona o upravnim sporovima.

([170]) Članci 35. i 36. Zakona o upravnim sporovima.

([171]) Odluka Vrhovnog suda br. 2006Du330 od 26. ožujka 2006.

([172]) Članak 30. stavak 1. Zakona o upravnim sporovima.

odluke/propusta, osim ako postoje opravdani razlozi ([173]). Prema sudskoj praksi Vrhovnog suda pojam „opravdani razlozi" treba široko tumačiti i zahtijeva procjenu toga je li društveno prihvatljivo dopustiti odgođenu pritužbu s obzirom na sve okolnosti predmeta ([174]). To primjerice uključuje (među ostalim) razloge za odgodu za koje se predmetna stranka ne može smatrati odgovornom (tj. situacije koje su izvan kontrole podnositelja pritužbe, na primjer ako nije bio obaviješten o prikupljanju njegovih osobnih informacija) ili višu silu (npr. prirodne katastrofe ili rat).

Na kraju, pojedinci mogu podnijeti i ustavnu žalbu pri Ustavnom sudu ([175]). Na temelju Zakona o Ustavnom sudu svaka osoba čija se temeljna prava zajamčena Ustavom povrijede izvršavanjem ili neizvršavanjem državnih ovlasti (ne uključujući sudske presude) može zahtijevati donošenje odluke o ustavnoj žalbi. Najprije treba iskoristiti druge pravne lijekove ako su dostupni. Prema sudskoj praksi Ustavnog suda strani državljani mogu podnijeti ustavnu tužbu ako su njihova osnovna prava priznata korejskim Ustavom (vidjeti objašnjenja u odjeljku 1.1.) ([176]). Ustavne tužbe moraju se podnijeti u roku od 90 dana od trenutka kad je pojedinac saznao za povredu i u roku od godine dana od njezina počinjenja. Budući da se postupak iz Zakona o upravnim sporovima primjenjuje na sporove na temelju Zakona o Ustavnom sudu ([177]), pritužba će i dalje biti prihvatljiva ako postoje „opravdani razlozi" prema tumačenju u skladu s prethodno opisanom sudskom praksom Vrhovnog suda.

Ako se najprije moraju iskoristiti drugi pravni lijekovi, ustavna žalba mora se podnijeti u roku od 30 dana od konačne odluke o takvom pravnom lijeku ([178]). Ustavni sud može proglasiti nevažećim izvršavanje državnih ovlasti koje je prouzročilo povredu ili potvrditi da je određeno nečinjenje protuustavno ([179]). U tom se slučaju od relevantnog tijela zahtijeva da poduzme mjere radi usklađivanja s odlukom Suda.

3. PRISTUP VLADE U SVRHU NACIONALNE SIGURNOSTI

3.1. Nadležna javna tijela u području nacionalne sigurnosti

Republika Koreja ima dvije posebne obavještajne agencije: NIS i Sigurnosno-obrambeno zapovjedništvo za podršku. Osim toga, policija i tužiteljstvo isto mogu prikupljati osobne informacije u svrhu nacionalne sigurnosti.

NIS je uspostavljen na temelju Zakona o Nacionalnoj obavještajnoj službi (dalje u tekstu „Zakon o NIS-u") i djeluje izravno pod nadležnošću i nadzorom predsjednika ([180]). NIS posebice prikuplja, kompilira i distribuira informacije o stranim državama (i Sjevernoj Koreji) ([181]), obavještajne podatke povezane sa zadaćom suzbijanja špijunaže (uključujući vojnu i industrijsku špijunažu), terorizma i aktivnosti međunarodnih kriminalnih udruga, obavještajne podatke o određenim vrstama kaznenih djela usmjerenih protiv javne i nacionalne sigurnosti (npr. unutarnje pobune, strana agresija) i obavještajne podatke povezane sa zadaćom osiguranja kibersigurnosti i sprečavanja kibernapada i prijetnji ([182]). U Zakonu o NIS-u, kojim se uspostavlja NIS i utvrđuju njegove zadaće, navode se i opća načela kojima se vode sve njegove aktivnosti. NIS u pravilu mora ostati politički neutralan te štititi slobodu i prava pojedinaca ([183]). Predsjednik NIS-a zadužen je za sastavljanje općenitih smjernica u kojima se utvrđuju načela, opseg i postupci za izvršavanje NIS-ovih dužnosti u vezi s prikupljanjem i upotrebom informacija te o njima mora izvještavati Nacionalnu skupštinu ([184]). Nacionalna skupština (preko svojeg Obavještajnog odbora) može zatražiti ispravak ili dopunu smjernica ako smatra da su nezakonite ili nepravedne. Općenitije govoreći, pri izvršavaju svojih dužnosti direktor i osoblje NIS-a ne smiju prisiliti nijednu instituciju, organizaciju ni pojedinca da učini nešto što nije obvezan činiti niti zlouporabom svojih službenih ovlasti spriječiti ostvarenje prava nijedne osobe ([185]). Usto, svaka cenzura pošte, presretanje telekomunikacija, prikupljanje informacija o lokaciji, prikupljanje podataka o potvrdi komunikacije ili snimanje ili prisluškivanje privatnih

([173]) Članak 20. Zakona o upravnim sporovima. Taj se rok primjenjuje i na zahtjev za potvrdu nezakonitosti propusta, vidjeti članak 38. stavak 2. Zakona o upravnim sporovima.
([174]) Odluka Vrhovnog suda br. 90Nu6521, 28. lipnja 1991.
([175]) Članak 68. stavak 1. Zakona o Ustavnom sudu.
([176]) Odluka Ustavnog suda br. 99HeonMa194, 29. studenoga 2001.
([177]) Članak 40. Zakona o Ustavnom sudu.
([178]) Članak 69. Zakona o Ustavnom sudu.
([179]) Članak 75. stavak 3. Zakona o Ustavnom sudu.
([180]) Članak 2. i članak 4. stavak 2. Zakona o NIS-u.
([181]) To ne obuhvaća informacije o pojedincima, već opće informacije o stranim državama (trendovi, kretanja) i aktivnostima državnih aktera trećih zemalja.
([182]) Članak 3. stavak 1. Zakona o NIS-u.
([183]) Članak 3. stavak 1., članak 6. stavak 2. te članci 11. i 21. Vidjeti i pravila o sukobu interesa, posebice članke 10. i 12.
([184]) Članak 4. stavak 2. Zakona o NIS-u.
([185]) Članak 13. Zakona o NIS-u.

komunikacija koje provodi NIS mora biti u skladu s CPPA-om, Zakonom o informacijama o lokaciji ili CPA-om ([186]). Svaka zlouporaba ovlasti ili prikupljanje informacija u suprotnosti s tim zakonima podliježe kaznenim sankcijama ([187]).

Sigurnosno-obrambeno zapovjedništvo za podršku je vojna obavještajna agencija uspostavljena u sklopu Ministarstva obrane. Odgovorno je za sigurnosna pitanja u vojsci, vojne kaznene istrage (koje podliježu Zakonu o vojnim sudovima) i vojne obavještajne podatke. Sigurnosno-obrambeno zapovjedništvo za podršku općenito ne nadzire civile, osim ako je to potrebno za izvršavanje njegovih vojnih funkcija. U osobe koje mogu biti pod istragom ubrajaju se vojno osoblje, civilni zaposlenici vojske, osobe u vojnoj obuci, osobe u vojnoj pričuvi ili službi novačenja i ratni zarobljenici ([188]). Pri prikupljanju informacija o komunikaciji u svrhu nacionalne sigurnosti Sigurnosno-obrambeno zapovjedništvo za podršku podliježe ograničenjima i zaštitnim mjerama utvrđenima u CPPA-u i njegovu Dekretu o izvršavanju.

3.2. **Pravna osnova i ograničenja**

CPPA, Zakon o borbi protiv terorizma radi zaštite građana i javne sigurnosti (dalje u tekstu „Zakon o borbi protiv terorizma") i TBA pružaju pravnu osnovu za prikupljanje osobnih informacija u svrhu nacionalne sigurnosti i njima se utvrđuju primjenjiva ograničenja i zaštitne mjere ([189]). Tim se ograničenjima i zaštitnim mjerama, kako su opisani u sljedećim odjeljcima, osigurava da su prikupljanje i obrada informacija ograničeni na ono što je strogo nužno za ostvarenje legitimnog cilja. To isključuje svako masovno i neselektivno prikupljanje osobnih informacija u svrhu nacionalne sigurnosti.

3.2.1. *Prikupljanje informacija o komunikaciji*

3.2.1.1. Prikupljanje informacija o komunikaciji koje vrše obavještajne agencije

3.2.1.1.1. Pravna osnova

CPPA-om se obavještajne agencije ovlašćuju da prikupljaju podatke o komunikaciji te se od pružatelja komunikacijskih usluga zahtijeva da postupaju u skladu sa zahtjevima tih agencija ([190]). Kako je opisano u odjeljku 2.2.2.1., u CPPA-u se razlikuju prikupljanje sadržaja komunikacija (tj. „mjere ograničavanja komunikacije" kao što su mjere „prisluškivanja" ili „cenzure" ([191])) i prikupljanje „podataka o potvrdi komunikacije" ([192]).

Razlikuje se prag za prikupljanje tih dviju vrsta informacija, no primjenjivi postupci i zaštitne mjere u velikoj su mjeri identični ([193]). Prikupljanje podataka o potvrdi komunikacije (ili metapodataka) može se vršiti za potrebe sprečavanja prijetnji nacionalnoj sigurnosti ([194]). Viši prag primjenjuje se na izvršavanje mjera ograničavanja komunikacije (tj. prikupljanja sadržaja komunikacija), koje se mogu poduzeti samo ako se očekuje da će nacionalna sigurnost biti u ozbiljnoj opasnosti, a prikupljanje obavještajnih podataka nužno je kako bi se spriječila takva opasnost (tj. ako postoji ozbiljan rizik za nacionalnu sigurnost, a prikupljanje podataka neophodno je za njegovo sprečavanje) ([195]). Nadalje, pristup sadržaju komunikacija može se ostvariti samo kao krajnja mjera radi osiguranja nacionalne sigurnosti, a potrebno je svesti kršenje privatnosti komunikacija na najmanju mjeru ([196]). Čak i ako se ishodi prikladno odobrenje/dopuštenje, takve se mjere moraju obustaviti odmah nakon što prestanu biti nužne, čime se osigurava da je svako kršenje komunikacijskih tajni pojedinca svedeno na najmanju mjeru ([197]).

3.2.1.1.2. Ograničenja i zaštitne mjere koji se primjenjuju na prikupljanje informacija o komunikaciji koje uključuje najmanje jednog korejskog državljanina

Prikupljanje informacija o komunikaciji (sadržaj i metapodaci) u kojem su jedan ili oba pojedinca uključena u komunikaciju korejski državljani može se vršiti samo uz dopuštenje višeg predsjednika Visokog

([186]) Članak 14. Zakona o NIS-u.
([187]) Članci 22. i 23. Zakona o NIS-u.
([188]) Članak 1. Zakona o vojnim sudovima.
([189]) Pri istrazi kaznenih djela povezanih s nacionalnom sigurnošću policija i NIS djelovat će na temelju CPA-a, a Sigurnosno-obrambeno zapovjedništvo za podršku podliježe Zakonu o vojnim sudovima.
([190]) Članak 15-2. CPPA-a.
([191]) Članak 2. stavci 6. i 7. CPPA-a.
([192]) Članak 2. točka 11. CPPA-a.
([193]) Vidjeti i članak 13-4. stavak 2. CPPA-a i članak 37. stavak 4. Dekreta o izvršavanju CPPA-a, kojima se propisuje da se postupci primjenjivi na prikupljanje sadržaja komunikacija primjenjuju *mutatis mutandis* na prikupljanje podataka o potvrdi komunikacije.
([194]) Članak 13-4. CPPA-a.
([195]) Članak 7. točka 1. CPPA-a.
([196]) Članak 3. točka 2. CPPA-a.
([197]) Članak 2. Dekreta o izvršavanju CPPA-a.

suda ([198]). Zahtjev obavještajne agencije mora se uputiti pisanim putem tužitelju ili višem državnom odvjetništvu ([199]). U njemu se moraju navesti razlozi za prikupljanje (tj. da se očekuje da će nacionalna sigurnost biti u ozbiljnoj opasnosti ili da je prikupljanje nužno kako bi se spriječile prijetnje nacionalnoj sigurnosti), zajedno s materijalima koji potkrjepljuju te razloge, uspostavom predmeta s jasnim dokazima i pojedinostima o zahtjevu (tj. svrhe, ciljani pojedinci, opseg, razdoblje valjanosti prikupljanja te način i mjesto prikupljanja) ([200]). Tužitelj/više državno odvjetništvo pak zahtijeva dopuštenje od višeg predsjednika Visokog suda ([201]). Predsjednik suda može dati pisano dopuštenje samo ako smatra zahtjev opravdanim, a odbacit će zahtjev ako smatra da je neutemeljen ([202]). U nalogu se navode vrsta, svrha, cilj, opseg i razdoblje valjanosti prikupljanja te mjesto i način na koji se to može činiti ([203]).

Primjenjuju se posebna pravila ako je cilj mjere istraga zavjere koja čini prijetnju nacionalnoj sigurnosti i ako postoji izvanredna situacija zbog koje nije moguće provesti navedene postupke ([204]). Ako su ti uvjeti ispunjeni, obavještajne agencije mogu provoditi mjere nadzora bez prethodnog odobrenja suda ([205]). Međutim, obavještajna agencija mora zatražiti dopuštenje suda odmah nakon izvršenja hitnih mjera. Ako se dopuštenje ne ishodi u roku od 36 sati nakon poduzimanja mjera, one se moraju odmah obustaviti ([206]). Prikupljanje informacija u izvanrednim situacijama mora se uvijek odvijati u skladu s „izjavom o hitnoj cenzuri/prisluškivanju”, a obavještajna agencija koja prikuplja informacije mora voditi registar svih izvanrednih mjera ([207]).

Ako se nadzor dovrši u kratkom roku, čime dopuštenje suda postaje bespredmetno, čelnik nadležnog višeg državnog odvjetništva mora čelniku nadležnog suda, koji čuva registar hitnih mjera, poslati obavijest koju je pripremila obavještajna agencija ([208]). Time se sudu omogućuje da preispita zakonitost prikupljanja.

3.2.1.1.3. Ograničenja i zaštitne mjere koji se primjenjuju na prikupljanje informacija o komunikaciji koje uključuje samo osobe koje nisu korejskog državljanstva

Za prikupljanje informacija o komunikacijama samo između osoba koje nisu korejskog državljanstva obavještajne agencije moraju dobiti prethodno pisano odobrenje predsjednika ([209]). Takve će se komunikacije prikupljati u svrhu nacionalne sigurnosti samo ako pripadaju jednoj od nekoliko navedenih kategorija, tj. komunikacije među državnim službenicima ili drugim pojedincima iz država koje su neprijatelji Republike Koreje, stranim agencijama, skupinama ili državljanima koji se sumnjiče za sudjelovanje u aktivnostima protiv Koreje ([210]) ili članovima skupina na Korejskom poluotoku koji ne potpadaju pod suverenitet Republike Koreje i njihovim krovnim skupinama koje se nalaze u stranim državama ([211]). Međutim, ako je jedna strana u komunikaciji korejski državljanin, a druga je osoba koja nije korejskog državljanstva, bit će potrebno odobrenje suda u skladu s postupkom opisanim u odjeljku 3.2.1.1.2.

Čelnik obavještajne agencije mora direktoru NIS-a podnijeti plan za mjere koje se namjeravaju poduzeti ([212]). Direktor NIS-a provjerava je li plan prikladan i, ako je tako, podnosi ga na odobrenje predsjedniku ([213]). Informacije koje je potrebno uključiti u plan iste su kao i informacije potrebne u zahtjevu za dopuštenje suda za prikupljanje informacija korejskih državljana (kako je prethodno opisano) ([214]). U njemu se moraju navesti razlozi za prikupljanje (tj. da se očekuje da će nacionalna sigurnost biti u ozbiljnoj opasnosti ili da je prikupljanje nužno kako bi se spriječile prijetnje nacionalnoj sigurnosti) te glavne osnove za sumnju, zajedno s materijalima koji potkrjepljuju te razloge,

([198]) Članak 7. stavak 1. točka 1. CPPA-a. Nadležan je visoki sud koji ima nadležnost nad mjestom prebivališta ili sjedišta jedne ili obiju stranaka pod nadzorom.
([199]) Članak 7. stavak 3. Dekreta o izvršavanju CPPA-a.
([200]) Članak 7. stavak 3. i članak 6. stavak 4. CPPA-a.
([201]) Članak 7. stavak 4. Dekreta o izvršavanju CPPA-a. U tužiteljevu zahtjevu sudu mora se utvrditi glavna osnova za sumnju i, ako se istodobno traži više dopuštenja, opravdanje za to (vidjeti članak 4. Dekreta o izvršavanju CPPA-a).
([202]) Članak 7. stavak 3., članak 6. stavak 5. i članak 6. stavak 9. CPPA-a.
([203]) Članak 7. stavak 3. i članak 6. stavak 6. CPPA-a.
([204]) Članak 8. CPPA-a.
([205]) Članak 8. točka 1. CPPA-a.
([206]) Članak 8. točka 2. CPPA-a.
([207]) Članak 8. točka 4. CPPA-a. Vidjeti odjeljak 2.2.2.2. za hitne mjere u kontekstu kaznenog progona.
([208]) Članak 8. stavci 5. i 7. CPPA-a. U toj se obavijesti moraju navesti svrha, cilj, opseg, razdoblje, mjesto izvršenja i metoda nadzora te razlozi zbog kojih zahtjev nije podnesen prije poduzimanja mjere (članak 8. stavak 6. CPPA-a).
([209]) Članak 7. stavak 1. točka 2. CPPA-a.
([210]) To se odnosi na aktivnosti kojima se ugrožavaju postojanje i sigurnost države, demokratski poredak ili život i sloboda građana.
([211]) Usto, ako je na jednoj strani osoba opisana u članku 7. stavku 1. točki 2. CPPA-a, a druga nije poznata ili se ne može utvrditi, primjenjuje se postupak opisan u članku 7. stavku 1. točki 2.
([212]) Članak 8. stavak 1. Dekreta o izvršavanju CPPA-a. Direktora NIS-a imenuje predsjednik nakon što ga potvrdi parlament (članak 7. Zakona o NIS-u).
([213]) Članak 8. stavak 2. Dekreta o izvršavanju CPPA-a.
([214]) Članak 8. stavak 3. Dekreta o izvršavanju CPPA-a u vezi s člankom 6. stavkom 4. CPPA-a.

uspostavom predmeta s jasnim dokazima i pojedinostima o zahtjevu (tj. svrhe, ciljani pojedinci, opseg, razdoblje valjanosti prikupljanja te način i mjesto prikupljanja). Ako se istodobno zahtijeva nekoliko dozvola, navode se svrhe i osnova za njih ([215]).

U izvanrednim situacijama ([216]) mora se ishoditi prethodno odobrenje ministra u čijoj se nadležnosti nalazi obavještajna agencija. Međutim, u tom slučaju obavještajna agencija mora zatražiti odobrenje predsjednika odmah nakon poduzimanja hitnih mjera. Ako obavještajna agencija ne ishodi odobrenje u roku od 36 sati nakon podnošenja zahtjeva, prikupljanje se mora odmah obustaviti ([217]). U takvim će se slučajevima prikupljene informacije uvijek uništiti.

3.2.1.1.4. Opća ograničenja i zaštitne mjere

Kad se zahtijeva suradnja privatnih subjekata, obavještajne agencije moraju im predočiti sudski nalog/dopuštenje predsjednika ili presliku naslovnice izjave o hitnoj cenzuri, što takav subjekt mora čuvati u svojim evidencijama ([218]). Subjekti od kojih se zatraži otkrivanje informacija obavještajnim agencijama na temelju CPPA-a mogu odbiti učiniti to ako se ovlaštenje ili izjava o hitnoj cenzuri odnose na pogrešan identifikator (npr. telefonski broj koji pripada nekoj drugoj osobi, a ne utvrđenom pojedincu). Usto, lozinke upotrijebljene za komunikacije ne smiju se otkrivati ni u kojem slučaju ([219]).

Obavještajne agencije mogu povjeriti provedbu mjera ograničavanja komunikacije ili prikupljanje informacija o potvrdi komunikacije poštanskom uredu ili pružatelju telekomunikacijskih usluga (kako je definirano Zakonom o telekomunikacijama) ([220]). I relevantna obavještajna agencija i pružatelj usluga kojem je upućen zahtjev za suradnju moraju tri godine čuvati registre u kojima se navode svrha zahtijevanja mjera, datum izvršenja ili suradnje i predmet mjera (npr. pošta, telefon, e-pošta) ([221]). Pružatelji telekomunikacijskih usluga koji pružaju podatke o potvrdi komunikacije moraju sedam godina čuvati informacije o učestalosti prikupljanja u svojim zapisnicima i dvaput godišnje izvješćivati ministra znanosti i IKT-a ([222]).

Obavještajne agencije moraju izvješćivati direktora NIS-a o informacijama koje su prikupile i ishodu aktivnosti nadzora ([223]). Kad je riječ o prikupljanju podataka o potvrdi komunikacije, moraju se voditi evidencije o tome da je upućen zahtjev za takve podatke te o samom pisanom zahtjevu i instituciji koja se oslonila na njega ([224]).

Prikupljanje sadržaja komunikacija i podataka o potvrdi komunikacije može trajati najviše četiri mjeseca i, ako se u međuvremenu ostvari predviđeni cilj, mora se odmah prekinuti ([225]). Ako se nastave uvjeti za dopuštenje, to se razdoblje može produljiti za najviše četiri mjeseca uz dopuštenje suda ili odobrenje predsjednika. Zahtjev za dobivanje odobrenja za produljenje mjera nadzora mora se uputiti u pisanom obliku te se moraju navesti razlozi za traženje produljenja i pružiti popratni materijali ([226]).

Ovisno o pravnoj osnovi za prikupljanje pojedinci se obično obavještavaju kad se prikupljaju njihove komunikacije. Točnije, neovisno o tome odnose li se prikupljene informacije na sadržaj komunikacija ili podatke o potvrdi komunikacije i neovisno o tome jesu li informacije pribavljene u okviru uobičajenog postupka ili u izvanrednoj situaciji, čelnik obavještajne agencije mora pisanim putem obavijestiti predmetnog pojedinca o mjeri nadzora u roku od 30 dana od datuma završetka nadzora ([227]). Obavijest mora uključivati 1. činjenicu da su informacije prikupljene, 2. agenciju koja je

([215]) Članak 8. stavak 3. i članak 4. Dekreta o izvršavanju CPPA-a.
([216]) To jest u slučajevima u kojima je cilj mjere zavjera koja čini prijetnju nacionalnoj sigurnosti, ako nema dovoljno vremena za dobivanje odobrenja predsjednika i ako nepoduzimanje hitnih mjera može narušiti nacionalnu sigurnost (članak 8. stavak 8. CPPA-a).
([217]) Članak 8. točka 9. CPPA-a.
([218]) Članak 9. stavak 2. CPPA-a i članak 12. Dekreta o izvršavanju CPPA-a.
([219]) Članak 9. točka 4. CPPA-a.
([220]) Članak 13. Dekreta o izvršavanju CPPA-a.
([221]) Članak 9. stavak 3. CPPA-a i članak 17. stavak 2. Dekreta o izvršavanju CPPA-a. To se razdoblje ne primjenjuje na podatke o potvrdi komunikacije (vidjeti članak 39. Dekreta o izvršavanju CPPA-a).
([222]) Članak 13. stavak 7. CPPA-a i članak 39. Dekreta o izvršavanju CPPA-a.
([223]) Članak 18. stavak 3. Dekreta o izvršavanju CPPA-a.
([224]) Članak 13. stavak 5. i članak 13-4. stavak 3. CPPA-a.
([225]) Članak 7. točka 2. CPPA-a.
([226]) Članak 7. stavak 2. CPPA-a i članak 5. Dekreta o izvršavanju CPPA-a.
([227]) Članak 9-2. stavak 3. CPPA-a. U skladu s člankom 13-4. CPPA-a to se primjenjuje na prikupljanje sadržaja komunikacija i podataka o potvrdi komunikacije.

izvršila prikupljanje informacija i 3. razdoblje izvršenja. Međutim, ako je vjerojatno da bi ta obavijest dovela u pitanje nacionalnu sigurnost ili ugrozila život i fizičku sigurnost građana, može se odgoditi ([228]). Obavijest je potrebno dati u roku od 30 dana nakon što osnova za odgodu prestane postojati ([229]).

Međutim, taj se zahtjev za obavješćivanje primjenjuje samo na prikupljanje informacija u kojem je barem jedna strana korejski državljanin. Zbog tog se razloga osobe koje nisu korejskog državljanstva obavješćuju samo kad se prikupljaju njihove komunikacije s korejskim državljanima. Stoga ne postoji zahtjev za obavješćivanje kad se prikupljaju komunikacije samo između osoba koje nisu korejskog državljanstva.

Sadržaj svih komunikacija i podaci o potvrdi komunikacije pribavljeni nadzorom na temelju CPPA-a mogu se upotrebljavati samo 1. za istragu, kazneni progon ili sprečavanje određenih kaznenih djela, 2. za stegovne postupke, 3. za sudske postupke u kojima se stranka koja je povezana s komunikacijom oslanja na njih pri traženju naknade štete ili 4. na temelju drugog zakonodavstva ([230]).

3.2.1.2. Prikupljanje informacija o komunikaciji koje vrši policija/tužiteljstvo u svrhu nacionalne sigurnosti

Policija/tužitelj može prikupljati informacije o komunikaciji (i sadržaj komunikacija i podatke o potvrdi komunikacije) u svrhu nacionalne sigurnosti pod istim uvjetima kakvi su opisanu u odjeljku 3.2.1.1. Kad djeluju u izvanrednim situacijama ([231]), primjenjuje se postupak koji je prethodno opisan u vezi s prikupljanjem sadržaja komunikacija u svrhu kaznenog progona u izvanrednim situacijama (tj. članak 8. CPPA-a).

3.2.2. *Prikupljanje informacija o osumnjičenicima za terorizam*

3.2.2.1. Pravna osnova

Zakonom o borbi protiv terorizma direktor NIS-a ovlašćuje se za prikupljanje informacija o osumnjičenicima za terorizam ([232]). „Osumnjičenik za terorizam” definiran je kao član terorističke skupine ([233]), osoba koja je proširila terorističku skupinu (promicanjem i širenjem ideja ili taktika terorističke skupine), prikupila ili doprinijela sredstva za terorizam ([234]) ili je sudjelovala u drugim aktivnostima pripreme, zavjere, širenja ili poticanja terorizma ili osoba za koju se na temelju valjanih razloga sumnja da se bavila takvim aktivnostima ([235]). Svaki javni službenik koji izvršava Zakon o borbi protiv terorizma općenito mora poštovati osnovna prava zajamčena Ustavom Koreje ([236]).

Zakonom o borbi protiv terorizma ne utvrđuju se posebne ovlasti, ograničenja ni zaštitne mjere za prikupljanje informacija o osumnjičenicima za terorizam, već se u njemu upućuje na postupke u drugim propisima. Prvo, na osnovu Zakona o borbi protiv terorizma direktor NIS-a može prikupljati 1. informacije o ulasku u Republiku Koreju i odlasku iz nje, 2. informacije o financijskim transakcijama i 3. informacije o komunikacijama. Ovisno o vrsti traženih informacija relevantni postupovni zahtjevi propisani su u Zakonu o imigraciji i Carinskom zakonu, ARUSFTI-ju odnosno CPPA-u ([237]). Kad je riječ o prikupljanju informacija o ulasku u Koreju i odlasku iz nje, Zakon o borbi protiv terorizma upućuje na postupke utvrđene u Zakonu o imigraciji i Carinskom zakonu. Međutim, tim se

([228]) Članak 9-2. stavak 4. CPPA-a.
([229]) Članak 13-4. stavak 2. i članak 9-2. stavak 6. CPPA-a.
([230]) Članak 5. stavci 1. i 2. te članci 12. i 13-5. CPPA-a.
([231]) To jest, ako je cilj mjere zavjera koja čini prijetnju nacionalnoj sigurnosti i ako postoji izvanredna situacija zbog koje nije moguće provesti uobičajeni postupak odobrenja (članak 8. stavak 1. CPPA-a).
([232]) Članak 9. Zakona o borbi protiv terorizma.
([233]) „Teroristička skupina” definirana je kao skupina terorista koju su proglasili Ujedinjeni narodi (članak 2. točka 2. Zakona o borbi protiv terorizma).
([234]) „Terorizam” je definiran u članku 2. točki 1. Zakona o borbi protiv terorizma kao postupanje čija je svrha narušiti izvršavanje ovlasti države, lokalne vlasti ili strane vlade (uključujući lokalne vlasti i međunarodne organizacije) ili u svrhu koja je primorava da djeluje na bilo koji način koji joj nije obvezan ili u svrhu prijetnje javnosti. To uključuje (a) ubojstvo ili predstavljanje opasnosti za nečiji život nanošenjem tjelesnih ozljeda ili uhićenjem, zatočeništvom, otmicom ili uzimanjem taoca, (b) određene vrste postupanja usmjerene na zrakoplove (npr. rušenje, protupravno oduzimanje ili nanošenje štete zrakoplovu u letu), (c) određene vrste postupanja povezane s brodovima (npr. preuzimanje broda ili morske strukture u upotrebi, uništenje broda ili morske strukture u upotrebi ili nanošenje štete brodu ili morskoj strukturi u mjeri kojom se ugrožava njezina sigurnost, uključujući nanošenje štete teretu na brodu ili morskoj strukturi u upotrebi), (d) postavljanje, detonaciju ili bilo kakvu drugu upotrebu biokemijskog, eksplozivnog ili zapaljivog oružja ili naprave s namjerom uzrokovanja smrti, ozbiljnih ozljeda ili ozbiljne materijalne štete ili koja ima takav učinak na određene vrste vozila ili objekata (npr. vlakovi, tramvaji, motorna vozila, javni parkovi i postaje, objekti za opskrbu električnom energijom, plinom i telekomunikacijama itd.), (e) određene vrste postupanja povezane s nuklearnim materijalima, radioaktivnim materijalima ili nuklearnim postrojenjima (npr. ugrožavanje ljudskih života, zdravlja ili imovine ili narušavanje javne sigurnosti na drugi način uništavanjem nuklearnog reaktora ili nepropisnom manipulacijom nuklearnim materijalima itd.).
([235]) Članak 2. stavak 3. Zakona o borbi protiv terorizma.
([236]) Članak 3. stavak 3. Zakona o borbi protiv terorizma.
([237]) Članak 9. stavak 1. Zakona o borbi protiv terorizma.

zakonima u ovom trenutku ne predviđaju takve ovlasti. Kad je riječ o prikupljanju informacija o komunikaciji i financijskim transakcijama, Zakon o borbi protiv terorizma upućuje na ograničenja i zaštitne mjere iz CPPA-a (koji su detaljnije opisani u nastavku) i ARUSFTI-ja (koji, kako je objašnjeno u odjeljku 2.1., nisu relevantni za potrebe ocjene odluke o primjerenosti).

Nadalje, u članku 9. stavku 3. Zakona o borbi protiv terorizma navodi se da direktor NIS-a može zatražiti osobne informacije ili informacije o lokaciji osumnjičenika za terorizam od voditelja obrade osobnih informacija ([238]) ili pružatelja informacija o lokaciji ([239]). Ta je mogućnost ograničena na zahtjeve za dobrovoljno otkrivanje, koje voditelji obrade osobnih informacija i pružatelji informacija o lokaciji ne moraju ispuniti, a to se ionako može učiniti samo u skladu s PIPA-om i Zakonom o informacijama o lokaciji (vidjeti odjeljak 3.2.2.2.)

3.2.2.2. Ograničenja i zaštitne mjere koji se primjenjuju na dobrovoljno otkrivanje na temelju PIPA-e i Zakona o informacijama o lokaciji

Zahtjevi za dobrovoljnu suradnju na temelju Zakona o borbi protiv terorizma moraju se ograničiti na informacije o osumnjičenicima za terorizam (vidjeti odjeljak 3.2.2.1.). Svaki takav zahtjev od NIS-a mora biti u skladu s načelima zakonitosti, nužnosti i proporcionalnosti koja proizlaze iz Ustava Koreje (članak 12. stavak 1. i članak 37. stavak 2.) ([240]) te zahtjevima iz PIPA-e za prikupljanje osobnih informacija (članak 3. stavak 1. PIPA-e, vidjeti odjeljak 1.2.). U Zakonu o NIS-u dodatno se utvrđuje da NIS ne smije prisiliti nijednu instituciju, organizaciju ni pojedinca da učini nešto što nije obvezan činiti niti zlouporabom svojih službenih ovlasti spriječiti ostvarenje prava nijedne osobe ([241]). Kršenje te zabrane može podlijegati kaznenim sankcijama ([242]).

Voditelji obrade osobnih informacija i pružatelji informacija o lokaciji koji primaju zahtjeve od NIS-a na temelju Zakona o borbi protiv terorizma nisu ih obvezni ispunjavati. Mogu dobrovoljno surađivati, no to je dopušteno samo u skladu s PIPA-om i Zakonom o informacijama o lokaciji.. Kad je riječ o usklađenosti s PIPA-om, voditelj obrade mora posebice uzeti u obzir interese ispitanika i ne smije otkrivati informacije ako bi se time vjerojatno nepošteno povrijedili interesi pojedinca ili treće strane ([243]). Usto, u skladu s Obavijesti br. 2021-1 o dopunskim pravilima za tumačenje i primjenu Zakona o zaštiti osobnih informacija, predmetni pojedinac mora se obavijestiti o otkrivanju. U iznimnim situacijama takva se obavijest može odgoditi, posebice ako i onoliko dugo koliko bi se njome ugrozila kaznena istraga u tijeku ili ako je vjerojatno da bi se ugrozio život ili zdravlje druge osobe čija prava ili interesi nedvojbeno imaju prednost pred pravima ispitanika ([244]).

3.2.2.3. Ograničenja i zaštitne mjere na temelju CPPA-a

Obavještajne agencije mogu na temelju Zakona o borbi protiv terorizma prikupljati samo informacije o komunikaciji (i sadržaju komunikacija i podacima o potvrdi komunikacije) kad je to potrebno za aktivnosti suzbijanja terorizma, tj. aktivnosti povezane sa sprečavanjem terorizma i protuterorističkim mjerama. Postupci iz CPPA-a opisani u odjeljku 3.2.1. primjenjuju se na prikupljanje informacija o komunikaciji u svrhu borbe protiv terorizma.

3.2.3. *Dobrovoljno otkrivanje telekomunikacijskih operatera*

Na temelju TBA-a telekomunikacijski operateri mogu ispuniti zahtjev za otkrivanje „podataka o komunikacijama” koji upućuje obavještajna agencija koja namjerava prikupljati informacije kako bi se spriječila prijetnja nacionalnoj sigurnosti ([245]). Svaki takav zahtjev mora biti u skladu s načelima zakonitosti, nužnosti i proporcionalnosti koja proizlaze iz Ustava Koreje (članak 12. stavak 1. i članak 37. stavak 2.) ([246]) te zahtjevima iz PIPA-e za prikupljanje osobnih informacija (članak 3. stavak 1. PIPA-e, vidjeti odjeljak 1.2.). Isto tako, primjenjuju se ista ograničenja i zaštitne mjere kao i za dobrovoljna otkrivanja u svrhe kaznenog progona (vidjeti odjeljak 2.2.3.) ([247]).

([238]) Kako je definiran u članku 2. PIPA-e, tj. javna institucija, pravna osoba, organizacija, pojedinac itd. koji izravno ili neizravno obrađuje osobne informacije radi upravljanja datotekama s osobnim informacijama u službene ili poslovne svrhe.

([239]) Kako je definiran u članku 5. Zakona o zaštiti, upotrebi i drugome u vezi s informacijama o lokaciji (dalje u tekstu „Zakon o informacijama o lokaciji”), tj. svatko tko je dobio dopuštenje od Korejskog povjerenstva za komunikacije za poslovanje s informacijama o lokaciji.

([240]) Vidjeti i članak 3. stavke 2. i 3. Zakona o borbi protiv terorizma.

([241]) Članak 11. stavak 1. Zakona o NIS-u.

([242]) Članak 19. Zakona o NIS-u.

([243]) Članak 18. stavak 2. PIPA-e.

([244]) Obavijest PIPC-a br. 2021-1 o dopunskim pravilima za tumačenje i primjenu Zakona o zaštiti osobnih informacija, odjeljak III., dio 2., točka iii.

([245]) Članak 83. stavak 3. TBA-a.

([246]) Vidjeti i članak 3. stavke 2. i 3. Zakona o borbi protiv terorizma.

([247]) Konkretnije, zahtjev mora biti u pisanom obliku i u njemu se moraju navesti razlozi za zahtjev, poveznica na relevantnog korisnika i opseg traženih informacija, a pružatelj telekomunikacijskih usluga mora voditi evidencije i dvaput godišnje izvješćivati ministra znanosti i IKT-a.

Telekomunikacijski operateri nisu obvezni surađivati, no mogu to činiti dobrovoljno i samo u skladu s PIPA-om. U tom se pogledu na telekomunikacijske operatere primjenjuju iste obveze, uključujući u pogledu obavješćivanja pojedinca, kao i kad primaju zahtjeve od tijela kaznenog progona, kako je detaljnije objašnjeno u odjeljku 2.2.3.

3.3. **Nadzor**

Razna tijela nadziru aktivnosti korejskih obavještajnih agencija. Nadzor Sigurnosno-obrambenog zapovjedništva za podršku provodi Ministarstvo nacionalne obrane na temelju Direktive o provedbi unutarnje revizije tog ministarstva. NIS nadziru direktor, Nacionalna skupština i druga neovisna tijela, kako je detaljnije objašnjeno u nastavku.

3.3.1. *Službenik za zaštitu ljudskih prava*

Kad obavještajne agencije prikupljaju informacije o osumnjičenicima za terorizam, u Zakonu o borbi protiv terorizma predviđa se nadzor koji provode Povjerenstvo za borbu protiv terorizma i Službenik za zaštitu ljudskih prava (dalje u tekstu „HRPO”) ([248]).

Povjerenstvo za borbu protiv terorizma među ostalim osmišljava politike o aktivnostima povezanima sa sprečavanjem terorizma i nadzire provedbu protuterorističkih mjera, kao i aktivnosti različitih nadležnih tijela u području borbe protiv terorizma ([249]). Tim povjerenstvom predsjedava premijer, a sastoji se od nekoliko ministara i čelnika vladinih agencija, uključujući ministra vanjskih poslova, ministra pravosuđa, ministra nacionalne obrane, ministra unutarnjih poslova i sigurnosti, direktora NIS-a, glavnog načelnika Nacionalne policijske agencije i predsjednika Povjerenstva za financijske usluge ([250]). Pri provedbi protuterorističkih istraga i praćenja osumnjičenika za terorizam radi prikupljanja informacija ili materijala potrebnih za aktivnosti suzbijanja terorizma direktor NIS-a mora izvješćivati predsjednika Povjerenstva za borbu protiv terorizma (tj. premijera) ([251]).

Zakonom o borbi protiv terorizma isto se tako uspostavlja HRPO kako bi se osnovna prava pojedinaca zaštitila od povreda uzrokovanih aktivnostima suzbijanja terorizma ([252]). HRPO-a imenuje predsjednik Povjerenstva za borbu protiv terorizma među pojedincima koji ispunjavaju kvalifikacije navedene u Dekretu o izvršavanju Zakona o borbi protiv terorizma (tj. svatko tko ima deset godina radnog iskustva kao odvjetnik ili tko ima stručno znanje u području ljudskih prava i tko najmanje deset godina radi ili je radio kao izvanredni profesor (ili više zvanje) ili tko je obnašao dužnost višeg javnog službenika u državnim agencijama ili lokalnim vlastima ili tko ima najmanje deset godina radnog iskustva u području ljudskih prava, npr. u nevladinoj organizaciji) ([253]). HRPO se imenuje na dvije godine (uz mogućnost obnavljanja mandata) i može se razriješiti dužnosti samo na određenoj i ograničenoj osnovi i zbog valjanih razloga, npr. ako je protiv njega podignuta optužnica u kaznenom predmetu povezanom s njegovim zadaćama, ako otkriva povjerljive informacije ili zbog dugotrajne mentalne ili fizičke nesposobnosti ([254]).

Kad je riječ o njegovim ovlastima, HRPO može izdati preporuke za poboljšanje zaštite ljudskih prava u agencijama koje su uključene u aktivnosti suzbijanja terorizma i može obrađivati zahtjeve građana (vidjeti odjeljak 3.4.3) ([255]). Ako se razumno može utvrditi postojanje povrede ljudskih prava pri izvršavanju službenih dužnosti, HRPO može preporučiti čelniku relevantne agencije da ispravi takvo kršenje ([256]). Relevantna agencija mora zatim obavijestiti HRPO o mjerama koje su poduzete kako bi se provela takva preporuka ([257]). Ako agencija ne provede preporuku HRPO-a, taj se slučaj prosljeđuje Povjerenstvu, uključujući njegova predsjednika, tj. premijera. Dosad nije bilo slučajeva u kojima preporuke HRPO-a nisu provedene.

3.3.2. *Nacionalna skupština*

Kako je objašnjeno u odjeljku 2.3.2., Nacionalna skupština može provoditi istragu i inspekcijske preglede javnih tijela te u tom kontekstu zahtijevati otkrivanje dokumenata i zatražiti od pojedinaca da svjedoče. Kad je riječ o pitanjima koja potpadaju pod nadležnost NIS-a, takav parlamentarni nadzor provodi Obavještajni odbor Nacionalne skupštine ([258]). Direktor

([248]) Članak 7. Zakona o borbi protiv terorizma.
([249]) Članak 5. stavak 3. Zakona o borbi protiv terorizma.
([250]) Članak 3. stavak 1. Dekreta o izvršavanju Zakona o borbi protiv terorizma.
([251]) Članak 9. stavak 4. Zakona o borbi protiv terorizma.
([252]) Članak 7. Zakona o borbi protiv terorizma.
([253]) Članak 7. stavak 1. Dekreta o izvršavanju Zakona o borbi protiv terorizma.
([254]) Članak 7. stavak 3. Dekreta o izvršavanju Zakona o borbi protiv terorizma.
([255]) Članak 8. stavak 1. Dekreta o izvršavanju Zakona o borbi protiv terorizma.
([256]) Članak 9. stavak 1. Dekreta o izvršavanju Zakona o borbi protiv terorizma. HRPO samostalno odlučuje o donošenju preporuka, no obvezan je o njima izvijestiti predsjednika Povjerenstva za borbu protiv terorizma.
([257]) Članak 9. stavak 2. Dekreta o izvršavanju Zakona o borbi protiv terorizma.
([258]) Članak 36. i članak 37. stavak 1. točka 16. Zakona o Nacionalnoj skupštini.

NIS-a, koji nadzire izvršavanje zadaća te agencije, izvješćuje Obavještajni odbor (i predsjednika) ([259]). Sam Obavještajni odbor može isto tako zatražiti izvješće o određenom pitanju, na koje direktor NIS-a mora dogovoriti bez odgode ([260]). On može odbiti odgovoriti Obavještajnom odboru ili svjedočiti pred njim samo kad je riječ o državnim tajnama povezanima s vojskom, diplomatskim pitanjima ili pitanjima povezanima sa Sjevernom Korejom u kojima javno znanje može imati ozbiljan učinak na sudbinu države ([261]). U tom slučaju Obavještajni odbor mora zatražiti objašnjenje od premijera. Ako se takvo objašnjenje ne podnese u roku od sedam dana od upućivanja zahtjeva, odgovor ili svjedočenje više se neće moći odbiti.

Ako Nacionalna skupština utvrdi postojanje nezakonitih ili neprikladnih aktivnosti, može od predmetnog javnog tijela zatražiti da poduzme korektivne mjere, uključujući isplatu naknade, poduzimanje stegovnih mjera i poboljšanje internih postupaka ([262]). To tijelo nakon takvog zahtjeva mora djelovati bez odgode i izvijestiti Nacionalnu skupštinu o ishodu. Postoje posebna pravila o parlamentarnom nadzoru kad je u pitanju upotreba mjera ograničavanja komunikacije (tj. prikupljanje sadržaja komunikacija) na temelju CPPA-a ([263]). Kad je riječ o potonjem, Nacionalna skupština može od čelnika obavještajnih agencija zatražiti izvješće o svim posebnim mjerama ograničavanja komunikacije. Isto tako, može provoditi inspekcijske preglede opreme za prisluškivanje na licu mjesta. Konačno, obavještajne agencije koje su prikupile informacije o sadržaju i operateri koji su otkrili takve informacije u svrhu nacionalne sigurnosti moraju na zahtjev Nacionalne skupštine izvješćivati o takvom otkrivanju.

3.3.3. *Revizijski i inspekcijski odbor*

BAI provodi iste funkcije nadzora u odnosu na obavještajne agencije kao i u području kaznenog progona (vidjeti odjeljak 2.3.2.) ([264]).

3.3.4. *Povjerenstvo za zaštitu osobnih informacija*

Kad je riječ o obradi podataka u svrhu nacionalne sigurnosti, uključujući fazu prikupljanja, dodatan nadzor provodi PIPC. Kako je detaljnije objašnjeno u odjeljku 1.2., to uključuje opća načela i obveze utvrđene u članku 3. i članku 58. stavku 4. PIPA-e te ostvarenje prava pojedinaca zajamčena člankom 4. PIPA-e. Usto, u skladu s člankom 7-8. stavcima 3. i 4. te člankom 7-9. stavkom 5. PIPA-e nadzor PIPC-a obuhvaća i moguće kršenje pravila iz određenih zakona o ograničenjima i zaštitnim mjerama u pogledu prikupljanja osobnih informacija, kao što su CPPA, Zakon o borbi protiv terorizma i TBA. S obzirom na zahtjeve iz članka 3. stavka 1. PIPA-e za zakonito i pošteno prikupljanje osobnih informacija, svako kršenje tih zakona ujedno je i kršenje PIPA-e. PIPC stoga ima ovlasti za istragu ([265]) kršenja zakona kojima se uređuje pristup podacima u svrhu nacionalne sigurnosti i pravila o obradi iz PIPA-e te izdaje savjete za poboljšanje, izriče korektivne mjere, preporučuje stegovne mjere i upućuje moguća kršenja relevantnim istražnim tijelima ([266]).

3.3.5. *Nacionalno povjerenstvo za ljudska prava*

Nadzor NHRC-a primjenjuje se na obavještajne agencije na isti način kao i na druga vladina tijela (vidjeti odjeljak 2.3.2).

3.4. **Pravna zaštita pojedinaca**

3.4.1. *Pravna zaštita službenika za zaštitu ljudskih prava*

Kad je riječ o prikupljanju osobnih informacija u kontekstu aktivnosti suzbijanja terorizma, posebnu mogućnost za pravnu zaštitu pruža HRPO, uspostavljen u okviru Povjerenstva za borbu protiv terorizma. HRPO obrađuje zahtjeve građana povezane s povredom ljudskih prava kao posljedicom aktivnosti suzbijanja terorizma ([267]). Može preporučiti korektivne mjere, a relevantna agencija mora izvješćivati Službenika o svim mjerama poduzetima radi provedbe takve preporuke. Pojedinci ne podliježu nijednom zahtjevu da bi podnijeli pritužbu HRPO-u. Stoga će HRPO obraditi pritužbu čak i ako predmetni pojedinac ne može činjenično dokazati povredu u fazi ispitivanja dopuštenosti.

([259]) Članak 18. Zakona o NIS-u.
([260]) Članak 15. stavak 2. Zakona o NIS-u.
([261]) Članak 17. stavak 2. Zakona o NIS-u. „Državne tajne" definirane su kao „činjenice, dobra ili znanje klasificirano kao državne tajne, kojima se pristup dopušta samo ograničenom broju osoba i koje se ne smiju otkrivati nijednoj drugoj državi ni organizaciji kako bi se izbjegle ozbiljne negativne posljedice za nacionalnu sigurnost", vidjeti članak 13. stavak 4. Zakona o NIS-u.
([262]) Članak 16. stavak 2. Zakona o inspekcijskom pregledu i istrazi državne uprave.
([263]) Članak 15. CPPA-a.
([264]) Kao i kad je riječ o Obavještajnom odboru Nacionalne skupštine, direktor NIS-a može odbiti odgovoriti BAI-ju samo u pogledu pitanja koja su državne tajne i ako bi javno znanje moglo imati ozbiljan učinak na nacionalnu sigurnost (članak 13. stavak 1. Zakona o NIS-u).
([265]) Članak 63. PIPA-e.
([266]) Članak 61. stavak 2., članak 65. stavak 1., članak 65. stavak 2. i članak 64. stavak 4. PIPA-e.
([267]) Članak 8. stavak 1. točka 2. Dekreta o izvršavanju Zakona o borbi protiv terorizma.

3.4.2. *Mehanizmi pravne zaštite dostupni na temelju PIPA-e*

Pojedinci mogu ostvariti svoja prava na pristup, ispravak, brisanje i suspenziju na temelju PIPA-e u odnosu na osobne informacije koje se obrađuju u svrhu nacionalne sigurnosti ([268]). Zahtjevi za ostvarivanje tih prava mogu se podnijeti izravno obavještajnoj agenciji ili neizravno preko PIPC-a. Obavještajna agencija može odgoditi, ograničiti ili odbiti ostvarivanje prava u mjeri i onoliko dugo koliko je to potrebno i razmjerno za zaštitu važnog cilja od javnog interesa (primjerice u mjeri i onoliko dugo koliko bi se izvršavanjem prava ugrozila istraga u tijeku ili nacionalna sigurnost) ili ako bi se izvršavanjem prava mogao ugroziti život ili zdravlje treće strane. Ako se zahtjev odbije ili ograniči, pojedinac se mora bez odgode obavijestiti o razlozima za to.

Nadalje, u skladu s člankom 58. stavkom 4. PIPA-e (zahtjev da se osigura prikladno rješavanje pojedinačnih pritužbi) i člankom 4. stavkom 5. PIPA-e (pravo na prikladnu pravnu zaštitu za svaku štetu koja proizlazi iz obrade osobnih informacija u okviru brzog i poštenog postupka), pojedinci imaju pravo na dobivanje pravne zaštite. To uključuje pravo na prijavljivanje navodnog kršenja Pozivnom centru za zaštitu privatnosti, kojim upravlja Korejska agencija za internet i sigurnost, te podnošenje pritužbe PIPC-u ([269]). Te su mogućnosti za pravnu zaštitu dostupne u slučaju mogućih povreda pravila iz određenih zakona u kojima se utvrđuju ograničenja i zaštitne mjere za prikupljanje osobnih informacija u svrhu nacionalne sigurnosti i PIPA-e. Kako je objašnjeno u Obavijesti br. 2021-1, pojedinac iz EU-a može podnijeti pritužbu PIPC-u preko svojeg nacionalnog tijela za zaštitu podataka. U tom će slučaju PIPC obavijestiti pojedinca preko nacionalnog tijela za zaštitu podataka nakon zaključenja istrage (prema potrebi uključujući informacije o izrečenim korektivnim mjerama). Protiv odluke ili nedjelovanja PIPC-a može se dodatno podnijeti žalba pri korejskim sudovima na temelju Zakona o upravnim sporovima.

3.4.3. *Pravna zaštita pri Nacionalnom povjerenstvu za ljudska prava*

Mogućnost dobivanja pravne zaštite za pojedince pri NHRC-u primjenjuje se na obavještajne agencije na isti način kao i na druga vladina tijela (vidjeti odjeljak 2.4.2.).

3.4.4. *Sudska zaštita*

Kao i kad je riječ o aktivnostima tijelâ kaznenog progona, pojedinci mogu na različite načine dobiti sudsku zaštitu protiv obavještajnih agencija u vezi s kršenjem navedenih ograničenja i zaštitnih mjera.

Prvo, pojedinci mogu dobiti naknadu štete na temelju Zakona o naknadi od države. Na primjer, u jednom je predmetu dodijeljena naknada zbog nezakonitog nadzora Sigurnosnog zapovjedništva za podršku (prethodnika Sigurnosno-obrambenog zapovjedništva za podršku) ([270]).

Drugo, Zakon o upravnim sporovima omogućuje pojedincima da ospore odluke i propuste upravnih agencija, uključujući obavještajne agencije ([271]).

Na kraju, pojedinci na temelju Zakona o Ustavnom sudu mogu podnijeti ustavnu žalbu pri Ustavnom sudu protiv mjera koje su poduzele obavještajne agencije.

([268]) Članak 3. stavak 5. i članak 4. stavci 1., 3. i 4. PIPA-e.
([269]) Članak 62. i članak 63. stavak 2. PIPA-e.
([270]) Odluka Vrhovnog suda br. 96Da42789 od 24. srpnja 1998.
([271]) Članci 3. i 4. Zakona o upravnim sporovima.