II

(Nelegislatívne akty)

ROZHODNUTIA

VYKONÁVACIE ROZHODNUTIE KOMISIE (EÚ) 2022/254

zo 17. decembra 2021

podľa nariadenia Európskeho parlamentu a Rady (EÚ) 2016/679 o primeranej ochrane osobných údajov zo strany Kórejskej republiky na základe zákona o ochrane osobných informácií

[oznámené pod číslom C(2021) 9316]

(Text s významom pre EHP)

EURÓPSKA KOMISIA,

so zreteľom na Zmluvu o fungovaní Európskej únie,

so zreteľom na nariadenie Európskeho parlamentu a Rady (EÚ) 2016/679 z 27. apríla 2016 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov, ktorým sa zrušuje smernica 95/46/ES (ďalej len „všeobecné nariadenie o ochrane údajov“) ([1]), a najmä na jeho článok 45 ods. 3,

keďže:

1. ÚVOD

(1) V nariadení (EÚ) 2016/679 sa stanovujú pravidlá prenosu osobných údajov od prevádzkovateľov alebo sprostredkovateľov v Únii do tretích krajín a medzinárodným organizáciám, pokiaľ tieto prenosy patria do rozsahu jeho pôsobnosti. Pravidlá upravujúce medzinárodné prenosy údajov sa stanovujú v kapitole V (článkoch 44 až 50) uvedeného nariadenia. Hoci je pre rozmach medzinárodnej spolupráce a cezhraničného obchodu nevyhnutný tok osobných údajov do krajín mimo Európskej únie aj z takýchto krajín, prenosy do tretích krajín nesmú ohrozovať zabezpečovanú úroveň ochrany osobných údajov v Únii ([2]).

(2) Podľa článku 45 ods. 3 nariadenia (EÚ) 2016/679 môže Komisia prostredníctvom vykonávacieho aktu rozhodnúť, že tretia krajina, územie alebo jeden či viaceré určené sektory v tretej krajine alebo medzinárodná organizácia zaručujú primeranú úroveň ochrany. Pod touto podmienkou sa prenosy osobných údajov do tretej krajiny môžu uskutočňovať bez potreby získania ďalšieho povolenia, ako sa stanovuje v článku 45 ods. 1 a v odôvodnení 103 nariadenia (EÚ) 2016/679.

(3) Ako sa uvádza v článku 45 ods. 2 nariadenia (EÚ) 2016/679, prijatie rozhodnutia o primeranosti musí vychádzať z komplexnej analýzy právneho poriadku tretej krajiny, pričom sa vzťahuje na pravidlá uplatniteľné na dovozcov údajov, ako aj na obmedzenia a záruky týkajúce sa prístupu k osobným údajom zo strany orgánov verejnej moci. Komisia musí v rámci svojho posúdenia určiť, či predmetná tretia krajina zaručuje úroveň ochrany, ktorá „v zásade zodpovedá“ úrovni zabezpečenej v rámci Európskej únie [odôvodnenie 104 nariadenia (EÚ) 2016/679]. Či ide o tento prípad, sa posúdi na základe právnych predpisov Únie, najmä nariadenia (EÚ) 2016/679, ako aj judikatúry Súdneho dvora Európskej únie ([3]).

([1]) Ú. v. EÚ L 119, 4.5.2016, s. 1.
([2]) Pozri odôvodnenie 101 nariadenia (EÚ) 2016/679.
([3]) Spomedzi najnovších pozri vec C-311/18, Facebook Ireland/Schrems (ďalej len „Schrems II“), ECLI:EU:C:2020:559.

(4) Ako objasnil Súdny dvor Európskej únie, nie je potrebné, aby bola zaistená rovnaká úroveň ochrany ([4]). Konkrétne prostriedky, ktoré dotknutá tretia krajina využíva na ochranu osobných údajov, sa môžu líšiť od prostriedkov využívaných v Únii, pokiaľ sa v praxi preukáže, že sa nimi účinne zabezpečuje primeraná úroveň ochrany ([5]). V záujme dosiahnutia štandardu primeranosti teda nie je potrebné, aby pravidlá druhej krajiny do detailu zodpovedali pravidlám Únie. Namiesto toho sa skôr overuje, či príslušný zahraničný systém ako celok zabezpečuje prostredníctvom hmotnoprávnej úpravy práv na súkromie a ich účinného uplatňovania, presadzovania, ako aj dohľadu nad nimi, požadovanú úroveň ochrany ([6]). Usmernenie v tomto smere sa poskytuje aj v Referenčnom kritériu primeranosti Európskeho výboru pre ochranu údajov, v ktorom sa tento štandard podrobnejšie objasňuje ([7]).

(5) Komisia dôkladne zanalyzovala kórejské právo a prax. Na základe zistení uvedených v odôvodneniach (8) – (208) Komisia dospela k záveru, že Kórejská republika zabezpečuje primeranú ochranu osobných údajov prenášaných od prevádzkovateľa alebo sprostredkovateľa v Únii ([8]) subjektom (napr. fyzickým a právnickým osobám, organizáciám, verejným inštitúciám) v Kórei, ktoré patria do rozsahu pôsobnosti zákona o ochrane osobných informácií (zákon č. 10465 z 29. marca 2011 naposledy zmenený zákonom č. 16930 zo 4. februára 2020). Vzťahuje sa to na prevádzkovateľov, ako aj sprostredkovateľov (ďalej len „poskytovatelia externých činností“ ([9])) v zmysle nariadenia (EÚ) 2016/679. Záver o primeranosti sa nevzťahuje na spracúvanie osobných údajov na účely vykonávania misijných činností náboženskými organizáciami a menovanie kandidátov politickými stranami ani na spracúvanie osobných úverových informácií podľa zákona o úverových informáciách prevádzkovateľmi, ktorí podliehajú dozoru Komisie pre finančné služby.

(6) V tomto závere sa prihliada na dodatočné záruky stanovené v oznámení č. 2021-5 (príloha I) a oficiálne vyhlásenia, uistenia a záväzky kórejskej vlády Komisii (príloha II).

(7) Na základe tohto rozhodnutia sa môžu prenosy prevádzkovateľom a sprostredkovateľom v Kórejskej republike uskutočňovať bez potreby získania ďalšieho povolenia. Nemá to vplyv na priame uplatňovanie nariadenia (EÚ) 2016/679 na také subjekty, v prípade ktorých sú splnené podmienky týkajúce sa územného rozsahu uvedeného nariadenia stanovené v jeho článku 3.

2. PRAVIDLÁ, KTORÉ SA UPLATŇUJÚ NA SPRACÚVANIE OSOBNÝCH ÚDAJOV

2.1. Rámec ochrany údajov v Kórejskej republike

(8) Právny systém, ktorým sa upravuje ochrana súkromia a údajov v Kórei, vychádza z kórejskej ústavy vyhlásenej 17. júla 1948. Hoci sa právo na ochranu osobných údajov v ústave výslovne nestanovuje, uznáva sa ako základné právo vyplývajúce z ústavných práv na ľudskú dôstojnosť a úsilie o šťastný život (článok 10), súkromný život (článok 17) a súkromie komunikácie (článok 18). Potvrdil to najvyšší ([10]) aj ústavný súd ([11]). Základné práva a slobody (vrátane práva na súkromie) možno obmedziť len zákonom, a to vtedy, ak je to potrebné z dôvodu národnej bezpečnosti alebo udržania verejného poriadku pre blaho verejnosti, pričom to nemôže mať vplyv na podstatu predmetného práva alebo slobody (článok 37 ods. 2).

([4]) Vec C-362/14, Maximillian Schrems/Data Protection Commissioner (ďalej len „Schrems“), ECLI:EU:C:2015:650, bod 73.
([5]) Vec Schrems, bod 74.
([6]) Pozri oznámenie Komisie Európskemu parlamentu a Rade Výmena a ochrana osobných údajov v globalizovanom svete [COM(2017) 7] z 10. 1. 2017, oddiel 3.1, s. 6 – 7.
([7]) Európsky výbor pre ochranu údajov, Referenčné kritérium primeranosti, WP 254 rev. 01, k dispozícii na tomto odkaze: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=614108.
([8]) Toto rozhodnutie má význam pre EHP. Dohodou o Európskom hospodárskom priestore (ďalej len „Dohoda o EHP“) sa vnútorný trh Európskej únie rozširuje o tri štáty EHP – Island, Lichtenštajnsko a Nórsko. Spoločný výbor EHP prijal 6. júla 2018 rozhodnutie, ktorým sa nariadenie (EÚ) 2016/679 začlenilo do prílohy XI k Dohode o EHP; uvedené rozhodnutie nadobudlo účinnosť 20. júla 2018. Spomínané nariadenie preto patrí do rozsahu pôsobnosti uvedenej dohody. Na účely tohto rozhodnutia sa preto majú odkazy na EÚ a členské štáty EÚ chápať ako odkazy na štáty EHP.
([9]) Pozri oddiel 2.2.3 tohto rozhodnutia.
([10]) Pozri napríklad rozhodnutie najvyššieho súdu č. 2014Da77970 z 15. októbra 2015 (anglické zhrnutie je k dispozícii v odkaze Vec Zverejnenie členov učiteľských odborov zákonodarcom na adrese https://www.privacy.go.kr/eng/enforcement_01.do) a v ňom citovanú judikatúru vrátane rozhodnutia č. 2012Da49933 z 24. júla 2014.
([11]) Pozri najmä rozhodnutie ústavného súdu č. 99Hun-ma513 z 26. mája 2005 (anglické zhrnutie je k dispozícii na adrese http://www.koreanlii.or.kr/w/index.php/99Hun-Ma513?ckattempt=2) a rozhodnutie č. 2014JHun-ma449 2013 Hun-Ba68 (konsolidované znenie) z 23. decembra 2015 (anglické zhrnutie je k dispozícii v odkaze Vec Zmena registračného čísla rezidenta na adrese https://www.privacy.go.kr/eng/enforcement_01.do).

(9) Hoci sa v ústave na viacerých miestach odkazuje na práva kórejských občanov, ústavný súd rozhodol, že aj cudzí štátni príslušníci majú základné práva ([12]). Konkrétne súd rozhodol, že ochrana dôstojnosti a hodnoty ľudskej bytosti, ako aj právo usilovať sa o šťastný život, sú práva prináležiace každej ľudskej bytosti, nielen občanom ([13]). Okrem toho sa podľa oficiálneho zastúpenia kórejskej vlády ([14]) vo všeobecnosti uznáva, že v článkoch 12 až 22 ústavy (ktoré obsahujú práva na súkromie) sa zabezpečujú základné ľudské práva ([15]). Hoci zatiaľ neexistuje žiadna judikatúra, ktorá by sa osobitne týkala práva na súkromie cudzích štátnych príslušníkov, jej ukotvenie v ochrane ľudskej dôstojnosti a úsilí o šťastný život tento záver podporuje ([16]).

(10) Okrem toho Kórea prijala súbor zákonov v oblasti ochrany údajov, ktorými sa poskytujú záruky pre všetkých jednotlivcov bez ohľadu na ich štátnu príslušnosť ([17]). Na účel tohto rozhodnutia medzi príslušné zákony patria:

— zákon o ochrane osobných informácií,

— zákon o používaní a ochrane úverových informácií ([18]),

— zákon o ochrane súkromia komunikácie.

(11) V zákone o ochrane osobných informácií sa stanovuje všeobecný právny rámec ochrany údajov v Kórejskej republike. Tento zákon dopĺňa vykonávací dekrét (prezidentský dekrét č. 23169 z 29. septembra 2011, naposledy zmenený prezidentským dekrétom č. 30892 zo 4. augusta 2020) (ďalej len „vykonávací dekrét k zákonu o ochrane osobných informácií“), ktorý je rovnako ako zákon o ochrane osobných informácií právne záväzný a vymožiteľný.

(12) Okrem toho sa ďalšie pravidlá výkladu a uplatňovania zákona o ochrane osobných informácií uvádzajú v regulačných „oznámeniach“ vydávaných Komisiou pre ochranu osobných informácií. Na základe článku 5 (Povinnosti štátu) a článku 14 (Medzinárodná spolupráca) zákona o ochrane osobných informácií prijala Komisia pre ochranu osobných informácií oznámenie č. 2021-1 z 1. septembra 2020 (zmenené oznámením č. 2021-1 z 21. januára 2021 a oznámením č. 2021-5 zo 16. novembra 2021, ďalej len „oznámenie č. 2021-5“) týkajúce sa výkladu, uplatňovania a presadzovania určitých ustanovení zákona o ochrane osobných informácií. V tomto oznámení sa uvádzajú objasnenia, ktoré sa uplatňujú na každé spracúvanie osobných údajov podľa zákona o ochrane osobných informácií, ako aj dodatočné záruky týkajúce sa osobných údajov prenášaných do Kórey na základe tohto rozhodnutia. Oznámenie je právne záväzné pre prevádzkovateľov osobných informácií a vymožiteľné Komisiou pre ochranu osobných informácií aj súdmi ([19]). Porušenie pravidiel stanovených v oznámení predstavuje porušenie príslušných ustanovení zákona o ochrane osobných informácií, ktorý dopĺňajú. Obsah dodatočných záruk sa preto analyzuje v rámci posudzovania príslušných článkov zákona o ochrane osobných informácií. A napokon sa ďalšie usmernenie týkajúce sa zákona o ochrane osobných informácií a jeho vykonávacieho dekrétu, v ktorom sa informuje o uplatňovaní a presadzovaní pravidiel ochrany údajov Komisiou pre ochranu osobných informácií, uvádza v príručke a usmerneniach k zákonu o ochrane osobných informácií, ktoré vydala Komisia pre ochranu osobných informácií ([20]).

([12]) Rozhodnutie ústavného súdu č. 93Hun-MA120 z 29. decembra 1994.

([13]) Rozhodnutie ústavného súdu č. 99HeonMa494 z 29. novembra 2001.

([14]) Pozri oddiel 1.1 prílohy II.

([15]) Pozri aj článok 1 zákona o ochrane osobných informácií, v ktorom sa výslovne odkazuje na „slobody a práva jednotlivcov“. Konkrétnejšie sa v ňom stanovuje, že účelom tohto zákona je „zabezpečiť spracúvanie a ochranu osobných informácií na účely ochrany slobody a práv jednotlivcov a prehlbovanie dôstojnosti a hodnoty jednotlivcov“. Podobne sa v článku 5 ods. 1 zákona o ochrane osobných informácií stanovuje zodpovednosť štátu za „formulovanie politík na predchádzanie škodlivým dôsledkom získavania informácií na iný ako stanovený účel, zneužívania a nesprávneho používania osobných informácií, nepovoleného sledovania a prenasledovania atď. a na posilnenie dôstojnosti ľudských bytostí a súkromia jednotlivcov“.

([16]) Okrem toho sa v článku 6 ods. 2 ústavy stanovuje, že postavenie cudzích štátnych príslušníkov sa zaručuje podľa medzinárodného práva a zmlúv. Kórea je zmluvnou stranou viacerých medzinárodných dohôd, v ktorých sa zaručuje právo na súkromie. Ide o Medzinárodný pakt o občianskych a politických právach (článok 17), Dohovor o právach osôb so zdravotným postihnutím (článok 22) a Dohovor o právach dieťaťa (článok 16).

([17]) Obsahujú pravidlá, ktoré sú relevantné pre ochranu osobných údajov, neuplatňujú sa však na situáciu, keď sa osobné údaje získané v Únii prenášajú do Kórey podľa nariadenia (EÚ) 2016/679, napríklad v zákone o ochrane, používaní atď. informácií o polohe.

([18]) Účelom tohto zákona je posilniť riadne nakladanie s úverovými informáciami, podporiť efektívne využívanie a systematické riadenie úverových informácií a ochranu súkromia pred zneužitím alebo nesprávnym použitím úverových informácií (článok 1 zákona).

([19]) Kórejské súdy napríklad rozhodli o dodržiavaní súladu s regulačnými oznámeniami vo viacerých prípadoch vrátane pripísania zodpovednosti kórejským prevádzkovateľom za porušenia oznámenia (pozri napr. rozhodnutie najvyššieho súdu č. 2018Da219406 z 25. októbra 2018, v ktorom súd nariadil prevádzkovateľovi, aby jednotlivcom zaplatil náhradu škody za škody utrpené v dôsledku porušenia „oznámenia normy pre opatrenia na zaistenie bezpečnosti osobných informácií“; pozri aj rozhodnutie najvyššieho súdu č. 2018Da219352 z 25. októbra 2018; rozhodnutie najvyššieho súdu č. 2011Da24555 zo 16. mája 2016; rozhodnutie soulského ústredného okresného súdu č. 2014Gahap511956 z 13. októbra 2016; rozhodnutie soulského ústredného okresného súdu č. 2009Gahap43176 z 26. januára 2010).

([20]) Článok 12 ods. 1 zákona o ochrane osobných informácií.

(13) Okrem toho sa v zákone o používaní a ochrane úverových informácií stanovujú osobitné pravidlá, ktoré sa uplatňujú na „bežné“ obchodné subjekty, ako aj na špecializované subjekty v rámci finančného sektora, pri spracúvaní osobných úverových informácií, t. j. informácií, ktoré sú potrebné na určenie úverovej bonity strán finančných alebo obchodných transakcií. Ide najmä o meno, kontaktné údaje, finančné transakcie, úverový rating, poistenie alebo zostatok úveru, ak sa takéto informácie používajú na určenie úverovej bonity jednotlivca ([21]). Naopak platí, že ak sa tieto informácie používajú na iné účely (napr. v oblasti ľudských zdrojov), zákon o ochrane osobných informácií sa uplatňuje vo svojej celistvosti. Pokiaľ ide o osobitné ustanovenia zákona o používaní a ochrane úverových informácií týkajúce sa ochrany údajov, ich dodržiavanie kontroluje čiastočne Komisia pre ochranu osobných informácií (v prípade obchodných organizácií, pozri článok 45-3 zákona o používaní a ochrane úverových informácií) a čiastočne Komisia pre finančné služby ([22]) (v prípade finančného sektora vrátane ratingových agentúr, bánk, poisťovní, vzájomných sporiteľní, špecializovaných finančných úverových spoločností, finančných spoločností poskytujúcich investičné služby, finančných spoločností obchodujúcich s cennými papiermi, úverových družstiev atď., pozri článok 45 ods. 1 zákona o používaní a ochrane úverových informácií v spojení s článkom 36-2 vykonávacieho dekrétu k zákonu o používaní a ochrane úverových informácií a článkom 38 zákona o Komisii pre finančné služby). V tomto zmysle sa rozsah tohto rozhodnutia obmedzuje na obchodných prevádzkovateľov, ktorí podliehajú dozoru Komisie pre ochranu osobných informácií ([23]). Osobitné pravidlá zákona o používaní a ochrane úverových informácií uplatňované v tejto súvislosti (všeobecné pravidlá zákona o ochrane osobných informácií sa uplatňujú vtedy, ak neexistujú osobitné pravidlá) sa uvádzajú v oddiele 2.3.11.

2.2. **Vecná a osobná pôsobnosť zákona o ochrane osobných informácií**

(14) S výnimkou odlišných osobitných ustanovení z iných zákonov sa ochrana osobných údajov upravuje v zákone o ochrane osobných informácií (článku 6). Vecná a osobná pôsobnosť jeho uplatňovania sa určuje na základe vymedzených pojmov „osobné informácie“, „spracúvanie“ a „prevádzkovateľ osobných informácií“.

2.2.1. *Vymedzenie osobných údajov*

(15) V článku 2 bode 1 zákona o ochrane osobných informácií sa osobné informácie vymedzujú ako informácie o žijúcom jednotlivcovi, na základe ktorých možno daného jednotlivca identifikovať priamo, napríklad na základe mena, registračného čísla rezidenta alebo fotografie, alebo nepriamo, konkrétne ak sa môžu informácie, na základe ktorých nemožno jednotlivca identifikovať priamo, jednoducho skombinovať s inými informáciami. To, či možno informácie „jednoducho“ skombinovať, závisí od toho, či je takáto kombinácia primerane pravdepodobná vzhľadom na možnosť získania ďalších informácií, ako aj na čas, náklady a technológie potrebné na identifikáciu jednotlivca.

(16) Okrem toho sa za osobné údaje podľa zákona o ochrane osobných informácií [článok 2 bod 1 písm. c) zákona o ochrane osobných informácií] považujú pseudonymné informácie, t. j. informácie, na základe ktorých nie je možné identifikovať konkrétneho jednotlivca bez ich použitia alebo skombinovania s dodatočnými informáciami na ich obnovu do pôvodného stavu. A naopak platí, že informácie, ktoré sú plne „anonymizované“, sú z rozsahu uplatňovania zákona o ochrane osobných informácií vylúčené (článok 58-2 zákona o ochrane osobných informácií). Ide o informácie, na základe ktorých nemožno identifikovať konkrétneho jednotlivca, a to ani vtedy, ak sa skombinujú s inými informáciami, pričom sa prihliadne na čas, náklady a technológie primerane potrebné na identifikáciu.

(17) To zodpovedá vecnej pôsobnosti uplatňovania nariadenia (EÚ) 2016/679 a jeho pojmov „osobné údaje“, „pseudonymizácia“ ([24]) a „anonymizované informácie“ ([25]).

([21]) Článok 2 ods. 1 zákona o používaní a ochrane úverových informácií.

([22]) Komisia pre finančné služby je kórejským orgánom dohľadu nad finančným sektorom a v rámci tejto právomoci vykonáva aj zákon o používaní a ochrane úverových informácií.

([23]) Ak by sa to v budúcnosti zmenilo, napr. by sa rozšírila právomoc Komisie pre ochranu osobných informácií na každé spracúvanie osobných úverových informácií podľa zákona o používaní a ochrane úverových informácií, možno zvážiť zmenu rozhodnutia o primeranosti tak, aby sa týkalo aj subjektov, ktoré v súčasnosti podliehajú dozoru Komisie pre finančné služby.

([24]) V zákone o ochrane osobných informácií sa „pseudonymné spracúvanie“ považuje za spracúvanie metódami, ako sú čiastočné vymazanie osobných údajov alebo čiastočne či úplné nahradenie osobných údajov tak, aby bez dodatočných informácií nebolo možné rozpoznať konkrétneho jednotlivca (článok 2 ods. 1 až 2 zákona o ochrane osobných informácií). Zodpovedá to vymedzeniu pseudonymizácie v článku 4 bode 5 nariadenia (EÚ) 2016/679, v ktorom sa uvádza, že ide o „spracúvanie osobných údajov takým spôsobom, aby osobné údaje už nebolo možné priradiť ku konkrétnej dotknutej osobe bez použitia dodatočných informácií, za predpokladu, že sa takéto dodatočné informácie uchovávajú oddelene a vzťahujú sa na ne technické a organizačné opatrenia s cieľom zabezpečiť, aby osobné údaje neboli priradené k identifikovanej alebo identifikovateľnej fyzickej osobe“.

([25]) Konkrétne sa v odôvodnení 26 nariadenia (EÚ) 2016/679 objasňuje, že nariadenie sa neuplatňuje na anonymizované informácie, t. j. informácie, ktoré sa netýkajú identifikovanej alebo identifikovateľnej fyzickej osoby. To však závisí od všetkých prostriedkov, pri ktorých existuje primeraná pravdepodobnosť, že ich prevádzkovateľ alebo iná osoba využije na priamu alebo nepriamu identifikáciu fyzickej osoby. Na zistenie toho, či je primerane pravdepodobné, že sa takéto prostriedky použijú, sa musia zohľadniť všetky objektívne faktory, ako sú náklady a čas potrebný na identifikáciu so zreteľom na technológiu dostupnú v čase spracúvania, ako aj na technologický vývoj.

2.2.2. *Vymedzenie spracúvania*

(18) Pojem „spracúvanie“ sa vo všeobecnosti vymedzuje v zákone o ochrane osobných informácií ako týkajúci sa „spracúvania, tvorby, pripájania, prepájania, zaznamenávania, ukladania, uchovávania, spracúvania s pridanou hodnotou, úpravy, vyhľadávania, výstupu, opravy, obnovy, používania, poskytovania a sprístupňovania, ničenia osobných informácií a ďalších podobných činností“ ([26]). Hoci sa v určitých ustanoveniach zákona o ochrane osobných údajov odkazuje iba na osobitné druhy spracúvania, akými sú „používanie“, „poskytovanie“ alebo „získavanie“ ([27]) informácií, pojem „používanie“ sa vykladá ako zahŕňajúci akýkoľvek druh spracúvania iný ako „získavanie“ alebo „poskytovanie“ informácií (tretím stranám). Týmto všeobecným výkladom pojmu „používanie“ sa teda zaručuje, že sa pri osobitných činnostiach spracúvania nijako neohrozí ochrana informácií. Pojem „spracúvanie“ teda zodpovedá vymedzeniu z nariadenia (EÚ) 2016/679.

2.2.3. *Prevádzkovateľ osobných informácií a „externý poskytovateľ činností“*

(19) Zákon o ochrane osobných informácií sa uplatňuje na prevádzkovateľov osobných informácií (ďalej len „prevádzkovateľ“). Podobne ako v nariadení (EÚ) 2016/679 to znamená akúkoľvek verejnú inštitúciu, právnickú osobu, organizáciu alebo fyzickú osobu, ktorá spracúva osobné údaje priamo alebo nepriamo pri vedení zložiek osobných údajov ako súčasť svojich činností ([28]). V tejto súvislosti znamená „zložka osobných údajov“ akýkoľvek „súbor alebo súbory osobných informácií, ktoré sú systematicky usporiadané alebo zatriedené na základe určeného pravidla, čím sa umožňuje jednoduchý prístup k osobným informáciám“ (článok 2 ods. 4 zákona o ochrane osobných informácií) ([29]). Prevádzkovateľ je povinný interne vyškoliť osoby vykonávajúce spracúvanie informácií pod jeho vedením, ako napríklad úradníkov alebo zamestnancov spoločnosti, a vykonávať nad nimi primeranú kontrolu a dohľad (článok 28 ods. 1 zákona o ochrane osobných informácií).

(20) Osobitné povinnosti sa uplatňujú vtedy, ak prevádzkovateľ („zadávateľ externých činností“) zadáva spracúvanie osobných údajov externej tretej strane („poskytovateľ externých činností“). Externé zabezpečovanie činností sa musí riadiť najmä právne záväznou dohodou (zvyčajne zmluvou) ([30]), v ktorej sa stanovuje rozsah externe zabezpečovanej práce, účel spracúvania, technické a riadiace záruky, ktoré sa majú uplatňovať, dohľad vykonávaný prevádzkovateľom, zodpovednosť (ako napríklad náhrada škody za škody spôsobené porušením zmluvných povinností), ako aj obmedzenia subsprostredkovania spracúvania ([31]) (článok 26 ods. 1 a 2 zákona o ochrane osobných informácií v spojení s článkom 28 ods. 1 vykonávacieho dekrétu) ([32]).

(21) Okrem toho musí prevádzkovateľ zverejniť a pravidelne aktualizovať podrobnosti o externe zabezpečovanej práci a totožnosti poskytovateľa externých činností, prípadne v rozsahu, v akom sa externe zabezpečované spracúvanie týka činností priameho marketingu, priamo oznámiť jednotlivcom príslušné informácie (článok 26 ods. 2 a 3 zákona o ochrane osobných informácií v spojení s článkom 28 ods. 2 až 5 vykonávacieho dekrétu) ([33]).

(22) Okrem toho má prevádzkovateľ podľa článku 26 ods. 4 zákona o ochrane osobných informácií v spojení s článkom 28 ods. 6 vykonávacieho dekrétu povinnosť „vzdelávať“ poskytovateľa externých činností o potrebných bezpečnostných opatreniach a vykonávať nad ním dohľad, a to aj prostredníctvom inšpekcií, pri ktorých sa kontroluje, či dodržiava všetky povinnosti prevádzkovateľa vyplývajúce zo zákona o ochrane osobných informácií ([34]), ako aj zmluvu o externom zabezpečovaní činností. Ak poskytovateľ externých činností spôsobí škodu v dôsledku porušenia zákona o ochrane osobných informácií, jeho konanie alebo nekonanie bude na účely stanovenia zodpovednosti priradené prevádzkovateľovi rovnako, ako by to bolo v prípade zamestnanca (článok 26 ods. 6 zákona o ochrane osobných informácií).

([26]) Článok 2 ods. 2 zákona o ochrane osobných informácií.

([27]) Napríklad v článkoch 15 až 19 zákona o ochrane osobných informácií sa odkazuje iba na získavanie, používanie a poskytovanie osobných informácií.

([28]) Článok 2 ods. 5 zákona o ochrane osobných informácií. Verejné inštitúcie v zmysle zákona o ochrane osobných informácií sú všetky ústredné správne útvary alebo orgány a ich prepojené subjekty, miestne samosprávy, školy a verejné subjekty miestnej samosprávy, správne orgány národného zhromaždenia a súdnictva (vrátane ústavného súdu) (článok 2 ods. 6 zákona o ochrane osobných informácií v spojení s článkom 2 vykonávacieho dekrétu k zákonu o ochrane osobných informácií).

([29]) Zodpovedá to vecnej pôsobnosti uplatňovania nariadenia (EÚ) 2016/679. Podľa článku 2 ods. 1 nariadenia (EÚ) 2016/679 sa nariadenie uplatňuje na „spracúvanie osobných údajov vykonávané úplne alebo čiastočne automatizovanými prostriedkami a na spracúvanie inými než automatizovanými prostriedkami v prípade osobných údajov, ktoré tvoria súčasť informačného systému alebo sú určené na to, aby tvorili súčasť informačného systému“. V článku 4 bode 6 nariadenia (EÚ) 2016/679 sa „informačný systém“ vymedzuje ako „akýkoľvek usporiadaný súbor osobných údajov, ktoré sú prístupné podľa určených kritérií“. V súlade s tým sa v odôvodnení 15 vysvetľuje, že ochrana jednotlivcov by sa mala uplatňovať na „spracúvanie osobných údajov automatizovanými prostriedkami, ako aj na manuálne spracúvanie, ak sú osobné údaje uložené v informačnom systéme alebo do neho majú byť uložené. Súbory alebo zbierky súborov, ako aj ich titulné strany, ktoré nie sú štruktúrované podľa špecifických kritérií, by nemali patriť do rozsahu pôsobnosti tohto nariadenia“.

([30]) Pozri príručku k zákonu o ochrane osobných informácií, kapitolu III oddiel 2 o článku 26 (s. 203 – 212), v ktorom sa vysvetľuje, že článok 26 ods. 1 zákona o ochrane osobných informácií odkazuje na záväzné dohody, ako napríklad zmluvy alebo podobné dohody.

([31]) Podľa článku 26 ods. 5 zákona o ochrane osobných informácií sa sprostredkovateľovi zakazuje používať akékoľvek osobné informácie nad rámec rozsahu externe zabezpečovanej práce alebo poskytovať osobné informácie tretej strane. Nedodržanie tejto požiadavky môže viesť k trestnoprávnej sankcii podľa článku 71 pododseku 2 zákona o ochrane osobných informácií.

([32]) Nedodržanie tejto požiadavky môže viesť k uloženiu pokuty, pozri článok 75 ods. 4 pododsek 4 zákona o ochrane osobných informácií.

([33]) Nedodržanie tejto požiadavky môže viesť k uloženiu pokuty, pozri článok 75 ods. 2 pododsek 1, článok 75 ods. 4 pododsek 5 zákona o ochrane osobných informácií.

([34]) Pozri aj článok 26 ods. 7 zákona o ochrane osobných informácií, podľa ktorého sa na sprostredkovateľa *mutatis mutandis* uplatňujú články 15 až 25, články 27 až 31, články 33 až 38 a článok 50.

(23) Hoci sa teda v zákone o ochrane osobných informácií pojmy „prevádzkovatelia“ a „sprostredkovatelia“ nevymedzujú odlišne, pravidlá externého zabezpečovania činností obsahujú povinnosti a záruky, ktoré v zásade zodpovedajú pravidlám, ktorými sa upravuje vzťah medzi prevádzkovateľmi a sprostredkovateľmi podľa nariadenia (EÚ) 2016/679.

2.2.4. *Osobitné ustanovenia týkajúce sa poskytovateľov informačných a komunikačných služieb*

(24) Zatiaľ čo zákon o ochrane osobných informácií sa uplatňuje na spracúvanie osobných údajov akýmkoľvek prevádzkovateľom, niektoré ustanovenia obsahujú osobitné pravidlá (ako *lex specialis*) týkajúce sa spracúvania osobných údajov „používateľov“ zo strany „poskytovateľov informačných a komunikačných služieb“ ([35]). Pojem „používatelia“ sa týka jednotlivcov, ktorí používajú informačné a komunikačné služby (článok 2 ods. 1 pododsek 4 zákona o podpore využívania informačnej a komunikačnej siete a ochrane informácií, ďalej len „sieťový zákon“). Vyžaduje si to, aby jednotlivec buď priamo používal telekomunikačné služby poskytované kórejským telekomunikačným operátorom, alebo informačné služby ([36]) poskytované komerčne (t. j. s cieľom dosiahnuť zisk) subjektom, ktorý využíva služby telekomunikačného operátora s povolením podnikať alebo zaregistrovaného v Kórei ([37]). V oboch prípadoch sú ustanovenia zákona o ochrane osobných informácií záväzné pre subjekt, ktorý ponúka online služby priamo jednotlivcovi (t. j. používateľovi).

(25) Naopak, konštatovaná primeranosť sa týka výlučne úrovne ochrany poskytovanej osobným údajom prenášaným prevádzkovateľom/sprostredkovateľom v Únii subjektu v tretej krajine (v tomto prípade: v Kórejskej republike). V druhej uvedenej situácii budú mať jednotlivci v Únii zvyčajne priamy vzťah iba s „vývozcom údajov“ v Únii, a nie s kórejským poskytovateľom informačných a komunikačných služieb ([38]). Preto sa budú osobitné ustanovenia zákona o ochrane osobných informácií týkajúce sa osobných údajov používateľov informačných a komunikačných služieb uplatňovať na osobné údaje prenášané podľa tohto rozhodnutia vo väčšine prípadov iba v obmedzených situáciách.

2.2.5. *Výnimka z určitých ustanovení zákona o ochrane osobných informácií*

(26) V článku 58 ods. 1 zákona o ochrane osobných informácií sa vylučuje uplatňovanie časti zákona o ochrane osobných informácií (t. j. článkov 15 až 57) na štyri kategórie spracúvania údajov ([39]). Konkrétne sa neuplatňujú časti zákona o ochrane osobných informácií zaoberajúce sa osobitnými dôvodmi spracúvania, určitými povinnosťami v oblasti ochrany údajov, podrobnými pravidlami uplatňovania individuálnych práv, ako aj pravidlami upravujúcimi riešenie sporov týkajúcich sa osobných informácií Výborom pre mediáciu sporov. Ostatné základné ustanovenia zákona o ochrane osobných informácií zostávajú uplatniteľné, konkrétne všeobecné ustanovenia týkajúce sa zásad ochrany údajov (článok 3 zákona o ochrane osobných informácií), a to napríklad vrátane zásad zákonnosti, uvedenia účelu a obmedzenia účelu, minimalizácie údajov, presnosti a bezpečnosti údajov, a týkajúce sa individuálnych práv (na prístup, opravu, vymazanie a pozastavenie spracúvania, pozri článok 4 zákona o ochrane osobných informácií). Okrem toho sa v článku 58 ods. 4 zákona o ochrane osobných informácií ukladajú osobitné povinnosti týkajúce sa týchto činností spracúvania, konkrétne pokiaľ ide o minimalizáciu údajov, obmedzené uchovávanie údajov, bezpečnostné opatrenia a vybavovanie sťažností ([40]). V dôsledku toho by jednotlivci v prípade nedodržania týchto zásad a povinností mohli naďalej podať sťažnosť Komisii pre ochranu osobných informácií, pričom Komisia pre ochranu osobných informácií by mala v prípade ich nedodržania právomoc zaviesť opatrenia na ich presadzovanie.

([35]) Pozri najmä článok 18 ods. 2 a kapitolu VI zákona o ochrane osobných informácií.

([36]) Informačné služby pozostávajú z poskytovania informácií a sprostredkovateľských služieb na poskytovanie informácií.

([37]) Pozri článok 2 ods. 1 pododsek 3 (v spojení s článkom 2 ods. 1 pododsekmi 2 a 4) sieťového zákona a článok 2 ods. 6 a 8 zákona o telekomunikáciách.

([38]) V rozsahu, v akom budú mať kórejskí poskytovatelia informačných a komunikačných služieb priamy vzťah k jednotlivcom v EÚ (na základe ponuky online služieb), to môže viesť k priamemu uplatňovaniu nariadenia (EÚ) 2016/679 podľa jeho článku 3 ods. 2 písm. a).

([39]) V článku 58 ods. 2 zákona o ochrane osobných informácií sa ďalej stanovuje, že články 15, 22, článok 27 ods. 1 až 2, články 34 a 37 sa neuplatňujú na osobné informácie spracúvané zariadeniami vizuálneho spracúvania údajov nainštalovanými a prevádzkovanými na verejných miestach. Keďže toto ustanovenie sa týka používania monitorovania kamerovým systémom v Kórei, t. j. priameho získavania osobných informácií od jednotlivcov v Kórei, nie je relevantné na účel tohto rozhodnutia, ktoré sa týka prenosu osobných údajov prevádzkovateľmi/sprostredkovateľmi v EÚ subjektom v Kórei. Okrem toho sa podľa článku 58 ods. 3 zákona o ochrane osobných informácií článok 15 (získavanie a používanie osobných informácií), článok 30 (povinnosť zaviesť verejnú politiku ochrany súkromia) a článok 31 (povinnosť menovať zodpovednú osobu pre ochranu súkromia) neuplatňujú na osobné informácie spracúvané na účely prevádzky priateľských skupín alebo združení (napr. záujmových krúžkov). Keďže takéto skupiny sa považujú za prirodzene osobné a nemajú prepojenie na odbornú alebo obchodnú činnosť, na získavanie a používanie ich informácií v tejto súvislosti sa nevyžaduje žiadny osobitný právny základ (napríklad súhlas dotknutých jednotlivcov). Všetky ostatné ustanovenia zákona o ochrane osobných informácií (napr. o minimalizácii údajov, obmedzení účelu, zákonnosti spracúvania, bezpečnosti a individuálnych právach) sa však naďalej uplatňujú. Okrem toho by sa táto výnimka nevzťahovala na žiadne spracúvanie osobných informácií nad rámec účelu založenia sociálnej skupiny.

([40]) Konkrétnejšie sa v článku 58 ods. 4 zákona o ochrane osobných informácií stanovuje povinnosť spracúvať osobné informácie v minimálnom rozsahu potrebnom na dosiahnutie zamýšľaného účelu, spracúvať ich počas minimálneho obdobia a prijať opatrenia potrebné na bezpečné riadenie a primerané spracúvanie takýchto osobných informácií. K takýmto podmienkam patria technické, riadiace a fyzické záruky, ako aj opatrenia na zabezpečenie riadneho vybavovania sťažností jednotlivcov.

(27) Po prvé sa čiastočná výnimka týka osobných údajov získaných podľa zákona o štatistike na účely spracúvania vykonávaného verejnými inštitúciami. Z objasnení kórejskej vlády vyplýva, že osobné údaje spracúvané v tejto súvislosti sa zvyčajne týkajú kórejských štátnych príslušníkov a môžu len výnimočne obsahovať informácie o cudzincoch, najmä ak ide o štatistiky o vstupe na územie a odchode z neho, alebo o zahraničných investíciách. Ani v týchto situáciách však takéto údaje zvyčajne neprenášajú prevádzkovatelia/sprostredkovatelia v Únii, ale priamo ich získavajú orgány verejnej moci v Kórei ([41]). Podobne, ako sa to stanovuje v odôvodnení 162 nariadenia (EÚ) 2016/679, spracúvanie údajov na základe zákona o štatistike navyše podlieha viacerým podmienkam a zárukám. Konkrétne v zákone o štatistike sa ukladajú osobitné povinnosti, napríklad na zabezpečenie presnosti, jednotnosti a nestrannosti; zaručenie dôvernosti informácií o jednotlivcoch; ochranu informácií o respondentoch štatistických prieskumov, a to aj z hľadiska ochrany takýchto informácií pred použitím na akýkoľvek iný účel ako zostavovanie štatistík; ako aj uloženie požiadaviek na dôvernosť, ktoré musia dodržiavať zamestnanci ([42]). Verejné orgány spracúvajúce štatistiku musia okrem iného dodržiavať aj zásady minimalizácie údajov, obmedzenia účelu a bezpečnosti (článok 3 a článok 58 ods. 4 zákona o ochrane osobných informácií) a umožniť jednotlivcom uplatňovať ich práva (na prístup, opravu, vymazanie a pozastavenie spracúvania, pozri článok 4 zákona o ochrane osobných informácií). A napokon údaje sa musia spracúvať v anonymizovanej alebo pseudonymizovanej forme, ak sa tým zaistí splnenie účelu spracúvania (článok 3 ods.7 zákona o ochrane osobných informácií).

(28) Po druhé sa v článku 58 ods. 1 zákona o ochrane osobných informácií odkazuje na osobné údaje získavané alebo vyžiadané na účely analýzy informácií súvisiacich s národnou bezpečnosťou. Rozsah a dôsledky tejto čiastočnej výnimky sa podrobnejšie uvádzajú v odôvodnení (149).

(29) Po tretie sa čiastočná výnimka uplatňuje na dočasné spracúvanie osobných údajov v prípade, ak je to naliehavo potrebné z dôvodov verejnej bezpečnosti alebo ochrany, a to aj verejného zdravia. Túto kategóriu vykladá výlučne Komisia pre ochranu osobných informácií a podľa poskytnutých informácií sa dosiaľ nikdy nepoužila. Uplatňuje sa iba v mimoriadnych situáciách, ktoré si vyžadujú naliehavé opatrenia, napríklad ak je potrebné vysledovať infekčné látky alebo zachrániť obete prírodných katastrof, prípadne im poskytnúť pomoc ([43]). Aj v uvedených situáciách sa čiastočná výnimka vzťahuje len na spracúvanie osobných údajov na obmedzený čas potrebný na vykonanie týchto opatrení. Situácie, v ktorých by sa to mohlo uplatňovať na prenosy údajov, na ktoré sa vzťahuje toto rozhodnutie, sú ešte zriedkavejšie, keďže je málo pravdepodobné, že by osobné údaje prenesené z Únie kórejským prevádzkovateľom boli takého druhu, pri ktorom by sa ich následné spracúvanie mohlo považovať za „naliehavo potrebné“ v takýchto mimoriadnych situáciách.

(30) A napokon sa čiastočná výnimka uplatňuje na osobné údaje získané alebo použité tlačou, na vykonávanie misijných činností náboženskými organizáciami alebo na menovanie kandidátov politickými stranami. Výnimka sa uplatňuje iba vtedy, ak osobné údaje spracúva tlač, náboženské organizácie alebo politické strany na tieto osobitné účely (t. j. žurnalistické činnosti, misijnú prácu a menovanie politických kandidátov). Ak tieto subjekty spracúvajú osobné údaje na iné účely, ako napríklad na účely riadenia ľudských zdrojov alebo vnútornej správy, zákon o ochrane osobných informácií sa na ne uplatňuje vo svojej celistvosti.

(31) Pokiaľ ide o spracúvanie osobných údajov tlačou na účely žurnalistických činností, rovnováhu medzi slobodou prejavu a inými právami (vrátane práva na súkromie) zabezpečuje zákon o arbitráži a náprave atď. škôd spôsobených článkami v tlači (ďalej len „tlačový zákon“) ([44]). Konkrétne sa v článku 5 tlačového zákona stanovuje, že tlač (t. j. vysielajúca organizácia, noviny, periodikum alebo internetové noviny), internetová spravodajská služba ani internetová multimediálna vysielajúca organizácia nesmú porušiť súkromie jednotlivcov. Ak napriek tomu k porušeniu súkromia dôjde, musí sa urýchlene napraviť v súlade s osobitnými postupmi stanovenými v zákone. V tejto súvislosti sa v zákone jednotlivcom, ktorí utrpeli škodu v dôsledku článku v tlači, priznáva viacero práv,

([41]) V tomto zmysle sa v článku 33 zákona o štatistike vyžaduje, aby verejné inštitúcie chránili informácie o respondentoch štatistických prieskumov, a to aj z hľadiska ochrany takýchto informácií pred použitím na akýkoľvek iný účel ako zostavovanie štatistík.
([42]) Článok 2 ods. 2 až 3, článok 30 ods. 2, články 33 a 34 zákona o štatistike.
([43]) Príručka k zákonu o ochrane osobných informácií, oddiel o článku 58.
([44]) V článku 4 tlačového zákona sa napríklad stanovuje, že články v tlači musia byť nestranné a objektívne, vo verejnom záujme, rešpektovať ľudskú dôstojnosť a hodnotu a nesmú sa v nich ohovárať iné osoby ani nesmú viesť k porušeniu ich práv, verejnej morálky či spoločenskej etiky.

ako napríklad právo na dosiahnutie zverejnenia opravy nepravdivého vyjadrenia, nápravu prostredníctvom vyjadrenia druhej strany alebo právo na ďalší článok (ak sa tento článok v tlači týka údajných trestných činov, v prípade ktorých je jednotlivec neskôr zbavený obvinenia) ([45]). Nároky jednotlivcov môžu médiá riešiť priamo (prostredníctvom ombudsmana) ([46]), prostredníctvom zmierovacieho či arbitrážneho konania (pred špecializovanou Komisiou pre mediálnu arbitráž) ([47]), prípadne pred súdmi. Jednotlivci môžu dosiahnuť aj náhradu škody, ak v dôsledku nezákonného konania tlače (úmyselného alebo z nedbanlivosti) utrpeli peňažnú škodu, bolo porušené ich právo na ochranu osobnosti alebo utrpeli citovú škodu ([48]). Podľa zákona tlač nenesie zodpovednosť v rozsahu, v akom článok v tlači, ktorý zasahuje do práv jednotlivca, nie je v rozpore so spoločenskými hodnotami, a je zverejnený buď so súhlasom dotknutého jednotlivca, alebo vo verejnom záujme (a existujú opodstatnené dôvody domnievať sa, že článok zodpovedá pravde) ([49]).

(32) Zatiaľ čo na spracúvanie osobných údajov tlačou na účely žurnalistických činností sa teda vzťahujú osobitné záruky vyplývajúce z tlačového zákona, neexistujú žiadne takéto dodatočné záruky, ktoré by sa vzťahovali na používanie výnimiek pri činnostiach spracúvania náboženskými organizáciami a politickými stranami porovnateľne s článkami 85, 89 a 91 nariadenia (EÚ) 2016/679. Komisia preto považuje za primerané vylúčiť z rozsahu uplatňovania tohto rozhodnutia náboženské organizácie v rozsahu, v akom spracúvajú osobné údaje na účely svojich misijných činností, a politické strany v rozsahu, v akom spracúvajú osobné údaje v súvislosti s menovaním kandidátov.

2.3. **Záruky, práva a povinnosti**

2.3.1. *Zákonnosť a spravodlivosť spracúvania*

(33) Osobné údaje by sa mali spracúvať zákonným a spravodlivým spôsobom.

(34) Táto zásada sa stanovuje v článku 3 ods. 1 a 2 zákona o ochrane osobných informácií a posilňuje sa v článku 59 zákona o ochrane osobných informácií, v ktorom sa zakazuje spracúvanie osobných údajov „podvodom, neprimeraným alebo nespravodlivým spôsobom“, „bez právneho povolenia“ alebo „nad rámec riadneho povolenia“ ([50]). Tieto všeobecné zásady zákonného spracúvania sú rozpracované v článkoch 15 až 19 zákona o ochrane osobných informácií, v ktorých sa stanovujú rôzne právne základy spracúvania (získavanie, používanie a poskytovanie tretím stranám), ako aj okolnosti, za ktorých môže dôjsť k zmene účelu (článok 18 zákona o ochrane osobných informácií).

([45]) Články 15 až 17 tlačového zákona.

([46]) Každé tlačové alebo iné médium musí mať vlastného ombudsmana na predchádzanie potenciálnym škodám spôsobeným tlačou a nápravu takýchto škôd (napr. vydávaním odporúčaní na opravu článkov v tlači, ktoré sú nepravdivé alebo poškodzujú dobré meno iných osôb), článok 6 tlačového zákona.

([47]) Komisia pozostáva zo 40 až 90 arbitrážnych komisárov menovaných ministrom kultúry, športu a cestovného ruchu spomedzi osôb s kvalifikáciou sudcu, advokáta, osôb s aspoň desaťročnou praxou v žurnalistike alebo spravodajstve, prípadne iných osôb s odbornými znalosťami v oblasti tlače. Arbitrážni komisári nemôžu byť zároveň verejnými činiteľmi, členmi politických strán ani novinármi. Podľa článku 8 tlačového zákona musia arbitrážni komisári vykonávať svoje povinnosti nezávisle a v súvislosti s plnením týchto povinností nesmú podliehať žiadnym usmerneniam ani pokynom. Okrem toho sú zavedené osobitné pravidlá na predchádzanie konfliktom záujmov, napríklad vylúčenie konkrétnych komisárov z riešenia prípadov, keď je stranou prípadu ich manželský partner alebo príbuzní (článok 10 tlačového zákona). Komisia môže riešiť spory prostredníctvom zmierovacieho alebo arbitrážneho konania, ale môže vypracúvať aj odporúčania na nápravu porušení (oddiel 5 tlačového zákona).

([48]) Článok 30 tlačového zákona.

([49]) Článok 5 tlačového zákona.

([50]) V článku 59 zákona o ochrane osobných informácií sa zakazuje každej osobe, „ktorá spracúva alebo niekedy spracúvala osobné informácie“, „získavať osobné informácie alebo súhlas so spracúvaním osobných informácií podvodom, neprimeraným alebo nespravodlivým spôsobom“, „bez povolenia odhaľovať osobné informácie získané v priebehu podnikania alebo ich poskytnúť na použitie akejkoľvek tretej strane“ alebo „poškodiť, zničiť, pozmeniť, sfalšovať alebo odhaliť osobné informácie iných osôb bez právneho povolenia alebo nad rámec riadneho povolenia“. Porušenie tohto zákona môže viesť k trestnoprávnym sankciám, pozri článok 71 ods. 5 a 6 a článok 72 ods. 2 zákona o ochrane osobných informácií. V článku 70 ods. 2 zákona o ochrane osobných informácií sa umožňuje uloženie trestnoprávnej sankcie za podvodné alebo inak nespravodlivé metódy získania osobných informácií spracúvaných tretími stranami alebo za ich poskytnutie tretej strane na účely tvorby zisku alebo na nespravodlivé účely, ako aj za navádzanie na takéto správanie alebo umožňovanie takého správania.

(35) Podľa článku 15 ods. 1 zákona o ochrane osobných informácií môže prevádzkovateľ získavať osobné údaje (v rozsahu účelu ich získavania) len v zriedkavých prípadoch podložených právnymi dôvodmi. Sú nimi 1. súhlas dotknutej osoby ([51]) (pododsek 1); 2. potreba realizovať a plniť zmluvu s dotknutou osobou (pododsek 4); 3. osobitné zákonné povolenie alebo potreba plnenia zákonnej povinnosti (pododsek 2); potreba ([52]) verejnej inštitúcie vykonávať v rámci svojej právomoci úlohy stanovené zákonom; 4. preukázať potrebu ochrany života, fyzickej integrity alebo majetkových záujmov dotknutej osoby alebo tretej strany pred bezprostredným nebezpečenstvom (iba ak dotknutá osoba nemôže vyjadriť svoj zámer alebo nemožno vopred získať jej súhlas) (pododsek 5); 5. potreba dosiahnuť „odôvodnený záujem" prevádzkovateľa, ak je „preukázateľne nadradený" záujmom dotknutej osoby (a iba vtedy, ak spracúvanie „podstatne súvisí" s oprávneným záujmom a nevykonáva sa nad rámec toho, čo je primerané) (pododsek 6) ([53]). Tieto dôvody spracúvania v zásade zodpovedajú dôvodom stanoveným v článku 6 nariadenia (EÚ) 2016/679, a to vrátane dôvodu „odôvodneného záujmu", ktorý sa rovná dôvodu „oprávneného záujmu" uvedeného v článku 6 ods. 1 písm. f) nariadenia (EÚ) 2016/679.

(36) Po získaní možno osobné údaje používať v rozsahu účelu ich získania (článok 15 ods. 1 zákona o ochrane osobných informácií) alebo „v rozsahu, ktorý primerane súvisí" s účelom ich získania, pričom sa prihliadne na možné nevýhody spôsobené dotknutej osobe, a za predpokladu, že sa prijali potrebné bezpečnostné opatrenia (napr. šifrovanie) (článok 15 ods. 3 zákona o ochrane osobných informácií). Na určenie toho, či účel používania „primerane súvisí" s pôvodným účelom získania informácií, sa vo vykonávacom dekréte stanovujú osobitné kritériá, ktoré sú podobné kritériám uvedeným v článku 6 ods. 4 nariadenia (EÚ) 2016/679. Konkrétne musí existovať významná súvislosť s pôvodným účelom; dodatočné používanie musí byť predvídateľné (napríklad vzhľadom na okolnosti, za ktorých sa informácie získali); a ak je to možné, údaje musia byť pseudonymizované ([54]). Osobitné kritériá použité prevádzkovateľom pri tomto posúdení musia byť zverejnené vopred v politike ochrany súkromia ([55]). Okrem toho je osobitnou povinnosťou zodpovednej osoby pre ochranu súkromia (pozri odôvodnenie (94)) preskúmať, či sa ďalšie používanie vykonáva v rámci uvedených parametrov.

([51]) Súhlas musí byť dobrovoľný, informovaný, osobitný a vyjadrený jedným zo spôsobov stanovených v zákone. V žiadnom prípade nemožno získať súhlas podvodom ani neprimeraným či nespravodlivým spôsobom (článok 59 ods. 1 zákona o ochrane osobných informácií) Po prvé podľa článku 4 pododseku 2 zákona o ochrane osobných informácií majú dotknuté osoby právo „udeliť alebo neudeliť súhlas" a „zvoliť si rozsah súhlasu", pričom by o tomto práve mali byť informované (článok 15 ods. 2, článok 16 ods. 2 a 3, článok 17 ods. 2 a článok 18 ods. 3 zákona o ochrane osobných informácií). Článok 22 ods. 5 zákona o ochrane osobných informácií obsahuje ďalšiu záruku, keďže sa prevádzkovateľovi zakazuje odmietnutie poskytnutia tovaru alebo služieb, ak by to mohlo ohroziť slobodnú voľbu jednotlivca v oblasti udelenia súhlasu. Týka sa to situácií, v ktorých si vyžadujú súhlas len niektoré druhy spracúvania (zatiaľ čo ostatné vychádzajú zo zmluvy), ako aj ďalšieho spracúvania osobných údajov získaných v súvislosti s poskytovaním tovaru alebo služieb. Po druhé podľa článku 15 ods. 2, článku 17 ods. 2 a 3 a článku 18 ods. 3 zákona o ochrane osobných informácií musí prevádzkovateľ v prípade vyžiadania súhlasu informovať dotknutú osobu o „náležitostiach" predmetných osobných údajov [napr. že ide o citlivé údaje, pozri článok 17 ods. 2 pododsek 2 písm. a) vykonávacieho dekrétu k zákonu o ochrane osobných informácií], účele spracúvania, období uchovávania a o všetkých príjemcoch údajov. Každá takáto žiadosť sa uskutoční „výslovne rozpoznateľným spôsobom", v ktorom sa rozlišuje medzi žiadosťou o súhlas a ostatnými záležitosťami (článok 22 ods. 1 až 4 zákona o ochrane osobných informácií). Po tretie v článku 17 ods. 1 pododsekoch 1 až 6 vykonávacieho dekrétu k zákonu o ochrane osobných informácií sa stanovujú osobitné metódy, ktorými prevádzkovateľ získava súhlas, ako je písomný súhlas s podpisom dotknutej osoby alebo súhlas vyjadrený e-mailom (odpovedaním na e-mail). Zatiaľ čo sa v zákone o ochrane osobných informácií jednotlivcom osobitne neposkytuje všeobecné právo odvolať súhlas, jednotlivci majú namiesto toho právo dosiahnuť pozastavenie spracúvania údajov, ktoré sa ich týkajú, čo v prípade jeho uplatnenia povedie k ukončeniu spracúvania a vymazaniu údajov (pozri odôvodnenie 78 o práve na pozastavenie spracúvania).

([52]) Podľa informácií prijatých od Komisie pre ochranu osobných informácií sa môžu verejné inštitúcie opierať o tento dôvod iba vtedy, ak je spracúvanie osobných informácií nevyhnutné, t. j. inštitúcia bez spracúvania údajov nemôže vykonávať svoje funkcie alebo ich môže vykonávať len s neprimeranými ťažkosťami.

([53]) V článku 39-3 zákona o ochrane osobných informácií sa ukladajú poskytovateľom informačných a komunikačných služieb osobitné (prísnejšie) povinnosti v oblasti získavania a používania osobných informácií ich používateľov. Konkrétne sa vyžaduje, aby poskytovateľ získal súhlas používateľa až po tom, ako mu poskytne informácie o účele získavania/používania informácií, kategóriách osobných informácií, ktoré sa majú získať, a období, počas ktorého sa budú informácie spracúvať (článok 39-3 ods. 1 zákona o ochrane osobných informácií). To isté platí v prípade zmeny ktoréhokoľvek z týchto aspektov. Na nezískanie súhlasu so získavaním informácií sa vzťahujú trestnoprávne sankcie (článok 71 ods. 4 až 5 zákona o ochrane osobných informácií). Výnimočne môžu poskytovatelia informačných a komunikačných služieb získavať alebo používať osobné informácie používateľov bez získania ich predchádzajúceho súhlasu. Platí to vtedy, ak 1. je z ekonomických alebo technologických príčin jednoznačne náročné získať bežný súhlas so spracúvaním osobných informácií, ktorý sa vyžaduje na plnenie zmluvy o poskytovaní informačných a komunikačných služieb (napr. ak sa v procese plnenia zmluvy osobné údaje nevyhnutne vytvoria, čo je prípad fakturačných informácií, prístupových logov a záznamov o platbách); 2. sú potrebné na úhradu poplatkov za poskytovanie informačných a komunikačných služieb; alebo 3. sa to povoľuje v iných zákonoch (napríklad v článku 21 ods. 1 pododseku 6 zákona o ochrane spotrebiteľa v elektronickom obchode sa stanovuje, že podnikateľské subjekty môžu získavať osobné informácie o právnych zástupcoch neplnoletých osôb s cieľom potvrdiť získanie platného súhlasu v mene neplnoletých osôb) (článok 39-3 ods. 2 zákona o ochrane osobných informácií). V každom prípade platí, že poskytovatelia informačných a komunikačných služieb nesmú odmietnuť poskytnutie služieb len preto, lebo používateľ neposkytol ďalšie osobné informácie okrem minimálne požadovaných informácií (t. j. informácii, ktoré sú potrebné na realizáciu základných prvkov dotknutej služby), pozri článok 39-3 ods. 3 zákona o ochrane osobných informácií.

([54]) Pozri článok 14-2 vykonávacieho dekrétu k zákonu o ochrane osobných informácií.

([55]) Článok 14-2 ods. 2 vykonávacieho dekrétu k zákonu o ochrane osobných informácií.

(37) Podobné (ale do určitej miery prísnejšie) pravidlá sa uplatňujú na poskytovanie údajov tretej strane. Podľa článku 17 ods. 1 zákona o ochrane osobných informácií je poskytnutie osobných údajov tretej strane povolené na základe súhlasu ([56]) alebo v rámci účelu získania informácií, ak sa informácie získali na základe niektorého právneho dôvodu uvedeného v článku 15 ods. 1 pododsekoch 2, 3 a 5 zákona o ochrane osobných informácií. Vylúčené je najmä akéhokoľvek sprístupnenie vychádzajúce z „odôvodneného záujmu" prevádzkovateľa. Okrem toho sa v článku 17 ods. 4 zákona o ochrane osobných informácií umožňuje poskytnutie informácií tretej strane „v rozsahu, ktorý primerane súvisí" s účelom ich získania, pričom sa opäť prihliadne na možné nevýhody spôsobené dotknutej osobe, a za predpokladu, že sa prijali potrebné bezpečnostné opatrenia (napr. šifrovanie). Na tie isté faktory, aké sú uvedené v odôvodnení (36), sa musí prihliadnuť pri posudzovaní toho, či je poskytnutie v rozsahu, ktorý primerane súvisí s účelom získania informácií, a či sa uplatňujú tie isté záruky (t. j. v súvislosti s transparentnosťou prostredníctvom politiky ochrany súkromia a zapojenia zodpovednej osoby pre ochranu súkromia).

(38) Prijatie osobných údajov z Únie kórejským prevádzkovateľom údajov sa v zmysle článku 15 zákona o ochrane osobných informácií považuje za „získanie". V oznámení č. 2021-5 (oddiel I prílohy I k tomuto rozhodnutiu) sa objasňuje, že účel, na ktorý dotknutý subjekt z EÚ prenáša údaje, predstavuje v prípade kórejského prevádzkovateľa údajov účel získania údajov. V dôsledku toho sa od kórejských prevádzkovateľov údajov, ktorí prijímajú osobné údaje z Únie, v zásade vyžaduje spracúvanie týchto informácií v rozsahu účelu prenosu v súlade s článkom 17 zákona o ochrane osobných informácií.

(39) Osobitné obmedzenia sa uplatňujú na situáciu, ak sa prevádzkovateľ usiluje použiť osobné údaje alebo ich poskytnúť tretej strane na iný účel ako účel ich získania ([57]). Podľa článku 18 ods. 2 zákona o ochrane osobných informácií môže súkromný prevádzkovateľ výnimočne ([58]) použiť osobné údaje alebo ich poskytnúť tretej strane na iný účel: 1. po získaní dodatočného (čiže samostatného) súhlasu dotknutej osoby; 2. ak sa to umožňuje na základe osobitných ustanovení právnych predpisov; alebo 3. ak je to preukázateľne potrebné na ochranu života, fyzickej integrity alebo majetkových záujmov dotknutej osoby alebo tretej strany pred bezprostredným nebezpečenstvom (iba ak dotknutá osoba nemôže vyjadriť svoj zámer a nemožno vopred získať jej súhlas) ([59]).

(40) Verejné inštitúcie môžu takisto v určitých situáciách osobné údaje používať alebo poskytovať tretej strane na iný účel. Platí to v prípadoch, keď by inak verejné inštitúcie nemohli plniť svoje zákonné povinnosti, pričom sa vyžaduje povolenie Komisie pre ochranu osobných informácií. Okrem toho môžu verejné inštitúcie poskytnúť osobné údaje inému orgánu alebo súdu, ak je to potrebné na vyšetrovanie a stíhanie trestných činov alebo vznesenie obžaloby; aby mohol súd plniť svoje funkcie v súvislosti s prebiehajúcim súdnym konaním; alebo na výkon trestnoprávnej sankcie, prípadne vydanie rozhodnutia o zverení do starostlivosti ([60]). Takisto môžu poskytnúť osobné údaje zahraničnej vláde alebo medzinárodnej organizácii na účely splnenia zákonnej povinnosti vyplývajúcej zo zmluvy alebo medzinárodného dohovoru, pričom v takom prípade musia splniť aj požiadavky na cezhraničných prenos údajov (pozri odôvodnenie (90)).

(41) Zásady zákonnosti a spravodlivosti spracúvania sú teda začlenené do kórejského právneho rámca spôsobom v zásade zodpovedajúcim nariadeniu (EÚ) 2016/679, keďže spracúvanie sa umožňuje iba z odôvodnených a jednoznačne vymedzených príčin. Ďalej sa vo všetkých uvedených prípadoch spracúvanie umožňuje iba vtedy, ak nie je pravdepodobné, že sa ním „nespravodlivo poškodia" záujmy dotknutej osoby alebo tretej strany, čo si vyžaduje vyváženie záujmov. Okrem toho sa v článku 18 ods. 5 zákona o ochrane osobných informácií stanovujú dodatočné záruky pri poskytovaní osobných údajov prevádzkovateľom tretej strane, ku ktorým môže patriť požiadavka na obmedzenie účelu a metódy použitia alebo zavedenie osobitných bezpečnostných opatrení. Od tretej strany sa vyžaduje vykonanie požadovaných opatrení.

([56]) Porušenia článku 17 ods. 1 pododseku 1 zákona o ochrane osobných informácií môžu viesť k uloženiu trestnoprávnych sankcií (článok 71 ods. 1 zákona o ochrane osobných informácií).

([57]) „Zamýšľaný účel" je účel, na ktorý sa získali informácie. Ak sa napríklad informácie získavajú na základe súhlasu dotknutého jednotlivca, zamýšľaným účelom je účel oznámený jednotlivcovi podľa článku 15 ods. 2 zákona o ochrane osobných informácií.

([58]) Pozri článok 18 ods. 1 zákona o ochrane osobných informácií. Porušenia článku 18 ods. 1 a 2 môžu viesť k uloženiu trestnoprávnych sankcií (článok 71 ods. 2 zákona o ochrane osobných informácií).

([59]) Poskytovatelia informačných a komunikačných služieb môžu osobné informácie použiť alebo poskytnúť tretej strane na iný ako pôvodný účel iba na základe dôvodov stanovených v článku 18 ods. 2 pododsekoch 1 a 2 zákona o ochrane osobných informácií (t. j. keď sa získa dodatočný súhlas alebo v zákone existujú osobitné ustanovenia). Pozri článok 18 ods. 2 zákona o ochrane osobných informácií.

([60]) Okrem situácie, keď je spracúvanie potrebné na vyšetrovanie trestných činov, vznesenie obžaloby a trestné stíhanie, musia verejné inštitúcie, ktoré používajú osobné informácie alebo ich poskytujú tretej strane na iný účel ako účel získania (napríklad, keď je to osobitne povolené zákonom alebo potrebné na plnenie zmluvy), zverejniť právne dôvody spracúvania, jeho účel a rozsah na svojom webovom sídle alebo v Úradnom vestníku a uchovávať záznamy o týchto skutočnostiach (článok 18 ods. 4 zákona o ochrane osobných informácií v spojení s článkom 15 vykonávacieho dekrétu k zákonu o ochrane osobných informácií).

(42) A napokon sa v článku 28-2 zákona o ochrane osobných informácií na základe osobitných záruk umožňuje (ďalšie) spracúvanie pseudonymizovaných informácií bez súhlasu dotknutého jednotlivca na účely štatistiky, vedeckého výskumu ([61]) a archivovania vo verejnom záujme. Podobne ako v nariadení (EÚ) 2016/679 ([62]) sa teda aj v zákone o ochrane osobných informácií uľahčuje (ďalšie) spracúvanie osobných údajov na takéto účely v rámci zabezpečovania primeraných záruk na ochranu práv jednotlivcov. Namiesto použitia pseudonymizácie ako možnej záruky sa v zákone o ochrane osobných informácií pseudonymizácia ukladá ako predpoklad vykonávania určitých činností spracúvania na účely štatistiky, vedeckého výskumu a archivovania vo verejnom záujme (aby bolo napríklad možné spracúvať údaje bez súhlasu alebo ich kombinovať s inými súbormi údajov).

(43) Okrem toho sa v zákone o ochrane osobných informácií ukladá viacero osobitných záruk, najmä pokiaľ ide o požadované technické a organizačné opatrenia, uchovávanie záznamov, obmedzenie spoločného využívania údajov a riešenie možných rizík opätovnej identifikácie. Kombináciou rôznych záruk uvedených v odôvodneniach (44) – (48) sa zabezpečuje, aby ochrana vzťahujúca sa na spracúvanie osobných údajov v tejto súvislosti v zásade zodpovedala ochrane, aká sa vyžaduje podľa nariadenia (EÚ) 2016/679.

(44) Po prvé, čo je najdôležitejšie, v článku 28-5 ods. 1 zákona o ochrane osobných informácií sa zakazuje spracúvanie pseudonymizovaných informácií na účel identifikovania konkrétneho jednotlivca. Ak sa napriek tomu pri spracúvaní pseudonymizovaných informácií vytvoria informácie, na základe ktorých možno jednotlivca identifikovať, prevádzkovateľ musí ihneď spracúvanie pozastaviť a takéto informácie zničiť (článok 28-5 ods. 2 zákona o ochrane osobných informácií). Na nedodržanie týchto ustanovení sa vzťahujú správne pokuty a toto nedodržanie predstavuje trestný čin ([63]). Znamená to, že aj v situáciách, keď by bolo *prakticky* možné jednotlivca opätovne identifikovať, je takáto opätovná identifikácia zo *zákona* zakázaná.

(45) Po druhé musí prevádzkovateľ pri (ďalšom) spracúvaní pseudonymizovaných informácií na tieto účely zaviesť osobitné technologické, riadiace a fyzické opatrenia na zaistenie bezpečnosti informácií (vrátane osobitného uloženia a riadenia informácií potrebných na obnovu pseudonymizovaných informácií do pôvodného stavu) ([64]). Okrem toho je potrebné uchovávať záznamy o spracúvaných pseudonymizovaných informáciách, účele ich spracúvania, histórii používania a všetkých tretích stranách, ktoré informácie prijímajú (článok 29-5 ods. 2 vykonávacieho dekrétu k zákonu o ochrane osobných informácií).

(46) A napokon po tretie sa v zákone o ochrane osobných informácií stanovujú osobitné záruky na predchádzanie identifikácii jednotlivcov tretími stranami v prípade spoločného využívania informácií. Konkrétne prevádzkovatelia nesmú do pseudonymizovaných informácií poskytovaných tretej strane na účel štatistiky, vedeckého výskumu a archivovania vo verejnom záujme zahrnúť informácie, ktoré by bolo možné použiť na identifikovanie konkrétneho jednotlivca (článok 28-2 ods. 2 zákona o ochrane osobných informácií) ([65]).

(47) Konkrétnejšie platí, že hoci sa v zákone o ochrane osobných informácií umožňuje kombinovať pseudonymizované informácie (spracúvané rôznymi prevádzkovateľmi) na účel štatistiky, vedeckého výskumu a archivovania vo verejnom záujme, táto právomoc sa v ňom vyhradzuje špecializovaným inštitúciám vybaveným osobitnými bezpečnostnými zariadeniami (článok 28-3 ods. 1 zákona o ochrane osobných informácií) ([66]). K žiadosti o skombinovanie pseudonymizovaných údajov musí prevádzkovateľ priložiť dokumentáciu, v ktorej sa okrem iného

([61]) Vedecký výskum sa vymedzuje v článku 2 ods. 8 zákona o ochrane osobných informácií ako „výskum, pri ktorom sa uplatňujú vedecké metódy, ako napríklad vývoj a predvádzanie technológie, základný výskum, aplikovaný výskum a súkromný výskum“. Tieto kategórie zodpovedajú kategóriám stanoveným v odôvodnení 159 nariadenia (EÚ) 2016/679.

([62]) Pozri článok 5 ods. 1 písm. b) a článok 89 ods. 1 až 2 a odôvodnenia 50 a 157 nariadenia (EÚ) 2016/679.

([63]) Pozri článok 28-6 ods. 1, článok 71 ods. 4-3 a článok 75 ods. 2 pododsek 4-4 zákona o ochrane osobných informácií.

([64]) Článok 28-4 zákona o ochrane osobných informácií a článok 29-5 vykonávacieho dekrétu k zákonu o ochrane osobných informácií. Na nedodržanie tejto povinnosti sa vzťahujú správne a trestnoprávne sankcie, pozri článok 73 ods. 1 a článok 75 ods. 2 pododsek 6 zákona o ochrane osobných informácií.

([65]) Porušenia týchto požiadaviek môžu viesť k uloženiu trestnoprávnych sankcií (článok 71 ods. 2 zákona o ochrane osobných informácií). Komisia pre ochranu osobných informácií začala tieto nové pravidlá bezodkladne presadzovať, napr. v rozhodnutí z 28. apríla 2021, v ktorom uložila pokutu a nápravné opatrenia spoločnosti, ktorá okrem iných porušení zákona o ochrane osobných informácií nesplnila požiadavku článku 28-2 ods. 2 zákona o ochrane osobných informácií, pozri stránku: https://www.pipc.go.kr/np/cop/bbs/selectBoardArticle.do?bbsId=BS074&mCode=C020010000&nttId=7298&fbclid=IwAR3SKcMQi6G5pR9k4I7j6GNXtc8aBVDOwcUReVvvzQtYI7AS40UKYXoOXo8.

([66]) Na získanie štatútu špecializovanej inštitúcie („odbornej agentúry pre kombinovanie údajov“) je potrebné podať žiadosť Komisii pre ochranu osobných informácií spolu so sprievodnými dokumentmi, v ktorých sa podrobne uvádzajú okrem iného zariadenia a vybavenie zavedené na bezpečné kombinovanie pseudonymizovaných údajov a potvrdzuje, že žiadateľ zamestnáva aspoň troch zamestnancov na plný pracovný úväzok s kvalifikáciou alebo praxou v oblasti ochrany osobných údajov (článok 29-2 ods. 1 až 2 vykonávacieho dekrétu k zákonu o ochrane osobných informácií). Podrobné požiadavky, napríklad na kvalifikáciu zamestnancov, dostupné zariadenia, bezpečnostné opatrenia, vnútorné politiky a postupy, ako aj finančné požiadavky, sa stanovujú v oznámení Komisie pre ochranu osobných informácií č. 2020-9 s názvom Kombinovanie a sprístupňovanie pseudonymizovaných informácií (plán I). Štatút odbornej agentúry pre kombinovanie údajov môže Komisia pre ochranu osobných informácií (po uskutočnení vypočutia) z určitých dôvodov odobrať, napríklad ak už agentúra nespĺňa bezpečnostné normy požadované na získanie štatútu alebo ak sa v súvislosti s kombinovaním údajov vyskytlo porušenie ochrany údajov (článok 29-2 ods. 5 a 6 vykonávacieho dekrétu k zákonu o ochrane osobných informácií). Komisia pre ochranu osobných informácií musí každý štatút odbornej agentúry pre kombinovanie údajov (alebo jeho odobratie) zverejniť (článok 29-2 ods. 7 vykonávacieho dekrétu k zákonu o ochrane osobných informácií).

uvádzajú údaje, ktoré sa majú kombinovať, účel kombinovania, ako aj navrhované bezpečnostné opatrenia pri spracúvaní kombinovaných údajov ([67]). Na povolenie kombinovania musí prevádzkovateľ zaslať údaje, ktoré sa majú kombinovať, špecializovanej inštitúcii a poskytnúť „kombinačný kľúč“ (t. j. informácie, ktoré sa použijú na pseudonymizáciu) Kórejskej agentúre pre internet a bezpečnosť ([68]). Na základe tohto kľúča sa vytvoria „údaje prepojenia kombinačných kľúčov“ (ktoré umožnia prepojenie kombinačných kľúčov z rôznych aplikácií na skombinovanie súborov údajov), ktoré sa poskytnú špecializovanej inštitúcii ([69]).

(48) Prevádzkovateľ žiadajúci o kombinovanie môže analyzovať skombinované informácie v priestoroch špecializovanej inštitúcie v mieste, v ktorom sa uplatňujú osobitné technické, fyzické a správne bezpečnostné opatrenia (článok 29-3 vykonávacieho dekrétu k zákonu o ochrane osobných informácií). Prevádzkovatelia, ktorí poskytli súbor údajov na takéto kombinovanie, môžu skombinované údaje preniesť mimo špecializovanú inštitúciu až po ďalšej pseudonymizácii alebo anonymizácii skombinovaných údajov a so súhlasom uvedenej inštitúcie (článok 28-3 ods. 2 zákona o ochrane osobných informácií) ([70]). Pri zvažovaní toho, či takéto povolenie poskytnúť, inštitúcia posúdi súvislosť medzi skombinovanými údajmi a účelom spracúvania, ako aj to, či bol vypracovaný osobitný bezpečnostný plán na používanie takýchto údajov ([71]). Exportovanie skombinovaných informácií mimo inštitúciu sa nepovolí, ak informácie obsahujú údaje, ktoré by umožnili identifikovanie jednotlivca ([72]). A napokon na kombinovanie a sprístupňovanie pseudonymizovaných údajov špecializovanou inštitúciou dohliada Komisia pre ochranu osobných informácií (článok 29-4 ods. 3 vykonávacieho dekrétu k zákonu o ochrane osobných informácií).

2.3.2. *Spracúvanie osobitných kategórií osobných údajov*

(49) Na spracúvanie „osobitných kategórií“ údajov by sa mali vzťahovať osobitné záruky.

(50) Zákon o ochrane osobných informácií obsahuje osobitné pravidlá týkajúce sa spracúvania citlivých údajov ([73]), ktoré sa vymedzujú ako osobné údaje odhaľujúce informácie o ideológii, viere, prijatí do odborov alebo politickej strany alebo vystúpení z nich, politických názoroch, zdraví a sexuálnom živote jednotlivca, ako aj ďalšie osobné informácie, ktoré pravdepodobne „značne“ ohrozujú súkromie dotknutej osoby a boli v prezidentskom dekréte uvedené ako citlivé informácie ([74]). Podľa objasnení, ktoré poskytla Komisia pre ochranu osobných informácií, sa pojem sexuálny život vzťahuje aj na sexuálnu orientáciu alebo sexuálne preferencie jednotlivca ([75]). Okrem toho sa v článku 18 vykonávacieho dekrétu do rozsahu citlivých údajov dopĺňajú ďalšie kategórie, konkrétne informácie o DNA získané na základe genetického testovania a údaje tvoriace záznamy v registri trestov. Nedávnou zmenou vykonávacieho dekrétu k zákonu o ochrane osobných informácií sa pojem citlivé informácie ešte viac rozšíril, a to o osobné údaje odhaľujúce rasový alebo etnický pôvod a biometrické informácie ([76]). Po tejto zmene pojem citlivé informácie podľa zákona o ochrane osobných informácií v zásade zodpovedá článku 9 nariadenia (EÚ) 2016/679.

(51) Podľa článku 23 ods. 1 zákona o ochrane osobných informácií a podobne podľa ustanovenia článku 9 ods. 1 nariadenia (EÚ) 2016/679 sa spracúvanie citlivých údajov vo všeobecnosti zakazuje, ak sa neuplatňuje niektorá z uvedených výnimiek ([77]). Nimi sa spracúvanie obmedzuje na prípady, keď prevádzkovateľ informuje dotknutú osobu v súlade s článkami 15 a 17 zákona o ochrane osobných informácií a získa jej osobitný súhlas (t. j. iný ako súhlas so spracúvaním iných osobných údajov) alebo keď sa spracúvanie vyžaduje alebo povoľuje v právnom predpise. Orgány verejnej moci môžu takisto spracúvať biometrické informácie, informácie o DNA získané na

([67]) Článok 8 ods. 1 až 2 oznámenia č. 2020-9 s názvom Kombinovanie a sprístupňovanie pseudonymizovaných informácií.
([68]) Článok 2 ods. 3 a 6 a článok 9 ods. 1 oznámenia č. 2020-9 s názvom Kombinovanie a sprístupňovanie pseudonymizovaných informácií.
([69]) Článok 2 ods. 4 a článok 9 ods. 2 až 3 oznámenia č. 2020-9 s názvom Kombinovanie a sprístupňovanie pseudonymizovaných informácií. Špecializovaná inštitúcia musí ihneď po skombinovaní údajov zničiť údaje prepojenia kombinačných kľúčov (článok 9 ods. 4 oznámenia).
([70]) Porušenia požiadaviek na kombinovanie súborov údajov môžu viesť k uloženiu trestnoprávnych sankcií (článok 71 ods. 4-2 zákona o ochrane osobných informácií). Pozri aj článok 29-2 ods. 4 vykonávacieho dekrétu k zákonu o ochrane súkromia komunikácie.
([71]) Postup schválenia sprístupnenia skombinovaných údajov sa stanovuje v článku 11 oznámenia č. 2020-9 s názvom Kombinovanie a sprístupňovanie pseudonymizovaných informácií. Konkrétne musí špecializovaná inštitúcia zriadiť „výbor na preskúmanie sprístupnenia informácií“, ktorý bude pozostávať z členov s hlbokými znalosťami a skúsenosťami v oblasti ochrany údajov.
([72]) Článok 29-2 ods. 4 vykonávacieho dekrétu k zákonu o ochrane osobných informácií a článok 11 oznámenia č. 2020-9.
([73]) Potrebu zaviesť osobitnú ochranu spracúvania citlivých údajov, ako sú údaje o zdraví alebo sexuálnom správaní, uznal aj Ústavný súd Kórejskej republiky, pozri rozhodnutie ústavného súdu č. HunMa 1139 z 31. mája 2007.
([74]) Článok 23 ods. 1 zákona o ochrane osobných informácií.
([75]) Pozri aj príručku k zákonu o ochrane osobných informácií, kapitolu III oddiel 2 o článku 23 (s. 157 – 164).
([76]) Teda osobné informácie vyplývajúce z osobitného technického spracúvania údajov týkajúcich sa fyzických, fyziologických alebo behaviorálnych vlastností jednotlivca na účely jedinečnej identifikácie uvedeného jednotlivca.
([77]) Nedodržanie týchto požiadaviek môže viesť k sankciám podľa článku 71 pododseku 3 zákona o ochrane osobných informácií.

základe genetického testovania, osobné informácie odhaľujúce rasový alebo etnický pôvod a údaje tvoriace záznamy v registri trestov z dôvodov, ktoré sa vzťahujú výlučne na ne (napríklad ak je to potrebné na vyšetrovanie trestnej činnosti, alebo aby mohol súd pokračovať v konaní vo veci) ([78]). Ako také sú právne základy dostupné pre spracúvanie citlivých údajov obmedzenejšie ako v prípade iných druhov osobných údajov a v kórejskom práve sú ešte prísnejšie ako podľa článku 9 ods. 2 nariadenia (EÚ) 2016/679.

(52) Okrem toho sa v článku 23 ods. 2 zákona o ochrane osobných informácií, ktorého nedodržanie môže viesť k sankciám ([79]), osobitne zdôrazňuje zaistenie primeranej bezpečnosti pri narábaní s citlivými údajmi, aby sa „nemohli stratiť, odcudziť, odhaliť, sfalšovať, pozmeniť alebo poškodiť“. Toto je všeobecná požiadavka vyplývajúca z článku 29 zákona o ochrane osobných informácií, pričom v článku 3 ods. 4 sa objasňuje, že úroveň bezpečnosti musí zodpovedať druhu osobných údajov, ktoré sa spracúvajú, čo znamená, že je potrebné prihliadnuť na osobitné riziká v oblasti spracúvania citlivých údajov. Okrem toho sa má spracúvanie údajov vždy vykonávať „tak, aby sa minimalizovala možnosť porušenia“ súkromia dotknutej osoby, a ak je to možné, aj „anonymne“ (článok 3 ods. 6 a 7 zákona o ochrane osobných informácií). Tieto požiadavky sú osobitne relevantné vtedy, ak sa spracúvanie týka citlivých údajov.

2.3.3. *Obmedzenie účelu*

(53) Osobné údaje by sa mali získavať na konkrétny účel a spôsobom, ktorý nie je nezlučiteľný s účelom spracúvania.

(54) Táto zásada sa zabezpečuje článkom 3 ods. 1 a 2 zákona o ochrane osobných informácií, podľa ktorého prevádzkovateľ „stanoví a výslovne uvedie“ účel spracúvania, spracúva osobné údaje primeraným spôsobom na dosiahnutie tohto účelu a nepoužije ich nad rámec tohto účelu. Všeobecná zásada obmedzenia účelu sa potvrdzuje v článku 15 ods. 1, článku 18 ods. 1, článku 19 a v prípade sprostredkovateľov (takzvaných poskytovateľov externých činností) v článku 26 ods. 1 pododseku 1, článku 26 ods. 5 a 7 zákona o ochrane osobných informácií. Konkrétne platí, že osobné údaje sa môžu v zásade používať a poskytovať tretím stranám len v rozsahu účelu, na ktorý sa získali (článok 15 ods. 1 a článok 17 ods. 1 pododsek 2). spracúvanie na zlučiteľný účel, t. j. „v rozsahu, ktorý primerane súvisí s pôvodným účelom získania informácií“, možno uskutočniť iba vtedy, ak nemá negatívny vplyv na príslušné dotknuté osoby a ak sú prijaté potrebné bezpečnostné opatrenia (napríklad šifrovanie) (článok 15 ods. 3 a článok 17 ods. 4 zákona o ochrane osobných informácií). Na určenie toho, či ide o ďalšie spracúvanie na zlučiteľný účel, sa vo vykonávacom dekréte k zákonu o ochrane osobných informácií uvádzajú osobitné kritériá podobné tým, ktoré sú uvedené v článku 6 ods. 4 nariadenia (EÚ) 2016/679, pozri odôvodnenie (36).

(55) Ako sa vysvetľuje v odôvodnení (38), účelom získavania informácií v prípade kórejských prevádzkovateľov prijímajúcich osobné údaje z Únie je účel, na ktorý sa údaje prenášajú. Zmena účelu prevádzkovateľom je povolená len výnimočne, a to v osobitných (uvedených) prípadoch (článok 18 ods. 2 pododseky 1 až 3 zákona o ochrane osobných informácií, pozri aj odôvodnenie (39)). V rozsahu, v akom je zmena účelu povolená zákonom, sa v takýchto zákonoch zase musí dodržiavať základné právo na súkromie a ochranu údajov, ako aj zásady nevyhnutnosti a primeranosti stanovené v kórejskej ústave. Okrem toho sa v článku 18 ods. 2 a 5 zákona o ochrane osobných informácií uvádzajú dodatočné záruky, konkrétne požiadavka, že takáto zmena účelu nesmie „nespravodlivo poškodzovať záujem dotknutej osoby“, čiže sa za každých okolností vyžaduje vyváženie záujmov. Tým sa zabezpečuje úroveň ochrany, ktorá v zásade zodpovedá úrovni ochrany podľa článku 5 ods. 1 písm. b) a článku 6 v spojení s odôvodnením 50 nariadenia (EÚ) 2016/679.

2.3.4. *Presnosť a minimalizácia údajov*

(56) Osobné údaje by mali byť presné a v prípade potreby by sa mali neustále aktualizovať. Zároveň by mali byť primerané, relevantné a obmedzené na to, čo je potrebné vo vzťahu k účelom, na ktoré sa spracúvajú.

([78]) V článku 18 vykonávacieho dekrétu k zákonu o ochrane osobných informácií sa stanovuje, že na kategórie v ňom uvedených údajov sa nevzťahuje uplatňovanie článku 23 ods. 1 zákona pri spracúvaní vykonávanom verejnou inštitúciou podľa článku 18 ods. 2 pododsekov 5 až 9 zákona o ochrane osobných informácií.

([79]) Pozri článok 73 pododsek 1 a článok 75 ods. 2 pododsek 6 zákona o ochrane osobných informácií.

(57) Zásada presnosti sa podobne uznáva v článku 3 ods. 3 zákona o ochrane osobných informácií, v ktorom sa vyžaduje, aby boli osobné údaje „presné, úplné a aktualizované v rozsahu potrebnom vo vzťahu k danému účelu“, na ktorý sa údaje spracúvajú. Minimalizácia údajov sa vyžaduje v článku 3 ods. 1 a 6 a článku 16 ods. 1 zákona o ochrane osobných informácií, v ktorých sa stanovuje, že prevádzkovateľ získava osobné údaje (iba) „v minimálnom potrebnom rozsahu“ na zamýšľaný účel, pričom v tejto súvislosti preberá dôkazné bremeno. Ak je možné splniť účel získavania spracúvaním informácií v anonymizovanej podobe, prevádzkovatelia by sa mali o takýto postup usilovať (článok 3 ods. 7 zákona o ochrane osobných informácií).

2.3.5. *Minimalizácia uchovávania*

(58) Osobné údaje by sa v zásade nemali uchovávať dlhšie, než je potrebné na účely, na ktoré sa osobné údaje spracúvajú.

(59) Zásada minimalizácie uchovávania sa podobne uvádza v článku 21 ods. 1 zákona o ochrane osobných informácií ([80]), v ktorom sa od prevádzkovateľa vyžaduje, aby bezodkladne „zničil“ ([81]) osobné údaje po dosiahnutí cieľa spracúvania alebo skončení obdobia ich uchovávania (podľa toho, čo nastane skôr), ak sa podľa právneho predpisu nevyžaduje ich ďalšie uchovávanie ([82]). Ak sa ďalšie uchovávanie vyžaduje, príslušné osobné údaje „sa uchovávajú a riadia oddelene od ostatných osobných informácií“ (článok 21 ods. 3 zákona o ochrane osobných informácií).

(60) Článok 21 ods. 1 zákona o ochrane osobných informácií sa neuplatňuje pri spracúvaní pseudonymizovaných údajov na štatistické účely, účely vedeckého výskumu alebo archivovania vo verejnom záujme ([83]). Na zabezpečenie dodržania zásady obmedzeného uchovávania údajov sa aj v tomto prípade v oznámení č. 2021-5 vyžaduje, aby prevádzkovatelia anonymizovali informácie v súlade s článkom 58-2 zákona o ochrane osobných informácií, ak údaje neboli zničené po dosiahnutí osobitného účelu spracúvania ([84]).

2.3.6. *Bezpečnosť údajov*

(61) Osobné údaje by sa mali spracúvať spôsobom, ktorým sa zaistí ich bezpečnosť vrátane ochrany pred neoprávneným alebo nezákonným spracúvaním a náhodnou stratou, zničením alebo poškodením. Na tento účel by podnikateľské subjekty mali prijať vhodné technické alebo organizačné opatrenia na ochranu osobných údajov pred možnými hrozbami. Tieto opatrenia by sa mali posúdiť s prihliadnutím na najmodernejšie postupy, súvisiace náklady a povahu, rozsah, súvislosti a účel spracúvania, ako aj na riziká, ktoré predstavujú pre práva jednotlivcov.

(62) Podobná zásada bezpečnosti sa stanovuje v článku 3 ods. 4 zákona o ochrane osobných informácií, podľa ktorého sa vyžaduje, aby prevádzkovatelia „riadili osobné informácie bezpečne podľa metód spracúvania, druhov atď. osobných informácií, pričom prihliadajú na možnosť porušenia práv dotknutej osoby a závažnosť príslušných rizík“. Okrem toho prevádzkovateľ „spracúva osobné informácie tak, aby sa minimalizovala možnosť porušenia súkromia dotknutej osoby“, pričom v tejto súvislosti sa, ak je to možné, usiluje o spracúvanie osobných údajov v anonymizovanej alebo pseudonymizovanej podobe (článok 3 ods. 6 a 7 zákona o ochrane osobných informácií).

(63) Tieto všeobecné požiadavky sa podrobnejšie rozpracúvajú v článku 29 zákona o ochrane osobných informácií, podľa ktorého každý prevádzkovateľ „prijme také technické, riadiace a fyzické opatrenia, ako je zavedenie plánu vnútorného riadenia a vedenie záznamov atď., ktoré sú potrebné na zaistenie bezpečnosti podľa prezidentského dekrétu, aby sa osobné informácie nestratili, neodcudzili, neodhalili, nesfalšovali, nepozmenili ani nepoškodili“. V článku 30 ods. 1 vykonávacieho dekrétu k zákonu o ochrane osobných informácií sa tieto opatrenia stanovujú

([80]) Článok 8 (v spojení s článkom 8-2 vykonávacieho dekrétu), článok 11 (v spojení s článkom 12 ods. 2 vykonávacieho dekrétu).

([81]) Informácie o metódach zničenia osobných informácií sa uvádzajú v článku 16 vykonávacieho dekrétu k zákonu o ochrane osobných informácií. V článku 21 ods. 2 zákona o ochrane osobných informácií sa objasňuje, že to zahŕňa „opatrenia potrebné na znemožnenie obnovy údajov“.

([82]) Nedodržanie týchto požiadaviek môže viesť k trestnoprávnym sankciám (článok 73 ods. 1 až 2 zákona o ochrane osobných informácií). V článku 39-6 zákona o ochrane osobných informácií sa poskytovateľom informačných a komunikačných služieb ukladá dodatočná požiadavka na vymazanie osobných informácií používateľov, ktorí nevyužili ponúkané informačné a komunikačné služby aspoň jeden rok (ak sa podľa zákona alebo na žiadosť jednotlivca nevyžaduje ďalšie uchovávanie). Jednotlivci musia byť informovaní o zamýšľanom vymazaní svojich informácií 30 dní pred uplynutím jednoročnej lehoty (článok 39-6 ods. 2 zákona o ochrane osobných informácií a článok 48-5 ods. 3 vykonávacieho dekrétu k zákonu o ochrane osobných informácií). Ak sa ďalšie uchovávanie vyžaduje zo zákona, uchovávané údaje musia byť uložené oddelene od ostatných informácií o používateľoch a môžu sa používať alebo sprístupňovať len v súlade s daným zákonom (článok 48-5 ods. 1 až 2 vykonávacieho dekrétu k zákonu o osobných informáciách).

([83]) Článok 28-7 zákona o ochrane osobných informácií.

([84]) Oznámenie č. 2021-5 (príloha I), oddiel 4.

odkazom na 1. vypracovanie a vykonávanie plánu vnútorného riadenia na účely bezpečného spracúvania osobných údajov; 2. kontroly a obmedzenia prístupov; 3. zavedenie šifrovacej technológie na bezpečné uloženie a prenos osobných údajov; 4. záznamy o prihláseniach; 5. bezpečnostné programy a 6. fyzické opatrenia, ako napríklad systém bezpečného uloženia alebo blokovania ([85]).

(64) Okrem toho sa uplatňujú osobitné povinnosti v prípade výskytu porušenia ochrany údajov (článok 34 zákona o ochrane osobných informácií v spojení s článkami 39 a 40 vykonávacieho dekrétu k zákonu o ochrane osobných informácií ([86]). Konkrétne sa od prevádzkovateľa vyžaduje, aby poškodeným dotknutým osobám bezodkladne oznámil podrobnosti o porušení ochrany ([87]) vrátane informácií o (povinných) protiopatreniach prijatých prevádzkovateľom a o tom, čo môžu dotknuté osoby urobiť na minimalizovanie rizika škody (článok 34 ods. 1 a 2 zákona o ochrane osobných informácií) ([88]). Ak sa porušenie ochrany údajov týka aspoň 1 000 dotknutých osôb, prevádzkovateľ bezodkladne oznámi porušenie ochrany údajov aj protiopatrenia Komisii pre ochranu osobných údajov a Kórejskej agentúre pre internet a bezpečnosť, ktoré mu môžu poskytnúť technickú pomoc (článok 34 ods. 3 zákona o ochrane osobných informácií v spojení s článkom 39 vykonávacieho dekrétu k zákonu o ochrane osobných informácií). Prevádzkovatelia podľa ustanovení Občianskeho zákonníka o zodpovednosti za porušenie povinností zodpovedajú za škody vyplývajúce z porušenia ochrany údajov (pozri aj oddiel 2.5 o prostriedkoch nápravy) ([89]).

(65) Pri plnení povinností v oblasti bezpečnosti musí prevádzkovateľovi pomáhať zodpovedná osoba pre ochranu súkromia, ktorej úlohou je okrem iného budovanie vnútorného kontrolného systému na „predchádzanie odhaleniu, zneužitiu a nesprávnemu použitiu osobných informácií“ (článok 31 ods. 2 pododsek 4 zákona o ochrane osobných informácií). Prevádzkovateľ je okrem toho povinný vykonávať „primeranú kontrolu a dohľad“ nad svojimi zamestnancami, ktorí uskutočňujú spracúvanie osobných údajov, a to aj v oblasti ich bezpečného riadenia; k tomu patrí potrebná odborná príprava („vzdelávanie“) zamestnancov (článok 28 ods. 1 a 2 zákona o ochrane osobných informácií). A napokon musí prevádzkovateľ v prípade subsprostredkovania uložiť „poskytovateľom externých činností“ požiadavky, ktoré sa okrem iného týkajú bezpečného riadenia osobných údajov („technické a riadiace záruky“), pričom musí dohliadať na ich vykonávanie prostredníctvom inšpekcií (článok 26 ods. 1 a 4 zákona o ochrane osobných informácií v spojení s článkom 28 ods. 1 pododsekmi 3 a 4 a článkom 28 ods. 6 vykonávacieho dekrétu k zákonu o ochrane osobných informácií).

2.3.7. *Transparentnosť*

(66) Dotknuté osoby by mali byť informované o hlavných znakoch spracúvania ich osobných údajov.

([85]) Pokiaľ ide o spracúvanie osobných údajov poskytovateľmi informačných a komunikačných služieb, v článku 39-5 zákona o ochrane osobných informácií sa výslovne stanovuje, že počet osôb, ktoré spracúvajú osobné informácie používateľov, je obmedzený na minimum. Okrem toho poskytovatelia informačných a komunikačných služieb zabezpečujú, aby osobné informácie používateľov neboli zverejnené prostredníctvom informačnej a komunikačnej siete (článok 39-10 ods. 1 zákona o ochrane osobných informácií). Zverejnené informácie sa musia na žiadosť Komisie pre ochranu osobných informácií vymazať alebo zablokovať (článok 39-10 ods. 2 zákona o ochrane osobných informácií). Všeobecnejšie platí, že na poskytovateľov informačných a komunikačných služieb (a tretie strany, ktoré prijímajú osobné údaje používateľov) sa vzťahujú dodatočné bezpečnostné povinnosti stanovené v článku 48-2 vykonávacieho dekrétu k zákonu o ochrane osobných informácií, napr. vypracovanie a vykonávanie plánu vnútorného riadenia bezpečnostných opatrení, opatrení na zaistenie kontroly prístupu, šifrovania, používania softvéru na vyhľadávanie škodlivých programov atď.

([86]) Okrem toho existuje všeobecný zákaz poškodzovania, ničenia, pozmeňovania, falšovania alebo úniku osobných informácií bez právneho povolenia, pozri článok 59 pododsek 3 zákona o ochrane osobných informácií.

([87]) Požiadavka na informovanie jednotlivca sa neuplatňuje v rozsahu, v ktorom sa porušenie ochrany údajov vyskytne v prípade pseudonymizovaných informácií spracúvaných na účely štatistiky, vedeckého výskumu alebo archivovania vo verejnom záujme (článok 28-7 zákona o ochrane osobných informácií, v ktorom sa stanovuje výnimka z článku 34 ods. 1 a článku 39-4 zákona o ochrane osobných informácií). Zabezpečenie informovania jednotlivca by si vyžadovalo, aby dotknutý prevádzkovateľ identifikoval jednotlivcov z pseudonymizovaného súboru údajov, čo je podľa článku 28-5 zákona o ochrane osobných informácií výslovne zakázané. Všeobecná požiadavka na oznámenie porušenia ochrany údajov (Komisii pre ochranu osobných informácií) sa však uplatňuje aj naďalej.

([88]) Požiadavky na oznamovanie vrátane jeho načasovania a možnosti oznamovania „vo fázach“ sa podrobnejšie uvádzajú v článku 40 vykonávacieho dekrétu k zákonu o ochrane osobných informácií. Prísnejšie pravidlá sa uplatňujú na poskytovateľov informačných a komunikačných služieb, ktorí musia do 24 hodín od zistenia skutočnosti, že došlo k strate, odcudzeniu alebo úniku osobných informácií, informovať dotknutú osobu a Komisiu pre ochranu osobných informácií (článok 39-4 ods. 1 zákona o ochrane osobných informácií). Toto oznámenie musí obsahovať podrobnosti o osobných informáciách, ktoré unikli, čas, kedy k tomu došlo, opatrenia, ktoré môže používateľ prijať, opatrenia prijaté v reakcii na túto udalosť poskytovateľom, ako aj kontaktné údaje na útvar, ktorému môže používateľ adresovať otázky (článok 39-4 ods. 1 pododseky 1 až 5 zákona o ochrane osobných informácií). Ak existuje opodstatnený dôvod, napr. neexistencia kontaktných údajov používateľa, možno použiť iné prostriedky oznámenia, napr. zverejnenie informácií na webovom sídle (článok 39-4 ods. 1 zákona o ochrane osobných informácií v spojení s článkom 48-4 ods. 4 a nasl. vykonávacieho dekrétu k zákonu o ochrane osobných informácií). V takom prípade musí byť Komisia pre ochranu osobných informácií informovaná o dôvodoch (článok 34-4 ods. 3 zákona o ochrane osobných informácií).

([89]) Pozri napr. rozhodnutia najvyššieho súdu č. 2011Da59834, č. 2011Da59858 a č. 2011Da59841 z 26. decembra 2012. Anglické zhrnutie je k dispozícii tu: http://library.scourt.go.kr/SCLIB_data/decision/9-69%2020 12.12.26.2011Da59834.htm.

(67) To sa v kórejskom systéme zabezpečuje viacerými spôsobmi. Okrem práva na informácie podľa článku 4 pododseku 1 (všeobecne) a článku 20 ods. 1 zákona o ochrane osobných informácií (osobné údaje získané od tretích strán), ako aj práva na prístup podľa článku 35 zákona o ochrane osobných informácií, sa v zákone o ochrane osobných informácií uvádza všeobecná požiadavka na transparentnosť účelu spracúvania (článok 3 ods. 1 zákona o ochrane osobných informácií), ako aj osobitné požiadavky na transparentnosť v prípade, ak sa spracúvanie vykonáva na základe súhlasu (článok 15 ods. 2, článok 17 ods. 2 a článok 18 ods. 3 zákona o ochrane osobných informácií) ([90]). Okrem toho sa v článku 20 ods. 2 zákona o ochrane osobných informácií od niektorých prevádzkovateľov (v prípade ktorých spracúvanie prekračuje určité prahové hodnoty) ([91]) vyžaduje, aby informovali dotknutú osobu, ktorej osobné údaje prijali od tretej strany, o zdroji informácií, účele ich spracúvania a práve dotknutej osoby požiadať o pozastavenie spracúvania, ak takéto oznámenie neznemožňuje nedostatok kontaktných informácií. Výnimky sa uplatňujú na niektoré zložky osobných informácií, ktoré uchovávajú orgány verejnej moci, a to najmä na zložky obsahujúce údaje spracúvané na účely národnej bezpečnosti, iné osobitne dôležité („závažné“) národné záujmy alebo na účely presadzovania práva v trestných veciach, prípadne na situácie, keď je pravdepodobné, že oznámenie spôsobí ujmu na živote alebo fyzickej integrite inej osoby, prípadne nespravodlivé poškodenie majetku a ďalších záujmov inej osoby, no len vtedy, ak sú predmetné verejné alebo súkromné záujmy „preukázateľne nadradené“ právam príslušných dotknutých osôb (článok 20 ods. 4 zákona o ochrane osobných informácií). To si vyžaduje vyváženie záujmov.

(68) Okrem toho sa v článku 3 ods. 5 zákona o ochrane osobných informácií stanovuje, že prevádzkovatelia zverejnia svoju politiku ochrany súkromia (a ďalšie skutočnosti súvisiace so spracúvaním osobných informácií). Táto požiadavka sa podrobnejšie uvádza v článku 30 zákona o ochrane osobných informácií v spojení s článkom 31 vykonávacieho dekrétu k zákonu o ochrane osobných informácií. Podľa týchto ustanovení musí verejná politika ochrany súkromia okrem iného obsahovať informácie o 1. druhoch spracúvaných osobných údajov; 2. účele spracúvania; 3. období uchovávania; 4. tom, či sa osobné údaje poskytujú tretej strane ([92]); 5. akomkoľvek subsprostredkovaní; 6. právach dotknutej osoby a spôsobe ich uplatňovania a 7. kontaktné informácie (vrátane mena zodpovednej osoby pre ochranu súkromia alebo názvu vnútorného útvaru zodpovedného za zabezpečenie súladu s pravidlami ochrany údajov a vybavovanie sťažností). Politika ochrany súkromia musí byť zverejnená tak, aby ju dotknuté osoby „mohli bez problémov rozpoznať“ (článok 30 ods. 2 zákona o ochrane osobných informácií) ([93]), a musí sa neustále aktualizovať (článok 31 ods. 2 vykonávacieho dekrétu k zákonu o ochrane osobných informácií).

(69) Na verejné inštitúcie sa vzťahuje dodatočná povinnosť zaregistrovať v Komisii pre ochranu osobných informácií najmä tieto informácie: 1. názov verejnej inštitúcie; 2. dôvody a účely spracúvania zložiek osobných informácií; 3. náležitosti osobných údajov, ktoré sa zaznamenávajú; 4. metódu spracúvania; 5. obdobie uchovávania; 6. počet dotknutých osôb, ktorých osobné údaje sa uchovávajú; 7. útvar, ktorý vybavuje žiadosti dotknutých osôb; a 8. príjemcovia osobných údajov, ak sa údaje poskytujú bežne alebo opakovane (článok 32 ods. 1 zákona o ochrane osobných informácií) ([94]). Zaregistrované zložky osobných informácií zverejňuje Komisia pre ochranu osobných informácií a odkazovať na ne musia aj verejné inštitúcie vo svojich politikách ochrany súkromia (článok 30 ods. 1 a článok 32 ods. 4 zákona o ochrane osobných informácií).

(70) Na zvýšenie transparentnosti pre dotknuté osoby v Únii, ktorých osobné údaje sa prenášajú do Kórey na základe tohto rozhodnutia, sa v oznámení č. 2021-5 (príloha I) ukladajú dodatočné požiadavky na transparentnosť. Po prvé musia kórejskí prevádzkovatelia po prijatí osobných údajov z Únie na základe tohto rozhodnutia bezodkladne oznámiť príslušným dotknutým osobám (a v každom prípade najneskôr jeden mesiac od uskutočnenia prenosu) názov a kontaktné údaje subjektov prenášajúcich a prijímajúcich informácie, prenášané osobné údaje (alebo ich kategórie), účel získavania v prípade kórejského prevádzkovateľa, obdobie uchovávania a práva

([90]) Najmä vtedy, ak sa osobné informácie spracúvajú so súhlasom jednotlivca, musí prevádzkovateľ informovať jednotlivca o účele spracúvania, podrobnostiach o spracúvaných informáciách, príjemcovi informácií, období uchovávania a používania osobných informácií, ako aj o skutočnosti, že jednotlivec má nárok odoprieť súhlas (a o všetkých nevýhodách, ktoré z toho môžu vyplývať).

([91]) Podľa článku 15-2 ods. 1 vykonávacieho dekrétu k zákonu o ochrane osobných informácií sa to týka prevádzkovateľov spracúvajúcich citlivé informácie aspoň 50 000 dotknutých osôb, prípadne „bežné“ osobné informácie aspoň 1 milióna dotknutých osôb. V článku 15-2 ods. 2 vykonávacieho dekrétu k zákonu o ochrane osobných informácií sa stanovujú metódy a načasovanie oznámenia, v článku 15-2 ods. 3 požiadavka na uchovávanie určitých záznamov o nich. Okrem toho sa uplatňujú osobitné pravidlá na určité kategórie poskytovateľov informačných a komunikačných služieb (ktorých príjmy zo zisku za predchádzajúci rok boli na úrovni aspoň 10 miliárd wonov alebo ktorí počas troch mesiacov pred koncom predchádzajúceho roka priemerne uchovávali/riadili osobné údaje aspoň jedného milióna používateľov denne), ktorí musia pravidelne informovať používateľov o histórii používania ich osobných informácií, ak to neznemožňuje nedostatok kontaktných informácií (článok 39-8 zákona o ochrane osobných informácií a článok 48-6 vykonávacieho dekrétu k zákonu o ochrane osobných informácií).

([92]) Podľa informácií, ktoré poskytla kórejská vláda, to znamená povinnosť uviesť vo verejnej politike ochrany súkromia príjemcov individuálne.

([93]) Ďalšie spôsoby sú stanovené v článku 31 ods. 3 vykonávacieho dekrétu k zákonu o ochrane osobných informácií.

([94]) Požiadavka na registráciu sa neuplatňuje na určité druhy zložiek osobných informácií, napríklad na tie, v ktorých sa zaznamenávajú skutočnosti súvisiace s národnou bezpečnosťou, diplomatickými tajomstvami, vyšetrovaním trestnej činnosti, trestným stíhaním, trestmi, vyšetrovaním daňových trestných činov, alebo na zložky, ktoré sa výlučne týkajú interného pracovného výkonu (článok 32 ods. 2 zákona o ochrane osobných informácií).

podľa zákona o ochrane osobných informácií. Po druhé musia byť pri poskytovaní osobných údajov prijatých z Únie na základe tohto rozhodnutia tretím stranám dotknuté osoby informované okrem iného o príjemcovi, osobných údajoch alebo kategóriách osobných údajov, ktoré sa majú poskytnúť, krajine, ktorej sa údaje poskytujú (ak ide o taký prípad), ako aj o právach poskytovaných podľa zákona o ochrane osobných informácií ([95]). Takýmto spôsobom sa v oznámení zabezpečuje neustále informovanie jednotlivcov z EÚ o konkrétnych prevádzkovateľoch spracúvajúcich ich informácie, voči ktorým si budú môcť uplatniť práva.

(71) V oddiele 3 písm. iii) oznámenia (príloha I) sa umožňujú určité obmedzené a oprávnené výnimky z týchto dodatočných povinností v oblasti transparentnosti, ktoré v zásade zodpovedajú nariadeniu (EÚ) 2016/679. Konkrétne sa oznamovanie dotknutým osobám v Únii nevyžaduje 1. ak a kým je potrebné obmedziť oznamovanie na určité dôvody verejného záujmu (napríklad ak sa informácie spracúvajú na účely národnej bezpečnosti alebo prebiehajúcich vyšetrovaní trestnej činnosti) v rozsahu, v akom sú tieto ciele verejného záujmu preukázateľne nadradené právam dotknutej osoby; 2. ak dotknutá osoba už má dané informácie; 3. ak a dovtedy, kým je pravdepodobné, že oznámenie spôsobí ujmu na živote alebo fyzickej integrite jednotlivca alebo inej osoby, prípadne nespravodlivé poškodenie majetkových záujmov inej osoby, ak sú tieto práva a záujmy preukázateľne nadradené právam dotknutej osoby; alebo 4. ak neexistujú žiadne kontaktné údaje o dotknutých jednotlivcoch alebo by sa na ich informovanie vyžadovalo neprimerané úsilie. Pri určovaní toho, či je možné kontaktovať dotknutú osobu alebo či toto kontaktovanie vyžaduje nadmerné úsilie, sa zváži možnosť spolupráce s vývozcom údajov v Únii.

(72) Pokiaľ ide o transparentnosť, pravidlami uvedenými v odôvodneniach (67) – (71) sa teda zabezpečuje úroveň ochrany v zásade zodpovedajúca nariadeniu (EÚ) 2016/679.

2.3.8. *Individuálne práva*

(73) Dotknuté osoby by mali mať určité práva, ktoré možno uplatniť voči prevádzkovateľovi alebo sprostredkovateľovi, najmä právo na prístup k údajom, právo na opravu údajov, právo namietať proti spracúvaniu a právo na vymazanie údajov. Zároveň sa môžu na tieto práva vzťahovať obmedzenia, ak sú potrebné a primerané na zabezpečenie dôležitých cieľov všeobecného verejného záujmu.

(74) Podľa článku 3 ods. 5 zákona o ochrane osobných informácií prevádzkovateľ zabezpečuje práva dotknutých osôb uvedené v článku 4 zákona o ochrane osobných informácií a podrobnejšie uvedené v článkoch 35 až 37, článkoch 39 a 39-2 zákona o ochrane osobných informácií.

(75) Po prvé majú jednotlivci právo na informácie a právo na prístup. Ak prevádzkovateľ získal osobné údaje od tretej strany – bude to tak vždy, keď sa údaje prenášajú z Únie –, dotknuté osoby majú vo všeobecnosti právo na získanie informácií o 1. „zdroji“ získaných osobných informácií (t. j. o prevádzateľovi); 2. účele spracúvania a 3. skutočnosti, že dotknutá osoba má nárok žiadať o pozastavenie spracúvania (článok 20 ods. 2 zákona o ochrane osobných informácií). Uplatňujú sa obmedzené výnimky, konkrétne ak je pravdepodobné, že takéto oznámenie spôsobí ujmu na živote alebo fyzickej integrite inej osoby, prípadne „nespravodlivé poškodenie majetku a ďalších záujmov“ inej osoby, no len vtedy, ak sú tieto záujmy tretích osôb „preukázateľne nadradené“ právam dotknutých osôb (článok 20 ods. 4 pododsek 2 zákona o ochrane osobných informácií).

(76) Okrem toho sa v článku 35 ods. 1 a 3 zákona o ochrane osobných informácií v spojení s článkom 41 ods. 4 vykonávacieho dekrétu k zákonu o ochrane osobných informácií poskytuje dotknutým osobám právo na prístup k ich osobným informáciám ([96]). Právo na prístup sa týka potvrdenia spracúvania, informácií o druhu spracúvaných údajov, účelu spracúvania, obdobia uchovávania, ako aj každého sprístupnenia tretej strane a poskytnutia

([95]) Oznámenie č. 2021-5, oddiel 3 písm. ii) (príloha I).

([96]) Podľa článku 35 ods. 3 zákona o ochrane osobných informácií v spojení s článkom 42 ods. 2 vykonávacieho dekrétu k zákonu o ochrane osobných informácií môže prevádzkovateľ odložiť prístup z „dobrého dôvodu“ (t. j. na základe opodstatnených dôvodov, napríklad ak je potrebný dlhší čas na posúdenie toho, či prístup možno poskytnúť), musí však dotknutej osobe takéto odôvodnenie do 10 dní oznámiť a poskytnúť jej informácie o spôsobe odvolania proti tomuto rozhodnutiu; po zániku dôvodu na odloženie musí byť prístup poskytnutý.

kópie spracúvaných osobných informácií (článok 4 pododsek 3 zákona o ochrane osobných informácií v spojení s článkom 41 ods. 1 vykonávacieho dekrétu k zákonu o ochrane osobných informácií) ([97]). Prístup môže byť obmedzený (čiastočný prístup) ([98]) alebo zamietnutý iba vtedy, ak sa to umožňuje v zákone ([99]), a to v situácii, ak je pravdepodobné, že by spôsobil ujmu na živote alebo fyzickej integrite tretej strany, prípadne neopodstatnené poškodenie majetku a iných záujmov inej osoby (článok 35 ods. 4 zákona o ochrane osobných informácií) ([100]). V druhom prípade je potrebné dosiahnuť rovnováhu medzi ústavne chránenými právami a slobodami jednotlivca na jednej strane a iných osôb na strane druhej. V prípade obmedzenia alebo zamietnutia prístupu musí prevádzkovateľ oznámiť dotknutej osobe príslušné dôvody a spôsob odvolania proti tomuto rozhodnutiu (článok 41 ods. 5, článok 42 ods. 2 vykonávacieho dekrétu k zákonu o ochrane osobných informácií).

(77) Po druhé majú dotknuté osoby právo na opravu alebo vymazanie ([101]) svojich osobných údajov, „ak sa v iných právnych predpisoch výslovne nestanovuje inak“ (článok 36 ods. 1 a 2 zákona o ochrane osobných informácií) ([102]). Po prijatí žiadosti musí prevádzkovateľ bezodkladne záležitosť preskúmať, prijať potrebné opatrenia ([103]) a do 10 dní to oznámiť dotknutej osobe; ak žiadosti nemožno vyhovieť, táto požiadavka na oznámenie sa vzťahuje na dôvody zamietnutia a spôsob odvolania (pozri článok 36 ods. 4 zákona o ochrane osobných informácií v spojení s článkom 43 ods. 3 vykonávacieho dekrétu k zákonu o ochrane osobných informácií ([104]).

(78) A napokon majú dotknuté osoby právo na bezodkladné pozastavenie spracúvania svojich osobných údajov ([105]), ak sa neuplatňuje niektorá z uvedených výnimiek (článok 37 ods. 1 a 2 zákona o ochrane osobných informácií) ([106]). Prevádzkovateľ môže zamietnuť žiadosť, 1. ak sa to výslovne umožňuje v zákone alebo je to potrebné („nevyhnutné“) na splnenie zákonných povinností; 2. ak je pravdepodobné, že pozastavenie by spôsobilo ujmu na živote alebo fyzickej integrite tretej strany, prípadne neopodstatnené poškodenie majetku a iných záujmov inej osoby; 3. ak by verejná inštitúcia bez spracúvania daných informácií nemohla vykonávať funkciu, ktorá jej vyplýva zo zákona; alebo 4. ak dotknutá osoba výslovne neukončí základnú zmluvu s prevádzkovateľom, hoci by bolo nepraktické vykonávať zmluvu bez takéhoto spracúvania údajov. V tomto prípade musí prevádzkovateľ bezodkladne oznámiť dotknutej osobe dôvody zamietnutia a spôsob odvolania sa (článok 37 ods. 2 zákona o ochrane osobných informácií v spojení s článkom 44 ods. 2 vykonávacieho dekrétu k zákonu o ochrane osobných informácií). Podľa článku 37 ods. 4 zákona o ochrane osobných informácií musí prevádzkovateľ pri plnení žiadosti o pozastavenie spracúvania bezodkladne „prijať potrebné opatrenia vrátane zničenia príslušných osobných informácií“ ([107]).

(79) Právo na pozastavenie spracúvania sa uplatňuje aj vtedy, ak sa osobné údaje používajú na účely priameho marketingu, t. j. s cieľom propagovať tovar alebo služby, prípadne podnietiť ich nákup. Okrem toho si takéto ďalšie spracúvanie vo všeobecnosti vyžaduje osobitný (dodatočný) súhlas dotknutej osoby (pozri článok 15 ods. 1 pododsek 1, článok 17 ods. 2 pododsek 1 zákona o ochrane osobných informácií) ([108]). Pri žiadosti o takýto súhlas musí prevádzkovateľ „výslovne rozpoznateľným spôsobom“ informovať dotknutú osobu najmä o zamýšľanom použití údajov na účely priameho marketingu, t. j. skutočnosti, že môže byť kontaktovaná na

([97]) Prístup k osobným informáciám spracúvaným verejnou inštitúciou možno získať priamo od inštitúcie alebo nepriamo podaním žiadosti Komisii pre ochranu osobných informácií, ktorá túto žiadosť bezodkladne postúpi (článok 35 ods. 2 zákona o ochrane osobných informácií a článok 41 ods. 3 vykonávacieho dekrétu k zákonu o ochrane osobných informácií).

([98]) Podľa článku 42 ods. 1 vykonávacieho dekrétu k zákonu o ochrane osobných informácií má prevádzkovateľ povinnosť priznať čiastočný prístup, ak sa aspoň na časť informácií nevzťahujú dôvody zamietnutia prístupu.

([99]) V takýchto zákonoch sa zase musí dodržiavať základné právo na súkromie a ochranu údajov, ako aj zásady nevyhnutnosti a primeranosti stanovené v kórejskej ústave.

([100]) Okrem toho môžu verejné inštitúcie zamietnuť priznanie prístupu, ak by to mohlo spôsobiť závažné problémy pri vykonávaní určitých funkcií vrátane prebiehajúcich auditov alebo ukladania, výberu či vrátenia daní (článok 35 ods. 4 zákona o ochrane osobných informácií).

([101]) V tomto prípade musí prevádzkovateľ prijať opatrenia na zabránenie obnove osobných informácií, pozri článok 36 ods. 3 zákona o ochrane osobných informácií.

([102]) Takéto právne predpisy musia spĺňať požiadavky ústavy, podľa ktorých môže byť základné právo obmedzené len vtedy, ak je potrebné z dôvodov národnej bezpečnosti alebo udržania verejného poriadku pre blaho verejnosti, pričom nesmie byť ovplyvnená podstata slobody alebo práva (článok 37 ods. 2 ústavy).

([103]) V článku 43 ods. 2 vykonávacieho dekrétu k zákonu o ochrane osobných informácií sa stanovuje osobitný postup v prípade, ak prevádzkovateľ spracúva zložky osobných informácií poskytnuté iným prevádzkovateľom.

([104]) Neprijatie potrebných opatrení na opravu alebo vymazanie osobných informácií a nepretržité používanie alebo poskytovanie takýchto informácií tretej strane môže viesť k trestnoprávnym sankciám (článok 73 ods. 2 zákona o ochrane osobných informácií).

([105]) Podľa článku 44 ods. 2 vykonávacieho dekrétu k zákonu o ochrane osobných informácií informuje prevádzkovateľ dotknutú osobu o skutočnosti, že riadne pozastavil spracúvanie, do 10 dní od prijatia žiadosti.

([106]) V prípade verejných inštitúcií možno právo na pozastavenie spracúvania uplatniť na informácie uvedené v zaregistrovaných zložkách osobných informácií (článok 37 v spojení s článkom 32 zákona o ochrane osobných informácií). Takáto registrácia sa v niektorých situáciách nevyžaduje, napr. ak sa zložky osobných informácií týkajú národnej bezpečnosti, vyšetrovaní trestnej činnosti, diplomatických vzťahov atď. (článok 32 ods. 2 zákona o ochrane osobných informácií).

([107]) Nepozastavenie spracúvania môže viesť k trestnoprávnym sankciám (článok 73 ods. 3 zákona o ochrane osobných informácií).

([108]) Výbor pre mediáciu sporov (pozri odôvodnenie 133) sa zaoberal viacerými prípadmi, keď sa jednotlivci sťažovali na používanie svojich údajov na účely priameho marketingu bez ich súhlasu, čo napríklad viedlo k zaplateniu náhrady škody a vymazaniu osobných údajov príslušným prevádzkovateľom (pozri napr. Výbor pre mediáciu sporov, rozhodnutie č. 20R10-024 z 18. novembra 2020, č. 20R08-015 z 28. augusta 2020, č. 20R07-031 z 1. septembra 2020).

účely propagácie tovaru alebo služieb alebo podnietenia ich nákupu (článok 22 ods. 2 a 4 zákona o ochrane osobných informácií v spojení s článkom 17 ods. 2 pododsekom 1 vykonávacieho dekrétu k zákonu o ochrane osobných informácií)

(80) Na uľahčenie uplatňovania individuálnych práv musí prevádzkovateľ stanoviť vyhradené postupy a zverejniť ich (článok 38 ods. 4 zákona o ochrane osobných informácií) ([109]). Patria k nim postupy vznesenia námietok proti zamietnutiu žiadosti (článok 38 ods. 5 zákona o ochrane osobných informácií). Prevádzkovateľ musí zabezpečiť, aby bol postup uplatňovania práv „priaznivý pre dotknuté osoby“ a aby nebol zložitejší ako postup získavania osobných údajov; k tomu patrí aj povinnosť poskytovať informácie o postupe na svojom webovom sídle (článok 41 ods. 2, článok 43 ods. 1 a článok 44 ods. 1 vykonávacieho dekrétu k zákonu o ochrane osobných informácií) ([110]). Jednotlivci môžu na podanie takejto žiadosti splnomocniť zástupcu (článok 38 ods. 1 zákona o ochrane osobných informácií v spojení s článkom 45 vykonávacieho dekrétu k zákonu o ochrane osobných informácií). Zatiaľ čo prevádzkovateľ má právo na uloženie poplatku (a poštového poplatku v prípade žiadosti o zaslanie kópií osobných údajov poštou), jeho výška sa musí stanoviť „v rámci skutočných výdavkov potrebných na spracovanie [žiadosti]“; poplatok (poštový poplatok) nemožno uložiť, ak žiadosť podal prevádzkovateľ (článok 38 ods. 3 zákona o ochrane osobných informácií v spojení s článkom 47 vykonávacieho dekrétu k zákonu o ochrane osobných informácií).

(81) Zákon o ochrane osobných informácií a jeho vykonávací dekrét neobsahujú všeobecné ustanovenia, ktoré by sa zaoberali otázkou rozhodnutí s vplyvom na dotknutú osobu a boli by založené výlučne na automatizovanom spracúvaní osobných údajov. Pokiaľ ide o osobné údaje získané v Únii, každé rozhodnutie založené na automatizovanom spracúvaní však zvyčajne prijme prevádzkovateľ v Únii (ktorý má priamy vzťah s príslušnou dotknutou osobou), a preto sa naň vzťahuje nariadenie (EÚ) 2016/679 ([111]). To zahŕňa situácie prenosu, v ktorých spracúvanie vykonáva zahraničný (napríklad kórejský) hospodársky subjekt konajúci ako zástupca (sprostredkovateľ) v mene prevádzkovateľa v Únii (alebo ako subsprostredkovateľ konajúci v mene sprostredkovateľa v Únii, ktorý dostal údaje od prevádzkovateľa z Únie, ktorý ich získal), ktorý na tomto základe následne prijme rozhodnutie. Neexistencia osobitných pravidiel týkajúcich sa automatizovaného rozhodovania v zákone o ochrane osobných informácií preto pravdepodobne nebude mať vplyv na úroveň ochrany osobných údajov prenášaných na základe tohto rozhodnutia.

(82) Výnimkou je, že ustanovenia o transparentnosti žiadosti (článok 20) a individuálnych právach (články 35 až 37), ako aj požiadavka na oznamovanie jednotlivcom, ktorá sa vzťahuje na poskytovateľov informačných a komunikačných služieb (článok 39-8 zákona o ochrane osobných informácií), sa neuplatňujú na pseudonymizované informácie, ak sa spracúvajú na účel štatistiky, vedeckého výskumu alebo archivovania vo verejnom záujme (článok 28-7 zákona o ochrane osobných informácií) ([112]). V súlade s prístupom z článku 11 ods. 2 (v spojení s odôvodnením 57) nariadenia (EÚ) 2016/679 sa to odôvodňuje skutočnosťou, že na zaistenie transparentnosti alebo priznanie individuálnych práv by prevádzkovateľ musel identifikovať, či (a ak áno, ktoré) údaje súvisia s jednotlivcom podávajúcim žiadosť, čo sa výslovne zakazuje podľa zákona o ochrane osobných informácií (článok 28-5 ods. 1 zákona o ochrane osobných informácií). Ak takáto opätovná identifikácia navyše zahŕňa odstránenie pseudonymizácie v prípade celého (pseudonymizovaného) súboru údajov, osobné informácie všetkých iných dotknutých jednotlivcov by sa vystavili zvýšeným rizikám. Zatiaľ čo nariadenie (EÚ) 2016/679 sa týka situácií, v ktorých je opätovná identifikácia prakticky nemožná, v zákone o ochrane osobných informácií sa uplatňuje prísnejší prístup, keďže sa výslovne zakazuje opätovná identifikácia vo všetkých situáciách, v ktorých sa spracúvajú pseudonymizované informácie.

(83) Kórejský systém, ako sa opisuje v odôvodneniach (74) – (82), teda obsahuje pravidlá o právach dotknutých osôb, ktorými sa zabezpečuje úroveň ochrany v zásade zodpovedajúca nariadeniu (EÚ) 2016/679.

([109]) Pozri aj článok 30 ods. 1 pododsek 5 zákona o ochrane osobných informácií o politike ochrany súkromia, ktorý okrem iného obsahuje informácie o právach, ktoré má jednotlivec k dispozícii, a o spôsobe ich uplatňovania.

([110]) Pozri aj článok 39-7 ods. 2 zákona o ochrane osobných informácií týkajúci sa poskytovateľov informačných a komunikačných služieb.

([111]) Naopak, vo výnimočnom prípade, keď má kórejský hospodársky subjekt priamy vzťah s dotknutou osobou z EÚ, pôjde spravidla o dôsledok toho, že osobe v Európskej únii ponúkal tovar alebo služby alebo monitoroval jej správanie. V takom prípade bude samotný kórejský hospodársky subjekt patriť do rozsahu pôsobnosti nariadenia (EÚ) 2016/679 (článok 3 ods. 2), a teda bude musieť priamo dodržiavať právne predpisy EÚ v oblasti ochrany údajov.

([112]) Pozri aj oznámenie č. 2021-5, v ktorom sa potvrdzuje, že oddiel III zákona o ochrane osobných informácií (vrátane článku 28-7) sa uplatňuje iba vtedy, ak sa pseudonymizované informácie spracúvajú na účely vedeckého výskumu, štatistiky alebo archivovania vo verejnom záujme, pozri oddiel 4 prílohy I k tomuto rozhodnutiu.

2.3.9. *Následné prenosy*

(84) Úroveň ochrany osobných údajov prenášaných z Únie prevádzkovateľom v Kórejskej republike nesmie byť oslabená ďalším prenosom takýchto údajov príjemcom v tretej krajine.

(85) Takéto „následné prenosy“ predstavujú z pohľadu kórejského prevádzkovateľa medzinárodné prenosy z Kórejskej republiky. V tomto zmysle sa v zákone o ochrane osobných informácií rozlišuje medzi externým zabezpečovaním spracúvania poskytovateľom externých činností (t. j. sprostredkovateľom) a poskytovaním osobných údajov tretím stranám ([113]).

(86) Po prvé, keď sa spracúvanie osobných údajov externe zadáva subjektu so sídlom v tretej krajine, kórejský prevádzkovateľ musí zabezpečiť súlad s ustanoveniami zákona o ochrane osobných informácií týkajúcimi sa externého zabezpečovania spracúvania (článok 26 zákona o ochrane osobných informácií). K tomu patrí aj zavedenie právne záväzného nástroja, ktorým sa okrem iného obmedzuje spracúvanie vykonávané poskytovateľom externých činností na účel externe zabezpečovanej práce, ukladajú technické a riadiace záruky a obmedzuje subsprostredkovanie (pozri článok 26 ods. 1 zákona o ochrane osobných informácií); a zverejňovanie informácií o externe zabezpečovanej práci. Okrem toho má prevádzkovateľ povinnosť „vzdelávať“ poskytovateľa externých činností o potrebných bezpečnostných opatreniach a vykonávať nad ním dohľad, a to aj prostredníctvom inšpekcií, pri ktorých sa kontroluje, či dodržiava všetky povinnosti prevádzkovateľa vyplývajúce zo zákona o ochrane osobných informácií ([114]), ako aj zmluvu o externom zabezpečovaní činností.

(87) Ak poskytovateľ externých činností spôsobí pri spracúvaní osobných údajov škodu v dôsledku porušenia zákona o ochrane osobných informácií, zodpovednosť za ňu bude pripísaná prevádzkovateľovi rovnako, ako by to bolo v prípade zamestnancov prevádzkovateľa (článok 26 ods. 6 zákona o ochrane osobných informácií). Kórejský prevádzkovateľ je preto naďalej zodpovedný za osobné údaje, ktoré externe poskytol, a musí zabezpečiť, aby zahraničný sprostredkovateľ spracúval informácie v súlade so zákonom o ochrane osobných informácií. Ak poskytovateľ externých činností pri spracúvaní informácií poruší zákon o ochrane osobných informácií, kórejský prevádzkovateľ môže niesť zodpovednosť za nedodržanie svojej povinnosti zabezpečiť súlad so zákonom o ochrane osobných informácií, napríklad prostredníctvom vykonávania dohľadu nad poskytovateľom externých činností. Zárukami uvedenými v zmluve o externom zabezpečovaní činností a zodpovednosťou kórejského prevádzkovateľa za činnosti poskytovateľa externých činností sa zabezpečuje kontinuita ochrany, ak sa spracúvanie osobných údajov externe zadáva subjektu mimo Kórey.

(88) Po druhé môžu kórejskí prevádzkovatelia poskytnúť osobné údaje tretej strane so sídlom mimo Kórey. Hoci sa v zákone o ochrane osobných informácií uvádza viacero právnych dôvodov, na základe ktorých sa vo všeobecnosti umožňuje poskytovanie tretím stranám, prevádzkovateľ musí v zásade ([115]) získať súhlas dotknutej osoby ([116]) po poskytnutí informácií dotknutej osobe o 1. druhu osobných údajov; 2. príjemcovi osobných údajov; 3. účele prenosu v zmysle účelu spracúvania vykonávaného príjemcom; 4. období uchovávania na účely spracúvania príjemcom, ako aj o 5. skutočnosti, že dotknutá osoba môže súhlas odmietnuť (článok 17 ods. 2 a 3 zákona o ochrane osobných informácií). V oddiele o transparentnosti oznámenia č. 2021-5 (pozri odôvodnenie (70)) sa vyžaduje, aby boli jednotlivci informovaní o tretej krajine, ktorej sa ich údaje poskytujú. Tým sa zabezpečuje, že dotknuté osoby v Únii môžu prijímať plne informované rozhodnutia o tom, či poskytnúť súhlas so spracúvaním v zahraničí. Okrem toho prevádzkovateľ nesmie uzavrieť zmluvu s treťou stranou ako príjemcom, ktorá by bola v rozpore so zákonom o ochrane osobných informácií, čo znamená, že zmluva nesmie obsahovať povinnosti, ktoré by boli v rozpore s požiadavkami uloženými prevádzkovateľovi v zákone o ochrane osobných informácií ([117]).

([113]) Na poskytovateľov informačných a komunikačných služieb sa uplatňujú osobitné pravidlá. V súlade s článkom 39-12 zákona o ochrane osobných informácií musia poskytovatelia informačných a komunikačných služieb v zásade získať súhlas používateľa s každým prenosom osobných informácií do zahraničia. V prípade prenosu osobných informácií pri externom zabezpečovaní činností spracúvania vrátane ukladania sa súhlas nevyžaduje, ak boli dotknutí jednotlivci informovaní priamo alebo prostredníctvom verejného oznámenia tak, že sa im vopred zabezpečuje jednoduchý prístup k 1. náležitostiam informácií, ktoré sa majú preniesť; 2. informáciám o krajine, do ktorej sa majú informácie preniesť (ako aj k informáciám o dátume a metóde prenosu); 3. informáciám o mene príjemcu a 4. účelu používania a uchovávania informácií príjemcom (článok 39-12 ods. 3 zákona o ochrane osobných informácií). Okrem toho sa v takom prípade uplatňujú všeobecné požiadavky na externé zabezpečovanie spracúvania. V prípade každého prenosu musia byť zavedené osobitné záruky týkajúce sa bezpečnosti, vybavovania sťažností a riešenia sporov, ako aj ďalšie opatrenia potrebné na ochranu informácií používateľov (článok 48-19 vykonávacieho dekrétu k zákonu o ochrane osobných informácií).

([114]) Pozri aj článok 26 ods. 7 zákona o ochrane osobných informácií, podľa ktorého sa na sprostredkovateľa *mutatis mutandis* uplatňujú články 15 až 25, články 27 až 31, články 33 až 38 a článok 50.

([115]) Na poskytnutie osobných informácií o používateľoch poskytovateľmi informačných a komunikačných služieb tretej strane sa vždy vyžaduje súhlas používateľa (článok 39-12 ods. 2 zákona o ochrane osobných informácií).

([116]) Ako sa podrobnejšie vysvetľuje v poznámke pod čiarou č. 51, aby bol takýto súhlas platný, musí byť dobrovoľný, informovaný a osobitný.

([117]) Pozri aj článok 39-12 ods. 1 zákona o ochrane osobných informácií týkajúci sa poskytovateľov informačných a komunikačných služieb.

(89) Bez súhlasu jednotlivca možno osobné údaje poskytnúť tretej strane (v zahraničí) vtedy, ak je účel sprístupnenia „v rozsahu, ktorý primerane súvisí“ s pôvodným účelom získavania (článok 17 ods. 4 zákona o ochrane osobných informácií, pozri odôvodnenie (36)). Pri rozhodovaní o tom, či sprístupní (alebo nesprístupní) osobné údaje na „súvisiaci“ účel, však musí prevádzkovateľ zvážiť, či toto sprístupnenie jednotlivca znevýhodní a či boli prijaté potrebné bezpečnostné opatrenia (ako napríklad šifrovanie). Vzhľadom na to, že tretia krajina, do ktorej sa osobné údaje prenášajú, nemusí poskytovať ochranu podobnú ochrane poskytovanej podľa zákona o ochrane osobných informácií, sa v oddiele 2 oznámenia č. 2021-5 uznáva, že takéto nevýhody môžu vzniknúť a možno im zabrániť len vtedy, ak kórejský prevádzkovateľ a príjemca v zahraničí prostredníctvom právne záväzného nástroja (napríklad zmluvy) zabezpečia úroveň ochrany rovnakú ako v prípade zákona o ochrane osobných informácií, a to aj v súvislosti s právami dotknutých osôb.

(90) Na sprístupnenie „mimo stanoveného účelu“, t. j. poskytnutie údajov tretej strane na nový (nesúvisiaci) účel, ktoré sa môže uskutočniť len na základe niektorého z dôvodov uvedených v článku 18 ods. 2 zákona o ochrane osobných informácií, ako sa to opisuje v odôvodnení(39), sa uplatňujú osobitné pravidlá. Aj za týchto podmienok sa však poskytnutie tretej strane umožňuje iba vtedy, ak nie je pravdepodobné, že sa ním „nespravodlivo poškodia“ záujmy dotknutej osoby alebo tretej strany, čo si vyžaduje vyváženie záujmov. Okrem toho musí prevádzkovateľ podľa článku 18 ods. 5 zákona o ochrane osobných informácií uplatňovať dodatočné záruky, ktoré môžu zahŕňať požiadavku na tretiu stranu, aby obmedzila účel a metódu spracúvania alebo zaviedla osobitné bezpečnostné opatrenia. Znovu platí, že vzhľadom na to, že tretia krajina, do ktorej sa osobné údaje prenášajú, nemusí poskytovať ochranu podobnú ochrane poskytovanej podľa zákona o ochrane osobných informácií, sa v oddiele 2 oznámenia č. 2021-5 uznáva, že takéto „nespravodlivé poškodenie“ záujmov jednotlivca alebo tretej strany môže vzniknúť a možno im zabrániť len vtedy, ak kórejský prevádzkovateľ a príjemca v zahraničí prostredníctvom právne záväzného nástroja (napríklad zmluvy) zabezpečia úroveň ochrany rovnakú ako v prípade zákona o ochrane osobných informácií, a to aj v súvislosti s právami dotknutých osôb.

(91) Pravidlami z odôvodnení (86) – (90) sa teda zabezpečuje kontinuita ochrany pri následnom prenose osobných údajov (poskytovateľovi externých činností alebo tretej strane) z Kórejskej republiky spôsobom, ktorý v zásade zodpovedá nariadeniu (EÚ) 2016/679.

2.3.10. *Zodpovednosť*

(92) Podľa zásady zodpovednosti sa od subjektov, ktoré spracúvajú údaje, vyžaduje, aby zaviedli vhodné technické a organizačné opatrenia v záujme účinného dodržiavania svojich povinností v oblasti ochrany údajov a aby vedeli takéto dodržiavanie preukázať, najmä príslušnému dozornému orgánu.

(93) Podľa článku 3 ods. 6 a 8 zákona o ochrane osobných informácií musí prevádzkovateľ spracúvať osobné údaje „tak, aby sa minimalizovala možnosť porušenia“ súkromia dotknutej osoby, a usiluje sa získať dôveru dotknutej osoby dodržiavaním a vykonávaním týchto povinností podľa zákona o ochrane osobných informácií a ďalších súvisiacich právnych predpisov. K tomu patrí zavedenie plánu vnútorného riadenia (článok 29 zákona o ochrane osobných informácií), ako aj primeraná odborná príprava zamestnancov a dohľad na nimi (článok 28 zákona o ochrane osobných informácií).

(94) Na zabezpečenie zodpovednosti sa v článku 31 zákona o ochrane osobných informácií v spojení s článkom 32 vykonávacieho dekrétu k zákonu o ochrane osobných informácií vytvára zodpovednosť prevádzkovateľov za menovanie zodpovednej osoby pre ochranu súkromia, ktorá „komplexne dohliada na spracúvanie osobných informácií“. Konkrétne je takáto zodpovedná osoba pre ochranu súkromia poverená týmito funkciami: 1. zavedením a vykonávaním plánu ochrany osobných údajov a vypracovaním politiky ochrany súkromia; 2. vykonávaním pravidelného preskúmania stavu a postupov spracúvania osobných údajov s cieľom napraviť nedostatky; 3. vybavovaním sťažností a naprávaním škôd; 4. zavedením systému vnútornej kontroly na zabránenie sprístupneniu, zneužitiu alebo nesprávnemu použitiu osobných údajov; 5. vypracovaním a vykonávaním vzdelávacieho programu; 6. ochranou, kontrolou a riadením zložiek osobných údajov a 7. ničením osobných údajov po dosiahnutí účelu spracúvania alebo skončení obdobia uchovávania. Pri vykonávaní týchto povinností môže zodpovedná osoba pre ochranu súkromia kontrolovať stav spracúvania osobných údajov a súvisiacich systémov a môže si vyžiadať príslušné informácie (článok 31 ods. 3 zákona o ochrane osobných informácií). Ak zodpovedná osoba pre ochranu súkromia zistí akékoľvek porušenie zákona o ochrane osobných informácií alebo iných príslušných právnych predpisov o ochrane údajov, okamžite prijme nápravné opatrenia a v prípade potreby ich oznámi vedeniu („vedúcemu“) prevádzkovateľa (článok 31 ods. 4 zákona o ochrane osobných informácií). Podľa článku 31 ods. 5 zákona o ochrane osobných informácií nesmie zodpovedná osoba pre ochranu súkromia v dôsledku výkonu týchto funkcií znášať neopodstatnené znevýhodnenie.

(95) Okrem toho sa musia prevádzkovatelia aktívne usilovať o uskutočňovanie posúdenia vplyvu na súkromie v prípade, ak vedenie zložiek osobných údajov predstavuje riziko pre súkromie (článok 33 ods. 8 zákona o ochrane osobných informácií). Na základe článku 33 ods. 1 a 2 zákona o ochrane osobných informácií v spojení s článkami 35, 36 a 38 vykonávacieho dekrétu k zákonu o ochrane osobných informácií budú pri posudzovaní miery ohrozenia práv dotknutých osôb relevantné faktory, ako napríklad druh a povaha spracúvaných údajov (najmä ak predstavujú citlivé informácie), ich objem, obdobie uchovávania a pravdepodobnosť porušenia ochrany údajov. Účelom posúdenia vplyvu na súkromie je zabezpečiť analýzu rizikových faktorov pre súkromie, ako aj bezpečnostných alebo iných protiopatrení, a uviesť záležitosti, ktoré je potrebné zlepšiť (pozri článok 33 ods. 1 zákona o ochrane osobných informácií v spojení s článkom 38 vykonávacieho dekrétu k zákonu o ochrane osobných informácií).

(96) Verejné inštitúcie sú povinné vykonať posúdenie vplyvu pri spracúvaní určitých zložiek osobných údajov, ktoré predstavujú vyššie riziko možných porušení súkromia (článok 33 ods. 1 zákona o ochrane osobných informácií). V súlade s článkom 35 vykonávacieho dekrétu k zákonu o ochrane osobných informácií je to tak okrem iného v prípade zložiek, ktoré obsahujú citlivé informácie aspoň o 50 000 dotknutých osobách, zložiek, ktoré budú priradené k iným zložkám a v dôsledku toho budú obsahovať informácie aspoň o 500 000 dotknutých osobách, alebo zložiek, ktoré obsahujú informácie aspoň o jednom milióne dotknutých osôb. Výsledok posúdenia vplyvu uskutočneného verejnou inštitúciou musí byť oznámený Komisii pre ochranu informácií (článok 33 ods. 1 zákona o ochrane osobných informácií), ktorá k nemu môže vypracovať stanovisko (článok 33 ods. 3 zákona o ochrane osobných informácií).

(97) A napokon sa v článku 13 zákona o ochrane osobných informácií stanovuje, že Komisia pre ochranu osobných informácií zavedie politiky potrebné na podporu „samoregulačných činností ochrany údajov“ vykonávaných prevádzkovateľmi, a to okrem iného prostredníctvom vzdelávania v oblasti ochrany údajov, podpory organizácií zapojených do ochrany údajov a poskytovania pomoci prevádzkovateľom pri zavádzaní a vykonávaní pravidiel samoregulácie. Okrem toho zavedie systém ePRIVACY Mark a uľahčí jeho prevádzku. V tejto súvislosti sa v článku 32-2 zákona o ochrane osobných informácií v spojení s článkami 34-2 až 34-8 vykonávacieho dekrétu k zákonu o ochrane osobných informácií poskytuje možnosť vydania certifikátu o tom, že systém (alebo systémy) prevádzkovateľa na spracúvanie a ochranu osobných údajov je v súlade s požiadavkami zákona o ochrane osobných informácií. Podľa týchto pravidiel môže byť udelený certifikát ([118]) (na obdobie troch rokov), ak prevádzkovateľ spĺňa certifikačné kritériá stanovené Komisiou pre ochranu osobných informácií vrátane zavedenia riadiacich, technických a fyzických záruk na ochranu osobných údajov ([119]). Komisia pre ochranu osobných informácií musí preskúmať systémy prevádzkovateľa relevantné pre certifikáciu aspoň raz ročne, aby sa zachovala platnosť certifikátu, inak môže byť certifikát zrušený (článok 32 ods. 4 zákona o ochrane osobných informácií v spojení s článkom 34-5 vykonávacieho dekrétu k zákonu o ochrane osobných informácií; tzv. „následné riadenie“).

(98) V kórejskom rámci sa teda vykonáva zásada zodpovednosti spôsobom, ktorým sa zabezpečuje úroveň ochrany v zásade zodpovedajúca nariadeniu (EÚ) 2016/679, a to vrátane poskytovania rôznych mechanizmov na zabezpečenie a preukazovanie súladu so zákonom o ochrane osobných informácií.

2.3.11. *Osobitné pravidlá týkajúce sa spracúvania osobných úverových informácií*

(99) Ako sa uvádza v odôvodnení (13), v zákone o používaní a ochrane úverových informácií sa stanovujú osobitné pravidlá na spracúvanie osobných úverových informácií obchodnými subjektmi. Pri spracúvaní osobných úverových informácií musia preto obchodné subjekty dodržiavať všeobecné požiadavky zákona o ochrane osobných informácií, ak zákon o používaní a ochrane úverových informácií neobsahuje konkrétnejšie pravidlá. Bude to tak napríklad vtedy, ak spracúvajú informácie spojené s kreditnými kartami alebo bankovým účtom v súvislosti s obchodnou transakciou jednotlivca. Keďže zákon o používaní a ochrane úverových informácií je odvetvovým právnym predpisom týkajúcim sa spracúvania úverových informácií (osobných a neosobných), nielenže sa v ňom ukladajú osobitné záruky na ochranu údajov (napríklad v oblasti transparentnosti a bezpečnosti), ale všeobecnejšie sa ním upravujú aj osobitné okolnosti, za ktorých možno osobné úverové informácie spracúvať. Odráža sa to najmä v podrobných požiadavkách na používanie a poskytovanie údajov tretej strane, ako aj na uchovávanie takýchto údajov.

(100) Rovnako ako v zákone o ochrane osobných informácií aj v zákone o používaní a ochrane úverových informácií sa odkazuje na zásadu zákonnosti a primeranosti. Po prvé sa v článku 15 ods. 1 zákona o používaní a ochrane úverových informácií ako všeobecná požiadavka umožňuje iba získavanie osobných úverových informácií primeranými a spravodlivými prostriedkami a v súlade s článkom 3 ods. 1 až ods. 2 zákona o ochrane osobných informácií v najmenšej možnej miere na konkrétny účel. Po druhé sa v zákone o používaní a ochrane úverových informácií konkrétne upravuje zákonnosť spracúvania osobných úverových informácií obmedzením ich získavania, používania a poskytovania tretej strane a vo všeobecnosti sa tieto činnosti spracúvania spájajú s požiadavkou na súhlas dotknutej osoby.

([118]) Okrem toho, ak prevádzkovateľ zamýšľa pri svojich podnikateľských činnostiach odkazovať na certifikáciu alebo propagovať certifikáciu, môže používať značku ochrany osobných informácií zavedenú Komisiou pre ochranu osobných informácií. Pozri článok 34-7 vykonávacieho dekrétu k zákonu o ochrane osobných informácií.

([119]) Od novembra 2018 sa vyvíja systém riadenia osobných informácií a informačnej bezpečnosti (ISMS-P), ktorým sa certifikujú prevádzkovatelia so zavedeným komplexným systémom riadenia.

(101) Osobné úverové informácie možno získavať z dôvodov uvedených v zákone o ochrane osobných informácií alebo z osobitných dôvodov stanovených v zákone o používaní a ochrane úverových informácií. Vzhľadom na to, že v článku 45 nariadenia (EÚ) 2016/679 sa predpokladá prenos osobných údajov prevádzkovateľom alebo sprostredkovateľom v Únii, ale neuvádza sa v ňom priame získavanie (napríklad od jednotlivca alebo z webového sídla) prevádzkovateľom v Kórei, pre toto rozhodnutie majú význam iba súhlas a dôvody uvedené v zákone o ochrane osobných informácií. K týmto dôvodom patria najmä situácie, keď je prenos potrebný na plnenie zmluvy s jednotlivcom alebo dosiahnutie oprávnených záujmov kórejského prevádzkovateľa (článok 15 ods. 1 pododseky 4 a 6 zákona o ochrane osobných informácií ([120]).

(102) Po získaní sa môžu osobné úverové informácie použiť 1. na pôvodný účel, na ktorý boli (priamo) poskytnuté jednotlivcom ([121]); 2. na účel, ktorý je zlučiteľný s pôvodným účelom získavania informácií ([122]); 3. na určenie toho, či nadviazať alebo zachovať obchodný vzťah požadovaný jednotlivcom ([123]); 4. na účel štatistiky, výskumu a archivovania vo verejnom záujme ([124]), ak sú informácie pseudonymizované ([125]); 5. ak sa získa ďalší súhlas alebo 6. v súlade so zákonom.

(103) Ak obchodný subjekt zamýšľa sprístupniť osobné úverové informácie tretej strane, musí získať súhlas jednotlivca ([126]) po tom, ako ho informuje o príjemcovi údajov, účele spracúvania príjemcom, podrobnostiach o údajoch, ktoré sa majú poskytnúť, období ich uchovávania príjemcom a práve na odmietnutie súhlasu (článok 32 ods. 1 zákona o používaní a ochrane úverových informácií a článok 28 ods. 2 vykonávacieho dekrétu k zákonu o používaní a ochrane úverových informácií) ([127]). Táto požiadavka na súhlas sa neuplatňuje v osobitných situáciách, konkrétne vtedy, ak sa osobné úverové informácií sprístupňujú ([128]): 1. poskytovateľovi externých činností na účely externého zabezpečovania činností ([129]); 2. tretej strane v prípade prevodu, rozdelenia alebo fúzie podniku; 3. na účel štatistiky, výskumu a archivovania vo verejnom záujme, ak sú informácie pseudonymizované; 4. na účel, ktorý je zlučiteľný s pôvodným účelom získavania informácií; 5. tretej strane, ktorá používa informácie na výber sumy, ktorú jednotlivec dlhuje ([130]); 6. na vykonanie súdneho príkazu; 7. prokurátorovi/príslušníkovi justičnej polície v mimoriadnej situácii, ak je ohrozený život jednotlivca alebo hrozí, že jednotlivec utrpí fyzické zranenie a nie je čas na vydanie

([120]) Zákon o používaní a ochrane úverových informácií obsahuje aj ďalšie právne základy pre získavanie, t. j. týkajúce sa získavania vyžadovaného zo zákona, a to v situáciách, v ktorých informácie zverejňuje verejná inštitúcia podľa právnych predpisov o slobodnom prístupe k informáciám alebo v ktorých sú informácie dostupné na sociálnej sieti. Ak sa chce obchodný subjekt opierať o posledný dôvod, musí vedieť preukázať, že získavanie sa uskutočňuje výlučne v rozsahu súhlasu dotknutej osoby, a to na základe primeraného („objektívneho“) výkladu a pri zohľadnení povahy údajov, zámeru a účelu ich sprístupnenia na sociálnej sieti, toho, či je účel ich získavania „veľmi relevantný“ vo vzťahu k danému účelu, atď. (článok 13 vykonávacieho dekrétu k zákonu o používaní a ochrane úverových informácií). Ako sa však vysvetľuje v odôvodnení (101), tieto dôvody v zásade nebudú relevantné v situácii prenosu.

([121]) Ak sa napríklad úverové informácie vytvoria/poskytnú v súvislosti s obchodnou transakciou s jednotlivcom. Toto však nemôže predstavovať dôvod použitia osobných úverových informácií na účely priameho marketingu (pozri článok 33 ods. 1 pododsek 3 zákona o používaní a ochrane úverových informácií).

([122]) Na určenie toho, či je účel použitia zlučiteľný s pôvodným účelom získavania informácií, sa musia zvážiť tieto faktory: 1. vzťah („relevantnosť“) medzi dvomi účelmi; 2. spôsob, akým sa informácie získali; 3. vplyv použitia informácií na jednotlivca a 4. či boli vykonané primerané bezpečnostné opatrenia, napríklad pseudonymizácia (pozri článok 32 ods. 6 pododsek 9-4 zákona o používaní a ochrane úverových informácií).

([123]) Prevádzkovateľ môže napríklad zohľadniť osobné úverové informácie, ktoré prijal od jednotlivca, pri rozhodovaní o tom, či mu predĺžiť zmluvu o úvere.

([124]) Článok 33 zákona o používaní a ochrane úverových informácií v spojení s článkom 32 ods. 6 pododsekmi 9-2, 9-4 a 10 zákona o používaní a ochrane úverových informácií.

([125]) Pseudonymizácia sa v článku 2 ods. 15 zákona o používaní a ochrane úverových informácií vymedzuje ako spracúvanie osobných úverových informácií tak, aby na základe týchto informácií už nebolo možné identifikovať jednotlivcov inak ako v kombinácii s dodatočnými informáciami. Hoci zákon o používaní a ochrane úverových informácií obsahuje osobitné záruky v oblasti spracúvania pseudonymizovaných informácií na účel štatistiky, výskumu a archivovania vo verejnom záujme (článok 40-2 zákona o používaní a ochrane úverových informácií), tieto pravidlá sa na obchodné organizácie neuplatňujú. Namiesto toho sa na ne vzťahujú osobitné požiadavky v oddiele III zákona o ochrane osobných informácií, ktoré sú opísané v odôvodneniach (42) – (48). V článku 40-3 zákona o používaní a ochrane úverových informácií sa ďalej stanovuje, že na spracúvanie pseudonymizovaných úverových informácií, ak sa uskutočňuje na účely štatistiky, vedeckého výskumu alebo archivovania vo verejnom záujme, sa vzťahuje výnimka z požiadaviek týkajúcich sa transparentnosti a individuálnych práv, ktorá je podobná ako výnimka v článku 28-7 zákona o ochrane osobných informácií a vzťahujú sa na ňu záruky z oddielu III zákona o ochrane osobných informácií, ako sú podrobnejšie opísané v odôvodneniach (42) – (48).

([126]) Neuplatňuje sa to, ak sa informácie poskytnú tretej strane na účely zachovania presnosti a aktuálnosti osobných úverových informácií, pokiaľ ustanovenie zostáva v rámci pôvodného účelu spracúvania (článok 32 ods. 1 zákona o používaní a ochrane úverových informácií). Môže sa to stať napríklad vtedy, ak sa aktuálne informácie poskytujú ratingovej agentúre na zabezpečenie presnosti jej záznamov.

([127]) Ak je nepraktické poskytnúť uvedené informácie, môže postačovať, ak sa jednotlivcovi oznámi príjemca tretej strany, ktorý získa požadované informácie.

([128]) Keďže v zákone o používaní a ochrane úverových informácií sa osobitne neupravuje zahraničné sprístupňovanie osobných úverových informácií, takéto sprístupňovanie musí byť v súlade so zárukami týkajúcimi sa následných prenosov, ktoré sú stanovené v oddiele 2 oznámenia č. 2021-5.

([129]) Externé zabezpečovanie spracúvania osobných úverových informácií sa môže uskutočniť len na základe písomnej zmluvy a v súlade s požiadavkami článku 26 ods. 1 až 3 a ods. 5 zákona o ochrane osobných informácií, ako sa to opisuje v odôvodnení (20) (článok 17 zákona o používaní a ochrane úverových informácií a článku 14 vykonávacieho dekrétu k zákonu o používaní a ochrane úverových informácií). Poskytovateľ externých činností nesmie informácie používať nad rámec povinností pri vykonávaní externých činností a spoločnosť vykonávajúca externé činnosti musí mať zavedené osobitné bezpečnostné požiadavky (napr. šifrovanie) a odborne pripraviť poskytovateľa externých činností v súvislosti so spôsobom, ako predchádzať strate, odcudzeniu, odhaleniu, pozmeneniu alebo prezradeniu úverových informácií.

([130]) Pozri aj článok 28 ods. 10 pododseky 1, 2 a 6 vykonávacieho dekrétu k zákonu o používaní a ochrane úverových informácií.

súdneho príkazu ([131]); 8. príslušným daňovým orgánom na dodržanie daňových zákonov; alebo 9. v súlade s inými zákonmi. V prípade sprístupnenia na základe niektorého z týchto dôvodov musí byť dotknutá osoba vopred informovaná (článok 32 ods. 7 zákona o používaní a ochrane úverových informácií).

(104) V zákone o používaní a ochrane úverových informácií sa osobitne upravuje aj trvanie spracúvania osobných úverových informácií na základe niektorého z uvedených dôvodov na použitie alebo poskytnutie informácií tretej strane po skončení obchodného vzťahu s jednotlivcom ([132]). Na základe dodatočných záruk (informácie musia byť uchovávané oddelene od úverových informácií, ktoré sa týkajú jednotlivcov so stále pretrvávajúcim obchodným vzťahom, musia byť chránené osobitnými bezpečnostnými opatreniami a prístup k nim môžu mať len oprávnení jednotlivci) možno uchovávať len informácie potrebné na nadviazanie alebo zachovanie takéhoto vzťahu ([133]). Všetky ostatné údaje sa musia vymazať (článok 17-2 ods. 1 pododsek 2 vykonávacieho dekrétu k zákonu o používaní a ochrane úverových informácií). Na určenie toho, ktoré údaje sú potrebné v rámci obchodného vzťahu, je potrebné zohľadniť viaceré faktory, napríklad či bude možné nadviazať vzťah bez údajov a či sa priamo týkajú tovaru alebo služieb dodávaných jednotlivcovi (článok 17-2 ods. 2 vykonávacieho dekrétu k zákonu o používaní a ochrane úverových informácií).

(105) Aj v prípadoch, keď sa osobné úverové informácie môžu v zásade uchovávať aj po skončení obchodného vzťahu, sa tieto informácie musia vymazať do troch mesiacov po dosiahnutí ďalšieho účelu spracúvania ([134]) alebo v každom prípade po piatich rokoch (článok 20-2 zákona o používaní a ochrane úverových informácií). Za určitých veľmi zriedkavých okolností možno osobné úverové informácie uchovávať dlhšie ako päť rokov, a to najmä vtedy, ak je to potrebné na splnenie zákonnej povinnosti; ak je to potrebné na dosiahnutie životne dôležitých záujmov týkajúcich sa ochrany života, fyzickej integrity alebo majetku jednotlivca; na archivovanie pseudonymizovaných informácií (ktoré sa použili na účely vedeckého výskumu, štatistiky alebo archivovania vo verejnom záujme); alebo na poisťovacie účely (konkrétne na účely platieb poistného, aby sa predišlo poisťovaciemu podvodu) ([135]). V týchto výnimočných prípadoch sa uplatňujú osobitné záruky (napríklad sa jednotlivcovi oznámi ďalšie použitie, uchovávané informácie sa oddelia od informácií týkajúcich sa jednotlivcov, s ktorými naďalej pretrváva obchodný vzťah, obmedzia sa prístupové práva, pozri článok 17-2 ods. 1 až 2 vykonávacieho dekrétu k zákonu o používaní a ochrane úverových informácií).

(106) V zákone o používaní a ochrane úverových informácií sa okrem toho ďalej stanovujú zásady presnosti a kvality údajov, preto sa v ňom vyžaduje, aby boli osobné úverové informácie „zaregistrované, upravené a riadené“ tak, aby sa zachovávala ich presnosť a aktuálnosť (článok 18 ods. 1 zákona o používaní a ochrane úverových informácií a článok 15 ods. 3 vykonávacieho dekrétu k zákonu o používaní a ochrane úverových informácií) ([136]). Pri poskytovaní úverových informácií určitým ďalším subjektom (napríklad ratingovým agentúram) sa od obchodných subjektov takisto osobitne vyžaduje, aby overovali presnosť informácií, a tým zabezpečovali, že príjemca zaregistruje a riadi iba presné informácie (článok 15 ods. 1 vykonávacieho dekrétu k zákonu o používaní a ochrane úverových informácií v spojení s článkom 18 ods. 1 zákona o používaní a ochrane úverových informácií). Všeobecnejšie sa v zákone o používaní a ochrane úverových informácií vyžaduje, aby sa uchovávali záznamy o získavaní, používaní osobných úverových informácií, ich sprístupňovaní tretej strane a ničení (článok 20 ods. 2 zákona o používaní a ochrane úverových informácií) ([137]).

(107) Ďalej sa na spracúvanie osobných úverových informácií vzťahujú osobitné požiadavky na bezpečnosť údajov. Konkrétne sa v zákone o používaní a ochrane úverových informácií vyžaduje zavedenie technologických, fyzických a organizačných opatrení na zabránenie nezákonnému prístupu do počítačových systémov, ako aj pozmeneniu, zničeniu alebo iným rizikám v súvislosti so spracúvanými údajmi (napríklad prostredníctvom kontroly prístupu, pozri článok 19 zákona o používaní a ochrane úverových informácií a článok°16 vykonávacieho dekrétu k zákonu o používaní a ochrane úverových informácií). Okrem toho sa musí na účely výmeny osobných úverových informácií s treťou stranou uzavrieť dohoda, v ktorej sa stanovia osobitné bezpečnostné opatrenia (článok 19 ods. 2 zákona o používaní a ochrane úverových informácií). Ak dôjde k porušeniu ochrany osobných úverových informácií, musia sa prijať opatrenia na minimalizovanie škôd a dotknutým jednotlivcom to musí byť bezodkladne oznámené (článok 39-4 ods. 1 až 2 zákona o používaní a ochrane úverových informácií). Okrem toho musí byť o oznámení jednotlivcom a prijatých opatreniach informovaná Komisia pre ochranu osobných informácií (článok 39-4 ods. 4 zákona o používaní a ochrane úverových informácií).

([131]) V takom prípade musí byť bezodkladne vydaný súdny príkaz. Ak sa súdny príkaz nevydá do 36 hodín, prijaté údaje sa musia bezodkladne vymazať (článok 32 ods. 6 pododsek 6 zákona o používaní a ochrane úverových informácií).

([132]) Napríklad preto, lebo boli splnené zmluvné podmienky, jedna zo strán uplatnila svoje právo na ukončenie zmluvy atď., pozri článok 17-2 ods. 5 vykonávacieho dekrétu k zákonu o používaní a ochrane úverových informácií.

([133]) Článok 20-2 ods. 1 zákona o používaní a ochrane úverových informácií a článok 17-2 ods. 1 pododsek 1 vykonávacieho dekrétu k zákonu o používaní a ochrane úverových informácií.

([134]) Pri tomto období sa prihliadne na to, že vymazanie nemusí byť vždy možné okamžite, ale zvyčajne si vyžaduje určité kroky (napr. oddelenie údajov, ktoré sa majú vymazať, od ostatných údajov a vykonanie vymazania bez toho, aby to malo vplyv na stabilitu informačných systémov), ktorých vykonanie trvá istý čas.

([135]) Článok 20-2 ods. 2 zákona o používaní a ochrane úverových informácií.

([136]) V článku 18 ods. 2 zákona o používaní a ochrane úverových informácií a článku 15 ods. 4 vykonávacieho dekrétu k zákonu o používaní a ochrane úverových informácií sa stanovujú konkrétnejšie pravidlá týkajúce sa tejto požiadavky na uchovávanie záznamov, napr. pre záznamy týkajúce sa informácií, ktoré môžu jednotlivca znevýhodniť, ako sú informácie o trestnej činnosti a konkurze.

([137]) Pokiaľ ide o ostatné mechanizmy zodpovednosti, v zákone o používaní a ochrane úverových informácií sa od niektorých organizácií (napr. družstiev a verejných subjektov, pozri článok 21 ods. 2 vykonávacieho dekrétu k zákonu o používaní a ochrane úverových informácií) vyžaduje, aby menovali „správcu/strážcu úverových informácií“, ktorý bude zodpovedať za monitorovanie súladu so zákonom o používaní a ochrane úverových informácií a vykonávať úlohy „zodpovednej osoby pre ochranu súkromia“ podľa zákona o ochrane osobných informácií (článok 20 ods. 3 a 4 zákona o používaní a ochrane úverových informácií).

(108) V zákone o používaní a ochrane úverových informácií sa ukladajú aj osobitné povinnosti v oblasti transparentnosti pri získavaní súhlasu s používaním alebo poskytovaním osobných úverových informácií (článok 32 ods. 4 a článok 34-2 zákona o používaní a ochrane úverových informácií a článok 30-3 vykonávacieho dekrétu k zákonu o používaní a ochrane úverových informácií) a všeobecnejšie pred poskytnutím informácií tretej strane (článok 32 ods. 7 zákona o ochrane úverových informácií) ([138]). Okrem toho majú jednotlivci právo vyžiadať si informácie o používaní a poskytovaní svojich úverových informácií tretím stranám za tri roky predchádzajúce žiadosti (vrátane účelu a dátumov takéhoto použitia/poskytnutia) ([139]).

(109) Podľa zákona o používaní a ochrane úverových informácií majú jednotlivci právo na prístup k svojim osobným úverovým informáciám (článok 38 ods. 1 zákona o používaní a ochrane úverových informácií) a právo na dosiahnutie opravy nepresných údajov (článok 38 ods. 2 až 3 zákona o používaní a ochrane úverových informácií) ([140]). Okrem všeobecného práva na vymazanie údajov podľa zákona o ochrane osobných informácií (pozri odôvodnenie (77)) sa v zákone o používaní a ochrane úverových informácií poskytuje aj osobné právo na vymazanie osobných úverových informácií, ktoré sa uchovávajú po skončení období uchovávania uvedených v odôvodnení (104), t. j. piatich rokov (v prípade osobných úverových informácií, ktoré boli potrebné na nadviazanie alebo zachovanie obchodného vzťahu) alebo troch mesiacov (v prípade ostatných druhov osobných úverových informácií) ([141]). Žiadosť o vymazanie môže byť výnimočne zamietnutá, ak je za okolností uvedených v odôvodnení (105) potrebné ďalšie uchovávanie. Ak jednotlivec požiada o vymazanie údajov, na ktoré sa vzťahuje niektorá z výnimiek, na dotknuté úverové informácie sa musia uplatňovať osobitné záruky (článok 38-3 ods. 3 zákona o používaní a ochrane úverových informácií a článok 33-3 vykonávacieho dekrétu k zákonu o používaní a ochrane úverových informácií). Informácie sa musia napríklad uchovávať osobitne od ostatných informácií, prístup k nim môže mať len oprávnená osoba a musia sa na ne vzťahovať osobitné bezpečnostné opatrenia.

(110) Okrem práv uvedených v odôvodnení (109) sa v zákone o používaní a ochrane úverových informácií zaručuje jednotlivcom právo požiadať prevádzkovateľa, aby ich prestal kontaktovať na účely priameho marketingu (článok 37 ods. 2 zákona) a právo na prenosnosť údajov. Pokiaľ ide o toto právo, v zákone o používaní a ochrane úverových informácií sa jednotlivcom umožňuje požiadať o prenos svojich osobných úverových informácií samým sebe alebo určitým tretím stranám (napríklad finančným inštitúciám a ratingovým spoločnostiam). Osobné úverové informácie musí tretia strana spracúvať a prenášať vo formáte, ktorý dokáže zariadenie na spracúvanie informácií (napríklad počítač) spracúvať.

(111) V rozsahu, v akom zákon o používaní a ochrane úverových informácií obsahuje osobitné pravidlá v porovnaní so zákonom o ochrane osobných informácií, sa preto Komisia domnieva, že aj týmito pravidlami sa zabezpečuje úroveň ochrany v zásade zodpovedajúca nariadeniu (EÚ) 2016/679.

2.4. **Dozor a presadzovanie**

(112) S cieľom zaistiť, aby bola primeraná úroveň ochrany údajov zabezpečená v praxi, by mal byť zriadený nezávislý dozorný orgán, ktorý bude mať právomoc monitorovať a presadzovať dodržiavanie pravidiel ochrany údajov. Tento orgán by mal pri plnení svojich úloh a výkone svojich právomocí konať úplne nezávisle a nestranne.

2.4.1. *Nezávislý dozor*

(113) V Kórejskej republike je nezávislým orgánom zodpovedným za monitorovanie zákona o ochrane osobných informácií a za jeho presadzovanie Komisia pre ochranu osobných informácií. Komisia pre ochranu osobných informácií pozostáva z predsedu, podpredsedu a siedmich komisárov. Predsedu a podpredsedu menuje prezident na odporúčanie predsedu vlády. Dvoch komisárov menuje prezident na odporúčanie predsedu a piatich komisárov na odporúčanie národného zhromaždenia [pričom dvoch z nich na odporúčanie politickej strany, ktorej

([138]) Patrí k nim všeobecná oznamovacia povinnosť (článok 32 ods. 7 zákona o používaní a ochrane úverových informácií) a osobitná povinnosť v oblasti transparentnosti v prípade poskytovania informácií, na základe ktorých sa určuje úverová bonita jednotlivca, niektorým subjektom, ako napríklad ratingovým agentúram a agentúram na získavanie úverových informácií (článok 35-3 zákona o používaní a ochrane úverových informácií a článok 30-3 vykonávacieho dekrétu k zákonu o používaní a ochrane úverových informácií), ako aj pre prípad zamietnutia alebo ukončenia obchodnej transakcie na základe osobných úverových informácií získaných od tretej strany (článok 36 zákona o používaní a ochrane úverových informácií a článok 31 vykonávacieho dekrétu k zákonu o používaní a ochrane úverových informácií).

([139]) Článok 35 zákona o používaní a ochrane úverových informácií. Na niektoré obchodné organizácie, napr. družstvá a verejné subjekty (článok 21 ods. 2 vykonávacieho dekrétu k zákonu o používaní a ochrane úverových informácií) sa vzťahujú dodatočné požiadavky v oblasti transparentnosti, napr. zverejňovanie niektorých informácií (článok 31 zákona o používaní a ochrane úverových informácií) a informovanie jednotlivcov o možnom zhoršení úverového ratingu po uskutočnení finančných transakcií predstavujúcich úverové riziká (článok 35-2 zákona o používaní a ochrane úverových informácií).

([140]) Na podmienky a výnimky týkajúce sa práv na prístup a opravu sa uplatňujú pravidlá zákona o ochrane osobných informácií (uvedené v odôvodneniach(76) – (77)). Okrem toho sa ďalšie spôsoby stanovujú v článku 38 ods. 4 až 8 zákona o používaní a ochrane úverových informácií a článku 33 vykonávacieho dekrétu k zákonu o používaní a ochrane úverových informácií. Konkrétne musí obchodný subjekt, ktorý opravil alebo vymazal nepresné úverové informácie, tieto skutočnosti oznámiť jednotlivcovi. Okrem toho musia byť príslušné skutočnosti oznámené každej tretej strane, ktorej sa dané informácie v priebehu predchádzajúcich šiestich mesiacov sprístupnili, ako aj dotknutému jednotlivcovi. Ak jednotlivec nie je spokojný s vybavením žiadosti o opravu, môže podať žiadosť Komisii pre ochranu osobných informácií, ktorá overí konanie prevádzkovateľa a môže mu uložiť nápravné opatrenia.

([141]) Článok 38-3 zákona o používaní a ochrane úverových informácií.

členom je prezident, a troch na odporúčanie iných politických strán (článok 7-2 ods. 2 zákona o ochrane osobných informácií), čo pomáha zabrániť zaujatosti v procese menovania] ([142]). Tento postup je v súlade s požiadavkami uplatniteľnými na menovanie členov orgánov pre ochranu údajov v Únii [článok 53 ods. 1 nariadenia (EÚ) 2016/679]. Okrem toho sa musia všetci komisári zdržať akýchkoľvek podnikateľských a politických činností a nesmú zastávať funkcie vo verejnej správe ani v národnom zhromaždení (článok 7-6 a článok 7-7 ods. 1 pododsek 3 zákona o ochrane osobných informácií) ([143]). Na všetkých komisárov sa vzťahujú osobitné pravidlá, podľa ktorých sa v prípade možného konfliktu záujmov nesmú zúčastňovať na rokovaniach (článok 7-11 zákona o ochrane osobných informácií). Komisii pre ochranu osobných informácií pomáha sekretariát (článok 7-13), pričom komisia môže zriadiť podkomisie (pozostávajúce z troch komisárov) na riešenie menej závažných porušení a opakovane sa vyskytujúcich vecí (článok 7-12 zákona o ochrane osobných informácií).

(114) Každý člen Komisie pre ochranu osobných informácií je menovaný na tri roky a môže byť menovaný opakovane (článok 7-4 ods. 1 zákona o ochrane osobných informácií). Komisárov možno odvolať len za osobitných okolností, konkrétne ak už nie sú schopní vykonávať svoje povinnosti z dôvodu dlhodobej duševnej poruchy alebo telesného postihnutia, konajú v rozpore so zákonom alebo spĺňajú niektorý z dôvodov na odvolanie z funkcie ([144]) (článok 7-5 zákona o ochrane osobných informácií). Týmto sa im poskytuje inštitucionálna ochrana pri výkone ich funkcií.

(115) Všeobecnejšie sa v článku 7 ods. 1 zákona o ochrane osobných informácií výslovne zaručuje nezávislosť Komisie pre ochranu osobných informácií a v článku 7-5 ods. 2 zákona o ochrane osobných informácií sa vyžaduje, aby komisári svoje povinnosti vykonávali nezávisle, v súlade so zákonom a svojím svedomím ([145]). Uvedené inštitucionálne a procesné záruky, a to aj tie, ktoré súvisia s menovaním a odvolávaním členov, zabezpečujú, že Komisia pre ochranu osobných informácií koná úplne nezávisle a nepodlieha žiadnym vonkajším vplyvom ani pokynom. Komisia pre ochranu osobných informácií ako ústredný správny orgán navyše každoročne predkladá návrh svojho rozpočtu (ktorý preskúma ministerstvo financií ako súčasť celkového štátneho rozpočtu pred jeho prijatím národným zhromaždením) a zodpovedá za riadenie vlastného personálu. Komisia pre ochranu osobných informácií v súčasnosti disponuje rozpočtom približne 35 miliónov EUR a má 154 zamestnancov (vrátane špecializovaných zamestnancov v oblasti informačných a komunikačných technológií, 32 zamestnancov, ktorí sa zameriavajú na vyšetrovania, a 40 právnych expertov).

(116) Úlohy a právomoci Komisie pre ochranu osobných informácií sa uvádzajú najmä v článkoch 7-8 a 7-9, ako aj v článkoch 61 až 66 zákona o ochrane osobných informácií ([146]). K úlohám Komisie pre ochranu osobných informácií konkrétne patrí poskytovanie poradenstva v oblasti zákonov a predpisov týkajúcich sa ochrany údajov, vypracúvanie politík a usmernení v oblasti ochrany údajov, vyšetrovanie porušení individuálnych práv, riešenie sťažností a mediácia sporov, presadzovanie dodržiavania zákona o ochrane osobných informácií, zabezpečovanie vzdelávania a podpory v oblasti ochrany údajov a výmena informácií a spolupráca s orgánmi pre ochranu údajov z tretích krajín ([147]).

(117) Na základe článku 68 zákona o ochrane osobných informácií v spojení s článkom 62 vykonávacieho dekrétu k zákonu o ochrane osobných informácií boli určité úlohy Komisie pre ochranu osobných informácií delegované na Kórejskú agentúru pre internet a bezpečnosť, konkrétne: 1. vzdelávanie a styk s verejnosťou; 2. odborná príprava špecialistov a vypracúvanie kritérií na posúdenie vplyvu na súkromie; 3. vybavovanie žiadostí o menovanie takzvanej inštitúcie na posudzovanie vplyvu na súkromie; 4. vybavovanie žiadostí o nepriamy prístup k osobným údajom vo vlastníctve orgánov verejnej moci (článok 35 ods. 2 zákona o ochrane osobných informácií); a 5. úloha vyžiadania materiálov a vykonávania inšpekcií týkajúcich sa sťažností prijatých prostredníctvom

([142]) Za komisárov Komisie pre ochranu osobných informácií môžu byť menovaní len jednotlivci, ktorí spĺňajú tieto kritériá: ide o vyšších štátnych zamestnancov zodpovedných za záležitosti súvisiace s osobnými informáciami; ide o bývalých sudcov, generálnych prokurátorov alebo právnikov aspoň s desaťročnou praxou; ide o bývalých manažérov s praxou v oblasti ochrany údajov, ktorí viac ako tri roky pracovali vo verejnej inštitúcii alebo organizácii alebo ich takáto inštitúcia či organizácia odporučila; a ak ide o docentov s odbornými znalosťami z oblasti ochrany údajov, ktorí aspoň päť rokov pracovali v akademickej inštitúcii (článok 7-2 zákona o ochrane osobných informácií).

([143]) Pozri aj článok 4-2 vykonávacieho dekrétu k zákonu o ochrane osobných informácií.

([144]) Pozri článok 7-7 zákona o ochrane osobných informácií, podľa ktorého sa cudzí štátni príslušníci a členovia politických strán nesmú stať členmi Komisie pre ochranu osobných informácií. To isté sa uplatňuje na jednotlivcov, ktorým boli uložené určité druhy trestnoprávnych sankcií, v priebehu posledných piatich rokov boli odvolaní z funkcie na základe disciplinárneho konania atď. (článok 7-7 zákona o ochrane osobných informácií v spojení s článkom 33 zákona o verejných činiteľoch).

([145]) Hoci sa v článku 7 ods. 2 zákona o ochrane osobných informácií odkazuje na všeobecnú právomoc predsedu vlády podľa článku 18 zákona o organizácii verejného sektora pozastaviť platnosť (so súhlasom prezidenta) každého nezákonného alebo nespravodlivého právneho aktu ústredného správneho orgánu alebo ho zrušiť, takáto právomoc sa nezaručuje pri vyšetrovacích právomociach alebo právomociach na presadzovanie práva Komisie pre ochranu osobných informácií (pozri článok 7 ods. 1 pododseky 1 a 2 zákona o ochrane osobných informácií). Podľa vysvetlení, ktoré poskytla kórejská vláda, je článok 18 zákona o organizácii verejnej správy určený na to, aby predsedovi vlády poskytol možnosť konať za mimoriadnych okolností, napr. pri riešení nezhôd medzi jednotlivými štátnymi orgánmi. Predseda vlády však túto právomoc od prijatia daného ustanovenia v roku 1963 ešte nikdy nevyužil.

([146]) Ak je potrebné vykonávať úlohy podľa článku 7-9 ods. 1 zákona o ochrane osobných informácií, Komisia pre ochranu osobných informácií si môže vyžiadať stanoviská príslušných verejných činiteľov, odborníkov v oblasti ochrany údajov, organizácií občianskej spoločnosti a príslušných hospodárskych subjektov. Okrem toho si môže Komisia pre ochranu osobných informácií vyžiadať príslušné materiály, môže vydávať odporúčania na zlepšenie a kontrolovať ich vykonávanie (článok 7-9 ods. 2 až 5 zákona o ochrane osobných informácií).

([147]) Pozri aj článok 9 zákona o ochrane osobných informácií (Trojročný dlhodobý plán ochrany osobných informácií), článok 12 zákona o ochrane osobných informácií (Štandardné usmernenia k ochrane osobných informácií), článok 13 zákona o ochrane osobných informácií (Politiky na podporu samoregulácie).

takzvaného call centra pre ochranu súkromia. V súvislosti s riešením sťažností prostredníctvom call centra pre ochranu súkromia postúpi Kórejská agentúra pre internet a bezpečnosť vec Komisii pre ochranu osobných informácií alebo prokuratúre, ak zistí, že bol porušený zákon. Možnosť podania sťažnosti call centru pre ochranu súkromia nebráni jednotlivcom v priamom podaní sťažnosti Komisii pre ochranu osobných informácií ani v kontaktovaní Komisie pre ochranu osobných informácií, ak ich sťažnosť Kórejská agentúra pre internet a bezpečnosť nevyriešila uspokojivo.

2.4.2. *Presadzovanie vrátane sankcií*

(118) S cieľom zabezpečiť dodržiavanie zákona o ochrane osobných informácií priznal zákonodarca Komisii pre ochranu osobných informácií vyšetrovacie právomoci aj právomoci v oblasti presadzovania práva od vydávania odporúčaní až po ukladanie správnych pokút. Tieto právomoci sú doplnené režimom trestnoprávnych sankcií.

(119) V rámci svojich vyšetrovacích právomocí môže Komisia pre ochranu informácií v prípade podozrenia na porušenie alebo oznámenia porušenia zákona o ochrane osobných informácií, prípadne ak je to potrebné na ochranu práv dotknutej osoby pred porušeniami, vykonať inšpekcie na mieste a vyžiadať si od prevádzkovateľov osobných údajov všetky relevantné materiály (ako napríklad články a dokumenty) (článok 63 zákona o ochrane osobných informácií v spojení s článkom 60 vykonávacieho dekrétu k zákonu o ochrane osobných informácií) ([148]).

(120) Pokiaľ ide o presadzovanie práva, podľa článku 61 ods. 2 zákona o ochrane osobných informácií môže Komisia pre ochranu osobných informácií poskytovať odporúčania prevádzkovateľom údajov o zlepšení úrovne ochrany osobných údajov pri konkrétnych činnostiach spracúvania. Prevádzkovatelia údajov sa musia v dobrej viere usilovať tieto odporúčania vykonať a o výsledku tohto úsilia musia informovať Komisiu pre ochranu osobných informácií. Okrem toho, ak existujú opodstatnené dôvody domnievať sa, že došlo k porušeniu zákona o ochrane osobných informácií, pričom neprijatie opatrení pravdepodobne spôsobí škodu, ktorú je ťažké napraviť, Komisia pre ochranu osobných informácií môže uložiť nápravné opatrenia (článok 64 ods. 1 zákona o ochrane osobných informácií) ([149]). V oddiele 5 oznámenia č. 2021-5 (príloha I) sa so záväzným účinkom objasňuje, že tieto podmienky sú splnené vtedy, ak dôjde k porušeniu akéhokoľvek ustanovenia zákona o ochrane osobných informácií, ktorým sa chránia práva na súkromie jednotlivcov v súvislosti s ich osobnými informáciami ([150]). Komisia pre ochranu osobných informácií má právomoc prijať opatrenia ako nariadenie ukončenia konania, ktorým sa porušuje zákon, dočasné pozastavenie spracúvania údajov, ako aj ďalšie potrebné opatrenia. Nevykonanie nápravného opatrenia môže viesť k sankcii v podobe pokuty v maximálnej výške 50 miliónov wonov (článok 75 ods. 2 pododsek 13 zákona o ochrane osobných informácií).

(121) Pokiaľ ide o určité orgány verejnej moci (ako napríklad národné zhromaždenie, ústredné správne orgány, orgány miestnej samosprávy a súdy), v článku 64 ods. 4 zákona o ochrane osobných informácií sa stanovuje, že Komisia pre ochranu osobných informácií môže „odporučiť“ niektoré z nápravných opatrení uvedených v odôvodnení (120) a že tieto orgány musia toto odporúčanie vykonať, ak nenastali mimoriadne okolnosti. Podľa oddielu 5 oznámenia č. 2021-5 sa to týka mimoriadnych skutkových alebo právnych okolností, o ktorých Komisia pre ochranu osobných informácií nevedela pri vydávaní odporúčania. Dotknutý orgán verejnej moci sa môže na takéto mimoriadne okolnosti odvolať len vtedy, ak jednoznačne preukáže, že nedošlo k žiadnemu porušeniu, pričom Komisia pre ochranu osobných informácií stanoví, že takýto prípad skutočne nenastal. Inak musí orgán verejnej moci na základe odporúčania Komisie pre ochranu osobných informácií „prijať nápravné opatrenie vrátane okamžitého ukončenia daného konania a v mimoriadnom prípade, keď napriek tomu dôjde k nezákonnému konaniu, nahradiť vzniknuté škody.“

(122) Komisia pre ochranu osobných informácií môže takisto požiadať iné správne orgány s osobitnou právomocou podľa odvetvových právnych predpisov (napr. v oblasti zdravia, vzdelávania) o vedenie vyšetrovania – samostatne alebo spoločne s Komisiou pre ochranu osobných informácií – (predpokladaných) porušení súkromia prevádzkovateľmi pôsobiacimi v týchto sektoroch v rámci ich jurisdikcie a ukladať nápravné opatrenia (článok 63 ods. 4 až 5 zákona o ochrane osobných informácií). V uvedenom prípade Komisia pre ochranu osobných informácií určí dôvody, predmet a rozsah vyšetrovania ([151]). Tento príslušný správny orgán musí potom predložiť Komisii pre ochranu osobných informácií plán inšpekcie a oznámiť jej výsledky inšpekcie. Komisia pre ochranu osobných informácií môže odporučiť prijatie osobitného nápravného opatrenia, pričom príslušný orgán sa musí usilovať ho vykonať. V každom prípade sa touto žiadosťou neobmedzuje kompetencia Komisie pre ochranu osobných informácií pri vykonávaní vlastného vyšetrovania alebo ukladaní sankcií.

([148]) Komisia pre ochranu osobných informácií môže okrem toho vstúpiť do priestorov prevádzkovateľa s cieľom vykonať inšpekciu stavu podnikateľských činností, záznamov, dokumentov atď. (článok 63 ods. 2 zákona o ochrane osobných informácií). Pozri aj článok 45-3 zákona o používaní a ochrane úverových informácií a článok 36-4 vykonávacieho dekrétu k zákonu o používaní a ochrane úverových informácií, v ktorých sa uvádzajú právomoci Komisie pre ochranu osobných informácií podľa uvedeného zákona.

([149]) Pozri aj článok 45-4 zákona o používaní a ochrane úverových informácií, v ktorom sa uvádzajú právomoci Komisie pre ochranu osobných informácií podľa uvedeného zákona.

([150]) V oddiele 5 oznámenia sa uvádza, že „závažné dôvody domnievať sa, že došlo k porušeniu ochrany osobných informácií, a neprijatie opatrenia, ktoré pravdepodobne spôsobí škodu, ktorú je ťažké napraviť, v zmysle článku 64 ods. 1 a 2 zákona o ochrane osobných informácií, odkazujú na porušenia akýchkoľvek zásad, práv a povinností v zákone, ktoré sa týkajú ochrany práv jednotlivcov na osobné informácie“. To isté sa podľa článku 45-4 zákona o používaní a ochrane úverových informácií uplatňuje na Komisiu pre ochranu osobných informácií.

([151]) Článok 60 vykonávacieho dekrétu k zákonu o ochrane osobných informácií.

(123) Okrem právomocí v oblasti nápravných opatrení má Komisia pre ochranu osobných informácií právomoci aj v oblasti ukladania správnych pokút od 10 do 50 miliónov wonov za porušenia rôznych požiadaviek zákona o ochrane osobných informácií (článok 75 zákona o ochrane osobných informácií) ([152]). Okrem iného ide o nedodržanie požiadaviek na zákonnosť spracúvania, neprijatie potrebných bezpečnostných opatrení, neoznámenie porušenia ochrany údajov dotknutým osobám, nedodržanie požiadaviek na subsprostredkovanie, nezavedenie a nezverejnenie politiky ochrany súkromia, nevymenovanie zodpovednej osoby pre ochranu súkromia alebo nekonanie v prípade žiadosti dotknutej osoby, ktorá si uplatňuje svoje individuálne práva, ako aj o určité procesné porušenia (nespolupráca pri vyšetrovaní). V prípade porušení viacerých ustanovení zákona o ochrane osobných informácií tým istým prevádzkovateľom možno uložiť pokutu za každé porušenie a pri stanovení výšky pokuty sa prihliadne na počet dotknutých jednotlivcov.

(124) Okrem toho, ak existujú opodstatnené dôvody na podozrenie z porušenia zákona o ochrane osobných informácií alebo akýchkoľvek iných „právnych predpisov týkajúcich sa ochrany údajov“, Komisia pre ochranu osobných informácií môže podať trestné oznámenie príslušnému vyšetrovaciemu orgánu (napríklad prokuratúre, pozri článok 65 ods. 1 zákona o ochrane osobných informácií). Ďalej môže Komisia pre ochranu osobných informácií odporučiť prevádzkovateľovi disciplinárne konanie proti zodpovednej osobe (vrátane zodpovedného manažéra, pozri článok 65 ods. 2 zákona o ochrane osobných informácií). Po prijatí musí takéto odporúčanie prevádzkovateľ vykonať ([153]) a Komisii pre ochranu osobných informácií musí písomne oznámiť jeho výsledok (článok 65 zákona o ochrane osobných informácií v spojení s článkom 58 vykonávacieho dekrétu k zákonu o ochrane osobných informácií).

(125) Pokiaľ ide o vydávanie odporúčaní podľa článku 61, nápravné opatrenia podľa článku 64, podávanie trestných oznámení alebo odporúčanie disciplinárneho konania podľa článku 65 a uloženie správnych pokút podľa článku 75 zákona o ochrane osobných informácií, Komisia pre ochranu osobných informácií môže skutočnosti ako porušenie, subjekt, ktorý porušil zákon, a uložené opatrenia zverejniť na svojom webovom sídle alebo všeobecne v celoštátnych novinách (článok 66 zákona o ochrane osobných informácií v spojení s článkom 61 ods. 1 vykonávacieho dekrétu k zákonu o ochrane osobných informácií) ([154]).

(126) A napokon sa dodržiavanie požiadaviek na ochranu údajov zo zákona o ochrane osobných informácií (ako aj ďalších „právnych predpisov o ochrane údajov“) podporuje režimom trestnoprávnych sankcií. V tejto súvislosti obsahujú články 70 až 73 zákona o ochrane osobných informácií ustanovenia o sankciách, z ktorých môžu vyplývať buď pokuty (od 20 do 100 miliónov wonov), alebo trest odňatia slobody (s maximálnou výškou od 2 do 10 rokov). Príslušné porušenia zahŕňajú okrem iného používanie osobných údajov alebo poskytnutie takýchto údajov tretej strane bez potrebného súhlasu, spracúvanie citlivých informácií v rozpore so zákazom z článku 23 ods.1 zákona o ochrane osobných informácií, nedodržanie platných požiadaviek na bezpečnosť, ktorého výsledkom je strata, odcudzenie, odhalenie, sfalšovanie, pozmenenie alebo poškodenie osobných údajov, neprijatie potrebných opatrení na opravu, vymazanie alebo pozastavenie spracúvania osobných údajov alebo nezákonný prenos osobných údajov do tretej krajiny ([155]). Podľa článku 74 zákona o ochrane osobných informácií je v každom z týchto prípadov zodpovedný zamestnanec, obchodný zástupca alebo zástupca prevádzkovateľa, ako aj samotný prevádzkovateľ ([156]).

(127) Okrem trestnoprávnych sankcií uvedených v zákone o ochrane osobných informácií môže nesprávne používanie osobných údajov predstavovať aj trestný čin podľa zákona o trestnom konaní. Je to tak najmä pri porušení listového tajomstva, utajenia dokumentov alebo elektronických záznamov (článok 316), sprístupnenia informácií, na ktoré sa vzťahuje služobné tajomstvo (článok 317), podvodu spáchaného za použitia počítačov (článok 347-2), ako aj sprenevery a narušenia dôvery (článok 355).

(128) V kórejskom systéme sa teda kombinujú rôzne druhy sankcií, od nápravných opatrení a správnych pokút po trestnoprávne sankcie, ktoré budú mať pravdepodobne na prevádzkovateľov a jednotlivcov narábajúcich s údajmi

([152]) Okrem toho, ak systémy na spracúvanie a ochranu osobných informácií, ktoré prevádzkuje prevádzkovateľ, boli certifikované ako kompatibilné so zákonom o ochrane osobných informácií, ale ak kritériá certifikácie podľa článku 34-2 ods. 1 zákona o ochrane osobných informácií neboli v skutočnosti dodržané, alebo v prípade vážneho porušenia „právnych predpisov o ochrane [osobných] informácií“ môže Komisia pre ochranu osobných informácií odňať certifikáciu (článok 32-2 ods. 3 a 5 zákona o ochrane osobných informácií). Komisia pre ochranu osobných informácií oznámi prevádzkovateľovi takéto odobratie a zverejní ho alebo uverejní na svojom webovom sídle, prípadne v Úradnom vestníku (článok 34-4 vykonávacieho dekrétu k zákonu o ochrane osobných informácií). Za porušenie zákona o používaní a ochrane úverových informácií sa takisto môžu uložiť správne pokuty (článok 52 zákona o používaní a ochrane úverových informácií) a trestnoprávne sankcie (článok 50 zákona o používaní a ochrane úverových informácií).

([153]) Podľa článku 58 ods. 2 vykonávacieho dekrétu k zákonu o ochrane osobných informácií musí prevádzkovateľ Komisii pre ochranu osobných informácií predložiť opodstatnené dôvody, ak sa pre osobitné okolnosti považuje vykonanie odporúčania za „nepraktické“.

([154]) Pri rozhodovaní o tom, či vykonať takéto zverejnenie, prihliadne Komisia pre ochranu osobných informácií na podstatu a závažnosť porušenia, jeho dĺžku a frekvenciu, ako aj na jeho dôsledky (rozsah škôd). Dotknutý subjekt bude vopred informovaný a bude mať príležitosť sa brániť. Pozri článok 61 ods. 2 a 3 vykonávacieho dekrétu k zákonu o ochrane osobných informácií.

([155]) Pozri článok 71 pododsek 2 v spojení s článkom 18 ods. 1 zákona o ochrane osobných informácií (nedodržanie podmienok z článku 17 ods. 3 zákona o ochrane osobných informácií, na ktorý odkazuje článok 18 ods. 1). Pozri aj článok 75 ods. 2 pododsek 1 v spojení s článkom 17 ods. 2 zákona o ochrane osobných informácií (neposkytnutie potrebných informácií dotknutému jednotlivcovi podľa článku 17 ods. 2 zákona o ochrane osobných informácií, na ktorý odkazuje článok 17 ods. 3).

([156]) Okrem toho sa v článku 74-2 zákona o ochrane osobných informácií umožňuje skonfiškovanie všetkých peňazí, tovaru alebo iných ziskov nadobudnutých v dôsledku porušenia zákona alebo ak skonfiškovanie nie je možné, „odobratie“ nezákonne získaného prospechu.

osobitne silný odrádzajúci účinok. Ihneď po svojom zriadení v roku 2020 začala Komisia pre ochranu osobných informácií tieto právomoci využívať. Z výročnej správy Komisie pre ochranu osobných informácií z roku 2021 vyplýva, že Komisia pre ochranu osobných informácií už vydala niekoľko odporúčaní, uložila niekoľko správnych pokút a nápravných opatrení proti verejnému sektoru (približne 34 verejným orgánom), ako aj súkromným prevádzkovateľom (približne 140 spoločnostiam) ([157]). Dôležité prípady zahŕňajú napríklad uloženie pokuty vo výške 6,7 miliardy wonov spoločnosti za porušenie rôznych ustanovení zákona o ochrane osobných informácií (vrátane požiadaviek na bezpečnosť, požiadaviek na súhlas na poskytnutie informácií tretej strane a transparentnosť) v decembri 2020 ([158]) a pokuty vo výške 103,3 miliónov wonov technologickej spoločnosti pôsobiacej v oblasti umelej inteligencie (okrem porušenia iných ustanovení za porušenie pravidiel týkajúcich sa zákonnosti spracúvania, konkrétne súhlasu, a spracúvania pseudonymizovaných informácií) v apríli 2021 ([159]). Komisia pre ochranu osobných informácií v auguste 2021 uzavrela ďalšie vyšetrovanie činností troch spoločností, ktoré viedlo k nápravným opatreniam a uloženiu pokút vo výške až 6,47 miliardy wonov (okrem iného za neinformovanie jednotlivcov o sprístupnení osobných údajov tretím stranám vrátane prenosov do tretích krajín) ([160]). Takisto platí, že už pred nedávnou reformou venovala Južná Kórea veľkú pozornosť presadzovaniu práva, pričom zodpovedné orgány využívali v prípade najrôznejších prevádzkovateľov vrátane poskytovateľov komunikačných služieb (Kórejská komisia pre komunikácie), ako aj obchodných subjektov, finančných inštitúcií, orgánov verejnej moci, univerzít a nemocníc (ministerstvo vnútra a bezpečnosti) širokú škálu opatrení na presadzovanie práva vrátane správnych pokút, nápravných opatrení a „zverejňovania porušiteľov“ ([161]). Vzhľadom na to Komisia dospela k záveru, že kórejský systém zabezpečuje účinné presadzovanie pravidiel ochrany údajov v praxi, a tak sa zabezpečuje úroveň ochrany v zásade zodpovedajúca nariadeniu (EÚ) 2016/679.

2.5. **Prostriedky nápravy**

(129) V záujme zabezpečenia primeranej ochrany, a najmä uplatňovania individuálnych práv, by dotknutá osoba mala mať k dispozícii účinné správne a súdne prostriedky nápravy vrátane náhrady škôd.

(130) V kórejskom systéme sa jednotlivcom poskytujú rôzne mechanizmy na účinné uplatňovanie svojich práv a dosiahnutie prostriedkov (súdnej) nápravy.

(131) Jednotlivci, ktorí sa domnievajú, že došlo k porušeniu ich práv na ochranu údajov alebo poškodeniu ich záujmov, sa môžu najskôr obrátiť na príslušného prevádzkovateľa. Podľa článku 30 ods. 1 pododseku 5 zákona o ochrane osobných informácií obsahuje politika ochrany súkromia vypracovaná prevádzkovateľom okrem iného informácie o právach dotknutých osôb a o ich uplatňovaní. Okrem toho obsahuje kontaktné informácie ako meno a telefónne číslo zodpovednej osoby pre ochranu súkromia alebo útvaru zodpovedného za ochranu údajov, aby bolo možné podávať sťažnosti („podnety“). Zodpovedná osoba pre ochranu súkromia v rámci organizácie má na starosti riešenie sťažností, prijímanie nápravných opatrení v prípade porušenia ochrany súkromia a naprávanie škôd (článok 31 ods. 2 pododsek 3 a článok 31 ods. 4 zákona o ochrane osobných informácií). Naprávanie škôd sa týka napríklad prípadu porušenia ochrany údajov, keďže prevádzkovateľ musí informovať dotknutú osobu okrem iného o kontaktnom mieste na nahlásenie škody (článok 34 ods. 1 pododsek 5 zákona o ochrane osobných informácií).

(132) Okrem toho sa v zákone o ochrane osobných informácií uvádza viacero možností, ako môžu jednotlivci dosiahnuť prostriedok nápravy proti prevádzkovateľom. Po prvé môže jednotlivec, ktorý sa domnieva, že prevádzkovateľ porušil jeho práva na ochranu údajov alebo záujmov, oznámiť takéto porušenie priamo Komisii pre ochranu osobných informácií a/alebo niektorej zo špecializovaných inštitúcií určenej Komisiou pre ochranu osobných informácií na prijímanie a riešenie sťažností; môže to byť napríklad Kórejská agentúra pre internet a bezpečnosť, ktorá na tento účel prevádzkuje call centrum pre porušovanie ochrany osobných informácií (takzvané „call centrum pre ochranu súkromia“) (článok 62 ods. 1 a 2 zákona o ochrane osobných informácií v spojení s článkom 59 vykonávacieho dekrétu k zákonu o ochrane osobných informácií). Call centrum pre ochranu súkromia vyšetruje a konštatuje porušenia, poskytuje poradenstvo v súvislosti so spracúvaním osobných

([157]) Pozri výročnú správu Komisie pre ochranu osobných informácií z roku 2021, s. 50 – 55 (k dispozícii iba v kórejčine) na stránke https://www.pipc.go.kr/np/cop/bbs/selectBoardArticle.do?bbsId=BS074&mCode=C020010000&nttId=7511#LINK.

([158]) Pozri na stránke (k dispozícii iba v kórejčine) https://www.pipc.go.kr/np/cop/bbs/selectBoardArticle.do?bbsId=BS074&mCode=C020010000&nttId=6954#LINK.

([159]) Pozri na stránke (k dispozícii iba v kórejčine) https://www.pipc.go.kr/np/cop/bbs/selectBoardArticle.do?bbsId=BS074&mCode=C020010000&nttId=7298&fbclid=IwAR3SKcMQi6G5pR9k4l7j6GNXtc8aBVDOwcURevvvzQtYI7AS40UKYXoOXo8.

([160]) Pozri na stránke (k dispozícii iba v kórejčine): https://www.pipc.go.kr/np/cop/bbs/selectBoardArticle.do?bbsId=BS074&mCode=C020010000&nttId=7497#LINK.

([161]) Pozri napríklad výročnú správu za rok 2020 na stránke (k dispozícii iba v kórejčine) https://www.pipc.go.kr/np/cop/bbs/selectBoardList.do?bbsId=BS079&mCode=D070020000 a príklady uvedené v angličtine na stránke https://www.privacy.go.kr/eng/enforcement_02.do.

údajov (článok 62 ods. 3 zákona o ochrane osobných informácií) a môže oznamovať porušenia Komisii pre ochranu osobných informácií (ako také však nemôže prijímať opatrenia na presadzovanie). Call centrum pre ochranu súkromia dostáva vysoký počet sťažností/žiadostí (napr. 177 457 v roku 2020; 159 255 v roku 2019 a 164 497 v roku 2018) ([162]). Podľa informácií, ktoré poskytla Komisia pre ochranu osobných informácií, samotná Komisia pre ochranu osobných informácií dostala v období od augusta 2020 do augusta 2021 okolo 1 000 žiadostí. V reakcii na sťažnosť môže Komisia pre ochranu osobných informácií vydávať odporúčania o zlepšeniach, nápravných opatreniach, podávaní trestných oznámení príslušnému vyšetrovaciemu orgánu (napríklad prokuratúre) alebo odporúčania o disciplinárnych konaniach (pozri články 61, 64 a 65 zákona o ochrane osobných informácií). Rozhodnutia Komisie o ochrane osobných informácií (napríklad zamietnutie riešenia sťažnosti alebo zamietnutie merita sťažnosti) možno napadnúť podľa Správneho súdneho poriadku ([163]).

(133) Po druhé môžu dotknuté osoby svoje nároky predložiť podľa článkov 40 až 50 zákona o ochrane osobných informácií v spojení s článkami 48-18 až 57 vykonávacieho dekrétu k zákonu o ochrane osobných informácií takzvanému „Výboru pre mediáciu sporov“, ktorý pozostáva zo zástupcov menovaných predsedom Komisie pre ochranu osobných informácií spomedzi členov riadiaceho útvaru Komisie pre ochranu osobných informácií a jednotlivcov menovaných na základe ich skúseností v oblasti ochrany údajov spomedzi určitých oprávnených skupín (pozri článok 40 ods. 2, 3 a 7 zákona o ochrane osobných informácií, článok 48-14 vykonávacieho dekrétu k zákonu o ochrane osobných informácií) ([164]). Možnosť využiť mediáciu pred Výborom pre mediáciu sporov poskytuje alternatívnu možnosť dosiahnutia nápravy, neobmedzuje však právo jednotlivca obrátiť sa namiesto toho na Komisiu pre ochranu osobných informácií alebo súdy. S cieľom preskúmať prípad môže výbor požiadať strany sporu o predloženie potrebných materiálov a/alebo predvolať príslušných svedkov (článok 45 zákona o ochrane osobných informácií). Po objasnení veci vypracuje výbor návrh mediačného riešenia ([165]), na ktorom sa musí zhodnúť väčšina jeho členov. Návrh mediácie môže obsahovať ukončenie porušovania zákona, potrebné prostriedky nápravy (vrátane návratu do pôvodného stavu alebo náhrady škody), ako aj iné opatrenia potrebné na zabránenie opakovaniu toho istého alebo podobného porušenia (článok 47 ods. 1 zákona o ochrane osobných informácií). Ak s mediačným riešením obe strany súhlasia, bude mať rovnaký účinok ako súdny zmier (článok 47 ods. 5 zákona o ochrane osobných informácií). Ani jednej strane sa nebráni podať počas prebiehajúcej mediácie žalobu na súd, pričom v takom prípade bude mediácia prerušená (pozri článok 48 ods. 2 zákona o ochrane osobných informácií) ([166]). Z výročných údajov, ktoré predložila Komisia pre ochranu osobných údajov, vyplýva, že jednotlivci pravidelne využívajú tento postup pred Výborom pre mediáciu sporov, čo často vedie k úspešnému výsledku. Napríklad v roku 2020 výbor riešil 126 prípadov, pričom 89 z nich sa vyriešilo pred výborom (v 77 prípadoch strany dosiahli dohodu už pred skončením mediácie a v 12 prípadoch strany súhlasili s návrhom na mediáciu), a teda miera mediácie dosiahla úroveň 70,6 % ([167]). Podobne v roku 2019 výbor riešil 139 prípadov, z ktorých sa vyriešilo 92, a teda miera mediácie dosiahla úroveň 62,2 %.

(134) Okrem toho, ak rovnakým alebo podobným spôsobom po výskyte toho istého (druhu) incidentu utrpí škodu aspoň 50 jednotlivcov alebo boli poškodené práva na ochranu ich údajov ([168]), dotknutá osoba alebo organizácia na ochranu údajov môže v mene celej skupiny podať žiadosť o kolektívnu mediáciu sporu; k takejto mediácii sa môžu pripojiť ďalšie dotknuté osoby, pričom Výbor pre mediáciu sporov to verejne oznámi (článok 49 ods. 1 až 3 zákona o ochrane osobných informácií v spojení s článkami 52 až 54 vykonávacieho dekrétu k zákonu o ochrane osobných informácií) ([169]). Výbor pre mediáciu sporov môže vybrať aspoň jednu osobu, ktorá bude

([162]) Pozri výročnú správu Komisie pre ochranu informácií z roku 2021, s. 174. V roku 2020 sa tieto sťažnosti týkali napríklad získavania údajov bez súhlasu, nedodržania požiadaviek na transparentnosť, porušení zákona o ochrane osobných informácií sprostredkovateľmi, nedostatočných bezpečnostných opatrení, nereagovaním na žiadosti predložené dotknutými osobami, ako aj všeobecných vyšetrovaní.

([163]) Konkrétne sa môžu jednotlivci odvolať proti výkonu alebo zamietnutiu výkonu verejnej moci správnym orgánom (článok 2 ods. 1 pododsek 1, článok 3 pododsek 1 Správneho súdneho poriadku). Podrobnejšie informácie o procesných aspektoch vrátane požiadaviek na prípustnosť sa uvádzajú v odôvodnení (181).

([164]) Všetci členovia musia mať pevne stanovené funkčné obdobie a môžu byť odvolaní len z opodstatnených dôvodov (pozri článok 40 ods. 5 a článok 41 zákona o ochrane osobných informácií). Ďalej sa v článku 42 zákona o ochrane osobných informácií uvádzajú záruky na ochranu pred konfliktmi záujmov.

([165]) Pozri článok 44 zákona o ochrane osobných informácií. Okrem toho môže vypracovať návrh riešenia sporu a odporučiť riešenie sporu bez mediácie (pozri článok 46 zákona o ochrane osobných informácií).

([166]) Okrem toho môže výbor odmietnuť mediáciu, ak sa domnieva, že nie je primerané riešiť spor takejto povahy mediáciou, alebo ak bola žiadosť o mediáciu podaná na nekalý účel (článok 48 zákona o ochrane osobných informácií).

([167]) Pozri výročnú správu Komisie pre ochranu informácií z roku 2021, s. 179 – 180. Tieto prípady sa týkali okrem iného porušení požiadavky na získanie súhlasu na získavanie údajov, zásady obmedzenia účelu a práv dotknutých osôb.

([168]) Pozri článok 49 ods. 1 zákona o ochrane osobných informácií, podľa ktorého musia dotknuté osoby utrpieť škodu alebo porušenie svojich práv „rovnakým alebo podobným spôsobom“, a článok 52 pododsek 2 vykonávacieho dekrétu k zákonu o ochrane osobných informácií, v ktorom sa vyžaduje, aby mali „hlavné problémy v dôsledku incidentu spoločnú skutkovú alebo právnu podstatu“.

([169]) Okrem toho aj strany, ktoré nie sú stranami mediácie, môžu využiť riešenie kolektívnej mediácie sporu, ktoré prijal sprostredkovateľ, pričom Výbor pre mediáciu sporov môže sprostredkovateľovi odporučiť, aby vypracoval a predložil plán náhrady škody, ktorý sa vzťahuje (aj) na ne (článok 49 ods. 5 zákona o ochrane osobných informácií).

najprimeranejšie zastupovať spoločný záujem ako zastupujúca strana (článok 49 ods. 4 zákona o ochrane osobných informácií). Ak prevádzkovateľ kolektívnu mediáciu sporov odmietne alebo neprijme mediačné riešenie, niektoré organizácie ([170]) môžu na vyriešenie porušenia práva podať skupinovú žalobu (články 51 až 57 zákona o ochrane osobných informácií).

(135) Po tretie má dotknutá osoba v prípade porušenia súkromia, ktoré jej spôsobilo „škodu“, právo na „rýchly a spravodlivý postup“ pri priznávaní primeraného prostriedku nápravy (článok 4 pododsek 5 a článok 39 zákona o ochrane osobných informácií) ([171]). Prevádzkovateľ sa môže zbaviť zodpovednosti, ak dokáže neexistenciu zavinenia („zlého úmyslu“ alebo nedbanlivosti). Ak dotknutá osoba utrpí škodu v dôsledku straty, odcudzenia, odhalenia, sfalšovania, pozmenenia alebo poškodenia svojich osobných údajov, súd môže stanoviť náhradu škody vo výške trojnásobku skutočnej škody, pričom prihliadne na viacero faktorov (článok 39 ods. 3 a 4 zákona o ochrane osobných informácií). Alternatívne môže dotknutá osoba žiadať o „primeranú výšku“ náhrady škody, ktorá nepresahuje 3 milióny wonov (článok 39-2 ods. 1 a 2 zákona o ochrane osobných informácií). Okrem toho podľa Občianskeho zákonníka možno podať nárok na náhradu škody proti každej osobe, „ktorá spôsobí straty alebo ujmu inej osobe nezákonným konaním, či už úmyselne, alebo z nedbanlivosti“ ([172]), prípadne proti osobe, „ktorá poškodila osobnú integritu, slobodu alebo dobré meno inej osoby, prípadne inej osobe spôsobila psychickú ujmu“ ([173]). Takúto zodpovednosť za škody vyplývajúce z porušenia pravidiel ochrany údajov potvrdil najvyšší súd ([174]). Ak bola škoda spôsobená nezákonným konaním verejného orgánu, nárok na náhradu škody možno ďalej podať na základe zákona o štátnom odškodnení ([175]). Nárok možno podľa zákona o štátnom odškodnení podať špecializovanej Rade pre odškodnenie alebo priamo na kórejských súdoch ([176]). Zodpovednosť štátu sa týka aj inej ako materiálnej škody (napríklad duševného utrpenia) ([177]). Ak je obeťou cudzí štátny príslušník, zákon o štátnom odškodnení sa naňho vzťahuje vtedy, ak jeho krajina pôvodu rovnako zabezpečuje štátne odškodnenie pre štátnych príslušníkov Kórey ([178]).

(136) Po štvrté najvyšší súd uznal, že jednotlivci majú právo žiadať o vydanie súdneho príkazu ukladajúceho povinnosť zdržať sa porušovania ich ústavných práv, a to aj práva na ochranu osobných údajov ([179]). V tejto súvislosti môže súd napríklad nariadiť prevádzkovateľom pozastaviť alebo ukončiť vykonávanie každej nezákonnej činnosti. Okrem toho možno práva na ochranu údajov vrátane práv chránených zákonom o ochrane osobných informácií uplatňovať prostredníctvom občianskych žalôb. Toto horizontálne uplatňovanie ústavnej ochrany súkromia na vzťahy medzi súkromnými stranami uznal najvyšší súd ([180]).

([170]) Konkrétne skupiny spotrebiteľov alebo mimovládne organizácie určitej veľkosti v zmysle počtu členov, ktorých stanoveným účelom je ochrana údajov (hoci v prípade MVO platí ďalšia požiadavka, aby aspoň 100 dotknutých osôb, ktorých práva boli rovnako porušené, podalo žiadosť o podanie skupinovej žaloby). Pozri článok 51 zákona o ochrane osobných informácií.

([171]) V článkoch 43 až 43-3 zákona o použití a ochrane úverových informácií sa takisto stanovuje povinnosť náhrady škody za škody vyplývajúce z porušení uvedeného zákona.

([172]) Článok 750 Občianskeho zákonníka.

([173]) Článok 751 ods. 1 Občianskeho zákonníka.

([174]) Pozri napríklad rozhodnutia najvyššieho súdu č. 2015Da251539, č. 251546, č. 251553, č. 251560, č. 251577 z 30. mája 2018. Okrem toho najvyšší súd potvrdil, že porušenia ochrany údajov môžu viesť k uloženiu povinnosti náhrady škody podľa Občianskeho zákonníka, pozri rozhodnutia najvyššieho súdu č. 2011Da59834, č. 59858, č. 59841 z 26. decembra 2012 (anglické zhrnutie je k dispozícii na adrese http://library.scourt.go.kr/SCLIB_data/decision/9-69%202012.12.26.2011Da59834.htm). V tomto prípade najvyšší súd objasnil, že na posúdenie toho, či jednotlivec utrpel emocionálnu úzkosť, ktorú možno považovať za odškodniteľnú, je potrebné zohľadniť viacero faktorov, ako napríklad druh a vlastnosti informácií, ktoré unikli, identifikovateľnosť jednotlivca v dôsledku porušenia ochrany údajov, možnosť prístupu k údajom tretími stranami, rozsah, v akom sa osobné informácie šírili, či to viedlo k nejakému ďalšiemu poškodeniu individuálnych práv, ako sa osobné informácie riadili a chránili, atď.

([175]) Na základe zákona o štátnom odškodnení môžu jednotlivci žiadať o náhradu škody za škody spôsobené verejnými činiteľmi pri výkone ich úradných povinností v rozpore so zákonom (článok 2 ods. 1 zákona).

([176]) Články 9 a 12 zákona o štátnom odškodnení. Zákonom sa zriaďujú okresné rady (ktorým predsedá zástupca prokurátora príslušnej prokuratúry), ústredná rada (ktorej predsedá námestník ministra spravodlivosti) a osobitná rada (zodpovedajúca za nároky na náhradu škody za škody spôsobené vojenským personálom alebo civilnými zamestnancami armády a ktorej predsedá námestník ministra národnej obrany). Nároky na náhradu škody v zásade vybavujú okresné rady, ktoré môžu za určitých okolností postúpiť prípady ústrednej/osobitnej rade, napr. ak náhrada škody presahuje určitú sumu alebo ide o žiadosť jednotlivca o opätovné preskúmanie. Všetky rady pozostávajú z členov menovaných ministrom spravodlivosti (napr. spomedzi verejných činiteľov ministerstva spravodlivosti, súdnych úradníkov, právnikov a osôb s odbornými znalosťami v oblasti štátneho odškodnenia) a vzťahujú sa na ne osobitné pravidlá v oblasti konfliktu záujmov (pozri článok 7 vykonávacieho dekrétu k zákonu o štátnom odškodnení).

([177]) Pozri článok 8 zákona o štátnom odškodnení (v ktorom sa odkazuje na Občiansky zákonník), ako aj článok 751 Občianskeho zákonníka.

([178]) Článok 7 zákona o štátnom odškodnení.

([179]) Rozhodnutie najvyššieho súdu č. 93Da40614 z 12. apríla 1996 a rozhodnutie č. 2008Da42430 z 2. septembra 2011 (anglické zhrnutie je k dispozícii na adrese https://www.scourt.go.kr/eng/supreme/decisions/NewDecisionsView.work?seq=696&pageIndex=1&mode=6&searchWord=).

([180]) Pozri napríklad rozhodnutie najvyššieho súdu č. 2008Da42430 z 2. septembra 2011 (anglické zhrnutie je k dispozícii na adrese https://www.scourt.go.kr/eng/supreme/decisions/NewDecisionsView.work?seq=696&pageIndex=1&mode=6&searchWord=).

(137) A napokon môžu jednotlivci podať prokurátorovi alebo príslušníkovi justičnej polície trestné oznámenie na základe zákona o trestnom konaní (článok 223) ([181]).

(138) Kórejský systém teda poskytuje viacero možností na dosiahnutie prostriedku nápravy od jednoducho dostupných a nízkonákladových možností [napríklad kontaktovania call centra pre ochranu súkromia alebo (kolektívnej) mediácie] po správne (pred Komisiou pre ochranu osobných informácií) a súdne možnosti vrátane možnosti získať náhradu škody.

3. PRÍSTUP K OSOBNÝM ÚDAJOM PRENÁŠANÝM Z EURÓPSKEJ ÚNIE ORGÁNMI VEREJNEJ MOCI V KÓREJSKEJ REPUBLIKE A ICH POUŽÍVANIE TÝMITO ORGÁNMI

(139) Komisia takisto posúdila obmedzenia a záruky vrátane mechanizmov dozoru a individuálnych prostriedkov nápravy, ktoré sú v kórejskom práve k dispozícii vo vzťahu k získavaniu a následnému používaniu osobných údajov prenášaných prevádzkovateľmi v Kórei, ktoré vo verejnom záujme uskutočňujú kórejské orgány verejnej moci, a to najmä na účely presadzovania práva v trestných veciach a na účely národnej bezpečnosti (ďalej len „prístup vlády“). Kórejská vláda poskytla Komisii v tejto súvislosti oficiálne vyhlásenia, uistenia a záväzky podpísané na najvyššej úrovni ministerstiev a orgánov, ktoré sú uvedené v prílohe II k tomuto rozhodnutiu.

(140) Komisia pri posudzovaní toho, či podmienky, na základe ktorých sa vláde poskytuje prístup k údajom prenášaným do Kórey podľa tohto rozhodnutia, spĺňajú kritérium „zásadnej rovnocennosti“ v súlade s článkom 45 ods. 1 nariadenia (EÚ) 2016/679, ako ho vykladá Súdny dvor Európskej únie so zreteľom na Chartu základných práv, zohľadnila najmä tieto kritériá.

(141) Po prvé akékoľvek obmedzenie práva na ochranu osobných údajov musí byť stanovené zákonom a v samotnom právnom základe, ktorý povoľuje zasahovanie do takéhoto práva, sa musí vymedziť, v akom rozsahu možno uplatňovanie príslušného práva obmedziť ([182]).

(142) Po druhé v záujme splnenia požiadavky proporcionality, podľa ktorej sa v demokratickej spoločnosti musia výnimky z ochrany osobných údajov a obmedzenia ochrany osobných údajov uplatňovať len do prísne nevyhnutnej miery, aby boli splnené konkrétne ciele všeobecného záujmu, ktoré sú rovnocenné s cieľmi uznávanými Úniou, sa v právnych predpisoch dotknutej tretej krajiny povoľujúcich zasahovanie musia stanovovať jasné a presné pravidlá upravujúce rozsah a uplatňovanie takýchto opatrení a zavádzať minimálne záruky, aby osoby, ktorých údaje boli prenesené, mali dostatočné záruky umožňujúce účinne chrániť ich osobné údaje pred rizikom zneužitia ([183]). V týchto právnych predpisoch sa musia najmä vymedziť okolnosti a podmienky, za ktorých možno prijať opatrenie upravujúce spracúvanie takýchto údajov ([184]), ako aj stanoviť povinnosť podrobiť splnenie takých požiadaviek nezávislému dozoru ([185]).

(143) Po tretie musia byť právne predpisy a ich požiadavky vo vnútroštátnom práve právne záväzné. Týka sa to predovšetkým orgánov predmetnej tretej krajiny, ale tieto právne požiadavky musia byť proti týmto orgánom uplatniteľné aj na súdoch ([186]). Dotknuté osoby musia mať najmä možnosť uplatniť právne prostriedky nápravy pred nezávislým a nestranným súdom, aby mali prístup k svojim osobným údajom, alebo dosiahnuť opravu alebo vymazanie takýchto údajov ([187]).

3.1. **Všeobecný právny rámec**

(144) Obmedzenia a záruky, ktoré sa uplatňujú na získavanie a následné používanie osobných údajov kórejskými orgánmi verejnej moci vyplývajú zo všeobecného ústavného rámca, osobitných zákonov, v ktorých sa upravujú ich činnosti v oblasti presadzovania práva v trestných veciach a v oblasti národnej bezpečnosti, ako aj z pravidiel, ktoré sa osobitne uplatňujú na spracúvanie osobných údajov.

([181]) Ako sa vysvetľuje v odôvodnení (127), nesprávne používanie údajov môže podľa zákona o trestnom konaní predstavovať trestný čin.

([182]) Pozri vec Schrems II, body 174 – 175 a citovanú judikatúru. Čo sa týka prístupu orgánov verejnej moci členských štátov, pozri aj vec C-623/17 Privacy International, ECLI:EU:C:2020:790, bod 65; a spojené veci C-511/18, C-512/18 a C-520/18 La Quadrature du Net a i., ECLI:EU:C:2020:791, bod 175.

([183]) Pozri vec Schrems II, body 176 a 181, ako aj citovanú judikatúru. Pokiaľ ide o prístup orgánov verejnej moci členských štátov, pozri aj vec Privacy International, bod 68; a La Quadrature du Net a i., bod 132.

([184]) Pozri vec Schrems II, bod 176. Pokiaľ ide o prístup orgánov verejnej moci členských štátov, pozri aj vec Privacy International, bod 68; a La Quadrature du Net a i., bod 132.

([185]) Pozri vec Schrems II, bod 179.

([186]) Pozri vec Schrems II, body 181 – 182.

([187]) Pozri vec Schrems I, bod 95 a vec Schrems II, bod 194. V tejto súvislosti Súdny dvor Európskej únie zdôraznil najmä to, že dodržiavanie článku 47 Charty základných práv, v ktorom sa zaručuje právo na účinný prostriedok nápravy pred nezávislým a nestranným súdom, „prispieva k úrovni ochrany požadovanej v rámci Únie a […] Komisia [ho musí] konštatovať skôr, než prijme rozhodnutie o primeranosti podľa článku 45 ods. 1 nariadenia“ (EÚ) 2016/679 (vec Schrems II, bod 186).

(145) Po prvé sa prístup kórejských orgánov verejnej moci k osobným údajom upravuje vo všeobecných zásadách zákonnosti, nevyhnutnosti a primeranosti, ktoré vyplývajú z kórejskej ústavy ([188]). Konkrétne možno základné práva a slobody (vrátane práva na súkromie a práva na súkromie korešpondencie) ([189]) obmedziť len zákonom a vtedy, ak je to potrebné z dôvodu národnej bezpečnosti alebo udržania verejného poriadku pre blaho verejnosti. Takéto obmedzenia nemôžu mať vplyv na podstatu predmetného práva alebo slobody. V ústave sa stanovuje, že najmä prehliadky a zaistenia predmetov možno vykonávať len podľa ustanovení zákona na základe príkazu vydaného sudcom a pri dodržaní riadneho postupu ([190]). A napokon sa môžu jednotlivci dovolávať svojich práv a slobôd na ústavnom súde, ak sa domnievajú, že ich orgány verejnej moci pri výkone svojich právomocí porušili ([191]). Podobne jednotlivci, ktorí utrpeli ujmu z dôvodu nezákonného konania, ktorého sa dopustil verejný činiteľ v priebehu vykonávania úradných povinností, majú právo podať nárok na spravodlivú náhradu škody ([192]).

(146) Po druhé, ako sa podrobnejšie opisuje v oddieloch 3.2.1 a 3.3.1, všeobecné zásady uvedené v odôvodnení (145) sa premietajú aj do osobitných zákonov, v ktorých sa upravujú právomoci orgánov presadzovania práva a orgánov národnej bezpečnosti. Pokiaľ ide o vyšetrovanie trestnej činnosti, v zákone o trestnom konaní sa napríklad stanovuje, že povinné opatrenia možno prijať len vtedy, ak sú výslovne uvedené v zákone o trestnom konaní, a len v rozsahu potrebnom na dosiahnutie účelu vyšetrovania ([193]). Podobne sa v článku 3 zákona o ochrane súkromia komunikácie zakazuje prístup k súkromnej komunikácii okrem situácie, ak sa uskutočňuje na základe zákona a vzťahujú sa naň obmedzenia a záruky stanovené v zákone. V oblasti národnej bezpečnosti sa v zákone o Národnej spravodajskej službe stanovuje, že každý prístup ku komunikácii alebo informáciám o polohe musí byť v súlade so zákonom, pričom na zneužitie právomoci a porušenia zákona sa vzťahujú trestnoprávne sankcie ([194]).

(147) Po tretie spracúvanie osobných údajov verejnými orgánmi, a to aj na účely presadzovania práva a národnej bezpečnosti, podlieha pravidlám ochrany údajov podľa zákona o ochrane osobných informácií ([195]). Vo všeobecnosti sa v článku 5 ods. 1 zákona o ochrane osobných informácií vyžaduje, aby orgány verejnej moci vypracovali politiky na zabránenie „zneužívaniu a nesprávnemu používaniu osobných informácií, nepovolenému sledovaniu atď. a na posilnenie dôstojnosti ľudských bytostí a súkromia jednotlivcov“. Okrem toho musí každý prevádzkovateľ spracúvať osobné údaje tak, aby sa minimalizovala možnosť porušenia súkromia dotknutej osoby (článok 3 ods. 6 zákona o ochrane osobných informácií).

(148) Všetky požiadavky zákona o ochrane osobných informácií, ktoré sú podrobne opísané v oddiele 2, sa uplatňujú na spracúvanie osobných údajov na účely presadzovania práva. Patria k nim základné zásady (ako je zákonnosť a spravodlivosť, obmedzenie účelu, presnosť, minimalizácia údajov, obmedzenie ukladania, bezpečnosť a transparentnosť), povinnosti (napríklad v súvislosti s oznamovaním porušenia ochrany údajov a s citlivými údajmi) a práva (na získanie prístupu, opravu, vymazanie a pozastavenie spracúvania údajov).

(149) Zatiaľ čo spracúvanie osobných údajov na účely národnej bezpečnosti podlieha obmedzenejšiemu súboru ustanovení na základe zákona o ochrane osobných informácií, uplatňujú sa základné zásady, ako aj pravidlá v oblasti dozoru, presadzovania a nápravy ([196]). Konkrétnejšie v článkoch 3 a 4 zákona o ochrane osobných informácií sa stanovujú všeobecné zásady ochrany údajov (zákonnosť a spravodlivosť, obmedzenie účelu, presnosť, minimalizácia údajov, bezpečnosť a transparentnosť) a individuálne práva (právo na informácie, právo na prístup a práva na opravu, vymazanie a pozastavenie spracúvania údajov) ([197]). V článku 4 ods. 5 zákona o ochrane osobných informácií sa ďalej stanovujú jednotlivci s právom na primeranú nápravu všetkých škôd vyplývajúcich zo spracúvania ich osobných údajov na základe rýchleho a spravodlivého postupu. Dopĺňajú to konkrétnejšie povinnosti

([188]) Pozri prílohu II oddiel 1.1.
([189]) Článok 37 ods. 2 ústavy.
([190]) Článok 16 a článok 12 ods. 3 ústavy. V článku 12 ods. 3 ústavy sa ďalej stanovujú mimoriadne okolnosti, za ktorých možno vykonať prehliadky alebo zaistenia predmetov bez súdneho príkazu (hoci sa stále vyžaduje vydanie súdneho príkazu *ex post*), t. j. *flagrante delicto* alebo trestné činy, za ktoré hrozí odňatie slobody v trvaní aspoň tri roky, ak existuje riziko zničenia dôkazov alebo úteku podozrivého.
([191]) Článok 68 ods. 1 zákona o ústavnom súde.
([192]) Článok 29 ods. 1 ústavy.
([193]) Článok 199 ods. 1 zákona o trestnom konaní. Všeobecnejšie musia orgány verejnej moci pri výkone svojich právomocí podľa zákona o trestnom konaní dodržiavať základné práva osôb podozrivých z trestnej činnosti a všetkých ďalších dotknutých osôb (článok 198 ods. 2 zákona o trestnom konaní).
([194]) Článok 14 zákona o Národnej spravodajskej službe.
([195]) Pozri prílohu II oddiel 1.2.
([196]) Článok 58 ods. 1 pododsek 2 zákona o ochrane osobných informácií. Pozri aj oddiel 6 oznámenia č. 2021-5 (príloha I). Táto výnimka z určitých ustanovení zákona o ochrane osobných informácií sa uplatňuje len vtedy, ak sa osobné údaje spracúvajú „na účely národnej bezpečnosti“. Po skončení situácie súvisiacej s národnou bezpečnosťou, ktorou sa odôvodňovalo spracúvanie údajov, už nemožno využívať výnimku a uplatňujú sa všetky požiadavky zákona o ochrane osobných informácií.
([197]) Takéto práva možno obmedziť len vtedy, ak sa to stanovuje v zákone, a to v takom rozsahu a na tak dlho, ako je to potrebné a primerané na ochranu dôležitého cieľa verejného záujmu, alebo ak by priznanie tohto práva mohlo spôsobiť ujmu na živote alebo fyzickej integrite tretej strany alebo neopodstatnené poškodenie majetku a iných záujmov tretej strany. Pozri oddiel 6 oznámenia č. 2021-5.

spracúvať osobné údaje len v minimálnom rozsahu potrebnom na dosiahnutie zamýšľaného účelu a počas minimálneho obdobia, zaviesť potrebné opatrenia na zaistenie bezpečného riadenia údajov a primeraného spracúvania (ako sú technické, riadiace a fyzické záruky), ako aj zaviesť opatrenia na primerané vybavovanie individuálnych sťažností ([198]). A napokon sa všeobecné zásady zákonnosti, nevyhnutnosti a primeranosti z kórejskej ústavy (pozri odôvodnenie (145)) uplatňujú aj na spracúvanie osobných údajov na účely národnej bezpečnosti.

(150) Na tieto všeobecné obmedzenia a záruky sa môžu jednotlivci pri dosahovaní prostriedku nápravy odvolať pred nezávislými orgánmi dozoru (napr. Komisiou pre ochranu osobných informácií a/alebo Národnou komisiou pre ľudské práva, pozri odôvodnenia (177) – (178)) a na súdoch (pozri odôvodnenia (179) – (183)).

3.2. **Prístup a používanie zo strany kórejských orgánov verejnej moci na účely presadzovania práva v trestných veciach**

(151) V práve Kórejskej republiky sa ukladá viacero obmedzení prístupu k osobným údajom a ich používania na účely presadzovania práva v trestných veciach a poskytujú sa mechanizmy dozoru a nápravy, ktoré sú v súlade s požiadavkami uvedenými v odôvodneniach (141) až (143) tohto rozhodnutia. Podmienky, za ktorých sa takýto prístup môže uskutočniť, a záruky, ktoré sa vzťahujú na uplatnenie týchto právomocí, sa podrobne posudzujú v nasledujúcich oddieloch.

3.2.1. *Právne základy, obmedzenia a záruky*

(152) Osobné údaje spracúvané kórejskými prevádzkovateľmi, ktoré by sa preniesli z Únie podľa tohto rozhodnutia ([199]), môžu kórejské orgány získať na účely presadzovania práva v trestných veciach v súvislosti s prehliadkami alebo zaisteniami predmetov (podľa zákona o trestnom konaní) tým, že získajú prístup k informáciám o komunikácii (na základe zákona o ochrane súkromia komunikácie) alebo získaním údajov o účastníkoch po podaní žiadostí o dobrovoľné sprístupnenie údajov (na základe zákona o telekomunikáciách) ([200]).

3.2.1.1. Prehliadky a zaistenia predmetov

(153) V zákone o trestnom konaní sa stanovuje, že prehliadky a zaistenia predmetov možno uskutočňovať len vtedy, ak je osoba podozrivá zo spáchania trestného činu, ak je to potrebné na účely vyšetrovania a ak sa určila spojitosť medzi vyšetrovaním a osobou, ktorá sa má prehľadať, alebo predmetom, ktorého inšpekcia sa má vykonať alebo ktorý sa má zaistiť ([201]). Okrem toho možno prehliadku alebo zaistenie predmetu (ako povinné opatrenie) povoliť/vykonať iba v najmenšom potrebnom rozsahu ([202]). Ak je predmetom prehliadky počítačový disk alebo iný nosič údajov, v zásade sa zaisťujú iba samotné údaje (skopírované alebo vytlačené), a nie fyzický nosič ([203]). Samotný nosič údajov môže byť zaistený iba vtedy, ak sa opodstatnene považuje za nemožné vytlačiť alebo skopírovať požadované údaje samostatne, prípadne ak sa opodstatnene považuje za nepraktické inak dosiahnuť účel prehliadky ([204]). V zákone o trestnom konaní sa teda stanovujú jednoznačné a presné pravidlá rozsahu a uplatňovania týchto opatrení, čím sa zabezpečuje obmedzenie zasahovania do práv jednotlivcov v prípade prehliadky alebo zaistenia predmetu na rozsah potrebný na osobitné vyšetrovanie trestnej činnosti a primeraný sledovanému cieľu.

([198]) Článok 58 ods. 4 zákona o ochrane osobných informácií.

([199]) Pozri prílohu II oddiel 2.1. Oficiálne zastúpenie kórejskej vlády (oddiel 2.1 prílohy II) odkazuje aj na možnosť získavať informácie o finančných transakciách na účel predchádzania praniu špinavých peňazí a financovania terorizmu na základe zákone o oznamovaní a používaní špecifikovaných informácií o finančných transakciách. V zákone o oznamovaní a používaní špecifikovaných informácií o finančných transakciách sa však prevádzkovateľom, ktorí spracúvajú osobné úverové informácie podľa zákona o používaní a ochrane úverových informácií a ktorí podliehajú dozoru Komisie pre finančné služby, ukladajú iba povinnosti v oblasti sprístupňovania informácií (pozri odôvodnenie (13)). Keďže spracúvanie osobných úverových informácií takýmito prevádzkovateľmi je vylúčené z rozsahu pôsobnosti tohto rozhodnutia, zákon o oznamovaní a používaní špecifikovaných informácií o finančných transakciách nie je pre toto posúdenie relevantný.

([200]) V článku 3 zákona o ochrane súkromia komunikácie sa ako možný právny základ pre získavanie údajov o komunikácii uvádza aj zákon o vojenskom súde. V tomto zákone sa však upravuje získavanie informácií o vojenskom personáli a na civilné obyvateľstvo ho možno uplatniť len v obmedzených prípadoch (napr. ak by člen vojenského personálu a civilná osoba spáchali trestný čin spoločne alebo ak jednotlivec spácha trestný čin na členovi vojenského personálu, možno začať konanie pred vojenským súdom, pozri článok 2 zákona o vojenskom súde). V každom prípade sa v ňom stanovujú všeobecné ustanovenia upravujúce prehliadky a zaistenia predmetov, ktoré sú podobné ako v zákone o trestnom konaní (pozri napr. články 146 – 149 a články 153 – 156 zákona o vojenskom súde), a napríklad aj to, že poštu možno získať len vtedy, ak je to potrebné na účely vyšetrovania, a len na základe príkazu vojenského súdu. Obmedzenia a záruky podľa zákona o ochrane súkromia komunikácie by sa uplatňovali v rozsahu, v akom by sa na základe uvedeného zákona získavala elektronická komunikácia. Pozri prílohu II oddiel 2.2.2 a poznámku pod čiarou č. 50.

([201]) Článok 215 ods. 1 a 2 zákona o trestnom konaní. Pozri aj článok 106 ods. 1, články 107 a 109 zákona o trestnom konaní, v ktorých sa uvádza, že súdy môžu vykonávať prehliadky a zaistenia predmetov, ak existuje prepojenie dotknutých predmetov alebo osôb s konkrétnym prípadom. Pozri prílohu II oddiel 2.2.1.2.

([202]) Článok 199 ods. 1 zákona o trestnom konaní.

([203]) Článok 106 ods. 3 zákona o trestnom konaní.

([204]) Článok 106 ods. 3 zákona o trestnom konaní.

(154) Pokiaľ ide o procesné záruky, v zákone o trestnom konaní sa vyžaduje vydanie súdneho príkazu na vykonanie prehliadky alebo zaistenia predmetov ([205]). Prehliadka alebo zaistenie predmetov bez súdneho príkazu sa umožňuje len výnimočne, a to za mimoriadnych okolností ([206]), na mieste v čase zatknutia alebo zadržania osoby podozrivej z trestnej činnosti ([207]), alebo vtedy, keď sa osoba podozrivá z trestnej činnosti alebo tretia osoba predmetu zbavila, prípadne bol vydaný dobrovoľne (v prípade osobných údajov samotnou dotknutou osobou) ([208]). Na nezákonné prehliadky a zaistenia predmetov sa vzťahujú trestnoprávne sankcie ([209]), pričom každý dôkaz, ktorý sa získa v dôsledku porušenia zákona o trestnom konaní, sa považuje za neprípustný ([210]). A napokon dotknutým jednotlivcom sa musí prehliadka alebo zaistenie predmetov (vrátane zaistenia ich údajov) vždy bezodkladne oznámiť ([211]), čím sa zase uľahčuje uplatňovanie hmotnoprávnych práv jednotlivca, ako aj práva na nápravu (pozri najmä možnosť napadnúť výkon súdneho príkazu na zaistenie predmetov, pozri odôvodnenie (180)).

3.2.1.2. Prístup k informáciám o komunikácii

(155) Na základe zákona o ochrane súkromia komunikácie môžu kórejské orgány presadzovania práva v trestných veciach prijímať dva druhy opatrení ([212]): na jednej strane získanie „potvrdzujúcich údajov o komunikácii“ ([213]), čiže údajov o záznamoch telekomunikácie, ktoré obsahujú dátum telekomunikácie, čas jej začatia a ukončenia, počet odchádzajúcich a prichádzajúcich hovorov, ako aj účastnícke číslo druhej strany, frekventovanosť využívania, logy týkajúce sa používania telekomunikačných služieb a informácie o polohe (napr. z prenosových veží, ktoré prijímajú signály); a na druhej strane „opatrenia na zachytenie komunikácie“, ktoré sa týkajú získania obsahu tradičnej pošty, ako aj odpočúvania obsahu telekomunikácie ([214]).

(156) Potvrdzujúce údaje o komunikácii možno získať len vtedy, ak je to potrebné na vedenie vyšetrovania trestnej činnosti alebo výkon trestu ([215]), a to na základe súdneho príkazu ([216]). V tejto súvislosti sa v zákone o ochrane súkromia komunikácie vyžaduje, aby sa podrobné informácie uvádzali tak v žiadosti o vydanie súdneho príkazu (napr. o dôvodoch žiadosti, vzťahu k cieľu/účastníkovi a o potrebných údajoch), ako aj v samotnom súdnom príkaze (napr. o zámere, cieli a rozsahu opatrenia) ([217]). Získavanie údajov bez súdneho príkazu možno vykonať len vtedy, ak z naliehavých dôvodov nie je možné získať povolenie súdu, v takom prípade sa však musí získať

([205]) Článok 215 ods. 1 a 2 a článok 113 zákona o trestnom konaní. Dotknutý orgán žiadajúci o vydanie súdneho príkazu musí predložiť materiály preukazujúce dôvody podozrenia, že jednotlivec spáchal trestný čin, že prehliadka, inšpekcia alebo zaistenie predmetov je potrebné a že príslušné predmety, ktoré je potrebné zaistiť, existujú (článok 108 ods. 1 nariadenia o trestnom konaní). V súdnom príkaze sa musí okrem ďalších náležitostí uvádzať meno osoby podozrivej z trestnej činnosti a trestný čin; miesto, osoba alebo predmety, ktorých prehliadku je potrebné vykonať, alebo predmety, ktoré je potrebné zaistiť; dátum vydania a obdobie jeho platnosti (článok 114 ods. 1 v spojení s článkom 219 zákona o trestnom konaní). Pozri prílohu II oddiel 2.2.1.2.

([206]) Teda vtedy, ak nie je možné získať súdny príkaz z dôvodu naliehavosti na mieste trestného činu (článok 216 ods. 3 zákona o trestnom konaní), pričom v takom prípade sa musí súdny príkaz následne bezodkladne získať (článok 216 ods. 3 zákona o trestnom konaní).

([207]) Článok 216 ods. 1 a 2 zákona o trestnom konaní.

([208]) Článok 218 zákona o trestnom konaní. Okrem toho, ako sa vysvetľuje v oddiele 2.2.1.2 prílohy II, dobrovoľne vydané predmety sa pripúšťajú ako dôkaz v súdnom konaní iba vtedy, ak neexistuje žiadna odôvodnená pochybnosť o dobrovoľnosti ich vydania, čo musí preukázať prokurátor.

([209]) Článok 321 zákona o trestnom konaní.

([210]) Článok 308 -2 zákona o trestnom konaní. Okrem toho môže byť dotknutý jednotlivec (a jeho zástupca) prítomný pri výkone súdneho príkazu na prehliadku alebo zaistenie predmetov, takže môže vzniesť námietku v čase vykonávania súdneho príkazu (články 121 a 219 zákona o trestnom konaní).

([211]) Články 121 a 122 zákona o trestnom konaní (týkajúce sa prehliadok) a článok 219 v spojení s článkom 106 ods. 4 zákona o trestnom konaní (týkajúce sa zaistenia predmetov).

([212]) Pozri prílohu II oddiel 2.2.2.1. Takéto opatrenia možno prijať na základe pomoci, ktorú musia telekomunikační operátori poskytnúť po predložení písomného povolenia vydaného súdom (článok 9 ods. 2 zákona o ochrane súkromia komunikácie), pričom toto povolenie musia operátori uchovať (článok 15-2 zákona o ochrane súkromia komunikácie a článok 12 vykonávacieho dekrétu k zákonu o ochrane súkromia komunikácie). Telekomunikační operátori môžu spoluprácu odmietnuť vtedy, ak sú informácie o zacielenej osobe uvedené v písomnom povolení súdu (napríklad telefónne číslo osoby) nesprávne, pričom sa za žiadnych okolností nepovoľuje sprístupniť heslá používané na telekomunikáciu (článok 9 ods. 4 zákona o ochrane súkromia komunikácie).

([213]) Článok 2 ods. 11 zákona o ochrane súkromia komunikácie.

([214]) Pozri článok 2 ods. 6 zákona o ochrane súkromia komunikácie, v ktorom sa odkazuje na pojem „cenzúra“ (otváranie pošty bez súhlasu dotknutej strany alebo získavanie poznatkov o jej obsahu, prípadne zaznamenávanie alebo zadržiavanie jej obsahu inými prostriedkami) a článok 2 ods. 7 zákona o ochrane súkromia komunikácie, v ktorom sa odkazuje na pojem „odpočúvanie“ (získavanie alebo nahrávanie obsahu telekomunikácie počúvaním alebo sledovaním okolitých zvukov, slov, symbolov alebo obrázkov komunikácie prostredníctvom elektronických a mechanických zariadení bez súhlasu dotknutej strany alebo zachytávanie ňou prenášanej alebo prijímanej komunikácie).

([215]) Článok 13 ods. 1 zákona o ochrane súkromia komunikácie. Pozri aj prílohu II oddiel 2.2.2.3. Okrem toho možno údaje o sledovaní polohy v reálnom čase a potvrdzujúce údaje o komunikácii týkajúce sa konkrétnej základnej stanice získať iba na účely vyšetrovania závažných trestných činov alebo ak by bolo inak ťažké zabrániť spáchaniu trestného činu alebo získať dôkazy (článok 13 ods. 2 zákona o ochrane súkromia komunikácie). Z toho vyplýva potreba poskytnúť dodatočné záruky v súlade so zásadou primeranosti v prípade opatrení, ktoré osobitne narúšajú súkromie.

([216]) Články 13 a 6 zákona o ochrane súkromia komunikácie.

([217]) Pozri článok 13 ods. 3 a 9 v spojení s článkom 6 ods. 4 a 6 zákona o ochrane súkromia komunikácie.

súdny príkaz ihneď po vyžiadaní údajov, pričom musí byť oznámený poskytovateľovi telekomunikačných služieb ([218]). Ak súd odmietne vydať následné povolenie, získané informácie sa musia zničiť ([219]).

(157) Pokiaľ ide o dodatočné záruky týkajúce sa získavania potvrdzujúcich údajov o komunikácii, v zákone o ochrane súkromia komunikácie sa ukladajú osobitné požiadavky na uchovávanie záznamov a transparentnosť ([220]). Konkrétne musia orgány presadzovania práva v trestných veciach ([221]), ako aj poskytovatelia telekomunikačných služieb ([222]) uchovávať záznamy o žiadostiach a uskutočnenom sprístupnení údajov. Okrem toho musia orgány presadzovania práva v trestných veciach v zásade oznámiť jednotlivcom skutočnosť, že sa získavajú potvrdzujúce údaje o ich komunikácii ([223]). Takéto oznámenie možno odložiť len za mimoriadnych okolností a na základe povolenia riaditeľa príslušnej okresnej prokuratúry ([224]). Takéto povolenie možno vydať len vtedy, ak je pravdepodobné, že po vykonaní oznámenia 1. by bola ohrozená národná bezpečnosť, verejná bezpečnosť alebo poriadok; 2. by došlo k smrti alebo fyzickej ujme; 3. by došlo k ohrozeniu spravodlivého súdneho konania (napríklad by malo za následok zničenie dôkazov alebo zastrašovanie svedkov); alebo 4. by došlo k ohováraniu podozrivej osoby, obetí alebo iných osôb súvisiacich s prípadom alebo k narušeniu ich súkromia. V týchto prípadoch sa musí oznámenie vykonať do 30 dní odo dňa, keď prestanú existovať dôvody na jeho odloženie ([225]). Po oznámení majú jednotlivci právo vyžiadať si informácie o dôvodoch získavania ich údajov ([226]).

(158) Prísnejšie pravidlá sa uplatňujú na opatrenia na zachytenie komunikácie, ktoré možno použiť len vtedy, ak existuje odôvodnené podozrenie, že sa plánuje spáchanie závažných trestných činov, páchajú sa alebo sa spáchali závažné trestné činy, ktoré sú výslovne uvedené v zákone o ochrane súkromia komunikácie ([227]). Okrem toho možno opatrenia na zachytenie komunikácie využiť len ako poslednú možnosť a vtedy, ak je inak ťažké zabrániť spáchaniu trestného činu, zatknúť páchateľa alebo získať dôkazy ([228]). Keď už nie sú potrebné, musia sa okamžite ukončiť, čím sa zabezpečí čo najmenšie porušovanie súkromia komunikácie ([229]). Ak sa informácie získali nezákonne na základe opatrení na zachytenie komunikácie, nie sú pripustené ako dôkaz v súdnom alebo disciplinárnom konaní ([230]).

(159) Pokiaľ ide o procesné záruky, v zákone o ochrane súkromia komunikácie sa vyžaduje získanie súdneho príkazu na vykonanie opatrení na zachytenie komunikácie ([231]). V zákone o ochrane súkromia komunikácie sa vyžaduje, aby sa v žiadosti o vydanie súdneho príkazu, ako aj v samotnom súdnom príkaze uvádzali podrobné informácie ([232]) vrátane odôvodnenia žiadosti, ako aj o komunikácii, ktorá sa má získať (pričom musí ísť o komunikáciu vyšetrovanej podozrivej osoby) ([233]). Takéto opatrenia môžu byť prijaté bez súdneho príkazu iba v prípade bezprostrednej hrozby organizovanej trestnej činnosti alebo ak bezprostredne hrozí spáchanie iného závažného trestného činu, ktorý môže priamo spôsobiť smrť alebo vážnu ujmu, pričom táto mimoriadna situácia bráni

([218]) Článok 13 ods. 2 zákona o ochrane súkromia komunikácie.
([219]) Článok 13 ods. 3 zákona o ochrane súkromia komunikácie.
([220]) Pozri prílohu II oddiel 2.2.2.3.
([221]) Článok 13 ods. 5 a 6 zákona o ochrane súkromia komunikácie.
([222]) Článok 13 ods. 7 zákona o ochrane súkromia komunikácie. Poskytovatelia telekomunikačných služieb musia okrem toho dvakrát ročne podávať ministerstvu pre vedu a IKT správu o sprístupňovaní potvrdzujúcich údajov o komunikácii.
([223]) Pozri článok 13-3 ods. 7 v spojení s článkom 9-2 zákona o ochrane súkromia komunikácie. Konkrétne musia byť jednotlivci informovaní do 30 dní po prijatí rozhodnutia o (ne)stíhaní alebo do 30 dní po uplynutí jedného roka od vydania rozhodnutia o zrušení obžaloby (hoci oznámenie sa musí v každom prípade vykonať do 30 dní po uplynutí jedného roka od získania informácií), pozri článok 13-3 ods. 1 zákona o ochrane súkromia komunikácie.
([224]) Článok 13-3 ods. 2 až 3 zákona o ochrane súkromia komunikácie.
([225]) Článok 13-3 ods. 4 zákona o ochrane súkromia komunikácie.
([226]) Článok 13-3 ods. 5 zákona o ochrane súkromia komunikácie. Na žiadosť jednotlivca musí prokurátor alebo príslušník justičnej polície do 30 dní od prijatia žiadosti písomne poskytnúť dôvody, ak sa na to neuplatňuje niektorá z výnimiek na odloženie (článok 13-3 ods. 6 zákona o ochrane súkromia komunikácie).
([227]) Napríklad povstanie, trestné činy súvisiace s drogami alebo trestné činy páchané pomocou výbušnín, ako aj trestné činy súvisiace s národnou bezpečnosťou, diplomatickými vzťahmi alebo vojenskými základňami a zariadeniami, pozri článok 5 ods. 1 zákona o ochrane súkromia komunikácie. Pozri aj prílohu II oddiel 2.2.2.2.
([228]) Článok 3 ods. 2 a článok 5 ods. 1 zákona o ochrane súkromia komunikácie.
([229]) Článok 2 vykonávacieho dekrétu k zákonu o ochrane súkromia komunikácie.
([230]) Článok 4 zákona o ochrane súkromia komunikácie.
([231]) Článok 6 ods. 1 a 2 a ods. 5 až 6 zákona o ochrane súkromia komunikácie.
([232]) V žiadosti o vydanie súdneho príkazu sa musí uvádzať: 1. odôvodnené podozrenie (*prima facie*), že sa plánuje, pácha alebo spáchal niektorý z trestných činov uvedených v zozname, ako aj sprievodné materiály; 2. opatrenia na zachytenie komunikácie, ako aj ich cieľ, rozsah, zámer a obdobie uplatňovania; a 3. miesto, na ktorom by sa opatrenia vykonávali, a spôsob, akým by sa vykonávali (článok 6 ods. 4 zákona o ochrane súkromia komunikácie a článok 4 ods. 1 vykonávacieho dekrétu k zákonu o ochrane súkromia komunikácie). V samotnom súdnom príkaze sa musia uvádzať opatrenia, ako aj ich cieľ, rozsah, obdobie uplatňovania, miesto ich vykonávania a spôsob ich realizácie (článok 6 ods. 6 zákona o ochrane súkromia komunikácie).
([233]) Opatrenia na zachytenie komunikácie musia byť zacielené na konkrétnu poštu alebo telekomunikáciu odoslanú alebo prijatú podozrivou osobou, prípadne na poštu alebo telekomunikáciu odoslanú alebo prijatú podozrivou osobou v priebehu konkrétneho časového obdobia (článok 5 ods. 2 zákona o ochrane súkromia komunikácie).

vykonaniu bežného postupu ([234]). V takom prípade je však potrebné ihneď po prijatí opatrenia podať žiadosť o vydanie súdneho príkazu ([235]). Opatrenia na zachytenie komunikácie možno vykonávať maximálne dva mesiace ([236]), pričom ich možno predĺžiť na základe súhlasu súdu, ak naďalej existujú podmienky na ich vykonávanie ([237]). Predĺžené obdobie nesmie prekročiť jeden rok, prípadne tri roky, ak ide o niektoré osobitne závažné trestné činy (napríklad trestné činy súvisiace s povstaním, zahraničnou agresiou, národnou bezpečnosťou) ([238]).

(160) Tak ako v prípade získavania potvrdzujúcich údajov o komunikácii sa v zákone o ochrane súkromia komunikácie vyžaduje ([239]), aby poskytovatelia telekomunikačných služieb a orgány presadzovania práva ([240]) uchovávali záznamy o vykonávaní opatrení na zachytenie komunikácie a informovali dotknutého jednotlivca, čo možno vo výnimočných prípadoch v prípade potreby odložiť z dôležitých dôvodov verejného záujmu ([241]).

(161) A napokon sa na nedodržanie viacerých obmedzení a záruk zákona o ochrane súkromia komunikácie (napríklad vrátane povinností získať súdny príkaz, uchovávať záznamy a informovať jednotlivcov) pri získavaní potvrdzujúcich údajov o komunikácii a používaní opatrení na zachytenie komunikácie vzťahujú trestnoprávne sankcie ([242]).

(162) Právomoci orgánov presadzovania práva v trestných veciach pri získavaní údajov o komunikácii na základe zákona o ochrane súkromia komunikácie (obsahu komunikácie, ako aj potvrdzujúcich údajov o komunikácii) sú teda uvedené v jasných a presných pravidlách a vzťahuje sa na ne viacero záruk. Týmito zárukami sa konkrétne zaručuje dozor nad vykonávaním takýchto opatrení, a to *ex ante* (prostredníctvom predchádzajúceho súhlasu súdu) aj *ex post* (prostredníctvom uchovávania záznamov a požiadaviek na oznamovanie) a uľahčuje prístup k účinným prostriedkom nápravy (zabezpečením informovanosti o získavaní ich údajov).

3.2.1.3. Žiadosti o dobrovoľné sprístupnenie údajov o účastníkoch

(163) Okrem využívania povinných opatrení uvedených v odôvodneniach (153) – (162) môžu kórejské orgány presadzovania práva požiadať poskytovateľov telekomunikačných služieb o dobrovoľné sprístupnenie „údajov o komunikácii“ na podporu trestného konania, vyšetrovania alebo výkonu trestu (článok 83 ods. 3 telekomunikačného zákona). Táto možnosť sa týka len obmedzených súborov údajov, t. j. mena, evidenčného čísla rezidenta, adresy a telefónneho čísla používateľov, dátumov začatia využívania služieb alebo ukončenia využívania služieb používateľmi, ako aj identifikačných kódov používateľov (čiže kódov používaných na identifikovanie oprávneného používateľa počítačových systémov alebo komunikačných sietí) ([243]). Keďže za používateľov sa považujú iba jednotlivci, ktorí majú priamo uzavreté zmluvy na poskytovanie služieb s kórejským poskytovateľom telekomunikačných služieb ([244]), jednotlivci z EÚ, ktorých údaje boli prenesené do Kórejskej republiky, by zvyčajne do tejto kategórie nepatrili ([245]).

(164) Na takéto dobrovoľné sprístupnenie sa uplatňujú rôzne obmedzenia, a to na výkon právomocí orgánov presadzovania práva, ako aj na reakciu telekomunikačného operátora. Vo všeobecnosti platí, že orgány presadzovania práva musia konať v súlade s ústavnými zásadami nevyhnutnosti a primeranosti (článok 12 ods. 1 a článok 37 ods. 2 ústavy), a to aj vtedy, ak žiadajú o dobrovoľné sprístupnenie informácií. Okrem toho musia dodržiavať zákon o ochrane osobných informácií, a to najmä tým, že získavajú minimálne osobné údaje v rozsahu

([234]) Článok 8 ods. 1 zákona o ochrane súkromia komunikácie. Získavanie informácií v mimoriadnych situáciách sa však musí vždy vykonávať v súlade s „vyhlásením o mimoriadnej cenzúre/odpočúvaní“, pričom orgán, ktorý ho vykonáva, musí uchovávať záznamy o všetkých mimoriadnych opatreniach (článok 8 ods. 4 zákona o ochrane súkromia komunikácie).

([235]) Získavanie sa musí okamžite ukončiť, ak orgán presadzovania práva nezíska do 36 hodín povolenie súdu (článok 8 ods. 2 zákona o ochrane súkromia komunikácie), pričom v takom prípade sa, ako sa vysvetľuje v oddiele 2.2.2.2 prílohy II, získané informácie v zásade zničia. Ak boli mimoriadne opatrenia uskutočnené v takom krátkom čase, že nebolo možné predísť potrebe získať povolenie, musí sa to takisto oznámiť súdu (napr. ak je podozrivá osoba zatknutá ihneď po začatí odpočúvania, pozri článok 8 ods. 5 zákona o ochrane súkromia komunikácie). V takom prípade sa súdu musia oznámiť informácie o zámere, cieli, rozsahu, období uplatňovania, mieste vykonávania a metóde získania informácií, ako aj o dôvodoch nepodania žiadosti o vydanie povolenia súdu (článok 8 ods. 6 až 7 zákona o ochrane súkromia komunikácie).

([236]) Článok 6 ods. 7 zákona o ochrane súkromia komunikácie. Ak sa zámer opatrení v rámci tohto obdobia dosiahne skôr, opatrenia sa musia okamžite ukončiť.

([237]) Článok 6 ods. 7 až 8 zákona o ochrane súkromia komunikácie.

([238]) Článok 6 ods. 8 zákona o ochrane súkromia komunikácie.

([239]) Článok 9 ods. 3 zákona o ochrane súkromia komunikácie.

([240]) Článok 18 ods. 1 vykonávacieho dekrétu k zákonu o ochrane súkromia komunikácie.

([241]) Konkrétne musí prokurátor informovať jednotlivca do 30 dní od vznesenia obžaloby alebo vykonania právneho úkonu, ktorým sa ruší obžaloba alebo zadržanie (článok 9-2 ods. 1 zákona o ochrane súkromia komunikácie). Oznámenie možno odložiť so súhlasom vedúceho okresnej prokuratúry, ak je pravdepodobné, že by závažne ohrozilo národnú bezpečnosť alebo narušilo verejnú bezpečnosť a poriadok, prípadne ak je pravdepodobné, že by malo za následok závažnú ujmu na životoch alebo fyzickej integrite ďalších osôb (článok 9-2 ods. 4 až 6 zákona o ochrane súkromia komunikácie).

([242]) Články 16 a 17 zákona o ochrane súkromia komunikácie.

([243]) Článok 83 ods. 3 zákona o telekomunikáciách. Pozri aj prílohu II oddiel 2.2.3.

([244]) Článok 2 ods. 9 zákona o telekomunikáciách.

([245]) Pozri aj prílohu II oddiel 2.2.3.

potrebnom na dosiahnutie oprávneného účelu, a tak, aby sa minimalizoval vplyv na súkromie jednotlivcov (napríklad podľa článku 3 ods. 1 zákona o ochrane osobných informácií). Konkrétnejšie platí, že žiadosti o získanie údajov o komunikácii na základe zákona o telekomunikáciách sa musia podávať písomne a musia sa v nich uvádzať dôvody žiadosti, súvis s príslušným používateľom a rozsah požadovaných údajov ([246]).

(165) Poskytovatelia telekomunikačných služieb nemusia týmto žiadostiam vyhovieť, pričom urobiť tak môžu len podľa zákona o ochrane osobných informácií. Znamená to konkrétne, že musia vyvážiť rôzne predmetné záujmy a nesmú poskytnúť údaje, ak by tým nespravodlivo poškodili záujmy jednotlivca alebo tretej strany ([247]). Bolo by to tak napríklad vtedy, ak by bolo jasné, že žiadajúci orgán zneužil svoju právomoc ([248]). Telekomunikační operátori musia uchovávať záznamy o zverejňovaní podľa zákona o telekomunikáciách a dvakrát ročne podávať správy ministrovi pre vedu a IKT ([249]).

(166) Okrem toho musia poskytovatelia telekomunikačných služieb v súlade s oddielom 3 oznámenia č. 2021-5 (príloha I) v zásade oznámiť dotknutému jednotlivcovi dobrovoľné vyhovenie žiadosti ([250]). Jednotlivec tak bude môcť uplatniť svoje práva a v prípade nezákonného sprístupnenia svojich údajov dosiahnuť prostriedok nápravy buď proti prevádzkovateľovi (napríklad za sprístupnenie údajov v rozpore so zákonom o ochrane osobných informácií alebo jednoznačne neprimeranú reakciu na žiadosť), alebo proti orgánu presadzovania práva (napríklad za konanie nad rámec toho, čo je potrebné a primerané alebo za nedodržanie procesných požiadaviek zákona o telekomunikáciách).

3.2.2. *Ďalšie používanie získaných informácií*

(167) Spracúvanie osobných údajov získaných kórejskými orgánmi presadzovania práva v trestných veciach podlieha všetkým požiadavkám zákona o ochrane osobných informácií, a to aj v súvislosti s obmedzením účelu (článok 3 ods. 1 až 2 zákona o ochrane osobných informácií), zákonnosťou ich používania a poskytovania tretím stranám (články 15, 17 a 18 zákona o ochrane osobných informácií), medzinárodnými prenosmi (články 17 a 18 zákona o ochrane osobných informácií v spojení s oddielom 2 oznámenia č. 2021-5) ([251]), primeranosťou/minimalizáciou údajov (článok 3 ods. 1 a 6 zákona o ochrane osobných informácií) a obmedzením uchovávania (článok 21 zákona o ochrane osobných informácií) ([252]).

(168) Pokiaľ ide o obsah komunikácie získavaný prostredníctvom vykonávania opatrení na zachytenie komunikácie, v zákone o ochrane súkromia komunikácie sa vyslovene obmedzuje jeho možné použitie na účely vyšetrovania, trestného stíhania alebo predchádzania závažným trestným činom ([253]); disciplinárneho konania týkajúceho sa tých istých trestných činov; nárokov na náhradu škody vznesených stranou komunikácie alebo vtedy, ak to umožňujú iné zákony ([254]). Okrem toho možno získaný obsah telekomunikácie prenášanej cez internet uchovávať len so súhlasom súdu, ktorý povolil dané opatrenia na zachytenie komunikácie ([255]), a to s cieľom použiť ho na účely vyšetrovania, trestného stíhania alebo predchádzania závažným trestným činom ([256]). Všeobecnejšie sa v zákone o ochrane súkromia komunikácie zakazuje sprístupnenie dôverných informácií získaných na základe opatrení na zachytenie komunikácie a použitie takýchto informácií na účely poškodenia dobrého mena osôb, na ktoré sa takého opatrenia vzťahovali ([257]).

3.2.3. *Dozor*

(169) V Kórei vykonávajú dozor nad činnosťami orgánov presadzovania práva v trestných veciach rôzne orgány ([258]).

([246]) Článok 83 ods. 4 zákona o telekomunikáciách. Ak nie je možné z dôvodov naliehavosti podať písomnú žiadosť, táto písomná žiadosť sa musí podať čo najskôr po uplynutí dôvodov naliehavosti (článok 83 ods. 4 zákona o telekomunikáciách).

([247]) Článok 18 ods. 2 zákona o ochrane osobných informácií.

([248]) Rozhodnutie najvyššieho súdu č. 2012Da105482 z 10. marca 2016. Pozri aj prílohu II oddiel 2.2.3 o tomto rozhodnutí najvyššieho súdu.

([249]) Článok 83 ods. 5 až 6 zákona o telekomunikáciách.

([250]) Na túto požiadavku sa vzťahujú obmedzené a kvalifikované výnimky, a to najmä ak a dovtedy, kým by mohlo oznámenie ohrozovať prebiehajúce vyšetrovanie trestnej činnosti, alebo ak je pravdepodobné, že oznámenie spôsobí ujmu na živote alebo fyzickej integrite inej osoby, ak sú tieto práva alebo záujmy preukázateľne nadradené právam dotknutej osoby. Pozri oddiel 3 písm. iii) pododsek 1 oznámenia.

([251]) Konkrétne kórejské verejné orgány sú povinné zabezpečiť prostredníctvom právne záväzného nástroja úroveň ochrany rovnakú ako v prípade zákona o ochrane osobných informácií, pozri aj odôvodnenie (90).

([252]) Pozri aj prílohu II oddiel 1.2.

([253]) Pozri odôvodnenie (158).

([254]) Článok 12 zákona o ochrane súkromia komunikácie. Pozri prílohu II oddiel 2.2.2.2.

([255]) Prokurátor alebo príslušník polície vykonávajúci opatrenia na zachytenie komunikácie musí vybrať telekomunikáciu, ktorá sa má uchovať, do 14 dní od ukončenia opatrení, a požiadať o súhlas súdu (príslušník polície podáva žiadosť prokurátorovi, ktorý ju potom podáva súdu), pozri článok 12-2 ods. 1 a 2 zákona o ochrane súkromia komunikácie.

([256]) Žiadosť o takéto povolenie musí obsahovať informácie o opatreniach na zachytenie komunikácie, súhrn výsledkov opatrení, dôvody uchovávania (spoločne so sprievodnými materiálmi) a telekomunikáciu, ktorá sa má uchovať (článok 12-2 ods. 3 zákona o ochrane súkromia komunikácie). Ak sa takáto žiadosť nepodá, získané údaje sa musia vymazať do 14 dní od ukončenia opatrenia na zachytenie komunikácie (článok 12-2 ods. 5 zákona o ochrane súkromia komunikácie), a ak je žiadosť zamietnutá, do siedmich dní (článok 12-2 ods. 5 zákona o ochrane súkromia komunikácie). V oboch prípadoch sa musí súdu, ktorý povolil získavanie údajov, do siedmich dní predložiť správa o vymazaní.

([257]) Článok 11 ods. 2 vykonávacieho dekrétu k zákonu o ochrane súkromia komunikácie.

([258]) Pozri prílohu II oddiel 2.3.

(170) Po prvé na políciu sa vzťahuje vnútorný dozor vykonávaný generálnym inšpektorom ([259]), ktorý kontroluje zákonnosť, a to aj v súvislosti s dodržiavaním ľudských práv. Funkcia generálneho inšpektora bola zriadená s cieľom vykonávať zákon o auditoch verejného sektora, v ktorom sa vyzýva na vytvorenie orgánov vnútorného auditu a stanovujú osobitné požiadavky na ich zloženie a úlohy. Konkrétne sa v zákone vyžaduje, aby bol vedúci orgánu vnútorného auditu menovaný z externého prostredia (napríklad spomedzi bývalých sudcov či profesorov) na obdobie dvoch až piatich rokov ([260]), pričom odvolať ho možno len z opodstatnených dôvodov (napríklad ak nemôže vykonávať svoje povinnosti zo zdravotných dôvodov alebo ak sa proti nemu vedie disciplinárne konanie) ([261]) a zaručuje sa mu nezávislosť v najväčšej možnej miere ([262]). Bránenie vo vykonávaní vnútorného auditu sa trestá správnymi pokutami ([263]). Správy o audite (ktoré môžu zahŕňať odporúčania, žiadosti o disciplinárne konanie a žiadosti o náhradu škody alebo nápravu) sa oznamujú vedúcemu príslušného verejného orgánu, Rade pre audit a inšpekciu ([264]) a vo všeobecnosti sa zverejňujú ([265]). Výsledky vykonávania správy sa musia oznamovať aj Rade pre audit a inšpekciu ([266]) (pozri odôvodnenie (173) týkajúce sa úlohy dozoru a právomocí Rady pre audit a inšpekciu).

(171) Po druhé Komisia pre ochranu osobných informácií dozerá na to, aby orgány presadzovania práva v trestných veciach dodržiavali pri spracúvaní údajov zákon o ochrane osobných informácií a iné zákony, ktorými sa chráni súkromie jednotlivcov, vrátane zákonov, ktorými sa upravuje získavanie (elektronických) dôkazov na účely presadzovania práva v trestných veciach, ako sa to uvádza v oddiele 3.2.1 ([267]). Konkrétne, keďže dozor Komisie pre ochranu osobných informácií je rozšírený na zákonnosť a spravodlivosť získavania a spracúvania údajov (článok 3 ods. 1 zákona o ochrane osobných informácií), ktoré sa porušia, ak sa osobné údaje získajú a použijú v rozpore s tými zákonmi ([268]), Komisia pre ochranu osobných informácií môže vyšetrovať a presadzovať aj dodržiavanie obmedzení a záruk uvedených v oddiele 3.2.1 ([269]). Pri vykonávaní tejto úlohy dozoru môže Komisia pre ochranu osobných informácií využívať všetky svoje právomoci v oblasti vyšetrovania a nápravy, ako sa podrobne uvádzajú v oddiele 2.4.2. Už pred nedávnou reformou zákona o ochrane osobných informácií (t. j. keď plnila predchádzajúcu úlohu dohľadu nad verejným sektorom) vykonávala Komisia pre ochranu osobných informácií viacero činností dozoru pri spracúvaní osobných údajov orgánmi presadzovania práva v trestných veciach, napr. v súvislosti s vypočúvaním podozrivých osôb (vec č. 2013-16 z 26. augusta 2013), poskytovaním oznámení jednotlivcov o uložení správnych pokút (vec č. 2015-02-04 z 26. januára 2015), spoločným využívaním údajov s inými orgánmi (vec č. 2018-15-146 z 9. júla 2018, vec č. 2018-25-308 z 10. decembra 2018; vec č. 2019-02-015 z 29. januára 2019), získavaním odtlačkov prstov alebo fotografií (vec č. 2019-17-273 z 9. septembra 2019), používaním dronov (vec č. 2020-01-004 z 13. januára 2020). V týchto prípadoch Komisia pre ochranu osobných informácií vyšetrovala súlad s viacerými ustanoveniami zákona o ochrane osobných informácií (napr. zákonnosťou spracúvania, zásadami obmedzenia účelu a minimalizácie údajov), ale aj príslušnými ustanoveniami iných zákonov, ako napríklad zákona o trestnom konaní, pričom v prípade potreby vydala odporúčania na zosúladenie spracúvania s požiadavkami na ochranu údajov.

(172) Po tretie nezávislý dohľad zabezpečuje Národná komisia pre ľudské práva ([270]), ktorá môže v rámci svojho všeobecného mandátu na ochranu základných práv podľa článkov 10 až 22 ústavy vyšetrovať porušenia práva na súkromie a práva na súkromie korešpondencie. Národná komisia pre ľudské práva pozostáva z 11 komisárov, ktorí musia mať osobitnú kvalifikáciu ([271]) a ktorých menuje prezident v súlade s postupmi stanovenými v zákone. Konkrétne sú štyria komisári menovaní na základe nominácie národného zhromaždenia, štyria na základe nominácie prezidenta a traja na základe nominácie predsedu najvyššieho súdu ([272]). Jej predsedu menuje prezident spomedzi komisárov a musí ho potvrdiť národné zhromaždenie ([273]). Komisári (vrátane predsedu) sa menujú na obnoviteľné obdobie troch rokov a môžu byť odvolaní len v prípade odsúdenia na trest odňatia slobody alebo ak

([259]) Pozri prílohu II oddiel 2.3.1. Pozri aj https://www.police.go.kr/eng/knpa/org/org01.jsp.
([260]) Podobne sa menujú audítori na základe osobných podmienok stanovených v zákone, pozri článok 16 a nasl. zákona o auditoch verejného sektora.
([261]) Články 8 – 11 zákona o auditoch verejného sektora.
([262]) Článok 7 zákona o auditoch verejného sektora.
([263]) Článok 41 zákona o auditoch verejného sektora.
([264]) Článok 23 ods. 1 zákona o auditoch verejného sektora.
([265]) Článok 26 zákona o auditoch verejného sektora.
([266]) Článok 23 ods. 3 zákona o auditoch verejného sektora.
([267]) Pozri článok 7-8 ods. 3 a 4 a článok 7-9 ods. 5 zákona o ochrane osobných informácií.
([268]) Pozri oznámenie Komisie pre ochranu osobných informácií č. 2021-5, oddiel 6 (príloha I).
([269]) Pozri aj prílohu II oddiel 2.3.4.
([270]) Článok 1 zákona o Národnej komisii pre ľudské práva.
([271]) Za komisára možno vymenovať osobu, ktorá 1. aspoň desať rokov pôsobila na univerzite alebo v oprávnenom výskumnom ústave minimálne na pozícii docenta; 2. aspoň desať rokov pôsobila na pozícii sudcu, prokurátora alebo advokáta; 3. aspoň desať rokov sa venovala činnostiam v oblasti ľudských práv (napr. pre neziskovú, mimovládnu alebo medzinárodnú organizáciu); alebo 4. odporučili ju skupiny pôsobiace v rámci občianskej spoločnosti (článok 5 ods. 3 zákona o Národnej komisii pre ľudské práva). Okrem toho komisári Národnej komisie pre ľudské práva po svojom vymenovaní nesmú súčasne zastávať funkciu v národnom zhromaždení, obecných zastupiteľstvách ani v regionálnych štátnych správach a miestnych samosprávach (ako verejní činitelia), pozri článok 10 zákona o Národnej komisii pre ľudské práva.
([272]) Článok 5 ods. 1 a 2 zákona o Národnej komisii pre ľudské práva.
([273]) Článok 5 ods. 5 zákona o Národnej komisii pre ľudské práva.

už nie sú schopní vykonávať svoje povinnosti z dôvodu dlhodobých problémov s fyzickým alebo duševným zdravím (v takom prípade musia s odvolaním súhlasiť dve tretiny komisárov) ([274]). Pri vyšetrovaní môže Národná komisia pre ľudské práva požiadať o predloženie príslušných materiálov, vykonávať inšpekcie a predvolávať jednotlivcov, aby podali svedeckú výpoveď ([275]). Pokiaľ ide o právomoci v oblasti nápravy, Národná komisia pre ľudské práva môže vydávať (zverejňovať) odporúčania na zlepšenie alebo nápravu osobitných politík a postupov, na ktoré musia orgány verejnej moci reagovať navrhnutím plánu ich vykonávania ([276]). Ak dotknutý orgán odporúčania nevykoná, musí o tom informovať komisiu ([277]), ktorá môže potom túto skutočnosť oznámiť národnému zhromaždeniu, a/alebo to zverejniť. Podľa oficiálneho zastúpenia kórejskej vlády (oddiel 2.5.3 prílohy II) kórejské orgány vo všeobecnosti plnia odporúčania Národnej komisie pre ľudské práva a majú na to silnú motiváciu, pretože ich vykonávanie sa posudzuje v rámci všeobecného priebežného hodnotenia pod vedením Úradu predsedu vlády. Z výročných údajov o jej činnostiach vyplýva, že Národná komisia pre ľudské práva aktívne dozerá na činnosti orgánov presadzovania práva v trestných veciach, a to buď na základe individuálnych petícií, alebo prostredníctvom vyšetrovaní *ex officio* ([278]).

(173) Po štvrté všeobecný dozor nad zákonnosťou činností orgánov verejnej moci vykonáva Rada pre audit a inšpekciu, ktorá skúma príjmy a výdavky štátu, ale všeobecnejšie dozerá aj na dodržiavanie povinností orgánov verejnej moci s cieľom zlepšiť činnosť verejnej správy ([279]). Rada pre audit a inšpekciu je formálne zriadená v rámci Úradu prezidenta Kórejskej republiky, pri vykonávaní svojich povinností má však nezávislé postavenie ([280]). Okrem toho sa jej zaručuje úplná nezávislosť pri menovaní, odvolávaní a organizácii svojich zamestnancov, ako aj pri zostavovaní svojho rozpočtu ([281]). Rada pre audit a inšpekciu pozostáva z predsedu (menovaného prezidentom so súhlasom národného zhromaždenia) ([282]) a šiestich komisárov (menovaných prezidentom na odporúčanie predsedu) ([283]), ktorí musia mať osobitnú kvalifikáciu stanovenú zákonom ([284]) a môžu byť odvolaní len na základe konania o zbavení funkcie v rámci zákonodarnej moci, odsúdenia na trest odňatia slobody alebo neschopnosti vykonávať svoje povinnosti z dôvodu dlhodobých problémov s duševným alebo fyzickým zdravím ([285]). Rada pre audit a inšpekciu vykonáva každoročne generálny audit, môže však vykonávať aj osobitné audity týkajúce sa záležitostí osobitného významu. Pri vykonávaní auditu alebo inšpekcie môže Rada pre audit a inšpekciu požiadať o predloženie dokumentov a takisto si môže vyžiadať prítomnosť jednotlivcov ([286]). Rada pre audit a inšpekciu môže vydávať odporúčania, žiadať o disciplinárne konania alebo podávať trestné oznámenia ([287]).

(174) A napokon národné zhromaždenie vykonáva parlamentný dozor nad orgánmi verejnej moci prostredníctvom vyšetrovaní a inšpekcií ([288]) ich činností ([289]). Môže si vyžiadať sprístupnenie dokumentov a predvolať svedkov ([290]), odporučiť nápravné opatrenia (ak dospeje k záveru, že sa vykonali nezákonné alebo nevhodné

([274]) Článok 7 ods. 1 a článok 8 zákona o Národnej komisii pre ľudské práva.
([275]) Článok 36 zákona o Národnej komisii pre ľudské práva. V súlade s článkom 6 ods. 7 zákona možno predloženie materiálov alebo predmetov zamietnuť, ak by sa tým mohla ohroziť dôvernosť štátneho tajomstva, čo by malo závažný vplyv na štátnu bezpečnosť alebo diplomatické vzťahy, alebo ak by to predstavovalo závažnú prekážku vo vyšetrovaní trestnej činnosti, prípadne v prebiehajúcom súdnom konaní. V takých prípadoch môže Komisia požiadať o ďalšie informácie vedúceho príslušného orgánu (ktorý musí žiadosti v dobrej viere vyhovieť), ak je to potrebné na povolenie preskúmania toho, či bolo zamietnutie poskytnutia informácií opodstatnené.
([276]) Článok 25 ods. 1 a 3 zákona o Národnej komisii pre ľudské práva.
([277]) Článok 25 ods. 4 zákona o Národnej komisii pre ľudské práva.
([278]) V rokoch 2015 až 2019 napríklad Národná komisia pre ľudské práva prijala každoročne od 1 380 do 1 699 petícií proti orgánom presadzovania práva v trestných veciach, pričom z nich vybavila porovnateľne vysoký počet (napr. v roku 2018 vybavila 1 546 sťažností na políciu a v roku 2019 vybavila 1 249 sťažností); takisto uskutočnila viacero vyšetrovaní *ex officio*, ako sa podrobnejšie uvádza vo výročnej správe Národnej komisie pre ľudské práva za rok 2018 (k dispozícii na adrese https://www.humanrights.go.kr/site/program/board/basicboard/view?menuid=002003003001&pagesize=10&boardtypeid=7017&boardid=7602641) a vo výročnej správe za rok 2019 (k dispozícii na adrese https://www.humanrights.go.kr/site/program/board/basicboard/view?menuid=002003003001&pagesize=10&boardtypeid=7017&boardid=7606217).
([279]) Články 20 a 24 zákona o Rade pre audit a inšpekciu. Pozri prílohu II oddiel 2.3.2.
([280]) Článok 2 ods. 1 zákona o Rade pre audit a inšpekciu.
([281]) Článok 2 ods. 2 zákona o Rade pre audit a inšpekciu.
([282]) Článok 4 ods. 1 zákona o Rade pre audit a inšpekciu.
([283]) Článok 5 ods. 1 a článok 6 zákona o Rade pre audit a inšpekciu.
([284]) Napríklad aspoň desaťročná služba vo funkcii sudcu, prokurátora alebo advokáta, aspoň osemročná prax na pozícii zamestnanca verejnej správy alebo vysokoškolského profesora, prípadne na vyššej pozícii, alebo aspoň desaťročná prax v kótovanej spoločnosti alebo inštitúcií so štátnymi investíciami (z čoho aspoň päť rokov na výkonnej pozícii), pozri článok 7 zákona o Rade pre audit a inšpekciu. Okrem toho sa komisárom zakazuje účasť na politických činnostiach a súbežné zastávanie funkcií v národnom zhromaždení, správnych orgánoch, organizáciách podliehajúcich auditu a inšpekcii vykonávaných Radou pre audit a inšpekciu, ako aj ďalších odmeňovaných funkcií a pozícií (článok 9 zákona o Rade pre audit a inšpekciu).
([285]) Článok 8 zákona o Rade pre audit a inšpekciu.
([286]) Pozri napr. článok 27 zákona o Rade pre audit a inšpekciu.
([287]) Článok 24 a články 31 až 35 zákona o Rade pre audit a inšpekciu.
([288]) Článok 128 zákona o národnom zhromaždení a články 2, 3 a 15 zákona o inšpekcii a vyšetrovaní štátnej správy. Patria sem aj každoročné inšpekcie vládnych záležitostí ako takých, ale aj vyšetrovanie osobitných záležitostí.
([289]) Pozri prílohu oddiel 2.2.3.
([290]) Článok 10 ods. 1 zákona o inšpekcii a vyšetrovaní štátnej správy. Pozri aj články 128 a 129 zákona o národnom zhromaždení.

činnosti) ([291]) a zverejniť výsledky svojich zistení ([292]). Ak národné zhromaždenie nariadi prijatie nápravných opatrení – ktoré môžu zahŕňať napríklad náhradu škody, disciplinárne konanie alebo zlepšenie vnútorných postupov –, príslušný verejný orgán je povinný bezodkladne konať a o výsledku prijatých opatrení podať správu národnému zhromaždeniu ([293]).

3.2.4. *Prostriedky nápravy*

(175) Kórejský systém poskytuje rôzne (súdne) spôsoby dosiahnutia nápravy vrátane náhrady škody.

(176) Po prvé v zákone o ochrane osobných informácií sa jednotlivcom poskytuje právo na prístup, opravu, vymazanie a pozastavenie spracúvania, pokiaľ ide o osobné informácie spracúvané na účely presadzovania práva v trestných veciach ([294]).

(177) Po druhé môžu jednotlivci využiť rôzne mechanizmy nápravy poskytované v zákone o ochrane osobných informácií, ak ich údaje spracúval orgán presadzovania práva v trestných veciach v rozpore so zákonom o ochrane osobných informácií alebo v rozpore s obmedzeniami a zárukami, ktorými sa riadi získavanie osobných údajov v iných zákonoch (t. j. v zákone o trestnom konaní alebo v zákone o ochrane súkromia komunikácie, pozri odôvodnenie (171)). Konkrétne môžu jednotlivci podať sťažnosť Komisii pre ochranu osobných informácií (a to aj prostredníctvom call centra pre ochranu súkromia, ktoré prevádzkuje Kórejská agentúra pre internet a bezpečnosť ([295])) alebo Výboru pre mediáciu sporov týkajúcich sa osobných informácií ([296]). Tieto možnosti nápravy nepodliehajú ďalším požiadavkám na prípustnosť. Ďalej sa môžu jednotlivci odvolať proti rozhodnutiam alebo nečinnosti/napadnúť rozhodnutia alebo nečinnosť Komisie pre ochranu osobných informácií podľa Správneho súdneho poriadku (pozri odôvodnenie (132)).

(178) Po tretie môže každý jednotlivec ([297]) podať sťažnosť na Národnú komisiu pre ľudské práva týkajúcu sa porušenia práva na súkromie a ochranu údajov zo strany kórejského orgánu presadzovania práva v trestných veciach. Národná komisia pre ľudské práva môže odporučiť opravu, prípadne zlepšenie všetkých príslušných právnych predpisov, inštitúcií, politík alebo postupov ([298]) alebo vykonanie prostriedkov nápravy, ako je mediácia ([299]), ukončenie porušovania ľudských práv, náhrada škody a opatrenia na zabránenie opakovaniu tých istých alebo podobných porušení ([300]). Podľa oficiálneho zastúpenia kórejskej vlády (oddiel 2.4.2 prílohy II) to môže zahŕňať aj vymazanie nezákonne získaných osobných údajov. V prípadoch, v ktorých Národná komisia pre ľudské práva nemá právomoc vydávať záväzné rozhodnutia, sa poskytuje neformálnejší nízkonákladový a jednoducho prístupný spôsob nápravy, a to najmä preto, že na vyšetrenie sťažnosti sa nevyžaduje preukázanie faktickej ujmy, ako sa vysvetľuje v prílohe II oddiele 2.4.2 ([301]). Tým sa zaručí, že sťažnosti jednotlivcov týkajúce sa získavania ich údajov možno vyšetrovať, a to aj v prípade, že jednotlivec nedokáže preukázať, že jeho údaje sa naozaj získali (napr. preto, že sa to jednotlivcovi ešte neoznámilo). Z výročných správ o činnosti Národnej komisie pre ľudské práva vyplýva, že jednotlivci v praxi využívajú tento spôsob aj na napadnutie činností orgánov presadzovania práva v trestných veciach, a to aj v súvislosti so spracúvaním osobných údajov ([302]). Ak jednotlivec nie je spokojný s výsledkom konania pred Národnou komisiou pre ľudské práva, môže napadnúť rozhodnutia

([291]) Článok 16 ods. 2 zákona o inšpekcii a vyšetrovaní štátnej správy.
([292]) Článok 12-2 zákona o inšpekcii a vyšetrovaní štátnej správy.
([293]) Článok 16 ods. 3 zákona o inšpekcii a vyšetrovaní štátnej správy.
([294]) Toto právo možno uplatniť priamo voči príslušnému orgánu alebo nepriamo voči Komisii pre ochranu osobných informácií (článok 35 ods. 2 zákona o ochrane osobných informácií). Ako sa podrobne uvádza v odôvodneniach (76) – (78), výnimky z týchto práv sa uplatňujú len vtedy, ak je to potrebné na ochranu (verejných) záujmov.
([295]) Článok 62 zákona o ochrane osobných informácií.
([296]) Články 40 – 50 zákona o ochrane osobných informácií a články 48-2 až 57 vykonávacieho dekrétu k zákonu o ochrane osobných informácií. Pozri aj prílohu II oddiel 2.4.1.
([297]) Ako sa vysvetľuje v prílohe II oddiele 2.4.2, hoci sa v článku 4 zákona o Národnej komisii pre ľudské práva odvoláva na občanov a cudzincov s pobytom v Kórejskej republike, pojem „pobyt“ sa týka jurisdikcie, a nie územia. Preto ak kórejské vnútroštátne inštitúcie porušili základné práva cudzinca, ktorý nie je štátnym príslušníkom Kórey, daný jednotlivec môže podať sťažnosť Národnej komisii pre ľudské práva. Platí to v prípade, ak k osobným údajom cudzinca preneseným do Kórey získali nezákonný prístup kórejské orgány verejnej moci. Pozri najmä vysvetlenia uvedené na adrese https://www.humanrights.go.kr/site/program/board/basicboard/list?boardtypeid=7025&menuid=002004005001&pagesize=10&currentpage=2.
([298]) Článok 44 zákona o Národnej komisii pre ľudské práva.
([299]) Jednotlivec môže žiadať aj o vyriešenie sťažnosti prostredníctvom mediácie, pozri článok 42 a nasl. zákona o Národnej komisii pre ľudské práva.
([300]) Článok 42 ods. 4 zákona o Národnej komisii pre ľudské práva. Národná komisia pre ľudské práva môže okrem toho prijať naliehavé opatrenia na riešenie problému v prípade prebiehajúceho porušenia, pričom je pravdepodobné, že ak sa neodstráni, spôsobí škodu, ktorú je ťažké napraviť, pozri článok 48 zákona o Národnej komisii pre ľudské práva.
([301]) Sťažnosť sa musí v zásade podať do jedného roka od porušenia, Národná komisia pre ľudské práva však môže rozhodnúť aj o vyšetrení sťažnosti podanej po uplynutí jedného roku, ak neuplynula premlčacia lehota podľa trestného alebo občianskeho práva (článok 32 ods. 1 pododsek 4 zákona o Národnej komisii pre ľudské práva).
([302]) Národná komisia pre ľudské práva v minulosti napríklad riešila sťažnosti a vydala odporúčania v súvislosti s nezákonnými zaisteniami predmetov a porušením požiadavky informovať jednotlivcov o takomto zaistení predmetov (pozri s. 80 a 91 výročnej správy Národnej komisie pre ľudské práva z roku 2018, k dispozícii na adrese https://www.humanrights.go.kr/site/program/board/basicboard/view?menuid=002003003001&pagesize=10&boardtypeid=7017&boardid=7604746), ako aj nezákonným spracúvaním osobných informácií políciou, prokuratúrou a súdmi (pozri s. 157 – 158 výročnej správy Národnej komisie pre ľudské práva z roku 2019, k dispozícii na adrese https://www.humanrights.go.kr/site/program/board/basicboard/view?menuid=002003003001&pagesize=10&boardtypeid=7017&boardid=7603308, a s. 76 výročnej správy z roku 2019, k dispozícii na adrese https://www.humanrights.go.kr/site/program/board/basicboard/view?menuid=002003003001&pagesize=10&boardtypeid=7017&boardid=7606217).

(napríklad rozhodnutie nepokračovať vo vyšetrovaní sťažnosti ([303])) a odporúčania Národnej komisie pre ľudské práva na kórejských súdoch podľa Správneho súdneho poriadku (pozri odôvodnenie (181)) ([304]). Okrem toho môže konanie pred Národnou komisiou pre ľudské práva ešte viac uľahčiť prístup k súdom, keďže jednotlivec by sa mohol v súlade s postupom uvedeným v odôvodneniach (181) – (183) domáhať ďalšieho prostriedku nápravy proti orgánu verejnej moci, ktorý podľa zistení Národnej komisie pre ľudské práva nezákonne spracúval jeho údaje.

(179) A napokon sú k dispozícii rôzne prostriedky súdnej nápravy, ktoré jednotlivcom umožňujú dosiahnuť nápravu odvolaním sa na obmedzenia a záruky uvedené v oddiele 3.2.1 ([305]).

(180) V súvislosti so zaistením predmetov (ako aj údajov) sa v zákone o trestnom konaní uvádza možnosť namietať proti vykonaniu súdneho príkazu alebo napadnúť jeho vykonanie, a to prostredníctvom „kvázisťažnosti“ podaním žiadosti o zrušenie alebo úpravu právneho úkonu vydaného prokurátorom alebo príslušníkom polície na príslušný súd ([306]).

(181) Všeobecnejšie platí, že jednotlivci môžu napadnúť konanie ([307]) alebo opomenutia ([308]) orgánov verejnej moci (vrátane orgánov presadzovania práva v trestných veciach) na základe Správneho súdneho poriadku ([309]). Správne opatrenie sa považuje za „napadnuteľný právny úkon“, ak má priamy vplyv na občianske práva a povinnosti ([310]), čo je, ako potvrdila kórejská vláda (oddiel 2.4.3 prílohy II), prípad opatrení na získavanie osobných údajov, a to priamo (napríklad prostredníctvom odpočúvania komunikácie), prostredníctvom záväzných žiadostí o sprístupnenie informácií (určených napríklad poskytovateľovi služieb) alebo žiadostí o dobrovoľnú spoluprácu. Sťažnosť podaná na základe Správneho súdneho poriadku je prípustná vtedy, ak má jednotlivec právny záujem na uplatnení nároku ([311]). Podľa judikatúry najvyššieho súdu možno „právny záujem“ vykladať ako „právom chránený záujem“, t. j. priamy a osobitný záujem chránený zákonmi a právnymi predpismi, z ktorých vychádzajú správne úkony (teda nie ako všeobecný, nepriamy a abstraktný záujem verejnosti) ([312]). Jednotlivci majú takýto právny záujem v prípade každého porušenia obmedzení a záruk, ktoré sa uplatňujú na získavanie ich osobných údajov na účely presadzovania práva v trestných veciach (podľa osobitných zákonov alebo zákona o ochrane osobných informácií). Na základe Správneho súdneho poriadku môže súd rozhodnúť o zrušení alebo úprave nezákonného právneho úkonu, určení jeho neplatnosti (t. j. určení toho, že právny úkon nemá právny účinok alebo v právnom poriadku neexistuje) alebo o nezákonnosti daného opomenutia ([313]). Rozsudok, ktorým sa konanie o veci končí, vydaný na základe Správneho súdneho poriadku je pre strany konania záväzný ([314]).

([303]) Ak napríklad Národná komisia pre ľudské práva výnimočne nedokáže vykonať inšpekciu určitých materiálov alebo zariadení, pretože predstavujú štátne tajomstvo, ktoré môže mať závažný vplyv na štátnu bezpečnosť alebo diplomatické vzťahy, alebo ak by takáto inšpekcia predstavovala závažnú prekážku vo vyšetrovaní trestnej činnosti, prípadne v prebiehajúcom súdnom konaní, čo bráni Národnej komisii pre ľudské práva vykonať vyšetrovanie potrebné na posúdenie predmetu petície, v súlade s článkom 39 zákona o Národnej komisii pre ľudské práva informuje jednotlivca o dôvodoch, na základe ktorých sťažnosť zamietla. V takom prípade by jednotlivec mohol napadnúť rozhodnutie Národnej komisie pre ľudské práva podľa Správneho súdneho poriadku.

([304]) Pozri napr. rozhodnutie Najvyššieho soulského súdu č. 2007Nu27259 z 18. apríla 2008, potvrdené rozhodnutím najvyššieho súdu č. 2008Du7854 z 9. októbra 2008; rozhodnutie Najvyššieho soulského súdu č. 2017Nu69382 z 2. februára 2018.

([305]) Pozri prílohu II oddiel 2.4.3.

([306]) Článok 417 zákona o trestnom konaní v spojení s článkom 414 ods. 2 zákona o trestnom konaní. Pozri aj rozhodnutie najvyššieho súdu č. 97Mo66 z 29. septembra 1997.

([307]) V Správnom súdnom poriadku sa odkazuje na „právny úkon“, t. j. výkon alebo zamietnutie výkonu verejnej moci v konkrétnom prípade.

([308]) Podľa Správneho súdneho poriadku to znamená dlhodobé nekonanie správneho orgánu pri prijímaní určitého právneho úkonu, ktorý má zákonnú povinnosť prijať.

([309]) Napadnutie v správnom konaní možno ako neformálnejší spôsob dosiahnutia nápravy najskôr predložiť komisiám pre správne opravné prostriedky, ktoré sú zriadené v rámci niektorých orgánov verejnej moci (napr. Národnej spravodajskej službe, Národnej komisii pre ľudské práva), alebo ústrednej komisii pre správne opravné prostriedky zriadenej v rámci Komisie pre občianske práva a boj proti korupcii (článok 6 zákona o správnych opravných prostriedkoch a článok 18 ods. 1 Správneho súdneho poriadku). Podnet však možno podať aj priamo na kórejské súdy, a to na základe Správneho súdneho poriadku.

([310]) Rozhodnutie najvyššieho súdu č. 98Du18435 z 22. októbra 1999, rozhodnutie najvyššieho súdu č. 99Du1113 z 8. septembra 2000 a rozhodnutie najvyššieho súdu č. 2010Du3541 z 27. septembra 2012.

([311]) Články 12, 35 a 36 Správneho súdneho poriadku. Okrem toho sa žiadosť o zrušenie/úpravu právneho úkonu a žiadosť o potvrdenie nezákonnosti opomenutia musí podať do 90 dní odo dňa, keď sa jednotlivec dozvedel o právnom úkone/opomenutí, a v zásade najneskôr jeden rok odo dňa vydania právneho úkonu alebo výskytu opomenutia, ak tomu nebránia opodstatnené dôvody (článok 20 a článok 38 ods. 2 Správneho súdneho poriadku). Pojem „opodstatnené dôvody“ vykladá najvyšší súd široko a vyžaduje si posúdenie toho, či je vzhľadom na všetky okolnosti prípadu spoločensky prijateľné umožniť podanie oneskorenej sťažnosti (rozhodnutie najvyššieho súdu č. 90Nu6521 z 28. júna 1991). Ako potvrdila kórejská vláda v oddiele 2.4.3 prílohy II, patria sem napríklad (nie však výhradne) dôvody oneskorenia, ktoré nezapríčinila dotknutá strana (t. j. situácie, na ktoré nemá sťažovateľ vplyv, ako napríklad, že nebol informovaný o získavaní svojich osobných údajov) alebo vyššia moc (napr. prírodná katastrofa, vojna).

([312]) Rozhodnutie najvyššieho súdu č. 2006Du330 z 26. marca 2006.

([313]) Články 2 a 4 Správneho súdneho poriadku.

([314]) Článok 30 ods. 1 Správneho súdneho poriadku.

(182) Okrem napadnutia opatrení vlády prostredníctvom správneho konania môžu jednotlivci podať aj ústavnú sťažnosť na ústavný súd týkajúcu sa akéhokoľvek porušenia ich základných práv v dôsledku výkonu alebo nevykonania štátnej moci (s výnimkou rozsudkov súdov) ([315]). Ak sú k dispozícii iné nápravné prostriedky, musia sa využiť ako prvé. Podľa judikatúry ústavného súdu môžu cudzí štátni príslušníci podať ústavnú sťažnosť v rozsahu, v akom sa ich základné práva uznávajú podľa kórejskej ústavy (pozri vysvetlenia v oddiele 1.1) ([316]). Ústavný súd môže zrušiť platnosť výkonu štátnej moci, ktorý spôsobil porušenie, alebo potvrdiť, že určité nekonanie je protiústavné ([317]). V takom prípade musí príslušný orgán prijať opatrenia na vykonanie rozhodnutia súdu.

(183) Okrem toho môžu jednotlivci na kórejských súdoch získať náhradu škody. Predovšetkým majú možnosť žiadať podľa článku 39 o náhradu škody za porušenie zákona o ochrane osobných informácií, ktorého sa dopustili orgány presadzovania práva v trestných veciach (pozri aj odôvodnenie (135)). Všeobecnejšie môžu jednotlivci podať žiadosť o náhradu škody za škody spôsobené verejnými činiteľmi pri vykonávaní ich úradných povinností v rozpore so zákonom na základe zákona o štátnom odškodnení (pozri aj odôvodnenie (135)) ([318]).

(184) Mechanizmy opísané v odôvodneniach (176) – (183) poskytujú dotknutým osobám účinné správne a súdne prostriedky nápravy, ktoré im umožňujú najmä uplatniť svoje práva vrátane práva na prístup k svojim osobným údajom alebo práva dosiahnuť opravu alebo vymazanie týchto údajov.

3.3. **Prístup a používanie zo strany kórejských orgánov verejnej moci na účely národnej bezpečnosti**

(185) Právo Kórejskej republiky obsahuje viacero obmedzení a záruk týkajúcich sa prístupu k osobným údajom a ich používania na účely národnej bezpečnosti a poskytuje mechanizmy dozoru a nápravy, ktoré sú v súlade s požiadavkami uvedenými v odôvodneniach (141) až (143) tohto rozhodnutia. Podmienky, za ktorých sa takýto prístup môže uskutočniť, a záruky, ktoré sa vzťahujú na uplatnenie týchto právomocí, sa podrobne posudzujú v nasledujúcich oddieloch.

3.3.1. *Právne základy, obmedzenia a záruky*

(186) V Kórejskej republike možno získať prístup k osobným údajom na účely národnej bezpečnosti na základe zákona o ochrane súkromia komunikácie, zákona o telekomunikáciách a zákona o boji proti terorizmu na ochranu občanov a verejnej bezpečnosti (ďalej len „zákon o boji proti terorizmu“) ([319]). Hlavným orgánom ([320]) s kompetenciami v oblasti národnej bezpečnosti je Národná spravodajská služba ([321]). Národná spravodajská služba môže získavať a používať osobné údaje v súlade s príslušnými právnymi požiadavkami (vyplývajúcimi zo zákona

([315]) Článok 68 ods. 1 zákona o ústavnom súde. Ústavné sťažnosti sa musia podať do 90 dní odo dňa, keď jednotlivec zistil porušenie, a do jedného roka od jeho výskytu. Ako sa vysvetľuje aj v prílohe II oddiele 2.4.3, vzhľadom na to, že postup podľa Správneho súdneho poriadku sa uplatňuje aj na žaloby podané podľa článku 40 zákona o ústavnom súde, bude sťažnosť prípustná aj vtedy, ak existujú „opodstatnené dôvody“ podľa výkladu judikatúry najvyššieho súdu opísaného v poznámke pod čiarou č 321. Ak je potrebné najskôr využiť ostatné prostriedky nápravy, ústavná sťažnosť sa musí podať do 30 dní od vydania konečného rozhodnutia o takomto prostriedku nápravy (článok 69 zákona o ústavnom súde).

([316]) Rozhodnutie ústavného súdu č. 99HeonMa194 z 29. novembra 2001.

([317]) Článok 75 ods. 3 zákona o ústavnom súde.

([318]) Článok 2 ods. 1 zákona o štátnom odškodnení.

([319]) Pozri prílohu II oddiel 3.1.

([320]) Výnimočne môže osobné informácie na účely národnej bezpečnosti získavať aj polícia a prokuratúra (pozri poznámku pod čiarou č. 327 a prílohu II oddiel 3.2.1.2). Právomoci v oblasti národnej bezpečnosti má navyše kórejský vojenský spravodajský orgán (Veliteľstvo pre podporu národnej obrany zriadené v rámci ministerstva obrany). Ako sa však vysvetľuje v prílohe II oddiele 3.1, zodpovedá len za vojenské spravodajstvo a sledovanie civilných osôb vykonáva len vtedy, ak je to potrebné na výkon jeho vojenských funkcií. Konkrétne môže vyšetrovať len vojenský personál, civilných zamestnancov armády, osoby absolvujúce vojenskú odbornú prípravu, príslušníkov v zálohe, brancov a vojnových zajatcov (článok 1 zákona o vojenskom súde). Pri získavaní informácií o komunikácii na účely národnej bezpečnosti sa na Veliteľstvo pre podporu národnej obrany vzťahujú obmedzenia a záruky stanovené v zákone o ochrane súkromia komunikácie a v jeho vykonávacom dekréte.

([321]) Národná spravodajská služba má mandát na získavanie, zostavovanie a distribúciu informácií o cudzích krajinách (t. j. všeobecných informácií o trendoch a vývoji vo vzťahu k cudzím krajinám alebo o činnostiach štátnych subjektov); spravodajských informácií v súvislosti s kontrašpionážou (vrátane vojenskej a priemyselnej špionáže), terorizmom a činnosťami medzinárodných zločineckých syndikátov; spravodajských informácií o určitých druhoch trestnej činnosti namierenej proti verejnosti a národnej bezpečnosti (napr. domáce povstanie, zahraničná agresia), ako aj spravodajských informácií v súvislosti s úlohou zabezpečovania kybernetickej bezpečnosti a zabraňovania kybernetickým útokom a hrozbám alebo bojom proti nim (článok 4 ods. 2 zákona o Národnej spravodajskej službe). Pozri aj prílohu II oddiel 3.1.

o ochrane osobných informácií a zákona o ochrane súkromia komunikácie) ([322]) a všeobecnými usmerneniami vypracovanými prezidentom a preskúmanými národným zhromaždením ([323]). Vo všeobecnosti platí, že Národná spravodajská služba musí zachovávať politickú neutralitu a chrániť slobodu a práva jednotlivcov ([324]). Okrem toho Národná spravodajská služba nesmie zneužívať svoju úradnú moc na to, aby nútila akúkoľvek inštitúciu, organizáciu alebo jednotlivca do činnosti, ktorú nemá povinnosť vykonávať (zo zákona), ani nesmie nikomu brániť v uplatňovaní svojich práv ([325]).

3.3.1.1. Prístup k informáciám o komunikácii

(187) Na základe zákona o ochrane súkromia komunikácie môžu kórejské orgány verejnej moci ([326]) získavať potvrdzujúce údaje o komunikácii (t. j. údaje o telekomunikácii, čase jej začatia a ukončenia, počte odchádzajúcich a prichádzajúcich hovorov, ako aj účastníckom čísle druhej strany, frekventovanosti využívania, logoch týkajúcich sa používania telekomunikačných služieb a informácií o polohe, pozri odôvodnenie (155)) a obsah komunikácie (prostredníctvom opatrení na zachytenie komunikácie, pozri odôvodnenie (155)) na účely národnej bezpečnosti (ako sa to stanovuje v mandáte Národnej spravodajskej služby, pozri poznámku pod čiarou č. 322). Tieto právomoci sú rozšírené na dva druhy informácií: 1. komunikáciu, ktorej jednu alebo obe strany tvoria kórejskí štátni príslušníci ([327]); a 2. komunikáciu a) krajín s nepriateľským postojom ku Kórejskej republike; b) zahraničných agentúr, skupín alebo štátnych príslušníkov podozrivých z účasti na protikórejských činnostiach ([328]) alebo c) členov skupín pôsobiacich na Kórejskom polostrove, no mimo suverenity Kórejskej republiky, a ich zastrešujúcich skupín so sídlom v cudzích krajinách ([329]). Komunikáciu jednotlivcov z EÚ prenášanú z Únie do Kórejskej republiky na základe tohto rozhodnutia možno preto získavať iba podľa zákona o ochrane súkromia komunikácie na účely národnej bezpečnosti (na základe podmienok stanovených v odôvodneniach (188) – (192)) vtedy, ak ide buď o komunikáciu medzi jednotlivcom z EÚ a kórejským štátnym príslušníkom, alebo výlučne medzi cudzími štátnymi príslušníkmi, ktorá patrí do niektorej z troch uvedených kategórií z odseku 2 písm. a), b) a c).

(188) V oboch situáciách možno získavanie potvrdzujúcich údajov o komunikácii vykonávať iba na účel predchádzania hrozbám pre národnú bezpečnosť ([330]), pričom opatrenia na zachytenie komunikácie možno prijať iba vtedy, ak hrozí veľké nebezpečenstvo v oblasti národnej bezpečnosti a získanie informácií je potrebné na to, aby sa mu zabránilo ([331]). Okrem toho môže byť prístup k obsahu komunikácie povolený iba ako posledná možnosť, pričom je potrebné vyvinúť úsilie s cieľom minimalizovať porušovanie súkromia komunikácie ([332]), čiže zabezpečiť, aby zostalo primerané k sledovanému cieľu v oblasti národnej bezpečnosti. Získavanie obsahu komunikácie, ako aj potvrdzujúcich údajov o komunikácii môže trvať maximálne štyri mesiace a ak sa sledovaný cieľ dosiahne skôr, musí sa okamžite ukončiť ([333]). Ak sú príslušné podmienky naďalej splnené, obdobie možno predĺžiť na základe predchádzajúceho povolenia súdu (v prípade opatrení uvedených v odôvodnení (189)) alebo prezidenta (v prípade opatrení uvedených v odôvodnení (190)) ([334]), a to najviac o ďalšie štyri mesiace.

(189) Tie isté procesné záruky sa uplatňujú na získavanie potvrdzujúcich údajov o komunikácii a obsahu komunikácie ([335]). Konkrétne platí, že ak je aspoň jedna osoba zapojená do komunikácie kórejským štátnym príslušníkom, spravodajský orgán musí predložiť písomnú žiadosť generálnej prokuratúre, ktorá potom musí

([322]) Pozri aj články 14, 22 a 23 zákona o Národnej spravodajskej službe.
([323]) Článok 4 ods. 2 zákona o Národnej spravodajskej službe.
([324]) Článok 3 ods. 1, článok 6 ods. 2, články 11, 21 zákona o Národnej spravodajskej službe. Pozri aj pravidlá týkajúce sa konfliktov záujmov, najmä články 10, 12 zákona o Národnej spravodajskej službe.
([325]) Článok 13 zákona o Národnej spravodajskej službe.
([326]) Ako napríklad spravodajské orgány (t. j. Národná spravodajská služba a Veliteľstvo pre podporu národnej obrany), ako aj polícia/prokuratúra.
([327]) Článok 7 ods. 1 pododsek 1 zákona o ochrane súkromia komunikácie.
([328]) Ako vysvetlila kórejská vláda v poznámke pod čiarou č. 244 z prílohy II, ide o činnosti ohrozujúce existenciu a bezpečnosť národa, demokratické usporiadanie štátu alebo prežitie a slobodu ľudí.
([329]) Článok 7 ods. 1 pododsek 2 zákona o ochrane súkromia komunikácie.
([330]) Článok 13-4 zákona o ochrane súkromia komunikácie.
([331]) Článok 7 ods. 1 zákona o ochrane súkromia komunikácie.
([332]) Článok 3 ods. 2 zákona o ochrane súkromia komunikácie. Okrem toho je potrebné opatrenia na zachytenie komunikácie bezodkladne ukončiť, keď už nie sú potrebné, a tým zabezpečiť čo najmenšie porušovanie komunikačného tajomstva jednotlivcov (článok 2 vykonávacieho dekrétu k zákonu o ochrane súkromia komunikácie).
([333]) Článok 7 ods. 2 zákona o ochrane súkromia komunikácie.
([334]) Žiadosť o získanie súhlasu s predĺžením opatrení sledovania musí byť podaná písomne a spoločne so sprievodnými materiálmi musí obsahovať dôvody, na základe ktorých sa žiada o predĺženie (článok 7 ods. 2 zákona o ochrane súkromia komunikácie a článok 5 vykonávacieho dekrétu k zákonu o ochrane súkromia komunikácie).
([335]) Pozri článok 13-4 ods. 2 zákona o ochrane súkromia komunikácie a článok 37 ods. 4 vykonávacieho dekrétu k zákonu o ochrane súkromia komunikácie, podľa ktorých sa postupy uplatniteľné na získavanie obsahu komunikácie uplatňujú aj na získavanie potvrdzujúcich údajov o komunikácii. Pozri aj prílohu II oddiel 3.2.1.1.1.

požiadať predsedu najvyššieho súdu o vydanie súdneho príkazu ([336]). V zákone o ochrane súkromia komunikácie sa uvádzajú informácie, ktoré sa musia nachádzať v žiadosti podanej prokurátorovi, žiadosti o vydanie súdneho príkazu a v samotnom súdnom príkaze, konkrétne odôvodnenie žiadosti a hlavné dôvody podozrenia, sprievodné materiály, ako aj informácie o zámere, cieli (t. j. zacielených jednotlivcoch), rozsahu a trvaní navrhovaného opatrenia ([337]). Získavanie informácií bez súdneho príkazu sa môže vykonávať len vtedy, ak existuje sprisahanie, ktoré ohrozuje národnú bezpečnosť, pričom mimoriadna situácia bráni dodržaniu uvedených postupov ([338]). Aj v takom prípade je však potrebné ihneď po prijatí opatrenia podať žiadosť o vydanie súdneho príkazu ([339]). V zákone o ochrane súkromia komunikácie sa teda jednoznačne vymedzuje rozsah a podmienky týchto druhov získavania informácií, pričom sa na ne vzťahujú osobitné (procesné) záruky (vrátane predchádzajúceho súhlasu súdu), ktorými sa zabezpečuje obmedzenie používania týchto opatrení na potrebný a primeraný rozsah. Požiadavkou na poskytnutie podrobných informácií pri podávaní žiadosti o vydanie súdneho príkazu, ako aj v samotnom súdnom príkaze sa okrem toho zabraňuje možnosti neobmedzeného prístupu.

(190) V prípade komunikácie medzi cudzími štátnymi príslušníkmi, ktorá patrí do niektorej z troch osobitných kategórií uvedených v odôvodnení (187), sa musí žiadosť podať riaditeľovi Národnej spravodajskej služby, ktorý musí po preskúmaní vhodnosti navrhovaných opatrení požiadať prezidenta Kórejskej republiky o predchádzajúci písomný súhlas ([340]). Žiadosť vypracovaná spravodajským orgánom musí obsahovať tie isté podrobné informácie ako žiadosť o vydanie súdneho príkazu (pozri odôvodnenie (189)), konkrétne odôvodnenie žiadosti a hlavné dôvody podozrenia, sprievodné materiály a informácie o zámeroch, zacielených jednotlivcoch, rozsahu a trvaní navrhovaných opatrení ([341]). V mimoriadnych situáciách ([342]) je potrebné získať predchádzajúci súhlas ministra, pod ktorého príslušný spravodajský orgán patrí, hoci spravodajský orgán musí požiadať o súhlas prezidenta ihneď po prijatí mimoriadnych opatrení ([343]). Aj pokiaľ ide o získavanie komunikácie výlučne medzi cudzími štátnymi príslušníkmi, sa v zákone o ochrane súkromia komunikácie obmedzuje používanie takýchto opatrení na to, čo je potrebné a primerané, a to jednoznačným zúžením obmedzených kategórií jednotlivcov, na ktorých sa môžu takéto opatrenia vzťahovať, a stanovením podrobných kritérií, ktoré musia spravodajské orgány dodržať na odôvodnenie žiadosti o získavanie informácií. Okrem toho sa tým opäť vylučuje možnosť neobmedzeného prístupu. Keďže tieto opatrenia si nevyžadujú žiadny predchádzajúci súhlas, nezávislý dozor zabezpečuje *ex post* najmä Komisia pre ochranu osobných informácií a Národná komisia pre ľudské práva (pozri napríklad odôvodnenia (199) – (200)).

(191) V zákone o ochrane súkromia komunikácie sa ďalej ukladá viacero dodatočných záruk, ktoré prispievajú k dozoru *ex post* a uľahčujú prístup jednotlivcov k účinným prostriedkom nápravy. Po prvé sa v zákone o ochrane súkromia komunikácie stanovujú rôzne spôsoby uchovávania záznamov a požiadavky na oznamovanie týkajúce sa každého druhu získavania informácií na účely národnej bezpečnosti. Najmä ak sa žiadajú o spoluprácu súkromné subjekty, spravodajské orgány im musia predložiť súdny príkaz/povolenie prezidenta alebo kópiu obálky vyhlásenia o mimoriadnej cenzúre, ktorú musí dožiadaný subjekt uchovávať vo svojej evidencii ([344]). Ak súkromné subjekty musia spolupracovať, žiadajúci orgán verejnej moci aj príslušný subjekt musia uchovávať záznamy o účele

([336]) Článok 6 ods. 5 a 8, článok 7 ods. 1 pododsek 1 a článok 7 ods. 3 zákona o ochrane súkromia komunikácie v spojení s článkom 7 ods. 3 až 4 vykonávacieho dekrétu k zákonu o ochrane súkromia komunikácie.

([337]) Pozri článok 7 ods. 3 a článok 6 ods. 4 zákona o ochrane súkromia komunikácie (v prípade žiadosti podanej spravodajským orgánom), článok 4 vykonávacieho dekrétu k zákonu o ochrane súkromia komunikácie (v prípade žiadosti podávanej prokurátorom) a článok 7 ods. 3 a článok 6 ods. 6 zákona o ochrane súkromia komunikácie (v prípade súdneho príkazu).

([338]) Článok 8 zákona o ochrane súkromia komunikácie.

([339]) Článok 8 ods. 2 a 8 zákona o ochrane súkromia komunikácie. Získavanie informácií sa musí okamžite ukončiť, ak sa povolenie súdu nezíska do 36 hodín od prijatia opatrení. Ak sa sledovanie ukončí v krátkom čase bez povolenia súdu, vedúci príslušnej generálnej prokuratúry musí zaslať oznámenie o mimoriadnom opatrení, ktoré vypracoval spravodajský orgán, vedúcemu príslušného súdu, ktorý môže na tomto základe preskúmať zákonnosť získavania informácií (článok 8 ods. 5 a 7 zákona o ochrane súkromia komunikácie). V tomto oznámení sa musí uvádzať zámer, cieľ, rozsah, obdobie uplatňovania, miesto vykonávania a metóda sledovania, ako aj dôvody nepodania žiadosti pred prijatím opatrenia (článok 8 ods. 6 zákona o ochrane súkromia komunikácie). Všeobecnejšie platí, že spravodajské orgány môžu prijať mimoriadne opatrenia len v súlade s „vyhlásením o mimoriadnej cenzúre/odpočúvaní“, pričom musia o týchto opatreniach uchovávať záznamy (článok 8 ods. 4 zákona o ochrane súkromia komunikácie).

([340]) Článok 8 ods. 1 a 2 vykonávacieho dekrétu k zákonu o ochrane osobných informácií.

([341]) Článok 8 ods. 3 vykonávacieho dekrétu k zákonu o ochrane súkromia komunikácie v spojení s článkom 6 ods. 4 zákona o ochrane súkromia komunikácie.

([342]) Teda v prípadoch, keď sú opatrenia zamerané na sprisahanie, ktoré ohrozuje národnú bezpečnosť, a nie je dostatok času na získanie súhlasu prezidenta, pričom neprijatie mimoriadnych opatrení môže ohroziť národnú bezpečnosť (článok 8 ods. 8 zákona o ochrane súkromia komunikácie).

([343]) Článok 8 ods. 9 zákona o ochrane súkromia komunikácie. Získavanie informácií sa musí okamžite ukončiť, ak sa povolenie nezíska do 36 hodín od momentu podania žiadosti.

([344]) Článok 9 ods. 2 zákona o ochrane súkromia komunikácie a článok 12 vykonávacieho dekrétu k zákonu o ochrane súkromia komunikácie. Pozri článok 13 vykonávacieho dekrétu k zákonu o ochrane súkromia komunikácie týkajúci sa možnosti vynútenia spolupráce pôšt a poskytovateľov telekomunikačných služieb. Súkromné subjekty, ktorým bola adresovaná žiadosť o sprístupnenie informácií, môžu túto žiadosť odmietnuť, ak sa v súdnom príkaze/povolení alebo vyhlásení o mimoriadnej cenzúre uvádza nesprávny identifikátor (napr. telefónne číslo patriace inému ako identifikovanému jednotlivcovi). V každom prípade majú zakázané sprístupniť heslá používané na komunikáciu (článok 9 ods. 4 zákona o ochrane súkromia komunikácie).

a zámere opatrení, ako aj o dátume ich vykonania ([345]). Okrem toho musia spravodajské orgány podávať riaditeľovi Národnej spravodajskej služby správy o informáciách, ktoré získali, ako aj o výsledkoch činnosti sledovania ([346]).

(192) Po druhé musí byť jednotlivcom oznámené získavanie ich údajov (potvrdzujúcich údajov o komunikácii alebo obsahu komunikácie) na účely národnej bezpečnosti, ak sa týka komunikácie, v ktorej je aspoň jednou zo strán kórejský štátny príslušník ([347]). Toto oznámenie je potrebné predložiť písomne do 30 dní odo dňa ukončenia získavania informácií (a to aj vtedy, ak sa údaje získali v súlade s mimoriadnym postupom) a možno ho odložiť len vtedy, ak a na tak dlho, ako by predstavovalo hrozbu pre národnú bezpečnosť alebo život či fyzickú bezpečnosť ľudí ([348]). Bez ohľadu na takéto oznámenie môžu jednotlivci dosiahnuť prostriedok nápravy rôznymi spôsobmi, ako sa podrobnejšie vysvetľuje v oddiele 3.3.4.

3.3.1.2. Získavanie informácií o osobách podozrivých z terorizmu

(193) V zákone o boji proti terorizmu sa stanovuje, že Národná spravodajská služba môže získavať údaje o osobách podozrivých z terorizmu ([349]) v súlade s obmedzeniami a zárukami stanovenými v iných zákonoch ([350]). Konkrétne môže Národná spravodajská služba získavať údaje o komunikácii (na základe zákona o ochrane súkromia komunikácie) a ďalšie osobné informácie (na základe žiadosti o dobrovoľné sprístupnenie informácií) ([351]). Pokiaľ ide o získavanie informácií o komunikácii (t. j. obsahu komunikácie alebo potvrdzujúcich údajov o komunikácii), uplatňujú sa obmedzenia a záruky uvedené v oddiele 3.3.1.1 vrátane požiadavky na získanie súdneho príkazu. Pokiaľ ide o žiadosti o dobrovoľné sprístupnenie iných druhov osobných údajov o osobách podozrivých z terorizmu, Národná spravodajská služba musí dodržiavať požiadavky ústavy a zákona o ochrane osobných informácií týkajúce sa nevyhnutnosti a primeranosti (pozri odôvodnenie (164)) ([352]). Prevádzkovatelia môžu takýmto žiadostiam vyhovieť dobrovoľne pri splnení podmienok stanovených v zákone o ochrane osobných informácií (napríklad v súlade so zásadou minimalizácie údajov a obmedzením vplyvu na súkromie jednotlivca) ([353]). V tomto prípade musia spĺňať aj požiadavku na oznámenie dotknutému jednotlivcovi na základe oznámenia č. 2021-5 (pozri odôvodnenie (166)).

([345]) V prípade opatrení na zachytenie komunikácie sa takéto záznamy musia uchovávať tri roky, pozri článok 9 ods. 3 zákona o ochrane súkromia komunikácie a článok 17 ods. 2 vykonávacieho dekrétu k zákonu o ochrane súkromia komunikácie. Pri potvrdzujúcich údajoch o komunikácii musia spravodajské orgány uchovávať záznamy o predložení žiadosti o takéto údaje, ako aj samotnú písomnú žiadosť a informácie o inštitúcii, ktorá ich využívala (článok 13 ods. 5 a článok 13-4 ods. 3 zákona o ochrane súkromia komunikácie). Poskytovatelia telekomunikačných služieb musia uchovávať záznamy sedem rokov a dvakrát ročne podávať ministrovi pre vedu a IKT správy o frekventovanosti sprístupňovania informácií (článok 9 ods. 3 zákona o ochrane súkromia komunikácie v spojení s článkom 13 ods. 7 zákona o ochrane súkromia komunikácii a článkom 37 ods. 4 a článkom 39 vykonávacieho dekrétu k zákonu o ochrane súkromia komunikácie).

([346]) Článok 18 ods. 3 vykonávacieho dekrétu k zákonu o ochrane súkromia komunikácie.

([347]) Článok 9-2 ods. 3 a článok 13-4 zákona o ochrane súkromia komunikácie. Oznámenie musí obsahovať 1. skutočnosť, že sa získavali informácie; 2. ktorý výkonný orgán získavanie vykonával; a 3. obdobie, počas ktorého sa získavanie vykonávalo.

([348]) Článok 9-2 ods. 4 zákona o ochrane súkromia komunikácie. V uvedenom prípade sa musí oznámenie predložiť do 30 dní po uplynutí dôvodov na odloženie, pozri článok 13-4 ods. 2 a článok 9-2 ods. 6 zákona o ochrane súkromia komunikácie.

([349]) Čiže členoch teroristickej skupiny (podľa určenia Organizáciou Spojených národov, pozri článok 2 ods. 2 zákona o boji proti terorizmu); osobách, ktoré propagujú a šíria myšlienky alebo taktiky teroristickej skupiny, získavajú finančné prostriedky na účely terorizmu alebo ho financujú, prípadne sa zapájajú do iných činností prípravy, sprisahania, propagandy alebo podnecovania terorizmu; alebo osobách, v prípade ktorých existujú dobré dôvody na podozrenie z vykonávania takýchto činností (článok 2 ods. 3 zákona o boji proti terorizmu). „Terorizmus“ sa podľa článku 2 ods. 1 zákona o boji proti terorizmu vymedzuje ako čin, ktorého cieľom je ochromiť činnosť štátneho orgánu, miestnej samosprávy alebo zahraničnej vlády (vrátane medzinárodných organizácií), alebo ich donútiť vykonať činnosť, ktorá nepatrí k ich zákonným povinnostiam, prípadne ohroziť verejnosť. K takýmto činom môže patriť napríklad zabitie, únos alebo vzatie osoby za rukojemníka; únos/obsadenie, zničenie alebo poškodenie lode alebo lietadla; použitie biochemických, výbušných alebo zápalných zbraní s cieľom spôsobiť smrť, závažnú ujmu alebo škodu; a zneužitie jadrových alebo rádioaktívnych materiálov.

([350]) Článok 9 ods. 1 a 3 zákona o boji proti terorizmu.

([351]) Hoci sa v zákone o boji proti terorizmu odkazuje aj na možnosť získavania informácií o vstupe do Kórejskej republiky a odchode z nej na základe imigračného zákona a colného zákona, tieto zákony v súčasnosti takúto právomoc neobsahujú (pozri oddiel 3.2.2.1 prílohy II). V každom prípade by sa v zásade neuplatňovali na údaje prenášané na základe tohto rozhodnutia, keďže by sa zvyčajne týkali informácií, ktoré by získavali priamo kórejské orgány (a nie prístupu k údajom, ktoré sa už predtým preniesli z Únie kórejským prevádzkovateľom). Okrem toho sa v zákone o boji proti terorizmu uvádza zákon o oznamovaní a používaní špecifikovaných informácií o finančných transakciách ako právny základ pre získavanie informácií o finančných transakciách. Ako sa však vysvetľuje v poznámke pod čiarou č. 200, druhy údajov, ktoré by sa mohli získavať na základe tohto zákona, nepatria do rozsahu pôsobnosti tohto rozhodnutia. A napokon sa v zákone o boji proti terorizmu stanovuje aj to, že Národná spravodajská služba môže získavať informácie o polohe na základe nezáväzných žiadostí, pričom v takom prípade by poskytovatelia informácií o polohe mohli dobrovoľne sprístupniť takéto informácie na základe podmienok stanovených v zákone o ochrane osobných informácií (ako sa opisujú v odôvodnení (193)) a zákona o informáciách o polohe. Ako sa však vysvetľuje aj v poznámke pod čiarou č. 17, informácie o polohe by sa na základe tohto rozhodnutia neprenášali z Únie kórejským prevádzkovateľom, ale vytvárali by sa v Kórei.

([352]) Pozri prílohu II oddiel 3.2.2.2.

([353]) Pozri článok 58 ods. 4 zákona o ochrane osobných informácií, v ktorom sa vyžaduje, aby sa osobné informácie spracúvali v minimálnom potrebnom rozsahu na dosiahnutie zamýšľaného účelu, a článok 3 ods. 6 zákona o ochrane osobných informácií, v ktorom sa stanovuje, že osobné informácie sa musia spracúvať tak, aby sa minimalizovala možnosť narušenia súkromia jednotlivca. Pozri aj článok 59 pododseky 2 a 3 zákona o ochrane osobných informácií, podľa ktorého sa prevádzkovateľom zakazuje sprístupňovať osobné informácie tretím stranám bez povolenia.

3.3.1.3. Žiadosti o dobrovoľné sprístupnenie údajov o účastníkoch

(194) Na základe zákona o telekomunikáciách môžu poskytovatelia telekomunikačných služieb dobrovoľne sprístupniť údaje o účastníkoch (pozri odôvodnenie (163)) na žiadosť spravodajského orgánu, ktorý zamýšľa získať takéto informácie na účely zabránenia hrozbe pre národnú bezpečnosť ([354]). Pokiaľ ide o takéto žiadosti Národnej spravodajskej služby, uplatňujú sa tie isté obmedzenia (vyplývajúce z ústavy, zákona o ochrane osobných informácií a telekomunikačného zákona) ako v oblasti presadzovania práva v trestných veciach, ako sa to stanovuje v odôvodnení (164) ([355]). Poskytovatelia telekomunikačných služieb im nemusia vyhovieť, pričom urobiť tak môžu len po splnení podmienok stanovených v zákone o ochrane osobných informácií (konkrétne v súlade so zásadou minimalizácie údajov a obmedzenia vplyvu na súkromie jednotlivca, pozri aj odôvodnenie (193)). Tie isté požiadavky týkajúce sa uchovávania záznamov a oznamovania dotknutému jednotlivcovi sa uplatňujú aj v oblasti presadzovania práva v trestných veciach (pozri odôvodnenia (165) a (166)).

3.3.2. *Ďalšie používanie získaných informácií*

(195) Spracúvanie osobných údajov získaných kórejskými orgánmi na účely národnej bezpečnosti podlieha zásadám obmedzenia účelu (článok 3 ods. 1 až 2 zákona o ochrane osobných informácií), zákonnosti a spravodlivosti spracúvania (článok 3 ods. 1 zákona o ochrane osobných informácií), primeranosti/minimalizácie údajov (článok 3 ods. 1 a 6 a článok 58 zákona o ochrane osobných informácií), presnosti (článok 3 ods. 3 zákona o ochrane osobných informácií), transparentnosti (článok 3 ods. 5 zákona o ochrane osobných informácií), bezpečnosti (článok 58 ods. 4 zákona o ochrane osobných informácií) a obmedzenia uchovávania (článok 58 ods. 4 zákona o ochrane osobných informácií) ([356]). Možné sprístupnenie osobných údajov tretím stranám (vrátane tretích krajín) sa môže uskutočniť iba v súlade s týmito zásadami (konkrétne zásadou obmedzenia účelu a minimalizácie údajov) po posúdení súladu so zásadami nevyhnutnosti a primeranosti (článok 37 ods. 2 ústavy), pričom sa zohľadní vplyv na práva dotknutých jednotlivcov (článok 3 ods. 6 zákona o ochrane osobných informácií).

(196) Pokiaľ ide o obsah komunikácie a potvrdzujúce údaje o komunikácii, v zákone o ochrane súkromia komunikácie sa ďalej obmedzuje používanie týchto údajov na účely súdneho konania, v ktorom sa na ne odvoláva strana komunikácie, ktorá sa domáha náhrady škody; alebo na situácie, keď sa ich použitie povoľuje podľa iných zákonov ([357]).

3.3.3. *Dozor*

(197) Dozor nad činnosťami kórejských orgánov národnej bezpečnosti vykonávajú rôzne orgány ([358]).

(198) Po prvé sa v zákone o boji proti terorizmu stanovujú osobitné mechanizmy dozoru pre činnosti boja proti terorizmu vrátane získavania údajov o osobách podozrivých z terorizmu. Konkrétne na činnosti boja proti terorizmu dozerá na výkonnej úrovni Komisia na boj proti terorizmu ([359]), ktorej musí riaditeľ Národnej spravodajskej služby podávať správy o vyšetrovaniach a sledovaní osôb podozrivých z terorizmu na účely získania informácií alebo materiálov potrebných na činnosti v oblasti boja proti terorizmu ([360]). Okrem toho osobitne na dodržiavanie základných práv pri činnostiach v oblasti boja proti terorizmu dozerá zodpovedná osoba pre ochranu ľudských práv ([361]). Zodpovednú osobu pre ochranu ľudských práv menuje predseda Komisie na boj proti terorizmu spomedzi jednotlivcov, ktorí majú osobitnú kvalifikáciu uvedenú vo vykonávacom dekréte k zákonu o boji proti terorizmu ([362]), na (obnoviteľné) obdobie dvoch rokov, pričom ju z funkcie možno odvolať len z osobitných obmedzených a opodstatnených dôvodov ([363]). Pri výkone svojej funkcie dozoru môže zodpovedná osoba pre

([354]) Článok 83 ods. 3 zákona o telekomunikáciách.
([355]) Pozri aj prílohu II oddiel 3.2.3.
([356]) Pozri prílohu II oddiel 1.2.
([357]) Článok 5 ods. 1 až 2, články 12 a 13-5 zákona o ochrane súkromia komunikácie.
([358]) Pozri prílohu II oddiel 3.3.
([359]) Článok 5 ods. 3 zákona o boji proti terorizmu. Komisii predsedá predseda vlády a pozostáva z niekoľkých ministrov a vedúcich štátnych orgánov, napríklad ministra zahraničných vecí, ministra spravodlivosti, ministra národnej obrany, ministra vnútra a bezpečnosti, riaditeľa Národnej spravodajskej služby a generálneho komisára Národnej policajnej agentúry (článok 3 ods. 1 vykonávacieho dekrétu k zákonu o boji proti terorizmu).
([360]) Článok 9 ods. 4 zákona o boji proti terorizmu.
([361]) Článok 7 zákona o boji proti terorizmu.
([362]) Teda spomedzi advokátov aspoň s desaťročnou praxou alebo odbornými znalosťami v oblasti ľudských práv, ktorí minimálne desať rokov pôsobia alebo pôsobili (aspoň) na pozícii docenta alebo ako vyšší verejní činitelia v štátnych orgánoch alebo miestnych samosprávach alebo majú aspoň desaťročnú prax v oblasti ľudských práv, napr. v mimovládnej organizácii (článok 7 ods. 1 vykonávacieho dekrétu k zákonu o boji proti terorizmu).
([363]) Napríklad v prípade obvinenia v trestnej veci v súvislosti s výkonom jej povinností, v prípade odhalenia dôverných informácií alebo z dôvodu dlhodobej duševnej alebo fyzickej nespôsobilosti (článok 7 ods. 3 vykonávacieho dekrétu k zákonu o boji proti terorizmu).

ochranu ľudských práv vydávať všeobecné odporúčania na zlepšenie ochrany ľudských práv ([364]) a osobitné odporúčania na nápravné opatrenia, ak sa zistilo porušenie ľudských práv ([365]). Orgány verejnej moci musia informovať zodpovednú osobu pre ochranu ľudských práv o činnostiach v nadväznosti na jej odporúčania ([366]).

(199) Po druhé dozerá Komisia pre ochranu osobných informácií na dodržiavanie pravidiel ochrany údajov orgánmi národnej bezpečnosti, ku ktorým patria platné ustanovenia zákona o ochrane osobných informácií (pozri odôvodnenie (149)), ako aj obmedzenia a záruky, ktoré sa uplatňujú na získavanie osobných údajov podľa iných zákonov (zákon o ochrane súkromia komunikácie, zákon o boji proti terorizmu a telekomunikačný zákon, pozri aj odôvodnenie (171)) ([367]). Pri vykonávaní tejto úlohy dozoru môže Komisia pre ochranu osobných informácií využívať všetky svoje právomoci v oblasti vyšetrovania a nápravy, ako sa podrobne uvádzajú v oddiele 2.4.2.

(200) Po tretie sa na činnosti orgánov národnej bezpečnosti vzťahuje nezávislý dozor Národnej komisie pre ľudské práva v súlade s postupmi uvedenými v odôvodnení (172) ([368]).

(201) Po štvrté sa funkcia dozoru vykonávaná Radou pre audit a inšpekciu rozširuje aj na orgány národnej bezpečnosti, hoci Národná spravodajská služba môže za mimoriadnych okolností odmietnuť poskytnúť niektoré informácie alebo materiály, t. j. vtedy, keď predstavujú štátne tajomstvá a ich zverejnenie by malo závažný vplyv na národnú bezpečnosť ([369]).

(202) A napokon parlamentný dozor nad činnosťami Národnej spravodajskej služby vykonáva národné zhromaždenie (prostredníctvom osobitného Výboru pre spravodajské činnosti) ([370]). V zákone o ochrane súkromia komunikácie sa stanovuje národnému zhromaždeniu osobitná úloha dozoru nad používaním opatrení na zachytenie komunikácie na účely národnej bezpečnosti ([371]). Konkrétne môže národné zhromaždenie vykonávať inšpekcie odpočúvacích zariadení na mieste a od Národnej spravodajskej služby a telekomunikačných operátorov môže vyžadovať podávanie správ o sprístupnení obsahu komunikácie. Národné zhromaždenie môže vykonávať aj svoje funkcie všeobecného dozoru (v súlade s postupmi uvedenými v odôvodnení (174)). V zákone o Národnej spravodajskej službe sa vyžaduje, aby riaditeľ Národnej spravodajskej služby bezodkladne vyhovel žiadosti Výboru pre spravodajské informácie o predloženie správy o konkrétnej veci ([372]) na základe osobitných pravidiel pre niektoré osobitne citlivé informácie. Konkrétne môže riaditeľ Národnej spravodajskej služby odmietnuť vyhovieť žiadosti alebo odmietnuť podať svedectvo pred Výborom pre spravodajskú činnosť len za mimoriadnych okolností, t. j. vtedy, ak sa žiadosť týka štátnych tajomstiev z vojenskej či diplomatickej oblasti alebo otázok súvisiacich so Severnou Kóreou, ktorých zverejnenie by mohlo mať závažný dosah na osud národa ([373]). V tomto prípade môže Výbor pre spravodajské informácie požiadať o vysvetlenie predsedu vlády a ak mu do siedmich dní nie je poskytnuté, vyhovenie alebo svedectvo nesmie odmietnuť.

3.3.4. *Prostriedky nápravy*

(203) Aj v oblasti národnej bezpečnosti poskytuje kórejský systém rôzne (súdne) spôsoby dosiahnutia prostriedku nápravy vrátane náhrady škody. Tieto mechanizmy poskytujú dotknutým osobám účinné správne a súdne prostriedky nápravy, ktoré im umožňujú najmä uplatniť svoje práva vrátane práva na prístup k svojim osobným údajom alebo práva dosiahnuť opravu alebo vymazanie týchto údajov.

(204) Po prvé môžu v súlade s článkom 3 ods. 5 a článkom 4 ods. 1, 3 a 4 zákona o ochrane osobných informácií jednotlivci uplatňovať vo vzťahu k orgánom národnej bezpečnosti svoje práva na prístup, opravu, vymazanie a pozastavenie spracúvania svojich informácií. V oddiele 6 oznámenia č. 2021-5 (príloha I k tomuto rozhodnutiu) sa ďalej objasňuje, ako sa tieto práva uplatňujú v súvislosti so spracúvaním údajov na účely národnej bezpečnosti.

([364]) Článok 8 ods. 1 vykonávacieho dekrétu k zákonu o boji proti terorizmu.

([365]) Článok 9 ods. 1 vykonávacieho dekrétu k zákonu o boji proti terorizmu. Zodpovedná osoba pre ochranu ľudských práv rozhoduje o prijatí odporúčaní nezávisle, ale musí podávať správy o odporúčaniach predsedovi Komisie pre boj proti terorizmu.

([366]) Článok 9 ods. 2 vykonávacieho dekrétu k zákonu o boji proti terorizmu. Podľa oficiálneho zastúpenia kórejskej vlády sa nevykonanie odporúčania zodpovednej osoby pre ochranu ľudských práv postúpi Komisii pre boj proti terorizmu, ako aj predsedovi vlády, hoci dosiaľ sa nestalo, že by odporúčania zodpovednej osoby pre ochranu ľudských práv neboli vykonané (pozri oddiel 3.3.1 prílohy II).

([367]) Príloha II oddiel 3.3.4.

([368]) Osobitne v prípade Národnej spravodajskej služby vykonala Národná komisia pre ľudské práva v minulosti vyšetrovania *ex officio* a vyriešila množstvo individuálnych sťažností. Pozri napríklad výročnú správu Národnej komisie pre ľudské práva za rok 2018, s. 128 (k dispozícii na adrese https://www.humanrights.go.kr/site/program/board/basicboard/view?menuid=002003003001&pagesize=10&boardtypeid=7017&boardid=7604746) a výročnú správu Národnej komisie pre ľudské práva za rok 2019, s. 70 (k dispozícii na adrese https://www.humanrights.go.kr/site/program/board/basicboard/view?menuid=002003003001&pagesize=10&boardtypeid=7017&boardid=7606217).

([369]) Článok 13 ods. 1 zákona o Národnej spravodajskej službe.

([370]) Článok 36 a článok 37 ods. 1 pododsek 15 zákona o národnom zhromaždení.

([371]) Článok 15 zákona o ochrane súkromia komunikácie.

([372]) Článok 15 ods. 2 zákona o Národnej spravodajskej službe.

([373]) Článok 17 ods. 2 zákona o Národnej spravodajskej službe. „Štátne tajomstvá" sa vymedzujú ako (utajené) skutočnosti, tovar alebo poznatky, ktoré sa nesprístupňujú žiadnej inej krajine ani organizácii, aby sa zabránilo akýmkoľvek závažným hrozbám pre národnú bezpečnosť, a ku ktorým je povolený len obmedzený prístup. Pozri článok 13 ods. 4 zákona o Národnej spravodajskej službe.

Konkrétne môže orgán národnej bezpečnosti výkon práva odložiť, obmedziť alebo odmietnuť len v takom rozsahu a na tak dlho, ako je to potrebné a primerané na ochranu dôležitého cieľa verejného záujmu (napríklad v takom rozsahu a na tak dlho, ako by priznanie tohto práva ohrozovalo prebiehajúce vyšetrovanie alebo národnú bezpečnosť), alebo ak by mohlo priznanie práva spôsobiť ujmu na živote alebo fyzickej integrite tretej strany. Použitie takéhoto obmedzenia si preto vyžaduje vyváženie práv a záujmov jednotlivca a príslušného verejného záujmu, pričom toto obmedzenie nesmie mať v žiadnom prípade vplyv na podstatu uvedeného práva (článok 37 ods. 2 ústavy). Ak sa žiadosť zamietne alebo obmedzí, jednotlivcovi sa bezodkladne oznámia dôvody.

(205) Po druhé majú jednotlivci právo na dosiahnutie prostriedku nápravy podľa zákona o ochrane osobných informácií, ak ich údaje spracúva orgán národnej bezpečnosti v rozpore so zákonom o ochrane osobných informácií alebo s obmedzeniami a zárukami z iných zákonov, ktorými sa riadi získavanie osobných údajov (najmä zo zákona o ochrane súkromia komunikácie, pozri odôvodnenie (171)) ([374]). Toto právo sa môže uplatniť prostredníctvom sťažnosti Komisii pre ochranu osobných informácií (a to aj prostredníctvom call centra pre ochranu súkromia, ktoré prevádzkuje Kórejská agentúra pre internet a bezpečnosť) ([375]). Okrem toho môžu jednotlivci z EÚ s cieľom uľahčiť prístup k prostriedku nápravy proti kórejským orgánom národnej bezpečnosti podať sťažnosť Komisii pre ochranu osobných informácií prostredníctvom svojho vnútroštátneho orgánu pre ochranu údajov ([376]). V takomto prípade Komisia pre ochranu osobných informácií informuje jednotlivca po skončení vyšetrovania (v prípade potreby aj o uložených nápravných opatreniach) prostredníctvom vnútroštátneho orgánu na ochranu údajov. Ďalej sa môžu jednotlivci odvolať proti rozhodnutiam alebo nečinnosti/napadnúť rozhodnutia alebo nečinnosť Komisie pre ochranu osobných informácií podľa Správneho súdneho poriadku (pozri odôvodnenie (132)).

(206) Po tretie môžu jednotlivci podať sťažnosť zodpovednej osobe pre ochranu ľudských práv týkajúcu sa porušenia svojho práva na súkromie/ochranu údajov v súvislosti s činnosťami boja proti terorizmu (t. j. podľa zákona o boji proti terorizmu) ([377]), ktorý môže odporučiť nápravné opatrenie. Keďže v prípade zodpovednej osoby pre ochranu ľudských práv nie sú stanovené požiadavky prípustnosti, sťažnosťou sa bude zaoberať aj vtedy, ak dotknutý jednotlivec nedokáže preukázať, že mu v skutočnosti vznikla ujma (napríklad z dôvodu údajného nezákonného získavania jeho údajov orgánom národnej bezpečnosti) ([378]). Príslušný orgán musí informovať zodpovednú osobu pre ochranu ľudských práv o všetkých opatreniach prijatých na vykonanie jej odporúčaní.

(207) Po štvrté môžu jednotlivci podať sťažnosť Národnej komisii pre ľudské práva týkajúcu sa získavania ich údajov orgánmi národnej bezpečnosti a dosiahnuť prostriedok nápravy v súlade s postupom uvedeným v odôvodnení (178) ([379]).

(208) A napokon sú k dispozícii rôzne prostriedky súdnej nápravy ([380]), ktoré jednotlivcom umožňujú dosiahnuť nápravu odvolaním sa na obmedzenia a záruky uvedené v oddiele 3.3.1. Jednotlivci môžu konkrétne napadnúť zákonnosť opatrení orgánov národnej bezpečnosti na základe Správneho súdneho poriadku (v súlade s postupom uvedeným v odôvodnení (181) alebo v zákone o ústavnom súde) (pozri odôvodnenie (182)). Okrem toho môžu získať náhradu škody na základe zákona o štátnom odškodnení (ako sa podrobnejšie uvádza v odôvodnení (183)).

4. ZÁVER

(209) Komisia sa domnieva, že Kórejská republika prostredníctvom zákona o ochrane osobných informácií, osobitných pravidiel platných pre určité sektory (analyzované v oddiele 2) a dodatočných záruk uvedených v odôvodnení č. 2021-5 (príloha I) zaisťuje úroveň ochrany osobných údajov prenášaných z Európskej únie, ktorá v zásade zodpovedá ochrane zaručenej nariadením (EÚ) 2016/679.

(210) Komisia sa okrem toho domnieva, že mechanizmy dozoru a možnosti dosiahnutia nápravy v kórejskom práve ako celok umožňujú v praxi odhaliť a riešiť porušenia pravidiel ochrany údajov zo strany prevádzkovateľov v Kórei a poskytujú dotknutej osobe právne prostriedky nápravy na získanie prístupu k jej osobným údajom, a prípadne aj dosiahnutie opravy alebo vymazania takýchto údajov.

([374]) Článok 58 ods. 4 a článok 4 ods. 5 zákona o ochrane osobných informácií. Pozri prílohu II oddiel 3.4.2.
([375]) Článok 62 a článok 63 ods. 2 zákona o ochrane osobných informácií.
([376]) Oznámenie č. 2021-5 (oddiel 6, príloha I).
([377]) Článok 8 ods. 1 pododsek 2 vykonávacieho dekrétu k zákonu o boji proti terorizmu.
([378]) Pozri prílohu II oddiel 3.4.1.
([379]) Napríklad Národná komisia pre ľudské práva pravidelne prijíma sťažnosti proti Národnej spravodajskej službe, pozri údaje vo výročnej správe Národnej komisie pre ľudské práva z roku 2019 týkajúce sa množstva sťažností prijatých v rokoch 2015 až 2019, s. 70 (k dispozícii na adrese https://www.humanrights.go.kr/site/program/board/basicboard/view?menuid=002003003001&pagesize=10&boardtypeid=7017&boardid=7606217).
([380]) Pozri prílohu II oddiel 3.4.4.

(211) A na záver na základe dostupných informácií o kórejskom právnom poriadku vrátane vyhlásení, uistení a záväzkov kórejskej vlády, ktoré sú uvedené v prílohe II, sa Komisia domnieva, že každý zásah do základných práv jednotlivcov, ktorých osobné údaje sa prenášajú z Európskej únie do Kórejskej republiky, zo strany kórejských orgánov verejnej moci na účely verejného záujmu, najmä na účely presadzovania práva v trestných veciach a na účely národnej bezpečnosti, bude obmedzený na to, čo je nevyhnutne potrebné na dosiahnutie daného oprávneného cieľa, a že existuje účinná právna ochrana proti takýmto zásahom.

(212) Vzhľadom na zistenia z tohto rozhodnutia by sa preto malo dospieť k záveru, že Kórejská republika zabezpečuje v zmysle článku 45 nariadenia (EÚ) 2016/679 vykladaného vzhľadom na Chartu základných práv Európskej únie primeranú úroveň ochrany osobných údajov prenášaných z Európskej únie do Kórejskej republiky prevádzkovateľom osobných informácií v Kórejskej republike podľa zákona o ochrane osobných informácií s výnimkou náboženských organizácií v rozsahu, v akom spracúvajú osobné údaje na účely svojich misijných činností; politických strán v rozsahu, v akom spracúvajú osobné údaje v súvislosti s menovaním kandidátov, a prevádzkovateľov, ktorí podliehajú dozoru Komisie pre finančné služby na účely spracúvania osobných úverových informácií podľa zákona o úverových informáciách v rozsahu, v akom spracúvajú takéto informácie.

5. ÚČINKY TOHTO ROZHODNUTIA A OPATRENIA ORGÁNOV PRE OCHRANU ÚDAJOV

(213) Členské štáty a ich orgány sú povinné prijať opatrenia potrebné na dosiahnutie súladu s aktmi inštitúcií Únie, keďže tieto akty požívajú prezumpciu zákonnosti a majú z tohto dôvodu právne účinky dovtedy, kým neboli derogované, zrušené v konaní o žalobe o neplatnosť alebo vyhlásené za neplatné v nadväznosti na návrh na začatie prejudiciálneho konania alebo námietku nezákonnosti.

(214) Rozhodnutie Komisie o primeranosti prijaté podľa článku 45 ods. 3 nariadenia (EÚ) 2016/679 je preto záväzné pre všetky orgány členských štátov, ktorým je určené, vrátane ich nezávislých dozorných orgánov. Konkrétne sa môžu prenosy prevádzkovateľa alebo sprostredkovateľa v Európskej únii prevádzkovateľom v Kórejskej republike uskutočňovať bez potreby získania akéhokoľvek ďalšieho povolenia.

(215) Zároveň treba pripomenúť, že podľa článku 58 ods. 5 nariadenia (EÚ) 2016/679 a objasnenia Súdneho dvora v rozsudku vo veci Schrems ([381]) platí, že ak vnútroštátny orgán pre ochranu údajov spochybňuje, a to aj na základe sťažnosti, zlučiteľnosť rozhodnutia Komisie o primeranosti so základnými právami jednotlivca na súkromie a ochranu údajov, vo vnútroštátnom práve sa mu musí poskytnúť právny prostriedok nápravy umožňujúci uplatniť tieto výhrady na vnútroštátnom súde, ktorý môže mať povinnosť podať návrh na začatie prejudiciálneho konania na Súdnom dvore ([382]).

6. MONITOROVANIE A PRESKÚMAVANIE TOHTO ROZHODNUTIA

(216) Podľa judikatúry Súdneho dvora ([383]) a ako sa uznáva v článku 45 ods. 4 nariadenia (EÚ) 2016/679, by mala Komisia po prijatí rozhodnutia o primeranosti nepretržite monitorovať príslušný vývoj v tretej krajine s cieľom posúdiť, či tretia krajina aj naďalej zabezpečuje v zásade zodpovedajúcu úroveň ochrany. Takéto overenie je v každom prípade potrebné, keď Komisia dostane informácie, na základe ktorých vzniknú dôvodné pochybnosti v tomto ohľade.

(217) Komisia by preto mala neustále monitorovať situáciu v Kórejskej republike, pokiaľ ide o právny rámec a skutočnú prax spracúvania osobných údajov, ktoré sa posudzujú v tomto rozhodnutí, vrátane dodržiavania vyhlásení, uistení a záväzkov uvedených v prílohe II zo strany kórejských orgánov. V záujme uľahčenia tohto procesu sa kórejské orgány vyzývajú, aby Komisiu bezodkladne informovali o podstatnom vývoji relevantnom, pokiaľ ide o spracúvanie osobných údajov hospodárskymi subjektmi a orgánmi verejnej moci, ako aj o obmedzenia a záruky uplatniteľné na prístup k osobným údajom zo strany orgánov verejnej moci.

([381]) Vec Schrems, bod 65.

([382]) Vec Schrems, bod 65: „V tomto ohľade je úlohou vnútroštátneho zákonodarcu stanoviť prostriedky nápravy umožňujúce dotknutému vnútroštátnemu dozornému orgánu uplatniť výhrady, ktoré považuje za dôvodné, na vnútroštátnych súdoch, aby tieto podali, ak majú rovnaké pochybnosti ako tento orgán, pokiaľ ide o platnosť rozhodnutia Komisie, návrh na začatie prejudiciálneho konania na účely preskúmania platnosti tohto rozhodnutia“.

([383]) Vec Schrems, bod 76.

(218) Navyše, aby Komisia mohla účinne vykonávať svoju monitorovaciu funkciu, mali by ju členské štáty informovať o všetkých relevantných opatreniach, ktoré prijali vnútroštátne orgány pre ochranu údajov, najmä pokiaľ ide o otázky alebo sťažnosti dotknutých osôb z EÚ týkajúce sa prenosu osobných údajov z Európskej únie prevádzkovateľom údajov v Kórejskej republike. Komisia by mala byť informovaná aj o akýchkoľvek známkach toho, že opatrenia kórejských orgánov verejnej moci zodpovedných za predchádzanie trestným činom, ich vyšetrovanie, odhaľovanie alebo stíhanie alebo za národnú bezpečnosť vrátane akýchkoľvek dozorných orgánov nezabezpečujú požadovanú úroveň ochrany.

(219) Podľa článku 45 ods. 3 nariadenia (EÚ) 2016/679 ([384]) a vzhľadom na skutočnosť, že úroveň ochrany zabezpečovaná kórejským právnym poriadkom sa môže zmeniť, by Komisia mala po prijatí tohto rozhodnutia pravidelne skúmať, či sú závery týkajúce sa primeranosti úrovne ochrany, ktorú zabezpečuje Kórejská republika, stále skutkovo a právne odôvodnené.

(220) Na tento účel by sa malo toto rozhodnutie podrobiť prvému preskúmaniu do troch rokov od nadobudnutia účinnosti. Po tomto prvom preskúmaní a v závislosti od jeho výsledku Komisia v úzkej spolupráci s výborom zriadeným podľa článku 93 ods. 1 nariadenia (EÚ) 2016/679 rozhodne, či by sa mal zachovať trojročný cyklus. Následné preskúmania by sa v každom prípade mali uskutočniť aspoň každé štyri roky ([385]). Preskúmanie by malo zahŕňať všetky aspekty fungovania tohto rozhodnutia, a najmä uplatňovanie dodatočných záruk uvedených v prílohe I k tomuto rozhodnutiu, pričom osobitnú pozornosť treba venovať ochrane zabezpečovanej v prípade následných prenosov; vývoj príslušnej judikatúry; pravidlá spracúvania pseudonymizovaných informácií na účely štatistiky, vedeckého výskumu a archivovania vo verejnom záujme, ako aj uplatňovanie výnimiek podľa článku 28 ods. 7 zákona o ochrane osobných informácií; účinnosť výkonu individuálnych práv, a to aj pred nedávno reformovanou Komisiou pre ochranu osobných informácií, a uplatňovanie výnimiek z týchto práv; uplatňovanie čiastočných výnimiek podľa zákona o ochrane osobných informácií; ako aj obmedzenia a záruky v súvislosti s prístupom vlády (ako sa stanovuje v prílohe II k tomuto rozhodnutiu) vrátane spolupráce Komisie pre ochranu osobných informácií s orgánmi EÚ pre ochranu údajov týkajúcej sa sťažností jednotlivcov. Malo by sa zameriavať aj na účinnosť dozoru a presadzovania práva, pokiaľ ide o zákon o ochrane osobných informácií, ako aj na oblasť presadzovania práva v trestných veciach a oblasť národnej bezpečnosti (vykonávaného najmä Komisiou pre ochranu osobných informácií a Národnou komisiou pre ľudské práva).

(221) V záujme vykonania preskúmania by sa Komisia mala stretnúť s Komisiou pre ochranu osobných informácií, ku ktorej by sa v prípade potreby mali pripojiť ďalšie kórejské orgány zodpovedné za prístup vlády vrátane príslušných dozorných orgánov. Na tomto stretnutí by mali mať možnosť zúčastniť sa zástupcovia členov Európskeho výboru pre ochranu údajov. Komisia by mala v rámci preskúmania požiadať Komisiu pre ochranu osobných informácií, aby poskytla komplexné informácie o všetkých aspektoch relevantných pre záver o primeranosti vrátane informácií o obmedzeniach a zárukách týkajúcich sa prístupu vlády ([386]). Komisia by si takisto mala vyžiadať vysvetlenia k všetkým informáciám relevantným pre toto rozhodnutie, ktoré dostala, vrátane verejných správ kórejských orgánov alebo iných zainteresovaných strán v Kórei, Európskeho výboru pre ochranu údajov, jednotlivých orgánov pre ochranu osobných údajov, skupín občianskej spoločnosti, mediálnych správ alebo akéhokoľvek iného dostupného zdroja informácií.

(222) Komisia by na základe preskúmania mala vypracovať verejnú správu, ktorá sa má predložiť Európskemu parlamentu a Rade.

7. POZASTAVENIE, ZRUŠENIE ALEBO ZMENA TOHTO ROZHODNUTIA

(223) Ak dostupné informácie, najmä informácie vyplývajúce z monitorovania tohto rozhodnutia alebo poskytnuté kórejskými orgánmi alebo orgánmi členských štátov, odhalia, že úroveň ochrany poskytovaná Kóreou už nemusí byť primeraná, Komisia by o tom mala bezodkladne informovať príslušné kórejské orgány a požiadať o prijatie náležitých opatrení v stanovenej primeranej lehote.

(224) Ak po uplynutí uvedenej stanovenej lehoty príslušné kórejské orgány neprijmú takéto opatrenie alebo inak uspokojivo nepreukážu, že toto rozhodnutie sa naďalej zakladá na primeranej úrovni ochrany, Komisia začne postup uvedený v článku 93 ods. 2 nariadenia (EÚ) 2016/679 s cieľom čiastočne alebo úplne pozastaviť platnosť tohto rozhodnutia alebo ho zrušiť.

(225) Alternatívne Komisia začne postup s cieľom zmeniť toto rozhodnutie, najmä podriadením prenosu údajov dodatočným podmienkam alebo obmedzením rozsahu konštatovanej primeranosti len na tie prenosy údajov, pri ktorých je naďalej zabezpečená primeraná úroveň ochrany.

([384]) Podľa článku 45 ods. 3 nariadenia (EÚ) 2016/679 „[v]o vykonávacom akte sa stanoví mechanizmus pravidelného preskúmania, […] v ktorom sa zohľadnia všetky významné zmeny v tretej krajine alebo medzinárodnej organizácii“.

([385]) V článku 45 ods. 3 nariadenia (EÚ) 2016/679 sa stanovuje, že pravidelné preskúmanie sa musí uskutočniť „aspoň každé štyri roky“. Pozri aj Európsky výbor pre ochranu údajov, Referenčné kritériá primeranosti, WP 254 rev. 01.

([386]) Pozri prílohu II k tomuto rozhodnutiu.

(226) Komisia by mala postup pozastavenia platnosti alebo zrušenia iniciovať predovšetkým v prípade, že budú existovať známky toho, že hospodárske subjekty, ktoré dostávajú osobné údaje podľa tohto rozhodnutia, nedodržiavajú dodatočné záruky uvedené v prílohe I a/alebo že sa tieto pravidlá účinne nepresadzujú, alebo že kórejské orgány nedodržiavajú vyhlásenia, uistenia a záväzky uvedené v prílohe II k tomuto rozhodnutiu.

(227) Komisia by mala zvážiť začatie postupu vedúceho k zmene, pozastaveniu platnosti alebo zrušeniu tohto rozhodnutia aj v prípade, že príslušné kórejské orgány v rámci preskúmania alebo inak neposkytnú informácie alebo objasnenia potrebné na posúdenie úrovne ochrany zabezpečovanej pre osobné údaje prenášané z Európskej únie do Kórejskej republiky alebo na dodržiavanie tohto rozhodnutia. Komisia by mala v tejto súvislosti zohľadniť, do akej miery možno príslušné informácie získať z iných zdrojov.

(228) Komisia využije z riadne odôvodnených vážnych a naliehavých dôvodov možnosť prijať v súlade s postupom uvedeným v článku 93 ods. 3 nariadenia (EÚ) 2016/679 okamžite uplatniteľné vykonávacie akty, ktorými sa pozastaví platnosť tohto rozhodnutia, zruší sa alebo sa zmení toto rozhodnutie

8. ZÁVEREČNÉ ÚVAHY

(229) Európsky výbor pre ochranu údajov zverejnil svoje stanovisko ([387]), ktoré bolo zohľadnené pri príprave tohto rozhodnutia.

(230) Opatrenia stanovené v tomto rozhodnutí sú v súlade so stanoviskom výboru zriadeného podľa článku 93 ods. 1 nariadenia (EÚ) 2016/679,

PRIJALA TOTO ROZHODNUTIE:

Článok 1

1. Na účel článku 45 nariadenia (EÚ) 2016/679 Kórejská republika zabezpečuje primeranú úroveň ochrany osobných údajov prenášaných z Európskej únie prevádzkovateľom osobných informácií v Kórejskej republike, na ktoré sa vzťahuje zákon o ochrane osobných informácií doplnený dodatočnými zárukami stanovenými v prílohe I spolu s oficiálnymi vyhláseniami, uisteniami a záväzkami uvedenými v prílohe II.

2. Toto rozhodnutie sa nevzťahuje na osobné údaje prenášané príjemcom, ktorí patria do jednej z nasledujúcich kategórií, pokiaľ všetky účely, na ktoré sa osobné údaje spracúvajú, alebo ich časť zodpovedá jednému z uvedených účelov:

a) náboženské organizácie v rozsahu, v akom spracúvajú osobné údaje na účely svojich misijných činností;

b) politické strany v rozsahu, v akom spracúvajú osobné údaje v súvislosti s menovaním kandidátov;

c) subjekty, ktoré podliehajú dozoru Komisie pre finančné služby na účely spracúvania osobných úverových informácií podľa zákona o úverových informáciách v rozsahu, v akom spracúvajú takéto informácie.

Článok 2

Vždy, keď príslušné orgány v členských štátoch uplatnia svoje právomoci podľa článku 58 nariadenia (EÚ) 2016/679, aby ochránili fyzické osoby v súvislosti so spracúvaním ich osobných údajov, pokiaľ ide o prenosy údajov patriacich do rozsahu pôsobnosti stanoveného v článku 1 tohto rozhodnutia, dotknutý členský štát o tejto skutočnosti bezodkladne informuje Komisiu.

Článok 3

1. Komisia nepretržite monitoruje uplatňovanie právneho rámca, z ktorého vychádza toto rozhodnutie, vrátane podmienok, za ktorých sa uskutočňujú následné prenosy, uplatňujú individuálne práva a za ktorých majú kórejské orgány verejnej moci prístup k údajom preneseným na základe tohto rozhodnutia, s cieľom posúdiť, či Kórejská republika naďalej zabezpečuje primeranú úroveň ochrany v zmysle článku 1.

([387]) Stanovisko č. 32/2021 týkajúce sa návrhu vykonávacieho rozhodnutia Európskej komisie podľa nariadenia (EÚ) 2016/679 o primeranej ochrane osobných údajov v Kórejskej republike, k dispozícii na tomto odkaze: https://edpb.europa.eu/our-work-tools/our-documents/opinion-art-70/opinion-322021-regarding-european-commission-draft_en.

2. Členské štáty a Komisia sa vzájomne informujú o prípadoch, v ktorých Komisia pre ochranu osobných informácií alebo akýkoľvek iný príslušný kórejský orgán nezabezpečuje dodržiavanie právneho rámca, na ktorom je založené toto rozhodnutie.

3. Členské štáty a Komisia sa vzájomne informujú o všetkých známkach toho, že zásahy kórejských orgánov verejnej moci do práva fyzických osôb na ochranu osobných údajov prekračujú rámec toho, čo je nevyhnutne potrebné, alebo že neexistuje účinná právna ochrana pred takými zásahmi.

4. Po troch rokoch od dátumu oznámenia tohto rozhodnutia členským štátom a následne aspoň každé štyri roky Komisia vyhodnotí záver uvedený v článku 1 ods. 1 na základe všetkých dostupných informácií vrátane informácií, ktoré získala v rámci preskúmania uskutočneného spolu s príslušnými kórejskými orgánmi.

5. Ak má Komisia informácie o tom, že primeraná úroveň ochrany už nie je zabezpečená, informuje príslušné kórejské orgány. V prípade potreby môže v súlade s článkom 45 ods. 5 nariadenia (EÚ) 2016/679 rozhodnúť o pozastavení platnosti, zmene alebo zrušení tohto rozhodnutia alebo obmedzení jeho rozsahu pôsobnosti, najmä ak existujú známky toho, že:

a) prevádzkovatelia v Kórei, ktorí na základe tohto rozhodnutia dostali osobné údaje z Európskej únie, nedodržiavajú dodatočné záruky uvedené v prílohe I, alebo že sa v tejto súvislosti nevykonáva dostatočný dozor a presadzovanie;

b) kórejské orgány verejnej moci nedodržiavajú vyhlásenia, uistenia a záväzky uvedené v prílohe II vrátane vyhlásení, uistení a záväzkov, pokiaľ ide o podmienky a obmedzenia získavania osobných údajov prenášaných na základe tohto rozhodnutia zo strany kórejských orgánov verejnej moci na účely presadzovania práva v trestných veciach alebo národnej bezpečnosti a podmienky a obmedzenia ich prístupu k takýmto osobným údajom.

Komisia môže tieto opatrenia prijať aj vtedy, ak v dôsledku nedostatočnej spolupráce kórejskej vlády nedokáže určiť, či Kórejská republika naďalej zabezpečuje primeranú úroveň ochrany.

Článok 4

Toto rozhodnutie je určené členským štátom.

V Bruseli 17. decembra 2021

Za Komisiu
Didier REYNDERS
člen Komisie

PRÍLOHA I

DOPLNKOVÉ PRAVIDLÁ PRE VÝKLAD A UPLATŇOVANIE ZÁKONA O OCHRANE OSOBNÝCH INFORMÁCIÍ PRI SPRACÚVANÍ OSOBNÝCH ÚDAJOV PRENÁŠANÝCH DO KÓREY

Obsah

I. Prehľad 54

II. Vymedzenie pojmov 55

III. Doplnkové pravidlá 55

1. Obmedzenie používania a poskytovania osobných informácií mimo stanoveného účelu (články 3, 15 a 18 zákona) 55

2. Obmedzenie následného prenosu osobných údajov (článok 17 ods. 3 a 4, článok 18 zákona) 57

3. Oznamovanie údajov, ak osobné údaje neboli získané od dotknutej osoby (článok 20 zákona) 58

4. Rozsah uplatňovania osobitnej výnimky zo spracúvania pseudonymizovaných informácií (články 28-2, 28-3, 28-4, 28-5, 28-6 a 28-7, článok 3, článok 58-2 zákona) 60

5. Nápravné opatrenia atď. (článok 64 ods. 1, 2 a 4 zákona) 61

6. Uplatňovanie zákona o ochrane osobných informácií na spracúvanie osobných údajov na účely národnej bezpečnosti, a to aj pri vyšetrovaní porušení a pri presadzovaní práva v súlade so zákonom o ochrane osobných informácií (článok 7-8, článok 7-9, článok 58, článok 3, článok 4 a článok 62 zákona o ochrane osobných informácií) 62

I. Prehľad

Kórea a Európska únia (ďalej len „EÚ“) viedli diskusie o primeranosti, na základe ktorých dospela Európska komisia k záveru, že Kórea zabezpečuje primeranú úroveň ochrany osobných údajov podľa článku 45 všeobecného nariadenia o ochrane údajov.

V tejto súvislosti prijala Komisia pre ochranu osobných informácií podľa článku 5 (Povinnosti štátu atď.) a článku 14 (Medzinárodná spolupráca) ([1]) zákona o ochrane osobných informácií toto oznámenie s cieľom objasniť výklad, uplatňovanie a presadzovanie určitých ustanovení zákona, a to aj pokiaľ ide o spracúvanie osobných údajov prenášaných do Kórey na základe rozhodnutia EÚ o primeranosti.

Keďže toto oznámenie má význam správneho pravidla stanoveného a oznámeného príslušným správnym orgánom s cieľom objasniť normy výkladu, uplatňovania a presadzovania zákona o ochrane osobných informácií v právnom systéme Kórey, je pre prevádzkovateľa osobných informácií právne záväzné, a preto možno každé porušenie tohto oznámenia považovať za porušenie príslušných ustanovení zákona o ochrana osobných informácií. Okrem toho platí, že ak v dôsledku porušenia tohto oznámenia dôjde k porušeniu osobných práv a záujmov, príslušní jednotlivci majú nárok na dosiahnutie nápravy pred Komisiou pre ochranu osobných informácií alebo na súde.

Ak teda prevádzkovateľ osobných informácií, ktorý spracúva osobné informácie prenesené do Kórey na základe rozhodnutia EÚ o primeranosti, neprijme opatrenia v súlade s týmto oznámením, vzhľadom na uvedené sa podľa článku 64 ods. 1 a 2 zákona dospeje k záveru, že „existujú závažné dôvody domnievať sa, že ochrana osobných informácií bola porušená, pričom neprijatie opatrení pravdepodobne spôsobí škodu, ktorú bude ťažké napraviť“. V takých prípadoch môže Komisia pre ochranu osobných informácií alebo súvisiace ústredné správne orgány na základe právomoci, ktorá im vyplýva z tohto ustanovenia, nariadiť príslušnému prevádzkovateľovi osobných informácií, aby

([1]) V článku 14 zákona o ochrane osobných informácií sa stanovuje kórejský štátny orgán, ktorý zavádza politiky na zvyšovanie úrovne ochrany osobných informácií v medzinárodnom prostredí a predchádzanie porušovaniu práv dotknutých osôb v dôsledku cezhraničného prenosu osobných informácií.

prijal nápravné opatrenia atď., pričom v závislosti od konkrétneho porušenia zákona mu môže byť uložený aj zodpovedajúci trest (sankcie, správne pokuty atď.).

II. **Vymedzenie pojmov**

Vymedzenie pojmov používaných v tomto ustanovení:

i) zákon: zákon o ochrane osobných informácií (zákon č. 16930 v znení zmien zo 4. februára 2020, ktorý sa začal uplatňovať 5. augusta 2020);

ii) prezidentský dekrét: vykonávací dekrét k zákonu o ochrane osobných informácií (prezidentský dekrét č. 30509 z 3. marca 2020, ktorým sa menia ďalšie zákony);

iii) dotknutá osoba: jednotlivec, ktorého možno identifikovať na základe spracúvaných informácií, a je teda dotknutý danými informáciami;

iv) prevádzkovateľ osobných informácií: verejná inštitúcia, právnická osoba, organizácia, fyzická osoba atď., ktorá v rámci svojej činnosti priamo alebo nepriamo spracúva osobné informácie;

v) EÚ: EÚ (od konca februára 2020 tvorená 27 členskými krajinami ([2]), konkrétne Belgickom, Nemeckom, Francúzskom, Talianskom, Luxemburskom, Holandskom, Dánskom, Írskom, Gréckom, Portugalskom, Španielskom, Rakúskom, Fínskom, Švédskom, Cyprom, Českou republikou, Estónskom, Maďarskom, Lotyšskom, Litvou, Maltou, Poľskom, Slovenskom, Slovinskom, Rumunskom, Bulharskom a Chorvátskom), ako aj krajiny pridružené k EÚ prostredníctvom Dohody o EHP (Island, Lichtenštajnsko, Nórsko);

vi) všeobecné nariadenie o ochrane údajov: všeobecný právny predpis EÚ o ochrane osobných informácií, všeobecné nariadenie EÚ o ochrane údajov [nariadenie (EÚ) 2016/679];

vii) rozhodnutie o primeranosti: podľa článku 45 ods. 3 všeobecného nariadenia o ochrane údajov Európska komisia rozhodla, že tretia krajina, územie tretej krajiny, prípadne jeden či viaceré sektory alebo medzinárodná organizácia zaručujú primeranú úroveň ochrany osobných informácií.

III. **Doplnkové pravidlá**

1. **Obmedzenie používania a poskytovania osobných informácií mimo stanoveného účelu (články 3, 15 a 18 zákona)**

<Zákon o ochrane osobných informácií

(zákon č. 16930, čiastočne zmenený 4. februára 2020)>

Článok 3 (Zásady ochrany osobných informácií) (1) Prevádzkovateľ osobných informácií výslovne stanoví účely, na ktoré sa osobné informácie spracúvajú; a osobné informácie získava zákonným a spravodlivým spôsobom v minimálnom rozsahu potrebnom na tieto účely.

(2) Prevádzkovateľ osobných informácií spracúva osobné informácie primeraným spôsobom potrebným na účely, na ktoré sa osobné informácie spracúvajú, a nepoužíva tieto informácie na iné účely.

Článok 15 (Získavanie a používanie osobných informácií) (1) Prevádzkovateľ osobných informácií môže osobné informácie získať za týchto okolností, pričom ich môže využívať v rozsahu účelu ich získavania:

1. ak získal súhlas dotknutej osoby;

2. ak sa v právnych predpisoch uvádzajú osobitné ustanovenia alebo je nevyhnutné dodržať zákonné povinnosti;

3. ak je to nevyhnutné na plnenie povinností vyplývajú z právnych predpisov verejnej inštitúcii v rámci jej právomoci atď.;

4. ak je to nevyhnutne potrebné na výkon a plnenie zmluvy s dotknutou osobou;

([2]) Do skončenia prechodného obdobia k nim patrilo aj Spojené kráľovstvo, ako sa to stanovuje v článkoch 126, 127 a 132 Dohody o vystúpení Spojeného kráľovstva Veľkej Británie a Severného Írska z Európskej únie a z Európskeho spoločenstva pre atómovú energiu (2019/C 384 I/01).

5. ak sa to považuje za preukázateľne potrebné na ochranu záujmov dotknutej osoby alebo tretej strany, ktoré sa týkajú jej života, fyzickej integrity a majetku, pred bezprostredným nebezpečenstvom v situácii, keď dotknutá osoba alebo jej právny zástupca nemôžu vyjadriť svoj zámer alebo nie je možné z dôvodu neznámej adresy atď. získať ich súhlas vopred;

6. ak je to potrebné na dosiahnutie odôvodneného záujmu prevádzkovateľa osobných informácií v prípade, ak je takýto záujem preukázateľne nadradený právam dotknutej osoby. V takýchto prípadoch sa spracúvanie umožňuje len v rozsahu, v akom v podstatnej miere súvisí s odôvodneným záujmom prevádzkovateľa osobných informácií a nepresahuje primeraný rozsah.

Článok 18 (Obmedzenie používania a poskytovania osobných informácií mimo stanoveného účelu) (1) Prevádzkovateľ osobných informácií nepoužíva osobné informácie nad rámec stanovený v článku 15 ods. 1 a v článku 39-3 ods. 1 a 2, ani ich neposkytuje žiadnej tretej strane nad rámec stanovený v článku 17 ods. 1 a 3.

(2) Bez toho, aby bol dotknutý odsek 1, môže prevádzkovateľ osobných informácií v situáciách, na ktoré sa vzťahuje niektorý z nasledujúcich pododsekov, používať osobné informácie alebo ich poskytovať tretej strane na iné účely, ak nie je pravdepodobné, že by sa tým nespravodlivo poškodil záujem dotknutej osoby alebo tretej strany, a to za predpokladu, že na poskytovateľov informačných a komunikačných služieb (vymedzených v článku 2 ods. 1 bode 3 zákona o podpore využívania informačnej a komunikačnej siete a ochrane informácií atď.; ďalej sa uplatňuje to isté) spracúvajúcich osobné informácie používateľov (vymedzených v článku 2 ods. 1 bode 4 zákona o podpore využívania informačnej a komunikačnej siete a ochrane informácií atď.; ďalej sa uplatňuje to isté) sa vzťahujú iba pododseky 1 a 2 a že pododseky 5 až 9 sa vzťahujú iba na verejné inštitúcie:

1. ak získal dodatočný súhlas dotknutej osoby;

2. ak sa v právnych predpisoch uvádzajú ďalšie osobitné ustanovenia;

3. ak sa to považuje za preukázateľne potrebné na ochranu záujmov dotknutej osoby alebo tretej strany, ktoré sa týkajú jej života, fyzickej integrity a majetku, pred bezprostredným nebezpečenstvom v situácii, keď dotknutá osoba alebo jej právny zástupca nemôžu vyjadriť svoj zámer alebo nie je možné z dôvodu neznámej adresy získať ich súhlas vopred;

4. vypúšťa sa;<zákonom č. 16930 zo 4. februára 2020>

5. ak si prevádzkovateľ osobných informácií v rámci svojej právomoci môže plniť povinnosti, ktoré mu vyplývajú zo zákona, len vtedy, ak použije osobné informácie na iný ako zamýšľaný účel alebo ich poskytne tretej strane, pričom tak môže urobiť až po konzultácii s komisiou a na základe jej rozhodnutia;

6. ak je potrebné poskytnúť osobné informácie zahraničnej vláde alebo medzinárodnej organizácii na účely vykonávania zmluvy alebo iného medzinárodného dohovoru;

7. ak je to potrebné na vyšetrovanie trestného činu, vznesenie obžaloby a na trestné stíhanie;

8. ak je to potrebné na výkon povinností súdu pri vedení procesu;

9. ak je to potrebné na výkon trestu, podmienečné prepustenie a zadržanie.

vypúšťajú sa odseky 3 až 4

(5) Ak prevádzkovateľ osobných informácií poskytne osobné informácie tretej strane na iný ako zamýšľaný účel v niektorom z prípadov uvedených v odseku 2, uvedený prevádzkovateľ osobných informácií požiada príjemcu osobných informácií, aby obmedzil účel a metódu ich použitia, ako aj ďalšie potrebné záležitosti, prípadne aby vypracoval všetky potrebné záruky na zaistenie bezpečnosti osobných informácií. V takýchto prípadoch prijme osoba, ktorej je táto žiadosť určená, potrebné opatrenia na zaistenie bezpečnosti osobných informácií.

i) V článku 3 ods. 1 a 2 zákona sa stanovuje zásada, že prevádzkovateľ osobných informácií smie získavať iba minimálne osobné informácie potrebné na vykonanie legálneho a zákonného spracúvania osobných informácií, pričom by tieto osobné informácie nemal používať na iné ako zamýšľané účely ([3]).

ii) Podľa tejto zásady sa v článku 15 ods. 1 zákona stanovuje, že osobné informácie získané prevádzkovateľom osobných informácií možno používať na účel získania, a v článku 18 ods. 1 sa stanovuje, že osobné informácie by sa nemali používať nad rámec účelu získania alebo poskytnúť tretej strane.

([3]) Keďže v týchto ustanoveniach sa stanovujú všeobecné zásady, ktoré sa uplatňujú na každé spracúvanie osobných informácií, čiže aj na spracúvanie, ktoré sa osobitne upravuje v iných zákonoch, objasnenia v tomto oddiele sa uplatňujú aj na situácie, v ktorých sa osobné údaje spracúvajú na základe iných zákonov (pozri napr. článok 15 ods. 1 zákona o úverových informáciách, v ktorom sa na tieto ustanovenia osobitne odkazuje).

iii) Aj vtedy, ak možno osobné informácie používať na iné účely ako zamýšľaný účel alebo poskytnúť vo výnimočných prípadoch ([4]) uvedených v pododsekoch článku 18 ods. 2 zákona tretej strane, sa musí žiadať o obmedzenie účelu alebo metódy použitia, aby bolo možné osobné informácie spracúvať bezpečne podľa odseku 5, alebo prijatie opatrení potrebných na zaistenie bezpečnosti osobných informácií.

iv) Uvedené ustanovenia sa uplatňujú rovnako na spracúvanie všetkých osobných informácií prijatých na území kórejskej jurisdikcie z tretej krajiny bez ohľadu na štátnu príslušnosť dotknutej osoby.

v) Ak napríklad prevádzkovateľ osobných informácií v EÚ uskutoční prenos osobných informácií kórejskému prevádzkovateľovi osobných informácií na základe rozhodnutia Európskej komisie o primeranosti, účel prenosu osobných informácií prevádzkovateľa osobných informácií v EÚ sa považuje za účel získania osobných informácií kórejského prevádzkovateľa osobných informácií a v takých prípadoch môže kórejský prevádzkovateľ osobných informácií používať osobné informácie alebo ich poskytnúť tretej strane len na účel získania, a to okrem výnimočných prípadov uvedených v pododsekoch článku 18 ods. 2 zákona.

2. **Obmedzenie následného prenosu osobných údajov (článok 17 ods. 3 a 4 a článok 18 zákona)**

<Zákon o ochrane osobných informácií

(zákon č. 16930, čiastočne zmenený 4. februára 2020)>

Článok 17 (Poskytovanie osobných informácií) (1) vypúšťa sa

(2) Prevádzkovateľ osobných informácií informuje po získaní súhlasu podľa odseku 1 pododseku 1 dotknutú osobu o týchto skutočnostiach. To isté platí v prípade úpravy niektorej z týchto skutočností:

1. príjemcovi osobných informácií;
2. účele, na ktorý príjemca osobných informácií tieto informácie používa;
3. podrobnostiach o tom, ktoré osobné informácie sa majú poskytnúť;
4. období, počas ktorého príjemca uchováva a používa osobné informácie;
5. skutočnosti, že dotknutá osoba má nárok na odopretie súhlasu, a o všetkých prípadných nevýhodách, ktoré z odopretia súhlasu vyplývajú.

(3) Prevádzkovateľ osobných informácií informuje dotknutú osobu o skutočnostiach uvedených v odseku 2 a získa súhlas dotknutej osoby s poskytnutím osobných informácií tretej strane v zahraničí; a neuzavrie zmluvu o cezhraničnom prenose osobných informácií, ktorá by bola v rozpore s týmto zákonom.

(4) Prevádzkovateľ osobných informácií môže poskytnúť osobné informácie bez súhlasu dotknutej osoby v rozsahu, ktorý primerane súvisí s účelmi, na ktoré sa osobné informácie pôvodne získali, a to podľa skutočností stanovených v prezidentskom dekréte, pričom prihliadne na to, či bude dotknutá osoba znevýhodnená a či boli prijaté potrebné opatrenia na zaistenie bezpečnosti, ako napríklad šifrovanie, atď.

※ Informácie o článku 18 pozri na stranách 3, 4 a 5.

< **Vykonávací dekrét k zákonu o ochrane osobných informácií**

([Dátum začatia uplatňovania: 5. februára 2021.] [Prezidentský dekrét č. 30892 zo 4. augusta 2020, ktorým sa menia ďalšie zákony])>

Článok 14-2 (Normy týkajúce sa ďalšieho použitia/poskytnutia osobných informácií atď.)

(1) Ak prevádzkovateľ osobných informácií použije alebo poskytne osobné informácie (ďalej len „ďalšie použitie alebo poskytnutie osobných informácií“) bez súhlasu dotknutej osoby vydaného v súlade s článkom 15 ods. 3 zákona alebo článkom 17 ods. 4 zákona, prevádzkovateľ osobných informácií zváži tieto skutočnosti:

1. či ďalšie použitie alebo poskytnutie primerane súvisí s pôvodným účelom, na ktorý sa osobné informácie získali;
2. či sa ďalšie použitie alebo poskytnutie osobných informácií predpokladá vzhľadom na okolnosti, za ktorých sa osobné informácie získali, a na postupy ich spracúvania;
3. či sa ďalším použitím alebo poskytnutím osobných informácií nespravodlivo nepoškodzujú záujmy dotknutej osoby a
4. či sa prijali opatrenia potrebné na zaistenie bezpečnosti, ako napríklad pseudonymizácia alebo šifrovanie.

([4]) Na poskytovateľov služieb informačnej komunikácie sa vzťahuje iba článok 18 ods. 2 pododseky 1 a 2. Pododseky 5 až 9 sa vzťahujú iba na verejné inštitúcie.

(2) Prevádzkovateľ osobných informácií v politike ochrany súkromia vopred oznámi podľa článku 30 ods. 1 zákona kritériá posudzovania skutočností uvedených v pododsekoch odseku 1 a zodpovedná osoba pre ochranu súkromia podľa článku 31 ods. 1 zákona overí, či prevádzkovateľ osobných informácií ďalej používa alebo poskytuje osobné informácie v súlade s príslušnými normami.

i) Ak prevádzkovateľ osobných informácií poskytne osobné informácie tretej strane v zahraničí, musí vopred informovať dotknutú osobu o všetkých skutočnostiach uvedených v článku 17 ods. 2 zákona a získať jej súhlas. Výnimkou sú prípady uvedené v odsekoch 1 a 2. Neuzavrie žiadnu zmluvu o cezhraničnom poskytnutí osobných údajov, ktorá by bola v rozpore s týmto zákonom.

(1) Ak sa osobné informácie poskytujú v rozsahu, ktorý primerane súvisí s pôvodným účelom získania informácií podľa článku 17 ods. 4 zákona. Prípady, na ktoré sa uplatňuje toto ustanovenie, sa však obmedzujú na prípady, pri ktorých sú splnené normy týkajúce sa ďalšieho použitia/poskytnutia osobných informácií stanovené v článku 14-2 vykonávacieho dekrétu. Okrem toho musí prevádzkovateľ osobných informácií zvážiť, či môže poskytnutie osobných informácií predstavovať pre dotknuté osoby nevýhodu, a či prijal potrebné opatrenia na zaistenie bezpečnosti, napríklad šifrovanie.

(2) Ak možno vo výnimočných prípadoch uvedených v článku 18 ods. 2 zákona (pozri strany 3 až 5) poskytnúť osobné informácie tretej strane. Aj v týchto prípadoch však platí, že ak by sa poskytnutím takýchto osobných informácií pravdepodobne nespravodlivo poškodili záujmy dotknutej osoby alebo tretej strany, osobné informácie nemožno tretej strane poskytnúť. Okrem toho musí poskytovateľ osobných informácií príjemcu osobných informácií požiadať o obmedzenie účelu alebo metódy použitia osobných informácií alebo o prijatie opatrení potrebných na zaistenie ich bezpečnosti, aby bolo možné osobné informácie bezpečne spracúvať.

ii) Ak sa osobné informácie poskytnú tretej strane v zahraničí, nemusí sa na ne vzťahovať úroveň ochrany zaručená kórejským zákonom o ochrane osobných informácií, keďže jednotlivé krajiny majú rôzne systémy ochrany osobných informácií. Vzhľadom na to sa budú takéto prípady považovať za „prípady, v ktorých môže dôjsť k znevýhodneniu dotknutej osoby“, ktoré sú uvedené v článku 17 ods. 4 zákona, alebo za „prípady, v ktorých je nespravodlivo poškodený záujem dotknutej osoby alebo tretej strany“, ktoré sú uvedené v článku 18 ods. 2 zákona a v článku 14-2 vykonávacieho dekrétu k tomu istému zákonu ([5]). Prevádzkovateľ osobných informácií a tretia strana musia preto s cieľom splniť požiadavky týchto ustanovení výslovne zabezpečiť úroveň ochrany rovnocennú úrovni ochrany v zákone, a to vrátane záruky uvedenej v právne záväzných dokumentoch, akými sú zmluvy, že dotknutá osoba si bude môcť uplatniť svoje práva aj po prenose osobných informácií do zahraničia.

3. **Oznamovanie údajov, ak osobné údaje neboli získané od dotknutej osoby (článok 20 zákona)**

<Zákon o ochrane osobných informácií

(zákon č. 16930, čiastočne zmenený 4. februára 2020)>

Článok 20 (Oznámenie zdrojov atď. osobných informácií získaných od tretích strán) (1) Ak prevádzkovateľ osobných informácií spracúva osobné informácie získané od tretích strán, bezodkladne oznámi dotknutej osobe na jej žiadosť tieto skutočnosti:

1. zdroj získaných osobných informácií;

2. účel spracúvania osobných informácií;

3. skutočnosť, že dotknutá osoba má nárok žiadať o pozastavenie spracúvania osobných informácií, ako sa to stanovuje v článku 37.

(2) Bez toho, aby bol dotknutý odsek 1, platí, že ak prevádzkovateľ osobných informácií spĺňajúci kritériá stanovené v prezidentskom dekréte a prihliadajúci na druhy a objem spracúvaných osobných informácií, počet zamestnancov, výšku zisku atď. získava osobné informácie od tretích strán a spracúva ich podľa článku 17 ods. 1 pododseku 1, oznámi dotknutej osobe skutočnosti uvedené v odseku 1, a to za predpokladu, že sa to neuplatňuje, ak informácie získané prevádzkovateľom osobných informácií neobsahujú žiadne osobné informácie, ako napríklad kontaktné informácie, na základe ktorých by bolo možné informovať dotknutú osobu.

([5]) Podľa článku 18 ods. 2 pododseku 2 zákona o ochrane osobných údajov sa to vzťahuje aj na poskytovanie osobných informácií tretím stranám v zahraničí na základe ustanovení iných zákonov (ako napr. zákona o úverových informáciách).

(3) Potrebné skutočnosti týkajúce sa času, metódy a postupu oznamovania dotknutej osobe podľa hlavnej vety odseku 2 sa stanovujú v prezidentskom dekréte.

(4) Odsek 1 a hlavná veta odseku 2 sa neuplatňujú na žiadnu z týchto okolností len za predpokladu, že ide o prípad, v ktorom je to podľa tohto zákona preukázateľne nadradené právam dotknutej osoby:

1. ak sú osobné informácie, na ktoré sa vzťahuje požiadavka na oznamovanie, súčasťou zložiek osobných informácií uvedených v niektorom z pododsekov článku 32 ods. 2;

2. ak je pravdepodobné, že toto oznámenie spôsobí ohrozenie života alebo fyzickej integrity akejkoľvek ďalšej osoby, prípadne nespravodlivé poškodenie majetku a ďalších záujmov akejkoľvek ďalšej osoby.

i) Ak prevádzkovateľ osobných informácií prijme osobné informácie prenesené z EÚ na základe rozhodnutia o primeranosti ([6]), musí bezodkladne, v každom prípade však najneskôr mesiac od prenosu, oznámiť dotknutej osobe informácie uvedené v pododsekoch 1 až 5.

   1. Meno a kontaktné informácie osôb, ktoré prenášajú a prijímajú osobné informácie.

   2. Položky alebo kategórie prenášaných osobných informácií.

   3. Účel získania a použitia osobných informácií (stanovený vývozcom údajov podľa bodu 1 tohto oznámenia).

   4. Obdobie uchovávania osobných informácií.

   5. Informácie o právach dotknutej osoby pri spracúvaní osobných informácií, metóde a postupe uplatňovania práv a o všetkých prípadných nevýhodách vyplývajúcich z uplatnenia daných práv.

ii) Aj v prípade, ak prevádzkovateľ osobných informácií poskytne osobné informácie uvedené v bode i) tretej strane v Kórejskej republike alebo v zahraničí, musí dotknutej osobe pred poskytnutím osobných informácií oznámiť informácie uvedené v pododsekoch 1 až 5.

   1. Meno a kontaktné informácie osôb, ktoré poskytujú a prijímajú osobné informácie.

   2. Položky alebo kategórie poskytnutých osobných informácií.

   3. Krajinu, ktorej sa osobné informácie poskytnú, predpokladaný dátum a metóda ich poskytnutia (obmedzuje sa na prípady, keď sa osobné informácie poskytujú tretej strane v zahraničí).

   4. Účel poskytovateľa osobných informácií a právny základ poskytovania osobných informácií.

   5. Informácie o právach dotknutej osoby pri spracúvaní osobných informácií, metóde a postupe uplatňovania práv a o všetkých prípadných nevýhodách vyplývajúcich z uplatnenia daných práv.

iii) Prevádzkovateľ osobných informácií nesmie uplatňovať podmienky z bodov i) alebo ii) v žiadnom z týchto prípadov uvedených v pododsekoch 1 až 4.

   1. Ak sú osobné informácie, ktoré je potrebné oznámiť, súčasťou niektorej zložky osobných informácií uvedenej v článku 32 ods. 2 zákona v rozsahu, v akom sú záujmy chránené týmto ustanovením preukázateľne nadradené právam dotknutej osoby a iba dovtedy, kým oznámenie ohrozuje plnenie príslušných záujmov, napríklad prebiehajúce vyšetrovanie trestného činu alebo národnú bezpečnosť.

   2. Ak a dovtedy, kým je pravdepodobné, že oznámenie spôsobí ohrozenie života alebo fyzickej integrity inej osoby, prípadne nespravodlivé poškodenie majetkových záujmov inej osoby, ak sú tieto práva a záujmy preukázateľne nadradené právam dotknutej osoby.

   3. Ak dotknutá osoba už má informácie, ktoré je prevádzkovateľ osobných informácií povinný oznámiť podľa bodu i) alebo ii).

   4. Ak prevádzkovateľ osobných informácií nemá žiadne kontaktné informácie o dotknutej osobe alebo by sa na kontaktovanie dotknutej osoby vyžadovalo nadmerné úsilie, a to aj v súvislosti so spracúvaním podľa podmienok stanovených v oddiele 3 zákona o ochrane osobných informácií. Pri určovaní toho, či je možné kontaktovať dotknutú osobu alebo či toto kontaktovanie vyžaduje nadmerné úsilie, by sa mala zvážiť možnosť spolupráce s vývozcom údajov v EÚ.

([6]) Povinnosti z bodov i), ii) a iii) sa uplatňujú aj vtedy, keď prevádzkovateľ, ktorý prijme osobné informácie z EÚ na základe rozhodnutia o primeranosti, spracúva takéto informácie na základe iných zákonov, napríklad zákona o úverových informáciách.

4. **Rozsah uplatňovania osobitnej výnimky zo spracúvania pseudonymizovaných informácií (články 28-2, 28-3, 28-4, 28-5, 28-6 a 28-7, článok 3 a článok 58-2 zákona)**

<Zákon o ochrane osobných informácií

(zákon č. 16930, čiastočne zmenený 4. februára 2020)>

Kapitola III Spracúvanie osobných informácií

ODDIEL 3 Osobitné prípady týkajúce sa pseudonymných údajov

Článok 28-2 (Spracúvanie pseudonymných údajov) (1) Prevádzkovateľ osobných informácií môže spracúvať pseudonymizované informácie bez súhlasu dotknutých osôb na štatistické účely, účely vedeckého výskumu a na archivačné účely vo verejnom záujme atď.

(2) Prevádzkovateľ osobných informácií nezačlení do pseudonymizovaných informácií poskytovaných tretej strane podľa odseku 1 informácie, ktoré možno použiť na identifikáciu konkrétneho jednotlivca.

Článok 28-3 (Obmedzenie kombinovania pseudonymných údajov) (1) Bez toho, aby bol dotknutý článok 28-2, uskutočňuje kombinovanie pseudonymizovaných informácií spracúvaných rôznymi prevádzkovateľmi osobných informácií na štatistické účely, vedecký výskum a archivovanie záznamov z dôvodu verejného záujmu atď. špecializovaná inštitúcia určená Komisiou pre ochranu osobných informácií alebo vedúcim súvisiaceho ústredného správneho orgánu.

(2) Prevádzkovateľ osobných informácií, ktorý zamýšľa sprístupniť kombinované informácie mimo organizácie, ktorá ich skombinovala, získa po spracovaní informácií do psedonymizovanej podoby alebo podoby uvedenej v článku 58-2 súhlas vedúceho špecializovanej inštitúcie.

(3) Potrebné skutočnosti vrátane postupov a metód kombinovania podľa odseku 1, normy a postupy menovania alebo zrušenia menovania vedenia špecializovanej inštitúcie a dohľadu nad ňou, ako aj normy a postupy vývozu a schvaľovania podľa odseku 2 sa stanovujú v prezidentskom dekréte.

Článok 28-4 (Povinnosť prijať bezpečnostné opatrenia v prípade pseudonymných údajov) (1) Pri spracúvaní pseudonymizovaných informácií prijme prevádzkovateľ osobných informácií také technické, organizačné a fyzické opatrenia na osobitné uloženie a riadenie dodatočných informácií potrebných na obnovu ich pôvodného stavu, ktoré môžu byť potrebné na zaistenie bezpečnosti podľa požiadaviek prezidentského dekrétu, aby sa osobné informácie nemohli stratiť, odcudziť, prezradiť, sfalšovať, upraviť alebo poškodiť.

(2) Prevádzkovateľ osobných informácií, ktorý zamýšľa spracúvať pseudonymizované informácie, vypracuje a uchováva záznamy týkajúce sa skutočností stanovených v prezidentskom dekréte, a to aj účelu spracúvania pseudonymizovaných informácií a tretej strany, ktorá prijíma pseudonymizované informácie, aby bolo možné riadiť spracúvanie pseudonymizovaných informácií.

Článok 28-5 (Zakázané konanie v rámci spracúvania pseudonymizovaných informácií) (1) Nikto nesmie spracúvať pseudonymizované informácie na účel identifikovania konkrétneho jednotlivca.

(2) Ak sa pri spracúvaní pseudonymizovaných informácií objavia informácie, na základe ktorých je možné identifikovať konkrétneho jednotlivca, prevádzkovateľ osobných informácií spracúvanie informácií okamžite ukončí a informácie vyhľadá a zničí.

Článok 28-6 (Uloženie správnych pokút za spracúvanie pseudonymizovaných informácií) (1) Komisia môže uložiť pokutu do výšky troch stotín celkového zisku prevádzkovateľa údajov, ktorý v rozpore s článkom 28-5 ods. 1 spracoval údaje na účel identifikovania konkrétneho jednotlivca, a to za predpokladu, že v prípade, ak sa nevytvoril zisk alebo je zložité vypočítať príjmy zo zisku, sa môže prevádzkovateľovi údajov uložiť pokuta vo výške najviac 400 miliónov wonov alebo troch stotín kapitálovej sumy podľa toho, ktorá suma je vyššia.

(2) Článok 34-2 ods. 3 až 5 sa *mutatis mutandis* uplatňuje na skutočnosti potrebné na uloženie a výber správnych pokút.

Článok 28-7 (Rozsah uplatňovania) Články 20, 21, 27, článok 34 ods. 1, články 35 až 37, 39-3, 39-4, 39-6 až 39-8 sa na pseudonymizované informácie neuplatňujú.

Kapitola I Všeobecné ustanovenia

Článok 3 (Zásady ochrany osobných informácií) (1) Prevádzkovateľ osobných informácií výslovne stanoví účely, na ktoré sa osobné informácie spracúvajú; a osobné informácie získava zákonným a spravodlivým spôsobom v minimálnom rozsahu potrebnom na tieto účely.

(2) Prevádzkovateľ osobných informácií spracúva osobné informácie primeraným spôsobom potrebným na účely, na ktoré sa osobné informácie spracúvajú, a nepoužíva tieto informácie na iné účely.

(3) Prevádzkovateľ osobných informácií zabezpečuje presnosť, úplnosť a aktuálnosť osobných informácií v rozsahu potrebnom na účely, na ktoré sa osobné informácie spracúvajú.

(4) Prevádzkovateľ osobných informácií riadi osobné informácie bezpečne podľa metód spracúvania, druhov atď. osobných informácií, pričom prihliada na možnosť porušenia práv dotknutej osoby a závažnosť príslušných rizík.

(5) Prevádzkovateľ osobných informácií zverejní svoju politiku ochrany súkromia a ďalšie skutočnosti súvisiace so spracúvaním osobných informácií; a zaručuje práva dotknutej osoby, akým je napríklad právo na prístup k svojim osobným informáciám.

(6) Prevádzkovateľ osobných informácií spracúva osobné informácie tak, aby minimalizoval možnosť porušenia ochrany súkromia dotknutej osoby.

(7) Ak možno účely získania osobných informácií dosiahnuť aj spracúvaním anonymizovaných alebo pseudonymizovaných osobných informácií, prevádzkovateľ osobných informácií sa usiluje o spracúvanie osobných informácií prostredníctvom anonymizácie, ak je anonymizácia možná, alebo prostredníctvom pseudonymizácie, ak účely získania osobných informácií nemožno dosiahnuť prostredníctvom anonymizácie.

(8) Prevádzkovateľ osobných informácií sa usiluje získať dôveru dotknutých osôb dodržiavaním a plnením povinností, ktoré mu vyplývajú z tohto zákona a ďalších súvisiacich právnych predpisov.

Kapitola IX Doplňujúce ustanovenia

Článok 58-2 (Výnimka z uplatňovania) Tento zákon sa neuplatňuje na informácie, na základe ktorých nie je možné po ich skombinovaní s inými informáciami identifikovať konkrétneho jednotlivca, pričom sa primerane prihliadne na čas, náklady, technológie atď. <Tento článok bol vložený zákonom č. 16930 zo 4. februára 2020>

i) V kapitole III oddiele 3 Osobitné prípady týkajúce sa pseudonymných údajov (články 28-2 až 28-7) sa umožňuje spracúvanie pseudonymizovaných informácií bez súhlasu dotknutej osoby na účely zostavovania štatistík, vedeckého výskumu a archivovania verejných záznamov atď. (článok 28-2), ale v týchto prípadoch sú povinné primerané záruky a zákazy potrebné na ochranu práv dotknutých osôb (články 28-4 a 28-5), pričom porušovateľom ustanovení možno uložiť sankčné pokuty (článok 28-6) a niektoré záruky, ktoré sú inak podľa zákona o ochrane osobných informácií dostupné, sa v tomto prípade neuplatňujú (článok 28-7).

ii) Tieto ustanovenia sa neuplatňujú na prípady, keď sa pseudonymizované informácie spracúvajú na účely iné ako zostavovanie štatistík, vedecký výskum, archivovanie verejných záznamov atď. Ak sa napríklad na účely iné ako zostavovanie štatistík, vedecký výskum, archivovanie verejných záznamov atď. pseudonymizujú osobné informácie jednotlivca z EÚ, ktoré boli prenesené do Kórey na základe rozhodnutia Európskej komisie o primeranosti, osobitné ustanovenia kapitoly III oddielu 3 sa neuplatňujú ([7]).

iii) Ak prevádzkovateľ osobných informácií spracúva pseudonymizované informácie na účely zostavovania štatistík, vedeckého výskumu, archivovania verejných záznamov atď. a ak pseudonymizované informácie neboli po dosiahnutí konkrétneho účelu spracúvania zničené v súlade s článkom 37 ústavy a článkom 3 (Zásady ochrany osobných informácií) zákona, anonymizuje informácie s cieľom zabezpečiť, aby sa už na ich základe nedal identifikovať konkrétny jednotlivec ani v prípade ich samostatného použitia, ani v prípade ich kombinácie s inými informáciami, pričom sa primerane prihliadne na čas, náklady, technológiu atď. v súlade s článkom 58-2 zákona o ochrane osobných informácií.

5. **Nápravné opatrenia atď. (článok 64 ods. 1, 2 a 4 zákona)**

<Zákon o ochrane osobných informácií

(zákon č. 16930, čiastočne zmenený 4. februára 2020)>

Článok 64 (Nápravné opatrenia) (1) Ak má Komisia pre ochranu osobných informácií závažné dôvody domnievať sa, že došlo k porušeniu ochrany osobných informácií, pričom neprijatie opatrení pravdepodobne spôsobí škodu, ktorú je ťažké napraviť, môže nariadiť porušiteľovi tohto zákona (okrem ústredných správnych orgánov, miestnych samospráv, národného zhromaždenia, súdu, ústavného súdu a národnej volebnej komisie) prijatie niektorých z týchto opatrení:

1. zastaviť porušovanie ochrany osobných informácií;

2. dočasne pozastaviť spracúvanie osobných informácií;

([7]) Podobne sa výnimka z článku 40-3 zákona o úverových informáciách uplatňuje iba na spracúvanie pseudonymizovaných úverových informácií na účely zostavovania štatistík, vedeckého výskumu a archivovania verejných záznamov.

3. prijať iné opatrenia potrebné na ochranu osobných informácií a predchádzanie porušovaniu ochrany osobných informácií.

(2) Ak má vedúci súvisiaceho ústredného správneho orgánu závažné dôvody sa domnievať, že došlo k porušeniu ochrany osobných informácií, pričom neprijatie opatrení pravdepodobne spôsobí škodu, ktorú je ťažké napraviť, môže nariadiť prevádzkovateľovi osobných informácií prijatie niektorých opatrení uvedených v pododseku 1 podľa predpisov, ktoré sa vzťahujú na súvisiaci ústredný správny orgán.

(4) Ak ústredný správny orgán, miestna samospráva, národné zhromaždenie, súd, ústavný súd alebo národná volebná komisia poruší tento zákon, Komisia pre ochranu osobných informácií môže odporučiť vedúcemu príslušného úradu prijatie niektorých opatrení uvedených v odseku 1. V takýchto prípadoch, ak nenastali žiadne mimoriadne okolnosti, orgán odporúčanie po jeho prijatí vykoná.

i) V súdnych rozsudkoch ([8]) ([9]) sa „škoda, ktorú je ťažké napraviť“ vykladá ako prípad, ktorý môže spôsobiť poškodenie osobných práv alebo súkromia jednotlivca.

ii) Vzhľadom na to sa „závažné dôvody sa domnievať, že došlo k porušeniu ochrany osobných informácií, pričom neprijatie opatrení pravdepodobne spôsobí škodu, ktorú je ťažké napraviť“ stanovené v článku 64 ods. 1 a 2 vzťahujú na prípady, keď sa porušenie zákona považuje za také, ktoré pravdepodobne porušuje práva a slobodu jednotlivcov v oblasti ochrany osobných informácií. Toto ustanovenie sa bude uplatňovať pri každom porušení zásad, práv a povinností vyplývajúcich zo zákona o ochrane osobných informácií ([10]).

iii) V článku 64 ods. 3 zákona o ochrane osobných informácií sa uvádza opatrenie týkajúce sa „porušenia tohto zákona“, t. j. opatrenie proti porušovaniu zákona o ochrane osobných informácií.

Ústredný správny orgán atď. ako orgán verejnej moci viazaný zásadami právneho štátu nesmie porušiť žiadny zákon a v mimoriadnom prípade, keď napriek tomu dôjde k nezákonnému konaniu, je povinný prijať nápravné opatrenie vrátane okamžitého zastavenia daného konania a nahradiť vzniknuté škody.

Vzhľadom na to musí ústredný správny orgán aj bez zásahu Komisie pre ochranu osobných informácií vykonaného podľa článku 64 ods. 4 zákona o ochrane osobných informácií prijať opatrenie na nápravu akéhokoľvek porušenia zákona, ak sa o ňom dozvie.

Konkrétne platí, že ak Komisia pre ochranu osobných informácií odporučí nápravné opatrenie, ústrednému správnemu orgánu musí byť objektívne jasné, že porušil zákon. Ak sa ústredný správny orgán atď. domnieva, že by nemal vykonať odporúčanie Komisie pre ochranu osobných údajov, musí predložiť jednoznačné dôvody, z ktorých vyplýva, že nedošlo k porušeniu zákona. Odporúčanie sa musí vykonať, ak Komisia pre ochranu osobných informácií stanoví, že takýto prípad nenastal.

Vzhľadom na to sa musia „mimoriadne okolnosti“ uvedené v článku 64 ods. 4 zákona o ochrane osobných informácií prísne obmedzovať na mimoriadne okolnosti, z ktorých jednoznačne vyplýva, že ústredné správne orgány atď. „v skutočnosti tento zákon neporušili“, ako sú „prípady s mimoriadnymi (skutkovými alebo právnymi) okolnosťami“, o ktorých Komisia pre ochranu osobných informácií pôvodne pri vydávaní odporúčania nevedela. Komisia pre ochranu osobných informácií potom určí, že k porušeniu zákona naozaj nedošlo.

6. **Uplatňovanie zákona o ochrane osobných informácií na spracúvanie osobných údajov na účely národnej bezpečnosti, a to aj pri vyšetrovaní porušení a pri presadzovaní práva v súlade so zákonom o ochrane osobných informácií (článok 7-8, článok 7-9, článok 58, článok 3, článok 4 a článok 62 zákona o ochrane osobných informácií)**

<Zákon o ochrane osobných informácií

(zákon č. 16930, čiastočne zmenený 4. februára 2020)>

Článok 7-8 (Práca Komisie pre ochranu osobných informácií) (1) Komisia pre ochranu osobných informácií sa zaoberá: […]

3. Záležitosťami týkajúcimi sa vyšetrovania porušenia práva dotknutých osôb a následných právnych úkonov.

4. Vybavovaním sťažností alebo nápravnými postupmi týkajúcimi sa spracúvania osobných informácií a mediáciou sporov v oblasti osobných informácií.

[…]

([8]) (Rozsudok najvyššieho súdu č. 97Da10215,10222 z 26. januára 1999). Ak sa trestná činnosť obvinenej osoby zverejní prostredníctvom médií, pravdepodobne to spôsobí nenapraviteľnú psychickú aj fyzickú škodu nielen obeti, t. j. navrhovateľovi, ale aj osobám v jej okolí vrátane rodinných príslušníkov.

([9]) (Rozsudok Najvyššieho soulského súdu č. 2006Na92006 zo 16. januára 2008). Ak sa zverejní hanlivý článok, pravdepodobne to príslušnej osobe spôsobí závažnú nenapraviteľnú škodu.

([10]) Rovnaké zásady, aké sa stanovujú v bode ii), sa uplatňujú v článku 45-4 zákona o úverových informáciách.

Článok 7-9 (Záležitosti podliehajúce konzultácii a rozhodnutiu Komisie pre ochranu osobných informácií) (1) Komisia pre ochranu osobných informácií konzultuje a rozhoduje o týchto záležitostiach: […]

5. Záležitostiach týkajúcich sa výkladu a fungovania právnych predpisov týkajúcich sa ochrany osobných informácií.

[…]

Článok 58 (Čiastočné vylúčenie z uplatňovania) (1) Kapitoly III až VII sa neuplatňujú na žiadne z týchto osobných informácií:

1. Osobné informácie získané podľa zákona o štatistike na účely spracúvania vykonávané verejnými inštitúciami.

2. Osobné informácie získané alebo vyžiadané na účely analýzy informácií súvisiacich s národnou bezpečnosťou.

3. Osobné informácie spracúvané dočasne v prípade naliehavej potreby zaistenia verejnej ochrany a bezpečnosti, verejného zdravia atď.

4. Osobné informácie získané alebo použité na vlastné účely podávania správ tlačou, vykonávanie misijných činností náboženskými organizáciami a vymenovanie kandidátov politických strán.

[vypúšťajú sa odseky 2 a 3]

(4) V prípade spracúvania osobných informácií podľa odseku 1 spracúva prevádzkovateľ osobných informácií osobné informácie v minimálnom rozsahu potrebnom na dosiahnutie zamýšľaného účelu a počas minimálneho obdobia; a takisto zabezpečuje potrebné úpravy, ako sú technické, riadiace a fyzické záruky, vybavuje individuálne sťažnosti a prijíma ďalšie potrebné opatrenia na bezpečné riadenie a primerané spracúvanie takýchto osobných informácií.

Článok 3 (Zásady ochrany osobných informácií) (1) Prevádzkovateľ osobných informácií výslovne stanoví účely, na ktoré sa osobné informácie spracúvajú; a osobné informácie získava zákonným a spravodlivým spôsobom v minimálnom rozsahu potrebnom na tieto účely.

(2) Prevádzkovateľ osobných informácií spracúva osobné informácie primeraným spôsobom potrebným na účely, na ktoré sa osobné informácie spracúvajú, a nepoužíva tieto informácie na iné účely.

(3) Prevádzkovateľ osobných informácií zabezpečuje presnosť, úplnosť a aktuálnosť osobných informácií v rozsahu potrebnom na účely, na ktoré sa osobné informácie spracúvajú.

(4) Prevádzkovateľ osobných informácií riadi osobné informácie bezpečne podľa metód spracúvania, druhov atď. osobných informácií, pričom prihliada na možnosť porušenia práv dotknutej osoby a závažnosť príslušných rizík.

(5) Prevádzkovateľ osobných informácií zverejní svoju politiku ochrany súkromia a ďalšie skutočnosti súvisiace so spracúvaním osobných informácií; a zaručuje práva dotknutej osoby, akým je napríklad právo na prístup k svojim osobným informáciám.

(6) Prevádzkovateľ osobných informácií spracúva osobné informácie tak, aby minimalizoval možnosť porušenia ochrany súkromia dotknutej osoby.

(7) Ak možno účely získania osobných informácií dosiahnuť aj spracúvaním anonymizovaných alebo pseudonymizovaných osobných informácií, prevádzkovateľ osobných informácií sa usiluje o spracúvanie osobných informácií prostredníctvom anonymizácie, ak je anonymizácia možná, alebo prostredníctvom pseudonymizácie, ak účely získania osobných informácií nemožno dosiahnuť prostredníctvom anonymizácie.

(8) Prevádzkovateľ osobných informácií sa usiluje získať dôveru dotknutých osôb dodržiavaním a plnením povinností, ktoré mu vyplývajú z tohto zákona a ďalších súvisiacich právnych predpisov.

Článok 4 (Práva dotknutých osôb) Dotknutá osoba má pri spracúvaní svojich osobných informácií tieto práva:

1. právo byť informovaná o spracúvaní takýchto osobných informácií;

2. právo určiť, či dá súhlas, ako aj určiť rozsah súhlasu so spracúvaním takýchto osobných informácií;

3. právo na potvrdenie toho, či sa osobné informácie spracúvajú, a právo žiadať prístup (vrátane poskytnutia kópií; ďalej sa uplatňuje to isté) k takýmto osobným informáciám;

4. právo na pozastavenie spracúvania takýchto osobných informácií, ako aj právo požiadať o ich opravu, vymazanie a zničenie;

5. právo na rýchlu a spravodlivú primeranú nápravu všetkých škôd vyplývajúcich zo spracúvania takýchto osobných informácií.

Článok 62 (Oznamovanie porušení) (1) Každý, kto v priebehu spracúvania osobných informácií prevádzkovateľom osobných informácií utrpí ujmu z dôvodu porušenia svojich práv alebo poškodenia svojich záujmov v súvislosti so svojimi osobnými informáciami, môže toto porušenie nahlásiť Komisii pre ochranu osobných informácií.

(2) Komisia pre ochranu osobných informácií môže určiť špecializovanú inštitúciu, ktorá bude efektívne prijímať a vybavovať uplatňované nároky podľa odseku 1, ako sa to stanovuje v prezidentskom dekréte. V uvedených prípadoch táto špecializovaná inštitúcia zriadi a prevádzkuje call centrum pre porušovanie ochrany osobných informácií (ďalej len „call centrum pre ochranu súkromia“).

(3) Call centrum pre ochranu súkromia má tieto povinnosti:

1. prijíma uplatňované nároky a poskytuje konzultácie v súvislosti so spracúvaním osobných informácií;

2. vyšetruje a preveruje prípady a vypočúva stanoviská súvisiacich strán;

3. vykonáva povinnosti uvedené v pododsekoch 1 a 2.

(4) Komisia pre ochranu osobných informácií môže v prípade potreby vyslať podľa článku 32-4 zákona o verejných činiteľoch do špecializovanej inštitúcie určenej podľa odseku 2 zákona verejného činiteľa, ktorý efektívne vyšetrí a preverí prípady podľa odseku 3 pododseku 2 zákona.

i) Získavanie osobných informácií na účely národnej bezpečnosti sa upravuje v osobitných zákonoch, v ktorých sa príslušným orgánom (napr. Národnej spravodajskej službe) udeľuje právomoc zachytávať komunikáciu alebo požiadať o sprístupnenie informácií za splnenia určitých podmienok a záruk (ďalej len „zákony o národnej bezpečnosti“). K týmto zákonom o národnej bezpečnosti patrí napríklad zákon o ochrane súkromia komunikácie, zákon o boji proti terorizmu na ochranu občanov a verejnej bezpečnosti alebo zákon o telekomunikáciách. Okrem toho musí byť získavanie a ďalšie spracúvanie osobných informácií v súlade s požiadavkami zákona o ochrane osobných informácií. V tomto zmysle sa v článku 58 ods. 1 pododseku 2 zákona o ochrane osobných informácií uvádza, že kapitoly III až VII sa neuplatňujú na osobné informácie získané alebo vyžiadané na účely analýzy informácií súvisiacich s národnou bezpečnosťou. Táto čiastočná výnimka sa teda uplatňuje na spracúvanie osobných informácií na účely národnej bezpečnosti.

Zároveň platí, že kapitola I (Všeobecné ustanovenia), kapitola II (Zavedenie politík na ochranu osobných informácií atď.), kapitola VIII (Skupinové žaloby za porušenie ochrany údajov), kapitola IX (Doplňujúce ustanovenia) a kapitola X (Sankčné ustanovenia) zákona o ochrane osobných informácií sa na spracúvanie takýchto informácií uplatňujú. Platí to aj pre všeobecné zásady ochrany údajov stanovené v článku 3 (Zásady ochrany osobných informácií) a individuálne práva zaručené článkom 4 zákona o ochrane osobných informácií (Práva dotknutých osôb).

Okrem toho sa v článku 58 ods. 4 zákona o ochrane osobných informácií uvádza, že takéto informácie sa musia spracúvať v minimálnom rozsahu potrebnom na dosiahnutie zamýšľaného účelu a počas minimálneho obdobia; okrem toho sa vyžaduje, aby prevádzkovateľ osobných informácií zaviedol potrebné opatrenia na zaistenie bezpečného riadenia a primeraného spracúvania údajov, ako sú technické, riadiace a fyzické záruky, ako aj primerané opatrenia na vybavovanie individuálnych sťažností.

A napokon sa uplatňujú ustanovenia upravujúce úlohy a právomoci Komisie pre ochranu osobných informácií (vrátane článkov 60 – 65 zákona o ochrane osobných informácií týkajúcich sa vybavovania sťažností a prijímania odporúčaní a nápravných opatrení), ako aj ustanovenia o správnych a trestných sankciách (článok 70 a nasl. zákona o ochrane osobných informácií). Podľa článku 7-8 ods. 1 pododsekov 3 a 4 a článku 7-9 ods. 1 pododseku 5 zákona o ochrane osobných informácií sa tieto vyšetrovacie a nápravné právomoci, a to aj vtedy, ak sa uplatňujú pri vybavovaní sťažností, týkajú aj možných porušení pravidiel uvedených v osobitných zákonoch, v ktorých sa stanovujú obmedzenia a záruky v oblasti získavania osobných informácií, ako sú zákony o národnej bezpečnosti. Vzhľadom na požiadavky článku 3 ods. 1 zákona o ochrane osobných informácií týkajúce sa získavania osobných informácií zákonným a spravodlivým spôsobom predstavuje každého takéto porušenie nedodržanie „tohto zákona“ v zmysle článkov 63 a 64, preto môže Komisia pre ochranu osobných informácií uskutočniť vyšetrovanie a prijať nápravné opatrenia ([11]). Uplatňovaním týchto právomocí Komisie pre ochranu osobných informácií sa dopĺňajú, no nenahrádzajú právomoci Národnej komisie pre ľudské práva podľa zákona o Komisii pre ľudské práva.

Pri uplatňovaní základných zásad, práv a povinností uvedených v zákone o ochrane osobných informácií na spracúvanie osobných informácií na účely národnej bezpečnosti sa prihliada na záruky zakotvené v ústave, ktoré sa týkajú ochrany práva jednotlivca na riadenie svojich osobných informácií. Podľa rozhodnutia ústavného súdu sem patrí právo jednotlivca ([12]) „na vlastné rozhodnutie o tom, kedy, komu alebo kým a v akom rozsahu budú jeho informácie zverejnené alebo použité. Je to základné právo ([13]), […], existujúce na ochranu osobnej slobody rozhodovania pred rizikom, ktoré predstavuje rozširovanie funkcií štátu a informačných a komunikačných technológií“. Každé obmedzenie uvedeného práva, napríklad ak je to potrebné v záujme ochrany národnej bezpečnosti, si vyžaduje vyváženie práv a záujmov jednotlivca a príslušného verejného záujmu, pričom toto obmedzenie nesmie mať vplyv na podstatu uvedeného práva (článok 37 ods. 2 ústavy).

([11]) Informácie o nápravných opatreniach podľa článku 64 sa uvádzajú aj v oddiele 5.
([12]) Rozsudok ústavného súdu, č. 99HunMa513, č. 2004HunMa190 z 26. mája 2005.
([13]) Rozsudok ústavného súdu, 2003HunMa282 z 21. júla 2005.

Preto prevádzkovateľ (napr. Národná spravodajská služba) pri spracúvaní osobných informácií na účely národnej bezpečnosti okrem iného:

(1) výslovne stanoví účely, na ktoré sa osobné informácie spracúvajú, pričom osobné informácie získava zákonným a spravodlivým spôsobom v minimálnom rozsahu potrebnom na tieto účely (článok 3 ods. 1 zákona o ochrane osobných informácií); konkrétne získava a ďalej spracúva osobné informácie iba na účel vykonávania povinností, ktoré mu vyplývajú z príslušných právnych predpisov, akým je napríklad zákon o Národnej spravodajskej službe;

(2) spracúva osobné informácie v minimálnom rozsahu potrebnom na dosiahnutie zamýšľaného účelu a počas minimálneho obdobia (článok 58 ods. 4 zákona o ochrane osobných informácií); po dosiahnutí účelu spracúvania prevádzkovateľ osobné informácie nezvratne zničí, ak ich ďalšie uchovanie nie je osobitne nariadené právnym predpisom, pričom v takom prípade sa príslušné osobné informácie uložia a riadia oddelene od ostatných osobných informácií, nepoužívajú sa na žiadny iný účel okrem účelu stanoveného v právnom predpise a po uplynutí obdobia uchovávania sa zničia;

(3) spracúva osobné informácie primeraným spôsobom potrebným na účely, na ktoré sa osobné informácie spracúvajú, a nepoužíva tieto informácie na iné účely (článok 3 ods. 2 zákona o ochrane osobných informácií);

(4) zabezpečuje presnosť, úplnosť a aktuálnosť osobných informácií v rozsahu potrebnom na účely, na ktoré sa osobné informácie spracúvajú (článok 3 ods. 3 zákona o ochrane osobných informácií);

(5) riadi osobné informácie bezpečne podľa metód spracúvania, druhov atď. osobných informácií, pričom prihliada na možnosť porušenia práv dotknutej osoby a závažnosť príslušných rizík (článok 3 ods. 4 zákona o ochrane osobných informácií);

(6) zverejní svoju politiku ochrany súkromia a ďalšie skutočnosti súvisiace so spracúvaním osobných informácií (článok 3 ods. 5 zákona o ochrane osobných informácií);

(7) spracúva osobné informácie tak, aby minimalizoval možnosť porušenia ochrany súkromia dotknutej osoby (článok 3 ods. 6 zákona o ochrane osobných údajov).

ii) V súlade s článkom 58 ods. 4 zákona o ochrane osobných údajov prevádzkovateľ (napr. orgány z oblasti národnej bezpečnosti ako Národná spravodajská služba) prijme potrebné opatrenia, ako je zavedenie technických, riadiacich a fyzických záruk, aby sa zaistil súlad s uvedenými zásadami a primerané spracúvanie osobných informácií. Môžu k nim napríklad patriť osobitné opatrenia na zaistenie bezpečnosti osobných informácií, ako je obmedzenie prístupu k osobným informáciám, riadenie prístupu, logy, zabezpečovanie špecializovaných školení pre zamestnancov v oblasti nakladania s osobnými informáciami atď.

Ďalej majú dotknuté osoby podľa článku 3 ods. 5 a článku 4 zákona o ochrane osobných údajov v oblasti osobných informácií spracúvaných na účely národnej bezpečnosti okrem iného tieto práva:

(1) právo na potvrdenie toho, či sa ich osobné informácie spracúvajú, ako aj na informácie o spracúvaní, a právo na prístup k týmto informáciám vrátane poskytnutia kópií (článok 4 ods. 1 a 3 zákona o ochrane osobných informácií);

(2) právo na pozastavenie spracúvania a na opravu, vymazanie a zničenie osobných informácií (článok 4 ods. 4 zákona o osobných informáciách).

iii) Dotknutá osoba môže na základe týchto práv podať žiadosť priamo prevádzkovateľovi alebo nepriamo prostredníctvom Komisie pre ochranu osobných informácií alebo tým môže poveriť aj svojho zástupcu. Ak dotknutá osoba podá žiadosť, prevádzkovateľ jej právo bezodkladne prizná; no za predpokladu, že môže uplatnenie tohto práva odložiť, obmedziť alebo zamietnuť, ak sa to výslovne stanovuje v iných právnych predpisoch alebo je to nevyhnutné na ich dodržanie, a to v takom rozsahu a na tak dlho, ako je to potrebné a primerané na ochranu dôležitého cieľa verejného záujmu (napríklad v takom rozsahu a na tak dlho, ako by priznanie tohto práva ohrozovalo prebiehajúce vyšetrovanie alebo národnú bezpečnosť), alebo ak by mohlo priznanie práva spôsobiť ohrozenie života alebo fyzickej integrity tretej strany, prípadne neopodstatnené poškodenie majetku a iných záujmov tretej strany. Ak sa žiadosť zamietne alebo obmedzí, dotknutej osobe sa bezodkladne oznámia dôvody. Prevádzkovateľ vypracuje metódu a postup podávania žiadostí dotknutými osobami a zverejní ich, aby sa s nimi mohli dotknuté osoby oboznámiť.

Okrem toho majú dotknuté osoby podľa článku 58 ods. 4 zákona o ochrane osobných informácií (požiadavka na zabezpečenie primeraného vybavovania individuálnych sťažností) a článku 4 ods. 5 zákona o ochrane osobných informácií (právo na rýchlu a spravodlivú primeranú nápravu všetkých škôd vyplývajúcich zo spracúvania osobných informácií) právo na dosiahnutie nápravy. K tomu patrí právo na oznámenie údajného porušenia centru pre oznamovanie porušovania ochrany osobných informácií (v súlade s článkom 62 ods. 3 zákona o ochrane osobných informácií), na podanie sťažnosti Komisii pre ochranu osobných informácií podľa článku 62 zákona o ochrane osobných informácií týkajúcej sa akéhokoľvek porušenia práv alebo záujmov v súvislosti s osobnými informáciami jednotlivca a právo na dosiahnutie súdneho prostriedku nápravy proti rozhodnutiam alebo nečinnosti Komisie pre ochranu osobných informácií podľa Správneho súdneho poriadku. Okrem toho môžu dotknuté osoby dosiahnuť súdny prostriedok nápravy podľa Správneho súdneho poriadku, ak došlo k porušeniu ich práv alebo záujmov v dôsledku právneho úkonu alebo opomenutia prevádzkovateľa (napr. získania osobných údajov nezákonným spôsobom), prípadne získať náhradu škody za spôsobené škody podľa zákona o štátnom odškodnení. Tieto možnosti dosiahnutia nápravy sú dostupné v prípade možných porušení pravidiel konkrétnych zákonov, v ktorých sa stanovujú obmedzenia a záruky pri získavaní osobných informácií, akými sú zákony o národnej bezpečnosti, ako aj zákona o ochrane osobných informácií.

Jednotlivec z EÚ môže podať sťažnosť Komisii pre ochranu osobných informácií prostredníctvom svojho vnútroštátneho orgánu na ochranu údajov a Komisia pre ochranu osobných informácií bude jednotlivca po skončení vyšetrovania a prípadnom uložení nápravného opatrenia informovať prostredníctvom jeho vnútroštátneho orgánu na ochranu údajov.

PRÍLOHA II

18. mája 2021

Jeho Excelencia, pán Didier Reynders, komisár Európskej komisie pre spravodlivosť

Vaša Excelencia,

vítam konštruktívne diskusie medzi Kóreou a Európskou komisiou zamerané na budovanie rámca na prenos osobných údajov z EÚ do Kórey.

Na základe žiadosti Európskej komisie adresovanej vláde Kórey Vám v prílohe zasielam dokument poskytujúci prehľad o právnom rámci týkajúcom sa prístupu k informáciám vládou Kórey.

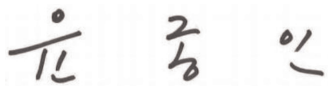
Tento dokument sa týka mnohých ministerstiev a orgánov štátnej správy Kórey a, pokiaľ ide o obsah dokumentu, príslušné ministerstvá a orgány (Komisia pre ochranu osobných informácií, ministerstvo spravodlivosti, Národná spravodajská služba, Národná komisia Kórey pre ľudské práva, Národné centrum pre boj proti terorizmu, Finančná spravodajská jednotka Kórey) sú zodpovedné za pasáže v rámci rozsahu ich príslušných právomocí. Príslušné ministerstvá a orgány s príslušnými podpismi sú uvedené ďalej.

Všetky otázky týkajúce sa tohto dokumentu možno zasielať Komisii pre ochranu osobných informácií, ktorá bude koordinovať potrebné odpovede medzi príslušnými ministerstvami a orgánmi.

Dúfam, že tento dokument bude užitočný pri prijímaní rozhodnutí v Európskej komisii.

Oceňujem Váš veľký doterajší prínos v tejto záležitosti.

S úctou



Yoon Jong In
predseda Komisie pre ochranu osobných informácií

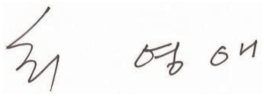
Tento dokument vypracovala Komisia pre ochranu osobných informácií a nasledujúce ministerstvá a orgány.



Park Jie Won
predseda (riaditeľ), Národná spravodajská služba



Lee Jung Soo
generálny riaditeľ, ministerstvo spravodlivosti



Choi Young Ae
predsedníčka, Národná komisia Kórey pre ľudské práva



Kim Hyuck Soo
riaditeľ, Národné centrum pre boj proti terorizmu



Kim Jeong Kag
komisár, Finančná spravodajská jednotka Kórey

Právny rámec na získavanie a používanie osobných údajov kórejskými orgánmi verejnej moci na účely presadzovania práva a národnej bezpečnosti

V tomto dokumente sa uvádza prehľad právneho rámca na získavanie a používanie osobných údajov kórejskými orgánmi verejnej moci na účely presadzovania práva v trestných veciach a národnej bezpečnosti (ďalej len „*prístup vlády*“), najmä pokiaľ ide o dostupné právne základy, uplatniteľné podmienky (obmedzenia) a záruky, ako aj nezávislý dozor a individuálne prostriedky nápravy.

1. VŠEOBECNÉ PRÁVNE ZÁSADY TÝKAJÚCE SA PRÍSTUPU VLÁDY

1.1. Ústavný rámec

V Ústave Kórejskej republiky sa stanovuje právo na súkromie vo všeobecnosti (článok 17) a právo na súkromie korešpondencie konkrétne (článok 18). Povinnosťou štátu je tieto základné práva zaručiť ([1]). Ďalej sa v ústave stanovuje, že práva a slobody občanov môžu byť obmedzené len zákonom a vtedy, ak je to potrebné z dôvodu národnej bezpečnosti alebo udržania verejného poriadku pre blaho verejnosti ([2]). Ani v prípade ich uloženia nemôžu tieto obmedzenia ovplyvňovať podstatu slobody alebo práva ([3]). Kórejské súdy uplatňujú tieto ustanovenia v prípadoch týkajúcich sa zasahovania štátu do súkromia. Najvyšší súd napríklad rozhodol, že monitorovanie civilného obyvateľstva je porušením základného práva na súkromie, a zdôraznil, že občania majú „*právo na sebaurčenie osobných informácií*“ ([4]). V inej veci ústavný súd rozhodol, že súkromie je základným právom, ktorým sa zabezpečuje ochrana pred zasahovaním štátu do súkromného života občanov a sledovaním súkromného života občanov ([5]).

V kórejskej ústave sa ďalej zaručuje, že nikto nebude nezákonne zatknutý, zadržiavaný, prehľadávaný či vypočúvaný, ani mu nebudú nezákonne zaistené žiadne predmety ([6]). Okrem toho možno prehliadky a zaistenie majetku vykonať len na základe príkazu, ktorý vydal sudca na žiadosť prokurátora, a pri dodržaní riadneho postupu ([7]). Za mimoriadnych okolností, t. j. v prípade zadržania podozrivého z trestnej činnosti pri páchaní trestného činu (*flagrante delicto*), alebo v prípade rizika, že osoba podozrivá zo spáchania trestného činu, za ktorý možno uložiť trest odňatia slobody aspoň tri roky, môže ujsť alebo zničiť dôkazy, môžu vyšetrovacie orgány vykonať prehliadku alebo zaistenie predmetov aj bez súdneho príkazu, pričom v takom prípade oň musia požiadať ex post ([8]). Tieto všeobecné zásady sa ďalej rozpracúvajú v konkrétnych zákonoch týkajúcich sa trestného konania a ochrany komunikácie (pozri podrobný prehľad ďalej).

Pokiaľ ide o cudzích štátnych príslušníkov, v ústave sa stanovuje, že ich postavenie je zaručené podľa medzinárodného práva a zmlúv ([9]). Kórea je zmluvnou stranou niekoľkých medzinárodných dohôd, v ktorých sa zaručuje právo na súkromie. Ide o Medzinárodný pakt o občianskych a politických právach (článok 17), Dohovor o právach osôb so zdravotným postihnutím (článok 22) a Dohovor o právach dieťaťa (článok 16). Okrem toho, hoci v ústave sa v zásade odkazuje na práva občanov, ústavný súd rozhodol, že držiteľmi základných práv sú aj cudzí štátni príslušníci ([10]). Konkrétne súd rozhodol, že ochrana dôstojnosti a ľudskej hodnoty človeka, ako aj právo usilovať sa o šťastný život,

([1]) Článok 10 Ústavy Kórejskej republiky vyhlásenej 17. júla 1948 (ďalej len „ústava“).
([2]) Článok 37 ods. 2 ústavy.
([3]) Článok 37 ods. 2 ústavy.
([4]) Rozhodnutie Najvyššieho súdu Kórey č. 96DA42789, 24. júla 1998.
([5]) Rozhodnutie ústavného súdu č. 2002Hun-Ma51, 30. októbra 2003. Podobne v rozhodnutiach č. 99Hun-Ma513 a č. 2004Hun-Ma190 (konsolidované znenie) z 26. mája 2005 ústavný súd objasnil, že „*právo na riadenie vlastných osobných informácií je právo osoby, na ktorú sa informácie vzťahujú, na vlastné rozhodnutie o tom, kedy, komu alebo kým a v akom rozsahu budú jej informácie zverejnené alebo použité. Je to základné právo, hoci sa v ústave neuvádza, existujúce na ochranu osobnej slobody rozhodovania pred rizikom, ktoré predstavuje rozširovanie funkcií štátu a informačných a komunikačných technológií.*“
([6]) Článok 12 ods. 1, prvá veta ústavy.
([7]) Článok 16 a článok 12 ods. 3 ústavy.
([8]) Článok 12 ods. 3 ústavy.
([9]) Článok 6 ods. 2 ústavy.
([10]) Rozhodnutie ústavného súdu č. 93Hun-MA120, štvrtok 29. decembra 1994. Pozri napríklad aj rozhodnutie ústavného súdu č. 2014Hun-Ma346 (31. mája 2018), v ktorom súd rozhodol, že bolo porušené ústavné právo sudánskeho štátneho príslušníka, ktorý bol zadržaný na letisku, na pomoc právneho zástupcu. V inej veci ústavný súd rozhodol, že sloboda vybrať si legálne pracovisko úzko súvisí s právom usilovať sa o šťastný život, ako aj s ľudskou dôstojnosťou a hodnotou, a preto nie je vyhradená iba občanom, ale môže sa zaručiť aj cudzincom, ktorí v Kórejskej republike legálne pracujú (rozhodnutie ústavného súdu č. 2007Hun-Ma1083, 29. septembra 2011).

sú práva prináležiace každej ľudskej bytosti, nielen občanom ([11]). Súd takisto objasnil, že právo na riadenie svojich informácií sa považuje za základné právo zakotvené v práve na dôstojnosť a práve usilovať sa o šťastný život, ako aj v práve na súkromný život ([12]). Hoci sa v judikatúre dosiaľ nerozhodovalo konkrétne o práve cudzích štátnych príslušníkov na súkromie, právni vedci vo všeobecnosti uznávajú, že v článkoch 12 – 22 ústavy (ktoré sa týkajú práva na súkromie, ako aj osobnú slobodu) sa stanovujú *„práva ľudských bytostí“*.

A napokon sa v ústave takisto poskytuje právo na spravodlivú náhradu škody zo strany orgánov verejnej moci ([13]). Okrem toho môže na základe zákona o ústavnom súde každý človek, ktorého základné práva zaručené ústavou boli porušené pri výkone štátnej moci (s výnimkou rozsudkov súdov), podať ústavnú sťažnosť na ústavný súd ([14]).

1.2. **Všeobecné pravidlá ochrany údajov**

Všeobecný zákon o ochrane údajov v Kórejskej republike (ďalej len *„zákon o ochrane osobných informácií“*) sa uplatňuje na súkromný aj verejný sektor. Pokiaľ ide o orgány verejnej moci, v zákone o ochrane osobných informácií sa konkrétne odkazuje na povinnosť formulovať politiky na zabránenie *„zneužívaniu a nesprávnemu používaniu osobných informácií, nepovolenému sledovaniu atď. a na posilnenie dôstojnosti ľudských bytostí a súkromia jednotlivcov*.“ ([15])

Na spracúvanie osobných údajov na účely presadzovania práva sa vzťahujú požiadavky zákona o ochrane osobných informácií vo svojej celistvosti. Znamená to napríklad, že orgány na presadzovanie práva v trestných veciach musia plniť povinnosti týkajúce sa zákonného spracúvania, t. j. musia sa pri získavaní, používaní alebo poskytovaní osobných informácií opierať o niektorý z právnych základov uvedených v zákone o ochrane osobných informácií (články 15 – 18 zákona o ochrane osobných informácií), musia dodržiavať zásady obmedzenia účelu (článok 3 ods. 1 a 2 zákona o ochrane osobných informácií), primeranosti/minimalizácie údajov (článok 3 ods. 1 a 6 zákona o ochrane osobných informácií), obmedzeného uchovávania údajov (článok 21 zákona o ochrane osobných informácií), bezpečnosti údajov vrátane oznamovania porušenia ochrany údajov (článok 3 ods. 4, články 29 a 34 zákona o ochrane osobných informácií) a transparentnosti (článok 3 ods. 1 a 5, články 20, 30 a 32 zákona o ochrane osobných informácií). Na citlivé informácie sa uplatňujú osobitné záruky (článok 23 zákona o ochrane osobných údajov). Okrem toho môžu v súlade s článkom 3 ods. 5 a článkom 4 zákona o ochrane osobných informácií, ako aj článkami 35 až 39-2 zákona o ochrane osobných informácií jednotlivci uplatňovať vo vzťahu k orgánom presadzovania práva svoje práva na prístup, opravu, vymazanie a pozastavenie spracúvania svojich informácií.

Hoci sa teda zákon o ochrane osobných informácií plne uplatňuje na spracúvanie osobných údajov na účely presadzovania práva v trestných veciach, obsahuje výnimku týkajúcu sa spracúvania osobných údajov na účely národnej bezpečnosti. Podľa článku 58 ods. 1 pododseku 2 zákona o ochrane osobných informácií sa články 15 – 50 zákona o ochrane osobných informácií neuplatňujú na osobné informácie získané alebo vyžiadané na účely analýzy informácií súvisiacich s národnou bezpečnosťou ([16]). Naopak, kapitola I (Všeobecné ustanovenia), kapitola II (Zavedenie politík na ochranu osobných informácií atď.), kapitola VIII (Skupinové žaloby za porušenie ochrany údajov), kapitola IX (Doplňujúce ustanovenia) a kapitola X (Sankčné ustanovenia) zákona o ochrane osobných informácií sa uplatňujú aj naďalej. Platí to aj pre všeobecné zásady ochrany údajov stanovené v článku 3 (Zásady ochrany osobných informácií) a individuálne práva zaručené článkom 4 zákona o ochrane osobných informácií (Práva dotknutých osôb). Znamená to, že hlavné zásady a práva sa zaručujú aj v tejto oblasti. Okrem toho sa v článku 58 ods. 4 zákona o ochrane osobných informácií uvádza, že takéto informácie sa musia spracúvať v minimálnom rozsahu potrebnom na dosiahnutie zamýšľaného účelu a počas minimálneho obdobia; takisto sa vyžaduje, aby prevádzkovateľ osobných informácií zaviedol potrebné opatrenia na zaistenie bezpečného riadenia údajov a primeraného spracúvania, ako sú technické, riadiace a fyzické záruky, ako aj opatrenia na primerané vybavovanie individuálnych sťažností.

V oznámení č. 2021-1 s názvom Doplnkové pravidlá pre výklad a uplatňovanie zákona o ochrane osobných informácií Komisia pre ochranu osobných informácií ďalej objasnila, ako sa zákon o ochrane osobných informácií vzhľadom na túto čiastočnú výnimku uplatňuje na spracúvanie osobných údajov na účely národnej bezpečnosti ([17]). Týka sa konkrétne práv jednotlivcov (na prístup, opravu, pozastavenie spracúvania a vymazanie informácií) a dôvodov, ako aj možných obmedzení týkajúcich sa týchto práv. Podľa oznámenia sa pri uplatňovaní základných zásad, práv a povinností

([11]) Rozhodnutie ústavného súdu č. 99HeonMa494, 29. novembra 2001.
([12]) Pozri napríklad rozhodnutie ústavného súdu č. 99.
([13]) Článok 29 ods. 1 ústavy.
([14]) Článok 68 ods. 1 zákona o ústavnom súde.
([15]) Článok 5 ods. 1 zákona o ochrane osobných informácií.
([16]) Článok 58 ods. 1 pododsek 2 zákona o ochrane osobných informácií.
([17]) Oznámenie Komisie pre ochranu osobných informácií č. 2021-1 s názvom Doplnkové pravidlá pre výklad a uplatňovanie zákona o ochrane osobných informácií, oddiel III ods. 6.

zákona o ochrane osobných informácií na spracúvanie osobných údajov na účely národnej bezpečnosti prihliada na záruky uvedené v ústave, ktoré sa týkajú ochrany práva jednotlivca na riadenie svojich osobných informácií. Každé obmedzenie uvedeného práva, napríklad ak je to potrebné v záujme ochrany národnej bezpečnosti, si vyžaduje vyváženie práv a záujmov jednotlivca a príslušného verejného záujmu, pričom toto obmedzenie nesmie mať vplyv na podstatu uvedeného práva (článok 37 ods. 2 ústavy).

2. PRÍSTUP VLÁDY NA ÚČELY PRESADZOVANIA PRÁVA

2.1. Príslušné orgány verejnej moci v oblasti presadzovania práva

Polícia, prokuratúry a súdy môžu získavať osobné údaje na účely presadzovania práva v trestných veciach na základe zákona o trestnom konaní, zákona o ochrane súkromia komunikácie a zákona o telekomunikáciách. V rozsahu, v akom sa v zákone o Národnej spravodajskej službe udeľuje táto právomoc aj Národnej spravodajskej službe, musí aj ona dodržiavať uvedené zákony ([18]). A napokon sa v zákone o oznamovaní a používaní špecifikovaných informácií o finančných transakciách poskytuje právny základ, podľa ktorého môžu finančné inštitúcie sprístupňovať informácie Finančnej spravodajskej jednotke Kórey na účel predchádzania praniu špinavých peňazí a financovania terorizmu. Tento špecializovaný orgán môže potom tieto informácie poskytovať orgánom presadzovania práva. Tieto sprístupňovacie povinnosti sa však vzťahujú len na prevádzkovateľov, ktorí spracúvajú osobné úverové informácie podľa zákona o úverových informáciách a podliehajú dohľadu Komisie pre finančné služby. Keďže spracúvanie osobných úverových informácií týmito prevádzkovateľmi je vylúčené z rozsahu pôsobnosti rozhodnutia o primeranosti, obmedzenia a záruky, ktoré sa uplatňujú na základe zákona o oznamovaní a používaní špecifikovaných informácií o finančných transakciách, nie sú v tomto dokumente podrobnejšie opísané.

2.2. Právne základy a obmedzenia

Právne základy na získavanie osobných informácií na účely presadzovania zákona a platné obmedzenia a záruky sa stanovujú v zákone o trestnom konaní (pozri oddiel 2.2.1), zákone o ochrane súkromia komunikácie (pozri oddiel 2.2.2) a v zákone o telekomunikáciách (pozri oddiel 2.2.3).

2.2.1. *Prehliadky a zaistenia predmetov*

2.2.1.1. Právny základ

Prokurátori a vyšší príslušníci justičnej polície môžu vykonávať inšpekciu predmetov, prehľadávať osoby alebo zaisťovať predmety len vtedy, ak 1. je osoba podozrivá zo spáchania trestného činu (osoba podozrivá z trestnej činnosti); 2. je to potrebné na účely vyšetrovania a 3. sa predpokladá, že predmety podliehajúce inšpekcii, prehľadávané osoby a zaistené predmety majú súvis s prípadom ([19]). Podobne aj súdy môžu vykonávať prehliadky a zaisťovať predmety, ktoré sa majú použiť ako dôkazy alebo podliehajú konfiškácii, ak sa predpokladá, že tieto predmety alebo osoby majú súvis s konkrétnym prípadom ([20]).

2.2.1.2. Obmedzenia a záruky

Všeobecnou povinnosťou prokurátorov a príslušníkov justičnej polície je dodržiavanie ľudských práv osôb podozrivých z trestnej činnosti, ako aj ostatných dotknutých osôb ([21]). Okrem toho sa môžu povinné opatrenia na dosiahnutie účelu vyšetrovania prijímať len vtedy, ak sa výslovne uvádzajú v zákone o trestnom konaní, pričom sa môžu zavádzať len v minimálne potrebnom rozsahu ([22]).

Prehliadky, inšpekcie alebo zaistenia predmetov vykonávané príslušníkmi polície alebo prokurátormi v rámci vyšetrovania trestnej činnosti sa môžu vykonávať iba na základe súdneho príkazu ([23]). Orgán žiadajúci o súdny príkaz musí predložiť materiály preukazujúce dôvody podozrenia, že jednotlivec spáchal trestný čin, že prehliadka, inšpekcia alebo zaistenie predmetov je potrebné a že príslušné predmety, ktoré je potrebné zaistiť, existujú ([24]). V súdnom príkaze sa musí okrem ďalších náležitostí uvádzať meno osoby podozrivej z trestnej činnosti a trestný čin; miesto, osoba alebo predmety, ktorých prehliadku je potrebné vykonať, alebo predmety, ktoré je potrebné zaistiť; dátum vydania a obdobie jeho platnosti ([25]). Podobne platí, že ak sa ako súčasť prebiehajúceho súdneho konania prehliadky a zaistenia predmetov nevykonávajú v rámci verejného pojednávania, súdny príkaz sa musí získať vopred ([26]). Dotknutý jednotlivec a jeho obhajcovia sú vopred informovaní o prehliadke alebo zaistení predmetov a pri výkone súdneho príkazu môžu byť prítomní ([27]).

([18]) Pozri článok 3 zákona o Národnej spravodajskej službe (zákon č. 12948), v ktorom sa odkazuje na vyšetrovanie určitých trestných činov, akými sú povstanie, vzbura a trestné činy súvisiace s národnou bezpečnosťou (napr. špionáž). V tejto súvislosti sa uplatňujú postupy zákona o trestnom konaní týkajúce sa prehliadok a zaistenia predmetov, pričom v zákone o ochrane súkromia komunikácie sa upravuje získavanie údajov o komunikácii (pozri časť 3 o ustanoveniach týkajúcich sa prístupu ku komunikácii na účely národnej bezpečnosti).

([19]) Článok 215 ods. 1 a 2 zákona o trestnom konaní.

([20]) Článok 106 ods. 1, články 107 a 109 zákona o trestnom konaní.

([21]) Článok 198 ods. 2 zákona o trestnom konaní.

([22]) Článok 199 ods. 1 zákona o trestnom konaní.

([23]) Článok 215 ods. 1 a 2 zákona o trestnom konaní.

([24]) Článok 108 ods. 1 nariadenia o trestnom konaní.

([25]) Článok 114 ods. 1 zákona o trestnom konaní v spojení s článkom 219 zákona o trestnom konaní.

([26]) Článok 113 zákona o trestnom konaní.

([27]) Články 121 a 122 zákona o trestnom konaní.

Ak je predmetom prehliadky alebo zaistenia predmetov počítačový disk alebo iný nosič údajov, v zásade sa zaisťujú iba samotné údaje (skopírované alebo vytlačené), nie fyzický nosič ([28]). Samotný nosič údajov možno zaistiť iba vtedy, ak sa opodstatnene považuje za nemožné vytlačiť alebo skopírovať požadované údaje samostatne, prípadne ak sa opodstatnene považuje za nepraktické inak dosiahnuť účel prehliadky ([29]). Dotknutý jednotlivec musí byť o prehliadke bezodkladne informovaný ([30]). Na túto povinnosť oznamovania vyplývajúcu zo zákona o trestnom konaní sa nevzťahujú žiadne výnimky.

Prehliadky, kontroly a zaistenia predmetov bez súdneho príkazu sa môžu vykonávať len v určitých situáciách. Po prvé vtedy, ak nie je možné získať súdny príkaz z dôvodu naliehavosti na mieste trestného činu ([31]). Súdny príkaz sa však musí následne bezodkladne získať ([32]). Po druhé možno prehliadky a inšpekcie bez súdneho príkazu vykonávať na mieste, keď je osoba podozrivá z trestnej činnosti zatknutá alebo zadržaná ([33]). A napokon môže prokurátor alebo vyšší príslušník justičnej polície zaistiť predmet bez súdneho príkazu, keď sa ho osoba podozrivá z trestnej činnosti alebo tretia osoba zbavila, prípadne bol vydaný dobrovoľne ([34]).

Dôkazy, ktoré boli získané v rozpore so zákonom o trestnom konaní, sa budú považovať za neprípustné ([35]). Okrem toho sa v zákone o trestnom konaní stanovuje, že za nezákonné prehliadky osôb alebo miesta pobytu osoby, stráženej budovy, stavby, automobilu, lode, lietadla alebo prenajatej izby možno uložiť trest odňatia slobody v maximálnej dĺžke tri roky ([36]). Toto ustanovenie sa teda uplatňuje aj vtedy, ak sú predmety, ako napríklad nosiče údajov, zaistené pri nezákonnej prehliadke.

2.2.2. *Získavanie informácií o komunikácii*

2.2.2.1. Právny základ

Získavanie informácií o komunikácii sa upravuje v osobitnom zákone, ktorým je zákon o ochrane súkromia komunikácie. Konkrétne sa v zákone o ochrane súkromia komunikácie stanovuje zákaz cenzurovania akejkoľvek pošty, odpočúvania akejkoľvek telekomunikácie, poskytovania potvrdzujúcich údajov o komunikácii alebo nahrávanie, prípadne počúvanie, nezverejňovaných rozhovorov medzi osobami, ak sa to nevykonáva podľa zákona o trestnom konaní, zákona o ochrane súkromia komunikácie alebo zákona o vojenskom súde ([37]). Pojem „*komunikácia*“ v zmysle zákona o ochrane súkromia komunikácie zahŕňa poštu aj telekomunikácie ([38]). Vzhľadom na to sa v zákone o ochrane súkromia komunikácie rozlišuje medzi „*opatreniami na zachytenie komunikácie*“ ([39]) a získavaním „*potvrdzujúcich údajov o komunikácii*“.

Pojem „opatrenia na zachytenie komunikácie“ zahŕňa „*cenzúru*“, t. j. získavanie obsahu tradičnej pošty, ako aj „*odpočúvanie*“, t. j. priame zachytenie (získanie alebo nahratie) obsahu telekomunikácie ([40]). Pojem „potvrdzujúce údaje o komunikácii“ zahŕňa „*údaje o telekomunikačných záznamoch*“, ktoré obsahujú dátum telekomunikácie, čas jej začatia a ukončenia, počet odchádzajúcich a prichádzajúcich hovorov, ako aj číslo účastníka na druhej strane, frekventovanosť využívania, logy týkajúce sa používania telekomunikačných služieb a informácie o polohe (napr. z prenosových veží, ktoré prijímajú signály) ([41]).

([28]) Článok 106 ods. 3 zákona o trestnom konaní.
([29]) Článok 106 ods. 3 zákona o trestnom konaní.
([30]) Článok 219 zákona o trestnom konaní v spojení s článkom 106 ods. 4 zákona o trestnom konaní.
([31]) Článok 216 ods. 3 zákona o trestnom konaní.
([32]) Článok 216 ods. 3 zákona o trestnom konaní.
([33]) Článok 216 ods. 1 a 2 zákona o trestnom konaní.
([34]) Článok 218 zákona o trestnom konaní. Pokiaľ ide o osobné informácie, vzťahuje sa to len na dobrovoľné uvedenie samotnou dotknutou osobou, nie na prevádzkovateľa osobných informácií, ktorý je držiteľom takýchto informácií (čo by si vyžadovalo osobitný právny základ podľa zákona o ochrane osobných informácií). Dobrovoľne vydané predmety sa pripúšťajú ako dôkaz v súdnom konaní iba vtedy, ak neexistuje žiadna odôvodnená pochybnosť o dobrovoľnosti ich vydania, čo musí preukázať prokurátor. Pozri rozhodnutie najvyššieho súdu č. 2013Do11233, 10. marca 2016.
([35]) Článok 308-2 zákona o trestnom konaní.
([36]) Článok 321 zákona o trestnom konaní.
([37]) Článok 3 zákona o ochrane súkromia komunikácie. Zákonom o vojenskom súde sa v zásade upravuje získavanie informácií o vojenskom personále a na civilné obyvateľstvo ho možno uplatniť len v obmedzených prípadoch (napr. ak člen vojenského personálu a civilná osoba spáchajú trestný čin spoločne alebo ak jednotlivec spácha trestný čin na členovi vojenského personálu, možno začať konanie pred vojenským súdom, pozri článok 2 zákona o vojenskom súde). Všeobecné ustanovenia upravujúce prehliadky a zaistenia predmetov sú podobné ako v zákone o trestnom konaní, pozri napr. články 146 – 149 a články 153 – 156 zákona o vojenskom súde. Poštu napríklad možno získať len vtedy, ak je to potrebné na účely vyšetrovania a na základe príkazu vydaného vojenským súdom. Obmedzenia a záruky podľa zákona o ochrane súkromia komunikácie sa uplatňujú v rozsahu, v akom sa získava elektronická komunikácia.
([38]) Článok 2 ods. 1 zákona o ochrane súkromia komunikácie, t. j. „*prenos alebo prijímanie všetkých druhov zvukov, slov, symbolov alebo obrázkov prostredníctvom káblového, bezdrôtového, optického alebo iného elektromagnetického systému vrátane telefónu, e-mailu, predplatenej informačnej služby, telefaxu a rádiovej pagingovej služby*“.
([39]) Článok 2 ods. 7 a článok 3 ods. 2 zákona o ochrane súkromia komunikácie.
([40]) „Cenzúra“ sa vymedzuje ako „*otváranie pošty bez súhlasu dotknutej strany alebo získavanie poznatkov o jej obsahu, prípadne zaznamenávanie alebo zadržiavanie jej obsahu inými prostriedkami*“ (článok 2 ods. 6 zákona o ochrane súkromia komunikácie). „Odpočúvanie“ je „*získavanie alebo nahrávanie obsahu telekomunikácie počúvaním alebo sledovaním okolitých zvukov, slov, symbolov alebo obrázkov komunikácie prostredníctvom elektronických a mechanických zariadení bez súhlasu dotknutej strany alebo zachytávanie ňou prenášanej alebo prijímanej komunikácie*“ (článok 2 ods. 7 zákona o ochrane súkromia komunikácie).
([41]) Článok 2 ods. 11 zákona o ochrane súkromia komunikácie.

V zákone o ochrane súkromia komunikácie sa stanovujú obmedzenia a záruky týkajúce sa získavania oboch druhov údajov a nedodržanie niektorých z týchto požiadaviek podlieha trestným sankciám ([42]).

2.2.2.2. Obmedzenia a záruky uplatniteľné na získavanie obsahu komunikácie (opatrenia na zachytenie komunikácie)

Získavanie obsahu komunikácie sa môže vykonávať ako doplnkový prostriedok na uľahčenie vyšetrovania trestnej činnosti (t. j. ako posledná možnosť), pričom je potrebné usilovať sa o minimalizovanie zasahovania do komunikačného tajomstva ľudí ([43]). V súlade s touto všeobecnou zásadou sa môžu opatrenia na zachytenie komunikácie využívať len vtedy, ak je ťažké iným spôsobom zabrániť spáchaniu trestného činu, zatknúť páchateľa alebo získať dôkazy ([44]). Orgány presadzovania práva získavajúce obsah komunikácie musia toto získavanie okamžite ukončiť, ak sa už prístup ku komunikácii nepovažuje za potrebný, čím sa zaručí, že zasahovanie do súkromia komunikácie je čo najmenšie ([45]).

Okrem toho možno opatrenia na zachytenie komunikácie použiť len vtedy, ak existuje odôvodnené podozrenie, že sa plánuje spáchanie závažných trestných činov, páchajú sa alebo sa spáchali závažné trestné činy, ktoré sú výslovne uvedené v zákone o ochrane súkromia komunikácie. Ide o trestné činy ako povstanie, trestné činy súvisiace s drogami alebo trestné činy páchané pomocou výbušnín, ako aj trestné činy súvisiace s národnou bezpečnosťou, diplomatickými vzťahmi alebo vojenskými základňami a zariadeniami ([46]). Opatrenia na zachytenie komunikácie musia byť zacielené na konkrétnu poštu alebo telekomunikáciu odoslanú alebo prijatú podozrivou osobou, prípadne na poštu alebo telekomunikáciu odoslanú alebo prijatú podozrivou osobou v priebehu konkrétneho časového obdobia ([47]).

Aj vtedy, ak sú tieto požiadavky splnené, sa môže získavanie údajov o obsahu uskutočňovať len na základe súdneho príkazu. Konkrétne môže prokurátor požiadať súd o vydanie povolenia na získanie údajov o obsahu v súvislosti s podozrivou alebo vyšetrovanou osobou ([48]). Podobne môže aj príslušník justičnej polície požiadať o povolenie prokurátora, ktorý môže potom požiadať súd o vydanie príkazu ([49]). Žiadosť o vydanie súdneho príkazu musí byť podaná písomne a musí obsahovať konkrétne náležitosti. Musí sa v nej predovšetkým uvádzať 1. odôvodnené podozrenie, že sa plánuje, pácha alebo spáchal niektorý z trestných činov uvedených v zozname, ako aj všetky materiály dokladajúce podozrenie *fumus boni iuris*; 2. opatrenia na zachytenie komunikácie, ako aj ich cieľ, rozsah, zámer a obdobie uplatňovania; a 3. miesto, na ktorom by sa opatrenia vykonávali, a spôsob, akým by sa realizovali ([50]).

Po splnení právnych požiadaviek môže súd vydať písomné povolenie na vykonanie opatrení na zachytenie komunikácie v súvislosti s podozrivou alebo vyšetrovanou osobou ([51]). V tomto súdnom príkaze sa uvádzajú druhy opatrení, ako aj ich cieľ, rozsah, obdobie uplatňovania, miesto ich vykonávania a spôsob ich realizácie ([52]).

Opatrenia na zachytenie komunikácie sa môžu realizovať maximálne dva mesiace ([53]). Ak sa zámer opatrení v rámci tohto obdobia dosiahne skôr, opatrenia sa musia okamžite ukončiť. Naopak, ak sú požadované podmienky stále splnené, v lehote dvoch mesiacov je potrebné podať žiadosť o predĺženie obdobia uplatňovania opatrení na zachytenie komunikácie. Táto žiadosť musí obsahovať materiály dokladajúce fumus boni iuris na predĺženie platnosti opatrení ([54]). Predĺžené obdobie nesmie byť dlhšie ako jeden rok, prípadne tri roky v prípade určitých osobitne závažných trestných činov (napr. trestných činov súvisiacich s povstaním, zahraničnou agresiou, národnou bezpečnosťou atď.) ([55]).

Orgány presadzovania práva si môžu vynútiť spoluprácu prevádzkovateľov komunikačných služieb predložením písomného povolenia súdu ([56]). Prevádzkovatelia komunikačných služieb musia spolupracovať a uchovávať toto povolenie vo svojej evidencii ([57]). Spoluprácu môžu odmietnuť vtedy, ak sú informácie o zacielenej osobe uvedené v písomnom povolení súdu (napríklad telefónne číslo osoby) nesprávne. Okrem toho nesmú za žiadnych okolností sprístupniť heslá používané na telekomunikáciu ([58]).

([42]) Články 16 a 17 zákona o ochrane súkromia komunikácie. Uplatňujú sa napríklad v prípade získavania údajov bez súdneho príkazu či neuchovania záznamov, prípadne ak sa pokračuje v získavaní údajov aj po skončení mimoriadnej situácie alebo ak nie je dotknutý jednotlivec informovaný.
([43]) Článok 3 ods. 2 zákona o ochrane súkromia komunikácie.
([44]) Článok 5 ods. 1 zákona o ochrane súkromia komunikácie.
([45]) Článok 2 vykonávacieho dekrétu k zákonu o ochrane súkromia komunikácie.
([46]) Článok 5 ods. 1 zákona o ochrane súkromia komunikácie.
([47]) Článok 5 ods. 2 zákona o ochrane súkromia komunikácie.
([48]) Článok 6 ods. 1 zákona o ochrane súkromia komunikácie.
([49]) Článok 6 ods. 2 zákona o ochrane súkromia komunikácie.
([50]) Článok 6 ods. 4 zákona o ochrane súkromia komunikácie a článok 4 ods. 1 vykonávacieho dekrétu k zákonu o ochrane súkromia komunikácie.
([51]) Článok 6 ods. 5 a článok 6 ods. 8 zákona o ochrane súkromia komunikácie.
([52]) Článok 6 ods. 6 zákona o ochrane súkromia komunikácie.
([53]) Článok 6 ods. 7 zákona o ochrane súkromia komunikácie.
([54]) Článok 6 ods. 7 zákona o ochrane súkromia komunikácie.
([55]) Článok 6 ods. 8 zákona o ochrane súkromia komunikácie.
([56]) Článok 9 ods. 2 zákona o ochrane súkromia komunikácie.
([57]) Článok 15-2 zákona o ochrane súkromia komunikácie a článok 12 vykonávacieho dekrétu k zákonu o ochrane súkromia komunikácie.
([58]) Článok 9 ods. 4 zákona o ochrane súkromia komunikácie.

Každý, kto vykonáva opatrenia na zachytenie komunikácie alebo bol požiadaný o spoluprácu, musí uchovávať záznamy o zámeroch opatrení, ich vykonávaní, dátume poskytnutia spolupráce a cieli spolupráce ([59]). Záznamy musia uchovávať aj orgány presadzovania práva vykonávajúce opatrenia na zachytenie komunikácie, pričom sa v nich uvádzajú podrobnosti a dosiahnuté výsledky ([60]). Príslušníci justičnej polície musia tieto informácie poskytnúť vo forme správy prokurátorovi po uzavretí vyšetrovania ([61]).

Keď prokurátor vznesie obžalobu v prípade, v ktorom sa využili opatrenia na zachytenie komunikácie, alebo vykoná právny úkon, ktorým sa príslušný jednotlivec zbavuje obžaloby alebo zadržania (t. j. nejde len o pozastavenie trestného stíhania), prokurátor musí jednotlivcovi, ktorý podlieha opatreniam na zachytenie komunikácie, oznámiť skutočnosť, že sa vykonávali opatrenia na zachytenie komunikácie, pričom ho musí informovať aj o orgáne, ktorý ich vykonával, a o období ich uplatňovania. Toto oznámenie sa musí realizovať písomne do 30 dní od vykonania tohto právneho úkonu ([62]). Oznámenie možno odložiť, ak je pravdepodobné, že bude závažne ohrozená národná bezpečnosť alebo narušený verejný poriadok, prípadne ak je pravdepodobné, že bude mať za následok závažnú ujmu na životoch alebo fyzickej integrite ďalších osôb ([63]). Prokurátor alebo príslušník justičnej polície, ktorý zamýšľa oznámenie odložiť, musí získať súhlas vedúceho okresnej prokuratúry ([64]). Oznámenie sa musí realizovať v priebehu 30 dní od momentu, keď prestanú existovať dôvody na odloženie ([65]).

V zákone o ochrane súkromia komunikácie sa stanovuje aj osobitný postup získavania obsahu komunikácie v mimoriadnych situáciách. Konkrétne môžu orgány presadzovania práva získavať obsah komunikácie v prípade bezprostrednej hrozby plánovania alebo vykonania organizovanej trestnej činnosti alebo iného závažného trestného činu, ktorý môže priamo spôsobiť smrť alebo vážnu ujmu, pričom táto mimoriadna situácia bráni vykonaniu bežného postupu (ako už bol uvedený) ([66]). V takejto mimoriadnej situácii môže príslušník polície alebo prokurátor prijať opatrenia na zachytenie komunikácie bez predchádzajúceho povolenia súdu, ihneď po ich vykonaní však musí požiadať súd o vydanie povolenia. Ak orgán presadzovania práva nezíska povolenie súdu do 36 hodín od vykonania mimoriadnych opatrení, získavanie informácií sa musí okamžite zastaviť, pričom získané informácie sa musia ihneď nato zničiť ([67]). Príslušníci polície vykonávajú mimoriadne sledovanie pod dohľadom prokurátora, prípadne, ak nie je možné vopred získať pokyny prokurátora z dôvodu potreby naliehavo konať, musí polícia získať súhlas prokurátora ihneď po začatí sledovania ([68]). Uvedené pravidlá týkajúce sa oznamovania jednotlivcovi sa uplatňujú aj na získavanie obsahu komunikácie v mimoriadnych situáciách.

Získavanie informácií v mimoriadnych situáciách sa musí vždy vykonávať v súlade s „*vyhlásením o mimoriadnej cenzúre/odpočúvaní*“, pričom orgán, ktorý ho vykonáva, musí uchovávať záznamy o všetkých mimoriadnych opatreniach ([69]). K žiadosti o vydanie povolenia na vykonanie mimoriadnych opatrení podanej na súd musí byť okrem sprievodných dokumentov priložený aj písomný dokument, v ktorom sa uvádzajú potrebné opatrenia na zachytenie komunikácie, cieľ, predmet, rozsah, obdobie uplatňovania, miesto ich vykonávania, metóda a vysvetlenie, ako príslušné opatrenia na zachytenie komunikácie spĺňajú požiadavky článku 5 ods. 1 zákona o ochrane súkromia komunikácie ([70]).

Ak sa mimoriadne opatrenia ukončia v krátkom čase, čiže bez povolenia súdu (napr. ak je podozrivá osoba zatknutá ihneď po začatí zachytávania, ktoré sa tým ukončí), vedúci príslušnej prokuratúry predloží príslušnému súdu oznámenie o mimoriadnom opatrení ([71]). V oznámení sa musí uvádzať zámer, cieľ, rozsah, obdobie uplatňovania, miesto vykonávania a metóda získania informácií, ako aj dôvody nepodania žiadosti o vydanie súdneho povolenia ([72]). Na základe tohto oznámenia môže prijímajúci súd preskúmať zákonnosť získavania informácií, pričom toto oznámenie sa musí zaevidovať v registri oznámení o mimoriadnych opatreniach.

([59]) Článok 9 ods. 3 zákona o ochrane súkromia komunikácie.
([60]) Článok 18 ods. 1 vykonávacieho dekrétu k zákonu o ochrane súkromia komunikácie.
([61]) Článok 18 ods. 2 vykonávacieho dekrétu k zákonu o ochrane súkromia komunikácie.
([62]) Článok 9-2 ods. 1 zákona o ochrane súkromia komunikácie.
([63]) Článok 9-2 ods. 4 zákona o ochrane súkromia komunikácie.
([64]) Článok 9-2 ods. 5 zákona o ochrane súkromia komunikácie.
([65]) Článok 9-2 ods. 6 zákona o ochrane súkromia komunikácie.
([66]) Článok 8 ods. 1 zákona o ochrane súkromia komunikácie.
([67]) Článok 8 ods. 2 zákona o ochrane súkromia komunikácie.
([68]) Článok 8 ods. 3 zákona o ochrane súkromia komunikácie a článok 16 ods. 3 vykonávacieho dekrétu k zákonu o ochrane súkromia komunikácie.
([69]) Článok 8 ods. 4 zákona o ochrane súkromia komunikácie.
([70]) Čiže existuje odôvodnené podozrenie, že sa plánujú, páchajú alebo spáchali určité trestné činy, a je prakticky nemožné iným spôsobom zabrániť spáchaniu trestného činu, zatknúť páchateľa alebo získať dôkazy.
([71]) Článok 8 ods. 5 zákona o ochrane súkromia komunikácie.
([72]) Článok 8 ods. 6 až 7 zákona o ochrane súkromia komunikácie.

Všeobecne platí, že obsah komunikácie získaný vykonávaním opatrení na zachytenie komunikácie na základe zákona o ochrane súkromia komunikácie sa môže použiť iba na účely vyšetrovania, trestného stíhania alebo zabránenia konkrétnym uvedeným trestným činom, na účely disciplinárneho konania týkajúceho sa tých istých trestných činov, nároku na náhradu škody vzneseného stranou komunikácie alebo vtedy, ak to umožňujú iné zákony ([73]).

Pri získavaní telekomunikácie prenášanej cez internet sa uplatňujú osobitné záruky ([74]). Takéto informácie možno použiť len na účely vyšetrovania závažných trestných činov uvedených v článku 5 ods. 1 zákona o ochrane súkromia komunikácie. Na uchovanie informácií je potrebné získať súhlas súdu, ktorý povolil opatrenia na zachytenie komunikácie ([75]). Žiadosť o uchovávanie musí obsahovať informácie o opatreniach na zachytenie komunikácie, súhrn výsledkov opatrení, dôvody uchovávania (spoločne so sprievodnými materiálmi) a telekomunikáciu, ktorá sa má uchovať ([76]). Ak sa takáto žiadosť nepodá, získaná telekomunikácia sa musí do 14 dní od ukončenia opatrení na zachytenie komunikácie vymazať ([77]). Ak sa žiadosť zamietne, telekomunikácia sa musí do siedmich dní zničiť ([78]). V prípade vymazania telekomunikácie sa musí do siedmich dní predložiť súdu, ktorý povolil opatrenia na zachytenie komunikácie, správa obsahujúca dôvody na vymazanie, ako aj podrobnosti a čas o ňom.

Všeobecnejšie platí, že ak sa informácie získali nezákonne na základe opatrení na zachytenie komunikácie, nie sú pripustené ako dôkaz v súdnom alebo disciplinárnom konaní ([79]). V zákone o ochrane súkromia komunikácie sa takisto zakazuje každému, kto prijíma opatrenia na zachytenie komunikácie, sprístupňovať dôverné informácie získané v priebehu vykonávania týchto opatrení a využívať získané informácie na poškodenie dobrého mena osôb, na ktoré sa tieto opatrenia vzťahujú ([80]).

2.2.2.3. Obmedzenia a záruky uplatniteľné na získavanie potvrdzujúcich informácií o komunikácii

Na základe zákona o ochrane súkromia komunikácie môžu orgány presadzovania práva požiadať telekomunikačných operátorov o poskytnutie potvrdzujúcich údajov o komunikácii, ak je to potrebné na vedenie vyšetrovania alebo výkon trestu ([81]). Na rozdiel od získavania údajov o obsahu nie je možnosť získania potvrdzujúcich údajov o komunikácii obmedzená na určité špecifické trestné činy. Tak ako v prípade údajov o obsahu si však získanie potvrdzujúcich údajov o komunikácii vyžaduje predchádzajúce písomné povolenie súdu, na ktoré sa vzťahujú tie isté podmienky, ktoré už boli uvedené ([82]). Ak z naliehavých dôvodov nie je možné získať povolenie súdu, potvrdzujúce údaje o komunikácii možno získať aj bez súdneho príkazu. V takom prípade sa povolenie musí získať ihneď po vyžiadaní údajov, ktoré musí byť oznámené poskytovateľovi telekomunikačných služieb ([83]). Ak sa nezíska následné povolenie, získané informácie sa musia zničiť ([84]).

Prokurátori, príslušníci justičnej polície a súdy musia viesť záznamy o žiadostiach o potvrdzujúce údaje o komunikácii ([85]). Poskytovatelia telekomunikačných služieb musia okrem toho ministerstvu pre vedu a IKT dvakrát ročne podávať správu o sprístupnení potvrdzujúcich údajov o komunikácii a musia o tom uchovávať záznamy sedem rokov od dátumu sprístupnenia údajov ([86]).

Jednotlivci sú v zásade informovaní o skutočnosti, že sa získavajú potvrdzujúce údaje o komunikácii ([87]). To, kedy sú o tom informovaní, závisí od okolností vyšetrovania ([88]). Po prijatí rozhodnutia začať alebo nezačať trestné stíhanie sa musí táto skutočnosť oznámiť do 30 dní. Naopak, ak sa vznesenie žaloby pozastaví, táto skutočnosť sa musí oznámiť do 30 dní od uplynutia jedného roka od prijatia tohto rozhodnutia. V každom prípade sa musí oznámenie realizovať do 30 dní od uplynutia jedného roka po získaní informácií.

Oznámenie možno odložiť, ak je pravdepodobné, že 1. by bola ohrozená národná bezpečnosť, verejná bezpečnosť a poriadok; 2. by viedlo k smrti alebo fyzickej ujme; 3. by viedlo k ohrozeniu spravodlivého súdneho konania (napr. by

([73]) Článok 12 zákona o ochrane súkromia komunikácie.
([74]) Článok 12-2 zákona o ochrane súkromia komunikácie.
([75]) Prokurátor alebo príslušník polície vykonávajúci opatrenia na zachytenie komunikácie musí vybrať telekomunikáciu, ktorá sa má uchovať, do 14 dní od ukončenia opatrení a požiadať o súhlas súdu (príslušník polície podáva žiadosť prokurátorovi, ktorý ju zase podáva na súd), pozri článok 12-2 ods. 1 a 2 zákona o ochrane súkromia komunikácie.
([76]) Článok 12-2 ods. 3 zákona o ochrane súkromia komunikácie.
([77]) Článok 12-2 ods. 5 zákona o ochrane súkromia komunikácie.
([78]) Článok 12-2 ods. 5 zákona o ochrane súkromia komunikácie.
([79]) Článok 4 zákona o ochrane súkromia komunikácie.
([80]) Článok 11 ods. 2 vykonávacieho dekrétu k zákonu o ochrane súkromia komunikácie.
([81]) Článok 13 ods. 1 zákona o ochrane súkromia komunikácie.
([82]) Články 13 a 6 zákona o ochrane súkromia komunikácie.
([83]) Článok 13 ods. 2 zákona o ochrane súkromia komunikácie. Rovnako ako v prípade naliehavých opatrení na zachytenie komunikácie sa musí vypracovať dokument, v ktorom sa uvádzajú podrobnosti o prípade (podozrivá osoba, opatrenia, ktoré sa majú prijať, podozrenie zo spáchania trestného činu, ako aj naliehavosť situácie). Pozri článok 37 ods. 5 vykonávacieho dekrétu k zákonu o ochrane súkromia komunikácie.
([84]) Článok 13 ods. 3 zákona o ochrane súkromia komunikácie.
([85]) Článok 13 ods. 5 a 6 zákona o ochrane súkromia komunikácie.
([86]) Článok 13 ods. 7 zákona o ochrane súkromia komunikácie.
([87]) Pozri článok 13-3 ods. 7 v spojení s článkom 9-2 zákona o ochrane súkromia komunikácie.
([88]) Článok 13-3 ods. 1 zákona o ochrane súkromia komunikácie.

malo za následok zničenie dôkazov alebo zastrašovanie svedkov); alebo 4. by došlo k ohováraniu podozrivej osoby, obetí alebo iných osôb súvisiacich s prípadom alebo k narušeniu ich súkromia ([89]). Oznámenie niektorého z uvedených dôvodov si vyžaduje povolenie riaditeľa príslušnej okresnej prokuratúry ([90]). Oznámenie sa musí realizovať v priebehu 30 dní od momentu, keď prestanú existovať dôvody odloženia ([91]).

Informovaní jednotlivci môžu podať písomnú žiadosť prokurátorovi alebo príslušníkovi justičnej polície týkajúcu sa dôvodov získavania potvrdzujúcich údajov o komunikácii ([92]). V takom prípade musí prokurátor alebo príslušník justičnej polície písomne uviesť dôvody do 30 dní od prijatia žiadosti, ak nie je splnená niektorá z uvedených podmienok (výnimiek týkajúcich sa odloženia oznámenia) ([93]).

2.2.3. *Dobrovoľné sprístupnenie telekomunikačnými operátormi*

V článku 83 ods. 3 zákona o telekomunikáciách sa telekomunikačným operátorom umožňuje dobrovoľne vyhovieť žiadosti (podanej na účely vedenia trestného konania, vyšetrovania alebo výkonu trestu) súdu, prokurátora alebo vedúceho vyšetrovacieho orgánu o sprístupnenie *„údajov o komunikácii“*. Podľa zákona o telekomunikáciách sa pod *„údajmi o komunikácii“* rozumie meno, evidenčné číslo rezidenta, adresa a telefónne číslo používateľov, dátumy začatia využívania služieb alebo ukončenia využívania služieb používateľmi, ako aj identifikačné kódy používateľov (t. j. kódy používané na identifikovanie oprávneného používateľa počítačových systémov alebo komunikačných sietí) ([94]). Na účely zákona o telekomunikáciách sa za používateľov považujú iba jednotlivci, ktorí majú priamo uzavreté zmluvy na poskytovanie služieb s kórejským poskytovateľom telekomunikačných služieb ([95]). Preto by sa jednotlivci z EÚ, ktorých údaje boli prenesené do Kórejskej republiky, považovali za používateľov podľa zákona o telekomunikáciách len výnimočne, keďže zvyčajne by títo jednotlivci neuzatvorili priamu zmluvu s kórejským telekomunikačným operátorom.

Žiadosti o získanie údajov o komunikácii na základe zákona o telekomunikáciách sa musia podávať písomne a musia sa v nich uvádzať dôvody žiadosti, súvis s príslušným používateľom a rozsah požadovaných údajov ([96]). Ak nie je možné z dôvodov naliehavosti podať písomnú žiadosť, táto písomná žiadosť sa musí podať čo najskôr po uplynutí dôvodov naliehavosti ([97]). Telekomunikační operátori, ktorí vyhovejú žiadostiam o sprístupnenie údajov o komunikácii, musia uchovávať registre so záznamami o poskytnutých údajoch o komunikácii, ako aj súvisiace materiály, ako napríklad písomné žiadosti ([98]). Okrem toho musia telekomunikační operátori dvakrát ročne podávať ministerstvu pre vedu a IKT správy o poskytovaní údajov o komunikácii ([99]).

Telekomunikační operátori nemusia podľa zákona o telekomunikáciách vyhovieť žiadostiam o sprístupnenie údajov o komunikácii. Každú žiadosť musí preto operátor posúdiť z hľadiska platných požiadaviek na ochranu údajov vyplývajúcich zo zákona o ochrane osobných informácií. Konkrétne musí telekomunikačný operátor prihliadnuť na záujmy dotknutej osoby a nesmie sprístupniť informácie, ak je pravdepodobné, že by bol nespravodlivo poškodený záujem jednotlivca alebo tretej strany ([100]). Okrem toho musí byť dotknutý jednotlivec o sprístupnení informovaný podľa oznámenia č. 2021-1 s názvom Doplnkové pravidlá pre výklad a uplatňovanie zákona o ochrane osobných informácií. Vo výnimočných situáciách možno takéto oznámenie odložiť, a to najmä ak a dovtedy, kým by mohlo oznámenie ohrozovať prebiehajúce vyšetrovanie trestnej činnosti, alebo ak je pravdepodobné, že oznámenie spôsobí ohrozenie života alebo fyzickej integrity inej osoby, ak sú tieto práva a záujmy preukázateľne nadradené právam dotknutej osoby ([101]).

V roku 2016 najvyšší súd potvrdil, že dobrovoľné poskytovanie údajov o komunikácii telekomunikačnými operátormi bez súdneho príkazu na základe zákona o telekomunikáciách nie je ako také porušením práva na informačné sebaurčenie používateľa telekomunikačnej služby. Zároveň súd objasnil, že o porušenie by išlo vtedy, ak by bolo preukázateľne zjavné, že žiadajúci orgán podaním žiadosti o sprístupnenie údajov o komunikácii zneužil svoju právomoc, a tým porušil záujmy dotknutého jednotlivca alebo tretej strany ([102]). Vo všeobecnosti platí, že každá žiadosť o dobrovoľné sprístupnenie podaná orgánom presadzovania práva musí byť v súlade so zásadami zákonnosti, nevyhnutnosti a primeranosti, ktoré vyplývajú z kórejskej ústavy (článok 12 ods. 1 a článok 37 ods. 2).

([89]) Článok 13-3 ods. 2 zákona o ochrane súkromia komunikácie.
([90]) Článok 13-3 ods. 3 zákona o ochrane súkromia komunikácie.
([91]) Článok 13-3 ods. 4 zákona o ochrane súkromia komunikácie.
([92]) Článok 13-3 ods. 5 zákona o ochrane súkromia komunikácie.
([93]) Článok 13-3 ods. 6 zákona o ochrane súkromia komunikácie.
([94]) Článok 83 ods. 3 zákona o telekomunikáciách.
([95]) Článok 2 ods. 9 zákona o telekomunikáciách.
([96]) Článok 83 ods. 4 zákona o telekomunikáciách.
([97]) Článok 83 ods. 4 zákona o telekomunikáciách.
([98]) Článok 83 ods. 5 zákona o telekomunikáciách.
([99]) Článok 83 ods. 6 zákona o telekomunikáciách.
([100]) Článok 18 ods. 2 zákona o ochrane osobných informácií.
([101]) Oznámenie Komisie pre ochranu osobných informácií č. 2021-1 s názvom Doplnkové pravidlá pre výklad a uplatňovanie zákona o ochrane osobných informácií, oddiel III ods. 2 bod iii).
([102]) Rozhodnutie najvyššieho súdu č. 2012Da105482, 10. marca 2016.

2.3. **Dozor**

Dozor nad orgánmi presadzovania práva v trestných veciach vykonávajú prostredníctvom rôznych mechanizmov vnútorné aj vonkajšie orgány.

2.3.1. *Vnútorný audit*

V súlade so zákonom o auditoch verejného sektora sa orgány verejnej moci vyzývajú na zriadenie vnútorného orgánu na vykonávanie vnútorného auditu, ktorý bude mať okrem iného za úlohu vykonávať kontrolu zákonnosti ([103]). Vedúcim takýchto orgánov auditu musí byť zaručená najväčšia možná nezávislosť ([104]). Konkrétne ide o to, že sú menovaní mimo príslušného orgánu (napr. spomedzi bývalých sudcov, profesorov) na obdobie dvoch až piatich rokov a môžu byť odvolaní len z opodstatnených dôvodov (napr. keď nie sú schopní plniť si povinnosti z dôvodu duševnej poruchy alebo fyzického ochorenia alebo sa proti nim vedie disciplinárne konanie) ([105]). Podobne sú aj audítori menovaní na základe osobitných podmienok stanovených v zákone ([106]). Audítorské správy môžu obsahovať odporúčania alebo žiadosti o náhradu škody alebo nápravu, ako aj pokarhania a odporúčania alebo žiadosti o disciplinárne konanie ([107]). Oznamujú sa vedúcemu orgánu verejnej moci, ktorého audit sa vykonáva, ako aj Rade pre audit a inšpekciu (pozri oddiel 2.3.2) do 60 dní od ukončenia auditu ([108]). Dotknutý orgán musí vykonať požadované opatrenia a podať správu o výsledkoch Rade pre audit a inšpekciu ([109]). Okrem toho sú výsledky auditu všeobecne prístupné verejnosti ([110]). Odmietnutie auditu alebo bránenie v jeho vykonaní sa trestá správnymi pokutami ([111]). V oblasti presadzovania práva v trestných veciach má Národná policajná agentúra na účely dodržania uvedených právnych predpisov zavedený systém generálnej inšpekcie na vykonávanie vnútorných auditov, a to aj v súvislosti s možným porušovaním ľudských práv ([112]).

2.3.2. *Rada pre audit a inšpekciu*

Rada pre audit a inšpekciu môže vykonávať inšpekciu činností orgánov verejnej moci a na základe týchto inšpekcií vydávať odporúčania, žiadať o disciplinárne konania alebo podávať trestné oznámenia ([113]). Rada pre audit a inšpekciu je zriadená v rámci Úradu prezidenta Kórejskej republiky, pri vykonávaní svojich povinností má však nezávislé postavenie ([114]). Okrem toho sa v zákone, ktorým sa zriaďuje Rada pre audit a inšpekciu, vyžaduje, aby sa Rade pre audit a inšpekciu zabezpečila maximálna možná miera nezávislosti, pokiaľ ide o menovanie, prepúšťanie a organizáciu zamestnancov, ako aj zostavovanie rozpočtu ([115]). Predsedu Rady pre audit a inšpekciu menuje prezident so súhlasom národného zhromaždenia ([116]). Šiestich zostávajúcich komisárov menuje na štvorročné obdobie prezident na odporúčanie predsedu ([117]). Komisári (vrátane predsedu) musia mať špecifickú kvalifikáciu stanovenú zákonom ([118]) a môžu byť odvolaní len na základe konania o zbavení funkcie v rámci zákonodarnej moci, odsúdenia na trest odňatia slobody alebo neschopnosti vykonávať povinnosti z dôvodu dlhodobých problémov s duševným alebo fyzickým zdravím ([119]). Okrem toho sa komisárom zakazuje účasť na politických činnostiach a súbežné zastávanie funkcií v národnom zhromaždení, správnych orgánoch, organizáciách podliehajúcich auditu a inšpekcii vykonávaných Radou pre audit a inšpekciu, ako aj ďalších odmeňovaných funkcií a pozícií ([120]).

Rada pre audit a inšpekciu vykonáva každoročne generálny audit, môže však vykonávať aj osobitné audity týkajúce sa záležitostí osobitného významu. Rada pre audit a inšpekciu môže počas inšpekcie požiadať o predloženie dokumentov a takisto si môže vyžiadať prítomnosť jednotlivcov ([121]). V rámci auditu Rada pre audit a inšpekciu skúma príjmy

([103]) Články 3 a 5 zákona o auditoch verejného sektora.
([104]) Článok 7 zákona o auditoch verejného sektora.
([105]) Články 8 – 11 zákona o auditoch verejného sektora.
([106]) Článok 16 a nasl. zákona o auditoch verejného sektora.
([107]) Článok 23 ods. 2 zákona o auditoch verejného sektora.
([108]) Článok 23 ods. 1 zákona o auditoch verejného sektora.
([109]) Článok 23 ods. 3 zákona o auditoch verejného sektora.
([110]) Článok 26 zákona o auditoch verejného sektora.
([111]) Článok 41 zákona o auditoch verejného sektora.
([112]) Pozri konkrétne rozdelenie v rámci generálneho riaditeľstva pre audit a inšpekciu: https://www.police.go.kr/eng/knpa/org/org01.jsp.
([113]) Články 24 a 31 – 35 zákona o Rade pre audit a inšpekciu.
([114]) Článok 2 ods. 1 zákona o Rade pre audit a inšpekciu.
([115]) Článok 2 ods. 2 zákona o Rade pre audit a inšpekciu.
([116]) Článok 4 ods. 1 zákona o Rade pre audit a inšpekciu.
([117]) Článok 5 ods. 1 a článok 6 zákona o Rade pre audit a inšpekciu.
([118]) Napríklad aspoň desaťročná služba vo funkcii sudcu, prokurátora alebo advokáta, aspoň osemročná prax na pozícii zamestnanca verejnej správy alebo vysokoškolského profesora, prípadne na vyššej pozícii, alebo aspoň desaťročná prax v kótovanej spoločnosti alebo inštitúcií so štátnymi investíciami (z čoho aspoň päť rokov na výkonnej pozícii), pozri článok 7 zákona o Rade pre audit a inšpekciu.
([119]) Článok 8 zákona o Rade pre audit a inšpekciu.
([120]) Článok 9 zákona o Rade pre audit a inšpekciu.
([121]) Pozri napr. článok 27 zákona o Rade pre audit a inšpekciu.

a výdavky štátu, ale dozerá aj na všeobecné plnenie povinností orgánov verejnej moci a verejných činiteľov s cieľom zlepšiť fungovanie verejnej správy ([122]). Dozor, ktorý vykonáva, preto presahuje rozpočtové aspekty a týka sa aj kontroly zákonnosti.

2.3.3. *Národné zhromaždenie*

Národné zhromaždenie môže vyšetrovať orgány verejnej moci a vykonávať v nich inšpekciu ([123]). Počas vyšetrovania alebo inšpekcie si môže národné zhromaždenie vyžiadať sprístupnenie dokumentov a predvolať svedkov ([124]). Na každého, kto počas vyšetrovania vedeného národným zhromaždením podá krivú výpoveď, sa vzťahujú trestnoprávne sankcie (trest odňatia slobody až na desať rokov) ([125]). Proces a výsledky inšpekcií môžu byť zverejnené ([126]). Ak národné zhromaždenie zistí nezákonnú alebo nesprávnu činnosť, môže príslušný orgán verejnej moci požiadať o prijatie nápravných opatrení, ku ktorým môže patriť náhrada škody, disciplinárne konanie a zlepšenie jeho vnútorných postupov ([127]). Po prijatí tejto žiadosti musí orgán bezodkladne konať a o výsledku prijatých opatrení podať správu národnému zhromaždeniu ([128]).

2.3.4. *Komisia pre ochranu osobných informácií*

Komisia pre ochranu osobných informácií vykonáva dozor nad spracúvaním osobných informácií orgánmi presadzovania práva v trestných veciach v súlade so zákonom o osobných informáciách. Okrem toho sa podľa článku 7-8 ods. 3 a 4 a článku 7-9 ods. 5 zákona o ochrane osobných informácií dozor vykonávaný Komisiou pre ochranu osobných informácií týka aj možných porušení pravidiel, v ktorých sa stanovujú obmedzenia a záruky pri získavaní osobných informácií vrátane tých, ktoré sa uvádzajú v osobitných zákonoch upravujúcich získavanie (elektronických) dôkazov na účely presadzovania práva v trestných veciach (pozri oddiel 2.2). Vzhľadom na požiadavky článku 3 ods. 1 zákona o ochrane osobných informácií týkajúce sa získavania osobných informácií zákonným a spravodlivým spôsobom predstavuje každé takéto porušenie aj nedodržanie zákona o ochrane osobných informácií, preto môže Komisia pre ochranu osobných informácií uskutočňovať vyšetrovanie a prijímať nápravné opatrenia ([129]).

Pri vykonávaní funkcie dozoru má Komisia pre ochranu osobných informácií prístup k všetkým relevantným informáciám ([130]). Komisia pre ochranu osobných informácií môže poskytovať poradenstvo orgánom presadzovania práva s cieľom zlepšiť úroveň ochrany osobných informácií pri ich činnostiach spracúvania, ukladať nápravné opatrenia (napr. pozastaviť spracúvanie údajov alebo prijať potrebné opatrenia na ochranu osobných informácií) alebo konzultovať s orgánom podnet na disciplinárne konanie ([131]). A napokon sa za niektoré porušenia zákona o ochrane osobných informácií ukladajú trestnoprávne sankcie, ako napríklad za nezákonné využívanie alebo sprístupňovanie osobných informácií tretím stranám alebo spracúvanie citlivých informácií nezákonným spôsobom ([132]). V tejto súvislosti môže Komisia pre ochranu osobných informácií postúpiť vec príslušnému vyšetrovaciemu orgánu (vrátane prokuratúry) ([133]).

2.3.5. *Národná komisia pre ľudské práva*

Národná komisia pre ľudské práva – nezávislý orgán poverený ochranou a podporou základných práv ([134]) – má právomoc vyšetrovať a napravať porušenia článkov 10 – 22 ústavy, súčasťou ktorých je právo na súkromie a právo na súkromie korešpondencie. Národná komisia pre ľudské práva sa skladá z 11 komisárov menovaných na návrh národného zhromaždenia (štyria), prezidenta (štyria) a predsedu najvyššieho súdu (traja) ([135]). Za komisára možno vymenovať osobu, ktorá 1. aspoň desať rokov pôsobila na univerzite alebo v oprávnenom výskumnom ústave minimálne na pozícii docenta; 2. aspoň desať rokov pôsobila na pozícii sudcu, prokurátora alebo advokáta; 3. aspoň desať rokov sa venovala činnostiam v oblasti ľudských práv (napr. pre neziskovú, mimovládnu alebo medzinárodnú organizáciu); alebo 4. odporučili ju skupiny pôsobiace v rámci občianskej spoločnosti ([136]). Jej predsedu menuje prezident

([122]) Články 20 a 24 zákona o Rade pre audit a inšpekciu.
([123]) Článok 128 zákona o národnom zhromaždení a články 2, 3 a 15 zákona o inšpekcii a vyšetrovaní štátnej správy. Patria sem aj každoročné inšpekcie vládnych záležitostí ako takých a vyšetrovanie osobitných záležitostí.
([124]) Článok 10 ods. 1 zákona o inšpekcii a vyšetrovaní štátnej správy. Pozri aj články 128 a 129 zákona o národnom zhromaždení.
([125]) Článok 14 zákona o svedeckej výpovedi a znaleckom posudku pred národným zhromaždením.
([126]) Článok 12-2 zákona o inšpekcii a vyšetrovaní štátnej správy.
([127]) Článok 16 ods. 2 zákona o inšpekcii a vyšetrovaní štátnej správy.
([128]) Článok 16 ods. 3 zákona o inšpekcii a vyšetrovaní štátnej správy.
([129]) Pozri oznámenie Komisie pre ochranu osobných informácií č. 2021-1 s názvom Doplnkové pravidlá pre výklad a uplatňovanie zákona o ochrane osobných informácií.
([130]) Článok 63 zákona o ochrane osobných informácií.
([131]) Článok 61 ods. 2, článok 65 ods. 1, článok 65 ods. 2 a článok 64 ods. 4 zákona o ochrane osobných informácií.
([132]) Články 70 – 74 zákona o ochrane osobných informácií.
([133]) Článok 65 ods. 1 zákona o ochrane osobných informácií.
([134]) Článok 1 zákona o Národnej komisii pre ľudské práva.
([135]) Článok 5 ods. 1 a 2 zákona o Národnej komisii pre ľudské práva.
([136]) Článok 5 ods. 3 zákona o Národnej komisii pre ľudské práva.

spomedzi komisárov a musí ho potvrdiť národné zhromaždenie ([137]). Komisári (vrátane predsedu) sa menujú na obnoviteľné obdobie troch rokov a môžu byť odvolaní len v prípade odsúdenia na trest odňatia slobody alebo ak už nie sú schopní vykonávať svoje povinnosti z dôvodu dlhodobých problémov s duševným alebo fyzickým zdravím (v takom prípade musia s odvolaním súhlasiť dve tretiny komisárov) ([138]). Komisári Národnej komisie pre ľudské práva nesmú súčasne zastávať funkciu v národnom zhromaždení, obecných zastupiteľstvách ani v regionálnych štátnych správach a miestnych samosprávach (ako verejní činitelia) ([139]).

Národná komisia pre ľudské práva môže začať vyšetrovanie z vlastnej iniciatívy alebo na základe petície jednotlivca. V rámci vyšetrovania môže Národná komisia pre ľudské práva požiadať o predloženie príslušných materiálov, vykonávať inšpekcie a predvolávať jednotlivcov, aby podali svedeckú výpoveď ([140]). Po vyšetrovaní môže Národná komisia pre ľudské práva vydať odporúčania na zlepšenie alebo opravu konkrétnych politík a postupov a zverejniť ich ([141]). Orgány verejnej moci musia oznámiť Národnej komisii pre ľudské práva plán splnenia takýchto odporúčaní do 90 dní od ich prijatia ([142]). Okrem toho musí dotknutý orgán v prípade neplnenia odporúčaní informovať Komisiu ([143]). Národná komisia pre ľudské práva môže toto neplnenie odporúčaní oznámiť národnému zhromaždeniu a/alebo ho zverejniť. Orgány verejnej moci vo všeobecnosti plnia odporúčania Národnej komisie pre ľudské práva a majú silnú motiváciu tak robiť, keďže ich plnenie sa posudzuje v rámci všeobecného hodnotenia, ktoré vykonáva Kancelária pre koordináciu verejných politík pod vedením Úradu predsedu vlády.

2.4. **Individuálne prostriedky nápravy**

2.4.1. *Mechanizmy nápravy dostupné podľa zákona o ochrane osobných informácií*

Jednotlivci môžu pri spracúvaní osobných informácií orgánmi presadzovania práva v trestných veciach uplatňovať svoje práva na prístup, opravu, vymazanie a pozastavenie spracúvania svojich informácií podľa zákona o osobných informáciách. O prístup možno požiadať priamo príslušný orgán alebo nepriamo Komisiu pre ochranu osobných informácií. ([144]) Príslušný orgán môže obmedziť alebo zamietnuť prístup len v prípadoch uvedených v zákone, ak je pravdepodobné, že to spôsobí škodu na živote alebo fyzickej integrite tretej strany, prípadne neopodstatnené poškodenie majetku a iných záujmov tretej strany (t. j. ak by záujmy inej osoby prevažovali nad záujmami jednotlivca podávajúceho žiadosť) ([145]). Ak je žiadosť o prístup zamietnutá, jednotlivec musí byť informovaný o dôvodoch zamietnutia a možnosti odvolania ([146]). Podobne môže byť v prípadoch uvedených v zákone zamietnutá aj žiadosť o opravu alebo vymazanie, pričom jednotlivec musí byť informovaný o dôvodoch zamietnutia a možnosti odvolania ([147]).

Pokiaľ ide o nápravu, jednotlivci môžu podať sťažnosť Komisii pre ochranu osobných informácií, a to aj prostredníctvom call centra pre ochranu súkromia, ktoré prevádzkuje Kórejská agentúra pre internet a bezpečnosť ([148]). Okrem toho môže jednotlivec využiť mediáciu prostredníctvom Výboru pre mediáciu sporov týkajúcich sa osobných informácií ([149]). Tieto možnosti dosiahnutia nápravy sú dostupné v prípade možných porušení pravidiel konkrétnych zákonov, v ktorých sa stanovujú obmedzenia a záruky pri získavaní osobných informácií (oddiel 2.2), ako aj zákona o ochrane osobných informácií. Ďalej môžu jednotlivci podľa Správneho súdneho poriadku napadnúť rozhodnutia alebo nečinnosť Komisie pre ochranu osobných informácií (pozri oddiel 2.4.3).

([137]) Článok 5 ods. 5 zákona o Národnej komisii pre ľudské práva.
([138]) Článok 7 ods. 1 a článok 8 zákona o Národnej komisii pre ľudské práva.
([139]) Článok 10 zákona o Národnej komisii pre ľudské práva.
([140]) Článok 36 zákona o Národnej komisii pre ľudské práva. V súlade s článkom 36 ods. 7 zákona možno predloženie materiálov alebo predmetov zamietnuť, ak by sa tým mohla ohroziť dôvernosť štátneho tajomstva, čo by malo závažný vplyv na štátnu bezpečnosť alebo diplomatické vzťahy, alebo ak by to predstavovalo závažnú prekážku vo vyšetrovaní trestnej činnosti, prípadne v prebiehajúcom trestnom konaní. V takých prípadoch môže Komisia požiadať o ďalšie informácie vedúceho príslušného orgánu (ktorý musí žiadosti v dobrej viere vyhovieť), ak je to potrebné na preskúmanie toho, či bolo zamietnutie poskytnutia informácií opodstatnené.
([141]) Článok 25 ods. 1 zákona o Národnej komisii pre ľudské práva.
([142]) Článok 25 ods. 3 zákona o Národnej komisii pre ľudské práva.
([143]) Článok 25 ods. 4 zákona o Národnej komisii pre ľudské práva.
([144]) Článok 35 ods. 2 zákona o ochrane osobných informácií.
([145]) Článok 35 ods. 4 zákona o ochrane osobných informácií.
([146]) Článok 42 ods. 2 vykonávacieho dekrétu k zákonu o ochrane osobných informácií.
([147]) Článok 36 ods. 1 až 2 zákona o ochrane osobných informácií a článok 43 ods. 3 vykonávacieho dekrétu k zákonu o ochrane osobných informácií.
([148]) Článok 62 zákona o ochrane osobných informácií.
([149]) Články 40 – 50 zákona o ochrane osobných informácií a články 48-2 až 57 vykonávacieho dekrétu k zákonu o ochrane osobných informácií.

2.4.2. *Prostriedky nápravy pred Národnou komisiou pre ľudské práva*

Národná komisia pre ľudské práva vybavuje sťažnosti jednotlivcov (kórejských aj cudzích štátnych príslušníkov) týkajúce sa porušení ľudských práv, ktorých sa dopúšťajú orgány verejnej moci ([150]). Na podávanie sťažnosti Národnej komisii pre ľudské práva jednotlivcami sa nevzťahuje požiadavka na aktívnu legitimitu ([151]). V dôsledku toho bude sťažnosť vybavovať Národná komisia pre ľudské práva aj vtedy, ak dotknutý jednotlivec nedokáže vo fáze zisťovania prípustnosti preukázať faktickú ujmu. V súvislosti so získavaním osobných informácií na účely presadzovania práva v trestných veciach by preto jednotlivec nato, aby bola sťažnosť prípustná, nebol povinný preukazovať Národnej komisii pre ľudské práva že k jeho osobným informáciám získali faktický prístup kórejské orgány verejnej moci. Jednotlivec môže takisto žiadať o vybavenie sťažnosti prostredníctvom mediácie ([152]).

Pri vyšetrovaní sťažnosti môže Národná komisia pre ľudské práva využiť svoje vyšetrovacie právomoci, na základe ktorých môže okrem iného požiadať o príslušné materiály, vykonávať inšpekcie a predvolávať jednotlivcov, aby podali svedeckú výpoveď ([153]). Ak z vyšetrovania vyplynie, že došlo k porušeniu príslušných zákonov, Národná komisia pre ľudské práva môže odporučiť vykonanie nápravy alebo opravy, prípadne zlepšenie všetkých príslušných predpisov, inštitúcií, politík alebo postupov ([154]). Navrhovanými nápravnými opatreniami môžu byť mediácia, ukončenie porušovania ľudských práv, náhrada škody a opatrenia na zabránenie opakovaniu tých istých alebo podobných porušení ([155]). V prípade nezákonného získania osobných informácií podľa platných pravidiel môžu nápravné opatrenia zahŕňať vymazanie získaných osobných informácií. Ak sa považuje za vysoko pravdepodobné, že porušovanie pokračuje, a ak sa považuje za pravdepodobné, že ak sa neodstráni, spôsobí škodu, ktorú je ťažké napraviť, Národná komisia pre ľudské práva môže prijať naliehavé opatrenia na riešenie problému ([156]).

Národná komisia pre ľudské práva nemá donucovaciu právomoc, jej rozhodnutia (napr. rozhodnutie zastaviť vyšetrovanie sťažnosti) ([157]) a odporúčania možno napadnúť na kórejských súdoch na základe Správneho súdneho poriadku (pozri oddiel 2.4.3) ([158]). Okrem toho, ak zo zistení Národnej komisie pre ľudské práva vyplynie, že orgán verejnej moci získal osobné údaje nezákonným spôsobom, jednotlivec by sa mohol domáhať ďalšej nápravy na kórejských súdoch proti danému orgánu verejnej moci, napr. napadnutím získavania údajov podľa Správneho súdneho poriadku, podaním ústavnej sťažnosti podľa zákona o ústavnom súde alebo žiadosti o náhradu škody podľa zákona o štátnom odškodnení (pozri oddiel 2.4.3).

2.4.3. *Súdne prostriedky nápravy*

Jednotlivci môžu využiť obmedzenia a záruky opísané v predchádzajúcich oddieloch na dosiahnutie nápravy na kórejských súdoch rôznymi spôsobmi.

Po prvé môže byť dotknutý jednotlivec a jeho zástupca podľa zákona o trestnom konaní prítomný pri výkone súdneho príkazu na prehliadku alebo zaistenie predmetov, a teda môže vzniesť námietku v čase vykonávania súdneho príkazu ([159]). Okrem toho sa v zákone o trestnom konaní uvádza tzv. mechanizmus kvázisťažnosti, ktorý jednotlivcom umožňuje obrátiť sa na príslušný súd so žiadosťou o zrušenie alebo úpravu právneho úkonu prokurátora alebo príslušníka polície vykonávajúceho zaistenie predmetov ([160]). Jednotlivci tak môžu napadnúť opatrenia prijaté na vykonanie súdneho príkazu na zaistenie predmetov.

([150]) Hoci sa článok 4 zákona o Národnej komisii pre ľudské práva odvoláva na občanov a cudzincov s pobytom v Kórejskej republike, pojem „pobyt“ sa týka skôr jurisdikcie ako územia. Preto ak kórejské vnútroštátne inštitúcie porušili základné práva cudzinca, ktorý nie je štátnym príslušníkom Kórey, daný jednotlivec môže podať sťažnosť Národnej komisii pre ľudské práva. Pozri napríklad súvisiacu otázku na stránke Národnej komisie pre ľudské práva s často kladenými otázkami, ktorá je k dispozícii na adrese: https://www.humanrights.go.kr/site/program/board/basicboard/list?boardtypeid=7025&menuid=002004005001&pagesize=10&currentpage=2. Platí to v prípade, ak k osobným údajom cudzinca preneseným do Kórey získali nezákonný prístup kórejské orgány verejnej moci.

([151]) Sťažnosť sa musí v zásade podať do jedného roka od porušenia, Národná komisia pre ľudské práva však môže rozhodnúť aj o vyšetrení sťažnosti podanej po roku, ak neuplynula premlčacia lehota podľa trestného alebo občianskeho práva (článok 32 ods. 1 pododsek 4 zákona o Národnej komisii pre ľudské práva).

([152]) Článok 42 a nasl. zákona o Národnej komisii pre ľudské práva.

([153]) Články 36 a 37 zákona o Národnej komisii pre ľudské práva.

([154]) Článok 44 zákona o Národnej komisii pre ľudské práva.

([155]) Článok 42 ods. 4 zákona o Národnej komisii pre ľudské práva.

([156]) Článok 48 zákona o Národnej komisii pre ľudské práva.

([157]) Ak napríklad Národná komisia pre ľudské práva výnimočne nedokáže vykonať inšpekciu určitých materiálov alebo zariadení, pretože predstavujú štátne tajomstvo, ktoré môže mať závažný vplyv na štátnu bezpečnosť alebo diplomatické vzťahy, alebo ak by takáto inšpekcia predstavovala závažnú prekážku vo vyšetrovaní trestnej činnosti, prípadne v prebiehajúcom trestnom konaní (pozri poznámku pod čiarou č. 166), čo bráni Národnej komisii pre ľudské práva vykonať vyšetrovanie potrebné na posúdenie predmetu prijatej petície, v súlade s článkom 39 zákona o Národnej komisii pre ľudské práva informuje jednotlivca o dôvodoch, na základe ktorých sťažnosť zamietla. V takom prípade by jednotlivec mohol napadnúť rozhodnutie Národnej komisie pre ľudské práva podľa Správneho súdneho poriadku.

([158]) Pozri napr. rozhodnutie Najvyššieho soulského súdu č. 2007Nu27259, 18. apríla 2008, potvrdené rozhodnutím najvyššieho súdu č. 2008Du7854, 9. októbra 2008; rozhodnutie Najvyššieho soulského súdu č. 2017Nu69382 z 2. februára 2018.

([159]) Články 121 a 219 zákona o trestnom konaní.

([160]) Článok 417 zákona o trestnom konaní v spojení s článkom 414 ods. 2 zákona o trestnom konaní. Pozri aj rozhodnutie najvyššieho súdu č. 97Mo66 z 29. septembra 1997.

Okrem toho môžu jednotlivci na kórejských súdoch získať náhradu škody. Na základe zákona o štátnom odškodnení môžu jednotlivci žiadať o náhradu škody za škody spôsobené verejnými činiteľmi pri výkone ich oficiálnych povinností v rozpore so zákonom ([161]). Nárok možno podľa zákona o štátnom odškodnení podať špecializovanej Rade pre odškodnenie alebo priamo na kórejských súdoch ([162]). Ak je obeťou cudzí štátny príslušník, zákon o štátnom odškodnení sa naňho vzťahuje vtedy, ak jeho krajina pôvodu rovnako zabezpečuje štátne odškodnenie pre štátnych príslušníkov Kórey ([163]). Podľa judikatúry je táto podmienka splnená vtedy, ak požiadavky na podanie žiadosti o náhradu škody v druhej krajine „*nie sú medzi Kóreou a druhou krajinou výrazne nevyvážené*“ a „*vo všeobecnosti nie sú prísnejšie ako požiadavky v Kórei, pričom medzi nimi nie sú žiadne vecné ani podstatné rozdiely*.“ ([164]) Občianskym zákonníkom sa upravuje zodpovednosť štátu za náhradu škody a v dôsledku toho sa zodpovednosť štátu týka aj inej ako majetkovej škody (napr. duševného utrpenia) ([165]).

Za porušenie pravidiel ochrany údajov sa v zákone o ochrane osobných informácií poskytuje dodatočný právny prostriedok nápravy. Podľa článku 39 zákona o ochrane osobných informácií môže každý jednotlivec, ktorý utrpel škodu v dôsledku porušenia zákona o ochrane osobných údajov, prípadne stratu, odcudzenie, odhalenie, falšovanie, úpravu alebo poškodenie svojich osobných informácií, získať náhradu škody na súde. Zo zákona o štátnom odškodnení nevyplýva žiadna podobná požiadavka na reciprocitu.

Okrem náhrady škody možno dosiahnuť správny prostriedok nápravy za konanie alebo opomenutie správnych orgánov, a to podľa Správneho súdneho poriadku. Každý jednotlivec môže napadnúť právny úkon (t. j. výkon alebo zamietnutie výkonu verejnej moci v konkrétnom prípade) alebo opomenutie (dlhodobé nekonanie správneho orgánu pri prijímaní právneho úkonu, ktorý má zákonnú povinnosť prijať), čo môže viesť k zrušeniu/úprave nezákonného právneho úkonu, určeniu jeho neplatnosti (t. j. určeniu toho, že právny úkon nemá právny účinok alebo v právnom poriadku neexistuje) alebo nezákonnosti daného opomenutia ([166]). Napadnúť možno len taký správny úkon, ktorý má priamy vplyv na občianske práva a povinnosti ([167]). Môže ísť o opatrenia na získavanie osobných údajov, či už priame (napr. zachytávanie komunikácie), alebo prostredníctvom žiadosti o sprístupnenie informácií (napr. podanej poskytovateľovi služieb).

Uvedené nároky možno najskôr predložiť komisiám pre správne opravné prostriedky, ktoré sú zriadené v rámci niektorých orgánov verejnej moci (napr. Národná spravodajská služba, Národná komisia pre ľudské práva), alebo ústrednej komisii pre správne opravné prostriedky zriadenej v rámci Komisie pre občianske práva a boj proti korupcii ([168]). Takýto správny opravný prostriedok predstavuje alternatívny a neformálnejší spôsob napadnutia právneho úkonu alebo opomenutia orgánu verejnej moci. Nárok však možno predložiť aj priamo kórejským súdom, a to podľa Správneho súdneho poriadku.

Žiadosť o zrušenie/úpravu právneho úkonu podľa Správneho súdneho poriadku môže podať každá osoba, ktorá má právny záujem o zrušenie/úpravu alebo o obnovenie svojich práv na zrušenie/úpravu v prípade, ak už právny úkon nemá účinok ([169]). Podobne žalobu o potvrdenie neplatnosti môže podať osoba, ktorá má právny záujem o takého potvrdenie, zatiaľ čo žalobu o potvrdenie nezákonnosti opomenutia môže podať každá osoba, ktorá podala žiadosť o právny úkon a má právny záujem o potvrdenie nezákonnosti opomenutia ([170]). Podľa judikatúry najvyššieho súdu možno „právny záujem“ vykladať ako „právom chránený záujem“, t. j. priamy a osobitný záujem chránený zákonmi a právnymi predpismi, z ktorých vychádzajú správne úkony (t. j. nie ako všeobecný, nepriamy a abstraktný záujem verejnosti) ([171]). Jednotlivci majú preto právny záujem v prípade akéhokoľvek porušenia obmedzení a záruk v oblasti získavania ich osobných údajov na účely presadzovania práva v trestných veciach (podľa osobitných zákonov alebo zákona o ochrane osobných informácií). Rozsudok, ktorým sa konanie o veci končí, vydaný na základe Správneho súdneho poriadku je pre strany konania záväzný ([172]).

Žiadosť o zrušenie/úpravu právneho úkonu a žiadosť o potvrdenie nezákonnosti opomenutia sa musí podať do 90 dní odo dňa, keď sa jednotlivec dozvedel o právnom úkone/opomenutí, a v zásade najneskôr jeden rok odo dňa vydania

([161]) Článok 2 ods. 1 zákona o štátnom odškodnení.
([162]) Články 9 a 12 zákona o štátnom odškodnení. Zákonom sa zriaďujú okresné rady (ktorým predsedá zástupca prokurátora príslušnej prokuratúry), ústredná rada (ktorej predsedá námestník ministra spravodlivosti) a osobitná rada (ktorej predsedá námestník ministra národnej obrany a ktorá má na starosti nároky na náhradu škody za škody spôsobené vojenským personálom alebo civilnými zamestnancami armády). Nároky na náhradu škody v zásade vybavujú okresné rady, ktoré môžu za určitých okolností postúpiť prípady ústrednej/osobitnej rade, napr. ak náhrada škody presahuje určitú sumu alebo ide o žiadosť jednotlivca o opätovné preskúmanie. Všetky rady pozostávajú z členov menovaných ministrom spravodlivosti (napr. spomedzi verejných činiteľov ministerstva spravodlivosti, súdnych úradníkov, právnikov a osôb s odbornými znalosťami v oblasti štátneho odškodnenia) a vzťahujú sa na ne osobitné pravidlá v oblasti konfliktu záujmov (pozri článok 7 vykonávacieho dekrétu k zákonu o štátnom odškodnení).
([163]) Článok 7 zákona o štátnom odškodnení.
([164]) Rozhodnutie najvyššieho súdu č. 2013Da208388, štvrtok 11. júna 2015.
([165]) Pozri článok 8 zákona o štátnom odškodnení, ako aj článok 751 Občianskeho zákonníka.
([166]) Články 2 a 4 Správneho súdneho poriadku.
([167]) Rozhodnutie najvyššieho súdu č. 98Du18435, 22. októbra 1999, rozhodnutie najvyššieho súdu č. 99Du1113, 8. septembra 2000 a rozhodnutie najvyššieho súdu č. 2010Du3541, 27. septembra 2012.
([168]) Článok 6 zákona o správnych opravných prostriedkoch a článok 18 ods. 1 Správneho súdneho poriadku.
([169]) Článok 12 Správneho súdneho poriadku.
([170]) Články 35 a 36 Správneho súdneho poriadku.
([171]) Rozhodnutie najvyššieho súdu č. 2006Du330, štvrtok nedeľa 26. marca 2006.
([172]) Článok 30 ods. 1 Správneho súdneho poriadku.

právneho úkonu/výskytu opomenutia, ak tomu nebránia opodstatnené dôvody ([173]). Podľa judikatúry najvyššieho súdu sa má pojem „opodstatnené dôvody“ vykladať široko a vyžaduje si posúdenie toho, či je vzhľadom na okolnosti prípadu spoločensky prijateľné umožniť podanie oneskorenej sťažnosti ([174]). Patria k nim napríklad (nie však výhradne) dôvody oneskorenia, ktoré nezapríčinila dotknutá strana (t. j. situácie, na ktoré nemá sťažovateľ vplyv, ako napríklad, že nebol informovaný o získavaní svojich osobných údajov) alebo vyššia moc (napr. prírodná katastrofa, vojna).

A napokon môžu jednotlivci podať ústavnú sťažnosť na ústavný súd ([175]). Na základe zákona o ústavnom súde môže každý človek, ktorého základné práva zaručené ústavou boli porušené v dôsledku výkonu alebo nevykonania štátnej moci (s výnimkou rozsudkov súdov), žiadať o rozhodnutie o ústavnej sťažnosti. Ak sú k dispozícii iné nápravné prostriedky, musia sa využiť ako prvé. Podľa judikatúry ústavného súdu môžu cudzí štátni príslušníci podať ústavnú sťažnosť v rozsahu, v akom sa ich základné práva uznávajú podľa kórejskej ústavy (pozri vysvetlenia v oddiele 1.1) ([176]). Ústavné sťažnosti sa musia podať do 90 dní odo dňa, keď jednotlivec zistil porušenie, a do jedného roka od jeho výskytu. Vzhľadom na to, že postup podľa Správneho súdneho poriadku sa uplatňuje na žaloby podané podľa zákona o ústavnom súde ([177]), bude sťažnosť prípustná aj vtedy, ak existujú „opodstatnené dôvody“ podľa opísaného výkladu judikatúry najvyššieho súdu.

Ak je potrebné najskôr využiť ostatné prostriedky nápravy, ústavná sťažnosť sa musí podať do 30 dní od vydania konečného rozhodnutia o takomto prostriedku nápravy ([178]). Ústavný súd môže zrušiť platnosť výkonu štátnej moci, ktorý spôsobil porušenie, alebo potvrdiť, že určité nekonanie je protiústavné ([179]). V takom prípade musí príslušný orgán prijať opatrenia na vykonanie rozhodnutia súdu.

3. PRÍSTUP VLÁDY NA ÚČELY NÁRODNEJ BEZPEČNOSTI

3.1. Príslušné orgány verejnej moci v oblasti národnej bezpečnosti

Kórejská republika má dva špecializované spravodajské orgány: Národnú spravodajskú službu a Veliteľstvo pre podporu národnej obrany. Okrem nich môže osobné informácie na účely národnej bezpečnosti získavať aj polícia a prokuratúra.

Národná spravodajská služba bola zriadená zákonom o Národnej spravodajskej službe a pôsobí priamo v rámci právomoci a dohľadu prezidenta ([180]). Národná spravodajská služba konkrétne získava, zostavuje a distribuuje informácie o cudzích krajinách (a Severnej Kórei) ([181]), spravodajské informácie v súvislosti s úlohou kontrašpionáže (vrátane vojenskej a priemyselnej špionáže), terorizmom a činnosťami medzinárodných zločineckých syndikátov, spravodajské informácie o určitých druhoch trestnej činnosti namierenej proti verejnosti a národnej bezpečnosti (napr. domáce povstanie, zahraničná agresia), ako aj spravodajské informácie v súvislosti s úlohou zabezpečovania kybernetickej bezpečnosti a zabraňovania kybernetickým útokom a hrozbám alebo bojom proti nim ([182]). V zákone o Národnej spravodajskej službe, ktorým sa zriaďuje Národná spravodajská služba a v ktorom sa stanovujú jej úlohy, sa uvádzajú aj všeobecné zásady platné pre všetky jej činnosti. Vo všeobecnosti platí, že Národná spravodajská služba musí zachovávať politickú neutralitu a chrániť slobodu a práva jednotlivcov ([183]). Prezident Národnej spravodajskej služby je poverený vypracovaním všeobecných usmernení, v ktorých sa stanovujú zásady, rozsah a postupy plnenia povinností Národnej spravodajskej služby v súvislosti so získavaním a používaním informácií, ktoré musí oznamovať národnému zhromaždeniu ([184]). Národné zhromaždenie (prostredníctvom svojho Výboru pre spravodajskú činnosť) môže požiadať o opravu alebo doplnenie usmernení, ak sa domnieva, že sú nezákonné alebo nespravodlivé. Vo všeobecnosti platí, že riaditeľ a zamestnanci Národnej spravodajskej služby nesmú pri plnení svojich povinností prostredníctvom zneužitia svojich právomocí nútiť žiadnu inštitúciu, organizáciu ani jednotlivca do žiadnej činnosti, ktorú nemajú povinnosť vykonávať, ani nesmú nikomu brániť v uplatňovaní svojich práv ([185]). Okrem toho musí byť každá cenzúra pošty, zachytávanie telekomunikácie, získavanie informácií o polohe, získavanie potvrdzujúcich údajov o komunikácii alebo nahrávanie či odpočúvanie

([173]) Článok 20 Správneho súdneho poriadku. Lehota sa vzťahuje aj na nárok týkajúci sa potvrdenia nezákonnosti opomenutia, pozri článok 38 ods. 2 Správneho súdneho poriadku.
([174]) Rozhodnutie najvyššieho súdu č. 90Nu6521, 28. júna 1991.
([175]) Článok 68 ods. 1 zákona o ústavnom súde.
([176]) Rozhodnutie ústavného súdu č. 99HeonMa194, 29. novembra 2001.
([177]) Článok 40 zákona o ústavnom súde.
([178]) Článok 69 zákona o ústavnom súde.
([179]) Článok 75 ods. 3 zákona o ústavnom súde.
([180]) Článok 2 a článok 4 ods. 2 zákona o Národnej spravodajskej službe.
([181]) Táto koncepcia sa netýka informácií o jednotlivcoch, ale všeobecných informácií o cudzích krajinách (trendoch, vývoji) a o činnostiach štátnych subjektov tretích krajín.
([182]) Článok 3 ods. 1 zákona o Národnej spravodajskej službe.
([183]) Článok 3 ods. 1, článok 6 ods. 2, články 11, 21. Pozri aj pravidlá týkajúce sa konfliktov záujmov, najmä články 10 a 12.
([184]) Článok 4 ods. 2 zákona o Národnej spravodajskej službe.
([185]) Článok 13 zákona o Národnej spravodajskej službe.

súkromnej komunikácie vykonávané Národnou spravodajskou službou v súlade so zákonom o ochrane súkromia komunikácie, zákonom o informáciách o polohe a zákonom o trestnom konaní ([186]). Na každé zneužitie právomoci alebo získanie informácií v rozpore s týmito zákonmi sa vzťahujú trestnoprávne sankcie ([187]).

Veliteľstvo pre podporu národnej obrany je vojenský spravodajský orgán zriadený v rámci ministerstva obrany. Zodpovedá za bezpečnostné záležitosti armády, vojenské vyšetrovanie trestnej činnosti (na základe zákona o vojenskom súde) a vojenské spravodajstvo. Vo všeobecnosti Veliteľstvo pre podporu národnej obrany nevykonáva sledovanie civilného obyvateľstva, ak to nie je potrebné na výkon jeho vojenských funkcií. Môže vyšetrovať vojenský personál, civilných zamestnancov armády, osoby absolvujúce vojenskú odbornú prípravu, príslušníkov v zálohe, brancov a vojnových zajatcov ([188]). Pri získavaní informácií o komunikácii na účely národnej bezpečnosti sa na Veliteľstvo pre podporu národnej obrany vzťahujú obmedzenia a záruky stanovené v zákone o ochrane súkromia komunikácie a v jeho vykonávacom dekréte.

3.2. **Právne základy a obmedzenia**

Právne základy pre získavanie osobných informácií na účely národnej bezpečnosti poskytujú zákon o ochrane súkromia komunikácie, zákon o boji proti terorizmu na ochranu občanov a verejnej bezpečnosti (ďalej len „*zákon o boji proti terorizmu*“) a zákon o telekomunikáciách, v ktorých sa stanovujú platné obmedzenia a záruky ([189]). Tieto obmedzenia a záruky, ktoré sú opísané v nasledujúcich oddieloch, zabezpečujú obmedzenie získavania a spracúvania informácií len na rozsah potrebný na dosiahnutie oprávneného zámeru. Tým je vylúčené akékoľvek plošné a nerozlišujúce získavanie osobných informácií na účely národnej bezpečnosti.

3.2.1. *Získavanie informácií o komunikácii*

3.2.1.1. Získavanie informácií o komunikácii spravodajskými orgánmi

3.2.1.1.1. Právny základ

V zákone o ochrane súkromia komunikácie sa spravodajským orgánom poskytujú právomoci na získavanie údajov o komunikácii a vyžaduje sa, aby poskytovatelia komunikačných služieb spolupracovali pri vybavovaní žiadostí týchto orgánov ([190]). Ako sa uvádza v oddiele 2.2.2.1, v zákone o ochrane súkromia komunikácie sa rozlišuje medzi získavaním obsahu komunikácie (t. j. „*opatreniami na zachytenie komunikácie*“, ako sú opatrenia „*odpočúvania*“ alebo „*cenzúry*“ ([191])) a získavaním „*potvrdzujúcich údajov o komunikácii*“ ([192]).

Prahová hodnota pre získavanie týchto dvoch druhov informácií sa líši, ale uplatniteľné postupy a záruky sú do veľkej miery rovnaké ([193]). Získavanie potvrdzujúcich údajov o komunikácii (alebo metaúdajov) sa môže vykonávať na účel predchádzania hrozbám pre národnú bezpečnosť ([194]). Vyššia prahová hodnota sa uplatňuje na vykonávanie opatrení na zachytenie komunikácie (t. j. na získavanie obsahu komunikácie), pričom tieto opatrenia možno vykonať len vtedy, ak sa očakáva, že dôjde k vážnemu ohrozeniu národnej bezpečnosti a získanie spravodajských informácií je potrebné na to, aby sa mu predišlo (t. j. ak existuje vážne riziko pre národnú bezpečnosť a získanie informácií je potrebné na to, aby sa mu predišlo) ([195]). Okrem toho môže byť prístup k obsahu komunikácie povolený ako posledná možnosť na zaistenie národnej bezpečnosti, pričom je potrebné minimalizovať porušovanie súkromia komunikácie ([196]). Aj vtedy, ak sa získa príslušný súhlas/povolenie, je potrebné takéto opatrenia bezodkladne ukončiť, keď už nie sú potrebné, a tým zabezpečiť čo najmenšie obmedzenie porušovania komunikačného tajomstva jednotlivcov ([197]).

3.2.1.1.2. Obmedzenia a záruky uplatňujúce sa na získavanie informácií o komunikácii, ktoré sa týka aspoň jedného kórejského štátneho príslušníka

Získavanie informácií o komunikácii (obsahu aj metaúdajov), v ktorej sú jeden alebo obaja účastníci komunikácie kórejskými štátnymi príslušníkmi, sa môže uskutočňovať iba s povolením predsedu najvyššieho

([186]) Článok 14 zákona o Národnej spravodajskej službe.
([187]) Články 22 a 23 zákona o Národnej spravodajskej službe.
([188]) Článok 1 zákona o vojenskom súde.
([189]) Pri vyšetrovaní trestnej činnosti súvisiacej s národnou bezpečnosťou budú polícia a Národná spravodajská služba konať podľa zákona o trestnom konaní, pričom na Veliteľstvo pre podporu národnej obrany sa vzťahuje zákon o vojenskom súde.
([190]) Článok 15-2 zákona o ochrane súkromia komunikácie.
([191]) Článok 2 ods. 6 a 7 zákona o ochrane súkromia komunikácie.
([192]) Článok 2 ods. 11 zákona o ochrane súkromia komunikácie.
([193]) Pozri aj článok 13-4 ods. 2 zákona o ochrane súkromia komunikácie a článok 37 ods. 4 vykonávacieho dekrétu k zákonu o ochrane súkromia komunikácie, v ktorých sa stanovuje, že postupy uplatniteľné na získavanie obsahu komunikácie sa uplatňujú mutatis mutandis na získavanie potvrdzujúcich údajov o komunikácii.
([194]) Článok 13-4 zákona o ochrane súkromia komunikácie.
([195]) Článok 7 ods. 1 zákona o ochrane súkromia komunikácie.
([196]) Článok 3 ods. 2 zákona o ochrane súkromia komunikácie.
([197]) Článok 2 vykonávacieho dekrétu k zákonu o ochrane súkromia komunikácie.

súdu ([198]). Žiadosť spravodajského orgánu musí byť podaná písomne prokurátorovi alebo generálnej prokuratúre ([199]). Musia sa v nej uvádzať dôvody získavania informácií (t. j. že sa očakáva, že dôjde k vážnemu ohrozeniu národnej bezpečnosti, alebo že získanie informácií je potrebné na zabránenie hrozbám pre národnú bezpečnosť) vrátane materiálov, ktorými sa dokladajú dôvody a fumus boni iuris, ako aj podrobnosti žiadosti (t. j. zámery, jednotlivci, na ktorých je zacielená, rozsah, obdobie získavania informácií, ako aj spôsob a miesto získavania informácií) ([200]). Prokurátor/generálna prokuratúra potom požiadajú o vydanie povolenia predsedu najvyššieho súdu ([201]). Predseda môže udeliť písomné povolenie len vtedy, ak sa domnieva, že žiadosť je opodstatnená, pričom žiadosť zamietne, ak ju považuje za neopodstatnenú ([202]). V súdnom príkaze sa uvádza druh, zámer, cieľ, rozsah a obdobie získavania informácií, ako aj miesto a spôsob jeho vykonávania ([203]).

V prípade, ak je opatrenie zamerané na vyšetrovanie sprisahania, ktoré ohrozuje národnú bezpečnosť, pričom existuje mimoriadna situácia, ktorá bráni dodržaniu uvedených postupov, sa uplatňujú osobitné pravidlá ([204]). Po splnení týchto podmienok môžu spravodajské orgány vykonávať opatrenia sledovania bez predchádzajúceho súhlasu súdu ([205]). Ihneď po vykonaní mimoriadnych opatrení však musí spravodajský orgán súd o povolenie požiadať. Ak sa povolenie nezíska do 36 hodín od prijatia opatrení, musia sa okamžite ukončiť ([206]). Získavanie informácií v mimoriadnych situáciách sa musí vždy vykonávať v súlade s „vyhlásením o mimoriadnej cenzúre/odpočúvaní“, pričom spravodajský orgán, ktorý ho vykonáva, musí uchovávať záznamy o všetkých mimoriadnych opatreniach ([207]).

Ak sa sledovanie ukončí v krátkom čase bez povolenia súdu, vedúci príslušnej generálnej prokuratúry musí zaslať oznámenie o mimoriadnom opatrení, ktoré vypracoval spravodajský orgán, vedúcemu príslušného súdu, ktorý vedie register mimoriadnych opatrení ([208]). Súdu to umožní preskúmať zákonnosť získavania informácií.

3.2.1.1.3. Obmedzenia a záruky uplatňujúce sa na získavanie informácií o komunikácii, ktoré sa týka výlučne cudzích štátnych príslušníkov

Na získanie informácií o komunikácii výlučne medzi cudzími štátnymi príslušníkmi musia spravodajské orgány získať predchádzajúci písomný súhlas prezidenta ([209]). Takáto komunikácia sa bude získavať len na účely národnej bezpečnosti, ak patrí do niektorej z uvedených kategórií, t. j. ide o komunikáciu medzi vládnymi úradníkmi alebo inými jednotlivcami z krajín s nepriateľským postojom ku Kórejskej republike, cudzími orgánmi, skupinami alebo štátnymi príslušníkmi podozrivými z protikórejskej činnosti ([210]), alebo členmi skupín z Kórejského polostrova mimo suverenity Kórejskej republiky a ich zastrešujúcimi skupinami so sídlom v cudzích krajinách ([211]). Naopak platí, že ak je jedna strana komunikácie kórejským štátnym príslušníkom a druhá strana komunikácie cudzím štátnym príslušníkom, vyžaduje sa súhlas súdu na základe postupu uvedeného v oddiele 3.2.1.1.2.

Vedúci spravodajského orgánu musí predložiť plán opatrení, ktoré má prijať riaditeľ Národnej spravodajskej služby ([212]). Riaditeľ Národnej spravodajskej služby preskúma, či je plán primeraný, a ak áno, predloží ho na schválenie prezidentovi ([213]). Plán musí obsahovať informácie, ktoré sa vyžadujú na uplatňovanie povolenia súdu na získavanie informácií o kórejských štátnych príslušníkoch (ako už boli uvedené) ([214]). Konkrétne sa v ňom musia uvádzať dôvody získavania informácií (t. j. že sa očakáva, že dôjde k vážnemu ohrozeniu národnej bezpečnosti, alebo že získanie

([198]) Článok 7 ods. 1 pododsek 1 zákona o ochrane súkromia komunikácie. Príslušným súdom je najvyšší súd s právomocou pre miesto bydliska alebo sídlo niektorej zo strán, na ktorú sa vzťahuje sledovanie.
([199]) Článok 7 ods. 3 vykonávacieho dekrétu k zákonu o ochrane súkromia komunikácie.
([200]) Článok 7 ods. 3 a článok 6 ods. 4 zákona o ochrane súkromia komunikácie.
([201]) Článok 7 ods. 4 vykonávacieho dekrétu k zákonu o ochrane súkromia komunikácie. V žiadosti prokurátora adresovanej súdu sa musia uvádzať hlavné dôvody podozrenia a v rozsahu, v akom sa zároveň žiada o viacero povolení, aj ich opodstatnenie (pozri článok 4 vykonávacieho dekrétu k zákonu o ochrane súkromia komunikácie).
([202]) Článok 7 ods. 3, článok 6 ods. 5 a článok 6 ods. 9 zákona o ochrane súkromia komunikácie.
([203]) Článok 7 ods. 3 a článok 6 ods. 6 zákona o ochrane súkromia komunikácie.
([204]) Článok 8 zákona o ochrane súkromia komunikácie.
([205]) Článok 8 ods. 1 zákona o ochrane súkromia komunikácie.
([206]) Článok 8 ods. 2 zákona o ochrane súkromia komunikácie.
([207]) Článok 8 ods. 4 zákona o ochrane súkromia komunikácie. Informácie o mimoriadnych opatreniach v súvislosti s presadzovaním práva sa uvádzajú v oddiele 2.2.2.2.
([208]) Článok 8 ods. 5 a 7 zákona o ochrane súkromia komunikácie. V tomto oznámení sa musí uvádzať zámer, cieľ, rozsah, obdobie uplatňovania, miesto vykonávania a metóda sledovania, ako aj dôvody nepodania žiadosti pred prijatím opatrenia (článok 8 ods. 6 zákona o ochrane súkromia komunikácie).
([209]) Článok 7 ods. 1 pododsek 2 zákona o ochrane súkromia komunikácie.
([210]) Ide o činnosti ohrozujúce existenciu a bezpečnosť národa, demokratické usporiadanie štátu alebo prežitie a slobodu ľudí.
([211]) Okrem toho, ak je jednou zo strán osoba opísaná v článku 7 ods. 1 pododseku 2 zákona o ochrane súkromia komunikácie a druhá strana je neznáma alebo ju nemožno určiť, uplatňuje sa postup stanovený v článku 7 ods. 1 pododseku 2.
([212]) Článok 8 ods. 1 vykonávacieho dekrétu k zákonu o ochrane súkromia komunikácie. Riaditeľa Národnej spravodajskej služby menuje prezident po potvrdení parlamentom (článok 7 zákona o Národnej spravodajskej službe).
([213]) Článok 8 ods. 2 vykonávacieho dekrétu k zákonu o ochrane súkromia komunikácie.
([214]) Článok 8 ods. 3 vykonávacieho dekrétu k zákonu o ochrane súkromia komunikácie v spojení s článkom 6 ods. 4 zákona o ochrane súkromia komunikácie.

informácií je potrebné na zabránenie hrozbám pre národnú bezpečnosť), hlavné dôvody podozrenia vrátane materiálov, ktorými sa dokladajú dôvody a *fumus boni iuris*, ako aj podrobnosti žiadosti (t. j. zámery, jednotlivci, na ktorých je zacielená, rozsah, obdobie získavania informácií, ako aj spôsob a miesto získavania informácií). Ak sa naraz žiada o viacero povolení, uvádza sa účel a dôvody všetkých z nich ([215]).

Za mimoriadnych okolností ([216]) sa musí získať predchádzajúci súhlas ministra, do ktorého právomoci príslušný spravodajský orgán patrí. V takom prípade si však musí spravodajský orgán vyžiadať súhlas prezidenta ihneď po prijatí mimoriadnych opatrení. Ak spravodajský orgán nezíska súhlas do 36 hodín od podania žiadosti, získavanie údajov sa musí ihneď ukončiť ([217]). V takých prípadoch sa získané informácie vždy zničia.

3.2.1.1.4. Všeobecné obmedzenia a záruky

Ak spravodajské orgány žiadajú o spoluprácu súkromné subjekty, musia im predložiť súdny príkaz/povolenie prezidenta alebo kópiu titulného listu vyhlásenia o mimoriadnej cenzúre, ktorú musí dožiadaný subjekt uchovávať vo svojej evidencii ([218]). Subjekty, ktorým bola adresovaná žiadosť o sprístupnenie informácií spravodajským orgánom na základe zákona o ochrane súkromia komunikácie, môžu túto žiadosť odmietnuť, ak sa v povolení alebo vyhlásení o mimoriadnej cenzúre uvádza nesprávny identifikátor (napr. telefónne číslo patriace inému jednotlivcovi ako identifikovanému). Okrem toho sa v žiadnom prípade nesmú sprístupniť heslá používané na komunikáciu ([219]).

Spravodajské orgány môžu poveriť vykonaním opatrení na zachytenie komunikácie alebo získavaním potvrdzujúcich informácií o komunikácii poštu alebo poskytovateľa telekomunikačných služieb (ako sa vymedzuje v zákone o telekomunikáciách) ([220]). Príslušný spravodajský orgán, ako aj poskytovateľ, ktorý prijal žiadosť o spoluprácu, musia vo svojej evidencii uchovávať informácie o účele žiadostí o opatrenia, dátume vykonania opatrení alebo poskytnutia spolupráce a predmetoch opatrení (napr. pošta, telefón, e-mail) tri roky ([221]). Poskytovatelia telekomunikačných služieb poskytujúci potvrdzujúce údaje o komunikácii musia uchovávať informácie o frekvencii získavania vo svojej evidencii sedem rokov a dvakrát ročne musia podávať správy ministerstvu pre vedu a IKT ([222]).

Spravodajské orgány musia podávať správy o informáciách, ktoré získali, a o výsledkoch činnosti sledovania riaditeľovi Národnej spravodajskej služby ([223]). Pri získavaní potvrdzujúcich údajov o komunikácii sa musia uchovávať záznamy o predložení žiadosti o takéto údaje, ako aj samotná písomná žiadosť a informácie o inštitúcii, ktorá ich využívala ([224]).

Získavanie obsahu komunikácie a potvrdzujúcich údajov o komunikácii môže trvať maximálne štyri mesiace a ak sa počas tohto obdobia dosiahne sledovaný cieľ, musí sa okamžite ukončiť ([225]). Ak podmienky povolenia pretrvávajú, toto obdobie možno predĺžiť o ďalšie štyri mesiace na základe povolenia súdu alebo súhlasu prezidenta. Žiadosť o súhlas s predĺžením opatrení sledovania musí byť podaná písomne a spoločne so sprievodnými materiálmi musí obsahovať dôvody, na základe ktorých sa žiada o predĺženie ([226]).

V závislosti od právneho základu získavania informácií sú jednotlivci vo všeobecnosti informovaní o získavaní svojej komunikácie. Konkrétne platí, že bez ohľadu na to, či sa získavané informácie týkajú obsahu komunikácie alebo potvrdzujúcich údajov o komunikácii, a bez ohľadu na to, či sa informácie získavajú bežným postupom alebo za mimoriadnych okolností, musí vedúci spravodajského orgánu písomne oznámiť dotknutému jednotlivcovi opatrenie sledovania do 30 dní od dátumu ukončenia sledovania ([227]). Oznámenie musí obsahovať 1. skutočnosť, že sa získavali

([215]) Článok 8 ods. 3 a článok 4 vykonávacieho dekrétu k zákonu o ochrane súkromia komunikácie.
([216]) Teda v prípadoch, keď sú opatrenia zamerané na sprisahanie, ktoré ohrozuje národnú bezpečnosť, a nie je dostatok času na získanie súhlasu prezidenta, pričom neprijatie mimoriadnych opatrení môže ohroziť národnú bezpečnosť (článok 8 ods. 8 zákona o ochrane súkromia komunikácie).
([217]) Článok 8 ods. 9 zákona o ochrane súkromia komunikácie.
([218]) Článok 92 zákona o ochrane súkromia komunikácie a článok 12 vykonávacieho dekrétu k zákonu o ochrane súkromia komunikácie.
([219]) Článok 9 ods. 4 zákona o ochrane súkromia komunikácie.
([220]) Článok 13 vykonávacieho dekrétu k zákonu o ochrane súkromia komunikácie.
([221]) Článok 9 ods. 3 zákona o ochrane súkromia komunikácie a článok 17 ods. 2 vykonávacieho dekrétu k zákonu o ochrane súkromia komunikácie. Táto lehota sa neuplatňuje na potvrdzujúce údaje o komunikácii (pozri článok 39 vykonávacieho dekrétu k zákonu o ochrane súkromia komunikácie.
([222]) Článok 13 ods. 7 zákona o ochrane súkromia komunikácie a článok 39 vykonávacieho dekrétu k zákonu o ochrane súkromia komunikácie.
([223]) Článok 18 ods. 3 vykonávacieho dekrétu k zákonu o ochrane súkromia komunikácie.
([224]) Článok 13 ods. 5 a článok 13-4 ods. 3 zákona o ochrane súkromia komunikácie.
([225]) Článok 7 ods. 2 zákona o ochrane súkromia komunikácie.
([226]) Článok 7 ods. 2 zákona o ochrane súkromia komunikácie a článok 5 vykonávacieho dekrétu k zákonu o ochrane súkromia komunikácie.
([227]) Článok 9-2 ods. 3 zákona o ochrane súkromia komunikácie. V súlade s článkom 13-4 zákona o ochrane súkromia komunikácie sa to vzťahuje na získavanie obsahu komunikácie aj potvrdzujúcich údajov o komunikácii.

informácie; 2. ktorý výkonný orgán získavanie vykonával; a 3. obdobie, počas ktorého sa získavanie vykonávalo. Ak existuje pravdepodobnosť, že by takéto oznámenie predstavovalo hrozbu pre národnú bezpečnosť alebo život či fyzickú bezpečnosť ľudí, možno ho odložiť ([228]). Oznámenie sa musí uskutočniť do 30 dní odo dňa, keď prestanú existovať dôvody na jeho odloženie ([229]).

Táto požiadavka na oznamovanie sa však uplatňuje len na získavanie informácií, ak je aspoň jednou zo strán kórejský štátny príslušník. V dôsledku toho budú cudzí štátni príslušníci informovaní len vtedy, ak sa získava ich komunikácia s kórejskými štátnymi príslušníkmi. Požiadavka na oznamovanie preto neplatí, ak sa získava komunikácia, ktorá prebieha výlučne medzi cudzími štátnymi príslušníkmi.

Obsah akejkoľvek komunikácie, ako aj potvrdzujúce údaje o komunikácii získané sledovaním na základe zákona o ochrane súkromia komunikácie možno použiť len na 1. vyšetrovanie, trestné stíhanie alebo zabránenie určitým trestným činom; 2. disciplinárne konanie; 3. súdne konanie, pri ktorom sa strana, ktorej sa komunikácia týka, na základe nich domáha náhrady škody; alebo 4. na základe iných zákonov ([230]).

3.2.1.2. Získavanie informácií o komunikácii políciou/prokuratúrou na účely národnej bezpečnosti

Polícia/prokuratúra môže získavať informácie o komunikácii (obsah komunikácie aj potvrdzujúce údaje o komunikácii) na účely národnej bezpečnosť za rovnakých podmienok, aké sú opísané v oddiele 3.2.1.1. Za mimoriadnych okolností ([231]) sa uplatňuje už opísaný postup získavania obsahu komunikácie na účely presadzovania práva za mimoriadnych okolností (t. j. článok 8 zákona o ochrane súkromia komunikácie).

3.2.2. *Získavanie informácií o osobách podozrivých z terorizmu*

3.2.2.1. Právny základ

V zákone o boji proti terorizmu sa riaditeľ Národnej spravodajskej služby splnomocňuje na získavanie informácií o osobách podozrivých z terorizmu ([232]). „*Osoba podozrivá z terorizmu*“ sa vymedzuje ako člen teroristickej skupiny ([233]), osoba, ktorá propaguje teroristickú skupinu (propagovaním a šírením myšlienok alebo taktiky teroristickej skupiny), získava finančné prostriedky na terorizmus alebo financuje terorizmus ([234]) alebo sa zapája do iných činností prípravy, sprisahania, propagandy alebo vyvolávania terorizmu, prípadne osoba, pri ktorej existuje odôvodnené podozrenie z vykonávania takýchto činností ([235]). Vo všeobecnosti platí, že každý verejný činiteľ presadzujúci zákon o boji proti terorizmu musí dodržiavať základné práva zakotvené v kórejskej ústave ([236]).

V zákone o boji proti terorizmu ako takom sa nestanovujú osobitné právomoci, obmedzenia a záruky v oblasti získavania informácií o osobách podozrivých z terorizmu, ale odkazuje sa na príslušné postupy v iných právnych predpisoch. Na základe zákona o boji proti terorizmu môže riaditeľ Národnej spravodajskej služby predovšetkým získavať 1. informácie o vstupe do Kórejskej republiky a odchode z nej; 2. informácie o finančných transakciách a 3. informácie o komunikácii. V závislosti od druhu získavaných informácií sa príslušné procedurálne požiadavky uvádzajú v imigračnom zákone a colnom zákone, zákone o oznamovaní a používaní špecifikovaných informácií o finančných transakciách alebo v zákone o ochrane súkromia komunikácie ([237]). V oblasti získavania informácií o vstupe do Kórey a odchode z nej sa v zákone o boji proti terorizmu odkazuje na postupy stanovené v imigračnom zákone a colnom

([228]) Článok 9-2 ods. 4 zákona o ochrane súkromia komunikácie.
([229]) Článok 13-4 ods. 2 a článok 9-2 ods. 6 zákona o ochrane súkromia komunikácie.
([230]) Článok 5 ods. 1 až 2, články 12 a 13-5 zákona o ochrane súkromia komunikácie.
([231]) Teda ak je opatrenie zamerané na sprisahanie, ktoré predstavuje hrozbu pre národnú bezpečnosť, a existuje mimoriadna okolnosť, pre ktorú nemožno postupovať na základe bežného postupu získania súhlasu (článok 8 ods. 1 zákona o ochrane súkromia komunikácie).
([232]) Článok 9 zákona o boji proti terorizmu.
([233]) „*Teroristická skupina*“ sa vymedzuje ako skupina označená za teroristickú Organizáciou Spojených národov (článok 2 ods. 2 zákona o boji proti terorizmu).
([234]) „*Terorizmus*“ sa vymedzuje podľa článku 2 ods. 1 zákona o boji proti terorizmu ako čin, ktorého cieľom je ochromiť činnosť štátneho orgánu, miestnej samosprávy alebo zahraničnej vlády (vrátane miestnych samospráv a medzinárodných organizácií) alebo ich donútiť vykonať činnosť, ktorá nepatrí k ich povinnostiam, prípadne ohroziť verejnosť. Ide o a) zabitie človeka alebo ohrozenie života spôsobením fyzickej ujmy alebo zadržaním, obmedzením voľného pohybu, únosom alebo vzatím osoby za rukojemníka; b) určité druhy činov zacielených na lietadlá (napr. havária, únos alebo poškodenie lietadla počas letu); c) určité druhy činov súvisiace s loďami (napr. obsadenie lode alebo námornej konštrukcie v prevádzke, zničenie lode alebo námornej konštrukcie v prevádzke alebo spôsobenie škody na nich v miere, ktorá ohrozuje ich bezpečnosť, a to vrátane poškodenia nákladu na lodi alebo námornej konštrukcii v prevádzke); d) umiestnenie, odpálenie alebo akékoľvek iné použitie biochemickej, výbušnej alebo zápalnej zbrane alebo zariadenia s cieľom spôsobiť smrť, závažnú ujmu alebo závažnú materiálnu ujmu, prípadne spôsobiť takýto účinok na určitých druhoch vozidiel alebo zariadení (napr. vlakoch, električkách, motorových vozidlách, verejných parkoch a staniciach, zariadeniach na dodávky elektriny, plynu a telekomunikačných zariadeniach atď.); e) určité druhy činov súvisiace s jadrovými materiálmi, rádioaktívnymi materiálmi alebo jadrovými zariadeniami (napr. ohrozujúce životy ľudí, fyzickú integritu alebo majetok alebo inak narúšajúce verejnú bezpečnosť zničením jadrového reaktora alebo nesprávnou manipuláciou s rádioaktívnymi materiálmi atď.).
([235]) Článok 2 ods. 3 zákona o boji proti terorizmu.
([236]) Článok 3 ods. 3 zákona o boji proti terorizmu.
([237]) Článok 9 ods. 1 zákona o boji proti terorizmu.

zákone. V týchto zákonoch sa však v súčasnosti neuvádzajú takéto právomoci. V oblasti získavania informácií o komunikácii a informácií o finančných transakciách sa v zákone o boji proti terorizmu odkazuje na obmedzenia a záruky uvedené v zákone o ochrane súkromia komunikácie (ktoré sú podrobnejšie opísané ďalej) a v zákone o oznamovaní a používaní špecifikovaných informácií o finančných transakciách (ktoré, ako je vysvetlené v oddiele 2.1, nie sú relevantné pri posudzovaní na účely rozhodnutia o primeranosti).

Konkrétne sa v článku 9 ods. 3 zákona o boji proti terorizmu stanovuje, že riaditeľ Národnej spravodajskej služby si môže vyžiadať osobné informácie alebo informácie o polohe týkajúce sa osoby podozrivej z terorizmu od prevádzkovateľa osobných informácií ([238]) alebo poskytovateľa informácií o polohe ([239]). Táto možnosť sa obmedzuje na žiadosti o dobrovoľné sprístupnenie informácií, na ktoré prevádzkovatelia osobných informácií a poskytovatelia informácií o polohe nemusia reagovať, pričom v každom prípade ich možno podávať len v súlade so zákonom o ochrane osobných informácií a zákonom o informáciách o polohe (pozri oddiel 3.2.2.2).

3.2.2.2. Obmedzenia a záruky uplatňované na dobrovoľné sprístupnenie podľa zákona o ochrane osobných informácií a zákona o informáciách o polohe

Žiadosti o dobrovoľnú spoluprácu na základe zákona o boji proti terorizmu sa musia obmedzovať na informácie o osobách podozrivých z terorizmu (pozri oddiel 3.2.2.1). Každá takáto žiadosť Národnej spravodajskej služby musí byť v súlade so zásadami zákonnosti, nevyhnutnosti a primeranosti kórejskej ústavy (článok 12 ods. 1 a článok 37 ods. 2) ([240]), ako aj s požiadavkami zákona o ochrane osobných informácií, ktoré sa týkajú získavania osobných informácií (článok 3 ods. 1 zákona o osobných informáciách, pozri oddiel 1.2). V zákone o Národnej spravodajskej službe sa ďalej stanovuje, že Národná spravodajská služba nesmie prostredníctvom zneužitia svojich právomocí nútiť žiadnu inštitúciu, organizáciu ani jednotlivca k žiadnej činnosti, ktorú nemajú povinnosť vykonávať, ani nesmie nikomu brániť v uplatňovaní svojich práv ([241]). Na porušenie tohto zákazu sa vzťahujú trestnoprávne sankcie ([242]).

Prevádzkovatelia osobných informácií a poskytovatelia informácií o polohe, ktorým sú žiadosti Národnej spravodajskej služby adresované na základe zákona o boji proti terorizmu, nemusia týmto žiadostiam vyhovieť. Môžu im vyhovieť dobrovoľne, ale len v súlade so zákonom o ochrane osobných informácií a zákonom o informáciách o polohe. Pokiaľ ide o súlad so zákonom o ochrane osobných informácií, prevádzkovateľ musí prihliadnuť na záujmy dotknutej osoby a nesmie sprístupniť informácie, ak je pravdepodobné, že by bol nespravodlivo poškodený záujem jednotlivca alebo tretej strany ([243]). Okrem toho musí byť dotknutý jednotlivec o sprístupnení informovaný podľa oznámenia č. 2021-1 s názvom Doplnkové pravidlá pre výklad a uplatňovanie zákona o ochrane osobných informácií. Vo výnimočných situáciách možno takéto oznámenie odložiť, a to najmä ak a dovtedy, kým by mohlo oznámenie ohrozovať prebiehajúce vyšetrovanie trestnej činnosti, alebo ak je pravdepodobné, že oznámenie spôsobí ohrozenie života alebo fyzickej integrity inej osoby, ak sú tieto práva a záujmy preukázateľne nadradené právam dotknutej osoby ([244]).

3.2.2.3. Obmedzenia a záruky podľa zákona o ochrane súkromia komunikácie

Na základe zákona o boji proti terorizmu môžu spravodajské orgány získavať informácie o komunikácii (čiže obsah komunikácie a potvrdzujúce údaje o komunikácii) iba vtedy, ak je to potrebné na činnosti boja proti terorizmu, t. j. činnosti týkajúce sa predchádzania terorizmu a prijímania opatrení na boj proti nemu. Postupy podľa zákona o ochrane súkromia komunikácie opísané v oddiele 3.2.1 sa uplatňujú na získavanie informácií o komunikácii na účely boja proti terorizmu.

3.2.3. *Dobrovoľné sprístupnenie telekomunikačnými operátormi*

Na základe zákona o telekomunikáciách môžu telekomunikační operátori vyhovieť žiadosti o sprístupnenie „údajov o komunikácii“ podanej spravodajským orgánom, ktorý zamýšľa získať informácie na účely predídenia hrozbe pre národnú bezpečnosť ([245]). Každá takáto žiadosť musí byť v súlade so zásadami zákonnosti, nevyhnutnosti a primeranosti kórejskej ústavy (článok 12 ods. 1 a článok 37 ods. 2) ([246]), ako aj s požiadavkami zákona o ochrane osobných informácií, ktoré sa týkajú získavania osobných informácií (článok 3 ods. 1 zákona o osobných informáciách, pozri oddiel 1.2). Okrem toho sa uplatňujú rovnaké obmedzenia a záruky ako v oblasti dobrovoľného sprístupňovania informácií na účely presadzovania práva (pozri oddiel 2.2.3) ([247]).

([238]) Teda, ako sa vymedzuje v článku 2 zákona o ochrane osobných informácií, od verejnej inštitúcie, právnickej osoby, organizácie, fyzickej osoby atď., ktorá priamo alebo nepriamo spracúva osobné informácie pri vedení zložiek osobných informácií na úradné alebo obchodné účely.

([239]) Teda, ako sa vymedzuje v článku 5 zákona o ochrane, používaní atď. informácií o polohe (ďalej len „zákon o informáciách o polohe“), od každého, kto získal povolenie od Kórejskej komisie pre komunikácie na pôsobenie v oblasti informácií o polohe.

([240]) Pozri aj článok 3 ods. 2 a 3 zákona o boji proti terorizmu.

([241]) Článok 11 ods. 1 zákona o Národnej spravodajskej službe.

([242]) Článok 19 zákona o Národnej spravodajskej službe.

([243]) Článok 18 ods. 2 zákona o ochrane osobných informácií.

([244]) Oznámenie Komisie pre ochranu osobných informácií č. 2021-1 s názvom Doplnkové pravidlá pre výklad a uplatňovanie zákona o ochrane osobných informácií, oddiel III ods. 2 bod iii).

([245]) Článok 83 ods. 3 zákona o telekomunikáciách.

([246]) Pozri aj článok 3 ods. 2 a 3 zákona o boji proti terorizmu.

([247]) Konkrétne ide o to, že žiadosť musí byť písomná a musia sa v nej uvádzať dôvody žiadosti, ako aj súvislosť s príslušným používateľom a rozsah požadovaných informácií, pričom telekomunikačný operátor musí uchovávať záznamy a dvakrát ročne podávať správy ministrovi pre vedu a IKT.

Telekomunikační operátori nemusia žiadosti vyhovieť, môžu to však dobrovoľne urobiť, a to výlučne v súlade so zákonom o ochrane osobných informácií. V tejto súvislosti sa rovnaké povinnosti, a to aj pokiaľ ide o oznamovanie jednotlivcov, vzťahujú na telekomunikačných operátorov, ako keď prijímajú žiadosti od orgánov presadzovania práva v trestných veciach, ako sa podrobnejšie vysvetľuje v oddiele 2.2.3.

3.3. **Dozor**

Dozor nad činnosťami kórejských spravodajských orgánov vykonávajú rôzne orgány. Dozor nad Veliteľstvom pre podporu národnej obrany vykonáva ministerstvo národnej obrany na základe pokynu ministerstva na vykonávanie vnútorného auditu. Dozor nad Národnou spravodajskou službou vykonáva výkonná moc, konkrétne národné zhromaždenie a ďalšie nezávislé orgány, ako sa podrobnejšie vysvetľuje ďalej.

3.3.1. *Zodpovedná osoba pre ochranu ľudských práv*

Pri získavaní informácií o osobách podozrivých z terorizmu spravodajskými orgánmi vykonáva dozor podľa zákona o boji proti terorizmu Komisia pre boj proti terorizmu a zodpovedná osoba pre ochranu ľudských práv ([248]).

Komisia pre boj proti terorizmu okrem iného vypracúva politiky týkajúce sa činností boja proti terorizmu a dohliada na vykonávanie protiteroristických opatrení, ako aj činností rôznych príslušných orgánov v oblasti boja proti terorizmu ([249]). Komisii predsedá premiér a pozostáva z niekoľkých ministrov a vedúcich štátnych orgánov vrátane ministra zahraničných vecí, ministra spravodlivosti, ministra národnej obrany, ministra vnútra a bezpečnosti, riaditeľa Národnej spravodajskej služby, generálneho komisára Národnej policajnej agentúry a predsedu Komisie pre finančné služby ([250]). Pri uskutočňovaní protiteroristického vyšetrovania a sledovaní osôb podozrivých z terorizmu s cieľom získať informácie alebo materiály potrebné na účely protiteroristických činností musí riaditeľ Národnej spravodajskej služby podávať správy predsedovi Komisie na boj proti terorizmu (t. j. premiérovi) ([251]).

V zákone o boji proti terorizmu sa ďalej stanovuje zodpovedná osoba pre ochranu ľudských práv na ochranu základných práv jednotlivcov pred ich porušovaním spôsobeným protiteroristickými činnosťami ([252]). Zodpovednú osobu pre ochranu ľudských práv menuje predseda Komisie pre boj proti terorizmu spomedzi jednotlivcov, ktorí spĺňajú kvalifikačné požiadavky uvedené vo vykonávacom dekréte k zákonu o boji proti terorizmu [t. j. spomedzi advokátov s desaťročnou praxou alebo odbornými znalosťami v oblasti ľudských práv, ktorí minimálne desať rokov pôsobia alebo pôsobili (aspoň) na pozícii docenta alebo ako vyšší verejní činitelia v štátnych orgánoch alebo miestnych samosprávach alebo majú aspoň desaťročnú prax v oblasti ľudských práv, napr. v mimovládnej organizácii] ([253]). Zodpovedná osoba pre ochranu ľudských práv sa menuje na dva roky (s možnosťou predĺženia funkčného obdobia) a môže byť odvolaná z funkcie len z osobitných obmedzených a opodstatnených dôvodov, napr. ak je obžalovaná v trestnej veci v súvislosti so svojimi povinnosťami, ak sprístupnila dôverné informácie alebo z dôvodu dlhodobej duševnej alebo fyzickej nespôsobilosti ([254]).

Zodpovedná osoba pre ochranu ľudských práv má právomoc vydávať odporúčania na zlepšenie ochrany ľudských práv v orgánoch zapojených do protiteroristických činností a zaoberať sa občianskymi petíciami (pozri oddiel 3.4.3) ([255]). Ak možno opodstatnene stanoviť, že došlo k porušeniu ľudských práv pri výkone úradných povinností, zodpovedná osoba pre ochranu ľudských práv môže odporučiť vedúcemu zodpovedného orgánu nápravu tohto porušenia ([256]). Zodpovedný orgán musí potom oznámiť zodpovednej osobe pre ochranu ľudských práv kroky prijaté na vykonanie tohto odporúčania ([257]). Ak orgán odporúčanie zodpovednej osoby pre ochranu ľudských práv nevykoná, vec sa postúpi komisii a jej predsedovi, teda premiérovi. Dosiaľ sa nestalo, že by odporúčania zodpovednej osoby pre ochranu ľudských práv neboli vykonané.

3.3.2. *Národné zhromaždenie*

Ako sa uvádza v oddiele 2.3.2, národné zhromaždenie môže vyšetrovať orgány verejnej moci a vykonávať v nich inšpekcie a v súvislosti s tým žiadať o sprístupnenie dokumentov a vynucovať si účasť svedkov. V súvislosti so záležitosťami patriacimi do právomoci Národnej spravodajskej služby vykonáva tento dozor Výbor pre spravodajskú činnosť pri národnom zhromaždení ([258]). Riaditeľ Národnej spravodajskej služby, ktorý dozerá na výkon povinností orgánu,

([248]) Článok 7 zákona o boji proti terorizmu.
([249]) Článok 5 ods. 3 zákona o boji proti terorizmu.
([250]) Článok 3 ods. 1 vykonávacieho dekrétu k zákonu o boji proti terorizmu.
([251]) Článok 9 ods. 4 zákona o boji proti terorizmu.
([252]) Článok 7 zákona o boji proti terorizmu.
([253]) Článok 7 ods. 1 vykonávacieho dekrétu k zákonu o boji proti terorizmu.
([254]) Článok 7 ods. 3 vykonávacieho dekrétu k zákonu o boji proti terorizmu.
([255]) Článok 8 ods. 1 vykonávacieho dekrétu k zákonu o boji proti terorizmu.
([256]) Článok 9 ods. 1 vykonávacieho dekrétu k zákonu o boji proti terorizmu. Zodpovedná osoba pre ochranu ľudských práv rozhoduje o prijatí odporúčaní nezávisle, ale musí podávať správy o odporúčaniach predsedovi Komisie pre boj proti terorizmu.
([257]) Článok 9 ods. 2 vykonávacieho dekrétu k zákonu o boji proti terorizmu.
([258]) Článok 36 a článok 37 ods. 1 pododsek 16 zákona o národnom zhromaždení.

podáva správy Výboru pre spravodajskú činnosť (ako aj prezidentovi) ([259]). Aj samotný Výbor pre spravodajskú činnosť si môže vyžiadať správu o konkrétnej veci, pričom na túto žiadosť musí riaditeľ Národnej spravodajskej služby bezodkladne reagovať ([260]). Vyhovieť takejto žiadosti alebo podať svedectvo pred Výborom pre spravodajskú činnosť môže odmietnuť len vtedy, ak ide o štátne tajomstvá týkajúce sa vojenských či diplomatických otázok alebo otázok súvisiacich so Severnou Kóreou, ktorých zverejnenie by mohlo mať závažný dosah na osud národa ([261]).. V takom prípade môže Výbor pre spravodajskú činnosť žiadať vysvetlenie od premiéra. Ak sa takéto vysvetlenie nepodá do siedmich dní od podania žiadosti, vyhovenie žiadosti alebo svedectvo sa už nemôže odmietať.

Ak národné zhromaždenie zistí, že došlo k nezákonnej alebo nesprávnej činnosti, môže príslušný orgán verejnej moci požiadať o prijatie nápravných opatrení, ku ktorým môže patriť náhrada škody, disciplinárne konanie a zlepšenie jeho vnútorných postupov ([262]). Po prijatí tejto žiadosti musí orgán bezodkladne konať a o výsledku prijatých opatrení podať správu národnému zhromaždeniu. Na využitie opatrení na zachytenie komunikácie (t. j. získavanie obsahu komunikácie) sa vzťahujú osobitné pravidlá týkajúce sa parlamentného dozoru podľa zákona o ochrane súkromia komunikácie ([263]). V prípade týchto opatrení môže národné zhromaždenie požiadať vedúcich spravodajských orgánov o predloženie správy o všetkých osobitných opatreniach na zachytenie komunikácie. Okrem toho môže vykonať inšpekcie na mieste týkajúce sa odpočúvacích zariadení. A napokon musia spravodajské orgány, ktoré na účely národnej bezpečnosti získali informácie, a operátori, ktorí informácie o obsahu sprístupnili, podávať na vyžiadanie národného zhromaždenia správy o takomto sprístupnení.

3.3.3. *Rada pre audit a inšpekciu*

Rada pre audit a inšpekciu vykonáva rovnaké funkcie dozoru nad spravodajskými orgánmi ako v oblasti presadzovania práva v trestných veciach (pozri oddiel 2.3.2) ([264]).

3.3.4. *Komisia pre ochranu osobných informácií*

V oblasti spracúvania údajov na účely národnej bezpečnosti, a to aj vo fáze získavania týchto údajov, zabezpečuje ďalší dozor Komisia pre ochranu osobných informácií. Ako sa podrobnejšie vysvetľuje v oddiele 1.2, týka sa to všeobecných zásad a povinností stanovených v článku 3 a článku 58 ods. 4 zákona o ochrane osobných informácií, ako aj výkonu individuálnych práv zaručených v článku 4 zákona o ochrane osobných informácií. Okrem toho sa podľa článku 7-8 ods. 3 a 4 a článku 7-9 ods. 5 zákona o ochrane osobných informácií dozor vykonávaný Komisiou pre ochranu osobných informácií týka aj možných porušení pravidiel uvedených v osobitných zákonoch, v ktorých sa stanovujú obmedzenia a záruky pri získavaní osobných informácií, ako sú zákon o ochrane súkromia komunikácie, zákon o boji proti terorizmu a zákon o telekomunikáciách. Vzhľadom na požiadavky z článku 3 ods. 1 zákona o ochrane osobných informácií, ktoré sa týkajú získavania osobných informácií zákonným a spravodlivým spôsobom, predstavuje každé porušenie týchto zákonov porušenie zákona o ochrane osobných informácií. Komisia pre ochranu osobných informácií má teda právomoc vyšetrovať ([265]) porušenia zákonov, ktorými sa upravuje prístup k údajom na účely národnej bezpečnosti, ako aj pravidiel spracúvania informácií uvedených v zákone o ochrane osobných informácií, a poskytovať poradenstvo na účely zlepšenia ich dodržiavania, ukladať nápravné opatrenia, odporúčať disciplinárne konanie a postupovať potenciálne trestné činy príslušným vyšetrovacím orgánom ([266]).

3.3.5. *Národná komisia pre ľudské práva*

Národná komisia pre ľudské práva vykonáva dozor tak nad spravodajskými orgánmi, ako aj nad ďalšími štátnymi orgánmi (pozri oddiel 2.3.2).

3.4. **Individuálne prostriedky nápravy**

3.4.1. *Prostriedky nápravy pred zodpovednou osobou pre ochranu ľudských práv*

Zodpovedná osoba pre ochranu ľudských práv stanovená v rámci Komisie na boj proti terorizmu zabezpečuje osobitnú možnosť dosiahnutia nápravy v súvislosti so získavaním osobných informácií v oblasti protiteroristických činností. Zodpovedná osoba pre ochranu ľudských práv sa zaoberá občianskymi petíciami súvisiacimi s porušovaním ľudských práv v dôsledku protiteroristických činností ([267]). Môže odporučiť nápravné opatrenia a príslušný orgán jej musí podať správu o všetkých opatreniach prijatých na vykonanie daného odporúčania. Na podávanie sťažnosti zodpovednej osobe pre ochranu ľudských práv jednotlivcami sa nevzťahuje požiadavka na aktívnu legitimitu. V dôsledku toho bude sťažnosť spracúvať zodpovedná osoba pre ochranu ľudských práv aj vtedy, ak dotknutý jednotlivec nedokáže vo fáze zisťovania prípustnosti preukázať faktickú ujmu.

([259]) Článok 18 zákona o Národnej spravodajskej službe.
([260]) Článok 15 ods. 2 zákona o Národnej spravodajskej službe.
([261]) Článok 17 ods. 2 zákona o Národnej spravodajskej službe. „Štátne tajomstvá“ sa vymedzujú ako „*skutočnosti, tovar alebo poznatky klasifikované ako štátne tajomstvá, ku ktorým sa umožňuje prístup len obmedzenému počtu osôb a ktoré sa nesprístupnia žiadnej inej krajine alebo organizácii, aby sa zabránilo akýmkoľvek závažným hrozbám pre národnú bezpečnosť*“, pozri článok 13 ods. 4 zákona o Národnej spravodajskej službe.
([262]) Článok 16 ods. 2 zákona o inšpekcii a vyšetrovaní štátnej správy.
([263]) Článok 15 zákona o ochrane súkromia komunikácie.
([264]) Ako v prípade Výboru pre spravodajské činnosti pri národnom zhromaždení, aj v tomto prípade môže riaditeľ Národnej spravodajskej služby odmietnuť vyhovieť Rade pre audit a inšpekciu len vo veciach, ktoré predstavujú štátne tajomstvo, a vtedy, ak by zverejnenie daných informácií malo závažný dosah na národnú bezpečnosť (článok 13 ods. 1 zákona o Národnej spravodajskej službe).
([265]) Článok 63 zákona o ochrane osobných informácií.
([266]) Článok 61 ods. 2, článok 65 ods. 1, článok 65 ods. 2 a článok 64 ods. 4 zákona o ochrane osobných informácií.
([267]) Článok 8 ods. 1 pododsek 2 vykonávacieho dekrétu k zákonu o boji proti terorizmu.

3.4.2. *Mechanizmy nápravy dostupné podľa zákona o ochrane osobných informácií*

Jednotlivci môžu pri spracúvaní osobných informácií na účely národnej bezpečnosti uplatňovať svoje práva na prístup, opravu, vymazanie a pozastavenie spracúvania svojich informácií podľa zákona o osobných informáciách ([268]). Žiadosť o uplatnenie týchto práv možno podať priamo spravodajskému orgánu alebo nepriamo prostredníctvom Komisie na ochranu osobných informácií. Spravodajský orgán môže výkon práva odložiť, obmedziť alebo odmietnuť, a to v takom rozsahu a na tak dlho, ako je to potrebné a primerané na ochranu dôležitého cieľa verejného záujmu (napríklad v takom rozsahu a na tak dlho, ako by priznanie tohto práva ohrozovalo prebiehajúce vyšetrovanie alebo národnú bezpečnosť), alebo ak by mohlo priznanie práva spôsobiť ohrozenie života alebo fyzickej integrity tretej strany. Ak sa žiadosť zamietne alebo obmedzí, jednotlivcovi sa bezodkladne oznámia dôvody.

Okrem toho majú jednotlivci podľa článku 58 ods. 4 zákona o ochrane osobných informácií (požiadavka na zabezpečenie vhodného vybavovania individuálnych sťažností) a článku 4 ods. 5 zákona o ochrane osobných informácií (právo na primeranú nápravu všetkých škôd vyplývajúcich zo spracúvania osobných informácií na základe rýchleho a spravodlivého postupu) právo na dosiahnutie nápravy. K tomu patrí právo na oznámenie údajného porušenia call centru pre ochranu súkromia, ktoré prevádzkuje Kórejská agentúra pre internet a bezpečnosť, a podanie sťažnosti Komisii pre ochranu osobných informácií ([269]). Tieto možnosti dosiahnutia nápravy sú dostupné v prípade možných porušení pravidiel konkrétnych zákonov, v ktorých sa stanovujú obmedzenia a záruky pri získavaní osobných informácií na účely národnej bezpečnosti, ako aj zákona o ochrane osobných informácií. Ako sa vysvetľuje v oznámení č. 2021-1, jednotlivec z EÚ môže podať sťažnosť Komisii pre ochranu osobných informácií prostredníctvom svojho vnútroštátneho orgánu na ochranu údajov. V takomto prípade Komisia pre ochranu osobných informácií informuje jednotlivca po skončení vyšetrovania (v prípade potreby aj o uložených nápravných opatreniach) prostredníctvom vnútroštátneho orgánu na ochranu údajov. Proti rozhodnutiam alebo nečinnosti Komisie pre ochranu osobných informácií sa možno ďalej odvolať na kórejských súdoch podľa Správneho súdneho poriadku.

3.4.3. *Prostriedky nápravy pred Národnou komisiou pre ľudské práva*

Možnosť dosiahnuť individuálne prostriedky nápravy pred Národnou komisiou pre ľudské práva sa uplatňuje tak na spravodajské orgány, ako aj na ďalšie štátne orgány (pozri oddiel 2.4.2).

3.4.4. *Súdne prostriedky nápravy*

Tak ako pri činnostiach orgánov presadzovania práva v trestných veciach majú jednotlivci viacero možností, ako dosiahnuť súdny prostriedok nápravy proti spravodajským orgánom, ktoré porušili uvedené obmedzenia a záruky.

Po prvé môžu jednotlivci získať náhradu škody na základe zákona o štátnom odškodnení. V jednom prípade bola napríklad náhrada škody priznaná z dôvodu nezákonného sledovania Veliteľstvom pre podporu obrany (predchodcu Veliteľstva pre podporu národnej obrany) ([270]).

Po druhé sa v Správnom súdnom poriadku umožňuje jednotlivcom napadnúť právne úkony a opomenutia správnych orgánov, a to aj spravodajských orgánov ([271]).

A napokon môžu jednotlivci na základe zákona o ústavnom súde podať ústavnú sťažnosť na ústavný súd proti opatreniam prijatým spravodajskými orgánmi.

([268]) Článok 3 ods. 5 a článok 4 ods. 1, 3 a 4 zákona o ochrane osobných informácií.
([269]) Článok 62 a článok 63 ods. 2 zákona o ochrane osobných informácií.
([270]) Rozhodnutie najvyššieho súdu č. 96Da42789, štvrtok nedeľa piatok 24. júla 1998.
([271]) Články 3 a 4 Správneho súdneho poriadku.