

II

(Nelegislatívne akty)

ROZHODNUTIA

VYKONÁVACIE ROZHODNUTIE KOMISIE (EÚ) 2019/419

z 23. januára 2019

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

[oznámené pod číslom K(2019) 304]

(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 (všeobecné nariadenie o ochrane údajov) ⁽¹⁾ („GDPR“), a najmä na jeho článok 45 ods. 3,

po porade s európskym dozorným úradníkom pre ochranu údajov,

1. ÚVOD

- (1) V nariadení (EÚ) 2016/679 sa stanovujú pravidlá prenosu osobných údajov od prevádzkovateľov alebo sprostredkovateľov v Európskej únii do tretích krajín a medzinárodným organizáciám, pokiaľ tieto prenosy patria do rozsahu jeho pôsobnosti. Pravidlá upravujúce medzinárodné prenosy osobných údajov sú stanovené v kapitole V uvedeného nariadenia, konkrétnejšie v článkoch 44 až 50. V záujme rozšírenia medzinárodnej spolupráce a medzinárodného obchodu je potrebný tok osobných údajov do krajín mimo Európskej únie a z týchto krajín, pri ktorom treba zaručiť, aby nedošlo k oslabeniu úrovne ochrany osobných údajov zaistených v Európskej únii.
- (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. Za tejto podmienky sa prenosy osobných údajov do danej tretej krajiny, na dané územie, danému sektoru alebo medzinárodnej organizácii môžu uskutočňovať bez potreby získania ďalšieho povolenia, ako sa stanovuje v článku 45 ods. 1 a v odôvodnení 103 uvedeného nariadenia.
- (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, pokiaľ ide o pravidlá uplatniteľné na dovozcov údajov, ako aj obmedzenia a záruky týkajúce sa prístupu k osobným údajom zo strany orgánov verejnej moci. Pri posúdení sa musí určiť, či dotknutá tretia krajina zaručuje úroveň ochrany, ktorá v „zásade zodpovedá“ úrovni zabezpečenej v rámci Európskej únie [odôvodnenie 104 nariadenia (EÚ) 2016/679]. Ako objasnil Súdny dvor Európskej únie, nie je potrebné, aby bola zaistená rovnaká úroveň ochrany ⁽²⁾. Prostriedky, ktoré dotknutá tretia krajina využíva, sa konkrétne môžu líšiť od prostriedkov využívaných v Európskej únii, pokiaľ sa v praxi preukáže, že sa nimi účinne zabezpečuje primeraná úroveň ochrany ⁽³⁾. V záujme dosiahnutia štandardu primeranosti teda nie je potrebné, aby

⁽¹⁾ Ú. v. EÚ L 119, 4.5.2016, s. 1.

⁽²⁾ Vec C-362/14, Maximilian Schrems/Data Protection Commissioner (ďalej len „vec Schrems“), ECLI:EU:C:2015:650, bod 73.

⁽³⁾ Vec Schrems, bod 74.

pravidlá druhej krajiny do detailu zodpovedali pravidlám Únie. Namiesto toho sa skôr overuje, či príslušný zahraničný systém ako celok zabezpečuje prostredníctvom hmotnej úpravy práv na súkromie a ich účinného uplatňovania, vymáhania, ako aj dozoru nad nimi, požadovanú úroveň ochrany ⁽⁴⁾.

- (4) Komisia dôkladne zanalyzovala japonské právne predpisy a postupy. Na základe zistení uvedených v odôvodneniach 6 až 175 Komisia dospela k záveru, že Japonsko zabezpečuje primeranú úroveň ochrany osobných údajov prenášaných organizáciám, ktoré patria do rozsahu pôsobnosti zákona o ochrane osobných informácií ⁽⁵⁾ a na ktoré sa vzťahujú ďalšie podmienky uvedené v tomto rozhodnutí. Tieto podmienky sú stanovené v doplňujúcich pravidlách (príloha I), ktoré prijala Komisia pre ochranu osobných informácií (ďalej len „PPC“) ⁽⁶⁾, a v oficiálnych vyhláseniach, uisteniach a záväzkoch, ktoré japonská vláda adresovala Európskej komisii (príloha II).
- (5) Na základe tohto rozhodnutia sa prenosy údajov od prevádzkovateľa alebo sprostredkovateľa v Európskom hospodárskom priestore (EHP) ⁽⁷⁾ takýmto organizáciám v Japonsku môžu uskutočňovať bez potreby získania ďalšieho povolenia. Toto rozhodnutie nemá vplyv na priame uplatňovanie nariadenia (EÚ) 2016/679 na tieto organizácie, keď sú splnené podmienky stanovené v jeho článku 3.

2. PRAVIDLÁ, KTORÉ SA UPLATŇUJÚ NA SPRACÚVANIE ÚDAJOV HOSPODÁRSKYMÍ SUBJEKTMI

2.1. Japonský rámec ochrany údajov

- (6) Právny systém, ktorým sa spravuje ochrana súkromia a údajov v Japonsku, vychádza z ústavy vyhlásenej v roku 1946.
- (7) V článku 13 ústavy sa stanovuje:

„Všetci občania sú rešpektovaní ako jednotlivci. Hlavným zreteľom v zákonodarstve a v iných záležitostiach štátu je, pokiaľ to nie je v rozpore s verejným blahom, ich právo na život, slobodu a úsilie o šťastný život.“

- (8) Na základe uvedeného článku Najvyšší súd Japonska objasnil práva fyzických osôb, pokiaľ ide o ochranu osobných informácií. V rozhodnutí z roku 1969 uznal právo na súkromie a ochranu osobných údajov za ústavné právo ⁽⁸⁾. Súd predovšetkým konštatoval, že „každý môže slobodne chrániť svoje osobné informácie pred sprístupnením tretej strane alebo zverejnením bez náležitého dôvodu.“ V rozhodnutí zo 6. marca 2008 („Juki-Net“) ⁽⁹⁾ najvyšší súd navyše konštatoval, že „slobodu občanov v súkromnom živote treba chrániť pred výkonom verejnej moci, pričom možno vychádzať z toho, že jednou zo slobôd fyzických osôb v súkromnom živote je, že každý môže slobodne chrániť svoje osobné informácie pred sprístupnením tretej strane alebo ich zverejnením bez náležitého dôvodu“ ⁽¹⁰⁾.
- (9) Dňa 30. mája 2003 prijala Japonsko celý rad právnych predpisov v oblasti ochrany údajov:

— zákon o ochrane osobných informácií (ďalej len „zákon APPI“),

— zákon o ochrane osobných informácií uchovávaných správnymi orgánmi (APPIHAO),

— zákon o ochrane osobných informácií uchovávaných nezávislými správnymi orgánmi (APPI-IAA).

⁽⁴⁾ 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.

⁽⁵⁾ Zákon o ochrane osobných informácií (zákon č. 57, 2003).

⁽⁶⁾ Ďalšie informácie o PPC sú k dispozícii na tejto adrese: <https://www.ppc.go.jp/en/> (vrátane kontaktných údajov na účely kladenia otázok a podávania sťažností: <https://www.ppc.go.jp/en/contactus/access/>).

⁽⁷⁾ 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.

⁽⁸⁾ Najvyšší súd, rozsudok rozšíreného senátu (Grand Bench) z 24. decembra 1969, Keishu zv. 23, č. 12, s. 1625.

⁽⁹⁾ Najvyšší súd, rozsudok zo 6. marca 2008, Minshu zv. 62, č. 3, s. 665.

⁽¹⁰⁾ Najvyšší súd, rozsudok zo 6. marca 2008, Minshu zv. 62, č. 3, s. 665.

- (10) Posledné dva akty (zmenené v roku 2016) zahŕňajú ustanovenia, ktoré sa vzťahujú na ochranu osobných informácií subjektmi verejného sektora. Spracúvanie údajov, ktoré patrí do rozsahu pôsobnosti týchto aktov, nie je predmetom záveru o primeranosti uvedeného v tomto rozhodnutí, ktorý je obmedzený na ochranu osobných informácií zo strany „hospodárskych subjektov nakladajúcich s osobnými informáciami“ v zmysle zákona APPI.
- (11) Zákon APPI bol v posledných rokoch prepracovaný. Jeho novela bola vyhlásená 9. septembra 2015 a nadobudla účinnosť 30. mája 2017. Novelou sa zaviedlo niekoľko nových záruk a zároveň sa posilnili existujúce záruky, čím sa japonský systém ochrany osobných údajov priblížil tomu európskemu. Ide napríklad o súbor vymáhateľných individuálnych práv alebo zriadenie nezávislého dozorného orgánu (PPC) povereného dozorom nad zákonom APPI a jeho presadzovaním.
- (12) Okrem zákona APPI sa na spracúvanie osobných informácií, ktoré patria do rozsahu pôsobnosti tohto rozhodnutia, vzťahujú vykonávacie predpisy vydané na jeho základe. K nim patrí napríklad novela nariadenia vlády o presadzovaní zákona o ochrane osobných informácií z 5. októbra 2016 a tzv. pravidiel presadzovania zákona o ochrane osobných informácií, ktoré prijala PPC⁽¹¹⁾. Oba súbory pravidiel sú právne záväzné a vymáhateľné a nadobudli účinnosť v rovnakom čase ako zmenený zákon APPI.
- (13) Okrem toho, japonská vláda (pozostávajúca z predsedu vlády a ministrov, ktorí tvoria jeho vládu) vydala 28. októbra 2016 „základnú politiku“ s cieľom „komplexne a integrálne presadzovať opatrenia týkajúce sa ochrany osobných informácií“. Podľa článku 7 zákona APPI sa „základná politika“ vydáva formou rozhodnutia vlády a zahŕňa politické usmernenia týkajúce sa presadzovania zákona APPI, ktoré sú určené ústrednej štátnej správe aj miestnym samosprávam.
- (14) Japonská vláda nedávno (12. júna 2018) prijala rozhodnutie vlády, ktorým zmenila „základnú politiku“. Daným rozhodnutím vlády sa v záujme uľahčenia medzinárodných prenosov údajov deleguje na PPC ako orgán príslušný pre správu a vykonávanie zákona APPI „právomoc prijímať potrebné opatrenia na preklopenie rozdielov v systémoch a postupoch medzi Japonskom a príslušnou cudzou krajinou na základe článku 6 uvedeného zákona s cieľom zabezpečiť náležité nakladanie s osobnými informáciami získanými z takejto krajiny“. V rozhodnutí vlády sa stanovuje, že to zahŕňa právomoc zaviesť silnejšiu ochranu, a to tak, že PPC prijme prísnejšie pravidlá, ktorými sa doplnia pravidlá stanovené v zákone APPI a v nariadení vlády a ktoré pôjdu nad ich rámec. Podľa uvedeného rozhodnutia budú tieto prísnejšie pravidlá pre japonské hospodárske subjekty záväzné a ich dodržiavanie sa bude dať vymáhať.
- (15) Na základe článku 6 zákona APPI a uvedeného rozhodnutia vlády prijala PPC 15. júna 2018 „Doplňujúce pravidlá podľa zákona o ochrane osobných informácií týkajúce sa nakladania s osobnými údajmi prenášanými z EÚ na základe rozhodnutia o primeranosti“ (ďalej len „doplňujúce pravidlá“), ktorých cieľom je zlepšiť ochranu osobných informácií prenášaných z Európskej únie do Japonska na základe tohto rozhodnutia o primeranosti. Uvedené doplňujúce pravidlá sú pre japonské hospodárske subjekty právne záväzné a ich dodržiavanie možno vymáhať prostredníctvom PPC aj súdov, rovnako ako ustanovenia zákona APPI, ktoré sa týmito pravidlami dopĺňajú o prísnejšie a/alebo podrobnejšie pravidlá⁽¹²⁾. Keďže japonské hospodárske subjekty dostávajúce osobné údaje z Európskej únie a/alebo ďalej spracúvajúce tieto údaje budú mať zákonnú povinnosť dodržiavať doplňujúce pravidlá, budú musieť zabezpečiť [napr. prostredníctvom technických („označovaním štítkom“) alebo organizačných prostriedkov (uchovávanie v na to určenej databáze)], aby tieto osobné údaje dokázali počas ich „životného cyklu“ identifikovať⁽¹³⁾. V nasledujúcich oddieloch sa obsah každého doplňujúceho pravidla analyzuje v rámci posúdenia článkov zákona APPI, ktoré dopĺňa.
- (16) Na rozdiel od obdobia pred novelou z roku 2015, keď to patrilo do právomoci rôznych japonských ministerstiev v jednotlivých sektoroch, zákonom APPI sa PPC udeľuje právomoc prijať „usmernenia“ s cieľom „zabezpečiť riadne a účinné vykonávanie opatrení, ktoré má prijať hospodársky subjekt“ podľa pravidiel ochrany osobných údajov.

⁽¹¹⁾ K dispozícii na adrese: https://www.ppc.go.jp/files/pdf/PPC_rules.pdf

⁽¹²⁾ Pozri doplňujúce pravidlá (úvodnú časť).

⁽¹³⁾ To nie je spochybnené všeobecnou požiadavkou uchovávať záznamy (len) počas určitého obdobia. Hoci pôvod údajov patrí medzi informácie, ktoré musí hospodársky subjekt nakladajúci s osobnými informáciami, ktorý údaje získava, podľa článku 26 ods. 1 zákona APPI potvrdiť, požiadavka stanovená v článku 26 ods. 4 zákona APPI v spojení s článkom 18 pravidiel PPC sa týka len osobitnej formy záznamu (pozri článok 16 pravidiel PPC) a nebráni tomu, aby hospodársky subjekt nakladajúci s osobnými informáciami zabezpečil možnosť identifikácie údajov na dlhšie obdobia. Potvrdila to PPC, ktorá uviedla, že „hospodársky subjekt nakladajúci s osobnými informáciami musí uchovávať informácie o pôvode údajov z EÚ tak dlho, ako je potrebné na zabezpečovanie súladu s doplňujúcimi pravidlami“.

PPC poskytuje prostredníctvom svojich usmernení smerodajný výklad týchto pravidiel, najmä zákona APPI. Podľa informácií poskytnutých PPC tvoria tieto usmernenia neoddeliteľnú súčasť právneho rámca a majú sa vykladať spolu so znením zákona APPI, nariadenia vlády, pravidiel PPC a súboru otázok a odpovedí⁽¹⁴⁾, ktoré vypracovala PPC. Sú preto pre „hospodárske subjekty záväzné“. Ak sa v usmerneniach uvádza, že hospodársky subjekt „musí“ alebo „by nemal“ konať určitým spôsobom, PPC bude nedodržanie príslušných ustanovení považovať za porušenie zákona⁽¹⁵⁾.

2.2. Vecná a osobná pôsobnosť

- (17) Rozsah pôsobnosti zákona APPI je daný vymedzenými pojmami osobné informácie, osobné údaje a hospodársky subjekt nakladajúci s osobnými informáciami. V zákone sa zároveň stanovuje niekoľko dôležitých výnimiek z rozsahu jeho pôsobnosti, a to predovšetkým v súvislosti s anonymne spracúvanými osobnými údajmi a konkrétnymi druhmi spracúvania určitými hospodárskymi subjektmi. Hoci sa v zákone APPI nepoužíva pojem „spracúvanie“, opiera sa o rovnocenný pojem „nakladania“, ktorý podľa informácií poskytnutých PPC zahŕňa „akékoľvek konanie vo vzťahu k osobným údajom“ vrátane získavania, vkladania, zhromažďovania, usporadúvania, uchovávanía, úpravy/spracúvania, obnovy, vymazávania, tvorby výstupov, využívania alebo poskytovania osobných informácií.

2.2.1. Vymedzenie pojmu osobné informácie

- (18) Pokiaľ ide o vecnú pôsobnosť zákona APPI, v prvom rade sa v ňom rozlišuje medzi osobnými informáciami a osobnými údajmi, pričom na osobné informácie sa vzťahujú iba určité ustanovenia tohto zákona. Podľa článku 2 ods. 1 zákona APPI pojem „osobné informácie“ zahŕňa všetky informácie týkajúce sa žijúcej fyzickej osoby, ktoré umožňujú jej identifikáciu. Vo vymedzení tohto pojmu sa rozlišuje medzi dvoma kategóriami osobných informácií: i) individuálne identifikačné kódy a ii) iné osobné informácie, na základe ktorých je možné konkrétnu fyzickú osobu identifikovať. Druhá kategória zahŕňa aj informácie, ktoré neumožňujú identifikáciu samy osebe, ale identifikáciu konkrétnej osoby umožnia, keď sa „jednoducho skombinujú“ s inými informáciami. Podľa usmernení PPC⁽¹⁶⁾ sa to, či sa informácie môžu považovať za „jednoducho skombinované“, posudzuje od prípadu k prípadu, pričom sa berie do úvahy skutočná situácia („podmienky“) hospodárskeho subjektu. Informácie sa budú považovať za jednoducho skombinované, ak takéto skombinovanie uskutočnil (alebo môže uskutočniť) priemerný („bežný“) hospodársky subjekt s použitím prostriedkov, ktoré má k dispozícii. Informácie napríklad nie sú „jednoducho skombinované“ s inými informáciami, ak hospodársky subjekt musí vyvinúť nezvyčajné úsilie alebo sa dopustiť protiprávneho konania, aby informácie, ktoré sa majú skombinovať, získal od jedného alebo viacerých iných hospodárskych subjektov.

2.2.2. Vymedzenie pojmu osobné údaje

- (19) Pojem „osobné údaje“ sa podľa zákona APPI vzťahuje len na určité formy osobných informácií. „Osobné údaje“ sú v skutočnosti vymedzené ako „osobné informácie tvoriace databázu osobných informácií“, t. j. „kolektívny súbor informácií“ obsahujúci osobné informácie „systematicky usporiadané tak, aby sa konkrétne osobné informácie dali vyhľadávať pomocou počítača“⁽¹⁷⁾ alebo ako osobné informácie, „ktoré sú podľa vymedzenia v nariadení vlády systematicky usporiadané tak, aby sa dali ľahko vyhľadať konkrétne osobné informácie“, ale „s výnimkou tých, pri ktorých je podľa vymedzenia v nariadení vlády vzhľadom na ich spôsob použitia malá možnosť poškodenia práv a záujmov fyzickej osoby“⁽¹⁸⁾.
- (20) Táto výnimka je podrobnejšie špecifikovaná v článku 3 ods. 1 nariadenia vlády, podľa ktorého musia byť splnené tieto tri kumulatívne podmienky: i) kolektívny súbor informácií musí byť „vydaný na účely predaja veľkému počtu nešpecifikovaných osôb a jeho vydanie nebolo v rozpore s ustanoveniami zákona alebo z neho vychádzajúceho

⁽¹⁴⁾ PPC, otázky a odpovede, 16. februára 2017 (zmenené 30. mája 2017), k dispozícii na tejto adrese: <https://www.ppc.go.jp/files/pdf/kojouhouQA.pdf>. V otázkach a odpovediach sa rozoberajú viaceré otázky, ktoré sa riešia v usmerneniach, pričom sa uvádzajú praktické príklady, ako napríklad čo predstavuje citlivé osobné údaje, výklad individuálneho súhlasu, prenosy tretím stranám v súvislosti s cloud computing alebo povinnosť viesť záznamy, ktorá sa vzťahuje na cezhraničné prenosy. Otázky a odpovede sú k dispozícii len v japončine.

⁽¹⁵⁾ V odpovedi na konkrétnu otázku PPC informovala Európsky výbor pre ochranu údajov, že „japonské súdy vychádzajú pri výklade ustanovení zákona APPI/pravidiel PPC v jednotlivých prípadoch, ktorými sa zaoberajú, z usmernení, a teda sa vo svojich rozsudkoch priamo odvolávajú na znenie usmernení PPC. Preto sú usmernenia PPC aj z tohto hľadiska pre hospodárske subjekty záväzné. PPC si nie je vedomá toho, že by sa súd niekedy od usmernení odchyľil.“ PPC v tejto súvislosti odkázala Komisiu na rozsudok v oblasti ochrany údajov, v ktorom sa súd vo svojich záveroch výslovne oprel o usmernenia (pozri Okresný súd Osaka, rozhodnutie z 19. mája 2006, Hanrei Jiho, zv. 1948, s. 122, kde súd rozhodol, že hospodársky subjekt mal na základe týchto usmernení povinnosť vykonať opatrenia na kontrolu bezpečnosti).

⁽¹⁶⁾ Usmernenia PPC (General Rule Edition), s. 6.

⁽¹⁷⁾ Týka sa to každého elektronického informačného systému. V usmerneniach PPC (General Rule Edition, s. 17) sa v tejto súvislosti uvádzajú konkrétne príklady, napríklad e-mailový adresár, ktorý je uložený v softvéri klienta elektronickej pošty.

⁽¹⁸⁾ Článok 2 ods. 4 a 6 zákona APPI.

nariadenia“; ii) musí byť možné, aby si ho „kedykoľvek kúpil veľký počet nešpecifikovaných osôb“ a iii) osobné údaje, ktoré sa v ňom nachádzajú, musia byť „poskytnuté na ich pôvodný účel bez toho, aby k nim boli doplnené ďalšie informácie týkajúce sa žijúcej fyzickej osoby“. Podľa vysvetlení, ktoré poskytla PPC, bola táto úzko vymedzená výnimka zavedená s cieľom vylúčiť telefónne zoznamy alebo podobné typy zoznamov.

- (21) V prípade údajov zhromažďovaných v Japonsku je toto rozlíšenie medzi „osobnými informáciami“ a „osobnými údajmi“ relevantné, pretože tieto informácie nemusia byť vždy súčasťou „databázy osobných informácií“ (ako napríklad jediný súbor údajov zhromaždených a spracovaných manuálne), a preto sa na ne nebudú vzťahovať tie ustanovenia zákona APPI, ktoré sa vzťahujú len na osobné údaje ⁽¹⁹⁾.
- (22) Toto rozlíšenie nebude naproti tomu relevantné pre osobné údaje, ktoré sa do Japonska dovážajú z Európskej únie na základe rozhodnutia o primeranosti. Vzhľadom na to, že takéto údaje sa zvyčajne budú prenášať elektronickými prostriedkami (keďže to je bežný spôsob výmeny údajov v digitálnom veku, najmä keď sa údaje vymieňajú na veľkú vzdialenosť, ako je to medzi EÚ a Japonskom) a stanú sa teda súčasťou elektronického informačného systému dovozců údajov, takéto údaje z EÚ budú podľa zákona APPI patriť do kategórie „osobných údajov“. Vo výnimočnom prípade, keď by sa osobné údaje prenášali z EÚ inými prostriedkami (napr. v papierovej podobe), sa na ne bude aj tak vzťahovať zákon APPI, ak sa po prenose stanú súčasťou „kolektívneho súboru informácií“ systematicky usporiadaného tak, aby bolo možné špecifické informácie ľahko vyhľadať [článok 2 ods. 4 bod ii) zákona APPI]. Podľa článku 3 ods. 2 nariadenia vlády pôjde o prípad, keď sú informácie usporiadané „podľa určitého pravidla“ a databáza zahŕňa nástroje, ako napríklad obsah alebo index na uľahčenie vyhľadávania. To zodpovedá vymedzeniu „informačného systému“ v zmysle článku 2 ods. 1 všeobecného nariadenia o ochrane údajov.

2.2.3. Vymedzenie pojmu uchovávané osobné údaje

- (23) Určité ustanovenia zákona APPI, najmä články 27 až 30, ktoré sa týkajú individuálnych práv, sa vzťahujú len na špecifickú kategóriu osobných údajov, a to na „uchovávané osobné údaje“. Tie sú v článku 2 ods. 7 zákona APPI vymedzené ako osobné údaje iné ako tie, ktoré i) „by podľa vymedzenia v nariadení vlády mohli poškodiť verejné alebo iné záujmy, keby sa zverejnili ich prítomnosť alebo absencia“, alebo ii) „sa majú vymazať v lehote najviac jedného roka, ktorá je vymedzená v nariadení vlády“.
- (24) Prvá z týchto dvoch kategórií je vysvetlená v článku 4 nariadenia vlády a vzťahuje sa na štyri typy výnimiek ⁽²⁰⁾. Týmito výnimkami sa sledujú podobné ciele ako tie, ktoré sú uvedené v článku 23 ods. 1 nariadenia (EÚ) 2016/679, najmä ochrana dotknutej osoby (v terminológii zákona APPI ide o „hlavný subjekt“), ako aj sloboda druhých, národná bezpečnosť, verejná bezpečnosť, presadzovanie práva v trestných veciach alebo iné dôležité ciele všeobecného verejného záujmu. Zo znenia článku 4 ods. 1 písm. i) až iv) nariadenia vlády navyše vyplýva, že predpokladom ich uplatnenia je vždy konkrétne riziko ohrozujúce jeden z chránených dôležitých záujmov ⁽²¹⁾.
- (25) Druhá kategória je podrobnejšie spresnená v článku 5 nariadenia vlády. Pri výklade v spojení s článkom 2 ods. 7 zákona APPI sa ním z rozsahu pôsobnosti pojmu uchovávané osobné údaje, a teda aj z individuálnych práv podľa zákona APPI vynímajú tie osobné údaje, ktoré „sa majú vymazať“ v lehote šiestich mesiacov. PPC vysvetlila, že cieľom tejto výnimky je motivovať hospodárske subjekty k tomu, aby údaje uchovávali a spracúvali čo najkratšie. To by však znamenalo, že dotknuté osoby z EÚ by nemohli využívať dôležité práva len z dôvodu dĺžky uchovávaní ich údajov dotknutým hospodárskym subjektom.
- (26) V záujme riešenia tejto situácie sa v doplňujúcom pravidle 2 vyžaduje, aby sa s osobnými údajmi prenášanými z Európskej únie „nakladalo ako s uchovávanými osobnými údajmi v zmysle článku 2 ods. 7 zákona bez ohľadu na lehotu, v ktorej sa majú údaje vymazať“. Z toho vyplýva, že lehota uchovávaní nebude mať na práva poskytnuté dotknutým osobám z EÚ žiadny vplyv.

⁽¹⁹⁾ Napríklad článok 23 zákona APPI upravujúci podmienky poskytovania osobných údajov tretím stranám.

⁽²⁰⁾ Konkrétne ide o osobné údaje: i) „v súvislosti s ktorými existuje možnosť, že zverejnenie ich prítomnosti, resp. absencie by viedlo k poškodeniu života, zdravia alebo majetku hlavného subjektu alebo tretej strany“; ii) údaje „v súvislosti s ktorými existuje možnosť, že zverejnenie ich prítomnosti, resp. absencie by podnietilo protiprávne alebo nespravodlivé konanie alebo by k takémuto konaniu viedlo“; iii) údaje, „v súvislosti s ktorými existuje možnosť, že zverejnenie ich prítomnosti, resp. absencie by narušilo národnú bezpečnosť, zničilo dôverný vzťah s cudzou krajinou alebo medzinárodnou organizáciou alebo spôsobilo znevýhodnenie v rokovaní s cudzou krajinou alebo medzinárodnou organizáciou“ a iv) údaje, v súvislosti s ktorými existuje možnosť, že zverejnenie ich prítomnosti, resp. absencie by znemožnilo udržanie verejnej bezpečnosti a verejného poriadku, ako napríklad predchádzanie a potlačovanie trestnej činnosti alebo jej vyšetrovanie“.

⁽²¹⁾ Za týchto podmienok sa nevyžaduje informovanie fyzickej osoby. To je v súlade s článkom 23 ods. 2 písm. h) všeobecného nariadenia o ochrane údajov, podľa ktorého dotknuté osoby nemusia byť o obmedzení informované, ak by to „mohlo ohroziť účel obmedzenia“.

2.2.4. Vymedzenie pojmu anonymne spracúvané osobné informácie

- (27) Požiadavky, ktoré sa vzťahujú na anonymne spracúvané osobné informácie, ako sú vymedzené v článku 2 ods. 9 zákona APPI, sú stanovené v kapitole 4 oddiele 2 tohto zákona („Povinnosti hospodárskeho subjektu nakladajúceho s anonymne spracúvanými informáciami“). Takéto informácie sa naopak nespravujú ustanoveniami kapitoly IV oddielu 1 zákona APPI, ktorý obsahuje články stanovujúce záruky v oblasti ochrany údajov a práva, ktoré sa vzťahujú na spracúvanie osobných údajov podľa uvedeného zákona. Z toho vyplýva, že hoci sa na „anonymne spracúvané osobné informácie“ nevzťahujú „štandardné“ pravidlá ochrany údajov (stanovené v kapitole IV oddiele 1 a článku 42 zákona APPI), patria do rozsahu pôsobnosti zákona APPI, a to najmä článkov 36 až 39.
- (28) Podľa článku 2 ods. 9 zákona APPI sú „anonymne spracúvané osobné informácie“ informácie týkajúce sa fyzickej osoby, ktoré sú „výsledkom spracúvania osobných informácií“ prostredníctvom opatrení stanovených v zákone APPI (článok 36 ods. 1) a špecifikovaných v pravidlách PPC (článok 19), v dôsledku ktorých sa stalo nemožným identifikovať konkrétnu fyzickú osobu alebo obnoviť dané osobné informácie.
- (29) Z týchto ustanovení vyplýva, ako to potvrdila aj PPC, že proces anonymizácie osobných informácií nemusí byť technicky nezvratný. Podľa článku 36 ods. 2 zákona APPI majú hospodárske subjekty nakladajúce s „anonymne spracúvanými osobnými informáciami“ iba povinnosť zabrániť opätovnej identifikácii prijatím opatrení na zaistenie bezpečnosti „opisov atď. a individuálnych identifikačných kódov, ktoré boli vymazané z osobných informácií použitých na vytvorenie anonymne spracúvaných informácií, a informácií týkajúcich sa realizovaného spôsobu spracovania“.
- (30) Vzhľadom na to, že „anonymne spracúvané osobné informácie“, ako sú vymedzené v zákone APPI, zahŕňajú aj údaje, pri ktorých je stále možná opätovná identifikácia danej fyzickej osoby, mohlo by to znamenať, že osobné údaje prenášané z Európskej únie by mohli prísť o časť dostupnej ochrany prostredníctvom procesu, ktorý by sa podľa nariadenia (EÚ) 2016/679 považoval skôr za formu „pseudonymizácie“ než „anonymizácie“ (čím by sa nezmenila ich povaha ako osobných údajov).
- (31) V záujme riešenia tejto situácie sa v doplňujúcich pravidlách stanovujú dodatočné požiadavky vzťahujúce sa len na osobné údaje prenášané z Európskej únie na základe tohto rozhodnutia. Podľa pravidla 5 doplňujúcich pravidiel sa takéto osobné informácie považujú za „anonymne spracúvané osobné informácie“ v zmysle zákona APPI len vtedy, „ak hospodársky subjekt nakladajúci s osobnými informáciami prijme opatrenia, na základe ktorých bude anonymizácia danej fyzickej osoby nezvratná pre všetkých, a to aj vymazaním informácií týkajúcich sa spôsobu spracovania atď.“ Tieto informácie sú v doplňujúcich pravidlách vymedzené ako informácie týkajúce sa opisov a individuálnych identifikačných kódov, ktoré boli vymazané z osobných informácií použitých na vytvorenie „anonymne spracúvaných informácií“, ako aj informácie týkajúce sa spôsobu spracovania uplatneného pri vymazávaní týchto opisov a individuálnych identifikačných kódov. Inými slovami, v doplňujúcich pravidlách sa vyžaduje, aby hospodársky subjekt, ktorý vytvára „anonymne spracúvané osobné informácie“, zničil „kľúč“ umožňujúci opätovné priradenie daných údajov fyzickej osobe. To znamená, že ustanovenia zákona APPI týkajúce sa „anonymne spracúvaných osobných informácií“ sa budú na osobné údaje pochádzajúce z Európskej únie vzťahovať len v prípadoch, keď by sa za anonymné informácie považovali aj podľa nariadenia (EÚ) 2016/679 ⁽²²⁾.

2.2.5. Vymedzenie pojmu hospodársky subjekt nakladajúci s osobnými informáciami

- (32) Pokiaľ ide o osobnú pôsobnosť, zákon APPI sa vzťahuje len na hospodárske subjekty nakladajúce s osobnými informáciami. Hospodársky subjekt nakladajúci s osobnými informáciami je v článku 2 ods. 5 zákona APPI vymedzený ako „osoba, ktorá poskytuje databázu osobných informácií atď. na účely podnikania“, s výnimkou štátnej správy a správnych orgánov na ústrednej aj miestnej úrovni.
- (33) Podľa usmernení PPC je „podnikanie“ akékoľvek „konanie zamerané na výkon spoločensky uznávanej podnikateľskej činnosti, a to za určitým cieľom, so ziskom alebo aj bez zisku, opakovane a nepretržite“. Organizácie, ktoré nemajú právnu subjektivitu (ako napríklad združenia *de facto*), alebo fyzické osoby sa považujú za hospodárske subjekty nakladajúce s osobnými informáciami, ak pre svoje podnikanie poskytujú (používajú) databázu osobných informácií atď. ⁽²³⁾. Pojem „podnikanie“ v zmysle zákona APPI je teda veľmi široký, keďže zahŕňa nielen ziskové, ale aj neziskové činnosti rôznych druhov organizácií a fyzických osôb. „Na účely podnikania“ sa okrem toho vzťahuje aj na osobné informácie, ktoré sa nepoužívajú vo (vonkajších) obchodných vzťahoch hospodárskeho subjektu, ale interne, ako je napríklad spracúvanie údajov o zamestnancoch.

⁽²²⁾ Pozri nariadenie (EÚ) 2016/679, odôvodnenie 26.

⁽²³⁾ Usmernenia PPC (General Rule Edition), s. 18.

- (34) Pokiaľ ide o prijímateľov ochrany stanovených v zákone APPI, v zákone sa nerobí žiadny rozdiel na základe štátnej príslušnosti, miesta pobytu alebo sídla fyzickej osoby. To isté platí pre možnosti fyzických osôb domáhať sa nápravy, či už u PPC alebo na súde.

2.2.6. Pojmy prevádzkovateľ a sprostredkovateľ

- (35) V rámci zákona APPI sa konkrétne nerozlišuje medzi povinnosťami uloženými prevádzkovateľom a sprostredkovateľom. Neexistencia tohto rozlíšenia nemá vplyv na úroveň ochrany, pretože všetky ustanovenia zákona sa vzťahujú na všetky hospodárske subjekty nakladajúce s osobnými informáciami. Hospodársky subjekt nakladajúci s osobnými informáciami, ktorý zverí nakladanie s osobnými údajmi správcovi (ktorý je ekvivalentom sprostredkovateľa podľa všeobecného nariadenia o ochrane údajov), má aj naďalej povinnosti podľa zákona APPI a doplňujúcich pravidiel týkajúce sa zverených údajov. Podľa článku 22 zákona APPI je okrem toho povinný nad správcom „vykonávať nevyhnutný a primeraný dozor“. Na druhej strane, ako potvrdila PPC, aj samotný správca je viazaný všetkými povinnosťami stanovenými v zákone APPI a v doplňujúcich pravidlách.

2.2.7. Odvetvové výnimky

- (36) V článku 76 zákona APPI sa z uplatňovania kapitoly IV tohto zákona, ktorá zahŕňa hlavné ustanovenia o ochrane údajov (základné zásady, povinnosti hospodárskych subjektov, individuálne práva, dozor zo strany PPC), vynímajú určité druhy spracúvania údajov. Na spracúvanie, na ktoré sa vzťahuje odvetvová výnimka podľa článku 76, sa podľa článku 43 ods. 2 zákona APPI nevzťahujú ani právomoci PPC v oblasti presadzovania práva ⁽²⁴⁾.
- (37) Kategórie relevantné pre odvetvovú výnimku uvedenú v článku 76 zákona APPI sú vymedzené použitím dvojitého kritéria založeného na type hospodárskeho subjektu nakladajúceho s osobnými informáciami a účele spracúvania. Táto výnimka sa konkrétnejšie vzťahuje na: i) vysielačie inštitúcie, vydavateľov novín, komunikačné agentúry alebo iné tlačové organizácie (vrátane všetkých fyzických osôb, ktoré vykonávajú tlačovú činnosť ako svoje podnikanie), pokiaľ spracúvajú osobné informácie na účely tlače; ii) osoby, ktoré sa profesionálne venujú písaniu, pokiaľ to zahŕňa osobné informácie; a iii) univerzity a všetky ostatné organizácie alebo skupiny zamerané na akademické štúdium alebo všetky osoby patriace k takejto organizácii, pokiaľ spracúvajú osobné informácie na účely akademických štúdií; iv) cirkevné organizácie, pokiaľ spracúvajú osobné informácie na účely náboženskej činnosti (vrátane všetkých súvisiacich činností); a v) politické organizácie, pokiaľ spracúvajú osobné informácie na účely svojej politickej činnosti (vrátane všetkých súvisiacich činností). Na spracúvanie osobných informácií na jeden z účelov uvedených v článku 76 inými typmi hospodárskych subjektov nakladajúcich s osobnými informáciami, ako aj spracúvanie osobných informácií jedným z uvedených hospodárskych subjektov nakladajúcich s osobnými informáciami na iné účely, napríklad v súvislosti so zamestnaním, sa naďalej vzťahujú ustanovenia kapitoly IV.
- (38) V záujme zabezpečenia primeranej úrovne ochrany osobných údajov prenášaných z Európskej únie hospodárskym subjektom v Japonsku by sa toto rozhodnutie malo vzťahovať len na spracúvanie osobných informácií, ktoré patria do rozsahu pôsobnosti kapitoly IV zákona APPI – t. j. na spracúvanie hospodárskymi subjektmi nakladajúcimi s osobnými informáciami, pokiaľ daná situácia spracúvania nezodpovedá jednej z odvetvových výnimiek. Jeho rozsah pôsobnosti by sa preto mal zosúladiť s rozsahom pôsobnosti zákona APPI. Podľa informácií poskytnutých PPC, ak by hospodársky subjekt nakladajúci s osobnými informáciami, na ktorého sa vzťahuje toto rozhodnutie, následne zmenil účel použitia (v rozsahu, v akom je to prípustné), pričom by sa naň potom vzťahovala jedna z odvetvových výnimiek uvedených v článku 76 zákona APPI, považovalo by sa to za medzinárodný prenos (keďže v takých prípadoch by sa už na spracúvanie osobných informácií nevzťahovala kapitola IV zákona APPI, a teda by nepatrilo do rozsahu pôsobnosti tohto zákona). To isté by platilo aj v prípade, keď hospodársky subjekt nakladajúci s osobnými informáciami poskytne osobné informácie subjektu, na ktorý sa vzťahuje článok 76 zákona APPI, aby ich použil na jeden z účelov spracúvania uvedených v danom ustanovení. V prípade osobných údajov prenášaných z Európskej únie by to teda predstavovalo následný prenos, na ktorý by sa vzťahovali príslušné záruky (najmä tie, ktoré sú uvedené v článku 24 zákona APPI a doplňujúcim pravidlom 4). Ak by sa hospodársky subjekt nakladajúci s osobnými informáciami spoliehal na súhlas ⁽²⁵⁾ dotknutej osoby, musel by jej poskytnúť všetky potrebné informácie vrátane informácie o tom, že dané osobné informácie už nebudú chránené podľa zákona APPI.

⁽²⁴⁾ Pokiaľ ide o iné hospodárske subjekty, PPC im nesmie pri výkone svojich právomocí v oblasti vyšetrovania a presadzovania práva brániť v uplatňovaní práva na slobodu prejavu, akademickú slobodu, slobodu náboženského vyznania a slobodu politickej činnosti (článok 43 ods. 1 zákona APPI).

⁽²⁵⁾ Ako vysvetlila PPC, súhlas sa v usmerneniach PPC vykladá ako „vyjadrenie úmyslu hlavného subjektu akceptovať, že s jeho osobnými informáciami sa môže nakladať spôsobom uvedeným podnikom nakladajúcim s osobnými informáciami“. V usmerneniach PPC (General Rule Edition, s. 24) sa uvádzajú spôsoby vyjadrenia súhlasu, ktoré sa považujú „v Japonsku za bežné obchodné postupy“, t. j. ústna dohoda, vyplnenie formulárov alebo iných dokumentov, súhlas prostredníctvom e-mailu, zaškrtnutie políčka na webovej stránke, kliknutie na domovskej stránke, použitie tlačidla na vyjadrenie súhlasu, poklopanie po dotykovom displeji atď. Všetky tieto spôsoby predstavujú výslovnú formu súhlasu.

2.3. Záruky, práva a povinnosti

2.3.1. Obmedzenie účelu

- (39) Osobné údaje by sa mali spracúvať na konkrétny účel a následne by sa mali používať len pokiaľ to nie je nezlučiteľné s daným účelom spracúvania. Táto zásada ochrany údajov je zaručená v článkoch 15 a 16 zákona APPI.
- (40) Zákon APPI vychádza zo zásady, že hospodársky subjekt musí určiť účel použitia „čo možno najjasnejšie“ (článok 15 ods. 1) a následne je týmto účelom pri spracúvaní údajov viazaný.
- (41) V tejto súvislosti sa v článku 15 ods. 2 zákona APPI stanovuje, že hospodársky subjekt nakladajúci s osobnými informáciami nesmie zmeniť pôvodný účel „nad rámec, ktorý sa považuje za primerane relevantný vzhľadom na účel použitia pred zmenou“, čo sa v usmerneniach PPC vykladá tak, že musí zodpovedať tomu, čo môže dotknutá osoba objektívne očakávať na základe „bežných spoločenských zvyklostí“⁽²⁶⁾.
- (42) Navyše, podľa článku 16 ods. 1 zákona APPI nesmú hospodárske subjekty nakladajúce s osobnými informáciami s týmito informáciami nakladať nad rámec „rozsahu nevyhnutného na dosiahnutie účelu použitia“ stanoveného v článku 15 bez toho, aby vopred získali súhlas dotknutej osoby, pokiaľ neplatí jedna z výnimiek uvedených v článku 16 ods. 3⁽²⁷⁾.
- (43) Pokiaľ ide o osobné informácie získané od iného hospodárskeho subjektu, hospodársky subjekt nakladajúci s osobnými informáciami môže v zásade voľne stanoviť nový účel použitia⁽²⁸⁾. S cieľom zabezpečiť, aby bol v prípade prenosu z Európskej únie takýto príjemca viazaný účelom, na ktorý boli údaje prenesené, sa v dopĺňujúcom pravidle 3 vyžaduje, že v prípadoch, „keď [hospodársky subjekt nakladajúci s osobnými informáciami] dostane osobné údaje z EÚ na základe rozhodnutia o primeranosti“, alebo ak takýto hospodársky subjekt „dostane osobné údaje, ktoré boli predtým prenesené z EÚ na základe rozhodnutia o primeranosti, od iného [hospodárskeho subjektu nakladajúceho s osobnými informáciami] (ďalšie poskytnutie)“, príjemca musí „konkrétne určiť účel použitia daných osobných údajov v rámci rozsahu účelu použitia, na ktorý boli údaje pôvodne alebo následne prijaté“. Inými slovami, týmto pravidlom sa zaručuje, že v kontexte prenosu bude účel konkrétne určený podľa nariadenia (EÚ) 2016/679 aj naďalej určovať spracúvanie a že na zmenu tohto účelu v ktorejkoľvek fáze spracovateľského reťazca v Japonsku by bol potrebný súhlas dotknutej osoby z EÚ. Na získanie tohto súhlasu sa hospodársky subjekt nakladajúci s osobnými informáciami bude musieť skontaktovať s dotknutou osobou, a ak to nebude možné, jednoducho sa bude musieť zachovať pôvodný účel.

2.3.2. Zákonnosť a čestnosť spracúvania

- (44) Doplnková ochrana uvedená v odôvodnení 43 je o to dôležitejšia, že japonský systém prostredníctvom zásady obmedzenia účelu zabezpečuje aj to, aby sa osobné údaje spracúvali zákonne a čestne.
- (45) Podľa zákona APPI musí hospodársky subjekt nakladajúci s osobnými informáciami pri zhromažďovaní osobných informácií podrobne určiť účel použitia daných osobných informácií⁽²⁹⁾ a bezodkladne o ňom informovať dotknutú osobu (alebo ho zverejniť)⁽³⁰⁾. V článku 17 zákona APPI sa okrem toho uvádza, že hospodársky subjekt nakladajúci s osobnými informáciami nesmie získať osobné informácie podvodom alebo inými nepatričnými prostriedkami. Pokiaľ ide o určité kategórie údajov, ako sú napríklad osobné informácie vyžadujúce osobitnú starostlivosť, na ich získanie je potrebný súhlas dotknutej osoby (článok 17 ods. 2 zákona APPI).

⁽²⁶⁾ V otázkach a odpovediach, ktoré PPC vydala, sa uvádza niekoľko príkladov na ilustráciu tohto pojmu. Príklady situácií, keď je rozsah zmeny primerane relevantný, zahŕňajú najmä používanie osobných informácií získaných od osôb kupujúcich tovar alebo služby v rámci obchodnej transakcie s cieľom informovať tieto osoby o inom relevantnom tovare alebo službách, ktoré sú k dispozícii (napr. prevádzkovateľ posilňovne, ktorý eviduje e-mailové adresy členov, aby ich informoval o kurzoch a programoch). V otázkach a odpovediach sa zároveň uvádza aj príklad situácie, keď zmena účelu použitia nie je prípustná, a to konkrétne keď spoločnosť zašle informácie o svojom tovare a službách na e-mailové adresy, ktoré zhromaždila na účely varovania pred podvodmi alebo krádežou členských kariet.

⁽²⁷⁾ Tieto výnimky môžu vyplývať z iných zákonov a právnych predpisov, alebo sa môžu týkať situácií, v ktorých je nakladanie s osobnými informáciami nevyhnutné i) v záujme „ochrany ľudského života, zdravia alebo majetku“; ii) na „zvýšenie verejnej hygieny alebo podporu rastu zdravých detí“; alebo iii) „v záujme spolupráce s orgánmi alebo subjektmi štátnej správy či s ich zástupcami“ pri výkone ich úloh vyplývajúcich zo zákona. Kategórie i) a ii) sa navyše uplatňujú len v prípade, že je obťažné získať súhlas dotknutej osoby, a kategória iii) len vtedy, ak existuje riziko, že získanie súhlasu dotknutej osoby by bránilo plneniu takýchto úloh.

⁽²⁸⁾ Na základe článku 23 ods. 1 zákona APPI je však na sprístupnenie údajov tretej strane v zásade potrebný súhlas danej fyzickej osoby. Fyzická osoba tak môže vykonávať určitú kontrolu nad používaním svojich údajov iným hospodárskym subjektom.

⁽²⁹⁾ Podľa článku 15 ods. 1 zákona APPI musí byť takéto určenie „čo možno najjasnejšie“.

⁽³⁰⁾ Článok 18 ods. 1 zákona APPI.

- (46) Následne, ako je vysvetlené v odôvodneniach 41 a 42, hospodársky subjekt nakladajúci s osobnými informáciami nesmie spracúvať osobné informácie na iné účely okrem prípadov, keď dotknutá osoba s takýmto spracúvaním súhlasí alebo keď platí jedna z výnimiek podľa článku 16 ods. 3 zákona APPI.
- (47) A napokon, pokiaľ ide o ďalšie poskytovanie osobných informácií tretej strane ⁽³¹⁾, v článku 23 ods. 1 zákona APPI sa takéto sprístupnenie obmedzuje na špecifické prípady, v ktorých je spravidla potrebný predchádzajúci súhlas dotknutej osoby ⁽³²⁾. V článku 23 ods. 2, 3 a 4 zákona APPI sa stanovujú výnimky z požiadavky na získanie súhlasu. Tieto výnimky sa však vzťahujú len na údaje, ktoré nie sú citlivé, pričom sa nimi vyžaduje, aby hospodársky subjekt vopred informoval dotyčné fyzické osoby o úmysle sprístupniť ich osobné informácie tretej strane a o možnosti namietat voči akémukoľvek ďalšiemu sprístupneniu ⁽³³⁾.
- (48) Pokiaľ ide o prenosy z Európskej únie, osobné údaje sa najprv budú musieť zhromaždiť a spracovať v EÚ v súlade s nariadením (EÚ) 2016/679. To bude vždy zahŕňať zhromažďovanie a spracúvanie vrátane spracúvania na účely prenosu z Európskej únie do Japonska na základe jedného z právnych dôvodov uvedených v článku 6 ods. 1 nariadenia na jednej strane a na druhej strane zhromažďovanie na konkrétne určený, výslovne uvedený a oprávnený účel, ako aj zákaz ďalšieho spracúvania, okrem iného aj formou prenosu, spôsobom, ktorý je nezlučiteľný s týmto účelom, ako je stanovené v článku 5 ods. 1 písm. b) a článku 6 ods. 4 nariadenia.
- (49) Podľa doplňujúceho pravidla 3 bude musieť hospodársky subjekt nakladajúci s osobnými informáciami, ktorý údaje dostane, po prenose „potvrdiť“ konkrétny účel, resp. účely, na ktoré sa prenos uskutočnil [t. j. účel konkrétne určený podľa nariadenia (EÚ) 2016/679], a ďalej spracúvať tieto údaje v súlade s týmto účelom, resp. účelmi ⁽³⁴⁾. To znamená, že nielen pôvodný príjemca takýchto osobných údajov v Japonsku, ale aj každý budúci príjemca týchto údajov (vrátane správcu) je viazaný účelom, resp. účelmi konkrétne určenými na základe nariadenia.
- (50) Okrem toho, keby hospodársky subjekt nakladajúci s osobnými informáciami chcel zmeniť účel, ktorý bol predtým konkrétne určený podľa nariadenia (EÚ) 2016/679, musel by podľa článku 16 ods. 1 zákona APPI v zásade získať súhlas dotknutej osoby. Bez tohto súhlasu by každé spracúvanie údajov nad rámec rozsahu nevyhnutného na dosiahnutie tohto účelu použitia predstavovalo porušenie článku 16 ods. 1, ktoré by bolo vymáhateľné PPC a súdmi.
- (51) Teda, vzhľadom na to, že podľa nariadenia (EÚ) 2016/679 je na prenos potrebný platný právny základ a konkrétne určený účel, ktoré sa odzrkadľujú v účele použitia „potvrdenom“ podľa zákona APPI, kombináciou príslušných ustanovení zákona APPI a doplňujúceho pravidla 3 sa zabezpečuje, že spracúvanie údajov z EÚ v Japonsku bude naďalej v súlade so zákonom.

2.3.3. Presnosť a minimalizácia údajov

- (52) Údaje by mali byť presné a v prípade potreby by sa mali aktualizovať. Zároveň by mali byť primerané, relevantné a nie nadmerné vo vzťahu k účelom, na ktoré sa spracúvajú.
- (53) Tieto zásady sú v japonskom právnom poriadku zabezpečené článkom 16 ods. 1 zákona APPI, ktorým sa zakazuje nakladanie s osobnými informáciami nad rámec „rozsahu nevyhnutného na dosiahnutie účelu použitia“. Ako vysvetlila PPC, to nielenže vylučuje používanie údajov, ktoré nie sú primerané, a nadmerné používanie údajov (nad rámec toho, čo je nevyhnutné na dosiahnutie účelu použitia), ale zahŕňa to aj zákaz nakladania s údajmi, ktoré nie sú relevantné z hľadiska dosiahnutia účelu použitia.

⁽³¹⁾ Hoci sú správcovia na účely uplatňovania článku 23 z rozsahu pojmu „tretia strana“ vylúčení (pozri odsek 5), toto vylúčenie sa uplatňuje len pokiaľ správca nakladá s osobnými údajmi v medziach poverenia („v rámci rozsahu nevyhnutného na dosiahnutie účelu použitia“), t. j. koná ako sprostredkovateľ.

⁽³²⁾ Medzi ďalšie (výnimočné) dôvody patrí: i) poskytovanie osobných informácií „na základe zákonov a iných právnych predpisov“; ii) prípady, „v ktorých je potrebné chrániť ľudský život, zdravie alebo majetok a v ktorých je obťažné získať súhlas hlavného subjektu“; iii) prípady, „v ktorých je osobitne potrebné zvýšiť verejnú hygienu alebo podporovať zaistenie zdravia detí a v ktorých je obťažné získať súhlas hlavného subjektu“; a iv) prípady, „v ktorých treba spolupracovať s organizáciou ústrednej štátnej správy alebo miestnej samosprávy či osobou, ktorú táto organizácia alebo samospráva poverili plnením úloh predpísaných zákonmi a inými právnymi predpismi, a v ktorých existuje možnosť, že získanie súhlasu hlavného subjektu by bránilo plneniu uvedených úloh“.

⁽³³⁾ Medzi informácie, ktoré sa majú poskytovať, patria najmä kategórie osobných údajov, ktoré sa majú poskytnúť tretej strane, a spôsob prenosu. Hospodársky subjekt nakladajúci s osobnými informáciami musí okrem toho informovať dotknutú osobu o možnosti namietat voči prenosu a o spôsobe podania takejto žiadosti.

⁽³⁴⁾ Podľa článku 26 ods. 1 bodu ii) zákona APPI sa od hospodárskeho subjektu nakladajúceho s osobnými informáciami vyžaduje, aby pri prijímaní osobných údajov od tretej strany „potvrdil“ (overil) „údaje o získaní osobných údajov treťou stranou“ vrátane účelu tohto získania. Hoci sa v článku 26 výslovne neuvádza, že hospodársky subjekt nakladajúci s osobnými informáciami sa následne musí týmto účelom riadiť, doplňujúcim pravidlom 3 sa to výslovne vyžaduje.

- (54) Pokiaľ ide o povinnosť uchovávať údaje presné a aktualizované, v článku 19 zákona APPI sa vyžaduje, aby sa hospodársky subjekt nakladajúci s osobnými informáciami „usiloval o to, aby boli osobné údaje udržiavané presné a aktualizované, a to v rozsahu nevyhnutnom na dosiahnutie účelu použitia“. Toto ustanovenie by sa malo vykladať spolu s článkom 16 ods. 1 zákona APPI: podľa vysvetlení poskytnutých PPC, ak hospodársky subjekt nakladajúci s osobnými informáciami nedodríava predpísané normy presnosti, spracúvanie osobných informácií sa nebude považovať za spracúvanie, pri ktorom sa dosahuje účel použitia, a preto sa nakladanie s údajmi z jeho strany stane v zmysle článku 16 ods. 1 nezákonným.

2.3.4. Obmedzenie uchovávania

- (55) Údaje by sa v zásade nemali uchovávať dlhšie, než je potrebné na účely, na ktoré sa osobné údaje spracúvajú.
- (56) Podľa článku 19 zákona APPI sa hospodárske subjekty nakladajúce s osobnými informáciami musia „usilovať [...] bezodkladne vymazať osobné údaje, keď už takéto použitie nebude nutné“. Uvedené ustanovenie sa musí vykladať v spojení s článkom 16 ods. 1 zákona APPI, ktorým sa zakazuje nakladať s osobnými informáciami nad rámec „rozsahu nevyhnutného na dosiahnutie účelu použitia“. Po dosiahnutí účelu použitia sa už spracúvanie osobných informácií nemôže považovať za nevyhnutné, a teda nemôže pokračovať (pokiaľ hospodársky subjekt nakladajúci s osobnými informáciami nezíska súhlas dotknutej osoby s ich ďalším spracúvaním).

2.3.5. Bezpečnosť údajov

- (57) 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 hospodárske subjekty mali prijať vhodné technické alebo organizačné opatrenia na ochranu osobných údajov pred možnými hrozbami. Tieto opatrenia by sa mali posudzovať s prihliadnutím na stav techniky a súvisiace náklady.
- (58) Táto zásada sa v japonskom právnom poriadku vykonáva článkom 20 zákona APPI, v ktorom sa stanovuje, že hospodársky subjekt nakladajúci s osobnými informáciami „prijme potrebné a primerané opatrenia na kontrolu bezpečnosti osobných údajov vrátane opatrení na zabránenie úniku, strate alebo poškodeniu osobných údajov, s ktorými nakladá.“ V usmerneniach PPC sa vysvetľujú opatrenia, ktoré sa majú prijať, vrátane spôsobov stanovenia základných politík, pravidiel nakladania s údajmi a rôznych „kontrolných opatrení“ (pokiaľ ide o organizačnú bezpečnosť, ako aj bezpečnosť ľudí, fyzickú a technologickú bezpečnosť)⁽³⁵⁾. V usmerneniach PPC a v osobitnom oznámení (dodatok 8 „Obsah opatrení v oblasti riadenia bezpečnosti, ktoré treba prijať“), ktoré uverejnila PPC, sa okrem toho uvádzajú ďalšie podrobnosti o opatreniach týkajúcich sa bezpečnostných incidentov, medzi ktoré patrí napríklad únik osobných informácií, prijímaných v rámci opatrení v oblasti riadenia bezpečnosti, ktoré majú hospodárske subjekty nakladajúce s osobnými informáciami prijať⁽³⁶⁾.
- (59) Okrem toho, podľa článkov 20 a 21 zákona APPI treba vždy, keď s osobnými informáciami nakladajú zamestnanci alebo subdodávatelia, zaistiť „nevyhnutný a primeraný dozor na účely kontroly bezpečnosti“. A napokon, na základe článku 83 zákona APPI sa úmyselný únik alebo krádež osobných informácií trestajú odňatím slobody s dĺžkou trvania až jeden rok.

2.3.6. Transparentnosť

- (60) Dotknuté osoby by mali byť informované o hlavných znakoch spracúvania ich osobných údajov.
- (61) V článku 18 ods. 1 zákona APPI sa požaduje, aby hospodársky subjekt nakladajúci s osobnými informáciami poskytol dotknutej osobe informácie o účele použitia získaných osobných informácií s výnimkou „prípadov, keď bol účel použitia vopred zverejnený“. Tá istá povinnosť sa vzťahuje aj na prípad prípustnej zmeny účelu (článok 18 ods. 3). Tým sa tiež zabezpečí, aby dotknutá osoba bola informovaná o skutočnosti, že jej údaje boli zhromaždené. Hoci sa v zákone APPI od hospodárskeho subjektu nakladajúceho s osobnými informáciami vo všeobecnosti nevyžaduje, aby v štádiu zhromažďovania údajov informoval dotknutú osobu o predpokladaných príjemcoch osobných informácií, takéto informácie sú nevyhnutnou podmienkou akéhokoľvek následného sprístupnenia informácií tretej strane (príjemcovi) na základe článku 23 ods. 2, teda ak k nemu dochádza bez predchádzajúceho súhlasu dotknutej osoby.

⁽³⁵⁾ Usmernenia PPC (General Rule Edition), s. 41 a s. 86 až 98.

⁽³⁶⁾ Podľa oddielu 3-3-2 usmernení PPC musí hospodársky subjekt nakladajúci s osobnými informáciami v prípade takéhoto úniku, poškodenia alebo straty vykonať potrebné vyšetrovania, a najmä posúdiť rozsah porušenia práv a záujmov fyzickej osoby, ako aj povahu a objem dotknutých osobných informácií.

- (62) Pokiaľ ide o „uchovávané osobné údaje“, v článku 27 zákona APPI sa stanovuje, že hospodársky subjekt nakladajúci s osobnými informáciami informuje dotknutú osobu o svojej totožnosti (kontaktných údajoch), o účele použitia a o postupoch na poskytnutie odpovede na žiadosť týkajúcu sa individuálnych práv dotknutej osoby podľa článkov 28, 29 a 30 zákona APPI.
- (63) Ako sa stanovuje v doplňujúcich pravidlách, osobné údaje prenášané z Európskej únie sa budú považovať za „uchovávané osobné údaje“ bez ohľadu na lehotu ich uchovávania (pokiaľ sa na ne nebudú vzťahovať výnimky) a budú vždy podliehať požiadavkám na transparentnosť podľa oboch uvedených ustanovení.
- (64) Na požiadavky uvedené v článku 18, ako aj na povinnosť informovať o účele použitia podľa článku 27 zákona APPI sa vzťahuje rovnaký súbor výnimiek, ktoré vychádzajú predovšetkým z dôvodov verejného záujmu a ochrany práv a záujmov dotknutej osoby, tretích strán a prevádzkovateľa⁽³⁷⁾. Podľa výkladu uvedeného v usmerneniach PPC sa dané výnimky uplatňujú vo veľmi špecifických situáciách, napríklad keď by informácie o účele použitia mohli ohroziť legitímne opatrenia, ktoré hospodársky subjekt prijal na ochranu určitých záujmov (napríklad boj proti podvodu, priemyselná špionáž, sabotáž).

2.3.7. Osobitné kategórie údajov

- (65) Na spracúvanie „osobitných kategórií“ údajov by sa mali vzťahovať osobitné záruky.
- (66) V článku 2 ods. 3 zákona APPI sú vymedzené „osobné informácie vyžadujúce osobitnú starostlivosť“. Uvedené ustanovenie sa týka „osobných informácií zahŕňajúcich rasový pôvod hlavného subjektu, jeho presvedčenie, spoločenské postavenie, anamnézu, záznam vedený v registri trestov, skutočnosť, že daná osoba utrpela ujmu v dôsledku trestného činu, alebo iných informácií atď., ktoré sú v nariadení vlády vymedzené ako informácie, s ktorými treba nakladať s osobitnou starostlivosťou, aby hlavný subjekt nebol vystavený nespravodlivej diskriminácii, predsudkom alebo inému znevýhodneniu.“ Tieto kategórie vo veľkej miere zodpovedajú zoznamu citlivých údajov uvedenému v článkoch 9 a 10 nariadenia (EÚ) 2016/679. „Anamnéza“ konkrétne zodpovedá údajom o zdravotnom stave, zatiaľ čo „záznam vedený v registri trestov a skutočnosť, že daná osoba utrpela ujmu v dôsledku trestného činu“ v podstate zodpovedajú kategóriám uvedeným v článku 10 nariadenia (EÚ) 2016/679. Kategórie uvedené v článku 2 ods. 3 zákona APPI sú podrobnejšie vyložené v nariadení vlády a v usmerneniach PPC. Podľa oddielu 2.3 bodu 8 usmernení PPC sa podkategórie „anamnézy“ uvedené v článku 2 bodoch ii) a iii) nariadenia vlády vykladajú tak, že sa vzťahujú na genetické a biometrické údaje. Aj keď v zozname nie sú výslovne zahrnuté pojmy „etnický pôvod“ a „politický názor“, spomína sa v ňom „rasový pôvod“ a „presvedčenie“. Ako sa vysvetľuje v oddiele 2.3 bodoch 1 a 2 usmernení PPC, odkaz na „rasový pôvod“ zahŕňa „etnické väzby alebo väzby na určitú časť sveta“, zatiaľ čo „presvedčenie“ sa chápe tak, že zahŕňa náboženské presvedčenie aj politické názory.
- (67) Ako jednoznačne vyplýva zo znenia uvedeného ustanovenia, nejde o uzavretý zoznam, keďže doň možno doplniť ďalšie kategórie údajov, pokiaľ je s ich spracúvaním spojené riziko „nespravodlivej diskriminácie, predsudkov alebo iného znevýhodnenia hlavného subjektu“.
- (68) Hoci je pojem „citlivé“ údaje vo svojej podstate spoločenským konštruktom, keďže vychádza z kultúrnych a právnych tradícií, morálnych úvah, politických rozhodnutí atď. danej spoločnosti, vzhľadom na dôležitosť zabezpečenia primeraných záruk vo vzťahu k citlivým údajom pri ich prenose hospodárskym subjektom v Japonsku, Komisia dosiahla, že osobitná ochrana, ktorá sa podľa japonského práva poskytuje „osobným informáciám vyžadujúcim osobitnú starostlivosť“, sa rozšíri na všetky kategórie, ktoré sú v nariadení (EÚ) 2016/679 uznané za „citlivé údaje“. Na tento účel sa v doplňujúcom pravidle 1 stanovuje, že hospodárske subjekty nakladajúce s osobnými informáciami spracúvajú údaje prenesené z Európskej únie týkajúce sa sexuálneho života fyzickej osoby, jej sexuálnej orientácie alebo členstva v odborových organizáciách „takým istým spôsobom ako osobné informácie vyžadujúce osobitnú starostlivosť v zmysle článku 2 ods. 3 [zákona APPI]“.

⁽³⁷⁾ Ide o i) prípady, v ktorých existuje možnosť, že informovanie dotknutej osoby o účele použitia alebo zverejnenie tohto účelu by „poškodilo život, zdravie, majetok alebo iné práva a záujmy hlavného subjektu alebo tretej strany“ alebo „práva alebo oprávnené záujmy [...] hospodárskeho subjektu nakladajúceho s osobnými informáciami“; ii) prípady, v ktorých „treba spolupracovať s organizáciou ústrednej štátnej správy alebo miestnej samosprávy“ pri plnení ich úloh podľa zákona a v ktorých by takéto informácie alebo sprístupnenie bránili plneniu takýchto úloh; iii) prípady, v ktorých účel použitia jasne vyplýva zo situácie, v ktorej boli údaje získané.

- (69) Pokiaľ ide o dodatočné vecné záruky, ktoré sa vzťahujú na osobné informácie vyžadujúce osobitnú starostlivosť, podľa článku 17 ods. 2 zákona APPI nesmú hospodárske subjekty nakladajúce s osobnými informáciami získavať takýto druh údajov bez predchádzajúceho súhlasu dotyčnej fyzickej osoby, pričom sa na to vzťahujú len obmedzené výnimky⁽³⁸⁾. Táto kategória osobných informácií je navyše vylúčená z možnosti sprístupnenia tretím stranám na základe postupu stanoveného v článku 23 ods. 2 zákona APPI (ktorý umožňuje prenos údajov tretím stranám bez predchádzajúceho súhlasu dotyčnej fyzickej osoby).

2.3.8. Zodpovednosť

- (70) 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.
- (71) Ako sa uvádza v poznámke pod čiarou č. 34 (odôvodnenie 49), hospodárske subjekty nakladajúce s osobnými informáciami sú podľa článku 26 ods. 1 zákona APPI povinné overiť totožnosť tretej strany, ktorá im poskytuje osobné údaje, a „okolnosti“, za akých daná tretia strana takéto údaje získala (v prípade osobných údajov, na ktoré sa vzťahuje toto rozhodnutie, tieto okolnosti podľa zákona APPI a doplňujúceho pravidla 3 zahŕňajú skutočnosť, že údaje pochádzajú z Európskej únie, ako aj účel pôvodného prenosu údajov). Cieľom tohto opatrenia je okrem iného zabezpečiť zákonnosť spracúvania údajov v celom reťazci hospodárskych subjektov nakladajúcich s osobnými informáciami, ktoré s uvedenými osobnými údajmi nakladajú. Navyše, podľa článku 26 ods. 3 zákona APPI sú hospodárske subjekty nakladajúce s osobnými informáciami povinné viesť záznamy o dátume prijatia a (povinných) informáciách prijatých od tretej strany podľa odseku 1, ako aj o mene dotyčnej fyzickej osoby (dotknutej osoby), kategóriách spracúvaných údajov a v relevantnom rozsahu aj o skutočnosti, že dotknutá osoba udelila súhlas s poskytnutím svojich osobných údajov. Ako sa uvádza v článku 18 pravidiel PPC, tieto záznamy sa musia v závislosti od okolností uchovávať minimálne počas lehoty jedného až troch rokov. PPC môže pri výkone svojich úloh požadovať predloženie takýchto záznamov⁽³⁹⁾.
- (72) Hospodárske subjekty nakladajúce s osobnými informáciami musia bezodkladne a vhodne riešiť sťažnosti dotknutých fyzických osôb týkajúce sa spracúvania ich osobných informácií. V záujme ľahšieho vybavovania sťažností zriadiť „systém potrebný na dosiahnutie [tohto] účelu“, z čoho vyplýva, že by mali v rámci svojej organizácie zaviesť vhodné postupy (napríklad stanoviť povinnosti alebo zabezpečiť kontaktné miesto).
- (73) A napokon, zákonom APPI sa vytvára rámec pre účasť odvetvových organizácií na zabezpečovaní vysokej miery súladu (pozri kapitolu IV oddiel 4). Úlohou takýchto akreditovaných organizácií pre ochranu osobných informácií⁽⁴⁰⁾ je presadzovať ochranu osobných informácií poskytovaním podpory podnikom v podobe svojich odborných znalostí, ale aj prispievať k implementácii záruk, najmä prostredníctvom vybavovania jednotlivých sťažností a pomoci pri riešení súvisiacich sporov. Na tento účel môžu prípadne požiadať zúčastnené hospodárske subjekty nakladajúce s osobnými informáciami, aby prijali nevyhnutné opatrenia⁽⁴¹⁾. Okrem toho, v prípade porušenia ochrany údajov alebo iných bezpečnostných incidentov musia hospodárske subjekty nakladajúce s osobnými informáciami v zásade informovať o tejto skutočnosti PPC, ako aj dotknutú osobu (alebo verejnosť) a prijať potrebné opatrenia vrátane opatrení na minimalizovanie akýchkoľvek škôd a zabránenie opätovnému výskytu podobných incidentov⁽⁴²⁾. Hoci ide o dobrovoľné režimy, k 10. augustu 2017 PPC evidovala 44 organizácií, pričom len najväčšia, Japonské centrum pre spracúvanie a vývoj informácií (JIPDEC), mala 15 436 členov z radov

⁽³⁸⁾ Uplatňujú sa tieto výnimky: i) „prípady vychádzajúce zo zákonov a iných právnych predpisov“; ii) „prípady, v ktorých je potrebné chrániť ľudský život, zdravie alebo majetok a v ktorých je obťažné získať súhlas hlavného subjektu“; iii) „prípady, v ktorých je osobitne potrebné zvýšiť verejnú hygienu alebo podporovať zaistenie zdravia detí a v ktorých je obťažné získať súhlas hlavného subjektu“; iv) „prípady, v ktorých treba spolupracovať s organizáciou ústrednej štátnej správy alebo miestnej samosprávy či s osobou, ktorú táto organizácia alebo samospráva poverili plnením úloh predpísaných zákonmi a inými právnymi predpismi, a v ktorých existuje možnosť, že získanie súhlasu hlavného subjektu by bránilo plneniu uvedených úloh“; a v) prípady, v ktorých dané osobné informácie vyžadujúce osobitnú starostlivosť sprístupní dotknutá osoba, organizácia štátnej správy, miestna samospráva, osoba patriaca do jednej z kategórií uvedených v článku 76 ods. 1 alebo iné osoby podľa pravidiel PPC. Ďalšia kategória sa týka „iných prípadov, ktoré sú podľa nariadenia vlády rovnocenné s prípadmi uvedenými v jednotlivých predchádzajúcich bodoch“ a na základe platného nariadenia vlády zahŕňa najmä zrejme znaky určitej osoby (napr. viditeľný zdravotný stav), ak boli citlivé údaje získané (neúmyselne) prostredníctvom vizuálneho pozorovania, filmovania alebo fotografovania dotknutej osoby, napr. kamerovým systémom (CCTV).

⁽³⁹⁾ Podľa článku 40 ods. 1 zákona APPI môže PPC požadovať, pokiaľ je to potrebné v záujme vykonávania príslušných ustanovení zákona APPI, aby hospodársky subjekt nakladajúci s osobnými informáciami predložil potrebné informácie alebo materiály týkajúce sa nakladania s osobnými informáciami.

⁽⁴⁰⁾ V zákone APPI sa okrem iného stanovujú pravidlá akreditácie takýchto organizácií; pozri články 47 – 50 zákona APPI.

⁽⁴¹⁾ Článok 52 zákona APPI.

⁽⁴²⁾ Oznámenie PPC č. 1/2017 „o opatreniach, ktoré sa majú prijať v prípadoch, keď došlo k porušeniu ochrany osobných údajov alebo inému incidentu“.

zúčastnených hospodárskych subjektov⁽⁴³⁾. Medzi akreditované organizácie režimy patria odvetvové združenia, ako je napríklad Japonské združenie obchodníkov s cennými papiermi, Japonské združenie autoškôl alebo Združenie sprostredkovateľov manželstva⁽⁴⁴⁾.

- (74) Akreditované organizácie pre ochranu osobných informácií predkladajú výročné správy o svojej činnosti. Podľa „Prehľadu o stave vykonávania zákona APPI v účtovnom roku 2015“, ktorý zverejnila PPC, dostali akreditované organizácie pre ochranu osobných informácií celkovo 442 sťažností, vyžiadali si 123 vysvetlení od hospodárskych subjektov v ich jurisdikcii, v 41 prípadoch požiadali tieto hospodárske subjekty o predloženie dokumentov, vydali 181 pokynov a dve odporúčania⁽⁴⁵⁾.

2.3.9. Obmedzenia týkajúce sa následných prenosov

- (75) Úroveň ochrany osobných údajov prenášaných z Európskej únie hospodárskym subjektom v Japonsku nesmie byť oslabená ďalším prenosom takýchto údajov príjemcom v tretej krajine mimo Japonska. Takéto „následné prenosy“, ktoré z hľadiska japonského hospodárskeho subjektu predstavujú medzinárodné prenosy z Japonska, by sa mali povoliť len v prípade, že ďalší príjemca mimo Japonska takisto podlieha pravidlám zabezpečujúcim podobnú úroveň ochrany, aká je zaručená v japonskom právnom poriadku.
- (76) Prvá ochrana je zakotvená v článku 24 zákona APPI, ktorým sa vo všeobecnosti zakazuje prenos osobných údajov tretej strane mimo územia Japonska bez predchádzajúceho súhlasu dotyčnej fyzickej osoby. Doplnujúcim pravidlom 4 sa zabezpečuje, že v prípade prenosov údajov z Európskej únie bude takýto súhlas obzvlášť dobre informovaný, keďže sa ním vyžaduje, aby sa dotyčným fyzickým osobám „poskytovali informácie o okolnostiach spojených s prenosom, ktoré sú potrebné na to, aby sa hlavný subjekt mohol rozhodnúť, či súhlas udelí“. Dotknutá osoba bude na tomto základe informovaná o skutočnosti, že údaje sa budú prenášať do zahraničia (mimo rozsahu pôsobnosti zákona APPI), a o konkrétnej cieľovej krajine. To jej umožní posúdiť riziko narušenia súkromia spojené s prenosom. Ako možno vyvodiť z článku 23 zákona APPI (pozri odôvodnenie 47), informácie poskytnuté hlavnému subjektu by mali zahŕňať aj povinné položky podľa odseku 2 uvedeného článku, teda kategórie osobných údajov poskytovaných tretej strane a spôsob sprístupnenia.
- (77) V článku 24 zákona APPI uplatňovaného spolu s článkom 11-2 pravidiel PPC sa stanovuje niekoľko výnimiek z tohto pravidla založeného na udelení súhlasu. Navyše, podľa článku 24 platia rovnaké výnimky, ako sú tie, ktoré sa uplatňujú podľa článku 23 ods. 1 zákona APPI, aj na medzinárodné prenosy údajov⁽⁴⁶⁾.
- (78) Na zabezpečenie kontinuity ochrany v prípade osobných údajov prenášaných z Európskej únie do Japonska podľa tohto rozhodnutia sa doplnujúcim pravidlom 4 zvyšuje úroveň ochrany vzťahujúca sa na následné prenosy takýchto údajov uskutočňované hospodárskym subjektom nakladajúcim s osobnými informáciami príjemcovi z tretej krajiny. Deje sa tak obmedzením a vymedzením základov pre medzinárodné prenosy, ktoré môže hospodársky subjekt nakladajúci s osobnými údajmi použiť ako alternatívu k súhlasu. Konkrétnejšie a bez toho, aby boli dotknuté výnimky stanovené v článku 23 ods. 1 zákona APPI, osobné údaje prenášané na základe tohto rozhodnutia sa môžu bez súhlasu (následne) prenášať iba v dvoch prípadoch: i) keď sa údaje zasielajú do tretej krajiny, ktorú PPC uznala podľa článku 24 zákona APPI za krajinu, ktorá zabezpečuje úroveň ochrany zodpovedajúcu úrovni zaručenej v Japonsku⁽⁴⁷⁾ alebo ii) keď hospodársky subjekt nakladajúci s osobnými informáciami a príjemca, ktorý je treťou stranou, spoločne zaviedli opatrenia zabezpečujúce úroveň ochrany zodpovedajúcu ochrane podľa zákona APPI vykladaného spolu s doplnujúcimi pravidlami, a to prostredníctvom zmluvy, iných foriem záväzných dohôd alebo záväzných dojednaní v rámci skupiny podnikov. Druhá kategória zodpovedá nástrojom používaným podľa nariadenia (EÚ) 2016/679 s cieľom zabezpečiť primerané záruky (najmä zmluvným doložkám a záväzným vnútropodnikovým pravidlami). Navyše, ako potvrdila PPC, dokonca aj v týchto prípadoch prenos naďalej podlieha všeobecným pravidlám, ktoré sa vzťahujú na každé poskytnutie osobných údajov tretej strane na základe zákona APPI (t. j. požiadavke na získanie súhlasu podľa článku 23 ods. 1 alebo prípadne požiadavke na informovanie s možnosťou neuplatňovania podľa článku 23 ods. 2 zákona APPI). V prípade, že sa s dotknutou

⁽⁴³⁾ Podľa údajov uverejnených na webovom sídle PrivacyMark organizácie JIPDEC z 2. októbra 2017.

⁽⁴⁴⁾ PPC, Zoznam akreditovaných organizácií pre ochranu osobných informácií je k dispozícii na adrese: <https://www.ppc.go.jp/personal/nintei/list/> or https://www.ppc.go.jp/files/pdf/nintei_list.pdf

⁽⁴⁵⁾ PPC, Prehľad o stave vykonávania zákona APPI v účtovnom roku 2015 (október 2016), dostupný (len v japončine) na stránke: https://www.ppc.go.jp/files/pdf/personal_sekougaiyou_27ppc.pdf

⁽⁴⁶⁾ Pozri poznámku pod čiarou č. 32.

⁽⁴⁷⁾ Podľa článku 11 pravidiel PPC si to vyžaduje nielen hmotnoprávne normy rovnocenné so zákonom APPI, ktoré podliehajú účinnému dozoru nezávislého orgánu presadzovania, ale aj to, aby bolo v tretej krajine zabezpečené vykonávanie príslušných pravidiel.

osobou nie je možné skontaktovať v súvislosti so žiadosťou o súhlas alebo s cieľom poskytnúť požadované predbežné informácie podľa článku 23 ods. 2 APPI, prenos sa nesmie uskutočniť.

- (79) Preto sa, s výnimkou prípadov, v ktorých PPC konštatovala, že predmetná tretia krajina zabezpečuje úroveň ochrany zodpovedajúcu ochrane zaručenej zákonom APPI ⁽⁴⁸⁾, požiadavkami stanovenými v doplňujúcom pravidle 4 vylučuje možnosť použiť nástroje na prenos, ktorými sa nevytvára záväzný vzťah medzi japonským vývozom údajov a dovozom údajov z tretej krajiny a ktoré nezaručujú požadovanú úroveň ochrany. Týka sa to napríklad systému pravidiel cezhraničnej ochrany súkromia v rámci Ázijsko-tichomorskej hospodárskej spolupráce (APEC Cross Border Privacy Rules – CBPR), na ktorom sa Japonsko zúčastňuje ⁽⁴⁹⁾, keďže v tomto systéme ochrana nevyplýva z dohody zaväzujúcej vývozcu a dovozcu v kontexte ich dvojstranného vzťahu a je jednoznačne na nižšej úrovni ako ochrana zaručená kombináciou zákona APPI a doplňujúcich pravidiel ⁽⁵⁰⁾.
- (80) A napokon, ďalšia záruka v prípade (následných) prenosov vyplýva z článkov 20 a 22 zákona APPI. Podľa týchto ustanovení, ak hospodársky subjekt z tretej krajiny (dovozca údajov) koná v mene hospodárskeho subjektu nakladajúceho s osobnými informáciami (vývozca údajov), to znamená ako (sub-) sprostredkovateľ, vývozca údajov musí zabezpečiť dozor nad dovozom údajov, pokiaľ ide o bezpečnosť spracúvania údajov.

2.3.10. Individuálne práva

- (81) Rovnako ako právne predpisy EÚ v oblasti ochrany údajov aj zákon APPI zaručuje fyzickým osobám celý rad vymožitelných práv. Ide okrem iného o právo na prístup („sprístupnenie“), opravu a výmaz, ako aj o právo namietat („ukončenie používania“).
- (82) Po prvé, podľa článku 28 ods. 1 a 2 zákona APPI má dotknutá osoba právo požiadať hospodársky subjekt nakladajúci s osobnými informáciami o „sprístupnenie uchovávaných osobných údajov, na základe ktorých ju možno identifikovať“ a hospodársky subjekt nakladajúci s osobnými informáciami po prijatí takejto žiadosti dotknutej osobe „[...] sprístupní uchovávané osobné údaje“. Články 29 (právo na opravu) a 30 (právo na ukončenie používania) majú rovnakú štruktúru ako článok 28.
- (83) V článku 9 nariadenia vlády sa uvádza, že sprístupnenie osobných informácií podľa článku 28 ods. 2 zákona APPI prebieha v písomnej forme, pokiaľ sa hospodársky subjekt nakladajúci s osobnými informáciami a dotknutá osoba nedohodli inak.
- (84) Na tieto práva sa vzťahujú tri druhy obmedzení, ktoré sa týkajú práv a záujmov danej fyzickej osoby alebo práv a záujmov tretej strany ⁽⁵¹⁾, závažného zasahovania do podnikateľskej činnosti hospodárskeho subjektu nakladajúceho s osobnými informáciami ⁽⁵²⁾, ako aj prípadov, v ktorých by sa sprístupnením porušili iné zákony alebo právne predpisy ⁽⁵³⁾. Situácie, v ktorých by sa tieto obmedzenia uplatňovali, sú podobné niektorým výnimkám uplatniteľným podľa článku 23 ods. 1 nariadenia (EÚ) 2016/679, ktorým sa umožňuje obmedzenie práv fyzických

⁽⁴⁸⁾ PPC zatiaľ ešte neprijala žiadne rozhodnutie podľa článku 24 zákona APPI, ktorým by uznala úroveň ochrany poskytovanej treťou krajinou za zodpovedajúcu úrovni zaručenej v Japonsku. Jediné rozhodnutie, o prijatí ktorého v súčasnosti uvažuje, sa týka EHP. Pokiaľ ide o prípadné ďalšie rozhodnutia v budúcnosti, Komisia bude situáciu podrobne monitorovať a v prípade potreby prijme vhodné opatrenia s cieľom riešiť prípadné nepriaznivé účinky na kontinuitu ochrany (pozri odôvodnenia 176, 177, 184 a článok 3 ods. 1 ďalej).

⁽⁴⁹⁾ Hoci v rámci systému CBPR organizácie APEC získali osvedčenie iba dve japonské spoločnosti (pozri https://english.jipdec.or.jp/sp/protection_org/cbpr/list.html). Mimo Japonska získal v rámci tohto systému osvedčenie len malý počet (23) spoločností z USA (pozri <https://www.trustarc.com/consumer-resources/trusted-directory/#apec-list>).

⁽⁵⁰⁾ Nie sú napríklad vymedzené citlivé údaje a osobitná ochrana citlivých údajov, nie je stanovená povinnosť obmedzeného uchovávania údajov. Pozri aj stanovisko 02/2014 pracovnej skupiny zriadenej podľa článku 29 k referenčným požiadavkám na záväzné vnútro-podnikové pravidlá, ktoré bolo predložené vnútroštátnym orgánom pre ochranu osobných údajov v EÚ, a cezhraničné pravidlá ochrany súkromia, ktoré boli 6. marca 2014 predložené subjektom organizácie APEC zodpovedným za pravidlá cezhraničnej ochrany súkromia.

⁽⁵¹⁾ Podľa PPC môžu byť dôvodom na obmedzenie iba také záujmy, ktoré je „hodné chrániť právnymi prostriedkami“. Túto skutočnosť treba posúdiť jednotlivo „s ohľadom na zásah do základného práva na súkromie vrátane ochrany údajov, ako sa uznáva v ústave a judikatúre.“ Medzi chránené záujmy môže napríklad patriť obchodné tajomstvo alebo iné tajomstvá v súvislosti s podnikaním.

⁽⁵²⁾ Pojem „závažné zasahovanie do riadneho výkonu podnikateľskej činnosti hospodárskeho subjektu“ sa v usmerneniach PPC ilustruje rôznymi príkladmi, napríklad opakovanými a totožnými komplexnými žiadosťami tej istej fyzickej osoby, keď takéto žiadosti predstavujú pre hospodársky subjekt značnú záťaž, ktorá by ohrozila jeho schopnosť odpovedať na iné žiadosti [usmernenia PPC (General Rule Edition), s. 62]. PPC vo všeobecnosti potvrdila, že táto kategória je obmedzená na výnimočné prípady, ktoré spôsobujú viac ako len neprijemnosti. Hospodársky subjekt nakladajúci s osobnými informáciami predovšetkým nemôže odmietnuť sprístupniť údaje len preto, že bol požiadaný o veľké množstvo údajov.

⁽⁵³⁾ Ako potvrdila PPC, takéto právne predpisy musia rešpektovať právo na súkromie zaručené v ústave, a teda „musia odrážať nevyhnutné a primerané obmedzenie“.

osôb z dôvodov súvisiacich s „ochranou dotknutej osoby alebo práv a slobôd iných osôb“ alebo „inými dôležitými cieľmi všeobecného verejného záujmu“. Hoci sa kategória prípadov, v ktorých by sa sprístupnením porušili „iné zákony alebo právne predpisy“, môže zdať široká, zákony a iné právne predpisy, ktorými sa stanovujú obmedzenia v tejto súvislosti, musia rešpektovať ústavné právo na súkromie a môžu ukladať obmedzenia len pokiaľ by výkon tohto práva predstavoval „zásah do verejného blaha“⁽⁵⁴⁾. Príslušné záujmy je potrebné vyvážiť.

- (85) V článku 28 ods. 3 zákona APPI sa stanovuje, že ak požadované údaje neexistujú, alebo ak sa príslušný hospodársky subjekt nakladajúci s osobnými informáciami rozhodne neposkytnúť prístup k uchovávaným údajom, musí bezodkladne informovať danú fyzickú osobu.
- (86) Po druhé, podľa článku 29 ods. 1 a 2 zákona APPI má dotknutá osoba právo požiadať o opravu, doplnenie alebo výmaz svojich uchovávaných osobných údajov, ak sú tieto údaje nepresné. Po prijatí takejto žiadosti hospodársky subjekt nakladajúci s osobnými informáciami „uskutoční [...] potrebné prešetrenie“ a na základe jeho výsledkov „vykoná opravu atď. obsahu uchovávaných údajov“.
- (87) Po tretie, podľa článku 30 ods. 1 a 2 zákona APPI má dotknutá osoba právo požiadať hospodársky subjekt nakladajúci s osobnými informáciami, aby osobné informácie prestal používať alebo aby ich vymazal, ak sa s nimi nakladá v rozpore s článkom 16 (týkajúcim sa obmedzenia účelu) alebo ak boli neoprávnene získané v rozpore s článkom 17 zákona APPI (týkajúceho sa získania podvodom, inými nevhodnými prostriedkami, alebo v prípade citlivých údajov bez súhlasu). Podobne, podľa článku 30 ods. 3 a 4 zákona APPI má fyzická osoba právo požadovať od hospodárskeho subjektu nakladajúceho s osobnými informáciami, aby informácie prestal poskytovať tretej strane, ak by tým porušoval ustanovenia článku 23 ods. 1 alebo článku 24 zákona APPI (týkajúce sa poskytovania tretím stranám vrátane medzinárodných prenosov).
- (88) Keď je žiadosť odôvodnená, hospodársky subjekt nakladajúci s osobnými informáciami bezodkladne prestane dané údaje používať alebo ich prestane poskytovať tretej strane, a to v rozsahu nevyhnutnom na nápravu porušenia, alebo ak sa na daný prípad vzťahuje výnimka (najmä ak by s ukončením používania boli spojené mimoriadne vysoké náklady)⁽⁵⁵⁾, uskutoční potrebné alternatívne opatrenia na ochranu práv a záujmov dotykanej fyzickej osoby.
- (89) Na rozdiel od práva EÚ sa v zákone APPI a príslušných podzákonných predpisoch nestanovujú právne ustanovenia, ktoré by sa osobitne zaoberali možnosťou namietať proti spracúvaniu na účely priameho marketingu. Takéto spracúvanie sa však bude podľa tohto rozhodnutia uskutočňovať v kontexte prenosu osobných údajov, ktoré boli predtým zhromaždené v Európskej únii. Podľa článku 21 ods. 2 nariadenia (EÚ) 2016/679 musí mať dotknutá osoba vždy možnosť namietať proti prenosu údajov v záujme spracúvania na účely priameho marketingu. Navyše, ako sa vysvetľuje v odôvodnení 43, podľa dopĺňajúceho pravidla 3 má hospodársky subjekt nakladajúci s osobnými informáciami povinnosť spracúvať údaje prijaté na základe tohto rozhodnutia na ten istý účel, na ktorý boli údaje prenesené z Európskej únie, pokiaľ dotknutá osoba neudelí súhlas so zmenou účelu použitia. Teda ak sa prenos uskutočnil na iný účel ako na priamy marketing, hospodársky subjekt nakladajúci s osobnými informáciami v Japonsku nebude môcť spracúvať údaje na účely priameho marketingu bez súhlasu dotknutej osoby z EÚ.
- (90) Vo všetkých prípadoch uvedených v článkoch 28 a 29 zákona APPI má hospodársky subjekt nakladajúci s osobnými informáciami povinnosť bezodkladne informovať danú fyzickú osobu o výsledku jej žiadosti a okrem toho musí vysvetliť akékoľvek (čiastočné) zamietnutie na základe zákonných výnimiek stanovených v článkoch 27 až 30 (článok 31 zákona APPI).

⁽⁵⁴⁾ Najvyšší súd vyložil článok 13 ústavy tak, že poskytuje právo na súkromie (pozri odôvodnenia 7 a 8). Hoci toto právo môže byť obmedzené v prípadoch, keď „zasahuje do verejného blaha“, najvyšší súd vo svojom rozsudku zo 6. marca 2008 (pozri odôvodnenie 8) jednoznačne uviedol, že akékoľvek obmedzenie (v tomto prípade umožňujúce orgánu verejnej moci zhromažďovať a spracúvať osobné údaje) musí byť vyvážené vzhľadom na právo na súkromie, pričom treba zohľadniť faktory, ako je povaha dotknutých údajov, riziká, ktoré spracúvanie týchto údajov vytvára pre fyzické osoby, uplatniteľné záruky a výhody z hľadiska verejného záujmu vyplývajúce zo spracúvania. Je to veľmi podobné typu vyváženia, ktoré sa vyžaduje podľa právnych predpisov EÚ, na základe zásad nevyhnutnosti a primeranosti, na povolenie akéhokoľvek obmedzenia práv na ochranu údajov a záruk v tejto súvislosti.

⁽⁵⁵⁾ Ďalšie vysvetlenia k týmto výnimkám sú uvedené v komentári profesora Katsuya Uga k jednotlivým článkom novely zákona o ochrane osobných informácií, 2015, s. 217. Ako príklad žiadosti spôsobujúcej „vysoké výdavky“ možno napríklad uviesť situáciu, keď sa v rozpore so zásadou obmedzenia účelu spracúvajú len niektoré mená v dlhom zozname (napr. v telefónnom zozname) a telefónny zoznam je už v predaji, pričom stiahnutie týchto výťažkov a ich nahradenie novými by bolo veľmi nákladné. V tom istom prípade – keď sa už kópie telefónneho zoznamu predali mnohým ľuďom a nie je možné všetky z nich zhromaždiť – by bolo zároveň „ťažké splniť požiadavku na ukončenie používania“. V týchto scenároch by „nevyhnutné alternatívne opatrenie“ mohlo zahŕňať napríklad uverejnenie alebo distribúciu oznámenia o oprave. Takéto opatrenie nevylučuje ďalšie formy (súdnych) prostriedkov nápravy, či už v súvislosti s narušením práv na súkromie, poškodením dobrého mena (ohováraním) spôsobeným uverejnením alebo poškodením iných záujmov.

- (91) Pokiaľ ide o podmienky predloženia žiadosti, v článku 32 zákona APPI (spolu s nariadením vlády) sa hospodárskemu subjektu nakladajúcemu s osobnými informáciami umožňuje stanoviť primerané postupy, a to aj pokiaľ ide o informácie potrebné na identifikáciu uchovávaných osobných údajov. Podľa odseku 4 daného článku však hospodárske subjekty nakladajúce s osobnými informáciami nesmú „hlavný subjekt nadmerne zaťažovať“. V niektorých prípadoch môžu hospodárske subjekty nakladajúce s osobnými informáciami stanoviť aj poplatky, pokiaľ ich výška zostane „v rozsahu, ktorý sa považuje za primeraný vzhľadom na skutočné náklady“ (článok 33 zákona APPI).
- (92) A napokon, fyzická osoba môže podľa článku 23 ods. 2 zákona APPI namietat proti sprístupneniu svojich osobných informácií tretej strane alebo odmietnuť udeliť súhlas podľa článku 23 ods. 1 (čím zabráni sprístupneniu v prípade, že by nebol k dispozícii žiadny iný právny základ). Fyzická osoba môže takisto zastaviť spracúvanie údajov na iný účel tým, že odmietne poskytnúť súhlas podľa článku 16 ods. 1 zákona APPI.
- (93) Na rozdiel od práva EÚ sa v zákone APPI a príslušných podzákonných predpisoch nestanovujú všeobecné ustanovenia, ktoré by sa zaoberali otázkou rozhodnutí, ktoré majú vplyv na dotknutú osobu a sú založené výlučne na automatizovanom spracúvaní osobných údajov. Táto otázka sa však rieši v niektorých odvetvových predpisoch platných v Japonsku, ktoré sú pre tento druh spracúvania obzvlášť relevantné. Týka sa to aj odvetví, v ktorých spoločnosti na prijatie rozhodnutí s vplyvom na fyzické osoby s najväčšou pravdepodobnosťou využijú automatizované spracúvanie osobných údajov (napr. finančný sektor). Napríklad v „Komplexných usmerneniach pre dohľad nad veľkými bankami“, ktoré boli revidované v júni 2017, sa vyžaduje, aby sa dotknutej fyzickej osobe konkrétne vysvetlili dôvody zamietnutia žiadosti o uzavretie dohody o úvere. Tieto predpisy teda zaisťujú ochranu v pravdepodobne pomerne obmedzenom počte prípadov, v ktorých by automatizované rozhodnutia prijímali samotný „dovážajúci“ japonský hospodársky subjekt (a nie „vyvážajúci“ prevádzkovateľ z EÚ).
- (94) V každom prípade, pokiaľ ide o osobné údaje zhromaždené v Európskej únii, každé rozhodnutie založené na automatizovanom spracúvaní zvyčajne prijme prevádzkovateľ v Únii (ktorý má priamy vzťah s príslušnou dotknutou osobou), a preto sa naň vzťahuje nariadenie (EÚ) 2016/679⁽⁵⁶⁾. To zahŕňa situácie prenosu, pri ktorých spracúvanie vykonáva zahraničný (napr. japonský) hospodársky subjekt konajúci ako zástupca (sprostredkovateľ) v mene prevádzkovateľa z EÚ (alebo ako subsprostredkovateľ konajúci v mene sprostredkovateľa z EÚ, ktorý dostal údaje od prevádzkovateľa z EÚ, ktorý ich zhromaždil), ktorý na tomto základe následne prijme rozhodnutie. Neexistencia osobitných pravidiel týkajúcich sa automatizovaného rozhodovania v zákone APPI preto pravdepodobne nebude mať vplyv na úroveň ochrany osobných údajov prenášaných na základe tohto rozhodnutia.

2.4. Dozor a presadzovanie

2.4.1. Nezávislý dozor

- (95) S cieľom zaistiť, aby bola primeraná úroveň ochrany údajov zabezpečená aj 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.
- (96) V Japonsku je orgánom zodpovedným za monitorovanie zákona APPI a jeho presadzovanie PPC. Skladá sa z predsedu a ôsmich komisárov menovaných predsedom vlády so súhlasom oboch snemovní parlamentu. Funkčné obdobie predsedu a každého z komisárov je päť rokov s možnosťou opätovného vymenovania (článok 64 zákona APPI). Komisárov je možné odvolať iba z náležitého dôvodu v obmedzenom počte výnimočných okolností⁽⁵⁷⁾, pričom sa nesmú aktívne zapájať do politických aktivít. Podľa zákona APPI navyše nesmú komisári, ktorí túto činnosť vykonávajú na plný pracovný čas, vykonávať žiadne iné činnosti, za ktoré prináleží odmena, ani vyvíjať podnikateľské aktivity. Na všetkých komisárov sa zároveň vzťahujú vnútorné pravidlá, podľa ktorých sa v prípade možného konfliktu záujmov nesmú zúčastňovať na rokovaníach. PPC pomáha sekretariát pod vedením generálneho tajomníka, ktorý bol zriadený na účely plnenia úloh zverených PPC (článok 70 zákona APPI). Komisári aj všetci úradníci sekretariátu sú viazaní prísnymi pravidlami mlčanlivosti (články 72 a 82 zákona APPI).

⁽⁵⁶⁾ Naopak vo výnimočnom prípade, keď má japonský 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 japonský 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.

⁽⁵⁷⁾ Podľa článku 65 zákona APPI je odvolanie proti vôli príslušného komisára možné len z jedného z týchto dôvodov: i) začatie konkurzného konania; ii) odsúdenie za porušenie zákona APPI alebo zákona o používaní identifikačných čísel; iii) odsúdenie na trest odňatia slobody bez nariadeného výkonu práce alebo ešte prísnejší trest; iv) neschopnosť plniť povinnosti z dôvodu duševného alebo telesného ochorenia alebo pochybenia.

- (97) Právomoci PPC, ktoré vykonáva úplne nezávisle⁽⁵⁸⁾, sú stanovené najmä v článkoch 40, 41 a 42 zákona APPI. Podľa článku 40 môže PPC požiadať hospodárske subjekty nakladajúce s osobnými informáciami o predloženie správ alebo dokumentov o spracovateľských operáciách a môže vykonávať aj kontroly, a to kontroly na mieste a kontroly účtovných kníh alebo iných dokumentov. Pokiaľ je to nevyhnutné na presadzovanie zákona APPI, PPC môže poskytovať hospodárskym subjektom nakladajúcim s osobnými informáciami aj usmernenia alebo poradenstvo vo vzťahu k nakladaniu s osobnými informáciami. PPC už túto právomoc na základe článku 41 zákona APPI využila, keď spoločnosti Facebook v nadväznosti na odhalenia v súvislosti s aférou Facebook/Cambridge Analytica adresovala usmernenie.
- (98) Najdôležitejšie je, že PPC má právomoc – konajúc na základe sťažnosti alebo z vlastnej iniciatívy – vydávať v jednotlivých prípadoch odporúčania a nariadenia s cieľom presadzovať zákon APPI a ďalšie záväzné pravidlá (vrátane doplňujúcich pravidiel). Tieto právomoci sú stanovené v článku 42 zákona APPI. Hoci sa v odsekoch 1 a 2 zákona stanovuje dvojstupňový mechanizmus, v rámci ktorého môže PPC vydať nariadenie (iba) na základe predchádzajúceho odporúčania, odsek 3 umožňuje prijať v naliehavých prípadoch priamo nariadenie.
- (99) Hoci v zozname v článku 42 ods. 1, ktorým sa zároveň určuje rozsah pôsobnosti článku 42 ods. 2, nie sú uvedené všetky ustanovenia kapitoly IV oddielu 1 zákona APPI, túto skutočnosť možno vysvetliť tým, že niektoré z týchto ustanovení sa netýkajú povinností hospodárskeho subjektu nakladajúceho s osobnými informáciami⁽⁵⁹⁾ a že všetky nevyhnutné ochranné opatrenia sú už stanovené v iných ustanoveniach, ktoré sú v tomto zozname zahrnuté. Napríklad, hoci sa článok 15 (v ktorom sa požaduje, aby hospodársky subjekt nakladajúci s osobnými informáciami stanovil účel použitia a spracúval príslušné osobné informácie výlučne v rámci jeho rozsahu) v zozname neuvádza, nesplnenie tejto požiadavky môže byť dôvodom na odporúčanie vychádzajúce z porušenia článku 16 ods. 1 (ktorým sa hospodárskemu subjektu nakladajúcemu s osobnými informáciami zakazuje spracúvať osobné informácie nad rámec toho, čo je potrebné na dosiahnutie účelu použitia, pokiaľ nezíska súhlas dotknutej osoby)⁽⁶⁰⁾. Ďalším ustanovením, ktoré nie je v článku 42 ods. 1 uvedené, je článok 19 zákona APPI o presnosti údajov a ich uchovávaní. Nedodržanie uvedeného ustanovenia možno vymáhať buď ako porušenie článku 16 ods. 1, alebo ako porušenie článku 29 ods. 2, ak dotyčná fyzická osoba žiada opravu alebo vymazanie chybných alebo nadmerných údajov a hospodársky subjekt nakladajúci s osobnými informáciami odmieta žiadosti vyhovieť. Pokiaľ ide o práva dotknutej osoby podľa článku 28 ods. 1, článku 29 ods. 1 a článku 30 ods. 1, dozor zo strany PPC sa zabezpečuje tým, že sa jej udelili práva na presadzovanie príslušných povinností hospodárskeho subjektu nakladajúceho s osobnými informáciami stanovených v uvedených článkoch.
- (100) Podľa článku 42 ods. 1 zákona APPI môže PPC, ak dospeje k záveru, že existuje „potreba chrániť práva a záujmy fyzickej osoby v prípadoch, keď [hospodársky subjekt nakladajúci s osobnými informáciami] porušil“ konkrétne ustanovenia zákona APPI, vydať odporúčanie, „aby prestal zákon porušovať alebo podnikol iné opatrenia potrebné na odstránenie porušovania“. Takéto odporúčanie nie je záväzné, ale otvára cestu k záväznému nariadeniu podľa článku 42 ods. 2 zákona APPI. Na základe tohto ustanovenia, ak sa odporúčanie nevykoná „bez toho, aby na to existovali oprávnené dôvody“ a PPC „dospeje k záveru, že bezprostredne hrozí závažné porušenie práv a záujmov fyzickej osoby“, môže nariadiť hospodárskemu subjektu nakladajúcemu s osobnými informáciami, aby prijal opatrenia v súlade s odporúčaním.
- (101) V doplňujúcich pravidlách sa ďalej objasňujú a posilňujú právomoci PPC v oblasti presadzovania práva. Konkrétnejšie, v prípadoch týkajúcich sa údajov dovážaných z Európskej únie bude PPC vždy považovať to, že hospodársky subjekt nakladajúci s osobnými informáciami neprijal opatrenie v súlade s odporúčaním, ktoré PPC vydala podľa článku 42 ods. 1, bez toho, aby na to existoval oprávnený dôvod, za závažné porušenie práv a záujmov fyzickej osoby bezprostrednej povahy v zmysle článku 42 ods. 2, a teda za porušenie opodstatňujúce vydanie záväzného nariadenia. PPC bude navyše ako „oprávnený dôvod“ na nevykonanie odporúčania akceptovať len „udalosť mimoriadnej povahy [znemožňujúcu dodržanie odporúčania] mimo kontroly [hospodárskeho subjektu nakladajúceho s osobnými informáciami], ktorú nemožno primerane predpokladať (napríklad prírodné katastrofy)“ alebo prípady, v ktorých potreba prijať opatrenie v súvislosti s odporúčaním „zanikla, pretože [hospodársky subjekt nakladajúci s osobnými informáciami] prijal alternatívne opatrenie, ktorým sa porušenie plne napraviť“.

⁽⁵⁸⁾ Pozri článok 62 zákona APPI.

⁽⁵⁹⁾ Niektoré ustanovenia sa napríklad týkajú dobrovoľných opatrení hospodárskych subjektov nakladajúcich s osobnými informáciami (články 32 a 33 zákona APPI), alebo povinností vynaložiť „maximálne úsilie“, ktoré sú ako také nevymožiteľné (články 31 a 35, článok 36 ods. 6 a článok 39 zákona APPI). Niektoré ustanovenia nie sú určené hospodárskym subjektom nakladajúcim s osobnými informáciami, ale iným aktérom. Je to tak napríklad v prípade článku 23 ods. 4, článku 26 ods. 2 a článku 34 zákona APPI (presadzovanie článku 26 ods. 2 zákona APPI je však zaistené prostredníctvom možnosti trestnoprávných sankcií podľa článku 88 písm. i) zákona APPI).

⁽⁶⁰⁾ Navyše, ako je vysvetlené v odôvodnení 48, „účel použitia“ v kontexte prenosu údajov podrobne určí vývozca údajov z EÚ, ktorý je v tejto súvislosti viazaný povinnosťou podľa článku 5 ods. 1 písm. b) nariadenia (EÚ) 2016/679. Túto povinnosť môže vymáhať príslušný orgán pre ochranu osobných údajov v Európskej únii.

- (102) Nedodržanie nariadenia PPC sa považuje za trestný čin podľa článku 84 zákona APPI a hospodárskemu subjektu nakladajúcemu s osobnými informáciami, ktorý bude uznaný vinným, môže byť uložený trest odňatia slobody s nariadeným výkonom práce v trvaní najviac šesť mesiacov alebo pokuta do výšky 300 000 jenov. Okrem toho, podľa článku 85 písm. i) zákona APPI môže byť za nedostatočnú spoluprácu s PPC alebo marenie jej vyšetřovania uložená pokuta do výšky 300 000 jenov. Tieto trestnoprávne sankcie sa uplatňujú na dôvazok k sankciám, ktoré možno uložiť za závažné porušenie zákona APPI (pozri odôvodnenie 108).

2.4.2. Súdne prostriedky nápravy

- (103) V záujme zabezpečenia primeranej ochrany, a najmä vymáhania individuálnych práv, by dotknutá osoba mala mať k dispozícii účinné správne a súdne prostriedky nápravy vrátane náhrady škôd.
- (104) Pred tým, ako sa fyzická osoba bude domáhať správnych alebo súdnych prostriedkov nápravy, alebo namiesto toho, aby sa ich domáhala, môže sa rozhodnúť podať sťažnosť týkajúcu sa spracúvania jej osobných údajov samotnému prevádzkovateľovi. Na základe článku 35 zákona APPI sa má hospodársky subjekt nakladajúci s osobnými informáciami usilovať riešiť takéto sťažnosti „vhodne a bezodkladne“ a v záujme dosiahnutia tohto cieľa zriadiť interné systémy vybavovania sťažností. PPC je okrem toho podľa článku 61 písm. ii) zákona APPI zodpovedná za „nevyhnutnú mediáciu v súvislosti s podanou sťažnosťou a poskytnutie spolupráce hospodárskemu subjektu, ktorý sťažnosť rieši“, čo v oboch prípadoch zahŕňa aj sťažnosti podané cudzincami. Japonský zákonodarca v tejto súvislosti zveril ústrednej štátnej správe aj úlohu prijať „potrebné opatrenia“ s cieľom umožniť a uľahčiť riešenie sťažností hospodárskymi subjektmi nakladajúcimi s osobnými informáciami (článok 9), zatiaľ čo miestne samosprávy sa majú usilovať zabezpečiť v takýchto prípadoch mediáciu (článok 13). Popri možnosti podať sťažnosť Národnému centru Japonska pre záležitosti spotrebiteľov môžu fyzické osoby v tejto súvislosti podať sťažnosť aj jednému z viac ako 1 700 spotrebiteľských centier zriadených miestnymi samosprávami na základe zákona o bezpečnosti spotrebiteľov⁽⁶¹⁾. Takéto sťažnosti sa môžu podávať aj v súvislosti s porušením zákona APPI. Podľa článku 19 základného zákona o ochrane spotrebiteľov⁽⁶²⁾ sa miestne samosprávy majú usilovať o mediáciu, pokiaľ ide o sťažnosti, a majú poskytovať stranám potrebné odborné znalosti. Tieto mechanizmy riešenia sporov sú podľa všetkého pomerne účinné, keďže v roku 2015 bolo takto vyriešených 91,2 % z viac než 75 000 prípadov sťažností.
- (105) Porušenie ustanovení zákona APPI hospodárskym subjektom nakladajúcim s osobnými informáciami môže viesť k občianskoprávnej žalobe, ako aj k trestnému konaniu a sankciám. Po prvé, ak sa fyzická osoba domnieva, že jej práva podľa článkov 28, 29 a 30 zákona APPI boli porušené, môže požiadať o vydanie súdneho príkazu, pričom požiada súd, aby hospodárskemu subjektu nakladajúcemu s osobnými informáciami nariadil splniť jej žiadosť podľa jedného z týchto ustanovení, t. j. sprístupnil uchovávané osobné údaje (článok 28), opravil uchovávané osobné údaje, ktoré sú nesprávne (článok 29), alebo ukončil nezákonné spracúvanie alebo poskytovanie tretej strane (článok 30). Takúto žalobu možno podať bez toho, aby bolo nutné vychádzať z článku 709 Občianskeho zákonníka⁽⁶³⁾ alebo inak z práva občianskoprávnych deliktov⁽⁶⁴⁾. To konkrétne znamená, že fyzická osoba nemusí preukazovať žiadnu ujmu.
- (106) Po druhé, v prípade, keď sa údajné porušenie netýka individuálnych práv podľa článkov 28, 29 a 30, ale všeobecných zásad alebo povinností hospodárskeho subjektu nakladajúceho s osobnými informáciami v oblasti ochrany údajov, môže dotknutá fyzická osoba podať na hospodársky subjekt občianskoprávnu žalobu na základe ustanovení japonského Občianskeho zákonníka o občianskoprávnych deliktoch, najmä článku 709. Zatiaľ čo v rámci súdneho sporu na základe článku 709 sa okrem zavinenia (úmyselného alebo z nedbanlivosti) vyžaduje aj preukázanie ujmy, podľa článku 710 Občianskeho zákonníka môže byť takáto ujma majetková aj nemajetková. Výška náhrady nie je nijakým spôsobom obmedzená.
- (107) Pokiaľ ide o dostupné prostriedky nápravy, v článku 709 japonského Občianskeho zákonníka sa hovorí o peňažnej náhrade. V japonskej judikatúre sa však tento článok vykladá tak, že udeľuje aj právo na získanie súdneho príkazu⁽⁶⁵⁾. Preto ak dotknutá osoba podá žalobu na základe článku 709 Občianskeho zákonníka a tvrdí, že jej práva alebo záujmy boli poškodené porušením ustanovenia zákona APPI zo strany odporcu, môže v tejto žalobe požadovať okrem náhrady škody aj vydanie súdneho príkazu, a to hlavne na zastavenie akéhokoľvek nezákonného spracúvania.

⁽⁶¹⁾ Zákon č. 50 z 5. júna 2009.

⁽⁶²⁾ Zákon č. 60 z 22. augusta 2012.

⁽⁶³⁾ Hlavným východiskom občianskoprávnych sporov o náhradu škody je článok 709 Občianskeho zákonníka. Podľa tohto ustanovenia „osoba, ktorá úmyselne alebo z nedbanlivosti porušila akékoľvek právo iných osôb alebo právom chránený záujem iných osôb, je povinná nahradiť všetky škody, ktoré následkom toho vzniknú“.

⁽⁶⁴⁾ Vrchný súd Tokio, rozsudok z 20. mája 2015 (nezverejnený); Okresný súd Tokio, rozsudok z 8. septembra 2014, Westlaw Japan 2014WLJPCA09088002. Pozri aj článok 34 ods. 1 a 3 zákona APPI.

⁽⁶⁵⁾ Pozri najvyšší súd, rozsudok z 24. septembra 2002 (Hanrei Times zv. 1106, s. 72).

- (108) Po tretie, okrem prostriedkov nápravy v oblasti občianskeho práva (práva občianskoprávných deliktov) môže dotknutá osoba v súvislosti s porušením ustanovení zákona APPI podať sťažnosť u generálneho prokurátora alebo príslušníka justičnej polície, ktorá môže viesť k trestnoprávnym sankciám. Kapitola VII zákona APPI zahŕňa celý rad trestnoprávných ustanovení. Najdôležitejšie z nich (článok 84) sa týka nevykonania nariadení PPC podľa článku 42 ods. 2 a 3 zo strany hospodárskeho subjektu nakladajúceho s osobnými informáciami. Ak hospodársky subjekt nevykoná nariadenie vydané PPC, predseda PPC (ako aj akýkoľvek iný úradník štátnej správy) ⁽⁶⁶⁾ môže vec postúpiť generálnemu prokurátorovi alebo príslušníkovi justičnej polície a týmto spôsobom spustiť začatie trestného konania. Trestom za porušenie nariadenia PPC je odňatie slobody s nariadeným výkonom práce v trvaní najviac šesť mesiacov alebo pokuta do výšky 300 000 jenov. Medzi ďalšie ustanovenia zákona APPI, v ktorých sa stanovujú sankcie pre prípad porušenia tohto zákona majúceho vplyv na práva a záujmy dotknutých osôb, patrí článok 83 zákona APPI (týkajúci sa „skrytého poskytovania alebo využívania“ databázy osobných informácií „na účely získania [...] nezákonných ziskov“) a článok 88 písm. i) zákona APPI (týkajúci sa skutočnosti, že tretia strana nesprávne informovala hospodársky subjekt nakladajúci s osobnými informáciami, keď mu poskytla osobné údaje v súlade s článkom 26 ods. 1 zákona APPI, najmä pokiaľ ide o podrobnosti o tom, ako predtým sama získala takéto údaje). Za takéto porušenia zákona APPI hrozí trest odňatia slobody s nariadeným výkonom práce v trvaní najviac jedného roka alebo pokuta do výšky 500 000 jenov (v prípade článku 83) alebo správna pokuta do výšky 100 000 jenov [v prípade článku 88 písm. i)]. Hoci silný odrádzajúci účinok na vedenie podniku, ktoré riadi spracovateľské operácie hospodárskeho subjektu nakladajúceho s osobnými informáciami, ako aj na jednotlivcov, ktorí s údajmi nakladajú, pravdepodobne má už samotná hrozba trestnoprávnej sankcie, v článku 87 zákona APPI sa objasňuje, že ak sa zástupca, zamestnanec alebo iný pracovník právnickej osoby dopustí porušenia podľa článkov 83 až 85 zákona APPI, „dotyčná osoba sa potrestá a danej právnickej osobe sa uloží pokuta stanovená v príslušných článkoch“. V tomto prípade možno zamestnancovi aj spoločnosti uložiť sankcie až do plnej maximálnej výšky.
- (109) A napokon, fyzické osoby sa môžu domáhať nápravy aj v prípade konania, resp. nekonania PPC. V japonskom právnom poriadku sa tejto súvislosti poskytuje viacero správnych a súdnych prostriedkov nápravy.
- (110) Ak fyzická osoba nie je spokojná s tým, ako PPC postupovala, môže podať správny opravný prostriedok podľa zákona o preskúmvaní sťažností v správnych veciach ⁽⁶⁷⁾. Na druhej strane, ak sa fyzická osoba domnieva, že PPC mala konať, ale nekonala, môže podľa článku 36-3 uvedeného zákona požiadať PPC, aby vydala dispozíciu alebo poskytla správne usmernenie, ak sa domnieva, že „dispozícia alebo správne usmernenie nevyhnutné na nápravu porušenia neboli vydané“.
- (111) Pokiaľ ide o súdne prostriedky nápravy, podľa Správneho súdneho poriadku môže fyzická osoba, ktorá nie je spokojná so správnou dispozíciou vydanou PPC, podať žalobu *mandamus* ⁽⁶⁸⁾ a požiadať súd, aby PPC nariadil prijať ďalšie opatrenia ⁽⁶⁹⁾. Aj súd môže v určitých prípadoch vydať predbežný príkaz *mandamus*, aby zabránil nezvratnej ujme ⁽⁷⁰⁾. Fyzická osoba môže navyše podľa toho istého zákona požiadať o zrušenie rozhodnutia PPC ⁽⁷¹⁾.
- (112) A napokon, fyzická osoba môže podať na PPC aj žalobu o náhradu škody zo strany štátu podľa článku 1 ods. 1 zákona o opravných prostriedkoch proti štátu, ak utrpela škodu v dôsledku toho, že nariadenie, ktoré PPC vydala hospodárskemu subjektu bolo protiprávne, resp. že PPC neuplatnila svoju právomoc.

3. PRÍSTUP K OSOBNÝM ÚDAJOM PRENÁŠANÝM Z EURÓPSKEJ ÚNIE ZO STRANY ORGÁNOV VEREJNEJ MOCI V JAPONSKU A ICH POUŽÍVANIE TÝMITO ORGÁNMI

- (113) Komisia takisto posúdila obmedzenia a záruky vrátane mechanizmov dozoru a individuálnych prostriedkov nápravy, ktoré sú v japonskom právnom poriadku k dispozícii vo vzťahu k zhromažďovaniu a následnému používaniu osobných údajov prenášaných hospodárskym subjektom v Japonsku, ktoré vo verejnom záujme uskutočňujú orgány verejnej moci, a to najmä na účely presadzovania práva v trestných veciach a na účely národnej bezpečnosti (ďalej len „prístup vlády“). Japonská 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.

⁽⁶⁶⁾ Článok 239 ods. 2 Trestného poriadku.

⁽⁶⁷⁾ Zákon č. 160 z roku 2014.

⁽⁶⁸⁾ Článok 37-2 Správneho súdneho poriadku.

⁽⁶⁹⁾ Podľa článku 3 ods. 6 Správneho súdneho poriadku sa pojem „žaloba *mandamus*“ vzťahuje na žalobu o vydanie príkazu, ktorým súd nariadi správnejmu orgánu, aby vydal pôvodnú správnu dispozíciu, ktorú „mal“ vydať, ale nevydal.

⁽⁷⁰⁾ Článok 37-5 Správneho súdneho poriadku.

⁽⁷¹⁾ Kapitola II oddiel 1 Správneho súdneho poriadku.

3.1. Všeobecný právny rámec

- (114) Prístup vlády je výkonom verejnej moci a ako taký sa musí v Japonsku uskutočňovať v plnom súlade s právnymi predpismi (zásada zákonnosti). V tejto súvislosti sú v japonskej ústave zahrnuté ustanovenia, ktorými sa obmedzuje a vymedzuje zhromažďovanie osobných údajov orgánmi verejnej moci. Ako už bolo uvedené v súvislosti so spracúvaním zo strany hospodárskych subjektov, Najvyšší súd Japonska uznal právo na súkromie a ochranu údajov, pričom vychádzal z článku 13 ústavy, ktorým sa okrem iného chráni právo na slobodu⁽⁷²⁾. Dôležitým aspektom tohto práva je sloboda neumožniť sprístupnenie svojich osobných informácií tretej strane bez súhlasu⁽⁷³⁾. Z toho vyplýva právo na účinnú ochranu osobných údajov pred zneužitím a (najmä) neoprávneným prístupom. Doplnková ochrana je zabezpečená článkom 35 ústavy, ktorý sa týka práva všetkých osôb na ochranu domovej slobody, písomností a majetku, čo si vyžaduje, aby orgány verejnej moci získali vo všetkých prípadoch „prehliadok a zaistení vecí“ súdny príkaz vydaný na základe „primeraného dôvodu“⁽⁷⁴⁾. Najvyšší súd vo svojom rozsudku z 15. marca 2017 (prípád GPS) objasnil, že táto požiadavka na súdny príkaz sa uplatňuje vždy, keď vláda zasahuje („vstupuje“) do súkromnej sféry spôsobom, ktorý potláča vôľu fyzickej osoby, teda „povinným vyšetrovaním“. Sudca môže takýto príkaz vydať len na základe konkrétneho podozrenia z trestného činu, t. j. keď mu predložia listinné dôkazy, na základe ktorých sa osoba, ktorej sa vyšetrovanie týka, môže považovať za osobu, ktorá spáchala trestný čin⁽⁷⁵⁾. Japonské orgány teda nemajú zákonnú právomoc zhromažďovať osobné informácie povinnými prostriedkami v situáciách, keď k porušeniu právnych predpisov ešte nedošlo⁽⁷⁶⁾, napríklad aby zabránili trestnému činu alebo inej bezpečnostnej hrozbe (ako je to v prípade vyšetrovaní z dôvodu národnej bezpečnosti).
- (115) Podľa zásady výhrady práva musí byť každé zhromažďovanie údajov, ku ktorému dochádza v rámci donucovacieho vyšetrovania, konkrétne povolené právnymi predpismi (ako sa uvádza napríklad v článku 197 ods. 1 Trestného poriadku o povinnom zhromažďovaní informácií na účely vyšetrovania trestného činu). Táto požiadavka sa vzťahuje aj na prístup k elektronickým informáciám.
- (116) Dôležité je, že článkom 21 ods. 2 ústavy sa zaručuje dôvernosc všetkých komunikačných prostriedkov, pričom obmedzenia sa môžu v právnych predpisoch stanoviť len z dôvodov verejného záujmu. Článkom 4 zákona o telekomunikáciách, podľa ktorého sa nesmie porušiť dôverný charakter komunikácie, s ktorou telekomunikačný prevádzkovateľ nakladá, sa táto požiadavka na zachovanie dôvernosti zavádza na úrovni štatutárneho práva. Uvedený článok sa vykladá ako zákaz sprístupňovania informácií z komunikácie s výnimkou prípadov, keď s ním používatelia súhlasili alebo keď sa naň vzťahuje jedna z výslovných výnimiek z trestnej zodpovednosti podľa Trestného zákona⁽⁷⁷⁾.
- (117) Ústava zaručuje aj právo na prístup k súdom (článok 32) a právo žalovať štát o nápravu v prípade, keď fyzickej osobe vznikne škoda v dôsledku protiprávneho konania verejného činiteľa (článok 17).
- (118) Pokiaľ ide konkrétne o právo na ochranu údajov, v kapitole III oddieloch 1, 2 a 3 zákona APPI sa stanovujú všeobecné zásady vzťahujúce sa na všetky odvetvia vrátane verejného sektora. V článku 3 zákona APPI sa konkrétne uvádza, že so všetkými osobnými informáciami sa musí nakladať v súlade so zásadou rešpektovania osobnosti fyzických osôb. Keď orgány verejnej moci zhromaždia („získajú“) osobné informácie, okrem iného aj ako súčasť elektronických záznamov⁽⁷⁸⁾, nakladanie s týmito informáciami sa spravuje zákonom o ochrane osobných

⁽⁷²⁾ Pozri napríklad najvyšší súd, rozsudok z 12. septembra 2003 vo veci č. 1656 [2002 (Ju)]. Najvyšší súd predovšetkým konštatoval, že „každý môže slobodne chrániť svoje osobné informácie pred sprístupnením tretej strane alebo zverejnením bez náležitého dôvodu.“

⁽⁷³⁾ Najvyšší súd, rozsudok zo 6. marca 2008 („Juki-net“).

⁽⁷⁴⁾ „Primeraný dôvod“ existuje len v prípade, že sa dotýčaná fyzická osoba (podozrivý, obvinený) považuje za osobu, ktorá spáchala trestný čin, a prehliadka a zaistenie vecí sú potrebné na účely vyšetrovania trestného činu. Pozri najvyšší súd, rozsudok z 18. marca 1969 vo veci č. 100 [1968 (Shi)].

⁽⁷⁵⁾ Pozri článok 156 ods. 1 Trestného poriadku.

⁽⁷⁶⁾ Treba však poznamenať, že zákonom o trestaní organizovanej trestnej činnosti a kontrole výnosov z trestnej činnosti z 15. júna 2017 sa zavádza nový trestný čin, ktorým sa kriminalizuje príprava teroristických činov a niektorých iných foriem organizovanej trestnej činnosti. Vyšetrovanie možno začať len v prípade konkrétneho podozrenia a na základe dôkazov o splnení všetkých troch nevyhnutných podmienok pre naplnenie skutkovej podstaty trestného činu (zapojenie organizovanej zločineckej skupiny, „akt plánovania“ a akt „prípravy uskutočnenia“ trestného činu). Pozri napr. aj články 38 – 40 zákona o predchádzaní podvratnej činnosti (zákon č. 240 z 21. júla 1952).

⁽⁷⁷⁾ Článok 15 ods. 8 Usmernení o ochrane osobných informácií v sektore telekomunikácií.

⁽⁷⁸⁾ Správne orgány, ako sú vymedzené v článku 2 ods. 1 zákona APPIHAO. Podľa informácií poskytnutých japonskou vládou spadajú pod definíciu „správnych orgánov“ všetky orgány verejnej moci okrem prefektúrnej polície. Prefektúrna polícia zároveň pôsobí v medziach právneho rámca daného prefektúrnymi nariadeniami o ochrane osobných informácií (pozri článok 11 zákona APPI a základnú politiku), v ktorých sa stanovujú ustanovenia na ochranu osobných informácií, ktoré sú rovnocenné so zákonom APPIHAO. Pozri oddiel I.B prílohy II. PPC vysvetlila, že podľa „základnej politiky“ musia byť tieto nariadenia schválené na základe obsahu zákona APPIHAO, pričom ministerstvo vnútra a komunikácií vydáva oznámenia, aby miestnym samosprávam poskytlo v tejto súvislosti potrebné usmernenia. Ako zdôraznila PPC, „[v] rámci týchto obmedzení musí byť nariadenie o ochrane osobných informácií v každej prefektúre stanovené [...] na základe základnej politiky a obsahu oznámení.“

informácií uchovávaných správnymi orgánmi (ďalej len „zákon APPIHAO“) ⁽⁷⁹⁾. To v zásade ⁽⁸⁰⁾ zahŕňa aj spracúvanie osobných informácií na účely presadzovania práva v trestných veciach alebo na účely národnej bezpečnosti. V zákone APPIHAO sa okrem iného stanovuje, že orgány verejnej moci: i) môžu uchovávať osobné informácie len v rozsahu nevyhnutnom na plnenie svojich úloh; ii) nesmú takéto informácie použiť na „neoprávnený“ účel alebo ich bez odôvodnenia sprístupniť tretej osobe; iii) konkrétne určia účel a tento účel nesmú zmeniť nad rámec toho, čo sa môže primerane považovať za relevantné na pôvodný účel (obmedzenie účelu); iv) nesmú v zásade použiť uchovávané osobné informácie na iné účely alebo ich na iné účely sprístupniť tretej osobe, a ak to považujú za potrebné, stanovujú obmedzenia účelu alebo spôsobu použitia tretími stranami; v) sa usilujú o zabezpečenie správnosti informácií (kvality údajov); vi) prijímajú potrebné opatrenia na riadnu správu informácií a na zabránenie úniku, strate alebo poškodeniu (bezpečnosť údajov); a vii) usilujú sa náležite a urýchlene spracovať všetky sťažnosti týkajúce sa spracúvania informácií ⁽⁸¹⁾.

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

- (119) V japonskom právnom poriadku sa stanovujú viaceré obmedzenia, pokiaľ ide o prístup k osobným údajom a ich použitie na účely presadzovania práva v trestných veciach, ako aj mechanizmy dozoru a nápravy, ktoré poskytujú dostatočné záruky, že tieto údaje budú účinne chránené pred nezákonnými zásahmi a rizikom zneužitia.

3.2.1. Právny základ a uplatniteľné obmedzenia/záruky

- (120) V japonskom právnom rámci sa zhromažďovanie elektronických informácií na účely presadzovania práva v trestných veciach môže uskutočňovať na základe súdneho príkazu (povinné zhromažďovanie) alebo žiadosti o dobrovoľné sprístupnenie.

3.2.1.1. Povinné vyšetrovanie na základe súdneho príkazu

- (121) Ako sa uvádza v odôvodnení 115, každé zhromažďovanie údajov v rámci donucovacieho vyšetrovania musí byť konkrétne povolené právnymi predpismi a môže sa uskutočňovať len na základe súdneho príkazu „vydaného z primeraného dôvodu“ (článok 35 ústavy). Pokiaľ ide o vyšetrovanie trestných činov, táto požiadavka sa odráža v ustanoveniach Trestného poriadku. Podľa článku 197 ods. 1 Trestného poriadku sa povinné opatrenia „neuplatňujú, pokiaľ v tomto zákone nie sú stanovené osobitné ustanovenia“. Pokiaľ ide o zhromažďovanie elektronických informácií, jediným relevantným ⁽⁸²⁾ právnym základom v tejto súvislosti je článok 218 Trestného poriadku (prehliadka a zaistenie) a článok 222-2 Trestného poriadku, podľa ktorých sa povinné opatrenia na odpočúvanie elektronickej komunikácie bez súhlasu jednej zo strán vykonávajú na základe iných zákonov, konkrétne zákona o odpočúvaní na účely vyšetrovania trestných činov (ďalej len „zákon o odpočúvaní“). V oboch prípadoch sa uplatňuje požiadavka na súdny príkaz.
- (122) Konkrétnejšie, podľa článku 218 ods. 1 Trestného poriadku môže generálny prokurátor, asistent generálneho prokurátora alebo príslušník justičnej polície vykonať, ak je to potrebné na vyšetrovanie trestného činu, prehliadku alebo zaistenie veci (vrátane nariadenia poskytnutia záznamov) na základe príkazu vopred vydaného sudcom ⁽⁸³⁾. V takomto súdnom príkaze sa musí okrem iného uvádzať meno podozrivého alebo obvineného, trestný čin, z ktorého je obvinený ⁽⁸⁴⁾, elektromagnetické záznamy, ktoré sa majú zaistiť, a „miesto alebo veci“, ktoré majú byť predmetom prehliadky (článok 219 ods. 1 Trestného poriadku).

⁽⁷⁹⁾ Na osobné informácie, ktoré úradníci správneho orgánu získajú pri plnení svojich úloh a ktoré daný správny orgán uchováva na organizačné účely, sa vzťahuje vymedzenie pojmu „uchovávané osobné informácie“ v zmysle článku 2 ods. 3 zákona APPIHAO, pokiaľ sú tieto informácie zaznamenané v „správnych dokumentoch“. To zahŕňa aj elektronické informácie, ktoré tieto orgány zhromažďujú a následne ďalej spracúvajú, keďže vymedzenie pojmu „správne dokumenty“ v článku 2 ods. 2 zákona o prístupe k informáciám uchovávaným správnymi orgánmi (zákon č. 42 z roku 1999) sa vzťahuje aj na elektromagnetické záznamy.

⁽⁸⁰⁾ Podľa článku 53-2 Trestného poriadku je však kapitola IV zákona APPIHAO vylúčená pre „dokumenty týkajúce sa súdnych konaní“, ktoré podľa poskytnutých informácií zahŕňajú elektronické informácie získané na základe súdneho príkazu alebo žiadosti o dobrovoľnú spoluprácu v rámci vyšetrovania trestného činu. Ani vo vzťahu k informáciám zhromaždeným v oblasti národnej bezpečnosti nebudú fyzické osoby schopné úspešne uplatniť svoje práva podľa zákona APPIHAO, ak má vedúci orgán verejnej moci „opodstatnené dôvody“ domnievať sa, že sprístupnenie „by mohlo viesť k ohrozeniu národnej bezpečnosti“ [pozri článok 14 písm. iv)]. V súvislosti s tým sa od orgánov verejnej moci vyžaduje, aby údaje sprístupnili pokiaľ možno aspoň čiastočne (článok 15).

⁽⁸¹⁾ Pozri konkrétne odkazy na zákon APPIHAO v oddiele II.A.1 písm. b) bode 2 prílohy II.

⁽⁸²⁾ Hoci je podľa článku 220 Trestného poriadku možné vykonať prehliadku a zaistenie veci „na mieste“ bez súdneho príkazu, ak generálny prokurátor, asistent generálneho prokurátora alebo príslušník justičnej polície zadrží podozrivého/zjavného páchatela, v súvislosti s prenosmi, a teda na účely tohto rozhodnutia, to nie je relevantné.

⁽⁸³⁾ Podľa článku 222 ods. 1 v spojení s článkom 110 Trestného poriadku sa súdny príkaz na prehliadku/zaistenie záznamov musí predložiť osobe, na ktorú sa dané opatrenie vzťahuje.

⁽⁸⁴⁾ Pozri aj článok 189 ods. 2 Trestného poriadku, podľa ktorého príslušník justičnej polície vyšetroje páchatela a skúma príslušné dôkazy „ak sa domnieva, že bol spáchaný trestný čin“. V článku 155 ods. 1 Trestného poriadku sa takisto stanovuje, že v písomnej žiadosti o vydanie súdneho príkazu sa musí okrem iného uvádzať „trestný čin, z ktorého je daná osoba obvinená“ a „zhrnutie skutkového stavu trestného činu“.

- (123) Pokiaľ ide o odpočúvanie komunikácie, v článku 3 zákona o odpočúvaní sa takéto opatrenia povoľujú len pri dodržaní prísnych podmienok. Orgány verejnej moci musia predovšetkým najprv získať súdny príkaz, ktorý môže byť vydaný len na účely vyšetrovania určitých závažných trestných činov (uvedených v prílohe k danému zákonu) ⁽⁸⁵⁾ a keď je „mimoriadne obťažné identifikovať páchatelia trestného činu alebo objasniť situáciu/podrobnosti spáchania trestného činu iným spôsobom“ ⁽⁸⁶⁾. Podľa článku 5 zákona o odpočúvaní sa súdny príkaz vydáva na obmedzený čas, pričom sudca môže uložiť dodatočné podmienky. V zákone o odpočúvaní sa navyše stanovuje niekoľko ďalších záruk, ako napríklad nevyhnutná prítomnosť svedkov (články 12 a 20), zákaz odpočúvania komunikácie určitých privilegovaných skupín (napr. lekárov a právnikov) (článok 15), povinnosť ukončiť odpočúvanie, ak už nie je odôvodnené, a to dokonca aj počas platnosti súdneho príkazu (článok 18) alebo všeobecná požiadavka informovať dotknutú osobu a umožniť prístup k záznamom do tridsiatich dní od ukončenia odpočúvania (články 23 a 24).
- (124) V prípade všetkých povinných opatrení založených na súdnom príkaze sa môže prehliadka vykonať len v rozsahu, „aký je nevyhnutný na dosiahnutie jej cieľa“ – teda ak ciele sledované vyšetrovaním nie je možné dosiahnuť inak (článok 197 ods. 1 Trestného poriadku). Hoci kritériá na určenie nevyhnutnosti nie sú v štatutárnom práve bližšie určené, Najvyšší súd Japonska rozhodol, že sudca vydávajúci súdny príkaz by mal vykonať celkové posúdenie, pričom by mal zohľadniť najmä i) závažnosť trestného činu a spôsob jeho spáchania; ii) hodnotu a význam materiálov, ktoré sa majú zaistiť ako dôkaz; iii) pravdepodobnosť (riziko) ukrytia alebo zničenia dôkazov; a iv) rozsah, v akom môže zaistenie vecí spôsobiť dotýčnej fyzickej osobe ujmu ⁽⁸⁷⁾.

3.2.1.2. Žiadosť o dobrovoľné sprístupnenie informácií na základe „žiadosti o sprístupnenie informácií“

- (125) Orgány verejnej moci môžu v medziach svojich právomocí zhromažďovať elektronické informácie aj na základe žiadostí o dobrovoľné sprístupnenie. Ide o nepovinnú formu spolupráce, pri ktorej nie je možné vyhovenie žiadosti vymáhať ⁽⁸⁸⁾, čím sú orgány verejnej moci zbavené povinnosti získať súdny príkaz.
- (126) Pokiaľ je takáto žiadosť adresovaná hospodárskemu subjektu a týka sa osobných informácií, hospodársky subjekt musí splniť požiadavky stanovené v zákone APPI. Podľa článku 23 ods. 1 zákona APPI môžu hospodárske subjekty sprístupniť osobné informácie tretím stranám bez súhlasu dotýčnej fyzickej osoby len v určitých prípadoch, čo zahŕňa aj prípady, keď sprístupnenie „vychádza zo zákonov a iných právnych predpisov“ ⁽⁸⁹⁾. V oblasti presadzovania práva v trestných veciach je právny základ pre takéto žiadosti stanovený v článku 197 ods. 2 Trestného poriadku, podľa ktorého „možno súkromné organizácie požiadať, aby informovali o nevyhnutných záležitostiach týkajúcich sa vyšetrovania.“ Keďže takáto „žiadosť o sprístupnenie informácií“ je prípustná iba v rámci vyšetrovania trestného činu, vždy sa pri nej predpokladá konkrétne podozrenie z už spáchaného trestného činu ⁽⁹⁰⁾. Navyše, keďže takéto vyšetrovania vo všeobecnosti vykonáva prefektúrna polícia, uplatňujú sa obmedzenia podľa článku 2 ods. 2 zákona o polícii ⁽⁹¹⁾. Podľa uvedeného ustanovenia sú činnosti polície „prísne obmedzené“ na plnenie jej povinností a úloh (t. j. predchádzanie trestným činom, ich potlačanie a vyšetrovanie). Okrem toho, polícia musí pri plnení svojich úloh konať nestrannne, nezaujato a spravodlivo a nikdy nesmie zneužiť svoje právomoci „spôsobom, ktorý by zasahoval do práv a slobôd fyzickej osoby zaručených Ústavou Japonska“ (čo zahŕňa právo na súkromie a ochranu údajov, ako už bolo uvedené) ⁽⁹²⁾.
- (127) Národná policajná agentúra ako federálny orgán, ktorý má okrem iného na starosti aj všetky záležitosti týkajúce sa kriminálnej polície – vydala osobitne v súvislosti s článkom 197 ods. 2 Trestného poriadku pre prefektúrne

⁽⁸⁵⁾ V uvedenej prílohe sa uvádza deväť druhov trestných činov, napr. trestné činy súvisiace s drogami a strelnými zbraňami, obchodovaním s ľuďmi a plánovanou vraždou. Treba poznamenať, že novozavedený trestný čin „prípravy trestných činov terorizmu a inej organizovanej trestnej činnosti“ (pozri poznámku pod čiarou č. 76) nie je v tomto restriktívnom zozname uvedený.

⁽⁸⁶⁾ Navyše, podľa článku 23 zákona o odpočúvaní musí vyšetrovací orgán písomne informovať fyzickú osobu, ktorej komunikácia je odpočúvaná (a teda zahrnutá do záznamu z odpočúvania), o tejto skutočnosti.

⁽⁸⁷⁾ Pozri oddiel II.A.1 písm. b) bod 1 prílohy II.

⁽⁸⁸⁾ Podľa poskytnutých informácií nevyplývajú pre hospodárske subjekty, ktoré nespolupracujú, zo žiadneho právneho predpisu nepriaznivé dôsledky (ani sankcie). Pozri oddiel II.A.2 písm. a) prílohy II.

⁽⁸⁹⁾ Podľa usmernení PPC (General Rule Edition) je základom pre sprístupnenie osobných informácií v reakcii na súdny príkaz (článok 218 Trestného poriadku), ako aj na „žiadosť o sprístupnenie informácií“ (článok 197 ods. 2 Trestného poriadku) článok 23 ods. 1 písm. i).

⁽⁹⁰⁾ To znamená, že „žiadosť o sprístupnenie informácií“ sa môže použiť len na zhromažďovanie informácií v jednotlivých prípadoch, a nie na prípadné rozsiahle zhromažďovanie osobných údajov. Pozri aj oddiel I.A.2 písm. b) bod 1 prílohy II.

⁽⁹¹⁾ Ako aj podľa predpisov príslušnej prefektúrnej komisie pre verejnú bezpečnosť, pozri článok 189 ods. 1 Trestného poriadku.

⁽⁹²⁾ Pozri aj článok 3 zákona o polícii, podľa ktorého služobný sľub, ktorý všetci príslušníci polície skladajú, znie: „verne plniť povinnosť chrániť a zachovávať ústavu a právne predpisy Japonska a plniť svoje úlohy nestrannne, spravodlivo, čestne a nezaujato“.

políciu⁽⁹³⁾ pokyny o „náležitom používaní písomných žiadostí vo veciach vyšetrovania“. Podľa tohto oznámenia sa žiadosti musia podávať na vopred určenom formulári („formulár č. 49“ alebo tzv. žiadosť o sprístupnenie informácií)⁽⁹⁴⁾, musia sa týkať záznamov „súvisiacich s konkrétnym vyšetrovaním“ a požadované informácie musia byť „pre [dané] vyšetrovanie nevyhnutné“. Hlavný vyšetrovateľ musí v každom prípade „plne preskúmať nevyhnutnosť, obsah atď. [danej] jednotlivej žiadosti“ a musí v rámci svojej organizácie získať súhlas vysokopostaveného úradníka.

- (128) Najvyšší súd Japonska okrem toho stanovil v dvoch rozsudkoch z rokov 1969 a 2008⁽⁹⁵⁾ obmedzenia týkajúce sa nepovinných opatrení, ktoré zasahujú do práva na súkromie⁽⁹⁶⁾. Súd predovšetkým konštatoval, že takéto opatrenia musia byť „primerané“ a nesmú prekračovať „všeobecne prípustné medze“, čo znamená, že musia byť nevyhnutné pre vyšetrovanie podozrivej osoby (zhromažďovanie dôkazov) a musia sa vykonať „spôsobmi vhodnými na dosiahnutie účelu vyšetrovania“⁽⁹⁷⁾. Z uvedených rozsudkov vyplýva, že to zahŕňa overenie primeranosti, pričom sa do úvahy berú všetky okolnosti daného prípadu (napr. miera zasahovania do práva na súkromie vrátane očakávania súkromia, závažnosť trestného činu, pravdepodobnosť získania užitočných dôkazov, dôležitosť takýchto dôkazov, možné alternatívne prostriedky vyšetrovania atď.)⁽⁹⁸⁾.
- (129) Okrem týchto obmedzení výkonu verejnej moci sa od samotných hospodárskych subjektov očakáva, že overia („potvrdia“) nevyhnutnosť a „rozumnosť“ poskytnutia informácií tretej strane⁽⁹⁹⁾. To zahŕňa otázku, či im v spolupráci bráni zákon. Takéto protichodné právne povinnosti môžu vyplývať najmä z povinností týkajúcich sa zachovávanie mlčanlivosti, ako je napríklad článok 134 Trestného zákona (týkajúci sa vzťahu medzi lekárom, právnikom, kňazom atď. a ich klientom). Zároveň musí „každá osoba, ktorá pôsobí v oblasti telekomunikácií, pri výkone svojej funkcie zachovávať tajomstvá druhých, o ktorých sa dozvedela v súvislosti s komunikáciou, s ktorou nakladá telekomunikačný operátor“ (článok 4 ods. 2 zákona o telekomunikáciách). Túto povinnosť sprevádza sankcia stanovená v článku 179 zákona o telekomunikáciách, podľa ktorého sa každá osoba, ktorá poruší dôvernú komunikáciu, s ktorou nakladá telekomunikačný operátor, dopustí trestného činu a potrestá sa trestom odňatia slobody s nariadeným výkonom práce v trvaní dvoch rokov alebo pokutou vo výške najviac jedného milióna jenov⁽¹⁰⁰⁾. Hoci táto požiadavka nie je absolútna a umožňuje najmä opatrenia porušujúce dôvernú komunikáciu, ktoré predstavujú „odôvodnené konanie“ v zmysle článku 35 Trestného zákona⁽¹⁰¹⁾, táto výnimka sa nevzťahuje na odpovede na nepovinné žiadosti orgánov verejnej moci o sprístupnenie elektronických informácií podľa článku 197 ods. 2 Trestného poriadku.

3.2.1.3. Ďalšie používanie zhromaždených informácií

- (130) Po zhromaždení japonskými orgánmi verejnej moci spadajú osobné informácie do rozsahu pôsobnosti zákona APPIHAO. Uvedeným zákonom sa upravuje nakladanie s „uchovávanými osobnými informáciami“ (ich

⁽⁹³⁾ Podľa článku 30 ods. 1 a článku 31 ods. 2 zákona o polícii generálny riaditeľ útvarov regionálnej polície (miestnych pobočiek Národnej policajnej agentúry) „usmerňuje prefektúrnú políciu a vykonáva nad ňou dozor“.

⁽⁹⁴⁾ V žiadosti o sprístupnenie informácií sa musia uviesť aj kontaktné údaje „zodpovednej osoby“ („názov útvaru [pozícia], meno, telefónne číslo kancelárie, číslo klapky atď.“).

⁽⁹⁵⁾ Najvyšší súd, rozsudok z 24. decembra 1969 [1965(A) 1187]; rozsudok z 15. apríla 2008 [2007(A) 839].

⁽⁹⁶⁾ Hoci sa tieto rozsudky netýkali zhromažďovania elektronických informácií, japonská vláda vysvetlila, že kritériá, ktoré stanovil najvyšší súd, platia pre všetky zásahy orgánov verejnej moci do práva na súkromie vrátane všetkých „dobrovoľných vyšetrovaní“, a preto sú tieto kritériá pre japonské orgány záväzné aj pri podávaní žiadostí o dobrovoľné sprístupnenie informácií. Pozri oddiel II.A.2 písm. b) bod 1 prílohy II.

⁽⁹⁷⁾ Podľa poskytnutých informácií sa tieto faktory musia považovať za „primerané v súlade so spoločensky akceptovanými konvenciami“. Pozri oddiel II.A.2 písm. b) bod 1 prílohy II.

⁽⁹⁸⁾ Pre podobné úvahy v kontexte povinných vyšetrovaní (odpočúvanie) pozri aj Najvyšší súd, rozsudok zo 16. decembra 1999, 1997 (A) 636.

⁽⁹⁹⁾ Japonské orgány v tejto súvislosti poukázali na usmernenia PPC (General Rule Edition) a na bod 5/14 „otázok a odpovedí“, ktoré PPC vypracovala k uplatňovaniu zákona APPI. Podľa japonských orgánov „vzhľadom na rastúce povedomie fyzických osôb, pokiaľ ide o ich práva na súkromie, ako aj vzhľadom na pracovné zaťaženie vyplývajúce z týchto žiadostí, sú hospodárske subjekty pri odpovediach na tieto žiadosti čoraz obozretnejšie“. Pozri oddiel II.A.2 prílohy II aj s odkazom na oznámenie Národnej policajnej agentúry z roku 1999. Podľa poskytnutých informácií skutočne došlo k prípadom, keď hospodárske subjekty odmietli spolupracovať. Napríklad spoločnosť LINE (najobľúbenejšia aplikácia pre zasielanie správ v Japonsku) vo svojej správe o transparentnosti z roku 2017 uvádza: „Po prijatí žiadostí od vyšetrovacích orgánov atď. [...] overíme primeranosť z hľadiska zákonnosti, ochrany používateľa atď. Ak pri tomto overení zistíme právne nedostatky, žiadosť zamietneme. Ak je rozsah žiadosti na účely vyšetrovania príliš široký, požiadame vyšetrovací orgán o vysvetlenie. Ak je vysvetlenie neodôvodnené, žiadosti nevyhovíme.“ Dostupné na internete: <https://linecorp.com/en/security/transparency/top>

⁽¹⁰⁰⁾ Každý osobe, ktorá „pôsobí v oblasti telekomunikácií“ môže byť uložený trest odňatia slobody s nariadeným výkonom práce v trvaní troch rokov alebo pokuta vo výške najviac 2 miliónov jenov.

⁽¹⁰¹⁾ Podľa Trestného zákona je „odôvodnené konanie“ najmä také konanie telekomunikačného operátora, ktorým vykonáva právoplatné opatrenia štátu (povinné opatrenia), napríklad keď vyšetrovacie orgány prijímajú opatrenia na základe príkazu vydaného sudcom. Pozri oddiel II.A.2 písm. b) bod 2 prílohy II s odkazom na Usmernenia o ochrane osobných informácií v oblasti telekomunikácií.

spracúvanie) a v súvislosti s ním sa stanovuje niekoľko obmedzení a záruk (pozri odôvodnenie 118) ⁽¹⁰²⁾. Obmedzenia pôvodného zhromažďovania navyše vyplývajú – aspoň nepriamo – aj zo skutočnosti, že správny orgán môže uchovávať osobné informácie „len ak je uchovávanie nevyhnutné na plnenie úloh v jeho právomoci stanovených zákonmi a inými právnymi predpismi“ (článok 3 ods. 1 zákona APPIHAO).

3.2.2. Nezávislý dozor

- (131) V Japonsku patrí zhromažďovanie elektronických informácií v oblasti presadzovania práva v trestných veciach predovšetkým ⁽¹⁰³⁾ do pôsobnosti prefektúrnej polície ⁽¹⁰⁴⁾, ktorá v tejto súvislosti podlieha rôznym úrovňam dozoru.
- (132) Po prvé, vo všetkých prípadoch, keď sa elektronické informácie zhromažďujú povinnými prostriedkami (prehliadka a zaistenie veci), musí polícia najprv získať súdny príkaz (pozri odôvodnenie 121). Preto v takýchto prípadoch zhromažďovanie vopred preverí sudca, a to na základe prísnej normy „primeraného dôvodu“.
- (133) V prípade žiadostí o dobrovoľné sprístupnenie siete k predchádzajúcemu prevereniu sudcom nedochádza, no hospodárske subjekty, ktorým sú takéto žiadosti adresované, môžu voči nim namietat bez toho, aby im hrozili akékoľvek nepriaznivé dôsledky (pričom budú musieť zohľadniť vplyv akéhokoľvek sprístupnenia informácií na súkromie). Navyše, podľa článku 192 ods. 1 Trestného poriadku musia príslušníci polície vždy spolupracovať s generálnym prokurátorom (a s prefektúrnou komisiou pre verejnú bezpečnosť) ⁽¹⁰⁵⁾ a koordinovať s nimi svoju činnosť. Generálny prokurátor môže zasa vydávať nevyhnutné všeobecné pokyny, ktorými stanoví normy pre spravodlivé vyšetrovanie, a/alebo vydať konkrétne príkazy v súvislosti s jednotlivým vyšetrovaním (článok 193 Trestného poriadku). Ak takéto pokyny a/alebo príkazy nebudú dodržané, prokuratúra môže podať návrh na začatie disciplinárneho konania (článok 194 Trestného poriadku). Prefektúrna polícia teda pôsobí pod dohľadom generálneho prokurátora.
- (134) Po druhé, podľa článku 62 ústavy môže každá snemovňa japonského parlamentu viesť vyšetrovania vo vzťahu k štátnej správe, a to aj pokiaľ ide o zákonnosť zhromažďovania informácií políciou. Na tento účel si môže vyžiadať prítomnosť a výpoveď svedkov a/alebo predloženie záznamov. Tieto vyšetrovacie právomoci sú bližšie vymedzené v zákone o parlamente, a to najmä v kapitole XII. V článku 104 zákona o parlamente sa konkrétne stanovuje, že vláda, orgány a ďalšie časti štátnej správy „musia plniť požiadavky ktorejkoľvek snemovne parlamentu alebo ktoréhokoľvek z jej výborov na predloženie správ a záznamov potrebných na posúdenie vyšetrovania.“ Odmietnutie vyhovieť takejto požiadavke je prípustné iba v prípade, keď štátna správa poskytne vierohodný dôvod, ktorý bude parlament považovať za prijateľný, alebo keď vydá formálne vyhlásenie o tom, že predloženie správ alebo záznamov by „vážne poškodilo národné záujmy“ ⁽¹⁰⁶⁾. Členovia parlamentu môžu okrem toho klásť vláde písomné otázky (články 74 a 75 zákona o parlamente), pričom v minulosti sa takéto „písomné otázky“ týkali aj nakladania s osobnými informáciami štátnou správou ⁽¹⁰⁷⁾. Úloha parlamentu pri dohľade nad výkonnou mocou je posilnená povinnosťami podávania správ, napríklad podľa článku 29 zákona o odpočúvaní.
- (135) Po tretie, prefektúrna polícia podlieha nezávislému dozoru aj v rámci výkonnej zložky moci. Ide najmä o prefektúrne komisie pre verejnú bezpečnosť zriadené na úrovni prefektúr s cieľom zabezpečiť demokratickú správu a politickú neutralitu polície ⁽¹⁰⁸⁾. Tieto komisie pozostávajú z členov menovaných guvernérom prefektúry (spomedzi občanov, ktorí v priebehu posledných piatich rokov nepracovali ako štátni zamestnanci v polícii) so súhlasom zhromaždenia prefektúry, ktorí majú zaistené funkčné obdobie (predovšetkým môžu byť odvolaní iba z náležitého dôvodu) ⁽¹⁰⁹⁾. Podľa poskytnutých informácií nie sú viazané pokynmi, a preto ich možno považovať za úplne nezávislé ⁽¹¹⁰⁾. Pokiaľ ide o úlohy a právomoci prefektúrnych komisií pre verejnú bezpečnosť, podľa

⁽¹⁰²⁾ Pokiaľ ide o práva dotýčajúcich fyzických osôb, pozri oddiel 3.1.

⁽¹⁰³⁾ Generálny prokurátor, prípadne asistent generálneho prokurátora konajúci na pokyn generálneho prokurátora, môže v zásade vyšetrovať trestný čin, ak to považuje za nevyhnutné (článok 191 ods. 1 Trestného poriadku).

⁽¹⁰⁴⁾ Podľa poskytnutých informácií Národná policajná agentúra nevykonáva jednotlivé trestné vyšetrovania. Pozri oddiel II.A.1 písm. a) prílohy II.

⁽¹⁰⁵⁾ Pozri aj článok 246 Trestného poriadku, podľa ktorého má justičná polícia povinnosť odovzdať po vykonaní vyšetrovania trestného činu spis daného prípadu generálnemu prokurátorovi („zásada odovzdávania všetkých prípadov“).

⁽¹⁰⁶⁾ Parlament môže alternatívne požadovať, aby odmietnutie odpovede prešetrila Rada pre dozor nad osobitne určenými tajomstvami a ich preskúmavanie. Pozri článok 104-II zákona o parlamente.

⁽¹⁰⁷⁾ Pozri oddiel II.B.4 prílohy II.

⁽¹⁰⁸⁾ Okrem toho, podľa ustanovení článku 100 zákona o miestnej samospráve má právomoc vyšetrovať činnosti orgánov presadzovania práva, ktoré boli zriadené na úrovni prefektúr, vrátane prefektúrnej polície aj miestne zhromaždenie.

⁽¹⁰⁹⁾ Pozri články 39 – 41 zákona o polícii. Pokiaľ ide o politickú neutralitu, pozri aj článok 42 zákona o polícii.

⁽¹¹⁰⁾ Pozri oddiel II.B.3 prílohy II („systém nezávislej rady“).

článku 38 ods. 3 v spojení s článkom 2 a článkom 36 ods. 2 zákona o polícii sú zodpovedné za „ochranu práv a slobôd fyzickej osoby“. Na tento účel majú právomoc „vykonávať dozor“⁽¹¹¹⁾ nad všetkými aktivitami prefektúrnej polície v oblasti vyšetrovania vrátane zhromažďovania osobných údajov. Komisie predovšetkým „môžu v prípade potreby dávať prefektúrnej polícii podrobné pokyny alebo pokyny v konkrétnom jednotlivom prípade skúmania zneužitia právomocí zamestnancami polície“⁽¹¹²⁾. Keď náčelník prefektúrnej polície⁽¹¹³⁾ dostane takýto pokyn alebo sa sám dozvie o možnom prípade zneužitia právomocí (vrátane porušenia zákonov alebo iného zanedbania povinností), musí daný prípad bezodkladne preskúmať a o výsledku preskúmania informovať prefektúrnu komisiu pre verejnú bezpečnosť (článok 56 ods. 3 zákona o polícii). Ak to komisia považuje za potrebné, môže tiež určiť jedného zo svojich členov, aby preskúmal stav vykonávania. Proces pokračuje až do momentu, keď je prefektúrna komisia pre verejnú bezpečnosť presvedčená o tom, že incident bol náležite vyriešený.

- (136) Navyše, pokiaľ ide o správne uplatňovanie zákona APPIHAO, príslušný minister alebo vedúci úradu (napr. generálny komisár Národnej policajnej agentúry) má právomoc vymáhať jeho dodržiavanie, pričom podlieha dohľadu ministerstva vnútra a komunikácií. Podľa článku 49 zákona APPIHAO môže ministerstvo vnútra a komunikácií „zhromažďovať správy o stave presadzovania tohto zákona“ od vedúcich správnych orgánov (ministrov). K výkonu tejto funkcie dozoru prispievajú vstupné informácie od 51 „všeobecných informačných centier“ ministerstva vnútra a komunikácií (jedno v každej prefektúre Japonska), ktoré každý rok spracúvajú tisíce dopytov od fyzických osôb⁽¹¹⁴⁾ (ktoré následne môžu odhaliť možné porušenia zákona). Ak to ministerstvo vnútra a komunikácií považuje za potrebné v záujme zabezpečenia dodržiavania zákona, môže požiadať o predloženie vysvetlení a materiálov týkajúcich sa nakladania s osobnými informáciami príslušným správnym orgánom, ako aj vydávať stanoviská v tejto súvislosti (články 50 a 51 zákona APPIHAO).

3.2.3. Individuálne prostriedky nápravy

- (137) Popri dozoru z moci úradnej majú niekoľko možností získať individuálne prostriedky nápravy aj fyzické osoby, a to prostredníctvom nezávislých orgánov (ako sú príslušné prefektúrne komisie pre verejnú bezpečnosť alebo PPC) a japonských súdov.
- (138) Po prvé, v súvislosti s osobnými informáciami zhromaždenými správnymi orgánmi majú správne orgány povinnosť „usiľovať sa náležite a urýchlene spracovať všetky sťažnosti“ týkajúce sa následného spracúvania týchto informácií (článok 48 zákona APPIHAO). Hoci kapitola IV zákona APPIHAO o individuálnych právach nie je uplatniteľná, pokiaľ ide o osobné informácie zaznamenané v „dokumentoch týkajúcich sa súdnych konaní a zaistených vecí“ (článok 53-2 ods. 2 Trestného poriadku) – čo zahŕňa osobné informácie zhromaždené v rámci vyšetrovania trestnej činnosti – fyzické osoby môžu podať sťažnosť a dovoľávať sa všeobecných zásad ochrany údajov, ako je napríklad povinnosť uchovávať osobné informácie len v prípade, „keď je uchovávanie nevyhnutné na plnenie [funkcií presadzovania práva]“ (článok 3 ods. 1 zákona APPIHAO).
- (139) Okrem toho sa článkom 79 zákona o polícii zaručuje fyzickým osobám, ktoré majú pochybnosti v súvislosti s „plnením úloh“ príslušníkmi polície, právo podať sťažnosť (príslušnej) nezávislej prefektúrnej komisii pre verejnú bezpečnosť. Uvedená komisia vybaví takéto sťažnosti „svedomito“ v súlade so zákonmi a miestnymi vyhláškami a písomne oboznámi sťažovateľa s výsledkami. Na základe svojej právomoci vykonávať dohľad nad prefektúrnou políciou a „usmerňovať ju“ so zreteľom na „zneužitie právomocí jej zamestnancami“ (článok 38 ods. 3, článok 43-2 ods. 1 zákona o polícii) môže požiadať prefektúrnu políciu, aby prešetrila skutočnosť, prijala vhodné opatrenia na základe výsledku tohto prešetrenia a podala správu o výsledkoch. Ak sa komisia domnieva, že šetrenie vykonané políciou nebolo dostatočné, môže zároveň vydať pokyny týkajúce sa vybavovania sťažnosti.
- (140) V záujme uľahčenia vybavovania sťažností Národná policajná agentúra vydala „oznámenie“ pre políciu a prefektúrne komisie pre verejnú bezpečnosť týkajúce sa riadneho vybavovania sťažností na plnenie úloh príslušníkmi polície. V tomto dokumente Národná policajná agentúra stanovuje normy pre výklad a vykonávanie článku 79 zákona o polícii. Okrem iného v ňom vyžaduje, aby prefektúrna polícia zriadila „systém vybavovania sťažností“ a aby „bezodkladne“ vybavovala všetky sťažnosti a oznamovala ich príslušnej prefektúrnej komisii pre verejnú

⁽¹¹¹⁾ Pozri článok 5 ods. 3 a článok 38 ods. 3 zákona o polícii.

⁽¹¹²⁾ Pozri článok 38 ods. 3 a článok 43-2 ods. 1 zákona o polícii. Ak prefektúrna komisia pre verejnú bezpečnosť „vydá pokyn“ v zmysle článku 43-2 ods. 1, môže nariadiť výboru, ktorý vymenovala, aby monitoroval jeho vykonávanie (odsek 2). Komisia môže takisto odporučiť disciplinárne konanie proti náčelníkovi prefektúrnej polície (článok 50 ods. 2), ako aj iným príslušníkom polície (článok 55 ods. 4 zákona o polícii) alebo ich odvolanie.

⁽¹¹³⁾ To isté sa vzťahuje na generálneho superintendanta Tokijskej metropolitnej polície (pozri článok 48 ods. 1 zákona o polícii).

⁽¹¹⁴⁾ Podľa poskytnutých informácií „všeobecné informačné centrá“ v účtovnom roku 2017 (od apríla 2017 do marca 2018) spracovali spolu 5 186 dopytov fyzických osôb.

bezpečnosť. V oznámení sa sťažnosti vymedzujú ako nároky, ktorých cieľom je náprava „konkrétneho znevýhodnenia, ku ktorému došlo v dôsledku nezákonného alebo nevhodného správania“⁽¹¹⁵⁾ alebo „neprijatia nevyhnutných opatrení zo strany príslušníka polície pri plnení jeho povinností“⁽¹¹⁶⁾, ako aj akékoľvek „sťažnosti/nespokojnosť v súvislosti s nevhodným spôsobom plnenia povinností príslušníkom polície“. Vecná pôsobnosť sťažnosti je teda vymedzená široko, aby zahŕňala všetky nároky týkajúce sa nezákonného zhromažďovania údajov, pričom sťažovateľ nemusí preukázať, že v dôsledku konania príslušníka polície utrpel ujmu. Dôležité je, že podľa oznámenia sa cudzincom (okrem iných) poskytne pomoc pri formulovaní sťažnosti. Prefektúrne komisie pre verejnú bezpečnosť majú v nadväznosti na sťažnosť zabezpečiť, aby prefektúrna polícia preskúmala skutočnosť, vykonala opatrenia „v závislosti od výsledku preskúmania“ a podala správu o výsledkoch. Ak sa komisia domnieva, že preskúmanie nie je dostatočné, vydá pokyn týkajúci sa vybavenia sťažnosti, ktorým sa prefektúrna polícia musí riadiť. Komisia na základe predložených správ a prijatých opatrení informuje danú fyzickú osobu, pričom okrem iného uvedie opatrenia prijaté na vybavenie sťažnosti. V oznámení Národnej policajnej agentúry sa zdôrazňuje, že sťažnosti treba vybavovať „úprimne“ a že výsledok treba oznámiť „v lehote [...], ktorá sa považuje za primeranú vzhľadom na spoločenské normy a zdravý rozum.“

- (141) Po druhé, keďže prostriedkov nápravy sa bude, prirodzene, treba domáhať v zahraničnom systéme a v cudzom jazyku, japonská vláda využila svoje právomoci a v záujme uľahčenia získania nápravy pre fyzické osoby z EÚ, ktorých osobné údaje sa prenášajú hospodárskym subjektom v Japonsku a následne k nim pristupujú orgány verejnej moci, vytvorila osobitný mechanizmus vybavovania a riešenia sťažností v tejto oblasti, ktorý spravuje a nad ktorým dohliada PPC. Tento mechanizmus vychádza z povinnosti spolupracovať, ktorú japonským orgánom verejnej moci ukladá zákon APPI, a z osobitnej úlohy PPC, pokiaľ ide o medzinárodné prenosy údajov z tretích krajín na základe článku 6 zákona APPI a základnej politiky (stanovenej japonskou vládou prostredníctvom nariadenia vlády). Podrobnosti o tomto mechanizme sú uvedené v oficiálnych vyhláseniach, uisteniach a záväzkoch poskytnutých japonskou vládou, ktoré sú pripojené k tomuto rozhodnutiu ako príloha II. Na tento mechanizmus sa nevzťahuje požiadavka na aktívnu legitímáciu a je dostupný každej fyzickej osobe bez ohľadu na to, či je podozrivá alebo obvinená zo spáchania trestného činu.
- (142) Na základe tohto mechanizmu môže fyzická osoba, ktorá má podozrenie, že orgány verejnej moci v Japonsku (vrátane tých, ktoré sú zodpovedné za presadzovanie práva v trestných veciach) zhromaždili alebo používajú jej údaje prenesené z Európskej únie v rozpore s platnými pravidlami, podať sťažnosť PPC (samostatne alebo prostredníctvom svojho orgánu pre ochranu údajov v zmysle článku 51 všeobecného nariadenia o ochrane údajov). PPC bude povinná zaoberať sa sťažnosťou a v prvom kroku o nej informovať príslušné orgány verejnej moci vrátane príslušných dozorných orgánov. Tieto orgány majú povinnosť spolupracovať s PPC „okrem iného tak, že jej poskytnú potrebné informácie a príslušné materiály, aby PPC mohla zhodnotiť, či k zhromaždeniu osobných informácií alebo ich následnému použitiu došlo v súlade s platnými pravidlami“⁽¹¹⁷⁾. Táto povinnosť, odvodená z článku 80 zákona APPI, (podľa ktorého majú japonské orgány verejnej moci povinnosť spolupracovať s PPC), má všeobecnú platnosť, a preto sa vzťahuje aj na preskúmanie akýchkoľvek opatrení v oblasti vyšetrovania, ktoré prijali takéto orgány, ktoré sa navyše k takejto spolupráci zaviazali prostredníctvom písomných uistení príslušných ministerstiev a vedúcich úradov, ako sú uvedené v prílohe II.
- (143) Ak z hodnotenia vyplynie, že došlo k porušeniu platných pravidiel, „spolupráca príslušných orgánov verejnej moci s PPC zahŕňa povinnosť toto porušenie napraviť“, čo v prípade nezákonného zhromažďovania osobných informácií zahŕňa vymazanie takýchto údajov. Dôležité je, že táto povinnosť sa plní pod dozorom PPC, ktorá „pred uzavretím hodnotenia potvrdí, že porušenie bolo v plnom rozsahu napravené.“
- (144) Po uzavretí hodnotenia PPC v primeranej lehote danej fyzickej osobe oznámi výsledok hodnotenia vrátane prípadných nápravných opatrení, ktoré sa prijali. PPC zároveň informuje fyzickú osobu o možnosti vyžiadať si od príslušného orgánu verejnej moci potvrdenie o výsledku a o tom, ktorému orgánu by sa takáto žiadosť

⁽¹¹⁵⁾ Podmienka „konkrétneho znevýhodnenia“ znamená len to, že konanie (alebo nekonanie) polície sa musí sťažovateľa konkrétne týkať, nie to, že by musel preukázať nejakú ujmu.

⁽¹¹⁶⁾ K týmto úlohám patrí aj dodržiavanie právnych predpisov vrátane právnych požiadaviek na zhromažďovanie a využívanie osobných údajov. Pozri článok 2 ods. 2 a článok 3 zákona o polícii.

⁽¹¹⁷⁾ Pri uskutočňovaní tohto hodnotenia bude PPC spolupracovať s ministerstvom vnútra a komunikácií, ktoré, ako sa vysvetľuje v odôvodnení 136, môže požiadať o predloženie vysvetlení a materiálov týkajúcich sa nakladania s osobnými informáciami príslušným správny orgánom, ako aj vydávať stanoviská v tejto súvislosti (články 50 a 51 zákona APPIHAO).

o potvrdenie mala podať. Možnosť získať takéto potvrdenie zahŕňajúce dôvody, z ktorých vychádza rozhodnutie príslušného orgánu, môže fyzickej osobe pomôcť pri prijímaní akýchkoľvek ďalších krokov, a to aj pri domáhaní sa súdnych prostriedkov nápravy. Podrobné informácie o výsledku hodnotenia možno obmedziť, ak existujú opodstatnené dôvody domnievať sa, že oznámenie takýchto informácií by mohlo ohroziť prebiehajúce vyšetrovanie.

- (145) Po tretie, fyzická osoba, ktorá nesúhlasí s rozhodnutím sudcu o zaistení (so súdnym príkazom na zaistenie) ⁽¹¹⁸⁾ jej osobných údajov alebo s opatreniami polície či prokuratúry, ktorými sa takéto rozhodnutie vykonáva, môže podať žiadosť o zrušenie alebo zmenu takeého rozhodnutia alebo takýchto opatrení (článok 429 ods. 1, článok 430 ods. 1 a 2 Trestného poriadku, článok 26 zákona o odpočúvaní) ⁽¹¹⁹⁾. Ak sa preskúmavajúci súd domnieva, že samotný súdny príkaz alebo jeho výkon („postup zaistenia“) je protiprávny, žiadosti vyhovie a nariadi vrátenie zaistených vecí ⁽¹²⁰⁾.
- (146) Po štvrté, fyzická osoba, ktorá sa domnieva, že zhromažďovanie jej osobných informácií v rámci vyšetrovania trestného činu bolo nezákonné, môže túto nezákonnosť uplatniť – ako nepriamejšiu formu súdnej kontroly – v rámci svojho trestného konania. Ak s tým bude súd súhlasiť, daný dôkaz bude vylúčený ako neprípustný.
- (147) A napokon, podľa článku 1 ods. 1 zákona o opravných prostriedkoch proti štátu môže súd priznať dotýčnej fyzickej osobe odškodnenie, ak jej štátny úradník vykonávajúci verejnú moc štátu pri plnení svojich úloh protiprávne a vlastnou vinou (úmyselne alebo z nebanlivosti) spôsobil škodu. Podľa článku 4 zákona o opravných prostriedkoch proti štátu vychádza zodpovednosť štátu za škody z ustanovení Občianskeho zákonníka. V tejto súvislosti sa v článku 710 Občianskeho zákonníka stanovuje, že zodpovednosť zahŕňa aj iné škody ako škody na majetku, a teda aj morálnu ujmu (napríklad v podobe „duševného utrpenia“). To zahŕňa prípady, keď bolo súkromie fyzickej osoby narušené protiprávnym sledovaním a/alebo zhromažďovaním jej osobných informácií (napr. protiprávnym vykonaním súdneho príkazu) ⁽¹²¹⁾.
- (148) Okrem peňažnej náhrady môžu fyzické osoby na základe svojich práv na súkromie podľa článku 13 ústavy ⁽¹²²⁾ za určitých podmienok získať aj súdny príkaz (napr. na vymazanie osobných údajov zhromaždených orgánmi verejnej moci).
- (149) V súvislosti so všetkými týmito možnosťami získania nápravy mechanizmus riešenia sporov vytvorený japonskou vládou zabezpečuje, že fyzická osoba, ktorá stále nie je spokojná s výsledkom tohto postupu, sa môže obrátiť na PPC, „ktorá fyzickú osobu informuje o rôznych možnostiach a podrobných postupoch získania nápravy podľa japonských zákonov a iných právnych predpisov.“ PPC navyše „poskytne danej fyzickej osobe podporu vrátane poradenstva a pomoci pri akýchkoľvek ďalších krokoch vo vzťahu k príslušnému správneému či súdneému orgánu.“
- (150) To zahŕňa aj využitie procesných práv podľa Trestného poriadku. Napríklad „ak z hodnotenia vyplynie, že daná fyzická osoba je podozrivá v trestnej veci, PPC ju informuje o tejto skutočnosti“ ⁽¹²³⁾, ako aj o možnosti, poskytovanej článkom 259 Trestného poriadku, požiadať prokuratúru, aby ju informovala, keď sa rozhodne nezačať trestné konanie. Taktiež, ak sa pri hodnotení zistí, že sa začalo konanie týkajúce sa osobných informácií danej fyzickej osoby a že dané konanie bolo ukončené, PPC upozorní danú fyzickú osobu na možnosť nahliadnuť do spisu podľa článku 53 Trestného poriadku (a článku 4 zákona o konečných trestných spisoch). Získanie prístupu

⁽¹¹⁸⁾ To zahŕňa aj súdny príkaz na odpočúvanie, v súvislosti s ktorým sa v zákone o odpočúvaní stanovuje osobitná oznamovacia povinnosť (článok 23). Podľa uvedeného ustanovenia musí vyšetrovací orgán písomne informovať fyzické osoby, ktorých komunikácia bola odpočúvaná (a teda zahrnutá do záznamu z odpočúvania), o tejto skutočnosti. Ďalším príkladom je článok 100 ods. 3 Trestného poriadku, podľa ktorého musí súd informovať odosielateľa alebo príjemcu, keď zaistí poštové zásielky alebo telegramy zaslané obvinenému alebo obvineným, s výnimkou prípadov, keď hrozí riziko, že by takéto informovanie bránilo súdneému konaniu. V článku 222 ods. 1 Trestného poriadku sa uvádzajú krížové odkazy na toto ustanovenie v súvislosti s prehliadkami a zaisteniami uskutočňovanými vyšetrovacím orgánom.

⁽¹¹⁹⁾ Hoci takáto žiadosť nemá automatický účinok pozastavenia výkonu rozhodnutia o zaistení, preskúmavajúci súd môže nariadiť pozastavenie až do vydania rozhodnutia vo veci samej. Pozri článok 429 ods. 2, článok 432 v spojení s článkom 424 Trestného poriadku.

⁽¹²⁰⁾ Pozri oddiel II.C.1 prílohy II.

⁽¹²¹⁾ Pozri oddiel II.C.2 prílohy II.

⁽¹²²⁾ Pozri napr. Okresný súd Tokio, rozsudok z 24. marca 1988 (č. 2925); Okresný súd Osaka, rozsudok z 26. apríla 2007 (č. 2925). Podľa Okresného súdu Osaka bude pritom treba nájsť rovnováhu medzi viacerými faktormi, ako napríklad: i) povaha a obsah predmetných osobných informácií; ii) spôsob, akým boli zhromaždené; iii) nevýhody pre fyzickú osobu v prípade, že sa informácie nevymažú a iv) verejný záujem vrátane nevýhod pre orgán verejnej moci v prípade, že sa informácie vymažú.

⁽¹²³⁾ V každom prípade, po začatí trestného konania dá prokuratúra obvinenej osobe možnosť do týchto dôkazov nahliadnuť (pozri články 298 až 299 Trestného poriadku). Pokiaľ ide o obete trestných činov, pozri články 316 až 333 Trestného poriadku.

k spisu je dôležité, pretože pomôže fyzickej osobe lepšie pochopiť vyšetrovanie, ktoré sa proti nej vedie, a pripraviť tak prípadnú žalobu na súd (napr. o náhradu škody) v prípade, že sa domnieva, že jej údaje boli zhromaždené alebo použité nezákonne.

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

- (151) Podľa japonských orgánov neexistuje v Japonsku žiadny zákon, ktorý by povoľoval povinné žiadosti o informácie alebo „správne odpočúvania“ mimo vyšetrovania trestných činov. Z dôvodov národnej bezpečnosti sa teda informácie môžu získavať len z informačného zdroja, ku ktorému má voľný prístup ktokoľvek, alebo dobrovoľným sprístupnením. Hospodárske subjekty, ktoré dostanú žiadosť o dobrovoľnú spoluprácu (vo forme sprístupnenia elektronických informácií), nie sú zo zákona povinné takéto informácie poskytnúť⁽¹²⁴⁾.
- (152) Navyše, podľa poskytnutých informácií majú právomoc zhromažďovať elektronické informácie uchovávané japonskými hospodárskymi subjektmi z dôvodov národnej bezpečnosti len štyri subjekty štátnej správy, a to: i) Spravodajská a vyšetrovacia služba vlády; ii) ministerstvo obrany; iii) polícia [Národná policajná agentúra⁽¹²⁵⁾ aj prefektúrna polícia]; a iv) Spravodajská služba pre verejnú bezpečnosť (ďalej len „PSIA“). Spravodajská a vyšetrovacia služba vlády však nikdy nezhrmažďuje informácie priamo od hospodárskych subjektov, a to ani prostredníctvom odpočúvania komunikácie. V prípade, že dostane informácie od iných orgánov štátnej správy, aby vláde poskytla analýzu, sú to tieto iné orgány, ktoré musia dodržať právne predpisy vrátane obmedzení a záruk analyzovaných v tomto rozhodnutí. Jej činnosti teda nie sú v kontexte prenosu relevantné.

3.3.1. Právny základ a uplatniteľné obmedzenia/záruky

- (153) Podľa poskytnutých informácií ministerstvo obrany zhromažďuje (elektronické) informácie na základe zákona o zriadení ministerstva obrany. Podľa článku 3 tohto zákona je poslaním ministerstva obrany riadiť ozbrojené sily a operovať s nimi a „plniť s tým súvisiace úlohy s cieľom zaistiť mier v krajine, ako aj nezávislosť a bezpečnosť národa.“ V článku 4 ods. 4 sa stanovuje, že ministerstvo obrany má právomoci v oblasti „obransy a ochrany“, akcií uskutočňovaných obrannými silami, ako aj vysielania ozbrojených síl vrátane zhromažďovania informácií nevyhnutných na plnenie uvedených úloh. (Elektronické) informácie od hospodárskych subjektov je však oprávnené zbierať iba prostredníctvom dobrovoľnej spolupráce.
- (154) Pokiaľ ide o prefektúrnu políciu, medzi jej povinnosti a úlohy patrí „udržiavanie verejnej bezpečnosti a verejného poriadku“ (článok 35 ods. 2 v spojení s článkom 2 ods. 1 zákona o polícii). V rámci tohto rozsahu právomoci môže polícia zhromažďovať informácie, ale len na dobrovoľnom základe bez právnej sily. Činnosti polície musia byť navyše „prísne obmedzené“ na to, čo je potrebné na plnenie jej úloh. Polícia musí okrem toho konať „nestranne, nezaujatane, nepredpojatá a spravodlivo“ a nikdy nesmie zneužiť svoje právomoci „akýmkoľvek spôsobom, ktorý by zasahoval do práv a slobôd fyzickej osoby zaručených Ústavou Japonska“ (článok 2 zákona o polícii).
- (155) A na záver, Spravodajská služba pre verejnú bezpečnosť môže uskutočňovať vyšetrovania na základe zákona o predchádzaní podvratnej činnosti (ďalej len „zákon SAPA“) a zákona o kontrole organizácií, ktoré sa dopustili plošnej masovej vraždy (ďalej len „zákon ACO“), keď sú takéto vyšetrovania nevyhnutné na prípravu prijatia opatrení na kontrolu určitých organizácií⁽¹²⁶⁾. Komisia pre skúmanie verejnej bezpečnosti môže na základe oboch zákonov a na základe žiadosti generálneho riaditeľa Spravodajskej služby pre verejnú bezpečnosť vydávať určité „dispozície“ (v prípade zákona ACO nariadiť sledovanie/vydať zákazy⁽¹²⁷⁾, v prípade zákona SAPA nariadiť zrušenie/vydať zákazy⁽¹²⁸⁾) a Spravodajská služba pre verejnú bezpečnosť môže v tejto súvislosti vykonávať vyšetrovania⁽¹²⁹⁾. Podľa poskytnutých informácií sa tieto vyšetrovania vždy vykonávajú na dobrovoľnom základe, čo

⁽¹²⁴⁾ Hospodárske subjekty sa preto môžu slobodne rozhodnúť, že nebudú spolupracovať, a to bez akéhokoľvek rizika sankcií alebo iných nepriaznivých dôsledkov. Pozri oddiel III.A.1 prílohy II.

⁽¹²⁵⁾ Podľa poskytnutých informácií je však hlavnou úlohou Národnej policajnej agentúry koordinovať vyšetrovania jednotlivých útvarov prefektúrnej polície a zabezpečovať výmenu informácií so zahraničnými orgánmi. Dokonca aj v tejto úlohe Národná policajná agentúra podlieha dozoru zo strany Národnej komisie pre verejnú bezpečnosť, ktorá okrem iného zodpovedá za ochranu práv a slobôd fyzických osôb (článok 5 ods. 1 zákona o polícii).

⁽¹²⁶⁾ Pozri oddiel III.A.1 bod 3 prílohy II. Rozsah pôsobnosti týchto dvoch zákonov je obmedzený, pričom zákon SAPA sa vzťahuje na „teroristické podvratné činnosti“ a zákon ACO na „skutok plošnej masovej vraždy“ (t. j. „teroristickú podvratnú činnosť“ podľa zákona SAPA „vedúcu k plošnej vražde veľkého počtu osôb“).

⁽¹²⁷⁾ Pozri články 5 a 8 zákona ACO. Súčasťou dispozície nariaďujúcej sledovanie je aj povinnosť informovať organizáciu, ktorej sa opatrenie týka. Pokiaľ ide o procesné záruky, najmä požiadavky na transparentnosť a predchádzajúce povolenie Komisiou pre skúmanie verejnej bezpečnosti, pozri články 12, 13, 15 – 27 zákona ACO.

⁽¹²⁸⁾ Pozri články 5 a 7 zákona SAPA. Pokiaľ ide o procesné záruky, najmä požiadavky na transparentnosť a predchádzajúce povolenie Komisiou pre skúmanie verejnej bezpečnosti, pozri články 11 – 25 zákona SAPA.

⁽¹²⁹⁾ Pozri článok 27 zákona SAPA a články 29 a 30 zákona ACO.

znamená, že Spravodajská služba pre verejnú bezpečnosť nemôže nútiť majiteľa osobných informácií, aby takéto informácie poskytol⁽¹³⁰⁾. Kontroly a vyšetrovania sa vždy vykonávajú iba v minimálnom rozsahu nevyhnutnom na dosiahnutie účelu kontroly a za žiadnych okolností sa nesmú vykonávať tak, aby „neprimerane“ obmedzovali práva a slobody zaručené Ústavou Japonska (článok 3 ods. 1 zákona SAPA/zákona ACO). Navyše, podľa článku 3 ods. 2 zákona SAPA/zákona ACO nesmie Spravodajská služba pre verejnú bezpečnosť za žiadnych okolností zneužívať takéto kontroly ani vyšetrovania uskutočňované na prípravu takýchto kontrol. Ak príslušník Spravodajskej služby pre verejnú bezpečnosť zneužil svoju právomoc podľa príslušného zákona tým, že určitú osobu donútil, aby urobila čokoľvek, čo urobiť nemusí, alebo zasahoval do výkonu práv danej osoby, môže čeliť trestnoprávnym sankciám podľa článku 45 zákona SAPA alebo článku 42 zákona ACO. A napokon, v oboch zákonoch sa výslovne stanovuje, že ich ustanovenia vrátane právomocí, ktoré sa v týchto zákonoch udeľujú, „sa za žiadnych okolností nesmú vykladať širšie“ (článok 2 zákona SAPA/zákona ACO).

(156) Vo všetkých prípadoch prístupu vlády z dôvodov národnej bezpečnosti opísaných v tomto oddiele sa uplatňujú obmedzenia stanovené Najvyšším súdom Japonska pre dobrovoľné vyšetrovania, čo znamená, že zhromažďovanie (elektronických) informácií musí byť v súlade so zásadami nevyhnutnosti a primeranosti („vhodný spôsob“)⁽¹³¹⁾. Ako výslovne potvrdili japonské orgány „zhromažďovanie a spracúvanie informácií sa uskutočňuje iba v rozsahu nevyhnutnom na vykonávanie konkrétnych úloh príslušného orgánu verejnej moci, ako aj na základe konkrétnych hrozieb“. Preto „na základe toho je vylúčené plošné a nerozlišujúce zhromažďovanie osobných informácií alebo prístup k nim na účely národnej bezpečnosti“⁽¹³²⁾.

(157) Aj všetky osobné informácie uchovávané orgánmi verejnej moci na účely národnej bezpečnosti budú po zhromaždení patriť do rozsahu pôsobnosti zákona APPIHAO a bude sa na ne teda vzťahovať ochrana zabezpečená týmto zákonom, pokiaľ ide o následné uchovávanie, používanie a sprístupňovanie týchto informácií (pozri odôvodnenie 118).

3.3.2. Nezávislý dozor

(158) Na zhromažďovanie osobných informácií na účely národnej bezpečnosti sa vzťahuje niekoľko úrovní dozoru zo strany troch zložiek štátnej správy.

(159) Po prvé, japonský parlament môže na základe svojich právomocí parlamentnej kontroly (článok 62 ústavy, článok 104 zákona o parlamente) prostredníctvom svojich osobitných výborov skúmať zákonnosť vyšetrovaní; pozri odôvodnenie 134. K tejto funkcii dozoru prispievajú osobitné povinnosti podávania správ o činnostiach vykonávaných podľa niektorých z už uvedených právnych základov⁽¹³³⁾.

(160) Po druhé, v rámci výkonnej zložky moci existuje niekoľko mechanizmov dozoru.

(161) Pokiaľ ide o ministerstvo obrany, dozor vykonáva Úrad generálneho inšpektora pre dodržiavanie právnych predpisov (ďalej len „úrad generálneho inšpektora“)⁽¹³⁴⁾, ktorý bol zriadený na základe článku 29 zákona o zriadení ministerstva obrany ako úrad v rámci ministerstva obrany, ktorý pôsobí pod dohľadom ministra obrany (ktorému podlieha), ale je nezávislý od prevádzkových útvarov tohto ministerstva. Úrad generálneho inšpektora má za úlohu zabezpečovať dodržiavanie zákonov a iných právnych predpisov, ako aj riadne plnenie úloh úradníkmi ministerstva obrany. Medzi jeho právomoci patrí právomoc vykonávať tzv. inšpekcie obrany, a to tak v pravidelných intervaloch („pravidelné inšpekcie obrany“), ako aj v jednotlivých prípadoch („osobitné inšpekcie obrany“), ktoré sa v minulosti vzťahovali aj na náležité nakladanie s osobnými informáciami⁽¹³⁵⁾. V súvislosti s takýmito inšpekciami môže úrad

⁽¹³⁰⁾ Pozri oddiel III.A.1 bod 3 prílohy II.

⁽¹³¹⁾ Pozri oddiel III.A.2 písm. b) prílohy II: „Z judikatúry najvyššieho súdu vyplýva, že na to, aby orgány mohli hospodárskemu subjektu adresovať žiadosť o dobrovoľnú spoluprácu, musí byť táto žiadosť nevyhnutná na vyšetrovanie podozrenia zo spáchania trestného činu a musí byť primeraná vzhľadom na dosiahnutie účelu daného vyšetrovania. Hoci sa vyšetrovania, ktoré vykonávajú vyšetrovacie orgány v oblasti národnej bezpečnosti, líšia od vyšetrovaní vedených vyšetrovacími orgánmi v oblasti presadzovania práva, tak pokiaľ ide o ich právny základ, ako aj účel, aj v oblasti národnej bezpečnosti sa podobne uplatňujú hlavné zásady nevyhnutnosti vyšetrovania a „vhodnosti spôsobu“, ktoré treba dodržiavať s náležitým zreteľom na konkrétnu okolnosť každého prípadu.“

⁽¹³²⁾ Pozri oddiel III.A.2 písm. b) prílohy II.

⁽¹³³⁾ Pozri napr. článok 36 zákona SAPA/článok 31 zákona ACO (pre Spravodajskú službu pre verejnú bezpečnosť).

⁽¹³⁴⁾ Vedúcim úradu generálneho inšpektora je bývalý generálny prokurátor. Pozri oddiel III.B.3 prílohy II.

⁽¹³⁵⁾ Pozri oddiel III.B.3 prílohy II. Podľa poskytnutého príkladu sa pravidelná inšpekcia obrany v súvislosti s „informovanosťou o dodržiavaní právnych predpisov a pripravenosťou naň“ uskutočnená v roku 2016 zameriavala okrem iného aj na „stav ochrany osobných informácií“ (správa, uchovávanie atď.). Vo výslednej správe sa uvádzajú prípady nenáležitej správy údajov a vyzýva sa na zlepšenia v tejto súvislosti. Ministerstvo obrany uverejnilo túto správu na svojom webovom sídle.

generálneho inšpektora vstupovať do priestorov (kancelárií) a požadovať predloženie dokumentov alebo informácií vrátane vysvetlení zástupcu námestníka ministra obrany. Inšpekcia sa uzatvára správou ministrovi obrany, v ktorej sa uvádzajú zistenia a opatrenia na zlepšenie (ktorých vykonanie možno opäť overiť prostredníctvom ďalších inšpekcií). Správa je následne východiskom pre pokyny ministra obrany na vykonanie opatrení nevyhnutných na riešenie danej situácie; vykonaním takýchto opatrení je poverený zástupca námestníka ministra, ktorý musí informovať o opatreniach prijatých v nadväznosti na správu.

- (162) Pokiaľ ide o prefektúrnu políciu, dozor zabezpečujú nezávislé prefektúrne komisie pre verejnú bezpečnosť, ako sa vysvetľuje v odôvodnení 135 v súvislosti s presadzovaním práva v trestných veciach.
- (163) A napokon, ako už bolo uvedené, Spravodajská služba pre verejnú bezpečnosť môže vykonávať vyšetrovania len pokiaľ sú nevyhnutné vzhľadom na prijatie dispozície nariaďujúcej zákaz, zrušenie alebo sledovanie podľa zákona SAPA/zákona ACO, pričom nezávislá⁽¹³⁶⁾ Komisia pre skúmanie verejnej bezpečnosti vykonáva nad týmito dispozíciami *ex ante* dozor. Osobitne určení inšpektori okrem toho vykonávajú pravidelné/periodické inšpekcie (ktoré sa komplexným spôsobom zameriavajú na operácie Spravodajskej služby pre verejnú bezpečnosť)⁽¹³⁷⁾ a osobitné vnútorné inšpekcie⁽¹³⁸⁾ činností jednotlivých útvarov/úradov atď., ktoré môžu viesť k vydaniu pokynov vedúcim príslušných útvarov atď., aby prijali opatrenia na nápravu alebo zlepšenie.
- (164) Tieto mechanizmy dozoru, ktoré sú ďalej posilnené možnosťou fyzických osôb iniciovať zásah PPC ako nezávislého dozorného orgánu (pozri ďalej bod 168), poskytujú primerané záruky proti riziku, že japonské orgány zneužijú svoje právomoci v oblasti národnej bezpečnosti, a proti akémukoľvek nezákonnému zhromažďovaniu elektronických informácií.

3.3.3. Individuálne prostriedky nápravy

- (165) Čo sa týka individuálnych prostriedkov nápravy, v súvislosti s osobnými informáciami zhromažďovanými, a teda „uchovávanými“ správnymi orgánmi, tieto orgány majú povinnosť „usilovať sa náležite a urýchlene spracovať všetky sťažnosti“ týkajúce sa takéhoto spracúvania (článok 48 zákona APPIHAO).
- (166) Okrem toho, na rozdiel od prípadov vyšetrovania trestných činov majú fyzické osoby (vrátane cudzích štátnych príslušníkov žijúcich v zahraničí) podľa zákona APPIHAO v zásade právo na sprístupnenie⁽¹³⁹⁾, opravu (vrátane vymazania) a zastavenie používania/poskytovania. Vedúci správneho orgánu však môže odmietnuť sprístupniť informácie „v súvislosti s ktorými existujú opodstatnené dôvody [...] konštatovať, že ich sprístupnenie by pravdepodobne viedlo k ohrozeniu národnej bezpečnosti“ [článok 14 bod iv) zákona APPIHAO], pričom tak dokonca môže urobiť bez odhalenia existencie týchto informácií (článok 17 zákona APPIHAO). Podobne, hoci fyzická osoba môže podľa článku 36 ods. 1 písm. i) zákona APPIHAO požiadať o ukončenie používania alebo o výmaz informácií, ak správny orgán získal tieto informácie nezákonne alebo ich uchováva/používa nad rámec toho, čo je nevyhnutné na dosiahnutie stanoveného účelu, orgán môže žiadosť zamietnuť, ak zistí, že ukončenie používania „by mohlo zabrániť riadnemu vykonaniu záležitostí súvisiacich s účelom použitia uchovávaných osobných informácií z dôvodu povahy uvedených záležitostí“ (článok 38 zákona APPIHAO). Ak je však možné jednoducho oddeliť a vylúčiť časti, na ktoré sa vzťahuje výnimka, správne orgány musia sprístupniť informácie aspoň čiastočne (pozri napr. článok 15 ods. 1 zákona APPIHAO)⁽¹⁴⁰⁾.

⁽¹³⁶⁾ Podľa zákona o zriadení Komisie pre skúmanie verejnej bezpečnosti vykonávajú predseda a členovia tejto komisie „svoju právomoc nezávisle“ (článok 3). Vymenúva ich predseda vlády so súhlasom oboch snemovni parlamentu, pričom môžu byť odvolaní len z „určitého dôvodu“ (napr. uväznenie, pochybenie, duševné alebo telesné ochorenie, začatie konkurzného konania).

⁽¹³⁷⁾ Nariadenie o periodickej inšpekcii Spravodajskej služby pre verejnú bezpečnosť (generálny riaditeľ Spravodajskej služby pre verejnú bezpečnosť, pokyn č. 4, 1986).

⁽¹³⁸⁾ Nariadenie o osobitnej inšpekcii Spravodajskej služby pre verejnú bezpečnosť (generálny riaditeľ Spravodajskej služby pre verejnú bezpečnosť, pokyn č. 11, 2008). Osobitné inšpekcie sa vykonávajú, keď to generálny riaditeľ Spravodajskej služby pre verejnú bezpečnosť bude považovať za potrebné.

⁽¹³⁹⁾ Ide o právo dostať kópiu „uchovávaných osobných informácií“.

⁽¹⁴⁰⁾ Pozri aj možnosť „sprístupnenia podľa vlastného uváženia“, dokonca aj v prípade, keď sú v „uchovávaných osobných informáciách“, ktorých sprístupnenie sa požaduje, zahrnuté „informácie, ktoré sa nemajú sprístupniť“ (článok 16 zákona APPIHAO).

- (167) Správny orgán musí v každom prípade v určitej lehote (30 dní, ktoré môžu byť za určitých podmienok predĺžené o ďalších 30 dní) prijať písomné rozhodnutie. Ak je žiadosť zamietnutá, ak sa jej vyhovie len sčasti alebo ak fyzická osoba považuje konanie správneho orgánu za „nezákonné alebo nespravodlivé“ z iných dôvodov, môže požiadať o správne preskúmanie na základe zákona o preskúmaní sťažností v správnych veciach⁽¹⁴¹⁾. V takom prípade vedúci správneho orgánu, ktorý rozhoduje o odvolaní, konzultuje s Radou pre preskúmanie sprístupňovania informácií a ochrany osobných informácií (články 42 a 43 zákona APPIHAO), ktorá je špecializovanou nezávislou radou, ktorej členovia sú menovaní predsedom vlády so súhlasom oboch snemovní parlamentu. Podľa poskytnutých informácií môže rada pre preskúmanie vykonať prešetrovanie⁽¹⁴²⁾ a v tejto súvislosti požiadať správny orgán, aby poskytol uchovávané osobné informácie vrátane akéhokoľvek utajeného obsahu, ako aj ďalšie informácie a dokumenty. Hoci konečná správa, zaslaná sťažovateľovi, ako aj správne orgánu a zverejnená, nie je právne záväzná, odporúčania v nej uvedené sa takmer vždy dodržia⁽¹⁴³⁾. Fyzická osoba má navyše možnosť napadnúť rozhodnutie o odvolaní na súde na základe Správneho súdneho poriadku. To otvára priestor na súdnu kontrolu používania výnimky, resp. výnimiek z dôvodu národnej bezpečnosti vrátane toho, či bola takáto výnimka zneužitá alebo je stále opodstatnená.
- (168) V záujme uľahčenia výkonu vyššie uvedených práv podľa zákona APPIHAO zriadilo ministerstvo vnútra a komunikácií 51 „všeobecných informačných centier“, ktoré poskytujú konsolidované informácie o týchto právach, uplatniteľných postupoch podávania žiadostí a možnostiach získania prostriedkov nápravy⁽¹⁴⁴⁾. Pokiaľ ide o správne orgány, tie sú povinné poskytovať „informácie, ktoré prispievajú k presnejšiemu určeniu uchovávaných osobných informácií“⁽¹⁴⁵⁾ a prijať „ďalšie vhodné opatrenia na uľahčenie veci pre osobu, ktorá má v úmysle podať žiadosť“ (článok 47 ods. 1 zákona APPIHAO).
- (169) Rovnako ako v prípade vyšetrení v oblasti presadzovania práva v trestných veciach, aj v oblasti národnej bezpečnosti môžu fyzické osoby získať individuálne prostriedky nápravy, keď sa obrátia priamo na PPC. Tým sa spustí osobitný postup riešenia sporov, ktorý japonská vláda zaviedla pre fyzické osoby z EÚ, ktorých osobné údaje sa prenášajú na základe tohto rozhodnutia (pozri podrobné vysvetlenia v odôvodneniach 141 až 144 a v odôvodnení 149).
- (170) Fyzické osoby sa môžu okrem toho domáhať súdnych prostriedkov nápravy formou žaloby o náhradu škody podľa zákona o opravných prostriedkoch proti štátu, čo zahŕňa aj morálnu ujmu a za určitých podmienok aj vymazanie zhromaždených údajov (pozri odôvodnenie 147).

4. ZÁVER: PRIMERANÁ ÚROVEŇ OCHRANY OSOBNÝCH ÚDAJOV PRENÁŠANÝCH Z EURÓPSKEJ ÚNIE HOSPODÁRSKYM SUBJEKTOM V JAPONSKU

- (171) Komisia sa domnieva, že zákon APPI doplnený doplňujúcimi pravidlami uvedenými v prílohe I spolu s oficiálnymi vyhláseniami, uisteniami a záväzkami uvedenými v prílohe II zaisťuje úroveň ochrany osobných údajov prenášaných z Európskej únie, ktorá v zásade zodpovedá ochrane zaručenej nariadením (EÚ) 2016/679.
- (172) Komisia sa okrem toho domnieva, že mechanizmy dozoru a možnosti získania nápravy v japonskom právnom poriadku umožňujú ako celok v praxi odhaliť a potrestať porušovanie právnych predpisov zo strany prijímajúcich hospodárskych subjektov nakladajúcich s osobnými informáciami a poskytujú dotknutej osobe právne prostriedky nápravy na získanie prístupu k osobným údajom, ktoré sa jej týkajú, a prípadne aj dosiahnutie opravy alebo vymazania takýchto údajov.

⁽¹⁴¹⁾ Zákon o preskúmaní sťažností v správnych veciach (zákon č. 160 z roku 2014), najmä článok 1 ods. 1.

⁽¹⁴²⁾ Pozri článok 9 zákona o zriadení Rady pre preskúmanie sprístupňovania informácií a ochrany osobných informácií (zákon č. 60 z roku 2003).

⁽¹⁴³⁾ Podľa poskytnutých informácií sa za 13 rokov od roku 2005 (keď zákon APPIHAO nadobudol účinnosť) vyskytli len dva prípady z viac ako 2000, keď sa správny orgán neriadil správou, hoci rada pre preskúmanie namietala proti správnym rozhodnutiam už viackrát. Navyše, ak správny orgán prijme rozhodnutie, ktoré sa odlišuje od zistení uvedených v správe, musí jasne uviesť dôvody, pre ktoré tak urobil. Pozri oddiel III.C prílohy II s odkazom na článok 50 ods. 1 bod iv) zákona o preskúmaní sťažností v správnych veciach.

⁽¹⁴⁴⁾ Všeobecné informačné centrá – jedno v každej prefektúre – poskytujú občanom vysvetlenia týkajúce sa osobných informácií, ktoré zhromažďujú orgány verejnej moci (napr. existujúcich databáz), a platných pravidiel ochrany údajov (zákon APPIHAO) vrátane toho, ako vykonávať práva na sprístupnenie, opravu alebo ukončenie používania. Zároveň slúžia ako kontaktné miesto pre otázky/sťažnosti občanov. Pozri oddiel II.C.4 písm. a) prílohy II.

⁽¹⁴⁵⁾ Pozri tiež články 10 a 11 zákona APPIHAO o „registri zložiek osobných informácií“, ktoré však zahŕňajú celý rad výnimiek, pokiaľ ide o „zložky osobných informácií“ vypracované alebo získané na účely vyšetrovania trestných činov alebo ktoré obsahujú veci týkajúce sa bezpečnosti a iných dôležitých záujmov štátu (pozri článok 10 ods. 2 písm. i) a ii) zákona APPIHAO).

- (173) A na záver, na základe dostupných informácií o japonskom právnom poriadku vrátane vyhlásení, uistení a záväzkov japonskej vlády, ktoré sú uvedené v prílohe II, sa Komisia domnieva, že každý zásah do základných práv fyzických osôb, ktorých osobné údaje sa prenášajú z Európskej únie do Japonska, zo strany japonských 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 legitímneho cieľa, a že existuje účinná právna ochrana proti takýmto zásahom.
- (174) Preto sa Komisia na základe zistení uvedených v tomto rozhodnutí domnieva, že Japonsko zabezpečuje primeranú úroveň ochrany osobných údajov prenášaných z Európskej únie hospodárskym subjektom nakladajúcim s osobnými informáciami v Japonsku, na ktoré sa vzťahuje zákon APPI, s výnimkou prípadov, keď príjemca patrí do jednej z kategórií uvedených v článku 76 ods. 1 zákona APPI a všetky účely spracúvania alebo ich časť zodpovedajú jednému z účelov stanovených v uvedenom ustanovení.
- (175) Komisia dospela na tomto základe k záveru, že štandard primeranosti podľa článku 45 nariadenia (EÚ) 2016/679, vykladaný s ohľadom na Chartu základných práv Európskej únie, a najmä rozsudok vo veci Schrems⁽¹⁴⁶⁾, je dosiahnutý.

5. OPATRENIA ORGÁNOV PRE OCHRANU ÚDAJOV A INFORMÁCIE POSKYTOVANÉ KOMISII

- (176) Podľa judikatúry Súdneho dvora⁽¹⁴⁷⁾ a ako sa uznáva v článku 45 ods. 4 nariadenia (EÚ) 2016/679, Komisia by mala po prijatí rozhodnutia o primeranosti nepretržite monitorovať príslušný vývoj v tretej krajine s cieľom posúdiť, či Japonsko 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.
- (177) Komisia by preto mala neustále monitorovať situáciu, 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 japonských orgánov. V záujme uľahčenia tohto procesu sa od japonských orgánov očakáva, že budú Komisiu informovať o podstatnom vývoji relevantnom tak pokiaľ ide o spracúvanie osobných údajov hospodárskymi subjektmi, ako aj o obmedzenia a záruky uplatniteľné na prístup k osobným údajom zo strany orgánov verejnej moci. To by malo zahŕňať všetky rozhodnutia prijaté PPC na základe článku 24 zákona APPI, v ktorých sa uznáva, že tretia krajina zabezpečuje úroveň ochrany zodpovedajúcu úrovni zaručenej v Japonsku.
- (178) 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 hospodárskym subjektom v Japonsku. Komisia by mala byť informovaná aj o akýchkoľvek známkach toho, že opatrenia japonských 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.
- (179) Členské štáty a ich orgány sú povinné prijať opatrenia potrebné na dosiahnutie súladu s aktmi inštitúcií Únie, lebo tieto akty požívajú prezumpciu zákonnosti a majú z tohto dôvodu právne účinky dovtedy, kým nebol derogovaný, zrušený v konaní o žalobe o neplatnosť alebo vyhlásený za neplatný v nadväznosti na návrh na začatie prejudiciálneho konania alebo námietku nezákonnosti. 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. Zároveň, ako Súdny dvor vysvetlil v rozsudku vo veci Schrems⁽¹⁴⁸⁾ a ako bolo uznané v článku 58 ods. 5 nariadenia, keď orgán pre ochranu osobných údajov spochybnil, okrem iného aj na základe sťažnosti, zlučiteľnosť rozhodnutia Komisie o primeranosti so základnými právami fyzickej osoby na súkromie a ochranu údajov, vnútroštátne právo mu musí poskytnúť právny prostriedok nápravy umožňujúci uplatniť tieto výhrady na vnútroštátnom súde, ktorý musí v prípade pochybností konanie prerušiť a podať návrh na začatie prejudiciálneho konania na Súdnom dvore⁽¹⁴⁹⁾.

⁽¹⁴⁶⁾ Pozri poznámku pod čiarou č. 3.

⁽¹⁴⁷⁾ Vec Schrems, bod 76.

⁽¹⁴⁸⁾ Vec Schrems, bod 65.

⁽¹⁴⁹⁾ Vec Schrems, bod 65: „V tomto ohľade je úlohou vnútroštátneho zákonodarcu stanoviť právne 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“.

6. PRAVIDELNÉ PRESKÚMANIE ZÁVERU O PRIMERANOSTI

- (180) Podľa článku 45 ods. 3 nariadenia (EÚ) 2016/679 ⁽¹⁵⁰⁾ a vzhľadom na skutočnosť, že úroveň ochrany zabezpečovaná japonským právnym poriadkom sa môže zmeniť, by Komisia mala po prijatí tohto rozhodnutia pravidelne overovať, či sú závery týkajúce sa primeranosti úrovne ochrany, ktorú zabezpečuje Japonsko, stále skutkovo a právne odôvodnené.
- (181) Na tento účel by sa malo toto rozhodnutie podrobiť prvému preskúmaniu do dvoch 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 všeobecného nariadenia o ochrane údajov rozhodne, či by sa mal zachovať dvojročný cyklus. Následné preskúmania by sa v každom prípade mali uskutočniť aspoň každé štyri roky ⁽¹⁵¹⁾. Preskúmanie by malo zahŕňať všetky aspekty fungovania tohto rozhodnutia, a najmä uplatňovanie doplňujúcich pravidiel (pričom treba osobitnú pozornosť venovať ochrane zabezpečovanej v prípade následných prenosov), uplatňovanie pravidiel týkajúcich sa súhlasu, a to aj v prípade odňatia, účinnosť výkonu individuálnych práv, ako aj obmedzenia a záruky v súvislosti s prístupom vlády vrátane mechanizmu nápravy stanoveného v prílohe II k tomuto rozhodnutiu. Malo by sa zameriavať aj na účinnosť dohľadu a presadzovania, pokiaľ ide o pravidlá uplatniteľné na hospodárske subjekty nakladajúce s osobnými informáciami, ako aj na oblasť presadzovania práva v trestných veciach a oblasť národnej bezpečnosti.
- (182) V záujme vykonania preskúmania by sa Komisia mala stretnúť s PPC, ku ktorej by sa v prípade potreby mali pripojiť ďalšie japonské orgány zodpovedné za prístup vlády vrátane príslušných dozorných orgánov. Na tomto stretnutí by sa mali môcť zúčastniť zástupcovia členov Európskeho výboru pre ochranu údajov. Komisia by mala v rámci spoločného preskúmania požiadať PPC, aby poskytla komplexné informácie o všetkých aspektoch relevantných pre záver o primeranosti vrátane informácií o obmedzeniach a zárukách týkajúcich sa prístupu vlády ⁽¹⁵²⁾. Komisia by si takisto mala vyžiadať vysvetlenia k všetkým informáciám relevantným pre toto rozhodnutie, ktoré dostala, vrátane verejných správ japonských orgánov alebo iných zainteresovaných strán v Japonsku, Európskeho výboru pre ochranu údajov, jednotlivých orgánov pre ochranu osobných údajov, skupín občianskej spoločnosti, mediálnych správ alebo akéhokoľvek iného dostupného zdroja informácií.
- (183) Komisia by na základe spoločného preskúmania mala vypracovať verejnú správu, ktorá sa predloží Európskemu parlamentu a Rade.

7. POZASTAVENIE ROZHODNUTIA O PRIMERANOSTI

- (184) Ak Komisia na základe pravidelných a *ad hoc* overení alebo akýchkoľvek iných dostupných informácií dospeje k záveru, že úroveň ochrany zabezpečovanú japonským právnym poriadkom už nie je možné považovať za v zásade zodpovedajúcu úrovni ochrany v Európskej únii, mala by o tom informovať príslušné japonské orgány a požadovať, aby sa v stanovenej primeranej lehote prijali vhodné opatrenia. To zahŕňa aj pravidlá, ktoré platia pre hospodárske subjekty aj japonské orgány verejnej moci zodpovedné za presadzovanie práva v trestných veciach alebo národnú bezpečnosť. Takýto postup by sa napríklad uplatnil v prípadoch, keď sa následné prenosy vrátane prenosov na základe rozhodnutí prijatých PPC podľa článku 24 zákona APPI, ktorými sa uznáva, že tretia krajina zabezpečuje úroveň ochrany zodpovedajúcu ochrane zaistenej v Japonsku, už nebudú uskutočňovať so zárukami zabezpečujúcimi kontinuitu ochrany v zmysle článku 44 všeobecného nariadenia o ochrane údajov.
- (185) Ak po uplynutí stanovenej lehoty príslušné japonské orgány uspokojivo nepreukážu, že toto rozhodnutie je naďalej založené na primeranej úrovni ochrany, Komisia by mala podľa článku 45 ods. 5 nariadenia (EÚ) 2016/679 začať postup vedúci k čiastočnému alebo úplnému pozastaveniu alebo zrušeniu tohto rozhodnutia. Alternatívne by Komisia mala začať postup zmeny tohto rozhodnutia, a to najmä tak, že stanoví ďalšie podmienky vzťahujúce sa na prenosy údajov alebo obmedzí rozsah záveru o primeranosti len na prenosy údajov, pri ktorých je zabezpečená kontinuita ochrany v zmysle článku 44 všeobecného nariadenia o ochrane údajov.

⁽¹⁵⁰⁾ Podľa článku 45 ods. 3 nariadenia (EÚ) 2016/679 „[V]o vykonávaní akte sa stanoví mechanizmus pravidelného preskúmania, ktoré sa uskutočňuje najmenej raz za štyri roky, v ktorom sa zohľadnia všetky významné zmeny v tretej krajine alebo medzinárodnej organizácii.“

⁽¹⁵¹⁾ 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.

⁽¹⁵²⁾ Pozri aj oddiel IV prílohy II. „V rámci pravidelného preskúmania rozhodnutia o primeranosti si PPC a Európska komisia vymienia informácie o spracúvaní údajov za podmienok záveru o primeranosti vrátane podmienok uvedených v tomto vyhlásení.“

- (186) Komisia by mala postup pozastavenia alebo zrušenia iniciovať predovšetkým v prípade, že budú existovať známky toho, že hospodárske subjekty, ktoré dostávajú osobné údaje podľa tohto rozhodnutia, nedodržiavajú doplňujúce pravidlá uvedené v prílohe I a/alebo že sa tieto pravidlá účinne nepresadzujú, alebo že japonské orgány nedodržiavajú vyhlásenia, uistenia a záväzky uvedené v prílohe II k tomuto rozhodnutiu.
- (187) Komisia by mala zvážiť začatie postupu vedúceho k zmene, pozastaveniu alebo zrušeniu tohto rozhodnutia aj v prípade, že príslušné japonské orgány v rámci spoločného preskúmania alebo inak neposkytnú informácie alebo objasnenia potrebné na posúdenie úrovne ochrany zabezpečovanej pre osobné údaje prenášané z Európskej únie do Japonska alebo na dodržiavanie tohto rozhodnutia. Komisia by mala v tejto súvislosti zohľadniť, do akej miery možno príslušné informácie získať z iných zdrojov.
- (188) V naliehavých a riadne odôvodnených prípadoch, napríklad ak hrozí riziko závažného porušenia práv dotknutých osôb, by Komisia mala zvážiť prijatie rozhodnutia o pozastavení alebo zrušení tohto rozhodnutia, ktoré by sa malo v súlade s článkom 93 ods. 3 nariadenia (EÚ) 2016/679 v spojení s článkom 8 nariadenia Európskeho parlamentu a Rady (EÚ) č. 182/2011 ⁽¹⁵³⁾ uplatňovať okamžite.

8. ZÁVEREČNÉ ÚVAHY

- (189) Európsky výbor pre ochranu údajov zverejnil svoje stanovisko ⁽¹⁵⁴⁾, ktoré bolo zohľadnené pri príprave tohto rozhodnutia.
- (190) Európsky parlament prijal uznesenie o stratégii digitálneho obchodu, v ktorom vyzýva Komisiu, aby uprednostnila a urýchlila prijímanie rozhodnutí o primeranosti vo vzťahu k významným obchodným partnerom v súlade s podmienkami stanovenými v nariadení (EÚ) 2016/679, keďže ide o dôležitý mechanizmus na zabezpečenie prenosu osobných údajov z Európskej únie ⁽¹⁵⁵⁾. Európsky parlament takisto prijal uznesenie o primeranosti ochrany osobných údajov zabezpečovanej Japonskom ⁽¹⁵⁶⁾.
- (191) Opatrenia stanovené v tomto rozhodnutí sú v súlade so stanoviskom výboru zriadeného podľa článku 93 ods. 1 všeobecného nariadenia o ochrane údajov,

PRIJALA TOTO ROZHODNUTIE:

Článok 1

1. Na účely článku 45 nariadenia (EÚ) 2016/679 Japonsko zabezpečuje primeranú úroveň ochrany osobných údajov prenášaných z Európskej únie hospodárskym subjektom nakladajúcim s osobnými informáciami v Japonsku, na ktoré sa vzťahuje zákon o ochrane osobných informácií doplnený doplňujúcimi pravidlami uvedenými v prílohe I spolu s oficiálnymi vyhláseniami, uisteniami a záväzkami uvedenými v prílohe II.

⁽¹⁵³⁾ Nariadenie Európskeho parlamentu a Rady (EÚ) č. 182/2011 zo 16. februára 2011, ktorým sa ustanovujú pravidlá a všeobecné zásady mechanizmu, na základe ktorého členské štáty kontrolujú vykonávanie vykonávacích právomocí Komisie (Ú. v. EÚ L 55, 28.2.2011, s. 13).

⁽¹⁵⁴⁾ Stanovisko 28/2018 k návrhu vykonávacieho rozhodnutia Európskej komisie o primeranej ochrane osobných údajov v Japonsku, prijaté 5. decembra 2018.

⁽¹⁵⁵⁾ Európsky parlament, uznesenie z 12. decembra 2017 s názvom „Smerom k stratégii digitálneho obchodu“ [2017/2065 (INI)]. Pozri najmä bod 8 („...pripomína, že osobné údaje sa môžu prenášať do tretích krajín bez použitia všeobecných pravidiel v obchodných dohodách, pokiaľ sú a budú splnené požiadavky zakotvené v [...] kapitole V nariadenia (EÚ) 2016/679; uznáva, že rozhodnutia o primeranosti vrátane čiastočných rozhodnutí a rozhodnutí pre konkrétne sektory sú základným nástrojom na ochranu prenosu osobných údajov z EÚ do tretej krajiny; konštatuje, že EÚ prijala rozhodnutia o primeranosti len so štyrmi zo svojich 20 najväčších obchodných partnerov...“) a bod 9 („vyzýva Komisiu, aby uprednostnila a urýchlila prijímanie rozhodnutí o primeranosti za predpokladu, že tretie krajiny na základe svojho vnútroštátneho práva alebo svojich medzinárodných záväzkov zabezpečia úroveň ochrany, ktorá „v zásade zodpovedá“ úrovni zaručenej v rámci EÚ...“).

⁽¹⁵⁶⁾ Uznesenie Európskeho parlamentu z 13. decembra 2018 „Primeranosť ochrany osobných údajov zo strany Japonska“ [2018/2979(RSP)].

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 zodpovedajú jednému z uvedených účelov:

- a) vysielacie inštitúcie, vydavatelia novín, komunikačné agentúry alebo iné tlačové organizácie (vrátane všetkých fyzických osôb, ktoré vykonávajú tlačovú činnosť ako svoje podnikanie), pokiaľ spracúvajú osobné údaje na účely tlače;
- b) osoby, ktoré sa profesionálne venujú písaniu, pokiaľ to zahŕňa osobné údaje;
- c) univerzity a všetky ostatné organizácie alebo skupiny zamerané na akademické štúdium alebo všetky osoby patriace k takejto organizácii alebo skupine, pokiaľ spracúvajú osobné údaje na účely akademických štúdií;
- d) cirkevné organizácie, pokiaľ spracúvajú osobné údaje na účely náboženskej činnosti (vrátane všetkých súvisiacich činností); ako aj
- e) politické organizácie, pokiaľ spracúvajú osobné údaje na účely svojej politickej činnosti (vrátane všetkých súvisiacich činností).

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, čo vedie k pozastaveniu alebo trvalému zákazu tokov údajov konkrétnemu hospodárskemu subjektu v Japonsku v rozsahu pôsobnosti stanovenom v článku 1, 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, s cieľom posúdiť, či Japonsko naďalej zabezpečuje primeranú úroveň ochrany v zmysle článku 1.

2. Členské štáty a Komisia sa vzájomne informujú o prípadoch, v ktorých Komisia pre ochranu osobných informácií alebo akýkoľvek iný príslušný japonský 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 japonských 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. Do dvoch rokov od dátumu oznámenia tohto rozhodnutia členským štátom a následne aspoň každé štyri roky Komisia vyhodnotí záver v článku 1 ods. 1 na základe všetkých dostupných informácií vrátane informácií, ktoré získala v rámci spoločného preskúmania uskutočneného spolu s príslušnými japonskými orgánmi.

5. Ak má Komisia informácie o tom, že primeraná úroveň ochrany už nie je zabezpečená, informuje príslušné japonské orgány. V prípade potreby môže rozhodnúť o pozastavení, zmene alebo zrušení tohto rozhodnutia, alebo obmedzení jeho rozsahu pôsobnosti, najmä ak existujú známky toho, že:

- a) hospodárske subjekty v Japonsku, ktoré na základe tohto rozhodnutia dostali osobné údaje z Európskej únie, nedodržiavajú ďalšie záruky stanovené v dopĺňujúcich pravidlách uvedených v prílohe I k tomuto rozhodnutiu, alebo že sa v tejto súvislosti nevykonáva dostatočný dozor a presadzovanie;
- b) japonské orgány verejnej moci nedodržiavajú vyhlásenia, uistenia a záväzky uvedené v prílohe II k tomuto rozhodnutiu vrátane vyhlásení, uistení a záväzkov, pokiaľ ide o podmienky a obmedzenia zhromažďovania osobných údajov prenášaných na základe tohto rozhodnutia zo strany japonských 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 návrh takýchto opatrení predložiť aj vtedy, ak v dôsledku nedostatočnej spolupráce japonskej vlády nedokáže určiť, či je dotknutý záver uvedený v článku 1 ods. 1 tohto rozhodnutia.

Článok 4

Toto rozhodnutie je určené členským štátom.

V Bruseli 23. januára 2019

Za Komisiu
Věra JOUROVÁ
členka Komisie

PRÍLOHA 1

DOPLŇUJÚCE PRAVIDLÁ PODĽA ZÁKONA O OCHRANE OSOBNÝCH INFORMÁCIÍ TÝKAJÚCE SA NAKLADANIA S OSOBNÝMI ÚDAJMI PRENÁŠANÝMI Z EÚ NA ZÁKLADE ROZHODNUTIA O PRIMERANOSTI

Obsah

1. Osobné informácie vyžadujúce osobitnú starostlivosť (článok 2 ods. 3 zákona)	38
2. Uchovávané osobné údaje (článok 2 ods. 7 zákona)	39
3. Konkrétne určenie účelu použitia, obmedzenia z dôvodu účelu použitia (článok 15 ods. 1, článok 16 ods. 1 a článok 26 ods. 1 a 3 zákona)	40
4. Obmedzenie poskytovania informácií tretej strane v cudzej krajine (článok 24 zákona; článok 11-2 pravidiel)	41
5. Anonymne spracúvané informácie (článok 2 ods. 9 a článok 36 ods. 1 a 2 zákona)	41

[Termíny]

„Zákon“	zákon o ochrane osobných informácií (zákon č. 57, 2003)
„Nariadenie vlády“	nariadenie vlády o presadzovaní zákona o ochrane osobných informácií (nariadenie vlády č. 507, 2003)
„Pravidlá“	pravidlá presadzovania zákona o ochrane osobných informácií (pravidlá Komisie pre ochranu osobných informácií č. 3, 2016)
„Usmernenia týkajúce sa všeobecných pravidiel“	usmernenia k zákonu o ochrane osobných informácií (zväzok o všeobecných pravidlách) (oznámenie Komisie pre ochranu osobných informácií č. 65, 2015)
„EÚ“	Európska únia vrátane jej členských štátov a, na základe dohody o EHP, Islandu, Lichtenštajnska a Nórska
„Všeobecné nariadenie o ochrane údajov“	nariadenie Európskeho parlamentu a Rady o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov, ktorým sa zrušuje smernica 95/46/ES (všeobecné nariadenie o ochrane údajov)
„Rozhodnutie o primeranosti“	rozhodnutie Európskej komisie o tom, že tretia krajina alebo územie v danej tretej krajine atď. zaručujú primeranú úroveň ochrany osobných údajov podľa článku 45 všeobecného nariadenia o ochrane údajov

Komisia pre ochranu osobných informácií na účely vzájomného a bezproblémového prenosu osobných údajov medzi Japonskom a EÚ určila EÚ za cudziu krajinu, ktorá zriaďuje systém ochrany osobných informácií, ktorého normy sa z hľadiska ochrany práv a záujmov fyzických osôb podľa článku 24 zákona považujú za rovnocenné normám v Japonsku, a Európska komisia súčasne rozhodla, že Japonsko zabezpečuje primeranú úroveň ochrany osobných údajov v súlade s článkom 45 všeobecného nariadenia o ochrane údajov.

Medzi Japonskom a EÚ sa tak uskutoční vzájomný a bezproblémový prenos osobných údajov spôsobom, ktorý zabezpečí vysokú úroveň ochrany práv a záujmov fyzických osôb. V záujme zabezpečenia vysokej úrovne ochrany osobných informácií poskytovaných z EÚ na základe rozhodnutia o primeranosti a vzhľadom na to, že napriek vysokému stupňu konvergenzie medzi týmito dvoma systémami existujú určité relevantné rozdiely, prijala Komisia pre ochranu osobných informácií tieto doplňujúce pravidlá na základe ustanovení zákona týkajúcich sa vykonávania atď. spolupráce s vládami iných krajín a s cieľom zabezpečiť náležité nakladanie s osobnými informáciami poskytnutými z EÚ hospodárskemu subjektu nakladajúcemu s osobnými informáciami na základe rozhodnutia o primeranosti a riadne a účinné vykonávanie povinností stanovených v týchto pravidlách ⁽¹⁾.

⁽¹⁾ Článok 4, článok 6, článok 8, článok 24, článok 60 a článok 78 zákona a článok 11 pravidiel.

Najmä v článku 6 zákona sa stanovuje právomoc prijímať potrebné legislatívne a iné opatrenia s cieľom zabezpečiť intenzívnejšiu ochranu osobných informácií a vybudovať medzinárodne vyhovujúci systém týkajúci sa osobných informácií prostredníctvom prísnejších pravidiel, ktoré dopĺňajú pravidlá stanovené v zákone a v nariadení vlády a idú nad ich rámec. Komisia pre ochranu osobných informácií ako orgán príslušný pre riadenie celkovej správy zákona má preto právomoc stanoviť podľa článku 6 zákona prísnejšie právne predpisy formulovaním súčasných doplnujúcich pravidiel, v ktorých sa stanovuje vyššia úroveň ochrany práv a záujmov fyzických osôb pri nakladaní s osobnými údajmi poskytnutými z EÚ na základe rozhodnutia o primeranosti, a to aj pokiaľ ide o vymedzenie osobných informácií vyžadujúcich osobitnú starostlivosť podľa článku 2 ods. 3 zákona a uchovávaných osobných údajov podľa článku 2 ods. 7 zákona (vrátane príslušnej lehoty uchovávania).

Na tomto základe sú doplnujúce pravidlá záväzné pre hospodársky subjekt nakladajúci s osobnými informáciami, ktorý dostáva osobné údaje prenášané z EÚ na základe rozhodnutia o primeranosti, a teda musí tieto pravidlá dodržiavať. Všetky práva a povinnosti sú ako právne záväzné pravidlá vymáhateľné Komisiou pre ochranu osobných informácií rovnako ako ustanovenia zákona, ktoré sa nimi dopĺňajú o prísnejšie a/alebo podrobnejšie pravidlá. V prípade porušenia práv a povinností vyplývajúcich z doplnujúcich pravidiel môžu fyzické osoby takisto získať prostriedky nápravy zo strany súdu, a to rovnako ako v prípade ustanovení zákona, ktoré sa nimi dopĺňajú o prísnejšie a/alebo podrobnejšie pravidlá.

Pokiaľ ide o presadzovanie Komisiou pre ochranu osobných informácií, ak hospodársky subjekt nakladajúci s osobnými informáciami nespĺňa jednu alebo niekoľko povinností podľa doplnujúcich pravidiel, Komisia pre ochranu osobných informácií má právomoc prijať opatrenia podľa článku 42 zákona. Pokiaľ ide všeobecne o osobné informácie poskytnuté z EÚ na základe rozhodnutia o primeranosti, skutočnosť, že hospodársky subjekt nakladajúci s osobnými informáciami neprijal opatrenie v súlade s odporúčaním prijatým podľa článku 42 ods. 1 zákona bez toho, aby na to existoval oprávnený dôvod⁽²⁾, sa považuje za závažné porušenie práv a záujmov fyzickej osoby bezprostrednej povahy v zmysle článku 42 ods. 2 zákona

1. Osobné informácie vyžadujúce osobitnú starostlivosť (článok 2 ods. 3 zákona)

Článok 2 (ods. 3) zákona

3. „Osobné informácie vyžadujúce osobitnú starostlivosť“ v tomto zákone sú osobné informácie zahŕňajúce rasový pôvod hlavného subjektu, jeho presvedčenie, spoločenské postavenie, anamnézu, záznam vedený v registri trestov, skutočnosť, že utrpel ujmu v dôsledku trestného činu, alebo iné opisy atď., ktoré sú v nariadení vlády vymedzené ako informácie, s ktorými treba nakladať s osobitnou starostlivosťou, aby hlavný subjekt nebol vystavený nespravodlivej diskriminácii, predsudkom alebo inému znevýhodneniu.

Článok 2 nariadenia vlády

Uvedené opisy atď., ktoré sú vymedzené v nariadení vlády podľa článku 2 ods. 3 zákona, sú opisy atď., ktoré obsahujú akékoľvek zo záležitostí uvedených v týchto bodoch (okrem tých, ktoré sa týkajú zdravotných záznamov alebo trestnej minulosti hlavného subjektu):

- i) skutočnosť, že hlavný subjekt má telesné postihnutie, intelektuálne postihnutie, mentálne postihnutie (vrátane vývojových porúch) alebo iné telesné postihnutie a funkčné mentálne postihnutie vymedzené v pravidlách Komisie pre ochranu osobných informácií;
- ii) výsledky lekárskej prehliadky alebo iného vyšetrenia (ďalej len „lekárska prehliadka atď.“ v nasledujúcom bode) hlavného subjektu na účely prevencie a včasného zistenia choroby, ktoré vykonáva lekár alebo iná osoba vykonávajúca povinnosti v oblasti medicíny (ďalej len „lekár atď.“ v nasledujúcom bode);
- iii) skutočnosť, že hlavný subjekt dostal od lekára atď. na základe výsledkov lekárskej prehliadky atď. alebo z dôvodu choroby, zranenia alebo iných duševných a telesných zmien usmernenie na zlepšenie duševného a telesného stavu, lekársku starostlivosť alebo lekársky predpis;
- iv) skutočnosť, že hlavný subjekt bol predmetom zadržania, prehliadky, zaistenia, väzby, trestného stíhania alebo iných postupov súvisiacich s trestným konaním ako podozrivá alebo obvinená osoba;

⁽²⁾ Oprávnený dôvod sa chápe ako udalosť mimoriadnej povahy mimo kontroly hospodárskeho subjektu nakladajúceho s osobnými informáciami, ktorú nemožno primerane predpokladať (napríklad prírodné katastrofy) alebo prípady, v ktorých potreba prijať opatrenie v súvislosti s odporúčaním vydaným Komisiou pre ochranu osobných informácií podľa článku 42 ods. 1 zákona zanikla, pretože hospodársky subjekt nakladajúci s osobnými informáciami prijal alternatívne opatrenie, ktorým sa porušenie plne napraviť.

- v) skutočnosť, že hlavný subjekt bol predmetom vyšetrovania, opatrení na sledovanie a ochranu, vypočúvania a rozhodnutia, ochranného opatrenia alebo iných postupov súvisiacich s prípadom ochrany mladistvých ako mladistvý delikvent alebo osoba podozrivá z toho, že je mladistvý delikvent podľa článku 3 ods. 1 zákona o mladistvých.

Článok 5 pravidiel

Telesné postihnutie a funkčné mentálne postihnutie, ktoré sú vymedzené v pravidlách Komisie pre ochranu osobných informácií podľa článku 2 bodu. i) nariadenia vlády, zahŕňa postihnutie uvedené v týchto bodoch:

- i) telesné postihnutie uvedené v pripojenej tabuľke zákona o starostlivosti o osoby s telesným postihnutím (zákon č. 283 z roku 1949);
- ii) intelektuálne postihnutie uvedené v zákone o starostlivosti o osoby s intelektuálnym postihnutím (zákon č. 37 z roku 1960);
- iii) mentálne postihnutie uvedené v zákone o duševnom zdraví a starostlivosti o osoby s mentálnym postihnutím (zákon č. 123 z roku 1950) (vrátane vývojových porúch vymedzených v článku 2 ods. 1 zákona o podpore osôb s vývojovými poruchami a okrem intelektuálneho postihnutia podľa zákona o starostlivosti o osoby s intelektuálnym postihnutím);
- iv) choroba, na ktorú neexistujú liečebné metódy, alebo iné neobvyklé choroby, ktorých závažnosť vymedzená v nariadení vlády podľa článku 4 ods. 1 zákona o komplexnej podpore každodenného a spoločenského života osôb s postihnutím (zákon č. 123 z roku 2005) zodpovedá závažnosti chorôb vymedzených ministerstvom zdravotníctva, práce a sociálnych vecí podľa uvedeného odseku.

Ak osobné údaje poskytnuté z EÚ na základe rozhodnutia o primeranosti obsahujú údaje týkajúce sa sexuálneho života fyzickej osoby, jej sexuálnej orientácie alebo členstva v odborových organizáciách, ktoré sú vo všeobecnom nariadení o ochrane údajov vymedzené ako osobitné kategórie údajov, hospodárske subjekty nakladajúce s osobnými informáciami sú povinné nakladať s uvedenými osobnými údajmi rovnako ako s osobnými informáciami vyžadujúcimi osobitnú starostlivosť v zmysle článku 2 ods. 3 zákona.

2. Uchovávané osobné údaje (článok 2 ods. 7 zákona)

Článok 2 (ods. 7) zákona

7. „Uchovávané osobné údaje“ v tomto zákone sú osobné údaje, v prípade ktorých má hospodársky subjekt nakladajúci s osobnými informáciami oprávnenie ich zverejniť, opraviť, pridať k nim obsah alebo z nich obsah vypustiť, ukončiť ich používanie, vymazať ich a ukončiť ich poskytovanie tretej strane, pričom nesmie ísť o osobné údaje, ktoré by podľa vymedzenia v nariadení vlády mohli poškodiť verejné alebo iné záujmy, keby sa zverejnili ich prítomnosť alebo absencia, ani osobné údaje, ktoré sa majú vymazať v lehote najviac jedného roka, ktorá je vymedzená v nariadení vlády.

Článok 4 nariadenia vlády

Osobné údaje vymedzené v nariadení vlády podľa článku 2 ods. 7 sú osobné údaje uvedené v týchto bodoch:

- i) osobné údaje, v súvislosti s ktorými existuje možnosť, že zverejnenie ich prítomnosti, resp. absencie by viedlo k poškodeniu života, zdravia alebo majetku hlavného subjektu alebo tretej strany;
- ii) osobné údaje, v súvislosti s ktorými existuje možnosť, že zverejnenie ich prítomnosti, resp. absencie by podnietilo protiprávne alebo nespravodlivé konanie alebo by k takémuto konaniu viedlo;
- iii) osobné údaje, v súvislosti s ktorými existuje možnosť, že zverejnenie ich prítomnosti, resp. absencie by narušilo národnú bezpečnosť, zničilo dôverný vzťah s cudzou krajinou alebo medzinárodnou organizáciou alebo spôsobilo znevýhodnenie v rokovaniach s cudzou krajinou alebo medzinárodnou organizáciou;
- iv) osobné údaje, v súvislosti s ktorými existuje možnosť, že zverejnenie ich prítomnosti, resp. absencie by znemožnilo udržanie verejnej bezpečnosti a verejného poriadku, ako napríklad predchádzanie a potláčanie trestnej činnosti alebo jej vyšetrovanie.

Článok 5 nariadenia vlády

Lehota vymedzená v nariadení vlády podľa článku 2 ods. 7 zákona je šesť mesiacov.

Vyžaduje sa, aby sa s osobnými údajmi poskytnutými z EÚ na základe rozhodnutia o primeranosti nakladalo ako s uchovávanými osobnými údajmi v zmysle článku 2 ods. 7 zákona bez ohľadu na lehotu, v ktorej sa majú údaje vymazať.

Ak osobné údaje poskytnuté z EÚ na základe rozhodnutia o primeranosti patria do rozsahu osobných údajov vymedzených v nariadení vlády ako osobné údaje, ktoré „by mohli poškodiť verejné alebo iné záujmy, keby sa zverejnili ich prítomnosť alebo absencia“, nemusí sa s nimi nakladať ako s uchovávanými osobnými údajmi (pozri článok 4 nariadenia vlády, usmernenia týkajúce sa všeobecných pravidiel, „2 – 7. Uchovávané osobné údaje“).

3. Konkrétne určenie účelu použitia, obmedzenia z dôvodu účelu použitia (článok 15 ods. 1, článok 16 ods. 1 a článok 26 ods. 1 a 3 zákona)

Článok 15 (ods. 1) zákona

1. Hospodársky subjekt nakladajúci s osobnými informáciami pri nakladaní s osobnými informáciami čo možno najvýslovnejšie určuje účel použitia osobných informácií (ďalej len „účel použitia“).

Článok 16 (ods. 1) zákona

1. Hospodársky subjekt nakladajúci s osobnými informáciami nenakladá s osobnými informáciami bez toho, aby vopred získal súhlas hlavného subjektu nad rámec rozsahu nevyhnutného na dosiahnutie účelu použitia stanoveného podľa ustanovení predchádzajúceho článku.

Článok 26 (ods. 1 a 3) zákona

1. Hospodársky subjekt nakladajúci s osobnými informáciami potvrdzuje pri prijímaní osobných údajov od tretej strany v súlade s pravidlami Komisie pre ochranu osobných informácií skutočnosti uvedené v týchto bodoch: (vypustené)

i) (vypustené);

ii) okolnosti, za ktorých daná tretia strana nadobudla dané osobné údaje.

3. Hospodársky subjekt nakladajúci s osobnými informáciami po potvrdení podľa ustanovení odseku 1 zaznamenáva podľa pravidiel Komisie pre ochranu osobných údajov dátum, kedy prijal osobné údaje, záležitosť týkajúcu sa daného potvrdenia a iné záležitosti stanovené v pravidlách Komisie pre ochranu osobných informácií.

Ak hospodárske subjekty nakladajúce s osobnými informáciami nakladajú s osobnými informáciami nad rámec potrebného rozsahu s cieľom dosiahnuť účel použitia uvedený v článku 15 ods. 1 zákona, získavajú príslušný súhlas hlavného subjektu vopred (článok 16 ods. 1 zákona). Pri prijímaní osobných údajov od tretej strany hospodárske subjekty nakladajúce s osobnými informáciami potvrdzujú podľa pravidiel také skutočnosti, ako sú okolnosti, za ktorých daná tretia strana získala dané osobné údaje, a tieto skutočnosti zaznamenávajú (článok 26 ods. 1 a 3 zákona).

Ak hospodársky subjekt nakladajúci s osobnými informáciami prijme osobné údaje od EÚ na základe rozhodnutia o primeranosti, k okolnostiam týkajúcim sa získania daných osobných údajov, ktoré sa musia potvrdiť a zaznamenať, ako je stanovené v článku 26 ods. 1 a 3, patrí účel použitia, na ktorý boli tieto údaje prijaté od EÚ.

Podobne, ak hospodársky subjekt nakladajúci s osobnými informáciami prijme od iného hospodárskeho subjektu nakladajúceho s osobnými informáciami osobné údaje, ktoré boli predtým prenesené z EÚ na základe rozhodnutia o primeranosti, okolnosti týkajúce sa získania daných osobných údajov, ktoré sa musia potvrdiť a zaznamenať, ako je stanovené v článku 26 ods. 1 a 3, zahŕňajú účel použitia, na ktorý boli tieto údaje prijaté od EÚ.

V uvedených prípadoch je hospodársky subjekt nakladajúci s osobnými informáciami povinný konkrétne určiť účel použitia daných osobných údajov v rámci rozsahu účelu použitia, na ktorý boli údaje pôvodne alebo následne prijaté, ako je potvrdené a zaznamenané v zmysle článku 26 ods. 1 a 3, a používať uvedené údaje v rámci uvedeného rozsahu (ako je vymedzené v článku 15 ods. 1 a článku 16 ods. 1 zmluvy).

4. Obmedzenie poskytovania informácií tretej strane v cudzej krajine (článok 24 zákona; článok 11-2 pravidiel)

Článok 24 zákona

Okrem prípadov uvedených v jednotlivých bodoch odseku 1 predchádzajúceho článku hospodársky subjekt nakladajúci s osobnými informáciami v prípade poskytovania osobných údajov tretej strane (okrem osoby, ktorá zriaďuje systém vyhovujúci normám stanoveným v pravidlách Komisie pre ochranu osobných informácií ako nevyhnutné na neustále prijímanie opatrení rovnocenných opatreniam, ktoré prijíma hospodársky subjekt nakladajúci s osobnými informáciami, pokiaľ ide o nakladanie s osobnými údajmi podľa ustanovení tohto oddielu; rovnako aj ďalej v tomto článku) v cudzej krajine (t. j. krajina alebo región mimo územia Japonska; rovnako aj ďalej) (okrem krajín vymedzených v pravidlách Komisie pre ochranu osobných informácií ako cudzia krajina, ktorá zriaďuje systém ochrany osobných informácií, ktorého normy sa z hľadiska ochrany práv a záujmov fyzických osôb považujú za rovnocenné normám v Japonsku; rovnako aj ďalej v tomto článku) vopred získava súhlas hlavného subjektu s poskytovaním informácií tretej strane v cudzej krajine. V tomto prípade sa neuplatňujú ustanovenia predchádzajúceho článku.

Článok 11-2 pravidiel

Normy stanovené v pravidlách Komisie pre ochranu osobných informácií podľa článku 24 zákona patria pod ktorýkoľvek z týchto bodov:

- i) pokiaľ ide o nakladanie s osobnými údajmi osobou, ktorá ich prijíma, hospodársky subjekt nakladajúci s osobnými informáciami a osoba, ktorá prijíma osobné údaje, zaistili vykonávanie opatrení v súlade s cieľom ustanovení kapitoly IV oddielu 1 zákona vhodnou a primeranou metódou;
- ii) osoba, ktorá prijíma osobné údaje, získala uznanie na základe medzinárodného rámca, ktorý sa týka nakladania s osobnými informáciami.

Hospodársky subjekt nakladajúci s osobnými informáciami v prípade poskytovania osobných údajov, ktoré dostal z EÚ na základe rozhodnutia o primeranosti, tretej strane v cudzej krajine vopred získava súhlas hlavného subjektu s poskytovaním informácií tretej strane v cudzej krajine podľa článku 24 zákona po tom, ako mu boli poskytnuté informácie o okolnostiach prevodu nevyhnutných na to, aby hlavný subjekt prijal rozhodnutie o svojom súhlase, okrem prípadov uvedených v týchto bodoch i) až iii):

- i) ak sa tretia strana nachádza v krajine vymedzenej v pravidlách ako cudzia krajina, ktorá zriaďuje systém ochrany osobných informácií, ktorého normy sa z hľadiska ochrany práv a záujmov fyzických osôb považujú za rovnocenné normám v Japonsku;
- ii) ak hospodársky subjekt nakladajúci s osobnými informáciami a tretia strana, ktorá prijíma osobné údaje, spolu vykonali v súvislosti s nakladaním s osobnými údajmi treťou stranou opatrenia zabezpečujúce rovnocennú úroveň ochrany ako zákon v spojení so súčasnými pravidlami, a to vhodnou a primeranou metódou (t. j. zmluva, iné formy záväzných dohôd alebo záväzné dohody v rámci skupiny podnikov);
- iii) v prípadoch, na ktoré sa vzťahujú jednotlivé body článku 23 ods. 1 zákona.

5. Anonymne spracúvané informácie (článok 2 ods. 9 a článok 36 ods. 1 a 2 zákona)

Článok 2 (ods. 9) zákona

- 9. „Anonymne spracúvané informácie“ v tomto zákone sú informácie týkajúce sa fyzickej osoby, ktoré možno získať spracúvaním osobných informácií tak, aby nebolo možné identifikovať konkrétnu fyzickú osobu, a to prijatím opatrení vymedzených v týchto jednotlivých bodoch v súlade s rozdelením osobných informácií uvedených v jednotlivých daných bodoch, ani obnoviť dané osobné informácie:

- i) osobné informácie, na ktoré sa vzťahuje odsek 1 bod i).

Vypustenie časti opisov atď. zahrnutých v daných osobných informáciách (vrátane nahradenia danej časti opisov atď. inými opismi atď. metódou, ktorá nevykazuje žiadnu pravidelnosť, podľa ktorej možno obnoviť danú časť opisov atď.);

- ii) osobné informácie, na ktoré sa vzťahuje odsek 1 bod ii).

Vypustenie všetkých individuálnych identifikačných kódov zahrnutých v daných osobných informáciách (vrátane nahradenia daných individuálnych identifikačných kódov inými opismi atď. metódou, ktorá nevykazuje žiadnu pravidelnosť, podľa ktorej možno obnoviť dané osobné identifikačné kódy).

Článok 36 (ods. 1) zákona

1. Hospodársky subjekt nakladajúci s osobnými informáciami pri vytváraní anonymne spracúvaných informácií (len tie, ktoré tvoria databázu anonymne spracúvaných informácií atď.; rovnako aj ďalej) spracúva osobné informácie v súlade s normami, ktoré sú stanovené v pravidlách Komisie pre ochranu osobných informácií ako nevyhnutné na znemožnenie identifikácie konkrétnej fyzickej osoby a obnovu osobných informácií použitých na získanie uvedených informácií.

Článok 19 pravidiel

Normy stanovené v predpisoch Komisie pre ochranu osobných informácií podľa článku 36 ods. 1 zákona sú takéto:

- i) vypustenie celých opisov atď. alebo ich časti, na základe ktorých možno identifikovať konkrétnu fyzickú osobu, ktorej sa osobné informácie týkajú (vrátane nahradenia takýchto opisov atď. inými opismi atď. metódou, ktorá nevykazuje žiadnu pravidelnosť, podľa ktorej možno obnoviť celé opisy atď. alebo ich časť);
- ii) vypustenie všetkých individuálnych identifikačných kódov zahrnutých v osobných informáciách (vrátane nahradenia takýchto kódov inými opismi atď. metódou, ktorá nevykazuje žiadnu pravidelnosť, podľa ktorej možno obnoviť individuálne identifikačné kódy);
- iii) vypustenie kódov (len tých kódov, ktoré navzájom prepájajú viac informácií, ktoré hospodársky subjekt nakladajúci s osobnými informáciami skutočne používa), ktoré prepájajú osobné informácie a informácie získané prijatím opatrení súvisiacich s osobnými informáciami (vrátane nahradenia daných kódov inými kódmi, na základe ktorých nemožno prepojiť dané osobné informácie a informácie získané prijatím opatrení v súvislosti s danými osobnými informáciami metódou, ktorá nevykazuje žiadnu pravidelnosť, podľa ktorej možno obnoviť dané kódy);
- iv) vypustenie idiosynkratických opisov atď. (vrátane nahradenia takýchto opisov atď. inými opismi atď. metódou, ktorá nevykazuje žiadnu pravidelnosť, podľa ktorej možno obnoviť dané idiosynkratické opisy atď.);
- v) popri opatreniach uvedených v jednotlivých predchádzajúcich bodoch prijatie primeraných opatrení vyplývajúcich z výsledkov zohľadnenia charakteristických znakov atď. databáz osobných informácií, ako je rozdiel medzi opismi atď. zahrnutými v osobných informáciách a opismi atď. zahrnutými v iných osobných informáciách tvoriacich databázu osobných informácií atď., ktorá zahŕňa dané osobné informácie.

Článok 36 (ods. 2) zákona

2. Hospodársky subjekt nakladajúci s osobnými informáciami po vytvorení anonymne spracúvaných informácií prijíma v súlade s normami, ktoré sú v predpisoch Komisie pre ochranu osobných informácií vymedzené ako nevyhnutné na zabránenie úniku informácií týkajúcich sa uvedených opisov atď. a individuálnych identifikačných kódov vypustených z osobných informácií použitých na získanie anonymne spracúvaných informácií a informácií týkajúcich sa spôsobu spracovania uplatneného podľa ustanovení predchádzajúceho odseku, opatrenia na kontrolu bezpečnosti takýchto informácií.

Článok 20 pravidiel

Normy stanovené v predpisoch Komisie pre ochranu osobných informácií podľa článku 36 ods. 2 zákona sú takéto:

- i) jasné vymedzenie právomoci a zodpovednosti osoby nakladajúcej s informáciami týkajúcimi sa uvedených opisov atď. a individuálnymi identifikačnými kódmi, ktoré boli vypustené z osobných informácií použitých na získanie anonymne spracúvaných informácií a informácií týkajúcich sa spôsobu spracovania uplatneného podľa ustanovení článku 36 ods. 1 (len tie, ktoré môžu dané osobné informácie pomocou takýchto súvisiacich informácií obnoviť) (ďalej v tomto článku len „informácie týkajúce sa spôsobu spracovania atď.“);
- ii) vytvorenie pravidiel a postupov, pokiaľ ide o nakladanie s informáciami týkajúcimi sa spôsobu spracovania atď., primerané nakladanie s informáciami týkajúcimi sa spôsobu spracovania atď. v súlade s pravidlami a postupmi, hodnotenie situácie nakladania s informáciami a prijímanie nevyhnutných opatrení na základe výsledkov takýchto hodnotení s cieľom dosiahnuť zlepšenie;
- iii) prijímanie nevyhnutných a primeraných opatrení na zabránenie osobe bez zákonnej právomoci nakladať s informáciami týkajúcimi sa spôsobu spracovania atď. v tom, aby nakladala s informáciami týkajúcimi sa spôsobu spracovania atď.

Osobné informácie poskytnuté z EÚ na základe rozhodnutia o primeranosti sa považujú za anonymne spracúvané informácie v zmysle článku 2 ods. 9 zákona len vtedy, ak hospodársky subjekt nakladajúci s osobnými informáciami prijíma opatrenia, na základe ktorých je znemožnenie identifikácie danej fyzickej osoby nezvratné pre všetkých, okrem iného aj vymazaním informácií týkajúcich sa spôsobu spracovania atď. [t. j. informácie týkajúce sa opisov atď. a individuálnych identifikačných kódov, ktoré boli vymazané z osobných informácií použitých na získanie anonymne spracúvaných informácií a informácií týkajúcich sa spôsobu spracovania uplatneného podľa ustanovení článku 36 ods. 1 zákona (len tie, ktoré môžu dané osobné informácie pomocou takýchto súvisiacich informácií obnoviť)].

PRÍLOHA 2

Jej excelencia pani Věra Jourová, komisárka Európskej komisie pre spravodlivosť, spotrebiteľov a rodovú rovnosť

Vaša Excelencia,

vítam konštruktívne diskusie medzi Japonskom a Európskou komisiou zamerané na budovanie rámca pre vzájomný prenos osobných údajov medzi Japonskom a EÚ.

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

Tento dokument sa týka mnohých ministerstiev a orgánov štátnej správy Japonska a, pokiaľ ide o obsah dokumentu, príslušné ministerstvá a orgány (sekretariát vlády, Národná policajná agentúra, Komisia pre ochranu osobných informácií, ministerstvo vnútra a komunikácií, ministerstvo spravodlivosti, Spravodajská služba pre verejnú bezpečnosť, ministerstvo obrany) 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

Yoko Kamikawa

ministerka spravodlivosti

Tento dokument vypracovalo ministerstvo spravodlivosti a nasledujúce ministerstvá a orgány.

Koichi Hamano

poradca, sekretariát vlády

Schunichi Kuryu

generálny komisár Národnej policajnej agentúry

Mari Sonoda

generálna tajomníčka, Komisia pre ochranu osobných informácií

Mitsuru Yasuda

námestník ministra, ministerstvo vnútra a komunikácií

Seimei Nakagawa

Spravodajská služba pre verejnú bezpečnosť

Kenichi Takahashi

administratívny námestník ministra obrany

14. septembra 2018

Zhromažďovanie a používanie osobných informácií japonskými orgánmi verejnej moci na účely presadzovania práva v trestných veciach a národnej bezpečnosti

V tomto dokumente sa uvádza prehľad právneho rámca pre zhromažďovanie a používanie osobných (elektronických) informácií japonských 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. Toto vyhlásenie je určené Európskej komisii s cieľom vyjadriť záväzok a poskytnúť uistenia, že prístup vlády k osobným informáciám prenášaným z EÚ do Japonska bude obmedzený na to, čo je nevyhnutné a primerané, pričom bude podliehať nezávislému dozoru, a že dotknuté fyzické osoby budú môcť v prípade akéhokoľvek možného porušenia ich základného práva na súkromie a ochranu údajov získať nápravu. V tomto vyhlásení sa takisto stanovuje vytvorenie nového mechanizmu nápravy, ktorý bude spravovať Komisia pre ochranu osobných informácií (PPC) a ktorý bude slúžiť na vybavovanie sťažností fyzických osôb z EÚ týkajúcich sa prístupu vlády k ich osobným údajom prenášaným z EÚ do Japonska.

I. Všeobecné právne zásady týkajúce sa prístupu vlády

Prístup vlády je výkonom verejnej moci a ako taký sa musí uskutočňovať v plnom súlade s právnymi predpismi (zásada zákonnosti). V Japonsku sú osobné informácie v súkromnom aj verejnom sektore chránené viacrústvom mechanizmom.

A. Ústavný rámec a zásada výhrady práva

V článku 13 ústavy a v judikatúre sa právo na súkromie uznáva ako ústavné právo. Najvyšší súd v tejto súvislosti konštatoval, že je prirodzené, že fyzické osoby nechcú, aby iní bez náležitého dôvodu poznali ich osobné informácie, a že toto očakávanie by malo byť chránené⁽¹⁾. Ďalšia ochrana je zakotvená v článku 21 ods. 2 ústavy, ktorým sa zabezpečuje rešpektovanie dôverného charakteru komunikácie, a v článku 35 ústavy, ktorým sa zaručuje právo nebyť predmetom prehliadky a zaistenia veci bez súdneho príkazu, čo znamená, že zhromažďovanie osobných informácií povinnými prostriedkami vrátane prístupu k nim musí byť vždy založené na súdnom príkaze. Takýto súdny príkaz môže byť vydaný len na účely vyšetrovania už spáchaného trestného činu. V právnom rámci Japonska preto nie je povolené zhromažďovanie informácií povinnými prostriedkami na účely (nie vyšetrovania trestného činu, ale) národnej bezpečnosti.

Okrem toho, v súlade so zásadou výhrady práva musí byť povinný zber informácií osobitne povolený právnymi predpismi. V prípade nepovinného/dobrovoľného zhromažďovania sa informácie získavajú zo zdroja, ktorý je voľne prístupný, alebo sa prijímajú na základe žiadosti o dobrovoľné sprístupnenie, t. j. žiadosti, vyhovieť ktorej nemožno od fyzickej alebo právnickej osoby, ktorá informácie uchováva, vymáhať. To je však prípustné len pokiaľ je orgán verejnej moci oprávnený vykonávať vyšetrovanie, keďže každý orgán verejnej moci môže konať len v rámci svojej správnej právomoci stanovenej zákonom (bez ohľadu na to, či jeho činnosti zasahujú do práv a slobôd fyzických osôb). Táto zásada sa vzťahuje na schopnosť orgánu zhromažďovať osobné informácie.

B. Osobitné pravidlá týkajúce sa ochrany osobných informácií

Zákomom o ochrane osobných informácií („zákon APPI“) a zákonom o ochrane osobných informácií uchovávaných správnymi orgánmi („zákon APPIHAO“), ktoré sú založené na ústavných ustanoveniach a podrobnejšie ich rozvídzajú, sa zaručuje právo na osobné informácie v súkromnom aj vo verejnom sektore.

V článku 7 zákona APPI sa stanovuje, že PPC by mala formulovať „základnú politiku ochrany osobných informácií“ („základná politika“). Základná politika, ktorá sa prijíma rozhodnutím japonského kabinetu ako ústredného orgánu japonskej vlády (premiéra a ministrov štátu), určuje smer ochrany osobných informácií v Japonsku. PPC ako nezávislý dozorný orgán tak slúži ako „veliteľské centrum“ japonského systému ochrany osobných informácií.

Vždy, keď správne orgány zhromažďujú osobné informácie, a bez ohľadu na to, či pritom využívajú povinné prostriedky alebo nie, musia v zásade⁽²⁾ dodržiavať požiadavky zákona APPIHAO. Zákon APPIHAO je všeobecný zákon uplatniteľný na spracúvanie „uchovávaných osobných informácií“⁽³⁾ „správnymi orgánmi“ (podľa vymedzenia v článku 2 ods. 1 zákona APPIHAO). Vztahuje sa teda aj na spracúvanie údajov v oblasti presadzovania práva v trestných veciach a

⁽¹⁾ Najvyšší súd, rozsudok z 12. septembra 2003 [2002 (Ju) č. 1656].

⁽²⁾ Výnimky týkajúce sa kapitoly 4 zákona APPIHAO sú uvedené ďalej v texte na strane 16.

⁽³⁾ „Uchovávané osobné informácie“ v článku 2 ods. 5 zákona APPIHAO sú osobné informácie pripravené alebo získané zamestnancom správneho orgánu v priebehu plnenia jeho úloh a uchovávané týmto správnym orgánom na organizačné použitie jeho zamestnancami.

národnej bezpečnosti. Medzi orgánmi verejnej moci, ktoré sú oprávnené uskutočňovať prístup vlády, sú všetky orgány s výnimkou prefektúrnej polície štátnymi orgánmi, ktoré spadajú pod vymedzenie „správnych orgánov“. Nakladanie s osobnými informáciami zo strany prefektúrnej polície sa riadi prefektúrnymi nariadeniami ⁽⁴⁾, v ktorých sa stanovujú zásady ochrany osobných informácií, práva a povinnosti, ktoré sú rovnocenné so zákonom APPIHAO.

II. Prístup vlády na účely presadzovania práva v trestných veciach

A) Právne základy a obmedzenia

1. Zhromažďovanie osobných informácií povinnými prostriedkami

a) Právne základy

Podľa článku 35 ústavy právo všetkých osôb na ochranu domovej slobody, písomností a majetku pred vstupom, prehliadkami a zaistením vecí nesmie byť porušené s výnimkou prípadov, keď k tomu dochádza na základe súdneho príkazu vydaného z „primeraného dôvodu“, v ktorom sa presne uvádza miesto, ktoré sa má prehľadať, a veci, ktoré sa majú zaistiť. Preto sa povinné zhromažďovanie elektronických informácií orgánmi verejnej moci v rámci vyšetrovania trestného činu môže uskutočniť len na základe súdneho príkazu. To platí tak pre zhromažďovanie elektronických záznamov, ktoré obsahujú (osobné) informácie, ako aj na odpočúvanie komunikácie v reálnom čase. Jedinou výnimkou z tohto pravidla (ktorá však nie je relevantná v súvislosti s elektronickým prenosom osobných informácií zo zahraničia) je článok 220 ods. 1 Trestného poriadku ⁽⁵⁾, podľa ktorého môže generálny prokurátor, asistent generálneho prokurátora alebo príslušník justičnej polície pri zadržaní podozrivého alebo „zjavného páchatela“ v prípade potreby vykonať prehliadku a zaistenie vecí „na mieste zadržania“.

V článku 197 ods. 1 Trestného poriadku sa stanovuje, že povinné vyšetrovacie úkony sa „neuplatňujú, pokiaľ v tomto zákone nie sú stanovené osobitné ustanovenia“. Pokiaľ ide o povinné zhromažďovanie elektronických informácií, relevantným právnym základom v tejto súvislosti je článok 218 ods. 1 Trestného poriadku (podľa ktorého môže generálny prokurátor, asistent generálneho prokurátora alebo príslušník justičnej polície, ak je to potrebné na účely vyšetrovania trestného činu, vykonať prehliadku, zaistenie vecí alebo kontrolu na základe príkazu vydaného sudcom) a článok 222-2 Trestného poriadku (podľa ktorého sa povinné opatrenia na odpočúvanie elektronickej komunikácie bez súhlasu jednej zo strán vykonávajú na základe iných zákonov). V druhom z uvedených ustanovení sa odkazuje na zákon o odpočúvaní na účely vyšetrovania trestných činov (ďalej len „zákon o odpočúvaní“), v článku 3 ods. 1 ktorého sa stanovujú podmienky, za ktorých sa môže odpočúvať komunikácia týkajúca sa určitých závažných trestných činov na základe príkazu na odpočúvanie vydaného sudcom ⁽⁶⁾.

Pokiaľ ide o políciu, vyšetrovaciu právomoc má vo všetkých prípadoch prefektúrna polícia, zatiaľ čo Národná policajná agentúra (NPA) vyšetrovanie trestných činov na základe Trestného poriadku vôbec nevykonáva.

b) Obmedzenia

Povinné zhromažďovanie elektronických informácií je obmedzené ústavou a splnomocňujúcim štatútom, ako sa vykladá v judikatúre, ktorými sa predovšetkým upravujú kritériá, ktoré majú súdy uplatňovať pri vydávaní súdnych príkazov. Zákonom APPIHAO sa okrem toho ukladá niekoľko obmedzení, ktoré sa uplatňujú tak na zhromažďovanie informácií, ako aj na nakladanie s informáciami (pričom v miestnych vyhláškach sa v podstate predpisujú rovnaké kritériá pre prefektúrnú políciu).

(1) Obmedzenia vyplývajúce z ústavy a splnomocňujúceho štatútu

Podľa článku 197 ods. 1 Trestného poriadku sa povinné dispozície neuplatňujú, pokiaľ v danom zákone nie sú stanovené osobitné ustanovenia. V článku 218 ods. 1 Trestného poriadku sa následne stanovuje, že zaistenie atď. môže byť vykonané na základe príkazu vydaného sudcom iba „ak je to potrebné na účely vyšetrovania trestného činu“. Hoci

⁽⁴⁾ Každá prefektúra má svoje vlastné „prefektúrne nariadenie“, ktoré sa uplatňuje na ochranu osobných informácií prefektúrnou políciou. Anglické preklady týchto prefektúrnych nariadení neexistujú.

⁽⁵⁾ V článku 220 ods. 1 Trestného poriadku sa stanovuje, že keď generálny prokurátor, asistent generálneho prokurátora alebo príslušník justičnej polície zadrží podozrivého, môže v prípade potreby prijať tieto opatrenia: a) vstup do sídla inej osoby atď. na účely prehliadky podozrivého; b) prehliadka, zaistenie vecí alebo kontrola na mieste zadržania.

⁽⁶⁾ V tomto ustanovení sa konkrétnejšie stanovuje, že „generálny prokurátor alebo justičná polícia môžu v prípadoch, ktoré patria do jedného z nasledujúcich bodov, a ak existuje dostatočné podozrenie, že sa uskutoční komunikácia v súvislosti so spáchaním trestného činu, prípravami naň, konšpiráciami, pokiaľ ide o následné opatrenia, ako je napríklad utajovanie dôkazov atď., pokyny a iná vzájomná komunikácia týkajúca sa trestného činu, ktoré sú stanovené v každom z uvedených bodov (v druhom a treťom bode ďalej len „sériová trestná činnosť“), ako aj komunikácia obsahujúca záležitosti týkajúce sa uvedeného trestného činu (v tomto odseku ďalej len „komunikácia týkajúca sa trestného činu“) a v prípadoch, keď existuje mimoriadne obťažné identifikovať páchatela trestného činu alebo objasniť situáciu/podrobnosti spáchania trestného činu iným spôsobom, odpočúvať komunikáciu týkajúcu sa trestného činu na základe súdneho príkazu na odpočúvanie vydaného sudcom vzťahujúceho sa na prostriedok komunikácie, ktorý je určený telefónnym číslom a ďalšími číslami/kódmi na identifikáciu zdroja alebo destinácie hovoru a ktorý používa podozrivý na základe zmluvy s telekomunikačnými operátormi atď. (s výnimkou tých, v prípadoch ktorých neexistuje podozrenie, že sa použijú na komunikáciu týkajúcu sa trestného činu), alebo v prípadoch, keď existujú dôvody na podozrenie, že sa používa na komunikáciu týkajúcu sa trestného činu“, možno vykonať odpočúvanie komunikácie týkajúcej sa trestného činu prostredníctvom tohto komunikačného prostriedku.“

kritériá na posúdenie potrebnosti nie sú v štatutárnom práve bližšie určené, Najvyšší súd ⁽⁷⁾ rozhodol, že pri posudzovaní potreby dispozícií by mal sudca vykonať celkové posúdenie, pričom by mal zohľadniť najmä tieto prvky:

- a) závažnosť trestného činu a spôsob jeho spáchania,
- b) hodnotu a význam materiálov, ktoré sa majú zaistiť ako dôkaz,
- c) pravdepodobnosť ukrytia alebo zničenia zaistených materiálov,
- d) miera znevýhodnenia spôsobeného zaistením,
- e) ďalšie súvisiace podmienky.

Obmedzenia vyplývajú aj z požiadavky „primeraného dôvodu“ stanovenej v článku 35 ústavy. Na základe normy „primeraného dôvodu“ môže byť súdny príkaz vydaný, ak: 1. je potrebné vykonať vyšetrovanie trestného činu {[pozri už uvedený rozsudok Najvyššieho súdu z 18. marca 1969 [1968 (Shi) č. 100]}}, 2. existuje situácia, keď sa predpokladá, že podozrivý (obvinený) spáchal trestný čin (článok 156 ods. 1 Trestného poriadku) ⁽⁸⁾, 3. súdny príkaz na vyšetrovanie osoby, vecí, obydliä alebo akéhokoľvek iného miesta inej osoby, než je obvinený, by mal byť vydaný, len ak sa odôvodnene predpokladá, že veci, ktoré by mali byť zaistené, existujú (článok 102 ods. 2 Trestného poriadku). Ak sa sudca domnieva, že listinné dôkazy, ktoré predložili vyšetrovacie orgány, nepredstavujú dostatočné dôvody na podozrenie z trestného činu, žiadosť o vydanie súdneho príkazu zamietne. V tejto súvislosti treba poznamenať, že podľa zákona o trestaní organizovanej trestnej činnosti a kontrole výnosov z trestnej činnosti „akty prípravy spáchania“ plánovaného trestného činu (napr. príprava peňazí na spáchanie trestného činu terorizmu) samy o sebe predstavujú trestný čin, a preto môžu podliehať povinnému vyšetrovaniu na základe súdneho príkazu.

A napokon, ak sa súdny príkaz týka vyšetrovania osoby, vecí, obydliä alebo akéhokoľvek iného miesta inej osoby, než je podozrivý alebo obvinený, vydá sa len vtedy, ak možno odôvodnene predpokladať, že veci, ktoré sa majú zaistiť, existujú (článok 102 ods. 2 a článok 222 ods. 1 Trestného poriadku).

Pokiaľ ide konkrétne o odpočúvanie komunikácie na účely vyšetrovania trestného činu na základe zákona o odpočúvaní, môže sa vykonať len vtedy, keď sú splnené prísne požiadavky stanovené v článku 3 ods. 1 daného zákona. Podľa uvedeného ustanovenia sa na účely odpočúvania vždy vyžaduje predchádzajúci súdny príkaz, ktorý môže byť vydaný len v obmedzených situáciách ⁽⁹⁾.

2. Obmedzenia vyplývajúce zo zákona APPIHAO

Pokiaľ ide o zhromažďovanie ⁽¹⁰⁾ osobných informácií správnymi orgánmi a ďalšie nakladanie (najmä uchovávanie, správu a využívanie) s nimi týmito orgánmi, v zákone APPIHAO sa stanovujú najmä tieto obmedzenia:

- a) Podľa článku 3 ods. 1 zákona APPIHAO môžu správne orgány uchovávať osobné informácie, len ak je uchovávanie potrebné na plnenie úloh, ktoré patria do ich právomoci, ako je stanovené v zákonoch a iných právnych predpisoch. Pri uchovávaní sa od nich takisto vyžaduje, aby konkrétne určili (v čo najväčšej možnej miere) účel použitia osobných informácií. Podľa článku 3 ods. 2 a 3 zákona APPIHAO správne orgány nesmú uchovávať osobné informácie nad rámec potrebný na dosiahnutie takto určeného účelu použitia a nesmú zmeniť účel použitia nad rámec toho, čo sa môže primerane považovať za primerane relevantné na pôvodný účel.
- b) V článku 5 zákona APPIHAO sa stanovuje, že vedúci správneho orgánu sa usiluje o zabezpečenie správnosti a aktuálnosti uchovávaných osobných informácií v rozsahu nevyhnutnom na dosiahnutie účelu použitia.
- c) V článku 6 ods. 1 zákona APPIHAO sa stanovuje, že vedúci správneho orgánu prijme opatrenia potrebné na zabránenie úniku, strate alebo poškodeniu, ako aj na riadnu správu uchovávaných osobných informácií.
- d) Podľa článku 7 zákona APPIHAO žiaden (ani bývalý) zamestnanec nesmie sprístupniť získané osobné informácie inej osobe bez oprávneného dôvodu, alebo takéto informácie použiť na neoprávnený účel.

⁽⁷⁾ Rozsudok z 18. marca 1969 [1968 (Shi) č. 100].

⁽⁸⁾ V článku 156 ods. 1 Trestného poriadku sa stanovuje: „Pri podaní žiadosti uvedenej v odseku 1 predchádzajúceho článku žiadateľ poskytne materiály, na základe ktorých by sa mal podozrivý alebo obvinený považovať za osobu, ktorá spáchala za trestný čin.“

⁽⁹⁾ Pozri poznámku pod čiarou č. 6.

⁽¹⁰⁾ V článku 3 ods. 1 a 2 zákona APPIHAO sa obmedzuje rozsah uchovávania, a teda aj zhromažďovania osobných informácií.

- e) Okrem toho sa v článku 8 ods. 1 zákona APPIHAO stanovuje, že ak sa v zákonoch a iných právnych predpisoch nestanovuje inak, vedúci správneho orgánu nesmie používať uchovávané osobné informácie na iné účely, ako je stanovený účel použitia, ani ich na takéto účely poskytnúť inej osobe. Hoci článok 8 ods. 2 obsahuje výnimky z tohto pravidla v konkrétnych situáciách, uplatňujú sa len vtedy, ak takéto výnimočné sprístupnenie pravdepodobne nespôsobí „nespravodlivé“ poškodenie práv a záujmov dotknutej osoby alebo tretej strany.
- f) Podľa článku 9 zákona APPIHAO, ak sa uchovávané osobné informácie poskytujú inej osobe, vedúci správneho orgánu v prípade potreby stanoví obmedzenia účelu alebo spôsobu použitia, alebo akékoľvek iné potrebné obmedzenia; zároveň môže prijímajúcu osobu požiadať, aby prijala opatrenia potrebné na zabránenie úniku a na riadnu správu informácií.
- g) V článku 48 zákona APPIHAO sa stanovuje, že vedúci správneho orgánu sa usiluje náležite a urýchlene spracovať všetky sťažnosti týkajúce sa nakladania s osobnými informáciami.

2. Zhromažďovanie osobných informácií na základe žiadostí o dobrovoľnú spoluprácu (dobrovoľné vyšetrowanie)

a) Právny základ

Osobné informácie sa okrem využitia povinných prostriedkov získavajú buď zo zdroja, ktorý je voľne prístupný, alebo na základe dobrovoľného sprístupnenia, a to aj hospodárskymi subjektmi, ktoré takéto informácie uchovávajú.

Pokiaľ ide o dobrovoľné sprístupnenie, článkom 197 ods. 2 Trestného poriadku sa prokuratúra a justičná polícia oprávňujú na podávanie „písomných žiadostí vo veciach vyšetrowania“ (tzv. „žiadostí o sprístupnenie informácií“). Podľa Trestného poriadku sa od dožiadaných osôb požaduje, aby vyšetrovacím orgánom poskytli informácie. Neexistuje však žiaden spôsob, ako dožiadané verejné úrady alebo verejnosť a/alebo súkromné organizácie prinútiť, aby vyšetrovacím orgánom poskytli informácie, ak odmietajú tejto požiadavke vyhovieť. Ak uvedené osoby na základe žiadostí neposkytnú vyšetrovacím orgánom informácie, nemôžu byť trestne stíhané ani im nemožno uložiť iné sankcie. Ak vyšetrovacie orgány považujú požadované informácie za nevyhnutné, budú musieť informácie získať vykonaním prehliadky a zaisťovaním vecí na základe súdneho príkazu.

Vzhľadom na rastúce povedomie fyzických osôb, pokiaľ ide o ich práva na súkromie, ako aj vzhľadom na pracovné zaťaženie vyplývajúce z týchto žiadostí, sú hospodárske subjekty pri odpovediach na tieto žiadosti čoraz obozretnejšie⁽¹¹⁾. Hospodárske subjekty pri rozhodovaní o tom, či spolupracovať, zohľadňujú najmä povahu požadovaných informácií, ich vzťah k osobe, ktorej sa informácie týkajú, riziká poškodenia ich povesti, riziká súdnych sporov atď.

b) Obmedzenia

Rovnako ako povinné zhromažďovanie elektronických informácií, aj dobrovoľné vyšetrowanie je obmedzené ústavou, ako sa vykladá v judikatúre, a splnomocňujúcim štatútom. Hospodárske subjekty navyše zo zákona nemôžu v určitých situáciách informácie sprístupňovať. A na záver, v zákone APPIHAO sa stanovuje niekoľko obmedzení, ktoré sa uplatňujú tak na zhromažďovanie informácií, ako aj na nakladanie s informáciami (pričom v miestnych vyhláškach sa v podstate predpisujú rovnaké kritériá pre prefektúrnú políciu).

1. Obmedzenia vyplývajúce z ústavy a splnomocňujúceho štatútu

Najvyšší súd pri zohľadnení účelu článku 13 ústavy stanovil v dvoch rozhodnutiach z 24. decembra 1969 [1965 (A) č. 1187] a 15. apríla 2008 [2007 (A) č. 839] obmedzenia pre dobrovoľné vyšetrowania vykonávané vyšetrovacími orgánmi. Hoci sa tieto rozhodnutia týkali prípadov, keď sa osobné informácie (vo forme snímok) zhromažďovali prostredníctvom fotografovania/natáčania, zistenia sú vo všeobecnosti relevantné pre dobrovoľné (nepovinné) vyšetrowania, ktoré zasahujú do súkromia jednotlivca. Preto sa uplatňujú a musia sa dodržiavať, pokiaľ ide o zhromažďovanie osobných informácií formou dobrovoľného vyšetrowania, s prihliadnutím na osobitné okolnosti každého prípadu.

Podľa týchto rozhodnutí závisí zákonnosť dobrovoľného vyšetrowania od splnenia troch kritérií, a to:

— „podozrenie z trestného činu“ (t. j. musí sa posúdiť, či bol spáchaný trestný čin),

— „potreba vyšetrowania“ (t. j. musí sa posúdiť, či je žiadosť v rozsahu toho, čo je potrebné na účely vyšetrowania) a

⁽¹¹⁾ Pozri aj oznámenie Národnej policajnej agentúry zo 7. decembra 1999 (uvedené na str. 9), v ktorom sa uvádza to isté.

— „vhodnosť metód“ (t. j. musí sa posúdiť, či je dobrovoľné vyšetrovanie „vhodné“ alebo primerané na to, aby sa dosiahol jeho účel) ⁽¹²⁾.

So zreteľom na uvedené tri kritériá sa zákonnosť dobrovoľného vyšetrovania vo všeobecnosti posudzuje z hľadiska toho, či ho možno považovať za primerané v súlade so spoločensky akceptovanými konvenciami.

Požiadavka, aby bolo vyšetrovanie „potrebné“, takisto vyplýva priamo z článku 197 Trestného poriadku a bola potvrdená v pokynoch vydaných Národnou policajnou agentúrou (NPA) prefektúrnej polícii v súvislosti s používaním „žiadostí o sprístupnenie informácií“. V oznámení NPA zo 7. decembra 1999 sa stanovuje niekoľko procesných obmedzení vrátane požiadavky používať „žiadosti o sprístupnenie informácií“ len v prípade, ak je to potrebné na účely vyšetrovania. Článok 197 ods. 1 Trestného poriadku je navyše obmedzený na vyšetrovanie trestných činov, a preto sa môže uplatňovať len vtedy, ak existuje konkrétne podozrenie z už spáchaného trestného činu. Naopak, tento právny základ sa pri zhromažďovaní a využívaní osobných informácií nemôže uplatniť, ak k porušeniu práva ešte nedošlo.

2. Obmedzenia vzťahujúce sa na určité hospodárske subjekty

V určitých oblastiach sa uplatňujú ďalšie obmedzenia na základe ochrany stanovenej v iných právnych predpisoch.

Po prvé, vyšetrovacie orgány, ako aj telekomunikační operátori, ktorí uchovávajú osobné informácie, majú povinnosť rešpektovať dôverný charakter komunikácie, ako je to zaručené v článku 21 ods. 2 ústavy ⁽¹³⁾. Telekomunikačné operátori okrem toho majú rovnakú povinnosť aj podľa článku 4 zákona o telekomunikáciách ⁽¹⁴⁾. Podľa „Usmernení o ochrane osobných informácií v oblasti telekomunikácií“, ktoré vydalo Ministerstvo vnútra a komunikácií na základe ústavy a zákona o telekomunikáciách, nesmú telekomunikační operátori v prípadoch, keď je ohrozený dôverný charakter komunikácie, sprístupňovať osobné informácie týkajúce sa dôverného charakteru komunikácie tretím stranám, s výnimkou prípadov, keď získali súhlas fyzickej osoby alebo ak sa môžu odvolať na jeden z „odôvodnených dôvodov“ nesúladiu s Trestným zákonom. Posledné uvedené súvisí s „odôvodneným konaním“ (článok 35 Trestného zákona), „sebaobranou“ (článok 36 Trestného zákona) a „odvrátením bezprostredného nebezpečenstva“ (článok 37 Trestného zákona). Podľa Trestného zákona je „odôvodnené konanie“ len také konanie telekomunikačného operátora, ktorým vykonáva povinné opatrenia štátu, čo vylučuje dobrovoľné vyšetrovanie. Preto, ak vyšetrovacie orgány požadujú osobné informácie na základe „žiadostí o sprístupnenie informácií“ (článok 197 ods. 2 Trestného poriadku), pre telekomunikačného operátora platí zákaz poskytnúť údaje.

Po druhé, hospodárske subjekty sú povinné zamietnuť žiadosti o dobrovoľnú spoluprácu, ak im zákon zakazuje sprístupňovať osobné informácie. Ide napríklad o prípady, keď má hospodársky subjekt povinnosť rešpektovať dôverný charakter informácií, napríklad podľa článku 134 Trestného zákona ⁽¹⁵⁾.

3. Obmedzenia na základe zákona APPIHAO

Pokiaľ ide o zhromažďovanie osobných informácií správnymi orgánmi a ďalšie nakladanie s týmito informáciami týmito orgánmi, v zákone APPIHAO sa stanovujú obmedzenia, ako je vysvetlené vyššie v oddiele II.A.1 písm. b) bode 2). Rovnaké obmedzenia vyplývajú z prefektúrnych nariadení, ktoré sa vzťahujú na prefektúrnú políciu.

B) Dozor

1. Justičný dozor

Pokiaľ ide o zhromažďovanie osobných informácií povinnými prostriedkami, musí sa uskutočňovať vždy na základe súdneho príkazu ⁽¹⁶⁾, a preto podlieha predchádzajúcemu preskúmaniu sudcom. V prípade, že vyšetrovanie bolo nezákonné, sudca môže vylúčiť takýto dôkaz pri následnom súdnom konaní vo veci. Fyzická osoba môže požiadať o takéto vylúčenie vo svojom súdnom konaní s tvrdením, že vyšetrovanie bolo nezákonné.

⁽¹²⁾ Dôležitými faktormi pri posudzovaní „vhodnosti metód“ sú závažnosť trestného činu a naliehavosť.

⁽¹³⁾ V článku 21 ods. 2 ústavy sa stanovuje: „Nesmie sa uplatňovať žiadna cenzúra, ani sa nesmie porušiť dôverný charakter žiadnych komunikačných prostriedkov.“

⁽¹⁴⁾ V článku 4 zákona o telekomunikáciách sa stanovuje: „1. Nesmie dôjsť k porušeniu dôverného charakteru komunikácie, s ktorou nakladá telekomunikačný operátor. 2. Žiadna osoba, ktorá pôsobí v oblasti telekomunikácií, nesmie sprístupniť tajomstvá, ktoré získala pri výkone svojej funkcie, pokiaľ ide o komunikáciu, s ktorou nakladá telekomunikačný operátor. To isté platí aj po jej odchode z funkcie.“

⁽¹⁵⁾ V článku 134 Trestného zákona sa stanovuje: „1. Ak lekár, farmaceut, distribútor liekov, pôrodná asistentka, advokát, obhajca, notár alebo akákoľvek iná osoba, ktorá v minulosti takéto povolanie vykonávala, bez oprávnených dôvodov sprístupní dôverné informácie inej osoby, o ktorých sa dozvedela počas výkonu tohto povolania, uloží sa jej trest odňatia slobody s nariadeným výkonom práce v trvaní najviac šesť mesiacov alebo pokuta vo výške najviac 100 000 jenov. 2. To isté platí v prípade, keď osoba, ktorá vykonáva alebo vykonávala náboženské povolanie, bez oprávnených dôvodov sprístupní dôverné informácie inej osoby, o ktorých sa dozvedela počas výkonu takýchto náboženských činností.“

⁽¹⁶⁾ Pokiaľ ide o výnimku z tohto pravidla, pozri poznámku pod čiarou č. 5.

2. Dohľad na základe zákona APPIHAO

V Japonsku má minister alebo vedúci každého ministerstva alebo agentúry právomoc dohľadu a presadzovania na základe zákona APPIHAO, pričom minister vnútra a komunikácií môže prešetrovať presadzovanie zákona APPIHAO na všetkých ostatných ministerstvách.

Ak to minister vnútra a komunikácií – napríklad na základe prešetrovania stavu presadzovania zákona APPIHAO ⁽¹⁷⁾, vybavovania sťažností alebo otázok určených jednému z jeho všeobecných informačných centier – považuje za potrebné na dosiahnutie účelu zákona APPIHAO, môže požiadať vedúceho správneho orgánu, aby predložil materiály a vysvetlenia týkajúce sa nakladania s osobnými informáciami v rámci príslušného správneho orgánu na základe článku 50 zákona APPIHAO. Minister môže predložiť vedúcemu správneho orgánu stanoviská týkajúce sa spracúvania osobných informácií v rámci správneho orgánu, ak to považuje za potrebné na dosiahnutie účelu tohto zákona. Minister môže okrem toho napríklad požiadať o revíziu opatrení prostredníctvom akcií, ktoré môže uskutočniť na základe článkov 50 a 51 zákona v prípade podozrenia, že došlo k porušeniu alebo nevhodnému výkonu zákona. Pomôže to zabezpečiť jednotné uplatňovanie a dodržiavanie zákona APPIHAO.

3. Dohľad komisií pre verejnú bezpečnosť týkajúci sa polície

Pokiaľ ide o policajnú správu, Národná policajná agentúra podlieha dohľadu zo strany Národnej komisie pre verejnú bezpečnosť, zatiaľ čo prefektúrna polícia podlieha dohľadu zo strany jednej z prefektúrnych komisií pre verejnú bezpečnosť, ktoré boli zriadené v každej prefektúre. Každý z týchto orgánov dohľadu zabezpečuje demokratickú správu a politickú neutralitu policajnej správy.

Národná komisia pre verejnú bezpečnosť zodpovedá za záležitosti, ktoré patria do jej právomoci podľa zákona o polícii a iných zákonov. Ide o vymenovanie generálneho komisára Národnej policajnej agentúry a miestnych vyšších príslušníkov polície, ako aj vypracovanie komplexných politík, ktorými sa stanovujú základné smery alebo opatrenia týkajúce sa správy Národnej policajnej agentúry.

Prefektúrne komisie pre verejnú bezpečnosť sa skladajú z členov zastupujúcich osoby v príslušnej prefektúre na základe zákona o polícii a riadia prefektúrnu políciu ako nezávislý systém rady. Členov vymenúva guvernér prefektúry so súhlasom zhromaždenia prefektúry na základe článku 39 zákona o polícii. Ich funkčné obdobie je tri roky a môžu byť odvolaní proti ich vôli iba z konkrétnych dôvodov uvedených v zákone (ako je napríklad neschopnosť vykonávať svoje povinnosti, porušovanie povinností, zneužitie právomocí atď.), čím sa zabezpečuje ich nezávislosť (pozri články 40 a 41 zákona o polícii). S cieľom zaručiť ich politickú neutralitu sa okrem toho v článku 42 zákona o polícii členovi komisie zakazuje, aby súčasne pôsobil ako člen legislatívneho orgánu, stal sa výkonným členom politickej strany alebo iného politického orgánu, alebo aby sa aktívne zapájal do politických hnutí. Aj keď každá komisia spadá pod právomoc príslušného guvernéra prefektúry, nevyplyva z toho, že by guvernér mal právomoc vydávať pokyny, pokiaľ ide o výkon jej funkcií.

Podľa článku 38 ods. 3 v spojení s článkom 2 a článkom 36 ods. 2 zákona o polícii sú prefektúrne komisie pre verejnú bezpečnosť zodpovedné za „ochranu práv a slobôd fyzických osôb“. Na tento účel dostávajú od náčelníkov prefektúrnej polície správy týkajúce sa činností v rámci ich právomoci, a to aj na pravidelných stretnutiach konaných trikrát alebo štyrikrát mesačne. Komisie poskytujú usmernenia k týmto záležitostiam prostredníctvom vypracovania komplexných politík.

Prefektúrne komisie pre verejnú bezpečnosť môžu navyše v rámci svojej funkcie dohľadu vydávať usmernenia pre prefektúrnu políciu ku konkrétnym individuálnym prípadom, v ktorých to považujú za potrebné v súvislosti s inšpekciou činností prefektúrnej polície alebo zneužitím právomocí zamestnancami polície. Komisie môžu, ak to považujú za potrebné, takisto určiť osobitného člena komisie na preskúmanie stavu vykonávania vydaného nariadenia (článok 43-2 zákona o polícii).

⁽¹⁷⁾ Na zabezpečenie transparentnosti a uľahčenie dohľadu zo strany ministerstva vnútra a komunikácií je podľa článku 11 zákona APPIHAO vedúci správneho orgánu povinný zaznamenať každý bod predpísaný v článku 10 ods. 1 zákona APPIHAO, ako napríklad názov správneho orgánu, ktorý uchováva zložku, účel použitia zložky, metódu zhromažďovania osobných informácií atď. (tzv. „register zložiek osobných informácií“). Zložky osobných informácií, na ktoré sa vzťahuje článok 10 ods. 2 zákona APPIHAO, ako napríklad zložky vypracované alebo získané v rámci vyšetrovania trestného činu alebo týkajúce sa záležitostí dôležitých pre národnú bezpečnosť, sú však oslobodené od povinnosti informovať ministerstvo vnútra a komunikácií a zaradiť ich do verejného registra. Podľa článku 7 zákona o správe verejných záznamov a archívov sa však od vedúceho správneho orgánu vyžaduje, aby vždy zaznamenával klasifikáciu, názov, lehotu a miesto uchovávania atď. správnych dokumentov („register správy zložiek správnych dokumentov“). Súpis informácií v oboch registroch je uverejnený na internete a umožňuje fyzickým osobám overiť, aký druh osobných informácií zložka obsahuje a ktorý správny orgán informácie uchováva.

4. Dohľad zo strany parlamentu

Parlament môže vykonávať vyšetrovanie vo vzťahu k činnostiam verejných orgánov a na tento účel vyžadovať vypracúvanie dokumentov a svedeckých výpovedí (článok 62 ústavy). V tomto kontexte môže príslušný parlamentný výbor preskúmať vhodnosť činností zhromažďovania informácií, ktoré vykonáva polícia.

Tieto právomoci sú bližšie špecifikované v parlamentnom zákone. V súlade s článkom 104 môže parlament vyžadovať, aby vláda a verejné agentúry vypracúvali správy a záznamy potrebné na vykonanie vyšetrovania. Členovia parlamentu môžu okrem toho predkladať „písomné otázky“ podľa článku 74 parlamentného zákona. Takéto otázky musí schváliť predseda parlamentu a v zásade na ne musí odpovedať vláda písomne do siedmich dní (ak nie je možné odpovedať v tejto lehote, musí to byť odôvodnené a musí sa stanoviť nový termín, článok 75 parlamentného zákona). V minulosti písomné otázky parlamentu zahŕňali aj nakladanie s osobnými informáciami v rámci štátnej správy⁽¹⁸⁾.

C) Individuálne prostriedky nápravy

Podľa článku 32 Ústavy Japonska nemá byť žiadnej osobe odopreté právo na prístup k súdom. Článok 17 ústavy okrem toho zaručuje každej osobe právo žalovať štát alebo verejný subjekt o nápravu (ako je stanovené v zákone) v prípade, keď jej vznikne škoda v dôsledku protiprávneho konania verejného činiteľa.

1. Súdne prostriedky nápravy proti povinnému zhromažďovaniu informácií na základe súdneho príkazu (článok 430 Trestného poriadku)

Podľa článku 430 ods. 2 Trestného poriadku fyzická osoba, ktorá nie je spokojná s opatreniami, ktoré vykonal policajný úradník v súvislosti so zaistením vecí (aj ak obsahujú osobné informácie) na základe súdneho príkazu, môže podať žiadosť (tzv. „kvázi sťažnosť“) na príslušnom súde, aby sa takéto opatrenia „zrušili alebo zmenili“.

Takúto výzvu možno zaslať bez toho, aby fyzická osoba musela čakať na uzavretie prípadu. Ak súd zistí, že zaistenie nebolo potrebné alebo že existujú iné dôvody, pre ktoré sa zaistenie považuje za nezákonné, môže nariadiť, aby sa takéto opatrenia zrušili alebo zmenili.

2. Súdne prostriedky nápravy podľa Občianskeho súdneho poriadku a zákona o opravných prostriedkoch proti štátu

Ak sa fyzické osoby domnievajú, že bolo porušené ich právo na súkromie podľa článku 13 ústavy, môžu podať občianskoprávnu žalobu so žiadosťou, aby osobné informácie zhromaždené v rámci vyšetrovania trestného činu boli vymazané.

Fyzická osoba môže takisto podať žalobu o náhradu škody na základe zákona o opravných prostriedkoch proti štátu v spojení s príslušnými článkami Občianskeho zákonníka, ak sa domnieva, že jej právo na súkromie bolo porušené a v dôsledku zhromažďovania jej osobných informácií alebo sledovania utrpela škodu⁽¹⁹⁾. Vzhľadom na to, že „škoda“, ktorá je predmetom žaloby o náhradu škody, nie je obmedzená na majetok (článok 710 Občianskeho zákonníka), môže sa vzťahovať aj na „psychické utrpenie“. Výšku náhrady za takúto morálnu ujmu posúdi sudca na základe „bezplatného hodnotenia s prihliadnutím na rôzne faktory v každom prípade“⁽²⁰⁾.

Podľa článku 1 ods. 1 zákona o opravných prostriedkoch proti štátu sa právo na odškodnenie prizná, ak i), ak štátny úradník vykonávajúci verejnú moc štátu alebo verejného subjektu ii) pri plnení svojich úloh iii) úmyselne alebo z nebanlivosti iv) protiprávne v) spôsobil škodu inej fyzickej osobe.

Fyzická osoba musí predložiť vec súdu v súlade s Občianskym súdnym poriadkom. Podľa platných pravidiel môže tak urobiť na súde, ktorý je príslušný podľa miesta, na ktorom bol spáchaný delikt.

⁽¹⁸⁾ Pozri napr. písomnú otázku snemovne radcov č. 92 z 27. marca 2009, ktorá sa týkala nakladania s informáciami zhromaždenými v súvislosti s vyšetrovaním trestného činu vrátane porušenia povinností týkajúcich sa zachovávaní mlčanlivosti zo strany policajných orgánov a orgánov prokuratúry.

⁽¹⁹⁾ Príkladom pre takéto opatrenie je „vec týkajúca sa zoznamu obrannej agentúry“, rozhodnutie súdu Niigata District z 11. mája 2006 [2002 (Wa) č. 514]. V tomto prípade úradník obrannej agentúry vypracoval, uchovával a distribuoval zoznam tých fyzických osôb, ktoré podali žiadosť o zverejnenie správnych dokumentov v obrannej agentúre. V tomto zozname boli uvedené opisy osobných informácií žalobcu. Žalobca požadoval, aby odporca zaplatil náhradu škody podľa článku 1 ods. 1 zákona o opravných prostriedkoch proti štátu, pričom tvrdil, že bolo porušené jeho súkromie, právo na informácie atď. Súd túto žiadosť čiastočne uznal a priznal žalobcovi čiastočnú náhradu.

⁽²⁰⁾ Rozhodnutie najvyššieho súdu z 5. apríla 1910 [1910 (O) č. 71].

3. Individuálne prostriedky nápravy proti nezákonným/neprimeraným vyšetrovaniam zo strany polície: sťažnosť určená Prefektúrnej komisii pre verejnú bezpečnosť (článok 79 zákona o polícii)

Podľa článku 79 zákona o polícii ⁽²¹⁾ ďalej objasneného v pokynoch vedúceho Národnej policajnej agentúry pre prefektúrnu políciu a prefektúrne komisie pre verejnú bezpečnosť ⁽²²⁾ môžu fyzické osoby podať na príslušnej Prefektúrnej komisii pre verejnú bezpečnosť písomnú sťažnosť ⁽²³⁾ proti akémukoľvek protiprávnemu alebo nevhodnému správaniu príslušníka polície pri výkone jeho povinností; zahŕňa to aj povinnosti týkajúce sa zhromažďovania a využívania osobných informácií. Uvedená komisia vybavuje takéto sťažnosti svedomito v súlade so zákonmi a miestnymi vyhláškami a písomne informuje sťažovateľa o vyšetrovaní.

Na základe svojej právomoci v oblasti dohľadu podľa článku 38 ods. 3 zákona o polícii Prefektúrna komisia pre verejnú bezpečnosť vydáva prefektúrnej polícii pokyn, aby vyšetrila skutočnosť, uplatnila potrebné opatrenia v súlade s výsledkom preskúmania a výsledky oznámila komisii. Ak to komisia považuje za potrebné, môže vydať aj pokyn na vybavenie sťažnosti, napríklad ak sa domnieva, že vyšetrovanie vykonané políciou je nedostatočné. Tento výkon funkcie je opísaný v oznámení, ktoré vydala Národná policajná agentúra pre vedúcich prefektúrnej polície.

Oznámenie výsledku vyšetrovania sťažovateľovi sa uskutočňuje aj vzhľadom na správy polície týkajúce sa vyšetrovania a opatrenia prijaté na žiadosť Komisie.

4. Individuálne prostriedky nápravy podľa zákona APPIHAO a Trestného poriadku

a) zákon APPIHAO

Podľa článku 48 zákona APPIHAO sa správne orgány musia usilovať náležite a urýchlene spracovať všetky sťažnosti týkajúce sa nakladania s osobnými informáciami. Ako prostriedok na poskytnutie konsolidovaných informácií fyzickým osobám (napr. o dostupných právach na zverejňovanie, opravu a pozastavenie používania podľa zákona APPIHAO) a ako kontaktné miesto pre otázky zriadilo ministerstvo vnútra a komunikácií všeobecné informačné centrá na zverejňovanie informácií/ochranu osobných informácií na každej z prefektúr, a to na základe článku 47 ods. 2 zákona APPIHAO. Otázky môžu klásť aj osoby bez trvalého pobytu. Napríklad v účtovnom roku 2017 (od apríla 2017 do marca 2018) všeobecné informačné centrá odpovedali na otázky atď. v celkovom počte 5 186 prípadov.

V článkoch 12 a 27 zákona APPIHAO sa fyzickým osobám priznáva právo požadovať zverejnenie a opravu uchovávaných osobných informácií. Podľa článku 36 zákona APPIHAO môžu fyzické osoby okrem toho požiadať o ukončenie používania alebo výmaz svojich uchovávaných osobných informácií, ak správny orgán získal tieto informácie nezákonne alebo ich uchováva, či používa v rozpore so zákonom.

Pokiaľ však ide o osobné informácie zhromaždené (na základe súdneho príkazu alebo prostredníctvom „žiadosti o sprístupnenie informácií“) a uchovávané na vyšetrovanie trestných činov ⁽²⁴⁾, takéto informácie vo všeobecnosti patria do kategórie „osobné informácie zaznamenané v dokumentoch týkajúcich sa súdnych konaní a zaistených vecí“. Takéto osobné údaje sú preto vylúčené z rozsahu uplatňovania individuálnych práv v kapitole 4 zákona APPIHAO podľa článku 53-2 Trestného poriadku ⁽²⁵⁾. Na spracovanie takýchto osobných informácií a práva fyzickej osoby na prístup a opravu sa

⁽²¹⁾ Článok 79 zákona o polícii (výňatok):

1. Každý, kto má výhrady proti výkonu povinností zamestnancami prefektúrnej polície, môže Prefektúrnej komisii pre verejnú bezpečnosť podať písomnú sťažnosť na základe postupu predpísaného vyhláškou Národnej komisie pre verejnú bezpečnosť.
2. Prefektúrna komisia pre verejnú bezpečnosť, ktorá dostala sťažnosť uvedenú v predchádzajúcom odseku, vybavuje takéto sťažnosti svedomito v súlade so zákonmi a miestnymi vyhláškami a písomne informuje sťažovateľa o vyšetrovaní, s výnimkou týchto prípadov:
 1. Sťažnosť môže byť uznaná za podanú s cieľom zabrániť zákonnosti výkonu povinností prefektúrnej polície;
 2. Súčasný pobyt sťažovateľa nie je známy;
 3. Sťažnosť môže byť uznaná za podanú spoločne s ostatnými sťažovateľmi a ostatným sťažovateľom už bol výsledok spoločnej sťažnosti oznámený.

⁽²²⁾ Národná policajná agentúra, Oznámenie o riadnom vybavovaní sťažností na výkon povinností príslušníkov polície z 13. apríla 2001 s dodatkom 1 „Normy týkajúce sa výkladu/vykonávania článku 79 zákona o polícii“.

⁽²³⁾ Podľa oznámenia Národnej policajnej agentúry (pozri predchádzajúcu poznámku pod čiarou) fyzické osoby, ktoré majú ťažkosti s napísaním sťažnosti, dostanú pomoc. Týka sa to výslovne aj cudzincov.

⁽²⁴⁾ Na druhej strane existujú dokumenty, ktoré nie sú klasifikované ako „dokumenty týkajúce sa súdnych konaní“, pretože neobsahujú informácie získané na základe súdneho príkazu alebo písomných žiadostí vo veciach vyšetrovania, ale boli vytvorené na základe takýchto dokumentov. Išlo by o prípad, keď súkromné informácie nepodliehajú článku 45 ods. 1 zákona APPIHAO, a preto by takéto informácie neboli vylúčené z uplatňovania kapitoly 4 zákona APPIHAO.

⁽²⁵⁾ V článku 53-2 ods. 2 Trestného poriadku sa stanovuje, že ustanovenia kapitoly IV zákona APPIHAO sa neuplatňujú na osobné informácie zaznamenané v dokumentoch týkajúcich sa súdnych konaní a zaistených vecí.

namiesto toho vzťahujú osobitné pravidlá podľa Trestného poriadku a zákona o konečných spisoch v trestných veciach (pozri ďalej) ⁽²⁶⁾. Toto vylúčenie je odôvodnené rôznymi faktormi, ako je ochrana súkromia dotknutých fyzických osôb, dôverný charakter vyšetrovaní a riadny priebeh súdneho konania. Ustanovenia kapitoly 2 zákona APPIHAO upravujúce zásady nakladania s takýmito informáciami zostávajú v platnosti.

b) Trestný poriadok

Podľa Trestného poriadku možnosti prístupu k osobným informáciám zhromaždeným na účely vyšetrovania trestných činov závisia od fázy konania a úlohy fyzickej osoby pri vyšetrovaní (podozrivý, obvinený, obeť atď.).

Ako výnimka z pravidla uvedeného v článku 47 Trestného poriadku, podľa ktorého sa dokumenty týkajúce sa súdneho konania nesmú zverejniť pred začatím súdneho konania (keďže by sa tým mohla porušiť česť a/alebo súkromie dotknutých osôb a mohlo by sa brániť vyšetrovaniu/súdnemu konaniu), je v zásade povolené, aby obeť trestného činu nahliadla do takýchto informácií v rozsahu, v akom sa to považuje za primerané vzhľadom na účel ustanovenia článku 47 Trestného poriadku ⁽²⁷⁾.

Pokiaľ ide o podozrivé osoby, obvyčajne sa o tom, že sú predmetom vyšetrovania trestného činu, dozvedia pri výsluchu od justičnej polície alebo generálneho prokurátora. Ak generálny prokurátor následne rozhodne nezačať trestné stíhanie, bezodkladne o tejto skutočnosti informuje podozrivú osobu na základe jej žiadosti (článok 259 Trestného poriadku).

Po začatí stíhania generálny prokurátor okrem toho poskytne obvinenému alebo jeho právnenému zástupcovi možnosť nahliadnuť do dôkazov pred tým, ako súd požiada o ich preskúmanie (článok 299 Trestného poriadku). To umožní, aby si obvinený overil svoje osobné informácie zhromaždené pri vyšetrovaní trestného činu.

V konečnom dôsledku je ochrana osobných informácií zhromaždených v súvislosti s vyšetrovaním trestného činu, ktoré sa týkajú podozrivého, obvineného alebo inej osoby (napr. obeť trestného činu) zaručená povinnosťou týkajúcou sa zachovávaní mlčanlivosti (článok 100 zákona o verejnej službe) a hrozbou pokuty v prípade úniku dôverných informácií v priebehu plnenia povinností súvisiacich s verejnou službou [článok 109 bod xii) zákona o verejnej službe].

5. Individuálne prostriedky nápravy proti nezákonným/neprimeraným vyšetrovaniam zo strany orgánov verejnej moci: sťažnosť PPC

Podľa článku 6 zákona APPI vláda v spolupráci s vládami tretích krajín prijíma potrebné opatrenia s cieľom vytvoriť medzinárodne konformný systém týkajúci sa osobných informácií prostredníctvom posilnenia spolupráce s medzinárodnými organizáciami a inými medzinárodnými rámcami. Na základe tohto ustanovenia základná politika ochrany osobných informácií (prijatá rozhodnutím vlády) deleguje na PPC ako orgán príslušný pre celkovú správu zákona APPI právomoc prijímať potrebné opatrenia na preklopenie rozdielov v systémoch a postupoch medzi Japonskom a príslušnou cudzou krajinou s cieľom zabezpečiť náležité nakladanie s osobnými informáciami získanými z takejto krajiny.

Ako sa stanovuje v článku 61 bodoch i) a ii) zákona APPI, je PPC poverená úlohou formulovať a presadzovať základnú politiku, ako aj mediáciu v prípade sťažností podaných proti hospodárskym subjektom. Správne orgány napokon navzájom úzko komunikujú a spolupracujú (článok 80 zákona APPI).

Na základe týchto ustanovení sa PPC bude zaoberať sťažnosťami, ktoré podali fyzické osoby, takto:

- a) Fyzická osoba, ktorá má podozrenie, že orgány verejnej moci v Japonsku vrátane tých, ktoré sú zodpovedné za činnosti uvedené v kapitole II a v kapitole III tohto „vyhlásenia“ zhromaždili alebo používajú jej údaje prenesené z EÚ v rozpore s platnými pravidlami vrátane tých, ktoré sú predmetom tohto „vyhlásenia“, môže podať sťažnosť PPC (samostatne alebo prostredníctvom svojho orgánu pre ochranu osobných údajov).
- b) PPC sa zaoberá sťažnosťou, pričom uplatňuje svoje právomoci podľa článku 6, článku 61 bodu ii) a článku 80 zákona APPI a informuje o sťažnosti príslušné orgány verejnej moci, ako aj príslušné orgány dohľadu.

⁽²⁶⁾ Podľa Trestného poriadku a zákona o konečných spisoch v trestných veciach prístup k zaisteným veciam, ako aj k dokladom/osobným informáciám týkajúcim sa súdnych konaní a ich oprava podliehajú jedinečnému a rozlišujúcemu systému pravidiel zameraných na ochranu súkromia dotknutých fyzických osôb, dôverný charakter vyšetrovaní a riadny priebeh súdneho konania atď.

⁽²⁷⁾ Konkrétnejšie je nahliadnutie do informácií týkajúcich sa objektívneho dôkazu v zásade povolené v prípade obetí trestných činov, pokiaľ ide o spisy o nestíhaní vo veciach podliehajúcich účasti obeť uvedených potom v článku 316-33 Trestného poriadku, s cieľom dosiahnuť, aby sa ochrana obetí trestnej činnosti stala uspokojivejšou.

Tieto orgány majú podľa článku 80 zákona APPI povinnosť spolupracovať s PPC okrem iného tak, že jej poskytnú potrebné informácie a príslušné materiály, aby PPC mohla zhodnotiť, či k zhromaždeniu osobných informácií alebo ich následnému použitiu došlo v súlade s platnými pravidlami. Pri uskutočňovaní tohto hodnotenia bude PPC spolupracovať s ministerstvom vnútra a komunikácií.

- c) Ak z hodnotenia vyplynie, že došlo k porušeniu platných pravidiel, spolupráca príslušných orgánov verejnej moci s PPC zahŕňa povinnosť toto porušenie napraviť.

V prípade nezákonného zhromažďovania osobných informácií podľa platných pravidiel táto povinnosť zahŕňa vymazanie zhromaždených informácií.

V prípade porušenia platných pravidiel PPC pred uzavretím hodnotenia zároveň potvrdí, že porušenie bolo v plnom rozsahu napravené.

- d) Po uzavretí hodnotenia PPC v primeranej lehote danej fyzickej osobe oznámi výsledok hodnotenia vrátane prípadných nápravných opatrení, ktoré sa prijali. Prostredníctvom tohto oznámenia PPC zároveň informuje fyzickú osobu o možnosti vyžiadať si od príslušného orgánu verejnej moci potvrdenie o výsledku a o tom, ktorému orgánu sa podáva takáto žiadosť o potvrdenie.

Podrobné informácie o výsledku hodnotenia možno obmedziť, ak existujú opodstatnené dôvody domnievať sa, že oznámenie takýchto informácií by mohlo ohroziť prebiehajúce vyšetrovanie.

Ak sa sťažnosť týka zhromažďovania alebo používania osobných údajov v oblasti presadzovania práva v trestných veciach, v prípade, že sa pri hodnotení zistí, že sa začalo konanie týkajúce sa osobných informácií danej fyzickej osoby a že dané konanie bolo ukončené, PPC upozorní fyzickú osobu na možnosť nahliadnuť do spisu podľa článku 53 Trestného poriadku a článku 4 zákona o konečných spisoch v trestných veciach.

Ak z hodnotenia vyplynie, že daná fyzická osoba je podozrivá v trestnej veci, PPC ju informuje o tejto skutočnosti, ako aj o možnosti podať žiadosť v súlade s článkom 259 Trestného poriadku.

- e) Ak fyzická osoba stále nie je spokojná s výsledkom tohto konania, môže sa obrátiť na PPC, ktorá informuje fyzickú osobu o rôznych možnostiach a podrobných postupoch získania prostriedkov nápravy podľa japonských zákonov a iných právnych predpisov. PPC navyše poskytne danej fyzickej osobe podporu vrátane poradenstva a pomoci pri akýchkoľvek ďalších krokoch vo vzťahu k príslušnému správnomu či súdnemu orgánu.

III. Prístup vlády na účely národnej bezpečnosti

A. Právne základy a obmedzenia pre zhromažďovanie osobných informácií

1. Právne základy pre zhromažďovanie informácií príslušným ministerstvom/orgánom

Ako sa uvádza vyššie, správne orgány môžu zhromažďovať osobné informácie na účely národnej bezpečnosti len v rámci svojej správnej právomoci.

V Japonsku neexistujú žiadne zákony, ktoré by umožňovali zhromažďovanie informácií povinnými prostriedkami výlučne na účely národnej bezpečnosti. Podľa článku 35 ústavy je nútené zhromažďovanie osobných informácií možné len na základe príkazu, ktorý vydal súd v súvislosti s vyšetrovaním trestného činu. Takýto príkaz môže byť teda vydaný len na účely vyšetrovania trestného činu. To znamená, že v japonskom právnom systéme nie je povolené zhromažďovať informácie alebo k nim pristupovať z dôvodov národnej bezpečnosti povinnými prostriedkami. V oblasti národnej bezpečnosti môžu príslušné ministerstvá alebo orgány namiesto toho získavať informácie len zo zdrojov, ktoré sú voľne prístupné, alebo prijímať informácie od hospodárskych subjektov alebo fyzických osôb len na základe dobrovoľného sprístupnenia. Hospodárske subjekty, ktoré dostanú žiadosť o dobrovoľnú spoluprácu, nie sú zo zákona povinné takéto informácie poskytnúť, a teda im nehrozia žiadne nepriaznivé dôsledky, ak odmietnu spolupracovať.

Právomocami v oblasti národnej bezpečnosti disponuje viacero ministerstiev a orgánov.

1. Sekretariát vlády

Sekretariát vlády zhromažďuje a vyhľadáva informácie týkajúce sa dôležitých politík vlády⁽²⁸⁾ vymedzené v článku 12-2 vládneho zákona⁽²⁹⁾. Nedisponuje však žiadnou právomocou zhromažďovať osobné informácie priamo od hospodárskych subjektov. Zhromažďuje, integruje, analyzuje a hodnotí informácie z voľne dostupných materiálov, od ostatných verejných orgánov atď.

2. Národná policajná agentúra/prefektúrna polícia

V každej prefektúre je prefektúrna polícia oprávnená zhromažďovať informácie v rámci svojej právomoci podľa článku 2 zákona o polícii. Môže sa stať, že informácie v rámci svojej právomoci na základe zákona o polícii zhromažďuje priamo Národná policajná agentúra. Týka sa to najmä činností bezpečnostného úradu Národnej policajnej agentúry a jej oddelenia pre zahraničné veci a spravodajské služby. V súlade s článkom 24 zákona o polícii je bezpečnostný úrad zodpovedný za záležitosti týkajúce sa bezpečnostnej polície⁽³⁰⁾ a oddelenie pre zahraničné veci a spravodajské služby zodpovedá za záležitosti týkajúce sa cudzích štátnych príslušníkov, ako aj japonských štátnych príslušníkov, ktorí majú sídlo činnosti v zahraničí.

3. Spravodajská služba pre verejnú bezpečnosť (PSIA)

Uplatňovanie zákona o predchádzaní podvratnej činnosti (ďalej len „zákon SAPA“) a zákona o kontrole organizácií, ktoré sa dopustili plošnej masovej vraždy (ďalej len „zákon ACO“) patrí hlavne do právomoci Spravodajskej služby pre verejnú bezpečnosť (PSIA). Ide o orgán ministerstva spravodlivosti.

V zákonoch SAPA a ACO sa stanovuje, že za prísnych podmienok môžu byť prijaté správne dispozície proti organizáciám, ktoré sa dopustili určitých závažných činov („teroristická podvratná činnosť“ alebo „skutok plošnej masovej vraždy“), ktoré sú podľa ústavy v rozpore s „verejnou bezpečnosťou“ alebo „základným spoločenským systémom“ (t. j. opatrenia, ktorými sa nariaďuje obmedzenie činností takýchto organizácií, ich zrušenie atď.). „Teroristická podvratná činnosť“ patrí do rozsahu pôsobnosti zákona SAPA (pozri článok 4 týkajúci sa činov, ako je povstanie, nábádanie na zahraničnú agresiu, vražda s politickým úmyslom atď.), zatiaľ čo zákon ACO sa vzťahuje na „skutky plošnej masovej vraždy“ (pozri článok 4 zákona ACO). Predmetom dispozícií prijatých podľa zákonov SAPA a ACO môžu byť len presne identifikované organizácie predstavujúce osobitnú vnútornú či vonkajšiu hrozbu pre verejnú bezpečnosť.

Na tento účel sa v zákonoch SAPA a ACO stanovuje zákonná vyšetrovacia právomoc. Základné vyšetrovacie právomoci úradníkov Spravodajskej služby pre verejnú bezpečnosť sú stanovené v článku 27 zákona SAPA a článku 29 zákona ACO. Vyšetrovania PSIA vykonávané podľa týchto ustanovení prebiehajú v rozsahu, v akom sú potrebné vzhľadom na uvedené dispozície na kontrolu organizácií (ako príklad organizácií, ktoré boli v minulosti predmetom vyšetrovania, možno uviesť radikálne ľavicové skupiny, sektu Óm širikjó a určité domáce skupiny úzko prepojené so Severnou Kóreou). V rámci týchto vyšetrovaní sa však nemožno spoliehať na povinné prostriedky, a preto nemôžu byť organizácie, ktoré disponujú osobnými informáciami, nútené poskytnúť takéto informácie.

Na zhromažďovanie a používanie informácií dobrovoľne sprístupnených PSIA sa vzťahujú príslušné zákonom stanovené záruky a obmedzenia, ako sú, okrem iného, dôverný charakter komunikácie zaručený ústavou či pravidlá týkajúce sa nakladania s osobnými informáciami stanovené v zákone APPIHAO.

4. Ministerstvo obrany

Pokiaľ ide o zhromažďovanie informácií ministerstvom obrany, toto ministerstvo zhromažďuje informácie na základe článkov 3 a 4 zákona o zriadení ministerstva obrany v rozsahu potrebnom na výkon jeho správnych právomocí, a to aj vo vzťahu k obrane a ochrane, akciám uskutočňovaným obrannými silami, ako aj vysielaniu pozemných, námorných a leteckých ozbrojených síl. Ministerstvo obrany môže zhromažďovať informácie na tieto účely len na základe dobrovoľnej spolupráce a z voľne dostupných zdrojov. Nezhromažďuje informácie o širokej verejnosti.

2) Obmedzenia a záruky

a) Zákonné obmedzenia

1. Všeobecné obmedzenia vyplývajúce zo zákona APPIHAO

Zákon APPIHAO je všeobecný zákon, ktorý sa uplatňuje na zhromažďovanie osobných informácií a ich spracúvanie správnymi orgánmi v akejkoľvek oblasti činnosti týchto orgánov. Preto sa obmedzenia a záruky opísané v oddiele II.A.1 písm. b) bode 2 uplatňujú aj na uchovávanie, ukladanie, používanie atď. osobných informácií v oblasti národnej bezpečnosti.

⁽²⁸⁾ Tieto činnosti vykonáva Spravodajská a vyšetrovacia služba vlády na základe článku 4 organizačného poriadku sekretariátu vlády.

⁽²⁹⁾ Zahŕňa to „zhromažďovanie a vyhľadávanie spravodajských informácií týkajúcich sa dôležitých politík vlády“.

⁽³⁰⁾ Bezpečnostná polícia je zodpovedná za boj proti trestnej činnosti vo vzťahu k verejnej bezpečnosti a v národnom záujme. To zahŕňa boj proti trestnej činnosti a zhromažďovanie informácií o nezákonných činoch vo vzťahu k extrémne ľavicovým skupinám, pravicovým skupinám a škodlivým činnostiam zameraným proti Japonsku.

2. Osobitné obmedzenia uplatniteľné na políciu (Národnú policajnú agentúru i prefektúrne políciu)

Ako je uvedené vyššie v oddiele o zhromažďovaní informácií na účely presadzovania práva, polícia môže zhromažďovať informácie len v rámci svojej právomoci, pričom môže v súlade s článkom 2 ods. 2 zákona o polícii konať len v rozsahu „prísne obmedzenom“ na plnenie jej úloh a „nestranne, nezaujato, nepredpojato a spravodlivo“. Jej právomoci okrem toho „nikdy nesmú byť zneužitie akýmkoľvek spôsobom, ktorý by zasahoval do práv a slobôd fyzickej osoby zaručených Ústavou Japonska“.

3. Osobitné obmedzenia uplatniteľné na PSIA

V článku 3 zákona SAPA a článku 3 zákona ACO sa stanovuje, že vyšetrovania vykonávané podľa týchto zákonov sa vedú iba v minimálnom rozsahu nevyhnutnom na dosiahnutie sledovaného účelu a nesmú sa vykonávať tak, aby nepriemerane obmedzovali základné ľudské práva. Okrem toho sa v článku 45 zákona SAPA a článku 42 zákona ACO stanovuje, že ak príslušník PSIA zneužije svoju právomoc, dopustí sa trestného činu, za ktorý možno uložiť prísnejšie trestné sankcie než za „všeobecné“ zneužitie právomoci v iných oblastiach verejného sektora.

4. Osobitné obmedzenia uplatniteľné na ministerstvo obrany

Pokiaľ ide o zhromažďovanie/organizáciu informácií na ministerstve obrany, ako sa uvádza v článku 4 zákona o zriadení ministerstva obrany, táto činnosť ministerstva je obmedzená na to, čo je „nevyhnutné“ na plnenie jeho úloh v súvislosti s 1) obranou a ochranou, 2) akciami uskutočňovanými obrannými silami a 3) organizáciou, počtom zamestnancov, štruktúrou, vybavením a vysielaním pozemných, námorných a leteckých ozbrojených síl.

b) Iné obmedzenia

Ako je vysvetlené v oddiele II.A.2 písm. b) bode 1 o vyšetrovaniach trestnej činnosti, z judikatúry najvyššieho súdu vyplýva, že na to, aby orgány mohli hospodárskemu subjektu adresovať žiadosť o dobrovoľnú spoluprácu, musí byť táto žiadosť nevyhnutná na vyšetrovanie podozrenia zo spáchania trestného činu a musí byť primeraná vzhľadom na dosiahnutie účelu daného vyšetrovania.

Hoci sa vyšetrovania, ktoré vykonávajú vyšetrovacie orgány v oblasti národnej bezpečnosti, líšia od vyšetrovaní vedených vyšetrovacími orgánmi v oblasti presadzovania práva, tak pokiaľ ide o ich právny základ, ako aj účel, aj v oblasti národnej bezpečnosti sa podobne uplatňujú hlavné zásady „nevyhnutnosti vyšetrovania“ a „vhodnosti spôsobu“, ktoré treba dodržiavať s náležitým zreteľom na konkrétne okolnosti každého prípadu.

Kombináciou vyššie uvedených obmedzení sa zabezpečuje, že zhromažďovanie a spracúvanie informácií sa uskutočňuje iba v rozsahu nevyhnutnom na plnenie konkrétnych úloh príslušného orgánu verejnej moci, ako aj na základe konkrétnych hrozieb. Tým je vylúčené plošné a nerozlišujúce zhromažďovanie osobných informácií alebo prístup k nim z dôvodov národnej bezpečnosti.

B. Dohľad

1. Dohľad na základe zákona APPIHAO

Ako je vysvetlené vyššie v oddiele II.B.2, v japonskom verejnom sektore je každý minister alebo vedúci každého ministerstva či orgánu oprávnený kontrolovať a presadzovať dodržiavanie zákona APPIHAO v rámci svojho ministerstva/orgánu. Minister vnútra a komunikácií môže okrem toho prešetriť stav presadzovania zákona, požiadať každého ministra o predloženie materiálov a poskytnutie vysvetlení na základe článkov 49 a 50 zákona a adresovať stanovisko každému ministrovi na základe článku 51 zákona. Napríklad môže požiadať o revíziu opatrení prostredníctvom krokov uvedených v článkoch 50 a 51 zákona.

2. Dohľad nad políciou vykonávaný komisiami pre verejnú bezpečnosť

Ako je vysvetlené v oddiele II s názvom Zhromažďovanie informácií na účely presadzovania práva v trestných veciach, nezávislé prefektúrne komisie pre verejnú bezpečnosť zabezpečujú dohľad nad činnosťami prefektúrnej polície.

Dohľad nad Národnou policajnou agentúrou vykonáva Národná komisia pre verejnú bezpečnosť. Podľa článku 5 zákona o polícii je táto komisia zodpovedná najmä za „ochranu práv a slobôd fyzických osôb“. Na tento účel najmä zavádza komplexné politiky, v rámci ktorých sa stanovujú pravidlá na spravovanie záležitostí opísaných v každom bode článku 5 ods. 4 zákona o polícii, ako aj iné základné usmernenia či opatrenia, ktoré by sa mali uplatňovať pri vykonávaní daných činností. Národná komisia pre verejnú bezpečnosť má rovnaký stupeň nezávislosti ako prefektúrne komisie pre verejnú bezpečnosť.

3. Dohľad nad ministerstvom obrany, ktorý vykonáva Úrad generálneho inšpektora pre dodržiavanie právnych predpisov

Úrad generálneho inšpektora pre dodržiavanie právnych predpisov (ďalej len „IGO“) je nezávislým útvarom ministerstva obrany, ktorý na základe článku 29 zákona o zriadení ministerstva obrany pôsobí pod priamym dohľadom ministra obrany. IGO môže kontrolovať dodržiavanie zákonov a iných právnych predpisov úradníkmi ministerstva obrany. Tieto kontroly sa nazývajú „inšpekcie obrany“.

IGO vykonáva inšpekcie ako nezávislý útvar s cieľom zabezpečiť dodržiavanie právnych predpisov na celom ministerstve vrátane obranných síl. Svoje úlohy plní nezávisle od prevádzkových útvarov ministerstva obrany. Bezodkladne po inšpekcii predkladá svoje zistenia priamo ministrovi obrany spolu s nevyhnutnými opatreniami na zlepšenie. Na základe správy IGO môže minister obrany nariadiť vykonanie opatrení nevyhnutných na nápravu situácie. Za vykonávanie týchto opatrení zodpovedá zástupca námestníka ministra obrany, ktorý musí podať ministrovi obrany správu o stave ich vykonávania.

V rámci dobrovoľného opatrenia na zaistenie transparentnosti sa zistenia z inšpekcí obrany teraz uverejňujú na webovom sídle ministerstva obrany (hoci to zákon nevyžaduje).

Existujú tri kategórie inšpekcí obrany:

- i) pravidelné inšpekcie obrany, ktoré sa vykonávajú v pravidelných intervaloch ⁽³¹⁾;
- ii) inšpekcie obrany na účel kontrol, ktoré sa vykonávajú s cieľom overiť, či sa skutočne prijali opatrenia na zlepšenie; a
- iii) osobitné inšpekcie obrany, ktorých vykonanie nariaďuje minister obrany v súvislosti s konkrétnymi záležitosťami.

V rámci týchto inšpekcí môže generálny inšpektor požiadať o vypracovanie správ na príslušných útvaroch, požiadať o predloženie dokumentov, vstupovať do príslušných priestorov s cieľom vykonať inšpekciu, požiadať zástupcu námestníka obrany o vysvetlenia atď. Vzhľadom na povahu inšpekčných úloh IGO vedú tento úrad veľmi skúsení právni experti (bývalý dozorný prokurátor).

4. Dohľad v rámci PSIA

PSIA vykonáva pravidelné aj osobitné inšpekcie operácií svojich jednotlivých úradov a útvarov (Úrad Spravodajskej služby pre verejnú bezpečnosť, útvary a podútvary Spravodajskej služby pre verejnú bezpečnosť atď.). Na účely pravidelnej inšpekcie je ako inšpektor určený zástupca generálneho riaditeľa a/alebo riaditeľ. Takéto inšpekcie sa tiež týkajú správy osobných informácií.

5. Dohľad, ktorý vykonáva parlament

Pokiaľ ide o zhromažďovanie informácií na účely presadzovania práva, parlament môže prostredníctvom svojho príslušného výboru skúmať zákonnosť zhromažďovania informácií v oblasti národnej bezpečnosti. Vyšetrovacie právomoci parlamentu sú založené na článku 62 ústavy a článkoch 74 a 104 zákona o parlamente.

C. Individuálne prostriedky nápravy

Individuálnu nápravu možno dosiahnuť rovnakými prostriedkami ako v oblasti presadzovania práva v trestných veciach. To zahŕňa aj nový mechanizmus nápravy na vybavovanie a riešenie sťažností podaných fyzickými osobami z EÚ, ktorý spravuje a na ktorý dozerá PPC. V tejto súvislosti sa odkazuje na príslušné pasáže oddielu II.C.

Okrem toho sú v oblasti národnej bezpečnosti k dispozícii osobitné individuálne prostriedky nápravy.

Zhromažďovanie osobných informácií správnym orgánom na účely národnej bezpečnosti podlieha ustanoveniam kapitoly 4 zákona APPIHAO. To zahŕňa právo požiadať o prístup (článok 12), opravu (vrátane doplnenia alebo vymazania) (článok 27) uchovávaných osobných informácií fyzickej osoby, ako aj právo požiadať o ukončenie používania osobných informácií, ak správny orgán získal dané informácie nezákonne (článok 36). V oblasti národnej bezpečnosti však výkon

⁽³¹⁾ Ako príklad možno uviesť inšpekciu v súvislosti s otázkami uvedenými v tomto vyhlásení, pričom možno odkázať na pravidelnú inšpekciu obrany z roku 2016 vykonanú v súvislosti s informovanosťou o dodržiavaní právnych predpisov a prípravou na ich dodržiavanie, keďže ochrana osobných informácií bola jedným z ústredných prvkov tejto inšpekcie. Konkrétnejšie sa inšpekcia týkala stavu správy, uchovávaní atď. osobných informácií. IGO identifikoval vo svojej správe viacero nedostatkov pri správe osobných informácií, ktoré by sa mali napraviť, ako je napríklad absencia ochrany údajov pomocou hesla. Správa je dostupná na webovom sídle ministerstva obrany.

týchto práv podlieha určitým obmedzeniam: žiadostiam o sprístupnenie, opravu alebo ukončenie používania informácií sa nevyhoví, pokiaľ sa týkajú „informácií, v súvislosti s ktorými existujú podľa vedúceho správneho orgánu opodstatnené dôvody konštatovať, že ich sprístupnenie by pravdepodobne viedlo k ohrozeniu národnej bezpečnosti, poškodeniu vzťahu s inou krajinou či medzinárodnou organizáciou založeného na vzájomnej dôvere alebo znevýhodneniu pri rokovaní s inou krajinou či medzinárodnou organizáciou“ [článok 14 písm. iv)]. Táto výnimka sa teda nevzťahuje na každý prípad dobrovoľného zhromažďovania informácií v oblasti národnej bezpečnosti, keďže v súvislosti s jej prípadným uplatnením sa vždy vyžaduje konkrétne posúdenie rizík vyplývajúcich zo sprístupnenia informácií.

Okrem toho, ak sa žiadosť fyzickej osoby zamietne s odôvodnením, že príslušné informácie nemožno sprístupniť v zmysle článku 14 písm. iv), daná osoba môže podať správne odvolanie a v rámci neho požiadať o preskúmanie tohto rozhodnutia, pričom môže napríklad tvrdiť, že v predmetnej veci nie sú splnené podmienky stanovené v článku 14 písm. iv). V takom prípade vedúci príslušného správneho orgánu pred prijatím rozhodnutia konzultuje s Radou pre preskúmanie sprístupňovania informácií a ochrany osobných informácií. Táto rada vykoná nezávislé preskúmanie odvolania. Ide o vysoko špecializovanú a nezávislú radu, ktorej členov menuje spomedzi popredných odborníkov predseda vlády so súhlasom oboch snemovní parlamentu⁽³²⁾. Rada disponuje rozsiahlymi vyšetrovacími právomocami vrátane možnosti požiadať o dokumenty a sprístupnenie predmetných osobných informácií, usporiadať rokovanie za zatvorenými dverami a uplatniť tzv. postup Vaughnovho indexu⁽³³⁾. Rada následne vypracuje písomnú správu, ktorú zašle danej osobe⁽³⁴⁾. Zistenia obsiahnuté v tejto správe sa zverejňujú. Hoci správa nie je z formálneho hľadiska právne záväzná, odporúčania v nej uvedené príslušné správne orgány takmer vždy dodržia⁽³⁵⁾.

A napokon, fyzická osoba má v súlade s článkom 3 ods. 3 Správneho súdneho poriadku možnosť podať žalobu na súd s cieľom domáhať sa zrušenia rozhodnutia správneho orgánu o nesprístupnení osobných informácií.

IV. Pravidelné preskúmanie

V rámci pravidelného preskúmania rozhodnutia o primeranosti si PPC a Európska komisia vymenia informácie o spracúvaní údajov za podmienok záveru o primeranosti vrátane podmienok uvedených v tomto vyhlásení.

⁽³²⁾ Pozri článok 4 zákona o zriadení Rady pre preskúmanie sprístupňovania informácií a ochrany osobných informácií.

⁽³³⁾ Pozri článok 9 zákona o zriadení Rady pre preskúmanie sprístupňovania informácií a ochrany osobných informácií.

⁽³⁴⁾ Pozri článok 16 zákona o zriadení Rady pre preskúmanie sprístupňovania informácií a ochrany osobných informácií.

⁽³⁵⁾ Za posledné 3 roky nedošlo k situácii, keď by príslušný správny orgán prijal rozhodnutie, ktoré sa líšilo od záverov Rady. Predtým k tomu došlo len vo veľmi malom počte prípadov: len v dvoch z celkovo 2 000 prípadov od roku 2005 (rok, keď zákon APPIHAO nadobudol účinnosť). Keď správny orgán dospeje k záveru/prijme rozhodnutie, ktorý(-é) sa odlišuje od záverov rady, musí v súlade s článkom 50 ods. 1 bodom 4 zákona o preskúmaní sťažností v správnych veciach v spojení s náhradou článku 42 ods. 2 zákona APPIHAO, jasne uviesť dôvody, pre ktoré tak urobil.