

II

(Nelegislativní akty)

ROZHODNUTÍ

PROVÁDĚCÍ ROZHODNUTÍ KOMISE (EU) 2019/419

ze dne 23. ledna 2019

podle nařízení Evropského parlamentu a Rady (EU) 2016/679 o odpovídající ochraně osobních údajů poskytované Japonskem na základě zákona o ochraně osobních informací

(oznámeno pod číslem K(2019) 304)

(Text s významem pro EHP)

EVROPSKÁ KOMISE,

s ohledem na Smlouvu o fungování Evropské unie,

s ohledem na nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů) ⁽¹⁾ („GDPR“), a zejména na čl. 45 odst. 3 uvedeného nařízení,

po konzultaci s evropským inspektorem ochrany údajů,

1. ÚVOD

- (1) Nařízení (EU) 2016/679 stanoví pravidla pro předávání osobních údajů správci nebo zpracovateli v Evropské unii do třetích zemí a mezinárodním organizacím, pokud toto předávání spadá do oblasti působnosti uvedeného nařízení. Pravidla pro mezinárodní předávání osobních údajů stanoví kapitola V uvedeného nařízení, a konkrétně články 44 až 50. Tok osobních údajů do zemí mimo Evropskou unii a z těchto zemí je nezbytný pro rozšiřování mezinárodní spolupráce a mezinárodního obchodu, a současně zaručit, aby nebyla oslabena úroveň ochrany poskytovaná osobním údajům v Evropské unii.
- (2) Podle čl. 45 odst. 3 nařízení (EU) 2016/679 může Komise prostřednictvím prováděcího aktu rozhodnout, že určitá třetí země, určité území či jedno nebo více konkrétních odvětví v určité třetí zemi nebo určitá mezinárodní organizace zajišťuje odpovídající úroveň ochrany. Za této podmínky lze osobní údaje do této třetí země, na toto území, do tohoto odvětví nebo této mezinárodní organizaci předat bez potřeby získat další povolení podle čl. 45 odst. 1 a 103. bodu odůvodnění uvedeného nařízení.
- (3) Podle čl. 45 odst. 2 nařízení (EU) 2016/679 musí přijetí rozhodnutí o odpovídající ochraně vycházet z komplexní analýzy právního řádu dané třetí země, a to jak z hlediska pravidel použitelných pro dovozce údajů, tak z hlediska omezení a záruk vztahujících se k přístupu orgánů veřejné moci k osobním údajům. Posouzení musí určit, zda daná třetí země zaručí úroveň ochrany „v zásadě rovnocennou“ úrovni ochrany zajištěné v Evropské unii (104. bod odůvodnění nařízení (EU) 2016/679). Jak objasnil Soudní dvůr Evropské unie, nevyžaduje to stejnou úroveň ochrany ⁽²⁾. Zejména prostředky, které dotyčná třetí země využívá, se mohou lišit od prostředků zavedených v Evropské unii, pokud se v praxi ukážou jako účinné k zajištění odpovídající úrovně ochrany ⁽³⁾. Standard

⁽¹⁾ Úř. věst. L 119, 4.5.2016, s. 1.

⁽²⁾ Rozsudek Soudního dvora ve věci *Maximillian Schrems v. Data Protection Commissioner* (dále jen „rozsudek ve věci Schrems“), C-362/14, ECLI:EU:C:2015:650, bod 73.

⁽³⁾ Rozsudek ve věci *Schrems*, bod 74.

odpovídající ochrany tedy nevyžaduje opakování pravidel Unie slovo od slova. Kritériem je spíše to, zda zahraniční systém jako celek zajišťuje prostřednictvím podstaty práva na soukromí a jeho účinného uplatňování, dozoru a vymáhání požadovanou úroveň ochrany ⁽⁴⁾.

- (4) Komise pečlivě analyzovala japonské právní předpisy a praxi. Na základě zjištění uvedených v 6. až 175. bodě odůvodnění dospěla Komise k závěru, že Japonsko zajišťuje odpovídající úroveň ochrany osobních údajů předáváním organizacím, které spadají do oblasti působnosti zákona o ochraně osobních informací ⁽⁵⁾ a které podléhají dalším podmínkám uvedeným v tomto rozhodnutí. Tyto podmínky jsou stanoveny v doplňkových pravidlech (příloha I) přijatých Komisí pro ochranu osobních informací ⁽⁶⁾ a v oficiálních prohlášeních, ujištěních a závazcích japonské vlády pro Evropskou komisi (příloha II).
- (5) Toto rozhodnutí má účinek v tom smyslu, že předávání údajů od správce nebo zpracovatele v Evropském hospodářském prostoru (EHP) ⁽⁷⁾ takovým organizacím v Japonsku může probíhat bez potřeby získat další povolení. Tímto rozhodnutím není dotčeno přímé uplatňování nařízení (EU) 2016/679 na tyto organizace, pokud jsou splněny podmínky jeho článku 3.

2. PRAVIDLA TÝKAJÍCÍ SE ZPRACOVÁNÍ ÚDAJŮ PODNIKATELSKÝMI SUBJEKTY

2.1 Japonský rámec ochrany údajů

- (6) Právní systém upravující ochranu soukromí a údajů v Japonsku se opírá o Ústavu vyhlášenou v roce 1946.
- (7) Článek 13 Ústavy stanoví:

„Všichni lidé jsou respektováni jako jednotlivci. Jejich právo na život, svobodu a usilování o štěstí, pokud nenarušuje veřejné blaho, je nejvýznamnějším kritériem v zákonodárství a jiných záležitostech státu.“

- (8) Na základě tohoto článku japonský Nejvyšší soud objasnil práva fyzických osob, pokud jde o ochranu osobních informací. V rozhodnutí z roku 1969 uznal Nejvyšší soud právo na soukromí a ochranu údajů jako ústavní právo ⁽⁸⁾. Soud zejména konstatoval, že „každý může svobodně chránit své osobní informace před bezdůvodným zpřístupněním třetí straně nebo zveřejněním“. Kromě toho v rozsudku ze dne 6. března 2008 (dále jen „rozsudek ve věci Juki-Net“) ⁽⁹⁾ Nejvyšší soud konstatoval, že „svoboda občanů v soukromém životě je chráněna před výkonem veřejné moci a lze mít za to, že jednou ze svobod jednotlivce v soukromém životě je, že každý může svobodně chránit své osobní informace před bezdůvodným zpřístupněním třetí straně nebo zveřejněním“ ⁽¹⁰⁾.
- (9) Dne 30. května 2003 Japonsko schválilo řadu právních předpisů v oblasti ochrany údajů:

— zákon o ochraně osobních informací,

— zákon o ochraně osobních informací uchovávaných správními orgány,

— zákon o ochraně osobních informací uchovávaných registrovanými správními agenturami (APPI-IAA).

⁽⁴⁾ Viz sdělení Komise Evropskému parlamentu a Radě, Výměna a ochrana osobních údajů v globalizovaném světě, COM (2017)7, 10.1.2017, oddíl 3.1, s. 6–7.

⁽⁵⁾ Zákon o ochraně osobních informací (zákon č. 57 z roku 2003).

⁽⁶⁾ Více informací o Komisi pro ochranu osobních informací je k dispozici na této adrese: <https://www.ppc.go.jp/en/contactus/access/>.

⁽⁷⁾ Toto rozhodnutí má význam pro EHP. Dohoda o Evropském hospodářském prostoru (Dohoda o EHP) rozšiřuje vnitřní trh Evropské unie na tři státy EHP, a to Island, Lichtenštejnsko a Norsko. Rozhodnutí Smíšeného výboru, kterým se do přílohy XI Dohody o EHP začleňuje nařízení (EU) 2016/679, přijal Smíšený výbor EHP dne 6. července 2018 a v platnost vstoupilo dne 20. července 2018. Uvedená dohoda se tedy na nařízení vztahuje.

⁽⁸⁾ Rozsudek Nejvyššího soudu (velkého senátu) ze dne 24. prosince 1969, Keishu, sv. 23, č. 12, s. 1625.

⁽⁹⁾ Rozsudek Nejvyššího soudu ze dne 6. března 2008, Minshu, sv. 62, č. 3, s. 665.

⁽¹⁰⁾ Rozsudek Nejvyššího soudu ze dne 6. března 2008, Minshu, sv. 62, č. 3, s. 665.

- (10) Poslední dva uvedené zákony (novelizované v roce 2016) obsahují ustanovení použitelná pro ochranu osobních informací subjekty veřejného sektoru. Zpracování údajů spadající do oblasti působnosti těchto zákonů není předmětem zjištění o odpovídající úrovni ochrany obsaženého v tomto rozhodnutí, které se omezuje na ochranu osobních informací „podnikatelskými subjekty nakládajícími s osobními informacemi“ ve smyslu zákona o ochraně osobních informací.
- (11) Zákon o ochraně osobních informací byl v posledních letech reformován. Novelizovaný zákon o ochraně osobních informací byl vyhlášen dne 9. září 2015 a nabyl účinnosti dne 30. května 2017. Novela zavedla řadu nových záruk a rovněž posílila stávající záruky, čímž japonský systém ochrany údajů přiblížila evropskému systému. To zahrnuje například soubor vymahatelných individuálních práv nebo zřízení nezávislého dozorového úřadu (Komise pro ochranu osobních informací) pověřeného dozorem nad zákonem o ochraně osobních informací a jeho prosazováním.
- (12) Kromě zákona o ochraně osobních informací podléhá zpracování osobních informací spadajících do oblasti působnosti tohoto rozhodnutí prováděcím pravidlům vydaným na základě zákona o ochraně osobních informací. Zahrnuje to novelu nařízení kabinetu o prosazování zákona o ochraně osobních informací ze dne 5. října 2016 a tzv. pravidla prosazování zákona o ochraně osobních informací přijatá Komisí pro ochranu osobních informací⁽¹¹⁾. Oba soubory pravidel jsou právně závazné a vymahatelné a nabyly účinnosti ve stejnou dobu jako novelizovaný zákon o ochraně osobních informací.
- (13) Kromě toho dne 28. října 2016 japonský kabinet (sestavající z premiéra a ministrů, kteří tvoří jeho vládu) vydal „základní politiku“ s cílem „komplexně a uceleně podpořit opatření týkající se ochrany osobních informací“. Podle článku 7 zákona o ochraně osobních informací se „základní politika“ vydává v podobě rozhodnutí kabinetu a zahrnuje směry politiky týkající se prosazování zákona o ochraně osobních informací určené ústředním a místním vládním institucím.
- (14) Rozhodnutím kabinetu ze dne 12. června 2018 japonská vláda „základní politiku“ nedávno pozměnila. Za účelem usnadnění mezinárodního předávání údajů uvedené rozhodnutí kabinetu přenáší na Komisi pro ochranu osobních informací jakožto orgán příslušný spravovat a provádět zákon o ochraně osobních informací „pravomoc přijímat nezbytná opatření k překlenutí rozdílů mezi systémy a operacemi Japonska a dotyčné cizí země na základě článku 6 zákona s cílem zajistit vhodné nakládání s osobními informacemi přijatými z takové země“. Rozhodnutí kabinetu stanoví, že to zahrnuje pravomoc zavést zesílené ochrany tím, že Komise pro ochranu osobních informací přijme přísnější pravidla, která doplní a zpřísní pravidla stanovená v zákoně o ochraně osobních informací a nařízení kabinetu. Podle uvedeného rozhodnutí budou tato přísnější pravidla pro japonské podnikatelské subjekty závazná a vymahatelná.
- (15) Na základě článku 6 zákona o ochraně osobních informací a uvedeného rozhodnutí kabinetu přijala Komise pro ochranu osobních informací dne 15. června 2018 „doplňková pravidla podle zákona o ochraně osobních informací pro nakládání s osobními údaji předávanými z EU na základě rozhodnutí o odpovídající ochraně“ (dále jen „doplňková pravidla“) s cílem posílit ochranu osobních informací předávaných z Evropské unie do Japonska na základě tohoto rozhodnutí o odpovídající ochraně. Tato doplňková pravidla jsou pro japonské podnikatelské subjekty právně závazná a vymahatelná, a to jak ze strany Komise pro ochranu osobních informací, tak ze strany soudů, stejně jako ustanovení zákona o ochraně osobních informací, která doplňují přísnějšími a/nebo podrobnějšími pravidly⁽¹²⁾. Jelikož japonské podnikatelské subjekty získávající a/nebo dále zpracovávající osobní údaje z Evropské unie budou mít zákonnou povinnost doplňková pravidla dodržovat, budou muset zajistit (např. technickými prostředky („označováním“) nebo organizačními prostředky (ukládáním ve vyhrazené databázi)), že jsou schopny takového osobní údaje identifikovat po celou dobu jejich „životního cyklu“⁽¹³⁾. V následujících oddílech je analyzován obsah každého doplňkového pravidla v rámci posouzení článků zákona o ochraně osobních informací, které dané pravidlo doplňuje.
- (16) Na rozdíl od novely z roku 2015, kdy toto spadalo do působnosti různých japonských ministerstev v jednotlivých odvětvích, zákon o ochraně osobních informací zmocňuje Komisi pro ochranu osobních informací k přijetí „pokynů“ „s cílem zajistit, aby opatření, které má určitý podnikatelský subjekt“ podle pravidel ochrany osobních údajů „přijmout, bylo provedeno řádně a účinně“. Prostřednictvím svých pokynů Komise pro ochranu osobních

⁽¹¹⁾ K dispozici na internetových stránkách (https://www.ppc.go.jp/files/pdf/PPC_rules.pdf)

⁽¹²⁾ Viz doplňková pravidla, (úvodní oddíl).

⁽¹³⁾ To není zpochybněno obecným požadavkem na uchovávání záznamů (pouze) po určitou dobu. Ačkoli původ údajů patří mezi informace, které musí přijímající podnikatelský subjekt nakládající s osobními informacemi potvrdit podle čl. 26 odst. 1 zákona o ochraně osobních informací, požadavek podle čl. 26 odst. 4 zákona o ochraně osobních informací ve spojení s článkem 18 pravidel Komise pro ochranu osobních informací se týká pouze určité podoby záznamu (viz článek 16 pravidel Komise pro ochranu osobních informací) a nebrání podnikatelskému subjektu nakládajícímu s osobními informacemi, aby zajistil identifikaci údajů po delší dobu. To potvrdila Komise pro ochranu osobních informací, která uvedla, že „[i]nformace o původu údajů z EU musí podnikatelský subjekt nakládající s osobními informacemi uchovávat tak dlouho, jak je nezbytné pro dodržení doplňkových pravidel“.

informací poskytuje závazný výklad těchto pravidel, a zejména zákona o ochraně osobních informací. Podle informací obdržených od Komise pro ochranu osobních informací tvoří tyto pokyny nedílnou součást právního rámce a mají být vykládány ve spojení s textem zákona o ochraně osobních informací, nařízení kabinetu, pravidel Komise pro ochranu osobních informací a souboru otázek a odpovědí⁽¹⁴⁾ vypracovaného Komisí pro ochranu osobních informací. Jsou proto „závazné pro podnikatelské subjekty“. Pokud pokyny uvádějí, že podnikatelský subjekt „musí“ nebo „by neměl“ jednat určitým způsobem, Komise pro ochranu osobních informací bude mít za to, že nedodržení příslušných ustanovení představuje porušení zákona⁽¹⁵⁾.

2.2 Věcná a osobní působnost

- (17) Oblast působnosti zákona o ochraně osobních informací je dána definovanými koncepty osobních informací, osobních údajů a podnikatelského subjektu nakládajícího s osobními informacemi. Souběžně zákon o ochraně osobních informací stanoví některé důležité výjimky z této oblasti působnosti, zejména pro anonymně zpracovávané osobní údaje a pro konkrétní typy zpracování určitými subjekty. Zákon o ochraně osobních informací sice nepoužívá pojem „zpracování“, vychází však z rovnocenného konceptu „nakládání“, který podle informací obdržených od Komise pro ochranu osobních informací zahrnuje „jakékoli zacházení s osobními údaji“ včetně získání, vstupu, shromáždění, uspořádání, uložení, úpravy/zpracování, obnovení, výmazu, výstupu, použití nebo poskytnutí osobních informací.

2.2.1 Definice osobních informací

- (18) Zprv, pokud jde o věcnou působnost, zákon o ochraně osobních informací odlišuje osobní informace od osobních údajů a na kategorii osobních informací se vztahují pouze určitá ustanovení zákona. Podle čl. 2 odst. 1 zákona o ochraně osobních informací koncept „osobních informací“ zahrnuje jakékoli informace týkající se žijící fyzické osoby, které umožňují tuto osobu identifikovat. Definice rozlišuje dvě kategorie osobních informací: i) individuální identifikační kódy a ii) jiné osobní informace, jejichž pomocí lze identifikovat konkrétní fyzickou osobu. Druhá kategorie zahrnuje rovněž informace, které samy o sobě identifikaci neumožňují, ale pokud jsou „snadno propojitelné“ s jinými informacemi, identifikaci konkrétní fyzické osoby umožňují. Podle pokynů Komise pro ochranu osobních informací⁽¹⁶⁾ se skutečnost, zda lze informace považovat za „snadno propojitelné“, posuzuje individuálně s přihlédnutím ke skutečné situaci („stavu“) podnikatelského subjektu. To bude předpokládáno, pokud propojení je (nebo může být) provedeno průměrným („běžným“) podnikatelským subjektem používajícím prostředky, které má tento subjekt k dispozici. Například informace nejsou „snadno propojitelné“ s jinými informacemi, pokud podnikatelský subjekt musí vyvinout neobvyklé úsilí nebo se dopustit protiprávního jednání, aby získal informace, které mají být propojeny, od jednoho nebo více jiných podnikatelských subjektů.

2.2.2 Definice osobních údajů

- (19) Pod pojem „osobní údaje“ spadají podle zákona o ochraně osobních informací pouze určité formy osobních informací. „Osobní údaje“ jsou vymezeny jako „osobní informace tvořící databázi osobních informací“, tj. „kolektivní soubor informací“ zahrnující osobní informace „systematicky uspořádané tak, aby umožňovaly vyhledávání konkrétních osobních informací za použití počítače“⁽¹⁷⁾ nebo „určené nařízením kabinetu jako systematicky uspořádané tak, aby umožňovaly snadné vyhledávání konkrétních osobních informací“, avšak „s výjimkou informací určených nařízením kabinetu jako informace, u nichž existuje omezená možnost zásahu do individuálních práv a zájmů s ohledem na metodu jejich využití“⁽¹⁸⁾.
- (20) Tato výjimka je dále specifikována v čl. 3 odst. 1 nařízení kabinetu, podle kterého musí být splněny tyto tři kumulativní podmínky: i) kolektivní soubor informací musel být „vydán pro účely prodeje velkému množství neurčených osob a jeho vydání nebylo v rozporu s ustanoveními zákona nebo nařízení z něj vycházejícího“; ii) musí umožňovat „zakoupení velkým množstvím neurčených osob, a to kdykoliv“ a iii) osobní údaje v tomto

⁽¹⁴⁾ Komise pro ochranu osobních informací, Otázky a odpovědi, 16. února 2017 (pozměněné dne 30. května 2017), k dispozici na internetových stránkách <https://www.ppc.go.jp/files/pdf/koujouhouQA.pdf>. Otázky a odpovědi se zabývají řadou záležitostí, které řeší pokyny, poskytnutím praktických příkladů, jako například co představuje citlivé osobní údaje, výklad individuálního souhlasu, předávání třetím stranám v kontextu cloud computingu nebo povinnost uchovávání záznamů vztahující se na přeshraniční předávání. Otázky a odpovědi jsou k dispozici pouze v japonštině.

⁽¹⁵⁾ V návaznosti na konkrétní dotaz Komise pro ochranu osobních informací informovala Evropský sbor pro ochranu osobních údajů, že „japonské soudy při aplikaci zákona o ochraně osobních informací / pravidel Komise pro ochranu osobních informací v jednotlivých případech, které řeší, zakládají [svůj] výklad na pokynech, a ve svých rozsudcích se tak přímo odvolávají na text pokynů Komise pro ochranu osobních informací. Pokyny Komise pro ochranu osobních informací jsou tedy pro podnikatelské subjekty závazné i z tohoto pohledu. Komise pro ochranu osobních informací si není vědoma, že by se soud někdy od pokynů odchýlil.“ V tomto ohledu Komise pro ochranu osobních informací odkázala Komisi na rozsudek ve věci ochrany údajů, v němž soud při svých zjištěních výslovně vycházel z pokynů (viz rozsudek Okresního soudu v Ósace ze dne 19. května 2006, Hanrei Jiho, sv. 1948, s. 122, v němž soud konstatoval, že podnikatelský subjekt měl na základě těchto pokynů povinnost přijmout opatření bezpečnostní kontroly).

⁽¹⁶⁾ Pokyny Komise pro ochranu osobních informací (General Rule Edition), s. 6.

⁽¹⁷⁾ To se vztahuje na veškeré systémy elektronické evidence. Pokyny Komise pro ochranu osobních informací (General Edition, s. 17) poskytují v tomto ohledu konkrétní příklady, například seznam e-mailových adres uložený v softwaru e-mailového klienta.

⁽¹⁸⁾ Ustanovení čl. 2 odst. 4 a 6 zákona o ochraně osobních informací.

souboru obsažené musí být „poskytnuty pro jejich původní účel bez doplňování jiných informací souvisejících s žijící osobou“. Podle vysvětlení obdržенých od Komise pro ochranu osobních informací byla tato úzce vymezená výjimka zavedena s cílem vyloučit telefonní seznamy nebo obdobné typy seznamů.

- (21) Pokud jde o údaje shromažďované v Japonsku, je toto rozlišení mezi „osobními informacemi“ a „osobními údaji“ relevantní, protože takové informace nemusí být vždy součástí „databáze osobních informací“ (například jednotný soubor údajů shromážděných a zpracovaných ručně), a proto se daná ustanovení zákona o ochraně osobních informací, která se vztahují pouze k osobním údajům, nepoužijí⁽¹⁹⁾.
- (22) Toto rozlišení naopak nebude relevantní pro osobní údaje dovážené z Evropské unie do Japonska na základě rozhodnutí o odpovídající ochraně. Jelikož budou takové údaje obvykle předávány elektronickými prostředky (vzhledem k tomu, že v digitální době je to obvyklý způsob výměny údajů, zejména na dlouhé vzdálenosti mezi EU a Japonskem), a stanou se tedy součástí elektronické evidence dovozce údajů, takovéto údaje z EU budou spadat do kategorie „osobních údajů“ podle zákona o ochraně osobních informací. Pokud by ve výjimečném případě byly osobní údaje předávány z EU jinými prostředky (např. v papírové podobě), bude se na ně zákon o ochraně osobních informací vztahovat, jestliže se po předání stanou součástí „kolektivního souboru informací“ systematicky uspořádaného tak, aby umožňoval snadné vyhledávání konkrétních informací (čl. 2 odst. 4 bod ii) zákona o ochraně osobních informací). Podle čl. 3 odst. 2 nařízení kabinetu tento případ nastane, pokud jsou informace uspořádány „podle určitého pravidla“ a databáze zahrnuje nástroje jako například obsah nebo rejstřík pro snazší vyhledávání. To odpovídá definici „evidence“ ve smyslu čl. 2 odst. 1 obecného nařízení o ochraně osobních údajů.

2.2.3 Definice uchovávaných osobních údajů

- (23) Určitá ustanovení zákona o ochraně osobních informací, zejména články 27 až 30 týkající se individuálních práv, se vztahují pouze na určitou kategorii osobních údajů, konkrétně „uchovávané osobní údaje“. Ty jsou vymezeny v čl. 2 odst. 7 zákona o ochraně osobních informací jako osobní údaje jiné než ty, které i) „jsou určeny nařízením kabinetu jako údaje, které pravděpodobně poškodí veřejné nebo jiné zájmy, pokud bude jejich přítomnost nebo absence zveřejněna“, nebo ii) „mají být vymazány ve lhůtě nepřesahující jeden rok, která je stanovena nařízením kabinetu“.
- (24) Pokud jde o první z uvedených dvou kategorií, je vysvětlena v článku 4 nařízení kabinetu a zahrnuje čtyři typy výjimek⁽²⁰⁾. Tyto výjimky mají obdobné cíle, jako jsou cíle uvedené v čl. 23 odst. 1 nařízení (EU) 2016/679, zejména ochranu subjektu údajů (v terminologii zákona o ochraně osobních informací „zmocnitel“) a svobodu druhých, národní bezpečnost, veřejnou bezpečnost, prosazování trestního práva nebo jiné důležité cíle obecného veřejného zájmu. Ze znění čl. 4 odst. 1 bodů i) až iv) nařízení kabinetu navíc vyplývá, že předpokladem jejich uplatnění je vždy konkrétní riziko pro některý z chráněných důležitých zájmů⁽²¹⁾.
- (25) Druhá kategorie je podrobněji specifikována v článku 5 nařízení kabinetu. Ve spojení s čl. 2 odst. 7 zákona o ochraně osobních informací jsou tímto z oblasti působnosti pojmu „uchovávané osobní údaje“, a tedy z individuálních práv podle zákona o ochraně osobních informací, vyloučeny ty osobní údaje, které „mají být vymazány“ ve lhůtě šesti měsíců. Komise pro ochranu osobních informací vysvětlila, že cílem této výjimky je motivovat podnikatelské subjekty, aby údaje uchovávaly a zpracovávaly nejkratší možnou dobu. To by však znamenalo, že subjekty údajů z EU by nemohly využívat důležitých práv pouze z důvodu doby uchovávání jejich údajů dotýčným podnikatelským subjektem.
- (26) Pro vyřešení této situace vyžaduje doplňkové pravidlo 2, aby se s osobními údaji předávanými z Evropské unie „nakládalo jako s uchovávanými osobními údaji ve smyslu čl. 2 odst. 7 zákona bez ohledu na lhůtu, v níž mají být vymazány“. Doba uchovávání nebude mít žádný vliv na práva poskytovaná subjektům údajů z EU.

⁽¹⁹⁾ Například článek 23 zákona o ochraně osobních informací týkající se podmínek pro sdílení osobních údajů se třetími stranami.

⁽²⁰⁾ Konkrétně osobní údaje, i) „v jejichž souvislosti existuje možnost, že pokud by byla přítomnost nebo absence uvedených osobních údajů zveřejněna, způsobilo by to újmu na životě, zdraví nebo majetku zmocnitele nebo třetí strany“; ii) údaje, „v jejichž souvislosti existuje možnost, že pokud by byla přítomnost nebo absence uvedených osobních údajů zveřejněna, motivovalo by to nebo vedlo k protiprávnímu nebo nepoctivému jednání“; iii) údaje, „v jejichž souvislosti existuje možnost, že pokud by byla přítomnost nebo absence uvedených osobních údajů zveřejněna, narušilo by to národní bezpečnost, zničilo vztah důvěry s cizí zemí nebo mezinárodní organizací nebo by to znamenalo nevýhodu při vyjednávání s cizí zemí nebo mezinárodní organizací“ a iv) ty údaje, „v jejichž souvislosti existuje možnost, že pokud by byla přítomnost nebo absence uvedených osobních údajů zveřejněna, bránilo by to zachování veřejné bezpečnosti a pořádku, například předcházení, potlačování nebo vyšetřování trestného činu“.

⁽²¹⁾ Za těchto podmínek se žádné oznámení fyzické osobě nevyžaduje. To je v souladu s čl. 23 odst. 2 písm. h) obecného nařízení o ochraně osobních údajů, který stanoví, že subjekty údajů nemusí být o daném omezení informovány, pokud toto informování „[může] být na újmu účelu omezení“.

2.2.4 Definice anonymně zpracovávaných osobních informací

- (27) Požadavky vztahující se na anonymně zpracovávané osobní informace vymezené v čl. 2 odst. 9 zákona o ochraně osobních informací jsou stanoveny v oddíle 2 kapitole 4 zákona („Povinnosti podnikatelského subjektu nakládajícího s anonymně zpracovávanými informacemi“). Takové informace se naopak neřídí ustanoveními oddílu 1 kapitoly IV zákona o ochraně osobních informací, který obsahuje články, které stanoví záruky a práva v oblasti ochrany údajů vztahující se na zpracování osobních údajů podle uvedeného zákona. „Anonymně zpracovávané osobní informace“ tedy sice nepodléhají „standardním“ pravidlům ochrany údajů (stanoveným v oddíle 1 kapitole IV a v článku 42 zákona o ochraně osobních informací), spadají však do oblasti působnosti zákona o ochraně osobních informací, zejména článků 36 až 39.
- (28) Podle čl. 2 odst. 9 zákona o ochraně osobních informací „anonymně zpracovávané osobní informace“ jsou informace týkající se fyzické osoby, které „vznikly zpracováním osobních informací“ prostřednictvím opatření stanovených v zákoně o ochraně osobních informací (čl. 36 odst. 1) a uvedených v pravidlech Komise pro ochranu osobních informací (článek 19), v důsledku čehož již není možné určit konkrétní fyzickou osobu nebo obnovit osobní informace.
- (29) Z uvedených ustanovení vyplývá, a potvrdila to také Komise pro ochranu osobních informací, že proces „anonymizace“ osobních informací nemusí být technicky nevratný. Podle čl. 36 odst. 2 zákona o ochraně osobních informací se pouze vyžaduje, aby podnikatelské subjekty nakládající s „anonymně zpracovávanými osobními informacemi“ zabránily opětovné identifikaci přijetím opatření, která zajistí bezpečnost „popisů atd.“, a vymazáním individuálních identifikačních kódů z osobních informací používaných k získání anonymně zpracovávaných informací a informací týkajících se použité metody zpracování.
- (30) Vzhledem k tomu, že „anonymně zpracovávané osobní informace“ vymezené zákonem o ochraně osobních informací zahrnují údaje, u nichž je opětovná identifikace fyzické osoby stále možná, mohlo by to znamenat, že osobní údaje předávané z Evropské unie by mohly přijít o část dostupných ochranných opatření během procesu, který by podle nařízení (EU) 2016/679 byl považován za formu „pseudonymizace“ spíše než „anonymizace“ (tedy beze změny jejich povahy jakožto osobních údajů).
- (31) Pro řešení této situace doplňková pravidla stanoví dodatečně požadavky vztahující se pouze na osobní údaje předávané z Evropské unie podle tohoto rozhodnutí. Podle pravidla 5 doplňkových pravidel se takové osobní informace považují za „anonymně zpracovávané osobní informace“ ve smyslu zákona o ochraně osobních informací pouze „v případě, že podnikatelský subjekt nakládající s osobními informacemi přijme opatření, na jejichž základě bude anonymizace fyzické osoby pro všechny nevratná, včetně vymazání informací týkajících se metody zpracování atd.“ Ty jsou v doplňkových pravidlech vymezeny jako informace související s popisy a individuálními identifikačními kódy, které byly vymazány z osobních informací použitých k vytváření „anonymně zpracovávaných osobních informací“, a rovněž jako informace související s použitou metodou zpracování, pokud byly tyto popisy a individuální identifikační kódy vymazány. Jinými slovy doplňková pravidla vyžadují, aby podnikatelský subjekt vytvářející „anonymně zpracovávané osobní informace“ zničil „klíč“ umožňující opětovnou identifikaci údajů. To znamená, že osobní údaje pocházející z Evropské unie podléhají ustanovením zákona o ochraně osobních informací, která se týkají „anonymně zpracovávaných osobních informací“ pouze v případech, kdy by tyto informace byly pravděpodobně považovány za anonymní i podle nařízení (EU) 2016/679 ⁽²²⁾.

2.2.5 Definice podnikatelského subjektu nakládajícího s osobními informacemi

- (32) Z hlediska osobní oblasti působnosti se zákon o ochraně osobních informací vztahuje pouze na podnikatelské subjekty nakládající s osobními informacemi. Podnikatelský subjekt nakládající s osobními informacemi je vymezen v čl. 2 odst. 5 zákona o ochraně osobních informací jako „osoba poskytující databázi osobních informací atd. pro účely podnikání“ s výjimkou vládních a správních agend, a to jak na ústřední, tak na místní úrovni.
- (33) Podle pokynů Komise pro ochranu osobních informací se „podnikáním“ rozumí jakékoli „jednání zaměřené na provozování společensky uznávaného podniku, a to s určitým cílem, za účelem zisku nebo neziskově, opakovaně a nepřetržitě“. Organizace bez právní subjektivity (jako například sdružení *de facto*) nebo fyzické osoby se považují za podnikatelský subjekt nakládající s osobními informacemi, pokud pro své podnikání poskytují (používají) databázi osobních informací atd. ⁽²³⁾. Pojem „podnikání“ podle zákona o ochraně osobních informací je tedy velmi široký, neboť zahrnuje nejen činnosti za účelem zisku, ale i činnosti neziskové provozované různými typy organizací a fyzických osob. „Použití pro účely podnikání“ navíc zahrnuje také osobní informace, které se nepoužívají v obchodních (vnějších) vztazích subjektu, ale interně, například pro zpracování údajů o zaměstnancích.

⁽²²⁾ Viz nařízení (EU) 2016/679, 26. bod odůvodnění.

⁽²³⁾ Pokyny Komise pro ochranu osobních informací (General Rule Edition), s. 18.

- (34) Pokud jde o příjemce ochrany stanovených v zákoně o ochraně osobních informací, zákon nečiní rozdíl na základě státní příslušnosti, bydliště nebo místa fyzické osoby. Totéž platí pro možnost fyzických osob domáhat se ochrany, ať už u Komise pro ochranu osobních informací, nebo u soudů.

2.2.6 Koncepty správce a zpracovatele

- (35) Zákon o ochraně osobních informací nijak nerozlišuje mezi povinnostmi uloženými správci a zpracovateli. Neexistence tohoto rozlišení neovlivňuje úroveň ochrany, protože všechny podnikatelské subjekty nakládající s osobními informacemi podléhají všem ustanovením zákona. Podnikatelský subjekt nakládající s osobními informacemi, který zpracovává osobní údaje svěří zmocněnci (ekvivalent zpracovatele podle obecného nařízení o ochraně osobních údajů), má i nadále povinnosti podle zákona o ochraně osobních informací a doplňkových pravidel, pokud jde o svěření údaje. Kromě toho podle článku 22 zákona o ochraně osobních informací je tento subjekt povinen nad zmocněncem „vykonávat potřebný a přiměřený dohled“. Jak potvrdila Komise pro ochranu osobních informací, samotný zmocněnec je pak vázán všemi povinnostmi podle zákona o ochraně osobních informací a doplňkových pravidel.

2.2.7 Odvětvové výjimky

- (36) Článek 76 zákona o ochraně osobních informací vylučuje určité typy zpracování údajů z působnosti kapitoly IV zákona, která obsahuje ustanovení o centrální ochraně údajů (základní zásady, povinnosti podnikatelských subjektů, individuální práva, dohled ze strany Komise pro ochranu osobních informací). Zpracování, na které se vztahuje odvětvová výjimka uvedená v článku 76, je rovněž vyjmuta z vymáhacích pravomocí Komise pro ochranu osobních informací podle čl. 43 odst. 2 zákona o ochraně osobních informací ⁽²⁴⁾.
- (37) Příslušné kategorie pro odvětvovou výjimku v článku 76 zákona o ochraně osobních informací jsou vymezeny použitím dvou kritérií na základě typu podnikatelského subjektu nakládajícího s osobními informacemi, který zpracovává osobní informace, a účelu zpracování. Konkrétně se výjimka vztahuje na tyto subjekty: i) rozhlasové a televizní společnosti, vydavatelé novin, komunikační agentury nebo jiné tiskové organizace (včetně všech fyzických osob, které provozují tiskové činnosti jako své podnikání), pokud zpracovávají osobní informace pro účely tisku; ii) osoby zabývající se profesionálním psaním, pokud toto psaní zahrnuje osobní informace; iii) vysoké školy a jakékoli jiné organizace nebo skupiny zaměřené na akademická studia nebo jakákoli osoba náležející do takové organizace, pokud zpracovávají osobní informace pro účely akademických studií; iv) církevní instituce, pokud zpracovávají osobní informace pro účely náboženské činnosti (včetně všech činností souvisejících), a v) politické orgány, pokud zpracovávají osobní informace pro účely své politické činnosti (včetně všech činností souvisejících). Zpracování osobních informací pro jeden z účelů uvedených v článku 76 jinými typy podnikatelských subjektů nakládajících s osobními informacemi, jakož i zpracování osobních informací jedním z uvedených podnikatelských subjektů nakládajících s osobními informacemi pro jiné účely, například v kontextu zaměstnání, podléhá ustanovením kapitoly IV.
- (38) Aby se zajistila odpovídající úroveň ochrany osobních údajů předávaných z Evropské unie podnikatelským subjektům v Japonsku, mělo by se toto rozhodnutí vztahovat pouze na zpracování osobních informací spadajících do oblasti působnosti kapitoly IV zákona o ochraně osobních informací – tj. na zpracování podnikatelským subjektem nakládajícím s osobními informacemi, pokud zpracování neodpovídá některé z odvětvových výjimek. Jeho oblast působnosti by proto měla být sladěna s oblastí působnosti zákona o ochraně osobních informací. Podle informací obdržených z Komise pro ochranu osobních informací by jakákoli následná změna účelu použití podnikatelským subjektem nakládajícím s osobními informacemi, na který se vztahuje toto rozhodnutí (v rozsahu, v jakém je to přípustné) a na který by se vztahovala některá z odvětvových výjimek podle článku 76 zákona o ochraně osobních informací, byla považována za mezinárodní předávání (vzhledem k tomu, že v takových případech by se na zpracování osobních informací již nevztahovala kapitola IV zákona o ochraně osobních informací, a tudíž by nespádalo do oblasti jeho působnosti). Totéž by platilo v případě, že podnikatelský subjekt nakládající s osobními informacemi poskytne osobní informace subjektu, na který se vztahuje článek 76 zákona o ochraně osobních informací, aby je použil k některému z účelů zpracování uvedených v daném ustanovení. Pokud jde o osobní údaje předávané z Evropské unie, představovalo by to tedy další předávání, na které se vztahují příslušné záruky (zejména záruky uvedené v článku 24 zákona o ochraně osobních informací a doplňkovém pravidle 4). Pokud podnikatelský subjekt nakládající s osobními informacemi potřebuje souhlas subjektu údajů ⁽²⁵⁾, musel by subjektu údajů poskytnout veškeré potřebné informace, včetně toho, že osobní informace již nebudou chráněny zákonem o ochraně osobních informací.

⁽²⁴⁾ Pokud jde o jiné podnikatele, Komise pro ochranu osobních informací při výkonu svých pravomocí v oblasti vyšetřování a vymáhání předpisů nikdy neomezuje jejich právo na svobodu vyjadřování, akademickou svobodu, náboženskou svobodu a svobodu politické činnosti (čl. 43 odst. 1 zákona o ochraně osobních informací).

⁽²⁵⁾ Jak vysvětlila Komise pro ochranu osobních informací, souhlas se v jejích pokynech vykládá jako „vyjádření úmyslu hlavního subjektu akceptovat, že se s jeho osobními informacemi může nakládat způsobem uvedeným podnikatelským subjektem nakládajícím s osobními informacemi“. V pokynech Komise pro ochranu osobních informací (General Rule Edition, s. 24) jsou uvedeny způsoby vyjádření souhlasu, které se považují „za běžné obchodní praktiky v Japonsku“, tj. ústní dohoda, vyplnění formulářů nebo jiných dokumentů, souhlas prostřednictvím e-mailu, zaškrtnutí políčka na internetové stránce, kliknutí na domovské stránce, použití tlačítka k vyjádření souhlasu, poklepání na dotykovém displeji atd. Všechny tyto způsoby představují výslovnou formu souhlasu.

2.3 Záruky, práva a povinnosti

2.3.1 Účelové omezení

- (39) Osobní údaje by měly být zpracovávány za konkrétním účelem a následně používány, pouze pokud to není neslučitelné s účelem zpracování. Tato zásada ochrany údajů je zaručena podle článků 15 a 16 zákona o ochraně osobních informací.
- (40) Zákon o ochraně osobních informací vychází ze zásady, že podnikatelský subjekt musí určit účel použití „co možná nejjasněji“ (čl. 15 odst. 1) a je pak tímto účelem při zpracování údajů vázán.
- (41) V tomto ohledu čl. 15 odst. 2 zákona o ochraně osobních informací stanoví, že původní účel nesmí podnikatelský subjekt nakládající s osobními informacemi změnit „nad rámec, který je považován za přiměřeně relevantní pro účely použití před změnou“, což je v pokynech Komise pro ochranu osobních informací vykládáno jako to, co odpovídá objektivnímu očekávání subjektu údajů na základě „běžných společenských zvyklostí“⁽²⁶⁾.
- (42) Kromě toho podle čl. 16 odst. 1 zákona o ochraně osobních informací je zakázáno, aby podnikatelské subjekty nakládaly s osobními informacemi nad „rámec rozsahu nezbytného pro dosažení účelu použití“ stanovený v článku 15 bez předchozího souhlasu subjektu údajů, ledaže by se použila jedna s výjimek uvedených v čl. 16 odst. 3⁽²⁷⁾.
- (43) Pokud jde o osobní informace získané od jiného podnikatelského subjektu, může podnikatelský subjekt nakládající s osobními informacemi v zásadě svobodně stanovit nový účel použití⁽²⁸⁾. Aby se zajistilo, že v případě předávání z Evropské unie je příslušný příjemce vázán účelem, pro který byly údaje předány, doplňkové pravidlo 3 vyžaduje, aby v případech „kdy [podnikatelský subjekt nakládající s osobními informacemi] obdrží osobní údaje z EU na základě rozhodnutí o odpovídající ochraně“ nebo takový subjekt „obdrží od jiného [podnikatelského subjektu nakládajícího s osobními informacemi] osobní údaje dříve předané z EU na základě rozhodnutí o odpovídající ochraně“ (další sdílení), příjemce musí „stanovit účel použití uvedených osobních údajů v rámci rozsahu účelu použití, pro který byly údaje původně nebo následně obdrženy“. Jinými slovy toto pravidlo zajišťuje, že v souvislosti s předáváním údajů účel stanovený podle nařízení (EU) 2016/679 i nadále určuje zpracování a že změna uvedeného účelu v jakékoli fázi zpracovatelského řetězce v Japonsku by vyžadovala souhlas subjektu údajů z EU. Jelikož získání souhlasu vyžaduje, aby podnikatelský subjekt nakládající s osobními informacemi kontaktoval subjekt údajů, pokud to není možné, důsledkem je jednoduše to, že musí být zachován původní účel.

2.3.2 Zákonnost a korektnost zpracování

- (44) Doplňková ochrana uvedená ve 43. bodě odůvodnění je o to důležitější, že prostřednictvím zásady účelového omezení japonský systém rovněž zajišťuje zákonné a korektní zpracování osobních údajů.
- (45) Pokud podnikatelský subjekt nakládající s osobními informacemi shromažďuje osobní informace, zákon o ochraně osobních informací vyžaduje, aby podrobně stanovil účel použití osobních informací⁽²⁹⁾ a tento účel použití bezodkladně sdělil subjektu údajů (nebo jej zveřejnil)⁽³⁰⁾. Kromě toho článek 17 zákona o ochraně osobních informací stanoví, že podnikatelský subjekt nakládající s osobními informacemi nezíská osobní informace podvodem nebo jinými nepatřičnými prostředky. Pokud jde o určité kategorie údajů, jako například osobní informace vyžadující zvláštní péči, k jejich získání je zapotřebí souhlas subjektu údajů (čl. 17 odst. 2 zákona o ochraně osobních informací).

⁽²⁶⁾ Otázky a odpovědi vydané Komisí pro ochranu osobních informací obsahují řadu příkladů dokládajících tento pojem. Příklady situací, kdy je rozsah změny přiměřeně relevantní, zahrnují zejména používání osobních informací získaných od odběratelů zboží a služeb v kontextu obchodní transakce za účelem informování uvedených odběratelů o jiném relevantním dostupném zboží nebo jiných relevantních dostupných službách (např. provozovatel fitness klubu, který si zaeviduje e-mailové adresy členů, aby je mohl informovat o kurzech a programech). Otázky a odpovědi zároveň zahrnují příklad situace, kdy změna účelu použití není přípustná, konkrétně pokud společnost zaslala informace o svém zboží a svých službách na e-mailové adresy, které shromáždila za účelem varování před podvodem nebo krádeží členské karty.

⁽²⁷⁾ Tyto výjimky mohou vyplývat z jiných právních předpisů nebo se týkají situací, kdy je nakládání s osobními informacemi nezbytné i) pro „ochranu lidského života, zdraví nebo majetku“; ii) pro „zlepšení veřejné hygieny nebo na podporu růstu zdravých dětí“ nebo iii) „ke spolupráci s vládními agenturami nebo orgány nebo jejich zástupci“ při plnění jejich zákonných povinností. Kromě toho kategorie i) a ii) se použijí pouze v případě, že je obtížné získat souhlas subjektu údajů, a kategorie iii) pouze v případě rizika, že získání souhlasu subjektu údajů by plnění takových povinností narušilo.

⁽²⁸⁾ Vzhledem k tomu je na základě čl. 23 odst. 1 zákona o ochraně osobních informací pro zpřístupnění údajů třetí straně v zásadě vyžadován souhlas fyzické osoby. Fyzická osoba tak může vykonávat určitou kontrolu nad používáním svých údajů jiným podnikatelským subjektem.

⁽²⁹⁾ Podle čl. 15 odst. 1 zákona o ochraně osobních informací musí být takové stanovení účelu „co možná nejjasnější“.

⁽³⁰⁾ Ustanovení čl. 18 odst. 1 zákona o ochraně osobních informací.

- (46) Jak je vysvětleno ve 41. a 42. bodě odůvodnění, podnikatelský subjekt nakládající s osobními informacemi nesmí zpracovávat osobní informace pro jiné účely, pokud subjekt údajů s takovým zpracováním neposkytne souhlas nebo pokud se nepoužije jedna s výjimek podle čl. 16 odst. 3 zákona o ochraně osobních informací.
- (47) V neposlední řadě, pokud jde o další poskytnutí osobních informací třetí straně⁽³¹⁾, čl. 23 odst. 1 zákona o ochraně osobních informací omezuje takové zpřístupnění na zvláštní případy, obecně s předchozím souhlasem subjektu údajů⁽³²⁾. Ustanovení čl. 23 odst. 2, 3 a 4 zákona o ochraně osobních informací stanoví výjimky z požadavku na získání souhlasu. Tyto výjimky jsou však použitelné pouze na údaje, které nejsou citlivé, a v případě, kdy musí podnikatelský subjekt dotčené fyzické osoby předem informovat o úmyslu zpřístupnit jejich osobní informace třetí straně a o možnosti vznést proti jakémukoli dalšímu zpřístupnění námitku⁽³³⁾.
- (48) Pokud jde o předávání z Evropské unie, osobní údaje budou muset být nejdříve shromážděny a zpracovány v EU v souladu s nařízením (EU) 2016/679. To bude vždy zahrnovat shromáždění a zpracování (i za účelem předání z Evropské unie do Japonska) na základě jednoho z právních důvodů uvedených v čl. 6 odst. 1 nařízení na straně jedné a shromáždění pro určitý, výslovně vyjádřený a legitimní účel, jakož i zákaz dalšího zpracování (i formou předání) způsobem, který je s takovým účelem neslučitelný, podle čl. 5 odst. 1 písm. b) a čl. 6 odst. 4 nařízení na straně druhé.
- (49) Po předání bude podle doplňkového pravidla 3 muset podnikatelský subjekt nakládající s osobními informacemi, který údaje obdrží, „potvrdit“ konkrétní účel(y) předání (tj. účel stanovený podle nařízení (EU) 2016/679) a tyto údaje dále zpracovávat v souladu s těmito účely⁽³⁴⁾. To znamená, že účely stanovenými podle nařízení je vázán nejen původní příjemce těchto osobních údajů v Japonsku, ale také jakýkoli budoucí příjemce údajů (včetně zmocněnce).
- (50) Pokud by navíc podnikatelský subjekt nakládající s osobními informacemi chtěl změnit účel dříve stanovený podle nařízení (EU) 2016/679, v souladu s čl. 16 odst. 1 zákona o ochraně osobních informací by v zásadě musel získat souhlas subjektu údajů. Bez uvedeného souhlasu by jakékoli zpracování údajů nad rámec rozsahu nezbytného pro dosažení uvedeného účelu použití představovalo porušení čl. 16 odst. 1, které by bylo vymahatelné Komisí pro ochranu osobních informací i soudy.
- (51) Vzhledem k tomu, že podle nařízení (EU) 2016/679 předání vyžaduje platný právní základ a konkrétní účel, které jsou zohledněny v účelu použití „potvrzeném“ podle zákona o ochraně osobních informací, kombinace příslušných ustanovení zákona o ochraně osobních informací a doplňkového pravidla 3 zajišťuje pokračující zákonnost zpracování údajů z EU v Japonsku.

2.3.3 Přesnost a minimalizace údajů

- (52) Údaje musí být přesné a v případě potřeby aktualizované. Měly by rovněž být přiměřené, relevantní a nikoli přebytečné ve vztahu k účelům, pro které jsou zpracovávány.
- (53) Tyto zásady jsou v japonském právu zajištěny v čl. 16 odst. 1 zákona o ochraně osobních informací, který zakazuje nakládání s osobními informacemi nad rámec „rozsahu nezbytného pro dosažení účelu použití“. Jak vysvětlila Komise pro ochranu osobních informací, to nejen vylučuje používání údajů, které jsou nepřiměřené, a nadbytečné používání údajů (nad rámec toho, co je nezbytné pro dosažení účelu použití), ale zahrnuje to také zákaz nakládání s údaji, které nejsou pro dosažení účelu použití relevantní.

⁽³¹⁾ Zmocněnci jsou sice z pojmu „třetí strana“ pro účely použití článku 23 (viz odstavec 5) vyloučeni, toto vyloučení však platí, pouze pokud zmocněnec nakládá s osobními údaji v mezích svého pověření („v rozsahu nezbytném pro dosažení účelu použití“), tj. jedná jako zpracovatel.

⁽³²⁾ Mezi další (výjimečné) důvody patří: i) poskytnutí osobních informací „na základě právních předpisů“; ii) případy, „kdy je zapotřebí chránit lidský život, zdraví nebo majetek a kdy je obtížné získat souhlas zmocnítele“; iii) případy, „kdy existuje zvláštní potřeba zlepšit veřejnou hygienu nebo podpořit zdravý růst dětí a kdy je obtížné získat souhlas zmocnítele“; a iv) případy, „kdy je zapotřebí spolupracovat s ústřední vládní organizací nebo místní vládní institucí nebo jimi pověřenou osobou při provádění záležitostí stanovených právními předpisy, a pokud by získání souhlasu zmocnítele mohlo plnění uvedených záležitostí narušit“.

⁽³³⁾ Poskytované informace zahrnují zejména kategorie osobních údajů, které mají být sdíleny se třetí stranou, a způsob přenosu. Kromě toho podnikatelský subjekt nakládající s osobními informacemi musí informovat subjekt údajů o možnosti přenos odmítnout a o způsobu předložení tohoto požadavku.

⁽³⁴⁾ Podle čl. 26 odst. 1 bodu ii) zákona o ochraně osobních informací musí podnikatelský subjekt nakládající s osobními informacemi v okamžiku, kdy obdrží osobní údaje od třetí strany, „potvrdit“ (ověřit) „podrobnosti získání osobních údajů třetí stranou“, včetně účelu uvedeného získání. Ačkoli článek 26 výslovně nestanoví, že podnikatelský subjekt nakládající s osobními informacemi se musí uvedeným účelem řídit, je to výslovně vyžadováno doplňkovým pravidlem 3.

- (54) Pokud jde o povinnost uchovávat údaje přesné a aktualizované, článek 19 zákona o ochraně osobních informací vyžaduje, aby podnikatelský subjekt nakládající s osobními informacemi „usiloval o to, aby byly osobní údaje udržovány přesné a aktualizované v rozsahu nezbytném pro dosažení účelu použití“. Uvedené ustanovení je třeba vykládat ve spojení s čl. 16 odst. 1 zákona o ochraně osobních informací: z vysvětlení obdržených od Komise pro ochranu osobních informací vyplývá, že pokud podnikatelský subjekt nakládající s osobními informacemi nesplňuje předepsané normy přesnosti, nebude zpracování osobních informací považováno za zpracování splňující účel použití, a nakládání s těmito informacemi se tedy podle čl. 16 odst. 1 stane protiprávním.

2.3.4 Omezení uložení

- (55) Je zapotřebí, aby údaje byly ukládány po dobu ne delší, než je nezbytné pro účely, pro které jsou osobní údaje zpracovávány.
- (56) Podle článku 19 zákona o ochraně osobních informací musí podnikatelské subjekty nakládající s osobními informacemi „usilovat [...] o to, aby byly osobní údaje bezodkladně vymazány, jakmile již jejich použití nebude nutné“. Uvedené ustanovení je rovněž třeba vykládat ve spojení s čl. 16 odst. 1 zákona o ochraně osobních informací, který zakazuje nakládání s osobními informacemi nad rámec „rozsahu nezbytného pro dosažení účelu použití“. Jakmile je účelu použití dosaženo, zpracování osobních informací již nelze považovat za nezbytné, a nemůže tedy pokračovat (pokud podnikatelský subjekt nakládající s osobními informacemi neobdrží od subjektu údajů příslušný souhlas).

2.3.5 Zabezpečení údajů

- (57) Osobní údaje by měly být zpracovávány způsobem, který zajišťuje jejich zabezpečení, včetně ochrany před neoprávněným nebo protiprávním zpracováním a před náhodnou ztrátou, zničením nebo poškozením. Za tímto účelem by podnikatelské subjekty měly přijmout vhodná technická nebo organizační opatření na ochranu osobních údajů před možnými hrozbami. Tato opatření by měla být posuzována s přihlédnutím ke stavu techniky a k souvisejícím nákladům.
- (58) Tato zásada je v japonském právu provedena článkem 20 zákona o ochraně osobních informací, který stanoví, že podnikatelský subjekt nakládající s osobními informacemi „přijme nezbytná a vhodná opatření pro kontrolu zabezpečení osobních údajů, včetně zamezení úniku, ztrátě nebo poškození osobních údajů, s nimiž nakládá“. Pokyny Komise pro ochranu osobních informací vysvětlují opatření, která mají být přijata, včetně způsobů zavedení základních politik, pravidel pro nakládání s údaji a různých „kontrolních opatření“ (pokud jde o organizační bezpečnost, jakož i o bezpečnost lidí a fyzické a technologické zabezpečení) ⁽³⁵⁾. Kromě toho pokyny Komise pro ochranu osobních informací a zvláštní oznámení (dodatek 8 „Obsah opatření pro řízení bezpečnosti, která musí být přijata“) zveřejněné Komisí pro ochranu osobních informací poskytují více podrobností o opatřeních týkajících se bezpečnostních incidentů, při nichž dojde například k úniku osobních informací, v rámci opatření pro řízení bezpečnosti, která má podnikatelský subjekt nakládající s osobními informacemi přijmout ⁽³⁶⁾.
- (59) Kromě toho kdykoli s osobními informacemi nakládají zaměstnanci nebo subdodavatelé, musí být zajištěn „nezbytný a přiměřený dohled“ podle článků 20 a 21 zákona o ochraně osobních informací pro účely bezpečnostních kontrol. V neposlední řadě podle článku 83 zákona o ochraně osobních informací je v případě úmyslného úniku nebo krádeže osobních informací stanoven trest odnětí svobody v délce až jeden rok.

2.3.6 Transparentnost

- (60) Subjekty údajů by měly být informovány o hlavních znacích zpracování jejich osobních údajů.
- (61) Ustanovení čl. 18 odst. 1 zákona o ochraně osobních informací vyžadují, aby podnikatelský subjekt nakládající s osobními informacemi poskytl subjektu údajů informace o účelu použití získaných osobních informací, s výjimkou „případů, kdy byl účel použití již dříve zveřejněn“. Stejná povinnost se použije v případě přípustné změny účelu (čl. 18 odst. 3). Tím se rovněž zaručí, že je subjekt údajů informován o skutečnosti, že jeho údaje byly shromážděny. Ačkoli zákon o ochraně osobních informací obecně nevyžaduje, aby podnikatelský subjekt nakládající s osobními informacemi informoval subjekt údajů o očekávaných příjemcích osobních informací ve fázi shromažďování, takové informace jsou nezbytnou podmínkou pro jakékoli následné zpřístupnění třetí straně (příjemci) na základě čl. 23 odst. 2, tedy pokud se tak děje bez předchozího souhlasu subjektu údajů.

⁽³⁵⁾ Pokyny Komise pro ochranu osobních informací (General Rule Edition), s. 41 a s. 86–98.

⁽³⁶⁾ Oddíl 3-3-2 pokynů Komise pro ochranu osobních informací stanoví, že dojde-li k úniku, poškození nebo ztrátě, podnikatelský subjekt nakládající s osobními informacemi musí provést nezbytná šetření, a zejména posoudit rozsah porušení práv a zájmů příslušné fyzické osoby, jakož i povahu a rozsah dotčených osobních informací.

- (62) Pokud jde o „uchovávané osobní údaje“, článek 27 zákona o ochraně osobních informací stanoví, že podnikatelský subjekt nakládající s osobními informacemi informuje subjekt údajů o své totožnosti (kontaktní údaje), účelu použití a postupech reakce na žádost týkající se individuálních práv subjektu údajů podle článků 28, 29 a 30 zákona o ochraně osobních informací.
- (63) Jelikož podle doplňkových pravidel budou osobní údaje předávané z Evropské unie považovány za „uchovávané osobní údaje“ bez ohledu na dobu jejich uchování (pokud se nepoužijí výjimky), budou vždy podléhat požadavkům na transparentnost podle obou výše uvedených ustanovení.
- (64) Na požadavky článku 18 i povinnost informovat o účelu použití podle článku 27 zákona o ochraně osobních informací se vztahuje stejný soubor výjimek, většinou odůvodněných veřejným zájmem a ochranou práv a zájmů subjektu údajů, třetích stran a správce⁽³⁷⁾. Podle výkladu obsaženého v pokynech Komise pro ochranu osobních informací se uvedené výjimky použijí pouze ve velmi specifických situacích, např. pokud by informace o účelu použití mohly narušit legitimní opatření přijatá podnikatelským subjektem na ochranu určitých zájmů (např. boj proti korupci, průmyslová špionáž, sabotáž).

2.3.7 Zvláštní kategorie údajů

- (65) Pokud se zpracovávají „zvláštní kategorie“ údajů, měly by existovat zvláštní záruky.
- (66) „Osobní informace vyžadující zvláštní péči“ jsou vymezeny v čl. 2 odst. 3 zákona o ochraně osobních informací. Uvedené ustanovení se odvolává na „osobní informace zahrnující rasu zmocnitele, jeho náboženské vyznání, společenské postavení, anamnézu, záznam v rejstříku trestů, utrpění újmy v důsledku trestného činu a jiné informace určené nařízením kabinetu jako informace, s nimiž musí být nakládáno se zvláštní péčí, aby nedocházelo k nespravedlivé diskriminaci, předpojatosti nebo jinému znevýhodňování zmocnitele“. Tyto kategorie z velké části odpovídají seznamu citlivých údajů podle článků 9 a 10 nařízení (EU) 2016/679. Zejména „anamnéza“ odpovídá zdravotním údajům, zatímco „záznam v rejstříku trestů a utrpění újmy v důsledku trestného činu“ jsou v zásadě stejné jako kategorie uvedené v článku 10 nařízení (EU) 2016/679. Kategorie uvedené v čl. 2 odst. 3 zákona o ochraně osobních informací podléhají dalšímu výkladu v nařízení kabinetu a pokynech Komise pro ochranu osobních informací. Podle oddílu 2.3 bodu 8) pokynů Komise pro ochranu osobních informací zahrnují podkategorie „anamnézy“ podrobně uvedené v čl. 2 bodech ii) a iii) nařízení kabinetu genetické a biometrické údaje. Seznam sice výslovně neobsahuje pojmy „etnický původ“ a „politický názor“, ale odkazuje na „rasu“ a „náboženské vyznání“. Jak je vysvětleno v oddílu 2.3 bodech 1) a 2) pokynů Komise pro ochranu osobních informací, odkaz na „rasu“ zahrnuje „etnické vazby nebo vazby na určitou část světa“, zatímco „náboženské vyznání“ zahrnuje náboženské i politické názory.
- (67) Ze znění ustanovení je jasné, že se nejedná o uzavřený seznam, neboť lze přidávat další kategorie údajů, pokud jejich zpracování vytváří riziko „nespravedlivé diskriminace, předpojatosti nebo jiných znevýhodnění zmocnitele“.
- (68) Zatímco pojetí „citlivých“ údajů je svou podstatou společenskou konstrukcí, neboť vychází z kulturních a právních tradic, morálních úvah, politických rozhodnutí atd. určité společnosti, s ohledem na důležitost zajištění přiměřených záruk pro citlivé údaje při předávání podnikatelským subjektům v Japonsku dosáhla Evropská komise toho, že zvláštní ochrany poskytované „osobním informacím, které vyžadují zvláštní péči“, podle japonského práva se rozšiřují na všechny kategorie uznávané jako „citlivé údaje“ v nařízení (EU) 2016/679. Za tímto účelem doplňkové pravidlo 1 stanoví, že údaje předávané z Evropské unie týkající se sexuálního života fyzické osoby, její sexuální orientace nebo členství v odborech budou zpracovávány podnikatelskými subjekty nakládajícími s osobními informacemi „stejným způsobem jako osobní informace vyžadující zvláštní péči ve smyslu čl. 2 odst. 3 [zákona o ochraně osobních informací]“.

⁽³⁷⁾ Jedná se o i) případy, kdy by informování subjektu údajů o účelu použití nebo jeho zveřejnění mohlo způsobit „újmu na životě, zdraví, majetku nebo jiných právech a zájmech zmocnitele nebo třetí strany“ nebo újmu na „právech nebo oprávněných zájmech [...] podnikatelského subjektu nakládajícího s osobními informacemi“; ii) případy, kdy „je zapotřebí spolupracovat s ústřední vládní organizací nebo místní vládní institucí“ při plnění jejich úkolů vyplývajících z právních předpisů, a pokud by uvedené informace nebo jejich zpřístupnění takové „záležitosti“ narušilo; iii) případy, kdy je účel použití jasný a vychází ze situace, v níž byly údaje získány.

- (69) Pokud jde o další hmotné záruky vztahující se na osobní informace vyžadující zvláštní péči, podle čl. 17 odst. 2 zákona o ochraně osobních informací podnikatelské subjekty nakládající s osobními informacemi nesmějí získávat tento typ údajů bez předchozího souhlasu dotyčné fyzické osoby, pouze s výhradou omezených výjimek⁽³⁸⁾. Dále je tato kategorie osobních informací vyloučena z možnosti zpřístupnění třetí straně na základě postupu podle čl. 23 odst. 2 zákona o ochraně osobních informací (umožňujícího přenos údajů třetím stranám bez předchozího souhlasu dotyčné fyzické osoby).

2.3.8 Odpovědnost

- (70) Podle zásady odpovědnosti se od subjektů zpracovávajících údaje vyžaduje zavedení vhodných technických a organizačních opatření, aby mohly účinně plnit své povinnosti v oblasti ochrany údajů a jejich plnění byly schopny prokázat, zejména příslušnému dozorovému úřadu.
- (71) Jak je uvedeno v poznámce pod čarou č. 34 (49. bod odůvodnění), podnikatelské subjekty nakládající s osobními informacemi musí podle čl. 26 odst. 1 zákona o ochraně osobních informací ověřit totožnost třetí strany, která jim poskytuje osobní údaje, a „okolnosti“, za kterých uvedená třetí strana takové údaje získala (v případě osobních údajů, na které se vztahuje toto rozhodnutí, uvedené okolnosti podle zákona o ochraně osobních informací a doplňkového pravidla 3 zahrnují skutečnost, že údaje pocházejí z Evropské unie, jakož i účel původního předání údajů). Cílem uvedeného opatření je mimo jiné zajistit zákonnost zpracování osobních údajů v rámci celého řetězce podnikatelských subjektů nakládajících s osobními informacemi, které s uvedenými osobními údaji nakládají. Podle čl. 26 odst. 3 zákona o ochraně osobních informací se dále vyžaduje, aby podnikatelské subjekty nakládající s osobními informacemi vedly záznamy o datu přijetí a (povinné) informace obdržené od třetí strany podle odstavce 1, jakož i jméno dotyčné fyzické osoby (subjektu údajů), kategorie zpracovaných údajů a v příslušném rozsahu skutečnost, že subjekt údajů poskytl se sdílením svých osobních údajů souhlas. Jak stanoví článek 18 pravidel Komise pro ochranu osobních informací, uvedené záznamy musí být uchovávány v závislosti na okolnostech po dobu nejméně jednoho roku až tří let. Při plnění svých úkolů může Komise pro ochranu osobních informací vyžadovat předložení těchto záznamů⁽³⁹⁾.
- (72) Podnikatelské subjekty nakládající s osobními informacemi musí neprodleně a řádně vyřizovat stížnosti od dotyčných fyzických osob týkající se zpracování jejich osobních informací. Pro snazší vyřizování stížností zavedou „systém nezbytný pro dosažení [tohoto] účelu“, což znamená, že by měly zavést vhodné postupy v rámci své organizace (například přidělení odpovědností nebo vytvoření kontaktního místa).
- (73) V neposlední řadě zákon o ochraně osobních informací vytváří rámec pro účast organizací z průmyslových odvětví na zajišťování vysoké úrovně souladu (viz oddíl 4 kapitoly IV). Úkolem takovýchto akreditovaných organizací působících v oblasti ochrany osobních informací⁽⁴⁰⁾ je prosazovat ochranu osobních informací podporou podniků prostřednictvím svých odborných znalostí a rovněž přispívat k provádění záruk, zejména vyřizováním jednotlivých stížností a napomáháním při řešení souvisejících sporů. Za tímto účelem mohou v případě potřeby vyžadovat, aby zapojené podnikatelské subjekty nakládající s osobními informacemi přijaly nezbytná opatření⁽⁴¹⁾. Kromě toho v případě porušení zabezpečení údajů nebo jiných bezpečnostních incidentů podnikatelské subjekty nakládající s osobními informacemi v zásadě informují Komisi pro ochranu osobních informací, jakož i subjekt údajů (nebo veřejnost) a podniknou nezbytné kroky, včetně přijetí opatření k minimalizaci jakékoli škody a k zamezení jakéhokoli opakování obdobných incidentů⁽⁴²⁾. Jedná se sice o dobrovolné režimy, ale k 10. srpnu 2017 měla Komise pro ochranu osobních informací na seznamu 44 organizací, přičemž jen samotná největší z nich, Japonské středisko pro rozvoj a zpracování informací (Japan Information Processing and Development Center, JIPDEC),

⁽³⁸⁾ Mezi výjimky patří: i) „případy vycházející z právních předpisů“; ii) „případy, kdy je zapotřebí chránit lidský život, zdraví nebo majetek a kdy je obtížné získat souhlas zmocnitele“; iii) „případy, kdy existuje zvláštní potřeba zlepšit veřejnou hygienu nebo podpořit zdravý růst dětí a kdy je obtížné získat souhlas zmocnitele“; iv) „případy, kdy je zapotřebí spolupracovat s ústřední vládou organizací nebo místní vládou institucí nebo jimi pověřenou osobou při provádění záležitostí stanovených právními předpisy, a pokud by získání souhlasu zmocnitele mohlo plnění uvedených záležitostí narušit“, a v) případy, kdy jsou uvedené osobní informace vyžadující zvláštní péči zveřejněny subjektem údajů, vládou organizací, místní vládou institucí, osobou spadající do jedné z kategorií čl. 76 odst. 1 nebo jinými osobami informacemi v pravidlech Komise pro ochranu osobních informací. Další kategorie se týká „jiných případů určených nařízením kabinetu jako rovnocenných k případům uvedeným v každém z předchozích bodů“ a podle stávajícího nařízení kabinetu zahrnuje zejména zřejmé znaky osoby (např. viditelný zdravotní stav), pokud byly citlivé údaje získány (neúmyslně) vizuálním pozorováním, filmováním nebo fotografováním subjektu údajů, např. kamerami CCTV.

⁽³⁹⁾ Podle čl. 40 odst. 1 zákona o ochraně osobních informací může Komise pro ochranu osobních informací v rozsahu nezbytném k provedení příslušných ustanovení zákona o ochraně osobních informací vyžadovat, aby podnikatelský subjekt nakládající s osobními informacemi předložil nezbytné informace nebo materiály týkající se zpracování osobních informací.

⁽⁴⁰⁾ Zákon o ochraně osobních informací mimo jiné stanoví pravidla pro akreditaci těchto organizací; viz články 47–50 zákona o ochraně osobních informací.

⁽⁴¹⁾ Článek 52 zákona o ochraně osobních informací.

⁽⁴²⁾ Oznámení Komise pro ochranu osobních informací č. 1/2017 „týkající se opatření, která mají být přijata v případech, kdy dojde k porušení zabezpečení osobních údajů nebo jinému incidentu“.

evidovala 15 436 zapojených podnikatelských subjektů⁽⁴³⁾. Mezi akreditované režimy patří odvětvová sdružení, například Japonská asociace obchodníků s cennými papíry, Japonská asociace autoškol nebo Asociace svatebních agentur⁽⁴⁴⁾.

- (74) Akreditované organizace pro ochranu osobních informací předkládají výroční zprávy o své činnosti. Podle „Přehledu stavu provádění zákona o ochraně osobních informací v rozpočtovém roce 2015“ zveřejněného Komise pro ochranu osobních informací obdržely akreditované organizace pro ochranu osobních informací celkem 442 stížností, vyžádaly si 123 vysvětlení od podnikatelských subjektů, které spadají do jejich pravomoci, ve 41 případech si od těchto subjektů vyžádaly dokumenty, poskytl 181 pokynů a vydaly dvě doporučení⁽⁴⁵⁾.

2.3.9 Omezení dalšího předávání

- (75) Úroveň ochrany poskytovaná osobním údajům předávaným z Evropské unie podnikatelským subjektům v Japonsku nesmí být oslabena dalším předáváním těchto údajů příjemcům ve třetí zemi mimo Japonsko. Toto „další předávání“, které z pohledu japonského podnikatelského subjektu představuje mezinárodní předávání z Japonska, by mělo být povoleno pouze v případě, že další příjemce mimo Japonsko sám podléhá pravidlům zajišťujícím obdobnou úroveň ochrany, jaká je zaručena v japonském právním řádu.
- (76) První ochrana je zakotvena v článku 24 zákona o ochraně osobních informací, který obecně zakazuje předávání osobních údajů třetí straně mimo území Japonska bez předchozího souhlasu dotyčné fyzické osoby. Doplnkové pravidlo 4 zajišťuje, že v případě předávání údajů z Evropské unie bude tento souhlas mimořádně dobře informovaný, neboť vyžaduje, aby dotyčná fyzická osoba „poskytla informace o okolnostech předání nezbytné k tomu, aby mohl zmocnitel o svém souhlasu rozhodnout“. Na základě toho je subjekt údajů informován o skutečnosti, že údaje budou předány do zahraničí (mimo oblast působnosti zákona o ochraně osobních informací), a o konkrétní zemi určení. To subjektu údajů umožní posoudit riziko pro ochranu soukromí spojené s předáním. Jak lze rovněž dovodit z článku 23 zákona o ochraně osobních informací (viz 47. bod odůvodnění), informace poskytnuté zmocniteli by měly pokrývat povinné položky podle odstavce 2, konkrétně kategorie osobních údajů poskytovaných třetí straně a způsob zpřístupnění.
- (77) Článek 24 zákona o ochraně osobních informací použitý ve spojení s článkem 11-2 pravidel Komise pro ochranu osobních informací uvádí několik výjimek z tohoto pravidla založeného na souhlasu. Dále pak podle článku 24 se na mezinárodní předávání údajů rovněž vztahují stejné odchylky, které jsou použitelné podle čl. 23 odst. 1 zákona o ochraně osobních informací⁽⁴⁶⁾.
- (78) Pro zajištění kontinuity ochrany v případě osobních údajů předávaných z Evropské unie do Japonska podle tohoto rozhodnutí doplňkové pravidlo 4 zvyšuje úroveň ochrany pro další předávání těchto údajů podnikatelským subjektem nakládajícím s osobními informacemi příjemci ve třetí zemi. Činí tak omezením a stanovením rámce základů pro mezinárodní předávání, které může podnikatelský subjekt nakládající s osobními informacemi použít jako alternativu souhlasu. Konkrétně, a aniž by byly dotčeny odchylky stanovené v čl. 23 odst. 1 zákona o ochraně osobních informací, osobní údaje předávané podle tohoto rozhodnutí mohou být předmětem (dalšího) předávání bez souhlasu pouze ve dvou případech: i) údaje se zasílají do třetí země, kterou Komise pro ochranu osobních informací uznala podle článku 24 zákona o ochraně osobních informací jako zemi poskytující úroveň ochrany, která je rovnocenná úrovni ochrany zaručené v Japonsku⁽⁴⁷⁾, nebo ii) podnikatelský subjekt nakládající s osobními informacemi a příjemce, který je třetí stranou, společně zavedli opatření poskytující úroveň ochrany, která je rovnocenná zákonu o ochraně osobních informací ve spojení s doplňkovými pravidly, a to prostřednictvím smlouvy, jiných forem závazných dohod nebo závazných ujednání v rámci skupiny podniků. Tato druhá kategorie odpovídá nástrojům používaným podle nařízení (EU) 2016/679 pro zajištění vhodných záruk (zejména smluvní ustanovení a závazná podniková pravidla). Kromě toho, jak potvrdila Komise pro ochranu osobních informací, předání dokonce i v těchto případech podléhá obecným pravidlům použitelným pro jakékoli poskytování osobních údajů třetí straně podle zákona o ochraně osobních informací (tj. požadavek získat souhlas podle čl. 23 odst. 1 nebo alternativně požadavek na informace s možností neuplatňování podle čl. 23 odst. 2 zákona o ochraně

⁽⁴³⁾ Podle údajů zveřejněných na internetových stránkách PrivacyMark střediska JIPDEC, ze dne 2. října 2017.

⁽⁴⁴⁾ Komise pro ochranu osobních informací, seznam akreditovaných organizací pro ochranu osobních informací, k dispozici na internetových stránkách (<https://www.ppc.go.jp/personal/nintei/list/> nebo https://www.ppc.go.jp/files/pdf/nintei_list.pdf)

⁽⁴⁵⁾ Komise pro ochranu osobních informací, Přehled stavu provádění zákona o ochraně osobních informací v rozpočtovém roce 2015 (říjen 2016), k dispozici (pouze v japonštině) na internetových stránkách (https://www.ppc.go.jp/files/pdf/personal_sekougaizou_27ppc.pdf)

⁽⁴⁶⁾ Viz poznámka pod čarou č. 32.

⁽⁴⁷⁾ Podle článku 11 pravidel Komise pro ochranu osobních informací to vyžaduje nejen hmotněprávní normy, které jsou rovnocenné zákonu o ochraně osobních informací a účinně dozorované nezávislým donucovacím orgánem, ale také aby bylo zajištěno provádění příslušných pravidel ve třetí zemi.

osobních informací). V případě, že od subjektu údajů není možné získat souhlas, nebo za účelem poskytnutí požadovaných předběžných informací podle čl. 23 odst. 2 zákona o ochraně osobních informací, nemůže dojít k převodu.

- (79) Proto s výjimkou případů, kdy Komise pro ochranu osobních informací zjistila, že dotyčná třetí země zajišťuje úroveň ochrany, která je rovnocenná úrovni ochrany zaručené zákonem o ochraně osobních informací⁽⁴⁸⁾, požadavky stanovené v doplňkovém pravidle 4 vylučují použití nástrojů pro předávání, které nevytvářejí závazný vztah mezi japonským vývozcem údajů a dovozcem údajů ze třetí země a které nezaručují požadovanou úroveň ochrany. To se bude týkat například systému přeshraničních pravidel ochrany soukromí zemí Asijsko-tichomořské hospodářské spolupráce (APEC), jehož součástí je i japonská ekonomika⁽⁴⁹⁾, neboť v uvedeném systému nevyplývají ochrany z ujednání zavazujících vývozce nebo dovozce v kontextu jejich dvoustranného vztahu a jejich úroveň je zcela zřejmě nižší než úroveň zaručená kombinací zákona o ochraně osobních informací a doplňkových pravidel⁽⁵⁰⁾.
- (80) V neposlední řadě další záruka v případě (dalšího) předávání vyplývá z článků 20 a 22 zákona o ochraně osobních informací. Pokud podle těchto ustanovení subjekt ze třetí země (dovozce údajů) jedná jménem podnikatelského subjektu nakládajícího s osobními informacemi (vývozce údajů), který je (dílčím) zpracovatelem, musí tento zpracovatel zajistit dozor nad prvním uvedeným subjektem, pokud jde o bezpečnost zpracování údajů.

2.3.10 Individuální práva

- (81) Obdobně jako právní předpisy na ochranu údajů v EU také zákon o ochraně osobních informací poskytuje fyzickým osobám řadu vymahatelných práv. To zahrnuje právo na přístup („zpřístupnění“), opravu a výmaz, jakož i právo vznést námitku („ukončení používání“).
- (82) Zaprvé podle čl. 28 odst. 1 a 2 zákona o ochraně osobních informací má subjekt údajů právo požadovat, aby podnikatelský subjekt nakládající s osobními informacemi „zpřístupnil uchovávané osobní údaje, které mohou subjekt údajů identifikovat,“ a podnikatelský subjekt nakládající s osobními informacemi po přijetí takové žádosti „[...] zpřístupní subjektu údajů uchovávané osobní údaje“. Článek 29 (právo na opravu) a článek 30 (právo na ukončení používání) mají stejnou strukturu jako článek 28.
- (83) Článek 9 nařízení kabinetu stanoví, že zpřístupnění osobních informací podle čl. 28 odst. 2 zákona o ochraně osobních informací se provede písemně, pokud se podnikatelský subjekt nakládající s osobními informacemi a subjekt údajů nedohodnou jinak.
- (84) Tato práva podléhají třem typům omezení, která se týkají vlastních práv a zájmů fyzické osoby nebo práv a zájmů třetích stran⁽⁵¹⁾, vážného zásahu do podnikatelské činnosti podnikatelského subjektu nakládajícího s osobními informacemi⁽⁵²⁾, jakož i případů, kdy by zpřístupněním byly porušeny jiné právní předpisy⁽⁵³⁾. Situace, kdy by se

⁽⁴⁸⁾ Komise pro ochranu osobních informací dosud nepřijala žádné rozhodnutí podle článku 24 zákona o ochraně osobních informací uznávající, že třetí země poskytuje rovnocennou úroveň ochrany, která je zaručena v Japonsku. Jediné rozhodnutí, jehož přijetí v současnosti zvažuje, se týká EHP. Pokud jde o další případná rozhodnutí v budoucnu, bude Komise situaci pozorně sledovat a v případě potřeby přijme vhodná opatření k řešení možných nepříznivých účinků na kontinuitu ochrany (viz níže 176., 177. a 184. bod odůvodnění a čl. 3 odst. 1).

⁽⁴⁹⁾ Ačkoli se v rámci systému přeshraničních pravidel ochrany soukromí zemí APEC certifikovaly pouze dvě japonské společnosti (viz internetové stránky https://english.jipdec.or.jp/sp/protection_org/cbpr/list.html). Jedinými podnikatelskými subjekty mimo Japonsko, které se v rámci tohoto systému certifikovaly, je malý počet (23) společností z USA (viz internetové stránky <https://www.trustarc.com/consumer-resources/trusted-directory/#apec-list>).

⁽⁵⁰⁾ Neexistuje například žádná definice a konkrétní ochrany pro citlivé údaje, neexistuje žádná povinnost omezeného uchovávání údajů. Viz také pracovní skupina zřízená podle článku 29, stanovisko č. 02/2014 k referenčnímu přehledu požadavků na závazná podniková pravidla předkládaná vnitrostátním orgánům pro ochranu údajů v EU a na pravidla pro ochranu soukromí na přeshraničním základě předkládaná subjektům APEC odpovědným za pravidla pro ochranu soukromí na přeshraničním základě, 6. března 2014.

⁽⁵¹⁾ Podle Komise pro ochranu osobních informací mohou omezení ospravedlnit pouze takové zájmy, které „stojí za právní ochranu“. Toto posouzení musí být provedeno individuálně „s přihlédnutím k zásahu do základního práva na soukromí včetně ochrany údajů, jak uznává Ústava a soudní precedenty“. Chráněné zájmy mohou zahrnovat například obchodní nebo jiná obdobná tajemství.

⁽⁵²⁾ Koncept „vážného zásahu do řádného provozování podnikatelské činnosti podnikatelského subjektu“ je názorně ukázán v pokynech Komise pro ochranu osobních informací prostřednictvím různých příkladů, například opakované a totožné komplexní požadavky téže fyzické osoby, kdy tyto požadavky představují významnou zátěž pro podnikatelský subjekt, která by ohrozila jeho schopnost reagovat na jiné požadavky (pokyny Komise pro ochranu osobních informací (General Rule Edition), s. 62). Obecněji řečeno Komise pro ochranu osobních informací potvrdila, že tato kategorie je omezena na výjimečné případy, které jdou nad rámec pouhých nepřijemností. Podnikatelský subjekt nakládající s osobními informacemi zejména nemůže odmítnout zpřístupnění pouze proto, že je vyžadováno velké množství údajů.

⁽⁵³⁾ Jak potvrdila Komise pro ochranu osobních informací, takovéto právní předpisy musí respektovat právo na soukromí, jak je zajištěno Ústavou, a tedy „odrážet nezbytné a přiměřené omezení“.

tato omezení použila, jsou obdobné jako výjimky použitelné podle čl. 23 odst. 1 nařízení (EU) 2016/679, který umožňuje omezení práv fyzických osob z důvodů spojených s „ochran[ou] subjektu údajů nebo práv a svobod druhých“ nebo „jin[ých] důležit[ých] cíl[ů] obecného veřejného zájmu“. Ačkoli se kategorie případů, kdy by zpřístupněním byly porušeny „jiné právní předpisy“, může zdát široká, právní předpisy, které stanoví omezení v tomto ohledu, musí respektovat ústavní právo na ochranu soukromí a omezení mohou uložit pouze v případech, že by výkon tohoto práva představoval „zásah do veřejného blaha“⁽⁵⁴⁾. To vyžaduje vyvažování dotčených zájmů.

- (85) V čl. 28 odst. 3 zákona o ochraně osobních informací se stanoví, že pokud požadované údaje neexistují nebo pokud se dotýčný podnikatelský subjekt nakládající s osobními informacemi rozhodne přístup k uchovávaným údajům neposkytnout, musí bezodkladně informovat danou fyzickou osobu.
- (86) Zadruhé podle čl. 29 odst. 1 a 2 zákona o ochraně osobních informací má subjekt údajů právo požadovat opravu, doplnění nebo výmaz svých uchovávaných osobních údajů, pokud jsou tyto údaje nepřesné. Po přijetí takové žádosti podnikatelský subjekt nakládající s osobními informacemi „[...] provede nezbytné šetření“ a na základě výsledků tohoto šetření „provede opravu atd. obsahu uchovávaných údajů“.
- (87) Zatřetí podle čl. 30 odst. 1 a 2 zákona o ochraně osobních informací má subjekt údajů právo požadovat, aby podnikatelský subjekt nakládající s osobními informacemi přestal osobní informace používat nebo tyto informace vymazal, pokud se s nimi nakládá v rozporu s článkem 16 (týkajícím se účelového omezení) nebo pokud byly získány v rozporu s článkem 17 zákona o ochraně osobních informací (týkajícím se získání podvodem, jinými nepatřičnými prostředky nebo v případě citlivých údajů bez souhlasu). Obdobně podle čl. 30 odst. 3 a 4 zákona o ochraně osobních informací má fyzická osoba právo požadovat, aby podnikatelský subjekt nakládající s osobními informacemi přestal poskytovat informace třetí straně, pokud by tím porušoval ustanovení čl. 23 odst. 1 a článku 24 zákona o ochraně osobních informací (týkající se poskytnutí třetí straně, včetně mezinárodního předávání).
- (88) Pokud je žádost odůvodněná, podnikatelský subjekt nakládající s osobními informacemi bezodkladně přestane údaje používat nebo je poskytovat třetí straně v rozsahu nezbytném pro nápravu porušení, nebo pokud se na daný případ vztahuje výjimka (zejména pokud by ukončení používání způsobilo zvláště vysoké náklady)⁽⁵⁵⁾, zavede nezbytná alternativní opatření na ochranu práv a zájmů dotčené fyzické osoby.
- (89) Na rozdíl od práva EU zákon o ochraně osobních informací a příslušná podzákonná pravidla neobsahují právní ustanovení konkrétně řešící možnost odmítnout zpracování pro účely přímého marketingu. Shromažďování osobních údajů, na které se vztahuje toto rozhodnutí, však bude vždy probíhat v kontextu předávání osobních údajů, které byly předtím shromažďovány v Evropské unii. Podle čl. 21 odst. 2 nařízení (EU) 2016/679 má subjekt údajů vždy možnost odmítnout předání údajů pro účely zpracování pro přímý marketing. Jak je navíc vysvětleno ve 43. bodě odůvodnění, podle doplňkového pravidla 3 musí podnikatelský subjekt nakládající s osobními informacemi zpracovávat údaje získané podle tohoto rozhodnutí pro stejný účel, pro jaký byly údaje předány z Evropské unie, pokud subjekt údajů neposkytne souhlas se změnou účelu použití. Pokud byly tedy údaje předány pro jakýkoli účel kromě přímého marketingu, podnikatelský subjekt nakládající s osobními informacemi v Japonsku nesmí údaje pro účel přímého marketingu zpracovávat bez souhlasu subjektu údajů z EU.
- (90) Ve všech případech uvedených v člancích 28 a 29 zákona o ochraně osobních informací se vyžaduje, aby podnikatelský subjekt nakládající s osobními informacemi bezodkladně uvědomil danou fyzickou osobu o výsledku její žádosti, a navíc musí vysvětlit jakékoli (částečné) zamítnutí na základě zákonných výjimek stanovených v člancích 27 až 30 (článek 31 zákona o ochraně osobních informací).

⁽⁵⁴⁾ Podle výkladu Nejvyššího soudu článek 13 Ústavy stanoví právo na ochranu soukromí (viz výše uvedený 7. a 8. bod odůvodnění). Ačkoli toto právo může být omezeno v případech, které představují „zásah do veřejného blaha“, ve svém rozsudku ze dne 6. března 2008 (viz 8. bod odůvodnění) Nejvyšší soud objasnil, že jakékoli omezení (v tomto případě umožňující, aby orgán veřejné moci shromažďoval a zpracovával osobní údaje) musí být poměřováno s právem na soukromí, s přihlédnutím k faktorům, jako jsou povaha daných údajů, rizika, která zpracování těchto údajů vytváří pro fyzické osoby, příslušné záruky a výhody z hlediska veřejného zájmu, které ze zpracování vyplývají. Velmi se to podobá typu poměřování vyžadovanému podle práva EU (na základě zásady nezbytnosti a přiměřenosti) pro povolení jakéhokoli omezení práv na ochranu údajů a záruk ochrany údajů.

⁽⁵⁵⁾ Další vysvětlení těchto výjimek viz profesor Katsuya Uga, komentované znění novelizovaného zákona o ochraně osobních informací, 2015, s. 217. Příkladem žádosti, která by způsobila „vysoké výdaje“ je případ, kdy pouze některá jména na dlouhém seznamu (např. v telefonním seznamu) jsou zpracována v rozporu se zásadou účelového omezení a telefonní seznam je již v prodeji a stahování těchto výstisků a jejich nahrazení novými by bylo velmi nákladné. Pokud by ve stejném případě byly výstisky telefonního seznamu již prodány mnoha lidem a není možné je všechny stáhnout, bylo by rovněž „obtížné dosáhnout ukončení používání“. V těchto situacích by „nezbytným alternativním opatřením“ mohlo být například zveřejnění nebo distribuce oznámení o opravě. Takovéto opatření nevylučuje jiné formy (soudní) ochrany, až již v případě zásahu do práv na soukromí, poškození dobré pověsti (pomluvy) v důsledku zveřejnění nebo porušení jiných zájmů.

- (91) Pokud jde o podmínky pro podání žádosti, článek 32 zákona o ochraně osobních informací (společně s nařízením kabinetu) umožňuje, aby podnikatelský subjekt nakládající s osobními informacemi určil přiměřené postupy, a to i pokud jde o informace nezbytné k identifikaci uchovávaných osobních údajů. Podle odstavce 4 tohoto článku však podnikatelské subjekty nakládající s osobními informacemi nesmějí klást „nadměrnou zátěž na zmocnitele“. V určitých případech mohou podnikatelské subjekty nakládající s osobními informacemi rovněž stanovit poplatky, pokud jejich výše zůstane „v rozmezí považovaném za přiměřené s ohledem na skutečné náklady“ (článek 33 zákona o ochraně osobních informací).
- (92) V neposlední řadě může fyzická osoba vznést námitku proti poskytnutí svých osobních informací třetí straně podle čl. 23 odst. 2 zákona o ochraně osobních informací nebo odmítnout souhlas podle čl. 23 odst. 1 (a tím zabránit zpřístupnění, pokud by žádný jiný právní základ nebyl dostupný). Obdobně může fyzická osoba zastavit zpracování údajů pro jiný účel odmítnutím poskytnout souhlas podle čl. 16 odst. 1 zákona o ochraně osobních informací.
- (93) Na rozdíl od práva EU zákon o ochraně osobních informací a příslušná podzákonná pravidla neobsahují obecná ustanovení řešící vydávání rozhodnutí, která se dotýkají subjektu údajů a jsou založena výhradně na automatizovaném zpracování osobních údajů. Věc je však řešena v určitých odvětvových pravidlech použitelných v Japonsku, která jsou zvláště relevantní pro tento typ zpracování. To zahrnuje odvětví, v nichž se společností nejpravděpodobněji uchylují k automatizovanému zpracování osobních údajů při přijímání rozhodnutí dotýkajících se fyzických osob (např. finanční odvětví). Například „Souhrnné pokyny pro dohled nad významnými bankami“ revidované v červnu 2017 vyžadují, aby se dotyčné fyzické osobě dostalo konkrétního vysvětlení důvodů zamítnutí žádosti uzavřít smlouvu o půjčce. Uvedená pravidla tedy poskytují ochranu v pravděpodobně poměrně omezeném počtu případů, kde by automatizovaná rozhodnutí činil sám „dovážející“ japonský podnikatelský subjekt (spíše než „vyvážející“ správce údajů v EU).
- (94) V každém případě, pokud jde o osobní údaje, které byly shromážděny v Evropské unii, jakékoli rozhodnutí založené na automatizovaném zpracování bude obvykle činit správce údajů v Unii (který má přímý vztah s dotyčným subjektem údajů), a vztahuje se tedy na něj nařízení (EU) 2016/679⁽⁵⁶⁾. To zahrnuje situace předávání, kdy zpracování provádí cizí (např. japonský) podnikatelský subjekt jednající jako zprostředkovatel (zpracovatel) jménem správce z EU (nebo jako externí zpracovatel jednající jménem zpracovatele z EU, který získal údaje od správce z EU, který je shromáždil), který na tomto základě činí rozhodnutí. Neexistence zvláštních pravidel pro automatizované rozhodování v zákoně o ochraně osobních informací tedy pravděpodobně neovlivní úroveň ochrany osobních údajů předávaných podle tohoto rozhodnutí.

2.4 Dozor a vymáhání

2.4.1 Nezávislý dozor

- (95) Aby se zajistilo, že odpovídající úroveň ochrany údajů je zaručena i v praxi, měl by být zřízen nezávislý dozorový úřad oprávněný monitorovat a vymáhat dodržování pravidel v oblasti ochrany údajů. Při plnění svých povinností a výkonu své pravomoci by tento úřad měl jednat zcela nezávisle a nestranně.
- (96) V Japonsku je orgánem pověřeným monitorovat a prosazovat zákon o ochraně osobních informací Komise pro ochranu osobních informací. Tvoří ji předseda a osm komisařů jmenovaných premiérem se souhlasem obou komor parlamentu. Funkční období předsedy a každého komisaře činí pět let, s možností opětovného zvolení (článek 64 zákona o ochraně osobních informací). Komisaři mohou být odvoláni pouze z vážných důvodů v omezeném výčtu výjimečných okolností⁽⁵⁷⁾ a nesmějí se aktivně zapojovat do politické činnosti. Kromě toho podle zákona o ochraně osobních informací se musí komisaři na plný úvazek zdržet jakékoli jiné výdělečné činnosti nebo podnikatelských činností. Na komisaře se vztahují také interní pravidla, která jim brání v účasti na rozhodování v případě možného střetu zájmů. Komisi pro ochranu osobních informací je nápomocen sekretariát vedený generálním tajemníkem, který byl zřízen pro účel plnění úkolů svěřených Komisi pro ochranu osobních informací (článek 70 zákona o ochraně osobních informací). Komisaři i všichni úředníci sekretariátu jsou vázáni přísnými pravidly mlčenlivosti (články 72 a 82 zákona o ochraně osobních informací).

⁽⁵⁶⁾ Naproti tomu ve výjimečném případě, kdy japonský subjekt má přímý vztah se subjektem údajů z EU, to obvykle bude důsledek jeho cíleného sledování fyzické osoby v Evropské unii tím, že jí nabízí zboží nebo služby nebo monitoruje její chování. V tomto případě bude japonský subjekt sám spadat do oblasti působnosti nařízení (EU) 2016/679 (čl. 3 odst. 2), a musí tedy přímo dodržovat právní předpisy EU na ochranu údajů.

⁽⁵⁷⁾ Podle článku 65 zákona o ochraně osobních informací je odvolání proti vůli příslušného komisaře možné pouze z jednoho z níže uvedených důvodů: i) zahájení konkursního řízení; ii) odsouzení za porušení zákona o ochraně osobních informací nebo zákona o používání čísel; iii) odsouzení k trestu odnětí svobody bez nařízeného výkonu práce nebo k ještě přísnějšímu trestu; iv) nezpůsobilost k výkonu povinností z důvodu duševní nebo tělesné poruchy nebo profesního pochybení.

- (97) Pravomoci Komise pro ochranu osobních informací, které tato komise vykonává zcela nezávisle⁽⁵⁸⁾, jsou stanoveny zejména v článcích 40, 41 a 42 zákona o ochraně osobních informací. Podle článku 40 může Komise pro ochranu osobních informací požadovat, aby podnikatelské subjekty nakládající s osobními informacemi podávaly zprávy nebo předkládaly dokumenty o operacích zpracování, a může rovněž provádět kontroly, a to jak na místě, tak účetních knih nebo jiných dokumentů. V rozsahu nezbytném pro prosazování zákona o ochraně osobních informací může Komise pro ochranu osobních informací rovněž poskytovat podnikatelským subjektům nakládajícím s osobními informacemi pokyny nebo poradenství, pokud jde o nakládání s osobními informacemi. Komise pro ochranu osobních informací již využila tuto pravomoc na základě článku 41 zákona o ochraně osobních informací, když společnost Facebook v návaznosti na odhalení v souvislosti s případem Facebook / Cambridge Analytica adresovala pokyny.
- (98) Komise pro ochranu osobních informací je zejména oprávněna (pokud jedná na základě stížnosti nebo z vlastní iniciativy) v jednotlivých případech vydávat doporučení a příkazy za účelem prosazování zákona o ochraně osobních informací a jiných závazných pravidel (včetně doplňkových pravidel). Tyto pravomoci stanoví článek 42 zákona o ochraně osobních informací. Zatímco odstavce 1 a 2 uvedeného zákona stanoví dvoustupňový mechanismus, kterým může Komise pro ochranu osobních informací vydat příkaz (pouze) po předchozím doporučení, odstavec 3 v naléhavých případech umožňuje přímé vydání příkazu.
- (99) Ačkoli ne všechna ustanovení oddílu 1 kapitoly IV zákona o ochraně osobních informací jsou uvedena v čl. 42 odst. 1, který rovněž určuje oblast působnosti čl. 42 odst. 2, lze to vysvětlit skutečností, že některá z těchto ustanovení se netýkají povinností podnikatelského subjektu nakládajícího s osobními informacemi⁽⁵⁹⁾ a že všechny zásadní ochrany již poskytují jiná ustanovení, která jsou v uvedeném seznamu zahrnuta. Ačkoli například článek 15 (vyžadující, aby podnikatelský subjekt nakládající s osobními informacemi stanovil účel použití a příslušné osobní informace zpracovával výlučně v rozsahu tohoto účelu) není zmíněn, nedodržení tohoto požadavku může být důvodem k vydání doporučení na základě porušení čl. 16 odst. 1 (zakazujícího, aby podnikatelský subjekt nakládající s osobními informacemi zpracovával osobní informace nad rámec toho, co je nezbytné pro dosažení účelu použití, pokud nezíská souhlas subjektu údajů)⁽⁶⁰⁾. Další ustanovení neuvedené v čl. 42 odst. 1 je článek 19 zákona o ochraně osobních informací týkající se přesnosti a uchovávání údajů. Nedodržování tohoto ustanovení může být vymáháno buď jako porušení čl. 16 odst. 1, nebo na základě porušení čl. 29 odst. 2, pokud dotyčná fyzická osoba požádá o opravu nebo výmaz chybných nebo nadbytečných údajů a podnikatelský subjekt nakládající s osobními informacemi odmítne této žádosti vyhovět. Pokud jde o práva subjektu údajů podle čl. 28 odst. 1, čl. 29 odst. 1 a čl. 30 odst. 1, dozor ze strany Komise pro ochranu osobních informací je zajištěn tím, že této komisi byly uděleny vymáhací pravomoci, pokud jde o odpovídající povinnosti podnikatelského subjektu nakládajícího s osobními informacemi stanovenými v uvedených článcích.
- (100) Podle čl. 42 odst. 1 zákona o ochraně osobních informací může Komise pro ochranu osobních informací, pokud uzná, že existuje „potřeba chránit práva a zájmy fyzické osoby v případech, kdy [podnikatelský subjekt nakládající s osobními informacemi] porušil“ konkrétní ustanovení zákona o ochraně osobních informací, vydat doporučení „pozastavit porušující jednání nebo přijmout jiná nezbytná opatření k nápravě porušení“. Takové doporučení není závazné, ale otevírá cestu pro závazný příkaz podle čl. 42 odst. 2 zákona o ochraně osobních informací. Pokud na základě tohoto ustanovení není doporučení „bez legitimních důvodů“ dodrženo a Komise pro ochranu osobních informací „uzná, že hrozí závažné porušení práv a zájmů fyzické osoby“, může nařídit, aby podnikatelský subjekt nakládající s osobními informacemi přijal opatření v souladu s doporučením.
- (101) Doplňková pravidla dále objasňují a posilují vymáhací pravomoci Komise pro ochranu osobních informací. Konkrétně v případech zahrnujících údaje dovážené z Evropské unie bude Komise pro ochranu osobních informací vždy považovat skutečnost, že podnikatelský subjekt nakládající s osobními informacemi bez legitimního důvodu nepřijal opatření v souladu s doporučením vydaným Komisí pro ochranu osobních informací podle čl. 42 odst. 1, za závažné a bezprostřední porušení práv a zájmů fyzické osoby ve smyslu čl. 42 odst. 2, a tedy za porušení vyžadující vydání závazného příkazu. Kromě toho Komise pro ochranu osobních informací uzná jako „legitimní důvod“ nesplnění doporučení pouze „údátost mimořádné povahy [zabraňující splnění] mimo kontrolu [podnikatelského subjektu nakládajícího s osobními informacemi], kterou nelze rozumně předpokládat (například přírodní katastrofy),“ nebo případy, kdy potřeba přijmout opatření v souvislosti s doporučením „zanikla, neboť [podnikatelský subjekt nakládající s osobními informacemi] přijal alternativní opatření, která zajistila úplnou nápravu porušení“.

⁽⁵⁸⁾ Viz článek 62 zákona o ochraně osobních informací.

⁽⁵⁹⁾ Například některá ustanovení se týkají opatření podnikatelského subjektu nakládajícího s osobními informacemi, která jsou nepovinná (články 32 a 33 zákona o ochraně osobních informací), nebo povinností „maximálního úsilí“, které jsou jako takové nevyhnutelné (články 31 a 35, čl. 36 odst. 6 a článek 39 zákona o ochraně osobních informací). Určitá ustanovení nejsou určena pro podnikatelský subjekt nakládající s osobními informacemi, ale pro jiné činitele. To se týká například čl. 23 odst. 4, čl. 26 odst. 2 a článku 34 zákona o ochraně osobních informací (vymáhání čl. 26 odst. 2 zákona o ochraně osobních informací je však zajištěno možností trestních sankcí podle čl. 88 bodu i) zákona o ochraně osobních informací).

⁽⁶⁰⁾ Jak je navíc vysvětleno ve 48. bodě odůvodnění, v kontextu předání bude „účel použití“ stanoven vývozcem údajů z EU, který je v tomto ohledu vázán povinností podle čl. 5 odst. 1 písm. b) nařízení (EU) 2016/679. Uvedená povinnost je vymahatelná příslušným úřadem pro ochranu osobních údajů v Evropské unii.

- (102) Nesplnění příkazu Komise pro ochranu osobních informací se považuje za trestný čin podle článku 84 zákona o ochraně osobních informací a podnikatelský subjekt nakládající s osobními informacemi, který bude shledán vinným, může být potrestán odnětím svobody s nařízeným výkonem práce až na dobu šesti měsíců nebo peněžitým trestem až do výše 300 000 jenů. Navíc podle čl. 85 bodu i) zákona o ochraně osobních informací je nedostatečná spolupráce s Komisí pro ochranu osobních informací nebo bránění v jejím vyšetřování postihnutelné peněžitým trestem až do výše 300 000 jenů. Tyto trestní sankce se uplatňují jako doplněk k sankcím, které mohou být uloženy za závažná porušení zákona o ochraně osobních informací (viz 108. bod odůvodnění).

2.4.2 Soudní ochrana

- (103) Aby se zajistila odpovídající ochrana, a zejména vymáhání individuálních práv, měla by být subjektu údajů poskytnuta účinná správní a soudní ochrana, včetně náhrady škody.
- (104) Dříve než fyzická osoba požádá o správní nebo soudní ochranu, nebo namísto ní, může se rozhodnout podat stížnost na zpracování svých osobních údajů samotnému správci. Na základě článku 35 zákona o ochraně osobních informací se podnikatelské subjekty nakládající s osobními informacemi snaží takové stížnosti vyřídit „přiměřeně a neprodleně“ a pro dosažení tohoto cíle zavedou interní systémy vyřizování stížností. Kromě toho podle čl. 61 bodu ii) zákona o ochraně osobních informací je Komise pro ochranu osobních informací odpovědná za „nezbytnou mediaci, pokud jde o podanou žádost a spolupráci nabídnutou podnikatelskému subjektu, který se stížností zabývá“, což v obou případech zahrnuje stížnosti podané cizinci. V této souvislosti japonský zákonodárce také pověřil ústřední vládní instituce úkolem přijmout „nezbytná opatření“ s cílem umožnit a usnadnit řešení stížností podnikatelskými subjekty nakládajícími s osobními informacemi (článek 9), zatímco místní vládní instituce se v takových případech snaží zajistit mediaci (článek 13). V tomto ohledu mohou fyzické osoby vedle možnosti podat stížnost k Národnímu centru pro spotřebitelské záležitosti Japonska podat stížnost k jednomu z více než 1 700 spotřebitelských center zřízených místními vládními institucemi na základě zákona o bezpečnosti spotřebitele ⁽⁶¹⁾. Tyto stížnosti lze podat i v souvislosti s porušením zákona o ochraně osobních informací. Podle článku 19 základního spotřebitelského zákona ⁽⁶²⁾ se místní vládní instituce v souvislosti se stížnostmi snaží zapojit do mediace a poskytovat stranám nezbytné odborné konzultace. Tyto mechanismy řešení sporů se zdají být celkem účinné: v roce 2015 se řešilo více než 75 000 případů stížností s mírou úspěšnosti 91,2 %.
- (105) Porušení ustanovení zákona o ochraně osobních informací podnikatelským subjektem nakládajícím s osobními informacemi může vést k podání občanskoprávní žaloby, jakož i k zahájení trestního řízení a sankcím. Zaprvé, pokud má fyzická osoba za to, že její práva podle článků 28, 29 a 30 zákona o ochraně osobních informací byla porušena, může se obrátit na soud a požádat o vydání příkazu, aby podnikatelský subjekt nakládající s osobními informacemi splnil její požadavek podle jednoho z těchto ustanovení, tj. zpřístupnil uchovávané osobní údaje (článek 28), provedl opravu osobních údajů, které jsou nesprávné, (článek 29) nebo ukončil protiprávní zpracování nebo poskytování třetí straně (článek 30). Tuto žalobu lze podat, aniž by bylo nutné vycházet z článku 709 občanského zákoníku ⁽⁶³⁾ nebo jinak z práva občanskoprávních deliktů ⁽⁶⁴⁾. To zejména znamená, že fyzická osoba nemusí prokazovat jakoukoli újmu.
- (106) Zadruhé v případě, kdy se údajné porušení netýká individuálních práv podle článků 28, 29 a 30, ale obecných zásad ochrany údajů nebo povinností podnikatelského subjektu nakládajícího s osobními informacemi, dotyčná fyzická osoba může podat občanskoprávní žalobu proti podnikatelskému subjektu na základě ustanovení o občanskoprávních deliktech japonského občanského zákoníku, zejména článku 709. Zatímco soudní spor podle článku 709 vyžaduje kromě zavinění (úmysl nebo nedbalost) i prokázání újmy, podle článku 710 občanského zákoníku může být tato újma hmotná i nehmotná. Pokud jde o výši odškodnění, není stanoveno žádné omezení.
- (107) Pokud jde o dostupné právní prostředky, článek 709 japonského občanského zákoníku odkazuje na peněžitě odškodnění. Japonská judikatura však tento článek vykládá také jako právo dosáhnout soudního příkazu nebo zákazu ⁽⁶⁵⁾. Pokud tedy subjekt údajů podá žalobu podle článku 709 občanského zákoníku a tvrdí, že jeho práva nebo zájmy byly poškozeny porušením ustanovení zákona o ochraně osobních informací ze strany žalovaného, tato žaloba může kromě odškodnění zahrnovat žádost o vydání soudního příkazu, zejména příkazu, jehož cílem je zastavit jakékoli protiprávní zpracování.

⁽⁶¹⁾ Zákon č. 50 ze dne 5. června 2009.

⁽⁶²⁾ Zákon č. 60 ze dne 22. srpna 2012.

⁽⁶³⁾ Článek 709 občanského zákoníku je základem pro občanskoprávní spory o náhradu škody. Podle tohoto ustanovení „osoba, která úmyslně nebo z nedbalosti poruší jakékoli právo druhých nebo právně chráněný zájem druhých, je povinna nahradit veškeré škody, které v důsledku jejího jednání vzniknou“.

⁽⁶⁴⁾ Rozsudek Vrchního soudu v Tokiu ze dne 20. května 2015 (nezveřejněný); rozsudek Okresního soudu v Tokiu ze dne 8. září 2014, Westlaw Japan 2014WLJPCA09088002. Viz také čl. 34 odst. 1 a 3 zákona o ochraně osobních informací.

⁽⁶⁵⁾ Viz rozsudek Nejvyššího soudu ze dne 24. září 2002, Hanrei Times, sv. 1106, s. 72.

- (108) Zatřetí kromě právních prostředků v oblasti občanského práva (práva občanskoprávních deliktů) může subjekt údajů podat stížnost ke státnímu zástupci nebo příslušníku soudní policie, pokud jde o porušení zákona o ochraně osobních informací, která může vést k trestním sankcím. Kapitola VII zákona o ochraně osobních informací obsahuje řadu trestních ustanovení. Nejdůležitější z nich (článek 84) se týká nedodržování příkazů Komise pro ochranu osobních informací ze strany podnikatelského subjektu nakládajícího s osobními informacemi podle čl. 42 odst. 2 a 3. Pokud podnikatelský subjekt nesplní příkaz vydaný Komisí pro ochranu osobních informací, předseda této komise (jakož i všichni ostatní státní úředníci) ⁽⁶⁶⁾ mohou věc předložit státnímu zástupci nebo příslušníku soudní policie, a tím vyvolat trestní řízení. Sankcí za porušení příkazu Komise pro ochranu osobních informací je trest odnětí svobody s nařízeným výkonem práce až na dobu šesti měsíců nebo peněžitý trest až do výše 300 000 jenů. Ostatní ustanovení zákona o ochraně osobních informací, která stanoví sankce pro případ porušení zákona o ochraně osobních informací dotýkajících se práv a zájmů subjektů údajů, zahrnují článek 83 zákona o ochraně osobních informací (týkající se „poskytování nebo používání“ databáze osobních informací „získané krádeží“ „pro účely dosažení [...] nezákonných zisků“) a čl. 88 bod i) zákona o ochraně osobních informací (týkající se případů, kdy třetí strana neinformuje podnikatelský subjekt nakládající s osobními informacemi, jakmile tento subjekt obdrží osobní údaje v souladu s čl. 26 odst. 1 zákona o ochraně osobních informací, zejména o tom, jak třetí strana tyto údaje sama získala). Použitelnými sankcemi za tato porušení zákona o ochraně osobních informací jsou trest odnětí svobody s nařízeným výkonem práce až na dobu jednoho roku nebo pokuta až do výše 500 000 jenů (v případě článku 83) nebo správní pokuta až do výše 100 000 jenů (v případě čl. 88 bodu i)). Ačkoli hrozba trestní sankce již pravděpodobně má silný odrazující účinek na vedení podniků, které řídí operace zpracování podnikatelského subjektu nakládajícího s osobními informacemi, jakož i na fyzické osoby nakládající s údaji, článek 87 zákona o ochraně osobních informací objasňuje, že pokud zástupce, zaměstnanec nebo jiný pracovník právnické osoby poruší články 83 až 85 zákona o ochraně osobních informací, „se pachatel potrestá a dané právnické osobě se uloží pokuta stanovená v příslušných člancích“. V tomto případě lze zaměstnanci i společnosti uložit sankce až do plné maximální výše.
- (109) V neposlední řadě mohou fyzické osoby požádat o právní ochranu v souvislosti s činností nebo nečinností Komise pro ochranu osobních informací. V tomto ohledu japonské právo stanoví několik způsobů správní a soudní ochrany.
- (110) Pokud není fyzická osoba spokojena s činností Komise pro ochranu osobních informací, může podat správní opravný prostředek podle zákona o přezkumu správních stížností ⁽⁶⁷⁾. Pokud má naopak fyzická osoba za to, že Komise pro ochranu osobních informací měla jednat, ale neučinila tak, může fyzická osoba Komisi pro ochranu osobních informací podle článku 36-3 uvedeného zákona požádat, aby vydala rozhodnutí nebo poskytla správní pokyn, pokud má za to, že „rozhodnutí nebo správní pokyn nezbytné pro nápravu porušení nebyly vydány nebo uloženy“.
- (111) Pokud jde o soudní ochranu, podle zákona o správních sporech může fyzická osoba, která není spokojena se správním rozhodnutím vydaným Komisí pro ochranu osobních informací, podat žalobu *mandamus* ⁽⁶⁸⁾ a žádat, aby soud Komisi pro ochranu osobních informací nařídil učinit další kroky ⁽⁶⁹⁾. V určitých případech může soud také vydat předběžný příkaz (*mandamus*), aby zabránil nezvratné újmě ⁽⁷⁰⁾. Kromě toho podle téhož zákona může fyzická osoba požádat o zrušení rozhodnutí Komise pro ochranu osobních informací ⁽⁷¹⁾.
- (112) V neposlední řadě může fyzická osoba podat proti Komisi pro ochranu osobních informací žalobu o náhradu škody státem podle čl. 1 odst. 1 zákona o státní ochraně v případě, že této fyzické osobě vznikla škoda z důvodu skutečnosti, že příkaz vydaný Komisí pro ochranu osobních informací vůči podnikatelskému subjektu byl proti právní nebo Komise pro ochranu osobních informací neuplatnila svou pravomoc.

3. PŘÍSTUP K OSOBNÍM ÚDAJŮM PŘEDÁVANÝM Z EVROPSKÉ UNIE A JEJICH POUŽITÍ ORGÁNY VEŘEJNÉ MOCI V JAPONSKU

- (113) Komise také posuzovala omezení a záruky, včetně dozoru a jednotlivých ochranných mechanismů dostupných v japonském právu, pokud jde o shromažďování a následné používání osobních údajů předávaných podnikatelským subjektům v Japonsku orgány veřejné moci pro účely veřejného zájmu, zejména pro účely prosazování trestního práva a národní bezpečnosti („přístup vlády“). V tomto ohledu japonská vláda předložila Komisi oficiální prohlášení, ujištění a závazky podepsané na nejvyšší úrovni ministerstev a orgánů, které jsou obsaženy v příloze II tohoto rozhodnutí.

⁽⁶⁶⁾ Ustanovení čl. 239 odst. 2 trestního řádu.

⁽⁶⁷⁾ Zákon č. 160 z roku 2014.

⁽⁶⁸⁾ Článek 37-2 zákona o správních sporech.

⁽⁶⁹⁾ Podle čl. 3 odst. 6 zákona o správních sporech se pojem „žaloba *mandamus*“ vztahuje k žalobě o vydání příkazu, kterým soud nařídí správnímu orgánu, aby vydal původní správní rozhodnutí, které „měl“ vydat, ale neučinil tak.

⁽⁷⁰⁾ Článek 37-5 zákona o správních sporech.

⁽⁷¹⁾ Oddíl 1 kapitoly II zákona o správních sporech.

3.1 Obecný právní rámec

- (114) V rámci výkonu veřejné moci musí být při přístupu vlády v Japonsku v plném rozsahu dodržovány právní předpisy (zásada zákonnosti). V tomto ohledu Ústava Japonska obsahuje ustanovení omezující a poskytující rámec pro shromažďování osobních údajů orgány veřejné moci. Jak již bylo zmíněno, pokud jde o zpracování podnikatelskými subjekty, Nejvyšší soud Japonska na základě článku 13 Ústavy, který mimo jiné chrání právo na svobodu, uznal právo na soukromí a ochranu údajů⁽⁷²⁾. Důležitým aspektem uvedeného práva je svoboda neumožnit zpřístupnění svých osobních informací třetí straně bez souhlasu⁽⁷³⁾. To znamená právo na účinnou ochranu osobních údajů před zneužitím a (zejména) neoprávněným přístupem. Doplňková ochrana je zajištěna článkem 35 Ústavy, který se týká práva všech osob na ochranu svobody domovní, písemností a majetku, což vyžaduje, aby orgány veřejné moci získaly soudní příkaz vydaný na základě „přiměřeného důvodu“⁽⁷⁴⁾ ve všech případech „prohlídky a zajištění věci“. Ve svém rozsudku ze dne 15. března 2017 (věc GPS) Nejvyšší soud objasnil, že tento požadavek na soudní příkaz se uplatní, kdykoli vláda zasahuje („vstupuje“) do soukromé sféry způsobem, který potlačuje vůli fyzické osoby, tedy „povinným vyšetřováním“. Soudce může takový příkaz vydat pouze na základě konkrétního podezření z trestného činu, tj. pokud jsou mu předloženy listinné důkazy, na jejichž základě může být osoba, které se vyšetřování týká, považována za osobu, která spáchala trestný čin⁽⁷⁵⁾. Japonské orgány tedy nemají žádnou zákonnou pravomoc shromažďovat osobní informace povinnými prostředky v situacích, kdy k porušení právních předpisů zatím nedošlo⁽⁷⁶⁾, například aby zabránily trestnému činu nebo jiné bezpečnostní hrozbě (jako je tomu při vyšetřování z důvodu národní bezpečnosti).
- (115) S výhradou právních zásad musí být jakékoli shromažďování údajů v rámci donucovacího vyšetřování konkrétně podloženo právními předpisy (například čl. 197 odst. 1 trestního řádu, který se týká povinného shromažďování informací pro účely trestního vyšetřování). Tento požadavek se vztahuje také na přístup k elektronickým informacím.
- (116) Důležité je, že čl. 21 odst. 2 Ústavy zaručuje důvěrnost všech komunikačních prostředků s tím, že omezení mohou stanovit pouze právní předpisy z důvodu veřejného zájmu. Článek 4 zákona o telekomunikacích, podle kterého nesmí být porušena důvěrnost sdělení, s nimiž nakládá provozovatel telekomunikačních sítí, zavádí tento požadavek důvěrnosti na úrovni zákona. To je vykládáno jako zákaz zpřístupnění komunikačních informací, pokud neexistuje souhlas uživatelů nebo pokud toto zpřístupnění nevychází z výslovných výjimek z trestní odpovědnosti podle trestního zákoníku⁽⁷⁷⁾.
- (117) Ústava také zaručuje právo na přístup k soudům (článek 32) a právo žalovat stát o náhradu škody v případě, kdy fyzické osobě vznikne škoda protiprávním jednáním úřední osoby (článek 17).
- (118) Pokud jde konkrétně o právo na ochranu údajů, oddíly 1, 2 a 3 kapitoly III zákona o ochraně osobních informací stanoví obecné zásady vztahující se na všechna odvětví, včetně veřejného sektoru. Zejména článek 3 zákona o ochraně osobních informací stanoví, že se všemi osobními informacemi musí být nakládáno v souladu se zásadou respektování osobnosti fyzické osoby. Jakmile orgány veřejné moci osobní informace, i jako součást elektronických záznamů, shromáždí („získají“) ⁽⁷⁸⁾, nakládání s nimi se řídí zákonem o ochraně osobních informací

⁽⁷²⁾ Viz například rozsudek Nejvyššího soudu ze dne 12. září 2003, věc č. 1656 (2002 (Ju)). Nejvyšší soud zejména konstatoval, že „každý jednotlivec může svobodně chránit své osobní informace před bezdůvodným zpřístupněním třetí straně nebo zveřejněním“.

⁽⁷³⁾ Rozsudek Nejvyššího soudu ze dne 6. března 2008 (Juki-net).

⁽⁷⁴⁾ „Přiměřený důvod“ existuje pouze v případě, že dotčená fyzická osoba (podezřelý, obviněný) je považována za osobu, která spáchala trestný čin, a prohlídka a zajištění věci jsou nezbytné pro vyšetřování trestného činu. Viz například rozsudek Nejvyššího soudu ze dne 18. března 1969, věc č. 100 (1968 (Shi)).

⁽⁷⁵⁾ Viz čl. 156 odst. 1 pravidel trestního řízení.

⁽⁷⁶⁾ Je však zapotřebí poznamenat, že zákon o trestání organizovaného zločinu a o kontrole výnosů z trestné činnosti ze dne 15. června 2017 zavádí nový trestný čin, který kriminalizuje přípravu teroristických činů a určitých jiných forem organizovaného zločinu. Vyšetřování může být zahájeno pouze v případě konkrétního podezření, na základě důkazů, že všechny nezbytné podmínky zakládající trestný čin (zapojení organizované zločinecké skupiny, akt „plánování“ a akt „přípravy“ trestného činu) jsou splněny. Viz také např. články 38–40 zákona o předcházení podvratným činnostem (zákon č. 240 ze dne 21. července 1952).

⁽⁷⁷⁾ Ustanovení čl. 15 odst. 8 pokynů k ochraně osobních informací v odvětví telekomunikací.

⁽⁷⁸⁾ Správní orgány, jak jsou vymezeny v čl. 2 odst. 1 zákona o ochraně osobních informací uchovávaných správními orgány. Podle informací obdržенých od japonské vlády se definice „správní orgány“ vztahuje na všechny orgány veřejné moci s výjimkou prefekturní policie. Prefekturní policie zároveň působí v právním rámci daném prefekturními nařízeními, která se týkají ochrany osobních informací (viz článek 11 zákona o ochraně osobních informací a základní politika) a obsahují ustanovení na ochranu osobních informací rovnocenná zákonu o ochraně osobních informací uchovávaných správními orgány. Viz příloha II, oddíl I. písm. B. Jak vysvětlila Komise pro ochranu osobních informací, podle „základní politiky“ musí být tato nařízení schválena na základě obsahu zákona o ochraně osobních informací uchovávaných správními orgány a Ministerstvo vnitra a komunikací vydává oznámení, kterými v tomto ohledu poskytuje místním vládním institucím nezbytné pokyny. Jak zdůraznila Komise pro ochranu osobních informací, „[v] rámci těchto omezení musí být nařízení týkající se ochrany osobních informací v každé prefektuře stanoveno [...] na základě základní politiky a obsahu oznámení“.

uchovávaných správními orgány⁽⁷⁹⁾. To v zásadě zahrnuje⁽⁸⁰⁾ také zpracování osobních informací pro účely prosazování trestního práva nebo národní bezpečnosti. Zákon o ochraně osobních informací uchovávaných správními orgány mimo jiné stanoví, že orgány veřejné moci: i) mohou osobní informace uchovávat pouze v rozsahu nezbytném pro plnění svých povinností; ii) tyto informace nepoužijí k „neoprávněnému“ účelu nebo je bezdůvodně nepřístupní třetí osobě; iii) stanoví účel a tento účel nezmění nad rámec toho, co lze přiměřeně považovat za relevantní pro původní účel (účelové omezení); iv) uchovávané osobní informace v zásadě nepoužijí ani je neposkytnou třetí straně pro jiné účely, a pokud to považují za nutné, stanoví omezení účelu nebo způsobu použití třetími stranami; v) usilují o zajištění správnosti informací (kvalita údajů); vi) přijmou nezbytná opatření pro řádnou správu informací a k zamezení jejich úniku, ztráty nebo poškození (zabezpečení údajů) a vii) usilují o řádné a rychlé vyřizování jakýchkoli stížností týkajících se zpracování informací⁽⁸¹⁾.

3.2 Přístup japonských orgánů veřejné moci k osobním údajům a jejich použití těmito orgány pro účely prosazování trestního práva

- (119) Japonské právo obsahuje řadu omezení přístupu k osobním údajům a použití těchto údajů pro účely prosazování trestního práva, jakož i dozorové a ochranné mechanismy, které poskytují dostatečné záruky k tomu, aby byly tyto údaje účinně ochráněny před nezákonnými zásahy a rizikem zneužití.

3.2.1 Právní základ a použitelná omezení/záruky

- (120) V japonském právním rámci je shromažďování elektronických informací pro účely prosazování trestního práva přípustné na základě příkazu (povinné shromažďování) nebo žádosti o dobrovolné zpřístupnění.

3.2.1.1 Povinné vyšetřování na základě soudního příkazu

- (121) Jak je uvedeno ve 115. bodě odůvodnění, jakékoli shromažďování údajů v rámci donucovacího vyšetřování musí být konkrétně podloženo právními předpisy a může být prováděno pouze se soudním příkazem „vydaným na základě přiměřeného důvodu“ (článek 35 Ústavy). Pokud jde o vyšetřování trestných činů, tento požadavek se odráží v ustanoveních trestního řádu. Podle čl. 197 odst. 1 trestního řádu se povinná opatření „nepoužijí, pokud trestní řád neobsahuje zvláštní ustanovení“. Pokud jde o shromažďování elektronických informací, jedinými relevantními⁽⁸²⁾ právními základy v tomto ohledu jsou článek 218 trestního řádu (prohlídka a zajištění věci) a článek 222-2 trestního řádu, podle nichž se povinná opatření pro odposlech elektronických komunikací bez souhlasu druhé strany provádějí na základě jiných zákonů, konkrétně zákona o odposleších pro trestní vyšetřování (dále jen „zákon o odposleších“). V obou případech se použije požadavek soudního příkazu.
- (122) Konkrétně podle čl. 218 odst. 1 trestního řádu může státní zástupce, asistent státního zástupce nebo příslušník soudní policie, pokud je to nezbytné pro vyšetřování trestného činu, provést prohlídku nebo zajištění věci (včetně nařízení záznamu) na základě příkazu předem vydaného soudcem⁽⁸³⁾. Takový příkaz mimo jiné obsahuje jméno podezřelého nebo obviněného, trestný čin, z něhož je obviněn⁽⁸⁴⁾, elektromagnetické záznamy, které mají být zajištěny, a „místo nebo věci“, které mají být předmětem prohlídky (čl. 219 odst. 1 trestního řádu).

⁽⁷⁹⁾ Osobní informace získané úředníky správního orgánu při plnění svých povinností a uchovávané uvedeným správním orgánem pro organizační účely spadají do definice „uchovávaných osobních informací“ ve smyslu čl. 2 odst. 3 zákona o ochraně osobních informací uchovávaných správními orgány, pokud jsou zaznamenány ve „správních dokumentech“. To zahrnuje elektronické shromažďování informací a jejich následné zpracování těmito orgány, neboť definice „správních dokumentů“ v čl. 2 odst. 2 zákona o přístupu k informacím uchovávaným správními orgány (zákon č. 42 z roku 1999) zahrnuje elektromagnetické záznamy.

⁽⁸⁰⁾ Podle článku 53-2 trestního řádu je však kapitola IV zákona o ochraně osobních informací uchovávaných správními orgány vyloučena pro „dokumenty týkající se soudních řízení“, které podle obdržených informací obsahují elektronické informace získané na základě příkazu nebo žádosti o dobrovolnou spolupráci v rámci trestního vyšetřování. Obdobně, pokud jde o informace shromažďované v oblasti národní bezpečnosti, fyzické osoby nebudou schopny úspěšně uplatňovat svá práva podle zákona o ochraně osobních informací uchovávaných správními orgány, pokud má vedoucí orgánu veřejné moci „přiměřené důvody“ se domnívat, že „zpřístupnění“ pravděpodobně naruší národní bezpečnost (viz čl. 14 bod iv)). Vzhledem k tomu musí orgány veřejné moci informace zpřístupnit pokud možno alespoň částečně (článek 15).

⁽⁸¹⁾ Viz konkrétní odkazy na zákon o ochraně osobních informací uchovávaných správními orgány v příloze II, oddíl II. písm. A. bod 1 písm. b) bod 2.

⁽⁸²⁾ Ačkoli článek 220 trestního řádu povoluje prohlídku a zajištění věci „na místě“ bez soudního příkazu, pokud státní zástupce, asistent státního zástupce nebo příslušník soudní policie zadrží podezřelého / zjevného pachatele, není to v kontextu předávání, a tedy pro účely tohoto rozhodnutí, relevantní.

⁽⁸³⁾ Podle čl. 222 odst. 1 ve spojení s článkem 110 trestního řádu musí být příkaz k prohlídce / zajištění věci pro účely záznamu předložen osobě, která se má tomuto opatření podrobit.

⁽⁸⁴⁾ Viz také čl. 189 odst. 2 trestního řádu, podle kterého příslušník soudní policie vyšetřuje pachatele a příslušné důkazy, „pokud se domnívá, že trestný čin byl spáchán“. Obdobně čl. 155 odst. 1 pravidel trestního řízení vyžaduje, aby písemná žádost o vydání soudního příkazu mimo jiné obsahovala „trestný čin, z něhož je pachatel obviněn,“ a „shrnutí skutkového stavu“.

- (123) Pokud jde o odposlechy komunikace, článek 3 zákona o odposleších tato opatření umožňuje pouze při dodržení přísných požadavků. Orgány veřejné moci musí zejména získat předchozí soudní příkaz, který může být vydán pouze v návaznosti na vyšetřování určitých závažných trestných činů (uvedených v příloze zákona) ⁽⁸⁵⁾, a pokud je „mimořádně obtížné identifikovat pachatele trestného činu nebo objasnit situace/podrobnosti spáchání trestného činu jinými prostředky“ ⁽⁸⁶⁾. Podle článku 5 zákona o odposleších se soudní příkaz vydává na omezenou dobu a soudce může uložit dodatečné podmínky. V zákoně o odposleších se navíc stanovuje řada dalších záruk, jako například nezbytná přítomnost svědků (články 12 a 20), zákaz odposlouchávání komunikace určitých privilegovaných skupin (např. lékařů a právníků) (článek 15), povinnost ukončit odposlech, pokud již není odůvodněný, a to dokonce i po dobu platnosti soudního příkazu (článek 18) nebo obecný požadavek informovat dotčenou osobu a umožnit přístup k záznamům do třiceti dnů od ukončení odposlechu (články 23 a 24).
- (124) U všech povinných opatření na základě příkazu může být výslech proveden (čl. 197 odst. 1 trestního řádu) pouze „v rozsahu nezbytném pro dosažení jeho cíle“, to znamená, pokud nelze cíl sledovaných vyšetřování dosáhnout jinak. Ačkoli kritéria pro určení nezbytnosti nejsou v právních předpisech dále specifikována, Nejvyšší soud Japonska konstatoval, že soudce vydávající soudní příkaz by měl celkově posoudit a vzít v úvahu zejména i) závažnost trestného činu a způsob jeho spáchání; ii) hodnotu a důležitost materiálů, které mají být zajištěny jako důkaz; iii) pravděpodobnost (riziko), že důkazy mohou být ukryty nebo zničeny, a iv) rozsah, v jakém může zajištění věci způsobit újmu dotyčné fyzické osobě ⁽⁸⁷⁾.

3.2.1.2 Žádost o dobrovolné zpřístupnění na základě „žádosti o zpřístupnění informací“

- (125) V mezích své pravomoci mohou orgány veřejné moci rovněž shromažďovat elektronické informace na základě žádostí o dobrovolné zpřístupnění. To se vztahuje k nepovinné formě spolupráce, kdy vyhovění žádosti nelze vymáhat ⁽⁸⁸⁾, a orgány veřejné moci jsou tak zbaveny povinnosti získat soudní příkaz.
- (126) Pokud je tato žádost určena podnikatelskému subjektu a týká se osobních informací, podnikatelský subjekt musí splnit požadavky zákona o ochraně osobních informací. Podle čl. 23 odst. 1 zákona o ochraně osobních informací mohou podnikatelské subjekty zpřístupnit osobní informace třetím stranám bez souhlasu dotyčné fyzické osoby pouze v určitých případech, včetně případů, kdy zpřístupnění těchto informací „vychází z právních předpisů“ ⁽⁸⁹⁾. V oblasti prosazování trestního práva je právní základ pro tyto žádosti uveden v čl. 197 odst. 2 trestního řádu, podle kterého „mohou být soukromé organizace požádány, aby podaly zprávy o nezbytných záležitostech souvisejících s vyšetřováním“. Jelikož je taková „žádost o zpřístupnění informací“ přípustná pouze jako součást trestního vyšetřování, vždy předpokládá konkrétní podezření z již spáchaného trestného činu ⁽⁹⁰⁾. Kromě toho, jelikož vyšetřování obvykle provádí prefekturní policie, použijí se omezení podle čl. 2 odst. 2 zákona o policii ⁽⁹¹⁾. Podle uvedeného ustanovení jsou činnosti policie „přísně omezeny“ na plnění jejich odpovědností a povinností (tj. předcházení trestných činů, jejich potlačování a vyšetřování). Kromě toho při plnění svých povinností policie jedná nestranně, nezájatě a spravedlivě a nesmí nikdy zneužít svých pravomocí „způsobem, který by zasahoval do práv a svobod jednotlivce zaručených Ústavou Japonska“ (které, jak již bylo uvedeno, zahrnují právo na soukromí a ochranu údajů) ⁽⁹²⁾.
- (127) Konkrétně, pokud jde o čl. 197 odst. 2 trestního řádu, Národní policejní agentura, jakožto federální orgán mimo jiné pověřený všemi záležitostmi, které se týkají trestní policie, vydal pokyny pro prefekturní

⁽⁸⁵⁾ Příloha uvádí devět druhů trestných činů, např. trestné činy související s drogami a zbraněmi, obchodováním s lidmi a organizovanou vraždou. Je třeba poznamenat, že nově zavedený trestný čin „přípravy teroristických činů a jiného organizovaného zločinu“ (viz poznámka pod čarou č. 76) není v tomto restriktivním seznamu zahrnut.

⁽⁸⁶⁾ Kromě toho podle článku 23 zákona o odposleších musí vyšetřující orgán uvědomit fyzickou osobu, jejíž komunikace je odposlouchávána (a tedy zahrnuta do záznamu odposlechu), o této skutečnosti písemně.

⁽⁸⁷⁾ Viz příloha II, oddíl II. písm. A bod 1 písm. b) bod 1.

⁽⁸⁸⁾ Podle obdržených informací podnikatelské subjekty, které nespolupracují, se podle žádného právního předpisu nevystavují riziku negativních důsledků (včetně sankcí). Viz příloha II, oddíl II. písm. A bod 2 písm. a).

⁽⁸⁹⁾ Podle pokynů Komise pro ochranu osobních informací (General Rule Edition) čl. 23 odst. 1 bod i) stanoví základ pro zpřístupnění osobních informací v reakci jak na soudní příkaz (článek 218 trestního řádu), tak na „žádost o zpřístupnění informací“ (čl. 197 odst. 2 trestního řádu).

⁽⁹⁰⁾ To znamená, že „žádost o zpřístupnění informací“ se smí použít pouze ke shromažďování informací v jednotlivých případech, a nikoli k rozsáhlému shromažďování osobních údajů. Viz též příloha II, oddíl I. písm. A bod 2 písm. b) bod 1.

⁽⁹¹⁾ Stejně jako předpisy příslušné prefekturní komise pro veřejnou bezpečnost, viz čl. 189 odst. 1 trestního řádu.

⁽⁹²⁾ Viz také článek 3 zákona o policii, podle kterého služební slib, který skládají všichni policisté, zní: „být věrný povinnosti hájit dodržování Ústavy a právních předpisů Japonska a na jejich dodržování dohlížet a plnit své povinnosti nezájatě, nestranně, poctivě a bez předsudků“.

policii⁽⁹³⁾ týkající se „správného používání písemných žádostí ve věcech vyšetřování“. Podle tohoto oznámení musí být žádosti předkládány za pomoci předtištěného formuláře („formulář č. 49“ neboli tzv. „žádost o zpřístupnění informací“)⁽⁹⁴⁾, týkat se záznamů „souvisejících s konkrétním vyšetřováním“ a požadované informace musí být „nezbytné pro [uvedené] vyšetřování“. V každém případě hlavní vyšetřovatel „v plném rozsahu přezkoumá nezbytnost, obsah atd. jednotlivých žádostí“ a musí získat interní souhlas od vysokého úředníka.

- (128) Ve dvou rozsudcích z let 1969 a 2008⁽⁹⁵⁾ Nejvyšší soud Japonska navíc stanovil omezení, pokud jde o nepovinná opatření, která zasahují do práva na soukromí⁽⁹⁶⁾. Soud měl zejména za to, že taková opatření musí být „přiměřená“ a nepřekračovat „obecně přípustné meze“, což znamená, že musí být nezbytná pro vyšetřování podezřelého (shromažďování důkazů) a prováděná „metodami vhodnými pro dosažení účelu vyšetřování“⁽⁹⁷⁾. Rozsudky ukazují, že to znamená test proporcionality s přihlédnutím ke všem okolnostem případu (např. míra zásahu do práva na soukromí, včetně očekávání soukromí, závažnost trestného činu, pravděpodobnost získání důležitých důkazů, důležitost takovýchto důkazů, možné alternativní prostředky vyšetřování atd.)⁽⁹⁸⁾.
- (129) Vedle těchto omezení výkonu veřejné moci se očekává, že podnikatelské subjekty samy zkontrolují („potvrdí“) nezbytnost a „rozumnost“ poskytnutí informací třetí straně⁽⁹⁹⁾. To zahrnuje otázku, zda jim ve spolupráci brání zákon. Takovéto protichůdné právní povinnosti mohou vyplývat zejména z povinností mlčenlivosti, např. článek 134 trestního zákoníku (týkající se vztahu mezi lékařem, advokátem, knězem atd. a jejich klientem). Rovněž „jakákoli osoba, která působí v odvětví telekomunikací při výkonu funkce zachovává tajemství druhých, která se dozví v souvislosti se sděleními, s nimiž nakládá provozovatel telekomunikačních sítí“ (čl. 4 odst. 2 zákona o telekomunikacích). Tato povinnost je doprovázena sankcí stanovenou v článku 179 zákona o telekomunikacích, podle něhož osoba, která poruší důvěrnost sdělení, s nimiž nakládá provozovatel telekomunikačních sítí, se dopustí trestného činu a bude potrestána trestem odnětí svobody s nařízeným výkonem práce na dobu až dvou let nebo pokutou v maximální výši jednoho milionu jenů⁽¹⁰⁰⁾. Ačkoli tento požadavek není absolutní, a zejména umožňuje opatření porušující důvěrnost sdělení, která představují „ospravedlnitelné jednání“ ve smyslu článku 35 trestního zákoníku⁽¹⁰¹⁾, nevztahuje se tato výjimka na nepovinné žádosti orgánů veřejné moci o zpřístupnění elektronických informací podle čl. 197 odst. 2 trestního řádu.

3.2.1.3 Další použití shromážděných informací

- (130) Osobní informace shromážděné japonskými orgány veřejné moci spadají do oblasti působnosti zákona o ochraně osobních informací uchovávaných správními orgány. Tento zákon upravuje nakládání s „uchovávanými informacemi“ (jejich

⁽⁹³⁾ Podle čl. 30 odst. 1 a čl. 31 odst. 2 zákona o policii generální ředitel útvarů regionální policie (místních poboček Národní policejní agentury) „dává prefekturní policii pokyny a vykonává nad ní dozor“.

⁽⁹⁴⁾ Žádost o zpřístupnění informací musí také uvádět kontaktní údaje osoby „nakládající“ s informacemi („název oddělení [pozice], jméno osoby nakládající s informacemi, telefonní číslo kanceláře, klapka atd.“).

⁽⁹⁵⁾ Rozsudek Nejvyššího soudu ze dne 24. prosince 1969 (1965(A) 1187); rozsudek ze dne 15. dubna 2008 (2007(A) 839).

⁽⁹⁶⁾ Tyto rozsudky se sice netýkaly shromažďování elektronických informací, japonská vláda však vysvětlila, že uplatňování kritérií vytvořených Nejvyšším soudem se vztahuje na všechny zásahy orgánů veřejné moci do práva na soukromí, včetně všech „dobrovolných vyšetřování“, a proto jsou tato kritéria pro japonské orgány také při podávání žádostí o dobrovolné zpřístupnění informací závazná. Viz příloha II, oddíl II. písm. A bod 2 písm. b) bod 1.

⁽⁹⁷⁾ Podle obdržených informací musí být tyto faktory „přiměřené v souladu se společenskými konvencemi“. Viz příloha II, oddíl II. písm. A bod 2 písm. b) bod 1.

⁽⁹⁸⁾ Z obdobných důvodů v souvislosti s povinným vyšetřováním (odposlechy) viz také rozsudek Nejvyššího soudu ze dne 16. prosince 1999, 1997 (A) 636.

⁽⁹⁹⁾ V tomto ohledu japonské orgány upozornily na pokyny Komise pro ochranu osobních informací (General Rule Edition) a bod 5/14 „otázek a odpovědí“ vypracovaných Komisí pro ochranu osobních informací pro použití zákona o ochraně osobních informací. Podle japonských orgánů „s ohledem na narůstající povědomí fyzických osob, pokud jde o jejich práva na soukromí, a rovněž s ohledem na pracovní zátěž, kterou takové žádosti vytvářejí, jsou podnikatelské subjekty při reakci na tyto žádosti stále obezřetnější. Viz příloha II, oddíl II. písm. A bod 2, rovněž s odvoláním na oznámení Národní policejní agentury z roku 1999. Podle obdržených informací skutečně existují případy, kdy podnikatelské subjekty spolupráci odmítly. Například ve své zprávě o transparentnosti z roku 2017 LINE (nejoblíbenější aplikace pro zaslání zpráv v Japonsku) uvádí: „Po obdržení žádosti od vyšetřovacích orgánů atd. [...] ověřujeme přiměřenost z hlediska zákonnosti, ochrany uživatele atd. Na základě tohoto ověřování žádost v daném okamžiku odmítneme, pokud má právní vady. Pokud je rozsah žádosti pro účely vyšetřování příliš široký, požádáme vyšetřovací orgán o vysvětlení. Pokud je vysvětlení neodůvodněné, této žádosti nevyhovíme.“ Viz internetové stránky (<https://linecorp.com/en/security/transparency/top>)

⁽¹⁰⁰⁾ Sankcemi mohou být trest odnětí svobody s nařízeným výkonem práce na dobu tří let nebo pokuta v maximální výši dvou milionů jenů pro kteroukoli osobu, která „působí v telekomunikacích“.

⁽¹⁰¹⁾ „Odůvodněným jednáním“ podle trestního zákoníku jsou zejména jednání provozovatele telekomunikačních sítí, která jsou v souladu s opatřeními státu, která jsou právně účinná (povinná opatření), například pokud vyšetřovací orgány přijmou opatření na základě příkazu vydaného soudcem. Viz příloha II, oddíl II. písm. A bod 2 písm. b) bod 2, s odvoláním na pokyny k ochraně osobních informací v odvětví telekomunikací.

zpracování) a stanoví řadu omezení a záruk (viz 118. bod odůvodnění)⁽¹⁰²⁾. Kromě toho skutečnost, že správní orgán může uchovávat osobní informace, „pouze pokud je uchovávaní nezbytné k provádění záležitostí v jeho pravomoci stanovené právními předpisy“ (čl. 3 odst. 1 zákona o ochraně osobních informací uchovávaných správními orgány), rovněž stanoví omezení – alespoň nepřímá – pro původní shromažďování.

3.2.2 Nezávislý dozor

- (131) V Japonsku shromažďování elektronických informací v oblasti prosazování trestního práva nejčastěji⁽¹⁰³⁾ spadá pod prefekturní policii⁽¹⁰⁴⁾, která v tomto ohledu podléhá různým úrovním dozoru.
- (132) Zaprvé ve všech případech, kdy jsou elektronické informace shromažďovány povinnými prostředky (prohlídka a zajištění věci), musí policie získat předchozí soudní příkaz (viz 121. bod odůvodnění). V takových případech bude tedy shromažďování soudcem kontrolováno *ex ante* na základě přísné normy „přiměřeného důvodu“.
- (133) V případě žádostí o dobrovolné zpřístupnění sice soudce žádnou kontrolu *ex ante* neprovádí, avšak podnikatelské subjekty, kterým jsou takové žádosti určeny, mohou proti nim vznést námitku, aniž by riskovaly jakékoli negativní důsledky (a budou muset přihlédnout k dopadu jakéhokoli zpřístupnění na soukromí). Kromě toho podle čl. 192 odst. 1 trestního řádu policisté vždy spolupracují a koordinují svou činnost se státním zástupcem (a příslušnou prefekturní komisí pro veřejnou bezpečnost)⁽¹⁰⁵⁾. Státní zástupce pak může poskytnout nezbytné obecné pokyny, kterými stanoví normy pro spravedlivé vyšetřování, a/nebo vydat konkrétní příkazy s ohledem na jednotlivé vyšetřování (článek 193 trestního řádu). Pokud takové pokyny a/nebo příkazy nejsou dodrženy, může státní zástupce vznést obvinění a zahájit disciplinární řízení (článek 194 trestního řádu). Prefekturní policie tedy působí pod dohledem státního zástupce.
- (134) Zadruhé podle článku 62 Ústavy může kterákoli z komor japonského parlamentu provádět vyšetřování v souvislosti s vládou, včetně vyšetřování týkajícího se zákonnosti shromažďování informací policií. Za tímto účelem může požadovat přítomnost a výpověď svědků a/nebo předložení záznamů. Tato vyšetřovací pravomoc je dále upravena v zákoně o parlamentu, zejména v kapitole XII. Zejména článek 104 zákona o parlamentu stanoví, že kabinet, veřejnoprávní subjekty a jiné části vlády „musí vyhovět žádosti kterékoli z komor nebo kteréhokoli z jejích výborů o předložení zpráv a záznamů nezbytných pro posouzení vyšetřování“. Odmítnutí vyhovět žádosti je přípustné pouze v případě, že vláda uvede přijatelný důvod, který bude parlament považovat za přijatelný, nebo v případě vydání formálního prohlášení, že předložení zpráv nebo záznamů by „vázně poškodilo národní zájmy“⁽¹⁰⁶⁾. Kromě toho členové parlamentu mohou klást kabinetu písemné dotazy (články 74 a 75 zákona o parlamentu) a v minulosti se takovéto „písemné dotazy“ týkaly rovněž nakládání s osobními informacemi státní správou⁽¹⁰⁷⁾. Úloha parlamentu při dohledu nad výkonnou mocí je posílena oznamovací povinností, například podle článku 29 zákona o odposleších.
- (135) Zatřetí prefekturní policie podléhá nezávislému dozoru i v rámci výkonné moci. To zahrnuje zejména prefekturní komise pro veřejnou bezpečnost zřízené na úrovni prefektur k zajištění demokratické správy a politické neutrality policie⁽¹⁰⁸⁾. Členové těchto komisí jsou jmenováni guvernérem prefektury se souhlasem prefekturního shromáždění (z občanů, kteří v předchozích pěti letech nebyli státními zaměstnanci u policie) a mají zajištěné funkční období (odvolání mohou být pouze z řádného důvodu)⁽¹⁰⁹⁾. Podle obdržených informací se na ně nevztahují pokyny, a proto je lze považovat za zcela nezávislé⁽¹¹⁰⁾. Pokud jde o úkoly a pravomoci prefekturních komisí pro

⁽¹⁰²⁾ Pokud jde o práva dotčených fyzických osob, viz oddíl 3.1.

⁽¹⁰³⁾ V zásadě státní zástupce – nebo asistent státního zástupce jednající na základě příkazu státního zástupce – může, pokud to považuje za nezbytné, vyšetřovat trestný čin (čl. 191 odst. 1 trestního řádu).

⁽¹⁰⁴⁾ Podle obdržených informací Národní policejní agentura neprovádí jednotlivá trestní vyšetřování. Viz příloha II, oddíl II. písm. A bod 1 písm. a).

⁽¹⁰⁵⁾ Viz také článek 246 trestního řádu, podle kterého je soudní policie povinna předat spis daného případu státnímu zástupci, jakmile uzavře vyšetřování trestného činu („zásada předání ve všech případech“).

⁽¹⁰⁶⁾ Alternativně může parlament vyžadovat, aby Rada pro dohled a přezkum zvláště určených tajemství prošetřila odmítnutí reagovat. Viz článek 104-II zákona o parlamentu.

⁽¹⁰⁷⁾ Viz příloha II, oddíl II. písm. B bod 4.

⁽¹⁰⁸⁾ Navíc podle ustanovení článku 100 zákona o místní autonomii má místní shromáždění pravomoc vyšetřovat činnosti donucovacích orgánů zřízených na prefekturní úrovni, včetně prefekturní policie.

⁽¹⁰⁹⁾ Viz články 39–41 zákona o policii. Pokud jde o politickou neutralitu, viz také článek 42 zákona o policii.

⁽¹¹⁰⁾ Viz příloha II, oddíl II. písm. B bod 3 („systém nezávislé rady“).

veřejnou bezpečnost, podle čl. 38 odst. 3 ve spojení s článkem 2 a čl. 36 odst. 2 zákona o policii jsou prefekturní komise zodpovědné za „ochranu práv a svobody jednotlivce“. Za tímto účelem mají pravomoc „vykonávat dozor“⁽¹¹¹⁾ nad všemi aktivitami prefekturní policie v oblasti vyšetřování, včetně shromažďování osobních údajů. Komise zejména „mohou [p]refekturní [p]olicii v případě potřeby dávat podrobné pokyny nebo pokyny v konkrétním případě kontroly zneužití pravomoci zaměstnanců policie“⁽¹¹²⁾. Pokud velitel prefekturní policie⁽¹¹³⁾ obdrží takový pokyn nebo se sám dozví o případném případu zneužití pravomoci (včetně porušení právních předpisů nebo jiného zanedbání povinností), musí bezodkladně případ prověřit a výsledek kontroly oznámit příslušné prefekturní komisi pro veřejnou bezpečnost (čl. 56 odst. 3 zákona o policii). Pokud to komise považuje za nezbytné, může rovněž jmenovat jednoho ze svých členů, aby přezkoumal stav provádění. Proces pokračuje, dokud není příslušná prefekturní komise pro veřejnou bezpečnost přesvědčena, že incident byl náležitě vyřešen.

- (136) Pokud jde o správné použití zákona o ochraně osobních informací uchovávaných správními orgány, příslušný ministr nebo vedoucí agentury (např. vrchní komisař Národní policejní agentury) má vymáhací pravomoc, která podléhá dohledu Ministerstva vnitra a komunikací. Podle článku 49 zákona o ochraně osobních informací uchovávaných správními orgány Ministerstvo vnitra a komunikací „může shromažďovat zprávy o stavu prosazování tohoto zákona“ od vedoucích správních orgánů (ministrů). Tato dohledová funkce je podpořena vstupy z 51 „všeobecných informačních středisek“ Ministerstva vnitra a komunikací (v každé prefektuře po celém Japonsku se nachází jedno), která každoročně zpracovávají tisíce dotazů od fyzických osob⁽¹¹⁴⁾ (které pak mohou odhalit možná porušení právních předpisů). Pokud to Ministerstvo vnitra a komunikací považuje za nezbytné k zajištění souladu s uvedeným zákonem, může si vyžádat předložení vysvětlení a materiálů a vydat stanoviska týkající se nakládání s osobními informacemi dotyčným správním orgánem (články 50 a 51 zákona o ochraně osobních informací uchovávaných správními orgány).

3.2.3 Individuální ochrana

- (137) Kromě dohledu z moci úřední mají fyzické osoby rovněž několik možností, jak dosáhnout individuální ochrany, a to jak prostřednictvím nezávislých orgánů (například příslušných prefekturních komisí pro veřejnou bezpečnost nebo Komise pro ochranu osobních informací), tak prostřednictvím japonských soudů.
- (138) Zaprvé, pokud jde o osobní informace shromažďované správními orgány, jsou tyto orgány povinny „usilovat o řádné a rychlé vyřízení jakékoli stížnosti“ týkající se následného zpracování informací (článek 48 zákona o ochraně osobních informací uchovávaných správními orgány). Kapitola IV zákona o ochraně osobních informací uchovávaných správními orgány týkající se individuálních práv sice není použitelná ve vztahu k osobním informacím zaznamenaným v „dokumentech týkajících se soudních řízení a zajištěných předmětů“ (čl. 53-2 odst. 2 trestního řádu), což zahrnuje osobní informace shromažďované v rámci trestního vyšetřování, fyzické osoby však mohou podat stížnost a dovolávat se obecných zásad ochrany údajů, jako je například povinnost uchovávat osobní informace pouze „v případě, že uchovávání je nezbytné pro plnění [funkcí prosazování práva]“ (čl. 3 odst. 1 zákona o ochraně osobních informací uchovávaných správními orgány).
- (139) Kromě toho článek 79 zákona o policii zaručuje fyzickým osobám, které mají obavy, pokud jde o „plnění povinností“ příslušníky policie, právo podat stížnost (příslušné) nezávislé prefekturní komisi pro veřejnou bezpečnost. Komise bude tyto stížnosti vyřizovat „svědomitě“ v souladu s právními předpisy a místními vyhláškami a stěžovatele bude o výsledku informovat písemně. Na základě své pravomoci dozorovat prefekturní policii a „dávat jí pokyny“, pokud jde o „zneužívání pravomoci příslušníků policie“ (čl. 38 odst. 3 a čl. 43-2 odst. 1 zákona o policii), může Komise požádat prefekturní policii, aby prošetřila skutečnosti, na základě tohoto šetření přijala přiměřená opatření a o výsledku podala zprávu. Pokud má komise za to, že šetření provedené policií není odpovídající, může rovněž poskytnout pokyny k vyřízení stížnosti.
- (140) Pro snazší vyřizování stížností vydala Národní policejní agentura „sdělení“ pro policii a prefekturní komise pro veřejnou bezpečnost týkající se řádného vyřizování stížností na plnění povinností policisty. V tomto dokumentu Národní policejní agentura stanoví normy pro výklad a provádění článku 79 zákona o policii. Mimo jiné vyžaduje,

⁽¹¹¹⁾ Viz čl. 5 odst. 3 a čl. 38 odst. 3 zákona o policii.

⁽¹¹²⁾ Viz čl. 38 odst. 3, čl. 43-2 odst. 1 zákona o policii. Pokud příslušná prefekturní komise pro veřejnou bezpečnost „vydá pokyn“ ve smyslu čl. 43-2 odst. 1, může nařídit výboru jmenovanému komisí, aby monitoroval jeho provádění (odstavec 2). Kromě toho může komise doporučit disciplinární opatření nebo odvolání velitele prefekturní policie (čl. 50 odst. 2), jakož i jiných policistů (čl. 55 odst. 4 zákona o policii).

⁽¹¹³⁾ Totéž se vztahuje na generálního superintendanta v případě Tokijské metropolitní policie (viz čl. 48 odst. 1 zákona o policii).

⁽¹¹⁴⁾ Podle obdržených informací bylo v rozpočtovém roce 2017 (duben 2017 až březen 2018) „všeobecnými informačními středisky“ zpracováno celkem 5 186 dotazů od fyzických osob.

aby prefekturní policie zavedla „systém pro vyřizování stížností“ a všechny stížnosti „bezodkladně“ vyřizovala a hlásila příslušné prefekturní komisi pro veřejnou bezpečnost. V oznámení se stížnosti vymezují jako nároky, jejichž cílem je náprava „konkrétního znevýhodnění, k němuž došlo v důsledku nezákonného nebo nevhodného chování“⁽¹¹⁵⁾ nebo „nepřijetí nezbytných opatření ze strany příslušníka policie při plnění jeho povinností“⁽¹¹⁶⁾, jakož i jakékoli „stížnosti/nespokojenost v souvislosti s nevhodným způsobem plnění povinností příslušníka policie“. Věcná působnost stížnosti je tedy vymezena široce, aby zahrnovala veškeré nároky týkající se nezákonného zpracování údajů, přičemž stěžovatel nemusí prokazovat, že v důsledku opatření příslušníka policie utrpěl újmu. Důležité je, že podle uvedeného sdělení bude cizincům (mimo jiné) poskytnuta pomoc při formulování stížnosti. V reakci na stížnost musí prefekturní komise pro veřejnou bezpečnost zajistit, aby prefekturní policie přezkoumala skutečnosti, „podle výsledku přezkoumání“ zavedla opatření a o výsledku podala zprávu. Pokud má komise za to, že přezkoumání je nedostačující, vydá pokyn k vyřízení stížnosti, který musí prefekturní policie dodržet. Na základě obdržení zprávy a přijatých opatření komise uvědomí danou fyzickou osobu a mimo jiné uvede opatření přijatá k vyřízení stížnosti. Sdělení Národní policejní agentury zdůrazňuje, že stížnosti je třeba vyřizovat „upřímně“ a že výsledek je třeba oznámit „ve lhůtě [...] považované za přiměřenou s ohledem na společenské normy a zdravý rozum“.

- (141) Zadruhé vzhledem k tomu, že právní ochranu bude přirozeně nutné hledat v zahraničí v cizím systému a cizím jazyce, pro usnadnění právní ochrany fyzických osob z EU, jejichž osobní údaje se předávají podnikatelským subjektům v Japonsku a k nimž mají následně přístup orgány veřejné moci, využila japonská vláda své pravomoci a vytvořila zvláštní mechanismus pro vyřizování a řešení stížností v této oblasti, který spravuje a dozoruje Komise pro ochranu osobních informací. Uvedený mechanismus vychází z povinnosti spolupráce, kterou japonským orgánům veřejné moci ukládá zákon o ochraně osobních informací, a ze zvláštní úlohy Komise pro ochranu osobních informací, pokud jde o mezinárodní předávání údajů ze třetích zemí podle článku 6 zákona o ochraně osobních informací a základní politiky (stanovené japonskou vládou prostřednictvím nařízení kabinetu). Podrobnosti tohoto mechanismu jsou uvedeny v oficiálních prohlášeních, ujištěních a závazcích obdržných od japonské vlády, které jsou připojeny k tomuto rozhodnutí jako příloha II. Na tento mechanismus se nevztahují žádné stávající požadavky a je otevřený pro každou fyzickou osobu bez ohledu na to, zda je podezřelá nebo obviněná z trestného činu,
- (142) Podle tohoto mechanismu může fyzická osoba, která má podezření, že její údaje předané z Evropské unie byly shromážděny nebo použity orgány veřejné moci v Japonsku (včetně orgánů odpovědných za prosazování trestního práva) v rozporu s použitelnými pravidly, podat stížnost ke Komisi pro ochranu osobních informací (individuálně nebo prostřednictvím svého úřadu pro ochranu osobních údajů ve smyslu článku 51 obecného nařízení o ochraně osobních údajů). Komise pro ochranu osobních informací bude povinna se stížností zabývat a v prvním kroku o ní informovat příslušné orgány veřejné moci, včetně příslušných dozorových úřadů. Tyto orgány musí spolupracovat s Komisí pro ochranu osobních informací, „včetně poskytnutí nezbytných informací a příslušných materiálů, tak aby Komise pro ochranu osobních informací mohla posoudit, zda shromáždění nebo následné použití osobních informací proběhlo v souladu s použitelnými pravidly“⁽¹¹⁷⁾. Tato povinnost, odvozená z článku 80 zákona o ochraně osobních informací (podle kterého mají japonské orgány veřejné moci povinnost spolupracovat s Komisí pro ochranu osobních informací), má všeobecnou platnost, a proto se vztahuje i na přezkum všech opatření přijatých těmito orgány v oblasti vyšetřování, které se k takové spolupráci navíc zavázaly prostřednictvím písemných ujištění příslušných ministerstev a vedoucích agentur, jak je uvedeno v příloze II.
- (143) Pokud posouzení ukáže, že došlo k porušení použitelných pravidel, „spolupráce dotyčných orgánů veřejné moci s Komisí pro ochranu osobních informací zahrnuje povinnost toto porušení napravit“, což v případě protiprávního shromažďování osobních informací zahrnuje výmaz takovýchto údajů. Důležité je, že na plnění této povinnosti dohlíží Komise pro ochranu osobních informací, která „před uzavřením posouzení potvrdí, že porušení bylo v plném rozsahu napraveno“.
- (144) Jakmile je posouzení uzavřeno, Komise pro ochranu osobních informací o jeho výsledku v přiměřené lhůtě uvědomí danou fyzickou osobu s uvedením případně přijatých nápravných opatření. Komise pro ochranu osobních informací zároveň informuje danou fyzickou osobu o možnosti vyžádat si od příslušného orgánu veřejné moci potvrzení výsledku a o tom, ke kterému úřadu takovou žádost o potvrzení podat. Možnost obdržet toto potvrzení,

⁽¹¹⁵⁾ Podmínka „konkrétního znevýhodnění“ znamená pouze to, že činnost (či nečinnost) policie se musí stěžovatele konkrétně týkat, nikoli to, že by musel prokázat jakoukoli újmu.

⁽¹¹⁶⁾ Mezi tyto povinnosti patří také dodržování zákona, včetně právních požadavků na shromažďování a používání osobních údajů. Viz čl. 2 odst. 2 a článek 3 zákona o policii.

⁽¹¹⁷⁾ Při provádění tohoto posouzení bude Komise pro ochranu osobních informací spolupracovat s Ministerstvem vnitra a komunikací, které (jak je vysvětleno ve 136. bodě odůvodnění) může požadovat předložení vysvětlení a materiálů a vydat stanoviska týkající se nakládání s osobními informacemi příslušným správním orgánem (články 50 a 51 zákona o ochraně osobních informací uchovávaných správními orgány).

včetně důvodů, z nichž rozhodnutí příslušného orgánu vychází, může fyzické osobě pomoci při jakýchkoli dalších krocích, a to i v případě, že bude žádat o soudní ochranu. Podrobné informace o výsledku posouzení lze omezit, pokud existují přiměřené důvody se domnívat, že sdělení takových informací pravděpodobně ohrozí probíhající vyšetřování.

- (145) Zatřetí fyzická osoba, která nesouhlasí s rozhodnutím o (příkazem k) zajištění věci ⁽¹¹⁸⁾ týkajícím se jejích osobních údajů vydaným soudcem nebo opatřeními policie nebo řízením o výkonu takového rozhodnutí, může podat žádost, aby dané rozhodnutí nebo uvedená opatření byla zrušena nebo změněna (čl. 429 odst. 1, čl. 430 odst. 1 a 2 trestního řádu, článek 26 zákona o odposleších) ⁽¹¹⁹⁾. Pokud má přezkoumávající soud za to, že buď samotný příkaz, nebo jeho výkon („zajišťovací postup“) je protiprávní, žádosti vyhovějí a nařídí vrácení zajištěných věcí ⁽¹²⁰⁾.
- (146) Začtvrté fyzická osoba, která má za to, že shromažďování jejích osobních informací jako součást trestního vyšetřování bylo protiprávní, se může v rámci svého trestního řízení dovolávat této protiprávnosti jakožto nepřímé formy soudní kontroly. Pokud bude soud souhlasit, povede to k vyloučení tohoto důkazu jako nepřipustného.
- (147) V neposlední řadě podle čl. 1 odst. 1 zákona o státní ochraně může soud přiznat odškodnění, pokud státní úředník, který vykonává veřejnou moc státu, při plnění svých povinností protiprávně a vlastní vinou (úmyslně nebo z nedbalosti) způsobil dotyčné fyzické osobě škodu. Podle článku 4 zákona o státní ochraně vychází odpovědnost státu za škody z ustanovení občanského zákoníku. V tomto ohledu článek 710 občanského zákoníku stanoví, že odpovědnost rovněž zahrnuje jiné než majetkové škody, a tedy i morální újmu (například v podobě „psychických problémů“). To zahrnuje případy, kdy je soukromí fyzické osoby narušeno protiprávním sledováním a/nebo shromažďováním jejích osobních informací (např. protiprávní výkon příkazu) ⁽¹²¹⁾.
- (148) Kromě peněžité náhrady mohou fyzické osoby za určitých podmínek rovněž dosáhnout soudního příkazu (např. k výmazu osobních údajů shromážděných orgány veřejné moci) na základě svých práv na soukromí podle článku 13 Ústavy ⁽¹²²⁾.
- (149) S ohledem na všechny tyto možnosti ochrany mechanismus řešení sporů vytvořený japonskou vládou stanoví, že fyzická osoba, která stále není spokojena s výsledkem řízení, se může obrátit na Komisi pro ochranu osobních informací, „která fyzickou osobu informuje o různých možnostech a detailních postupech pro dosažení právní ochrany podle japonských právních předpisů“. Kromě toho Komise pro ochranu osobních informací „poskytne dané fyzické osobě podporu, včetně poradenství a pomoci ohledně jakýchkoli dalších kroků ve vztahu k příslušnému správnímu nebo soudnímu orgánu“.
- (150) To zahrnuje využití procesních práv podle trestního řádu. Například „[p]okud posouzení odhalí, že fyzická osoba je podezřelá v trestní věci, Komise pro ochranu osobních informací danou fyzickou osobu informuje o této skutečnosti“ ⁽¹²³⁾ a rovněž o možnosti podle článku 259 trestního řádu požádat státního zástupce, aby ji uvědomil, jakmile se rozhodne nezahájit trestní řízení. Pokud pak posouzení odhalí, že bylo zahájeno řízení ve věci zahrnující osobní informace dané fyzické osoby a že toto řízení je ukončeno, Komise pro ochranu osobních informací bude fyzickou osobu informovat o tom, že lze nahlédnout do spisu podle článku 53 trestního řádu (a článku 4 zákona o konečném trestním spise). Získání přístupu ke svému spisu je důležité, neboť to fyzické osobě pomůže lépe

⁽¹¹⁸⁾ To zahrnuje příkaz k odposlechu, pro který zákon o odposleších stanoví zvláštní oznamovací povinnost (článek 23). Podle uvedeného ustanovení musí vyšetřující orgán uvědomit fyzické osoby, jejichž komunikace je odposlouchávána (a tedy zahrnuta do záznamu odposlechlů), o této skutečnosti písemně. Jiným příkladem je čl. 100 odst. 3 trestního řádu, podle kterého soud, pokud zajistí poštovní zásilky nebo telegramy odeslané obviněnému nebo obviněným, uvědomí odesílatele nebo příjemce, ledaže by existovalo riziko, že takové oznámení bude bránit soudnímu řízení. S tímto ustanovením upravujícím prohlídky a zajištění věci prováděné vyšetřujícím orgánem se prolíná ustanovení čl. 222 odst. 1 trestního řádu.

⁽¹¹⁹⁾ Tato žádost sice nemá automatický účinek pozastavení výkonu rozhodnutí o zajištění, přezkoumávající soud však může pozastavení nařídit, dokud ve věci samé nerozhodne. Viz čl. 429 odst. 2 a článek 432 ve spojení s článkem 424 trestního řádu.

⁽¹²⁰⁾ Viz příloha II, oddíl II. písm. C bod 1.

⁽¹²¹⁾ Viz příloha II, oddíl II. písm. C bod 2.

⁽¹²²⁾ Viz např. rozsudek Okresního soudu v Tokiu ze dne 24. března 1988 (č. 2925); rozsudek Okresního soudu v Ósace ze dne 26. dubna 2007 (č. 2925). Podle Okresního soudu v Ósace je nutné zvážit řadu faktorů, jako například: i) povahu a obsah sporných osobních informací; ii) způsob, jakým byly shromážděny; iii) nevýhody pro fyzickou osobu v případě, že tyto informace nebudou vymazány, a iv) veřejný zájem, včetně nevýhod pro orgán veřejné moci v případě, že tyto informace budou vymazány.

⁽¹²³⁾ V každém případě státní zástupce po zahájení trestního řízení obviněnému poskytne příležitost do těchto důkazů nahlédnout (viz články 298–299 trestního řádu). Pokud jde o oběti trestných činů, viz články 316–333 trestního řádu.

pochopit vyšetřování, které proti ní bylo vedeno, a připravit tak případné soudní kroky (např. podání žaloby o náhradu škody) v případě, že má za to, že její údaje byly shromažďovány nebo použity protiprávně.

3.3 Přístup japonských orgánů veřejné moci k osobním údajům a jejich použití těmito orgány pro účely národní bezpečnosti

- (151) Podle japonských orgánů neexistuje v Japonsku žádný zákon, který by připouštěl povinné žádosti o informace nebo „správní odposlechy“ mimo trestní vyšetřování. Z důvodu národní bezpečnosti lze tedy informace získat pouze z informačního zdroje, k němuž má přístup kdokoli, nebo dobrovolným zpřístupněním. Podnikatelské subjekty, které obdrží žádost o dobrovolnou spolupráci (formou zpřístupnění elektronických informací), nejsou tedy ze zákona povinny takovéto informace poskytnout⁽¹²⁴⁾.
- (152) Kromě toho podle obdržených informací jsou pouze čtyři vládní instituce oprávněny shromažďovat elektronické informace uchovávané japonskými podnikatelskými subjekty z důvodu národní bezpečnosti, a to konkrétně: i) Zpravodajská a vyšetřovací služba kabinetu; ii) Ministerstvo obrany; iii) policie (Národní policejní agentura⁽¹²⁵⁾ i prefekturní policie) a iv) Zpravodajská služba pro veřejnou bezpečnost. Zpravodajská a vyšetřovací služba kabinetu však nikdy neshromažďuje informace přímo od podnikatelských subjektů, a to ani prostřednictvím odposlechu komunikací. Pokud obdrží informace od jiných vládních institucí, aby mohla poskytnout analýzu kabinetu, musí tyto jiné instituce dodržovat právní předpisy, včetně omezení a záruk analyzovaných v tomto rozhodnutí. Její činnost tedy není v kontextu předávání relevantní.

3.3.1 Právní základ a použitelná omezení/záruky

- (153) Podle obdržených informací Ministerstvo obrany shromažďuje (elektronické) informace na základě zákona o zřízení Ministerstva obrany. Podle článku 3 uvedeného zákona je posláním Ministerstva obrany řídit vojenské síly a operovat s nimi a „vykonávat související záležitosti s cílem zajistit národní mír a nezávislost a bezpečnost národa“. Ustanovení čl. 4 odst. 4 stanoví, že Ministerstvo obrany má pravomoc nad „obranou a stráží“, nad akcemi uskutečňovanými domobranou, jakož i nad rozmisťováním vojenských sil, včetně shromažďování informací nezbytných k provádění uvedených záležitostí. (Elektronické) informace od podnikatelských subjektů je oprávněna shromažďovat pouze prostřednictvím dobrovolné spolupráce.
- (154) Pokud jde o prefekturní policii, její odpovědnosti a povinnosti zahrnují „udržování veřejné bezpečnosti a veřejného pořádku“ (čl. 35 odst. 2 ve spojení s čl. 2 odst. 1 zákona o policii). V rozsahu této pravomoci může policie shromažďovat informace, ale pouze na základě dobrovolnosti bez právní síly. Kromě toho jsou činnosti policie „přísně omezeny“ na ty, které jsou nezbytné k plnění jejich povinností. Kromě toho policie jedná „nezaujatě, nestranně, nepředpojatě a spravedlivě“ a nikdy nezneužívá svých pravomocí „způsobem, který by zasahoval do práv a svobod fyzických osob zaručených Ústavou Japonska“ (článek 2 zákona o policii).
- (155) V neposlední řadě může Zpravodajská služba pro veřejnou bezpečnost provádět vyšetřování podle zákona o předcházení podvrtným činnostem a zákona o kontrole organizací, které se dopouštějí bezohledného masového vraždění, kdy tato vyšetřování jsou nezbytná k přípravě přijetí kontrolních opatření vůči určitým organizacím⁽¹²⁶⁾. Podle obou zákonů může Přezkumná komise pro veřejnou bezpečnost na žádost generálního ředitele Zpravodajské služby pro veřejnou bezpečnost vydávat určitá „rozhodnutí“ (sledování/zákazy v případě zákona o kontrole organizací, které se dopouštějí bezohledného masového vraždění⁽¹²⁷⁾, zrušení/zákazy v případě zákona o předcházení podvrtným činnostem⁽¹²⁸⁾) a v této souvislosti může Zpravodajská služba pro veřejnou bezpečnost provádět vyšetřování⁽¹²⁹⁾. Podle obdržených informací se tato vyšetřování provádějí vždy na dobrovolném základě, což

⁽¹²⁴⁾ Podnikatelské subjekty se tedy mohou svobodně rozhodnout nespolupracovat bez jakéhokoli rizika sankcí nebo jiných negativních důsledků. Viz příloha II, oddíl III. písm. A bod 1.

⁽¹²⁵⁾ Hlavní úlohou Národní policejní agentury je podle obdržených informací koordinace vyšetřování různých útvarů prefekturní policie a výměna informací s cizími orgány. Dokonce i v této roli podléhá Národní policejní agentura dohledu Národní komise pro veřejnou bezpečnost, která je mimo jiné zodpovědná za ochranu práv a svobod fyzických osob (čl. 5 odst. 1 zákona o policii).

⁽¹²⁶⁾ Viz příloha II, oddíl III. písm. A bod 1. část 3. Příslušná oblast působnosti těchto dvou zákonů je omezena: zákon o předcházení podvrtným činnostem se vztahuje na „teroristické podvrtné činnosti“ a zákon o kontrole organizací, které se dopouštějí bezohledného masového vraždění, se vztahuje na „případy bezohledného masového vraždění (což znamená „teroristickou podvrtnou činnost“ podle zákona o předcházení podvrtné činnosti, „při které je bezohledně zavražděno velké množství osob“).

⁽¹²⁷⁾ Viz články 5 a 8 zákona o kontrole organizací, které se dopouštějí bezohledného masového vraždění. Rozhodnutí o sledování rovněž zahrnuje povinnost podávání zpráv pro organizaci, které se opatření týká. Procesní záruky, zejména požadavky na transparentnost a předchozí souhlas Přezkumné komise pro veřejnou bezpečnost, viz články 12, 13 a 15–27 zákona o kontrole organizací, které se dopouštějí bezohledného masového vraždění.

⁽¹²⁸⁾ Viz články 5 a 7 zákona o předcházení podvrtným činnostem. Procesní záruky, zejména požadavky na transparentnost a předchozí souhlas Přezkumné komise pro veřejnou bezpečnost, viz články 11–25 zákona o kontrole organizací, které se dopouštějí bezohledného masového vraždění.

⁽¹²⁹⁾ Viz článek 27 zákona o předcházení podvrtným činnostem a články 29 a 30 zákona o kontrole organizací, které se dopouštějí bezohledného masového vraždění.

znamená, že Zpravodajská služba pro veřejnou bezpečnost nesmí vlastníka osobních informací nutit, aby tyto informace poskytl⁽¹³⁰⁾. Kontroly a vyšetřování se provádějí pouze v minimálním rozsahu nezbytném pro dosažení účelu kontroly a za žádných okolností nesmějí být prováděny tak, aby „nepřiměřeně“ omezovaly práva a svobody zaručené Ústavou Japonska (čl. 3 odst. 1 zákona o předcházení podvratným činnostem / zákona o kontrole organizací, které se dopouštějí bezohledného masového vraždění). Kromě toho podle čl. 3 odst. 2 zákona o předcházení podvratným činnostem / zákona o kontrole organizací, které se dopouštějí bezohledného masového vraždění nesmí Zpravodajská služba pro veřejnou bezpečnost za žádných okolností těchto kontrol nebo probíhajícího vyšetřování k přípravě těchto kontrol zneužít. Pokud důstojník Zpravodajské služby pro veřejnou bezpečnost zneužije svou pravomoc podle příslušného zákona tím, že určitou osobu donutí udělat něco, co daná osoba udělat nemusí, nebo zasáhne do výkonu práv určité osoby, může takový důstojník nebo policista podléhat trestním sankcím podle článku 45 zákona o předcházení podvratným činnostem nebo podle článku 42 zákona o kontrole organizací, které se dopouštějí bezohledného masového vraždění. V neposlední řadě oba zákony výslovně stanoví, že jejich ustanovení, včetně pravomocí těmito zákony udělených, „za žádných okolností nesmějí být vykládána šířeji“ (článek 2 zákona o předcházení podvratným činnostem / zákona o kontrole organizací, které se dopouštějí bezohledného masového vraždění).

- (156) Ve všech případech přístupu vlády z důvodů národní bezpečnosti popsaných v tomto oddíle platí omezení stanovená japonským Nejvyšším soudem pro dobrovolná vyšetřování, což znamená, že shromažďování (elektronických) informací musí odpovídat zásadám nutnosti a přiměřenosti („vhodná metoda“)⁽¹³¹⁾. Jak výslovně potvrdily japonské orgány, „shromažďování a zpracovávání informací probíhá pouze v míře nezbytné pro plnění konkrétních povinností příslušného orgánu veřejné moci, jakož i na základě konkrétních hrozeb“. Proto „je tak vyloučen masový a neselektivní sběr osobních informací nebo přístup k těmto osobním informacím z důvodu národní bezpečnosti“⁽¹³²⁾.
- (157) Jakmile jsou navíc jakékoli osobní informace uchovávané orgány veřejné moci pro účely národní bezpečnosti shromážděny, vztahuje se na ně v souvislosti s jejich následným uložením, použitím a zpřístupněním ochrana podle zákona o ochraně osobních informací uchovávaných správními orgány (viz 118. bod odůvodnění).

3.3.2 Nezávislý dozor

- (158) Shromažďování osobních informací pro účely národní bezpečnosti podléhá několika úrovním dozoru tří vládních složek.
- (159) Zprv japonský parlament může prostřednictvím svých specializovaných výborů přezkoumávat zákonnost vyšetřování na základě svých pravomocí v oblasti parlamentní kontroly (článek 62 Ústavy, článek 104 zákona o parlamentu; viz 134. bod odůvodnění). Tato dozorová funkce je podpořena zvláštními povinnostmi podávání zpráv o prováděných činnostech, které vycházejí z některého z výše uvedených právních základů⁽¹³³⁾.
- (160) Zadruhé v rámci výkonné moci existuje několik dozorových mechanismů.
- (161) Pokud jde o Ministerstvo obrany, dozor vykonává kancelář generálního inspektora pro dodržování právních předpisů⁽¹³⁴⁾, která byla zřízena na základě článku 29 zákona o zřízení Ministerstva obrany jako úřad v rámci Ministerstva obrany pod dohledem ministra obrany (kterému podléhá), ale nezávisle na provozních útvarech Ministerstva obrany. Kancelář generálního inspektora má za úkol zajišťovat dodržování právních předpisů, jakož i řádné plnění povinností úředníků Ministerstva obrany. Mezi jeho pravomoci patří provádět tzv. „inspekce obrany“, a to jak v pravidelných intervalech („pravidelné inspekce obrany“), tak v individuálních případech („zvláštní inspekce obrany“), které v minulosti zahrnovaly také řádné nakládání s osobními informacemi⁽¹³⁵⁾. V souvislosti s těmito inspekcemi může kancelář generálního inspektora vstupovat do prostor (kanceláří) a požadovat předložení

⁽¹³⁰⁾ Viz příloha II, oddíl III. písm. A bod 1. část 3.

⁽¹³¹⁾ Viz příloha II, oddíl III. písm. A bod 2 písm. b). „Z judikatury Nejvyššího soudu vyplývá, že na to, aby orgány mohly hospodářskému subjektu zaslat žádost o dobrovolnou spolupráci, musí být tato žádost nezbytná pro vyšetřování podezření z trestné činnosti a musí být přiměřená, pokud jde o dosažení účelu vyšetřování. Ačkoli se vyšetřování prováděná vyšetřovacími orgány v oblasti národní bezpečnosti liší od vyšetřování prováděných vyšetřovacími orgány v oblasti prosazování práva, pokud jde o právní základ i účel, ústřední zásady „nutnosti vyšetřování“ a „vhodnosti metody“ se použijí obdobně v oblasti národní bezpečnosti a musí být dodrženy s náležitým přihlédnutím ke konkrétním okolnostem každého případu.“

⁽¹³²⁾ Viz příloha II, oddíl III. písm. A bod 2 písm. b).

⁽¹³³⁾ Viz např. článek 36 zákona o předcházení podvratným činnostem / článek 31 zákona o kontrole organizací, které se dopouštějí bezohledného masového vraždění (pro Zpravodajskou službu pro veřejnou bezpečnost).

⁽¹³⁴⁾ Vedoucím kanceláře generálního inspektora je bývalý státní zástupce. Viz příloha II, oddíl III. písm. B bod 3.

⁽¹³⁵⁾ Viz příloha II, oddíl III. písm. B bod 3. Podle poskytnutého příkladu zahrnovala pravidelná inspekce obrany v roce 2016, pokud jde o „informovanost / připravenost na dodržování právních předpisů“, mimo jiné „stav ochrany osobních informací“ (správa, uložení atd.). Výsledná zpráva zjistila případy nevhodné správy údajů a vyzvala v tomto ohledu ke zlepšení. Ministerstvo obrany zprávu zveřejnilo na svých internetových stránkách.

dokumentů nebo informací, včetně vysvětlení náměstka ministra obrany. Inspekce se uzavírá zprávou ministrově obrany, která uvádí zjištění a opatření ke zlepšení (jejichž zavedení může být opět kontrolováno prostřednictvím dalších inspekci). Zpráva pak tvoří základ pro pokyny ministra obrany k zavedení opatření nezbytných k řešení situace; zavedením takovýchto opatření je pověřen náměstek ministra a musí o opatřeních přijatých v návaznosti na zjištění podat zprávu.

- (162) Pokud jde o prefekturní policii, dozor zajišťují nezávislé prefekturní komise pro veřejnou bezpečnost, jak je vysvětleno ve 135. bodě odůvodnění s ohledem na prosazování trestního práva.
- (163) Jak již bylo uvedeno, Zpravodajská služba pro veřejnou bezpečnost může provádět vyšetřování pouze v rozsahu nezbytném s ohledem na přijetí rozhodnutí o zákazu, zrušení nebo sledování podle zákona o předcházení podvrhatým činnostem / zákona o kontrole organizací, které se dopouštějí bezohledného masového vraždění, a pro tato rozhodnutí vykonává dozor *ex ante* nezávislá⁽¹³⁶⁾ Přezkumná komise pro veřejnou bezpečnost. Kromě toho zvláště určení inspektoři provádějí pravidelné / periodické inspekce (které komplexně posuzují činnost Zpravodajské služby pro veřejnou bezpečnost)⁽¹³⁷⁾ a zvláštní interní inspekce⁽¹³⁸⁾ činností jednotlivých útvarů/kanceláří atd., které mohou vést k vydání pokynů pro vedoucí příslušných útvarů atd., aby přijali opatření k nápravě nebo zlepšení.
- (164) Tyto dozorové mechanismy, které jsou dále posíleny možností fyzických osob vyvolat zásah Komise pro ochranu osobních informací jakožto nezávislého dozorového úřadu (viz níže uvedený 168. bod odůvodnění), poskytují odpovídající záruky ve vztahu k riziku zneužití pravomoci japonskými orgány v oblasti národní bezpečnosti a ve vztahu k jakémukoli protiprávnímu shromažďování elektronických informací.

3.3.3 Individuální ochrana

- (165) Pokud jde o individuální ochranu, s ohledem na osobní informace shromažďované a tedy „uchovávané“ správními orgány jsou tyto orgány povinny „usilovat o řádné a rychlé vyřízení jakékoli stížnosti“ týkající se zpracování (článek 48 zákona o ochraně osobních informací uchovávaných správními orgány).
- (166) Kromě toho na rozdíl od trestního vyšetřování mají fyzické osoby (včetně cizích státních příslušníků žijících v zahraničí) v zásadě právo na zpřístupnění⁽¹³⁹⁾, opravu (včetně výmazu) a přerušení používání/poskytování informací podle zákona o ochraně osobních informací uchovávaných správními orgány. Vzhledem k tomu může vedoucí správního orgánu odmítnout zpřístupnění ve vztahu k informacím, u kterých existují přiměřené důvody [...] se domnívat, že zpřístupnění pravděpodobně naruší národní bezpečnost“ (čl. 14 bod iv) zákona o ochraně osobních informací uchovávaných správními orgány), a může tak učinit bez odhalení existence těchto informací (článek 17 zákona o ochraně osobních informací uchovávaných správními orgány). Obdobně fyzická osoba sice může požádat o přerušení používání nebo o výmaz podle čl. 36 odst. 1 bodu i) zákona o ochraně osobních informací uchovávaných správními orgány v případě, že správní orgán získal informace protiprávně nebo je uchovává/používá nad rámec toho, co je nutné pro dosažení stanoveného účelu, úřad však může žádost zamítnout, pokud zjistí, že přerušení používání „pravděpodobně zabráni řádnému výkonu záležitostí vztahujících se k účelu použití uchovávaných osobních informací z důvodu povahy uvedených záležitostí“ (článek 38 zákona o ochraně osobních informací uchovávaných správními orgány). Nicméně, pokud je možné snadno oddělit a vyloučit části, které podléhají výjimce, správní orgány musí umožnit alespoň částečné zpřístupnění (viz např. čl. 15 odst. 1 zákona o ochraně osobních informací uchovávaných správními orgány)⁽¹⁴⁰⁾.

⁽¹³⁶⁾ Podle zákona o zřízení Přezkumné komise pro veřejnou bezpečnost vykonávají předseda a členové komise „svou funkci nezávisle“ (článek 3). Jsou jmenováni předsedou vlády se souhlasem obou komor parlamentu a mohou být odvoláni pouze „z vážných důvodů“ (např. uvěznění, profesní pochybení, duševní nebo tělesná porucha, zahájení konkursního řízení).

⁽¹³⁷⁾ Nařízení o pravidelných inspekcích Zpravodajské služby pro veřejnou bezpečnost (generální ředitel Zpravodajské služby pro veřejnou bezpečnost, pokyn č. 4, 1986).

⁽¹³⁸⁾ Nařízení o zvláštních inspekcích Zpravodajské služby pro veřejnou bezpečnost (generální ředitel Zpravodajské služby pro veřejnou bezpečnost, pokyn č. 11, 2008). Zvláštní inspekce budou prováděny, pokud to generální ředitel Zpravodajské služby pro veřejnou bezpečnost považuje za nezbytné.

⁽¹³⁹⁾ To se vztahuje na právo obdržet kopii „uchovávaných osobních informací“.

⁽¹⁴⁰⁾ Viz také možnost „zpřístupnění dle vlastního uvážení“ i v případě, kdy jsou v „uchovávaných osobních informacích“, jejichž zpřístupnění se požaduje, zahrnuty „informace, které zpřístupněny být nemají“ (článek 16 zákona o ochraně osobních informací uchovávaných správními orgány).

- (167) V každém případě musí správní orgán přijmout písemné rozhodnutí v určité lhůtě (tato lhůta činí 30 dní a může být za určitých podmínek prodloužena na dalších 30 dní). Pokud fyzická osoba žádosti nevyhoví, nebo jí vyhoví jen částečně, nebo z jiných důvodů považuje postup správního orgánu za „nezákonný nebo nespravedlivý“, může požádat o správní přezkum podle zákona o přezkumu správních stížností⁽¹⁴¹⁾. V tomto případě vedoucí správního orgánu, který rozhoduje o oprávněném prostředku, vede konzultace s Radou pro přezkum ochrany osobních informací a zpřístupnění informací (články 42 a 43 zákona o ochraně osobních informací uchovávaných správními orgány), specializovanou a nezávislou radu, jejíž členy jmenuje předseda vlády se souhlasem obou komor parlamentu. Podle obdržených informací může tato rada pro přezkum provádět šetření⁽¹⁴²⁾ a v této souvislosti požádat správní orgán, aby poskytl uchovávané osobní informace, včetně utajeného obsahu, jakož i další informace a dokumenty. Ačkoli konečná zpráva, která se zasílá stěžovateli, jakož i správnímu orgánu a která se zveřejňuje, není právně závazná, téměř ve všech případech je dodržována⁽¹⁴³⁾. Kromě toho má fyzická osoba možnost soudně napadnout rozhodnutí o oprávněném prostředku podle zákona o správním řízení. Tím se otevírá cesta pro soudní kontrolu používání výjimek v oblasti národní bezpečnosti, včetně toho, zda taková výjimka byla zneužita, nebo je dosud odůvodněná.
- (168) Aby se usnadnil výkon výše uvedených práv podle zákona o ochraně osobních informací uchovávaných správními orgány, Ministerstvo vnitra a komunikací zřídilo 51 „všeobecných informačních středisek“, která poskytují souhrnné informace o uvedených právech, použitelných postupech pro podání žádosti a způsobech ochrany⁽¹⁴⁴⁾. Pokud jde o správní orgány, musí poskytnout „informace, které přispívají k určení uchovávaných osobních informací,“⁽¹⁴⁵⁾ a přijmout „další vhodná opatření s ohledem na praktické potřeby osoby, která má v úmyslu žádost podat (čl. 47 odst. 1 zákona o ochraně osobních informací uchovávaných správními orgány).
- (169) Stejně jako v případě vyšetřování v oblasti prosazování trestního práva i v oblasti národní bezpečnosti mohou fyzické osoby získat individuální ochranu, pokud přímo kontaktují Komisi pro ochranu osobních informací. To vyvolá zvláštní postup řešení sporu, který japonská vláda zavedla pro fyzické osoby z EU, jejichž osobní údaje se předávají podle tohoto rozhodnutí (viz podrobné vysvětlení ve 141. až 144. a 149. bodě odůvodnění).
- (170) Kromě toho se mohou fyzické osoby domáhat soudní ochrany v podobě žaloby o náhradu škody podle zákona o státní ochraně, což rovněž zahrnuje morální újmu a za určitých podmínek výmaz shromážděných údajů (viz 147. bod odůvodnění).

4. ZÁVĚR: ODPOVÍDAJÍCÍ ÚROVEŇ OCHRANY OSOBNÍCH ÚDAJŮ PŘEDÁVANÝCH Z EVROPSKÉ UNIE PODNIKATELSKÝM SUBJEKTŮM V JAPONSKU

- (171) Komise má za to, že zákon o ochraně osobních informací rozšířený o doplňková pravidla obsažená v příloze I společně s oficiálními prohlášeními, ujištěními a závazky obsaženými v příloze II zajišťuje úroveň ochrany osobních údajů předávaných z Evropské unie, která je v zásadě rovnocenná úrovni ochrany zaručené nařízením (EU) 2016/679.
- (172) Kromě toho má Komise za to, že jako celek dozorové mechanismy a způsoby ochrany v japonských právních předpisech umožňují, aby porušení ze strany přijímajících podnikatelských subjektů nakládajících s osobními informacemi byla identifikována a v praxi potrestána, a subjektu údajů nabízí právní prostředky pro získání přístupu k osobním údajům, které se ho týkají, a případně pro dosažení opravy nebo výmazu takovýchto údajů.

⁽¹⁴¹⁾ Zákon o přezkumu správních stížností (zákon č. 160 z roku 2014), zejména čl. 1 odst. 1.

⁽¹⁴²⁾ Viz článek 9 zákona o zřízení Rady pro přezkum ochrany osobních informací a zpřístupnění informací (zákon č. 60 z roku 2003).

⁽¹⁴³⁾ Podle obdržených informací se během třinácti let od roku 2005 (kdy zákon o ochraně osobních informací uchovávaných správními orgány nabyl účinnosti) správní orgán zprávy nedržel pouze ve dvou z více než 2000 případů navzdory skutečnosti, že správní rozhodnutí byla radou pro přezkum při řadě příležitostí rozporována. Kromě toho, pokud správní orgán přijme rozhodnutí, které se liší od zjištění uvedených ve zprávě, musí jasně uvést důvody, proč se od uvedených zjištění odchýlil. Viz příloha II, oddíl III písm. C, s odvoláním na čl. 50 odst. 1 položku iv) zákona o přezkumu správních stížností.

⁽¹⁴⁴⁾ Všeobecná informační střediska (v každé prefektuře jedno) poskytují občanům vysvětlení k osobním informacím shromažďovaným orgány veřejné moci (např. stávající databáze) a k použitelným pravidlům pro ochranu údajů (zákon o ochraně osobních informací uchovávaných správními orgány) včetně toho, jak uplatnit právo na zpřístupnění, opravu nebo pozastavení používání. Zároveň tato střediska fungují jako kontaktní místo pro dotazy/stížnosti občanů. Viz příloha II, oddíl II. písm. C bod 4 písm. a).

⁽¹⁴⁵⁾ Viz také články 10 a 11 zákona o ochraně osobních informací uchovávaných správními orgány týkající se „registru souborů osobních informací“, které však obsahují řadu výjimek, pokud jde o soubory osobních informací vypracované nebo získané pro potřeby trestního vyšetřování nebo které obsahují věci týkající se bezpečnosti a jiných důležitých státních zájmů (viz čl. 10 odst. 2 body i) a ii) zákona o ochraně osobních informací uchovávaných správními orgány).

- (173) V neposlední řadě na základě dostupných informací o japonském právním řádu, včetně prohlášení, ujištění a závazků japonské vlády obsažených v příloze II, má Komise za to, že jakýkoli zásah do základních práv fyzických osob, jejichž osobní údaje se předávají z Evropské unie do Japonska, ze strany japonských orgánů veřejné moci pro účely veřejného zájmu, zejména pro účely prosazování trestního práva a národní bezpečnosti, bude omezen na rozsah nezbytný pro dosažení daného oprávněného cíle a že existuje účinná právní ochrana před takovým zásahem.
- (174) S ohledem na zjištění tohoto rozhodnutí má tedy Komise za to, že Japonsko zajišťuje odpovídající úroveň ochrany osobních údajů předávaných z Evropské unie podnikatelským subjektům nakládajícím s osobními informacemi v Japonsku, které podléhají zákonu o ochraně osobních informací, s výjimkou případů, kdy příjemce spadá do jedné z kategorií uvedených v čl. 76 odst. 1 zákona o ochraně osobních informací a účely zpracování zcela nebo částečně odpovídají jednomu z účelů stanovených v daném ustanovení.
- (175) Na základě toho dospěla Komise k závěru, že standard odpovídající ochrany podle článku 45 nařízení (EU) 2016/679, vykládaný s ohledem na Listinu základních práv Evropské unie, a zejména v rozsudku ve věci *Schrems* ⁽¹⁴⁶⁾, je splněn.

5. POSTUP ÚŘADŮ PRO OCHRANU ÚDAJŮ A INFORMACE PRO KOMISI

- (176) Podle judikatury Soudního dvora ⁽¹⁴⁷⁾ a podle čl. 45 odst. 4 nařízení (EU) 2016/679 by Komise po přijetí rozhodnutí o odpovídající ochraně měla neustále sledovat příslušný vývoj ve třetí zemi, aby mohla posoudit, zda Japonsko stále zajišťuje v zásadě rovnocennou úroveň ochrany. Takové ověřování je každopádně závazné tehdy, když Komise obdrží informace vyvolávající v tomto ohledu určité odůvodněné pochybnosti.
- (177) Komise by tedy měla průběžně sledovat situaci, pokud jde o právní rámec a skutečnou praxi zpracování osobních údajů, jak jsou posouzeny v tomto rozhodnutí, včetně toho, zda japonské orgány dodržují prohlášení, ujištění a závazky obsažené v příloze II. K usnadnění tohoto procesu se očekává, že japonské orgány budou Komisi informovat o podstatném vývoji relevantním pro toto rozhodnutí, pokud jde o zpracování osobních údajů podnikatelskými subjekty i o omezení a záruky použitelné pro přístup k osobním údajům ze strany orgánů veřejné moci. To by mělo zahrnovat jakákoli rozhodnutí přijatá Komisí pro ochranu osobních informací podle článku 24 zákona o ochraně osobních informací uznávající, že třetí země poskytuje rovnocennou úroveň ochrany, která je zaručena v Japonsku.
- (178) Aby Komise navíc mohla účinně plnit svou funkci sledování, měly by ji členské státy informovat o veškerých relevantních krocích vnitrostátních úřadů pro ochranu údajů, zejména v souvislosti s dotazy nebo stížnostmi subjektů údajů z EU týkajícími se předávání osobních údajů z Evropské unie podnikatelským subjektům v Japonsku. Komise by rovněž měla informovat o jakýchkoli známkách toho, že kroky japonských orgánů veřejné moci odpovědných za prevenci, vyšetřování, odhalování nebo stíhání trestných činů nebo za národní bezpečnost, včetně jakýchkoli dozorových úřadů, nezajišťují požadovanou úroveň ochrany.
- (179) Členské státy a jejich orgány musí přijmout opatření nezbytná k dosažení souladu s akty orgánů Unie, neboť jim v zásadě svědčí presumpce legality, a tudíž zakládají právní účinky tak dlouho, dokud nejsou vzaty zpět, zrušeny v rámci žaloby na neplatnost nebo prohlášeny za neplatné v návaznosti na žádost o rozhodnutí o předběžné otázce nebo na námitku protiprávnosti. V důsledku toho je rozhodnutí Komise o odpovídající ochraně podle čl. 45 odst. 3 nařízení (EU) 2016/679 závazné pro všechny orgány členských států, kterým je určeno, a to i pro nezávislé dozorové úřady. Zároveň, jak je vysvětleno v rozsudku Soudního dvora ve věci *Schrems* ⁽¹⁴⁸⁾ a jak uznává čl. 58 odst. 5 nařízení, jestliže úřad pro ochranu osobních údajů zpochybňuje, i na základě stížnosti, slučitelnost rozhodnutí Komise o odpovídající ochraně se základními právy fyzické osoby na soukromí a ochranu údajů, musí mu vnitrostátní právo poskytnout procesní prostředek, který mu umožní uplatnit tyto výtky před vnitrostátním soudem, který v případě pochybností musí přerušit řízení a předložit Soudnímu dvoru žádost o rozhodnutí o předběžné otázce ⁽¹⁴⁹⁾.

⁽¹⁴⁶⁾ Viz výše pozn. pod čarou č. 3.

⁽¹⁴⁷⁾ Rozsudek ve věci *Schrems*, bod 76.

⁽¹⁴⁸⁾ Rozsudek ve věci *Schrems*, bod 65.

⁽¹⁴⁹⁾ Rozsudek ve věci *Schrems*, bod 65: „V tomto ohledu přísluší vnitrostátnímu normotvůrci, aby stanovil procesní prostředky, které by dotyčnému vnitrostátnímu orgánu dozoru umožnily uplatnit výtky, jež považuje za opodstatněné, před vnitrostátními soudy, aby tyto soudy v případě, že sdílejí pochybnosti vyjádřené tímto orgánem ohledně platnosti rozhodnutí Komise, předložily žádost o rozhodnutí o předběžné otázce za účelem přezkumu platnosti tohoto rozhodnutí.“

6. PRAVIDELNÝ PŘEZKUM ZJIŠTĚNÍ O ODPOVÍDAJÍCÍ ÚROVNI OCHRANY

- (180) Podle čl. 45 odst. 3 nařízení (EU) 2016/679⁽¹⁵⁰⁾ a s ohledem na skutečnost, že úroveň ochrany poskytovaná japonským právním řádem se může změnit, měla by Komise po přijetí tohoto rozhodnutí pravidelně ověřovat, zda zjištění týkající se odpovídající úrovně ochrany zajištěné Japonskem jsou nadále skutkově i právně podložena.
- (181) Za tímto účelem by toto rozhodnutí mělo být předmětem prvního přezkumu do dvou let po jeho vstupu v platnost. Po tomto prvním přezkumu a v závislosti na jeho výsledku Komise v úzké konzultaci s výborem zřízeným podle čl. 93 odst. 1 GDPR rozhodne, zda by měl být dvouletý cyklus zachován. V každém případě by se následné přezkumy měly provádět alespoň každé čtyři roky⁽¹⁵¹⁾. Přezkum by měl zahrnovat všechny aspekty fungování tohoto rozhodnutí, a zejména použití doplňkových pravidel (se zvláštní pozorností věnovanou ochranám poskytovaným v případě dalšího předávání), použití pravidel týkajících se souhlasu, včetně v případě odnětí, účinnost výkonu individuálních práv, jakož i omezení a záruky, pokud jde o přístup vlády, včetně ochranných mechanismů stanovených v příloze II tohoto rozhodnutí. Měl by rovněž zahrnovat účinnost dozoru a prosazování práva, pokud jde o pravidla platná jak pro podnikatelské subjekty nakládající s osobními informacemi, tak v oblasti prosazování trestního práva a národní bezpečnosti.
- (182) K provedení přezkumu by se Komise měla setkat s Komisí pro ochranu osobních informací, případně doprovázenou dalšími japonskými orgány odpovědnými za přístup vlády, včetně příslušných dozorových úřadů. Účast na této schůzce by měla být otevřena zástupcům členů Evropského sboru pro ochranu osobních údajů. V rámci společného přezkumu by Komise měla požadovat, aby Komise pro ochranu osobních informací poskytla souhrnné informace o všech aspektech relevantních pro zjištění o odpovídající úrovni ochrany, včetně omezení a záruk týkajících se přístupu ze strany vlády⁽¹⁵²⁾. Komise by měla rovněž požadovat vysvětlení jakýchkoli obdržených informací relevantních pro toto rozhodnutí, včetně veřejných zpráv japonských orgánů nebo jiných zúčastněných stran v Japonsku, Evropského sboru pro ochranu osobních údajů, jednotlivých úřadů pro ochranu osobních údajů, skupin občanské společnosti, tiskových zpráv nebo jakéhokoli jiného dostupného zdroje informací.
- (183) Na základě společného přezkumu by Komise měla připravit veřejnou zprávu, kterou předloží Evropskému parlamentu a Radě.

7. POZASTAVENÍ ROZHODNUTÍ O ODPOVÍDAJÍCÍ OCHRANĚ

- (184) Pokud Komise na základě pravidelných a *ad hoc* kontrol nebo jakýchkoli jiných dostupných informací dojde k závěru, že úroveň ochrany poskytovanou japonským právním řádem již nelze považovat za v zásadě rovnocennou ochraně poskytované v Evropské unii, měla by o tom informovat příslušné japonské orgány a požadovat, aby byla ve stanovené, přiměřené lhůtě přijata vhodná opatření. To zahrnuje pravidla použitelná jak pro podnikatelské subjekty, tak pro japonské orgány veřejné moci odpovědné za prosazování trestního práva nebo národní bezpečnost. Takový postup by mohl být například zahájen v případech, kdy další předávání, včetně předávání na základě rozhodnutí přijatých Komisí pro ochranu osobních informací podle článku 24 zákona o ochraně osobních informací uznávajících, že třetí země poskytuje rovnocennou úroveň ochrany, která je zaručena v Japonsku, již nebudou v rámci záruk zajišťujících kontinuitu ochrany ve smyslu článku 44 GDPR prováděna.
- (185) Pokud po uplynutí této stanovené lhůty příslušné japonské orgány uspokojivě neprokáží, že toto rozhodnutí nadále vychází z odpovídající úrovně ochrany, měla by Komise podle čl. 45 odst. 5 nařízení (EU) 2016/679 zahájit postup vedoucí k částečnému nebo úplnému pozastavení nebo zrušení tohoto rozhodnutí. Alternativně by Komise mohla zahájit postup pro změnu tohoto rozhodnutí, zejména tím, že se na předávání údajů budou vztahovat další podmínky, nebo že se omezí působnost zjištění o odpovídající úrovni ochrany jen na předávání údajů, u nichž je zaručena kontinuita ochrany ve smyslu článku 44 GDPR.

⁽¹⁵⁰⁾ Podle čl. 45 odst. 3 nařízení (EU) 2016/679 „[u]vedený prováděcí akt stanoví mechanismus pro pravidelný přezkum prováděný nejméně každé čtyři roky, který zohlední veškerý relevantní vývoj v dotčené třetí zemi nebo mezinárodní organizaci“.

⁽¹⁵¹⁾ V čl. 45 odst. 3 nařízení (EU) 2016/679 se stanoví, že pravidelný přezkum se musí provádět nejméně každé čtyři roky. Viz také Evropský sbor pro ochranu osobních údajů, Referenční rámec pro odpovídající ochranu, WP 254 rev. 01.

⁽¹⁵²⁾ Viz též příloha II, oddíl IV: „V rámci pravidelného přezkumu rozhodnutí o odpovídající ochraně si budou Komise pro ochranu osobních informací a Evropská komise vyměňovat informace o zpracování údajů za podmínek zjištění o odpovídající úrovni ochrany, včetně podmínek stanovených v tomto prohlášení.“

- (186) Zejména by Komise měla zahájit postup k pozastavení nebo zrušení tohoto rozhodnutí, pokud existují známky toho, že doplňková pravidla obsažená v příloze I nejsou podnikatelskými subjekty přijímajícími osobní údaje podle tohoto rozhodnutí dodržována a/nebo účinně vymáhána nebo že japonské orgány nedodržují prohlášení, ujištění a závazky obsažené v příloze II tohoto rozhodnutí.
- (187) Komise by rovněž měla zvážit zahájení postupu vedoucího ke změně, pozastavení nebo zrušení tohoto rozhodnutí, pokud v souvislosti se společným přezkumem nebo jinak neposkytnou příslušné japonské orgány informace nebo objasnění nezbytná k posouzení úrovně ochrany poskytované osobním údajům předávaným z Evropské unie do Japonska nebo dodržování tohoto rozhodnutí. V tomto směru by Komise měla vzít v potaz míru, do jaké lze relevantní informace získat z jiných zdrojů.
- (188) V naléhavých a řádně odůvodněných případech, například hrozí-li vážné porušení práv subjektů údajů, by Komise měla zvážit přijetí rozhodnutí o pozastavení nebo zrušení tohoto rozhodnutí, které by mělo být použitelné okamžitě, podle čl. 93 odst. 3 nařízení (EU) 2016/679 ve spojení s článkem 8 nařízení Evropského parlamentu a Rady (EU) č. 182/2011 ⁽¹⁵³⁾.

8. ZÁVĚREČNÉ ÚVAHY

- (189) Evropský sbor pro ochranu osobních údajů zveřejnil své stanovisko ⁽¹⁵⁴⁾, které bylo při přípravě tohoto rozhodnutí zohledněno.
- (190) Evropský parlament přijal usnesení o strategii v oblasti digitálního obchodu, které vyzývá Komisi, aby si jako prioritu vytyčila urychlení přijetí rozhodnutí o odpovídající ochraně s důležitými obchodními partnery za podmínek stanovených v nařízení (EU) 2016/679 jako důležitého mechanismu pro zajištění předávání osobních údajů z Evropské unie ⁽¹⁵⁵⁾. Evropský parlament přijal také usnesení o odpovídající úrovni ochrany osobních údajů v Japonsku ⁽¹⁵⁶⁾.
- (191) Opatření stanovená tímto rozhodnutím jsou v souladu se stanoviskem výboru zřízeného podle čl. 93 odst. 1 GDPR,

PŘIJALA TOTO ROZHODNUTÍ:

Článek 1

1. Pro účely článku 45 nařízení (EU) 2016/679 Japonsko zajišťuje odpovídající úroveň ochrany osobních údajů předávaných z Evropské unie podnikatelským subjektům nakládajícím s osobními informacemi v Japonsku podle zákona o ochraně osobních informací doplněného o doplňková pravidla stanovená v příloze I, společně s oficiálními prohlášeními, ujištěními a závazky obsaženými v příloze II.

⁽¹⁵³⁾ Nařízení Evropského parlamentu a Rady (EU) č. 182/2011 ze dne 16. února 2011, kterým se stanoví pravidla a obecné zásady způsobu, jakým členské státy kontrolují Komisi při výkonu prováděcích pravomocí (Úř. věst. L 55, 28.2.2011, s. 13).

⁽¹⁵⁴⁾ Stanovisko 28/2018 k návrhu prováděcího rozhodnutí Evropské komise o přiměřené ochraně osobních údajů v Japonsku, přijaté 5. prosince 2018.

⁽¹⁵⁵⁾ Usnesení Evropského parlamentu ze dne 12. prosince 2017 „Směrem ke strategii v oblasti digitálního obchodu“ (2017/2065(INI)). Viz zejména bod 8 („[...] připomíná, že osobní údaje mohou být předávány do třetích zemí, aniž by byla využívána obecná pravidla v obchodních dohodách, pokud jsou a budou splněny požadavky zakotvené v [...] kapitole V nařízení (EU) 2016/679; uznává, že základním mechanismem pro zajištění předávání osobních údajů z EU do třetí země jsou rozhodnutí o přiměřenosti, včetně parciálních a odvětvových rozhodnutí; konstatuje, že EU přijala rozhodnutí o přiměřenosti pouze se čtyřmi z 20 největších obchodních partnerů [...]“) a bod 9 („vyzývá Komisi, aby si jako prioritu vytyčila urychlení přijetí rozhodnutí o přiměřenosti, pokud třetí země prostřednictvím svých vnitrostátních právních předpisů nebo svých mezinárodních závazků zajistí úroveň ochrany, která bude „v zásadě rovnocenná“ ochraně zaručené v EU [...]“).

⁽¹⁵⁶⁾ Usnesení Evropského parlamentu ze dne 13. prosince 2018 o odpovídající úrovni ochrany osobních údajů v Japonsku (2018/2979(RSP)).

2. Toto rozhodnutí se nevztahuje na osobní údaje předávané příjemcům, kteří spadají do jedné z níže uvedených kategorií, v rozsahu, ve kterém účely zpracování osobních údajů zcela nebo částečně odpovídají jednomu z uvedených účelů, konkrétně:

- a) rozhlasové a televizní společnosti, vydavatelé novin, komunikační agentury nebo jiné tiskové organizace (včetně všech fyzických osob, které provozují tiskové činnosti jako své podnikání), pokud zpracovávají osobní údaje pro účelu tisku;
- b) osoby zabývající se profesionálním psaním, pokud toto psaní zahrnuje osobní údaje;
- c) vysoké školy a jakékoli jiné organizace nebo skupiny zaměřené na akademická studia nebo jakákoli osoba náležející do takové organizace nebo skupiny, pokud zpracovávají osobní údaje pro účely akademických studií;
- d) církevní instituce, pokud zpracovávají osobní údaje pro účely náboženské činnosti (včetně všech činností souvisejících),
a
- e) politické orgány, pokud zpracovávají osobní údaje pro účely své politické činnosti (včetně všech činností souvisejících).

Článek 2

Pokud příslušné orgány v členských státech za účelem ochrany fyzických osob s ohledem na zpracování jejich osobních údajů uplatní pravomoc podle článku 58 nařízení (EU) 2016/679 vedoucí k přerušení nebo trvalému zákazu toku údajů konkrétnímu podnikatelskému subjektu v Japonsku v rozsahu působnosti stanovené v článku 1, oznámí dotýčný členský stát tuto skutečnost bezodkladně Komisi.

Článek 3

1. Komise neustále monitoruje uplatňování právního rámce, na němž je založeno toto rozhodnutí, včetně podmínek, za kterých dochází k dalšímu předávání, s cílem posoudit, zda Japonsko i nadále zajišťuje odpovídající úroveň ochrany ve smyslu článku 1.
2. Členské státy a Komise se vzájemně informují o případech, kdy Komise pro ochranu osobních informací nebo jakýkoli jiný příslušný japonský orgán nezajišťuje soulad s právním rámcem, na němž je toto rozhodnutí založeno.
3. Členské státy a Komise se vzájemně informují o jakýchkoli známkách toho, že zásahy japonských orgánů veřejné moci do práva fyzických osob na ochranu jejich osobních údajů přesahují rámec toho, co je striktně nezbytné, nebo že proti takovým zásahům není účinná právní ochrana.
4. Do dvou let ode dne oznámení tohoto rozhodnutí členským státům a poté nejméně každé čtyři roky Komise vyhodnotí zjištění v čl. 1 odst. 1 na základě veškerých dostupných informací, včetně informací získaných v rámci společného přezkumu prováděného společně s příslušnými japonskými orgány.
5. Pokud má Komise informace o tom, že odpovídající úroveň ochrany již není zajištěna, informuje příslušné japonské orgány. Případně může rozhodnout o pozastavení, změně nebo zrušení tohoto rozhodnutí nebo o omezení jeho působnosti, jsou-li známky toho, že:
 - a) podnikatelské subjekty v Japonsku, které přijaly osobní údaje z Evropské unie podle tohoto rozhodnutí, nedodržují další záruky stanovené v doplňkových pravidlech obsažených v příloze I tohoto rozhodnutí nebo že v tomto ohledu jsou dozor a prosazování práva nedostačující;
 - b) japonské orgány veřejné moci nedodržují prohlášení, ujištění a závazky obsažené v příloze II tohoto rozhodnutí, včetně těch, které se týkají podmínek a omezení pro shromažďování osobních údajů předávaných podle tohoto rozhodnutí a přístupu k nim ze strany japonských orgánů veřejné moci pro účely prosazování trestního práva nebo národní bezpečnosti.

Komise může také předložit návrh opatření v případě, kdy nedostatečná spolupráce japonské vlády brání Komisi v určení, zda je dotčeno zjištění podle čl. 1 odst. 1 tohoto rozhodnutí.

Článek 4

Toto rozhodnutí je určeno členským státům.

V Bruselu dne 23. ledna 2019.

Za Komisi
Věra JOUROVÁ
členka Komise

PŘÍLOHA 1

DOPLŇKOVÁ PRAVIDLA PODLE ZÁKONA O OCHRANĚ OSOBNÍCH INFORMACÍ PRO NAKLÁDÁNÍ S OSOBNÍMI ÚDAJI PŘEDÁVANÝMI Z EU NA ZÁKLADĚ ROZHODNUTÍ O ODPOVÍDAJÍCÍ OCHRANĚ

Obsah

1) Osobní informace vyžadující zvláštní péči (čl. 2 odst. 3 zákona).	38
2) Uchovávané osobní údaje (čl. 2 odst. 7 zákona)	39
3) Stanovení účelu použití, omezení na základě účelu použití (čl. 15 odst. 1, čl. 16 odst. 1 a čl. 26 odst. 1 a 3 zákona)	40
4) Omezení poskytování informací třetí straně v cizí zemi (článek 24 zákona; článek 11-2 pravidel)	41
5) Anonymně zpracované informace (čl. 2 odst. 9 a čl. 36 odst. 1 a 2 zákona)	41

[Pojmy]

„zákon“	zákon o ochraně osobních informací (zákon č. 57 z roku 2003)
„nařízení kabinetu“	nařízení kabinetu o prosazování zákona o ochraně osobních informací (nařízení kabinetu č. 507 z roku 2003)
„pravidla“	pravidla prosazování zákona o ochraně osobních informací (pravidla Komise pro ochranu osobních informací č. 3 z roku 2016)
„pokyny k obecným pravidlům“	pokyny k zákonu o ochraně osobních informací (svazek o obecných pravidlech) (oznámení Komise pro ochranu osobních informací č. 65 z roku 2015)
„EU“	Evropská unie, včetně jejích členských států, a s ohledem na Dohodu o EHP Island, Lichtenštejnsko a Norsko
„GDPR“	nařízení Evropského parlamentu a Rady o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů)
„rozhodnutí o odpovídající ochraně“	rozhodnutí Evropské komise, že třetí země nebo území v dané třetí zemi atd. zaručuje odpovídající úroveň ochrany osobních údajů podle článku 45 GDPR

Komise pro ochranu osobních informací za účelem provádění vzájemného a bezproblémového předávání osobních údajů mezi Japonskem a EU označila EU za cizí zemi, která zavedla systém ochrany osobních údajů, jehož normy se z hlediska ochrany práv a zájmů fyzických osob na základě článku 24 zákona považují za rovnocenné normám v Japonsku, a Evropská komise současně rozhodla, že Japonsko zajišťuje odpovídající úroveň ochrany osobních údajů podle článku 45 GDPR.

Mezi Japonskem a EU tak bude docházet k vzájemnému a bezproblémovému předávání osobních údajů způsobem, který zajišťuje vysokou úroveň ochrany práv a zájmů fyzických osob. Aby byla zajištěna tato vysoká úroveň ochrany osobních informací obdržených z EU na základě rozhodnutí o odpovídající ochraně a s ohledem na skutečnost, že navzdory vysokému stupni konvergence mezi oběma systémy existují určité významné rozdíly, Komise pro ochranu osobních informací přijala tato doplňková pravidla, a to na základě ustanovení zákona o provádění atd. spolupráce s vládami v jiných zemích a s cílem zajistit vhodné nakládání s osobními informacemi získanými z EU na základě rozhodnutí o odpovídající ochraně podnikatelským subjektem nakládajícím s osobními informacemi a řádné a účinné provádění povinností stanovených v těchto pravidlech ⁽¹⁾.

⁽¹⁾ Článek 4, článek 6, článek 8, článek 24, článek 60 a článek 78 zákona a článek 11 pravidel.

Zejména článek 6 zákona stanoví pravomoc přijímat nezbytná legislativní a jiná opatření s cílem zajistit zvýšenou ochranu osobních informací a pomocí přísnějších pravidel, která doplňují pravidla stanovená zákonem a nařízením kabinetu a jdou nad jejich rámec, vytvořit mezinárodně vyhovující systém týkající se osobních informací. Komise pro ochranu osobních informací proto jako orgán odpovědný za řízení celkového provádění zákona má pravomoc stanovit podle článku 6 zákona přísnější předpisy tím, že vypracuje tato doplňková pravidla poskytující vyšší úroveň ochrany práv a zájmů fyzických osob, pokud jde o nakládání s osobními údaji získanými z EU na základě rozhodnutí o odpovídající ochraně, mimo jiné s ohledem na definici osobních informací vyžadujících zvláštní péči podle čl. 2 odst. 3 zákona a uchovávaných osobních údajů podle čl. 2 odst. 7 zákona (včetně příslušné doby uchovávání).

Na tomto základě jsou doplňková pravidla pro podnikatelský subjekt nakládající s osobními informacemi, který přijímá osobní údaje předávané z EU na základě rozhodnutí o odpovídající ochraně, závazná, a proto je musí splňovat. Jelikož jde o právně závazná pravidla, může Komise pro ochranu osobních informací veškerá práva a povinnosti vymáhat stejným způsobem jako ustanovení zákona, která doplňují přísnějšími a/nebo podrobnějšími pravidly. V případě porušení práv a povinností vyplývajících z doplňkových pravidel se mohou fyzické osoby domáhat nápravy u soudů stejným způsobem, jako v případě ustanovení zákona, která doplňují přísnějšími a/nebo podrobnějšími pravidly.

Pokud jde o vymáhání v případě, že podnikatelský subjekt nakládající s osobními informacemi nesplňuje jednu nebo několik povinností podle doplňkových pravidel, má Komise pro ochranu osobních informací pravomoc přijmout opatření podle článku 42 zákona. Pokud jde obecně o osobní informace obdržené z EU na základě rozhodnutí o odpovídající ochraně, považuje se skutečnost, že podnikatelský subjekt nakládající s osobními informacemi bez legitimního důvodu ⁽²⁾ nepřijal opatření v souladu s doporučením přijatým podle čl. 42 odst. 1 zákona, za závažné a bezprostřední porušení práv a zájmů fyzické osoby ve smyslu čl. 42 odst. 2 zákona.

1) Osobní informace vyžadující zvláštní péči (čl. 2 odst. 3 zákona).

čl. 2 odst. 3 zákona

3) „Osobními informacemi vyžadujícími zvláštní péči“ v tomto zákoně se rozumí osobní informace zahrnující rasu zmocnitele, jeho náboženské vyznání, společenské postavení, anamnézu, záznam v rejstříku trestů, utrpění újmy v důsledku trestného činu a jiné popisy určené nařízením kabinetu jako informace, s nimiž musí být nakládáno se zvláštní péčí, aby nedocházelo k nespravedlivé diskriminaci, předpojatosti nebo jinému znevýhodňování zmocnitele.

článek 2 nařízení kabinetu

Těmito popisy atd. podle nařízení kabinetu podle čl. 2 odst. 3 zákona jsou takové popisy atd., které obsahují některý z těchto následujících údajů (s výjimkou těch, které spadají pod lékařské záznamy nebo trestní rejstřík zmocnitele):

- i) skutečnost, že osoba má tělesné postižení, intelektové nebo mentální postižení (včetně vývojových poruch) nebo jiné tělesné nebo duševní funkční postižení podle pravidel Komise pro ochranu osobních informací;
- ii) výsledky lékařského vyšetření nebo jiného vyšetření (dále jen „lékařské vyšetření“) pro účely prevence a stanovení včasné diagnózy provedeného u zmocnitele lékařem nebo jinou osobou vykonávající uložené povinnosti související s léčbou (dále jen „lékař“);
- iii) skutečnost, že zmocnitel obdržel od lékaře na základě výsledků lékařského vyšetření nebo z důvodu onemocnění, zranění nebo jiných duševních a fyzických změn doporučení ke zlepšení duševních a fyzických podmínek nebo lékařskou péči či předpis;
- iv) skutečnost, že ve vztahu ke zmocniteli jako podezřelému nebo obžalovanému došlo k zatčení, prohlídce, zajištění, zadržení, trestnímu stíhání nebo jinému řízení;

⁽²⁾ Legitimním důvodem se rozumí událost mimořádné povahy mimo kontrolu podnikatelského subjektu nakládajícího s osobními informacemi, kterou nelze rozumně předpokládat (například přírodní katastrofy), nebo případy, kdy potřeba přijmout opatření v souvislosti s doporučením vydaným Komisí pro ochranu osobních informací podle čl. 42 odst. 1 zákona zanikla, neboť podnikatelský subjekt nakládající s osobními informacemi přijal alternativní opatření, která zajistila úplnou nápravu porušení.

- v) skutečnost, že proti zmocniteli jako mladistvému delikventovi nebo osobě podezřelé podle čl. 3 odst. 1 zákona o mladistvých bylo vedeno vyšetřování, použito opatření pro sledování a ochranu, slyšení a rozhodnutí, ochranné opatření nebo jiné postupy týkající se případu ochrany mladistvých.

článek 5 pravidel

Tělesným a duševním funkčním postižením podle pravidel Komise pro ochranu osobních informací podle čl. 2 bodu i) nařízení se rozumí postižení uvedená v následujících bodech:

- i) tělesná postižení uvedená v příložené tabulce zákona o zabezpečení osob s tělesným postižením (zákon č. 283 z roku 1949);
- ii) intelektová postižení uvedená v zákoně o zabezpečení osob s intelektovým postižením (zákon č. 37 z roku 1960);
- iii) mentální postižení podle zákona o mentálním zdraví a zabezpečení osob s mentálním postižením (zákon č. 123 z roku 1950) (včetně vývojových poruch podle čl. 2 odst. 1 zákona o podpoře osob s vývojovými poruchami, kromě intelektových postižení podle zákona o zabezpečení osob s intelektovým postižením);
- iv) nemoc bez možnosti léčení nebo jiná nemoc, jejíž závažnost podle nařízení kabinetu podle čl. 4 odst. 1 zákona o komplexní podpoře každodenního a sociálního života osob se zdravotním postižením (zákon č. 123 z roku 2005) odpovídá závažnosti stanovené ministrem zdravotnictví, práce a sociálních věcí v uvedeném odstavci.

Pokud osobní údaje získané z EU na základě rozhodnutí o odpovídající ochraně obsahují údaje týkající se sexuálního života nebo sexuální orientace fyzické osoby nebo jejího členství v odborových organizacích, které jsou podle obecného nařízení o ochraně osobních údajů definovány jako zvláštní kategorie osobních údajů, jsou podnikatelské subjekty nakládající s osobními informacemi povinny s těmito osobními údaji nakládat stejným způsobem jako s osobními informacemi vyžadujícími zvláštní péči ve smyslu čl. 2 odst. 3 zákona.

2) Uchovávané osobní údaje (čl. 2 odst. 7 zákona)

čl. 2 odst. 7 zákona

- 7) „Uchovávanými osobními údaji“ se v tomto zákoně rozumí osobní informace, které podnikatelský subjekt nakládající s osobními informacemi je oprávněn zveřejnit, opravit, doplnit jejich obsah nebo jej vypustit, přestat používat, vymazat či je přestat poskytovat třetí straně a mezi něž nepatří údaje, které podle nařízení kabinetu mohou poškodit veřejné či jiné zájmy, pokud se objeví informace o jejich přítomnosti nebo absenci, ani údaje, které mají být vymazány ve lhůtě maximálně jednoho roku předepsané nařízením kabinetu.

článek 4 nařízení kabinetu

Informace určené nařízením kabinetu podle čl. 2 odst. 7 jsou informace uvedené v následujících bodech:

- i) informace, v jejichž souvislosti existuje možnost, že pokud se objeví informace o jejich přítomnosti nebo absenci, způsobilo by to újmu na životě, zdraví nebo majetku zmocnitele nebo třetí strany;
- ii) informace, v jejichž souvislosti existuje možnost, že pokud se objeví informace o jejich přítomnosti nebo absenci, motivovalo by to nebo vedlo k protiprávnímu nebo nepoctivému jednání;
- iii) informace, v jejichž souvislosti existuje možnost, že pokud se objeví informace o jejich přítomnosti nebo absenci, narušilo by to národní bezpečnost, zničilo vztah důvěry s cizí zemí nebo mezinárodní organizací nebo by to znamenalo nevýhodu při vyjednávání s cizí zemí nebo mezinárodní organizací;
- iv) informace, v jejichž souvislosti existuje možnost, že pokud se objeví informace o jejich přítomnosti nebo absenci, bránilo by to zachování veřejné bezpečnosti a pořádku, například předcházení, potlačování nebo vyšetřování trestného činu.

článek 5 nařízení kabinetu

Lhůta předepsaná nařízením kabinetu podle čl. 2 odst. 7 zákona činí šest měsíců.

S osobními údaji obdrženými z EU, které jsou založeny na rozhodnutí o odpovídající ochraně, se musí nakládat jako s uchovávanými osobními údaji ve smyslu čl. 2 odst. 7 zákona bez ohledu na lhůtu, v níž mají být vymazány.

Pokud osobní údaje získané z EU na základě rozhodnutí o odpovídající ochraně spadají mezi osobní údaje, které podle kabinetu „mohou poškodit veřejné či jiné zájmy, pokud se objeví informace o jejich přítomnosti nebo absenci“, nemusí se s těmito údaji nakládat jako s uchovávanými osobními údaji (viz článek 4 nařízení kabinetu; pokyny k obecným pravidlům, článek „2-7. Uchovávané osobní údaje“).

3) Stanovení účelu použití, omezení na základě účelu použití (čl. 15 odst. 1, čl. 16 odst. 1 a čl. 26 odst. 1 a 3 zákona)

čl. 15 odst. 1 zákona

1) Podnikatelský subjekt nakládající s osobními informacemi musí při nakládání s osobními informacemi co nejpřesněji uvést účel použití osobních informací (dále jen „účel použití“).

čl. 16 odst. 1 zákona

1) Podnikatelský subjekt nakládající s osobními informacemi nesmí bez předchozího souhlasu zmocnitele nakládat s osobními informacemi nad rámec rozsahu, který je nezbytný pro dosažení účelu použití stanoveného podle ustanovení předchozího článku.

čl. 26 odst. 1 a 3 zákona

1) Podnikatelský subjekt nakládající s osobními informacemi potvrzuje při přijímání osobních údajů od třetí strany níže uvedené skutečnosti v souladu s pravidly Komise pro ochranu osobních informací. (vynechané)

i) (vynechané)

ii) okolnosti, za kterých daná třetí strana uvedené osobní údaje získala.

3) Podnikatelský subjekt nakládající s osobními informacemi po potvrzení podle ustanovení odstavce 1 zaznamená podle pravidel Komise pro ochranu osobních informací datum, kdy osobní údaje obdržel, skutečnosti týkající se uvedeného potvrzení a další záležitosti předepsané v pravidlech Komise pro ochranu osobních informací.

Pokud podnikatelské subjekty nakládající s osobními informacemi nakládají s osobními informacemi nad rámec rozsahu nezbytného pro dosažení účelu použití stanoveného v čl. 15 odst. 1 zákona, musí získat předchozí souhlas zmocnitele (čl. 16 odst. 1 zákona). Při přijímání osobních údajů od třetí strany potvrdí podnikatelský subjekt nakládající s osobními informacemi v souladu s pravidly takové skutečnosti, jako jsou okolnosti, za nichž daná třetí strana uvedené osobní údaje získala, a tyto skutečnosti zaznamená (čl. 26 odst. 1 a 3 zákona).

Pokud podnikatelský subjekt nakládající s osobními informacemi obdrží osobní údaje z EU na základě rozhodnutí o odpovídající ochraně, okolnosti týkající se získání uvedených osobních údajů, které mají být potvrzeny a zaznamenány podle čl. 26 odst. 1 a 3, zahrnují účel použití, pro který byly tyto informace z EU přijaty.

Obdobně v případě, kdy podnikatelský subjekt nakládající s osobními informacemi obdrží od jiného podnikatelského subjektu nakládajícího s osobními informacemi osobní údaje předtím předané z EU na základě rozhodnutí o odpovídající ochraně, okolnosti týkající se získání uvedených osobních údajů, které mají být potvrzeny a zaznamenány podle čl. 26 odst. 1 a 3, zahrnují účel použití, pro který byly tyto informace přijaty.

Ve výše uvedených případech má podnikatelský subjekt nakládající s osobními informacemi povinnost konkrétně stanovit účel použití uvedených osobních údajů v rámci rozsahu účelu použití, pro který byly údaje původně nebo následně získány, jak je potvrzeno a zaznamenáno podle čl. 26 odst. 1 a 3, a používat uvedené údaje v rámci tohoto rozsahu (jak je vymezeno v čl. 15 odst. 1 a čl. 16 odst. 1 zákona).

4) Omezení poskytování informací třetí straně v cizí zemi (článek 24 zákona; článek 11-2 pravidel)

článek 24 zákona

Kromě případů uvedených v jednotlivých bodech odstavce 1 předchozího článku podnikatelský subjekt nakládající s osobními informacemi musí v případě poskytnutí osobních údajů třetí straně (kromě osoby, která zřídí systém vyhovující normám vymezeným v pravidlech Komise pro ochranu osobních informací jako nezbytné pro průběžné přijímání opatření rovnocenných opatřením, která přijímá podnikatelský subjekt nakládající s osobními informacemi, pokud jde o nakládání s osobními údaji podle ustanovení tohoto oddílu; rovněž dále v tomto článku) v cizí zemi (tedy v zemi nebo regionu mimo území Japonska; rovněž dále) (kromě zemí uvedených v pravidlech Komise pro ochranu osobních informací jako cizí země, která zavedla systém ochrany osobních údajů, jehož normy se z hlediska ochrany práv a zájmů fyzických osob považují za rovnocenné normám v Japonsku; rovněž dále v tomto článku), získat předchozí souhlas zmocnitele v tom smyslu, že souhlasí s poskytnutím informací třetí straně v cizí zemi. V takovém případě se ustanovení předcházejícího článku nepoužijí.

článek 11-2 pravidel

Normy předepsané v pravidlech Komise pro ochranu osobních informací podle článku 24 zákona spadají do kteréhokoli z následujících bodů:

- i) podnikatelský subjekt nakládající s osobními informacemi a osoba, která přijímá osobní údaje, zajistily s ohledem na nakládání s osobními údaji osobou, která je přijímá, provedení opatření v souladu cílem ustanovení kapitoly IV oddílu 1 zákona vhodnou a přiměřenou metodou;
- ii) osoba, která přijímá osobní údaje, získala uznání na základě mezinárodního rámce pro nakládání s osobními informacemi.

Podnikatelský subjekt nakládající s osobními informacemi v případech poskytování osobních údajů, které obdržel z EU na základě rozhodnutí o odpovídající ochraně, třetí straně v cizí zemi musí získat předchozí souhlas zmocnitele v tom smyslu, že souhlasí s poskytnutím informací třetí straně v cizí zemi podle článku 24 zákona poté, co mu byly poskytnuty informace o okolnostech předání nezbytné k tomu, aby mohl zmocnitel o svém souhlasu rozhodnout, kromě případů spadajících pod jeden z následujících bodů i) až iii);

- i) pokud se třetí strana nachází v zemi vymezené v pravidlech jako cizí země, která zavádí systém ochrany osobních údajů, jehož normy se z hlediska ochrany práv a zájmů fyzických osob považují za rovnocenné normám v Japonsku;
- ii) pokud podnikatelský subjekt nakládající s osobními informacemi a třetí strana, která přijímá osobní údaje, ve vztahu k nakládání s osobními údaji třetí stranou společně zavedly opatření poskytující úroveň ochrany, která je rovnocenná zákonu ve spojení s těmito pravidly, a to prostřednictvím vhodné a přiměřené metody (např. smlouvy, jiných forem závazných dohod nebo závazných ujednání v rámci skupiny podniků);
- iii) v případech, na které se vztahují jednotlivé body čl. 23 odst. 1 zákona.

5) Anonymně zpracované informace (čl. 2 odst. 9 a čl. 36 odst. 1 a 2 zákona)

čl. 2 odst. 9 zákona

- 9) „Anonymně zpracovanými informacemi“ se v tomto zákoně rozumí informace týkající se fyzické osoby, které lze získat zpracováním osobních informací tak, aby nebylo možné identifikovat konkrétní fyzickou osobu přijetím opatření vymezených v každém z následujících bodů v souladu s rozdělením osobních informací uvedených v každém uvedeném bodě, ani dané osobní informace obnovit:

- i) osobní informace, na které se vztahuje odst. 1 bod i);

Vymazání části popisů atd. obsažených v uvedených osobních informacích (včetně nahrazení uvedené části popisu atd. jinými popisy atd. metodou, která nevykazuje pravidelnost, podle níž by mohla být uvedená část popisů atd. obnovena);

- ii) osobní informace, na které se vztahuje odst. 1 bod ii);

Vymazání všech individuálních identifikačních kódů obsažených v uvedených osobních informacích (včetně nahrazení uvedených individuálních identifikačních kódů jinými popisy atd. metodou, která nevykazuje pravidelnost, podle níž by mohly být uvedené individuální identifikační kódy obnoveny).

čl. 36 odst. 1 zákona

- 1) Podnikatelský subjekt nakládající s osobními informacemi musí při vytváření anonymně zpracovávaných osobních informací (pouze ty, které tvoří databázi anonymně zpracovávaných informací atd.; rovněž dále) zpracovávat osobní informace v souladu s normami, které jsou v pravidlech Komise pro ochranu osobních informací stanoveny jako nezbytné pro to, aby se znemožnilo určení konkrétní fyzické osoby a obnovily osobní informace použité k jejich vytvoření.

článek 19 pravidel

Normy stanovené v pravidlech Komise pro ochranu osobních informací podle čl. 36 odst. 1 zákona jsou tyto:

- i) vymazání celých popisů atd. nebo jejich části na jejichž základě lze identifikovat konkrétní fyzickou osobu, které se osobní informace týkají (včetně nahrazení těchto popisů atd. jinými popisy atd. metodou, která nevykazuje pravidelnost, podle níž by mohly být celé popisy atd. nebo jejich část obnovena);
- ii) vymazání všech individuálních identifikačních kódů obsažených v osobních informacích (včetně nahrazení těchto kódů jinými popisy atd. metodou, která nevykazuje pravidelnost, podle níž by mohly být individuální identifikační kódy obnoveny);
- iii) vymazání těchto kódů (pouze těch kódů, které vzájemně propojují více informací a které podnikatelský subjekt nakládající s osobními informacemi skutečně používá), které propojují osobní informace a informace získané přijetím opatření ve vztahu k osobním informacím (včetně nahrazení uvedených kódů jinými kódy, na jejichž základě nelze propojit uvedené osobní informace a informace získané přijetím opatření ve vztahu k uvedeným osobním informacím metodou, která nevykazuje pravidelnost, podle níž by mohly být uvedené kódy obnoveny);
- iv) vymazání idiosynkratických popisů atd. (včetně nahrazení těchto popisů atd. jinými popisy atd. metodou, která nevykazuje pravidelnost, podle níž by mohly být idiosynkratické popisy obnoveny);
- v) vedle opatření stanovených v každém předchozím bodě přijetí vhodných opatření na základě výsledků zohlednění charakteristických znaků atd. databáze osobních informací atd., jako je rozdíl mezi popisy atd. obsaženými v osobních informacích a popisy atd. obsaženými v jiných osobních informacích tvořících databázi osobních informací atd., která zahrnují uvedené osobní informace.

čl. 36 odst. 2 zákona

- 2) Podnikatelský subjekt nakládající s osobními informacemi musí při vytváření anonymně zpracovávaných osobních informací v souladu s normami, které jsou v pravidlech Komise pro ochranu osobních informací stanoveny jako nezbytné k zamezení úniku informací souvisejících s uvedenými popisy atd. a individuálními identifikačními kódy, které byly vymazány z osobních informací použitých k vytváření anonymně zpracovávaných informací, a informací souvisejících s metodou zpracování použitou podle ustanovení přechozího odstavce, přijmout opatření pro kontrolu zabezpečení těchto informací.

článek 20 pravidel

Normy stanovené v pravidlech Komise pro ochranu osobních informací podle čl. 36 odst. 2 zákona jsou tyto:

- i) jasné vymezení pravomoci a odpovědnosti osoby nakládající s informacemi týkajícími se uvedených popisů atd. a individuálními identifikačními kódy, které byly vymazány z osobních informací použitých k vytváření anonymně zpracovávaných informací, a informace související s metodou zpracování použitou podle ustanovení čl. 36 odst. 1 zákona (omezeno na ty, které mohou obnovit osobní informace použitím těchto souvisejících informací) (dále v tomto článku jen „informace související s metodou zpracování atd.“)
- ii) zavedení pravidel a postupů, pokud jde o nakládání s informacemi souvisejícími s metodou zpracování atd., vhodné nakládání s informacemi souvisejícími s metodou zpracování atd. v souladu s pravidly a postupy, hodnocení situace nakládání s informacemi a přijímání nezbytných opatření na základě výsledků těchto hodnocení s cílem dosáhnout zlepšení;
- iii) přijetí nezbytných a vhodných opatření s cílem zabránit osobě bez zákonné pravomoci nakládat s informacemi souvisejícími s metodou zpracování atd. v nakládání s informacemi týkajícími se způsobu zpracování.

Osobní informace obdržené od EU na základě rozhodnutí o odpovídající ochraně se považují za anonymně zpracované informace ve smyslu čl. 2 odst. 9 zákona pouze v případě, jestliže podnikatelský subjekt nakládající s osobními informacemi přijme opatření, na jejichž základě bude anonymizace fyzické osoby pro všechny nevratná, včetně vymazání informací souvisejících s metodou zpracování atd. (vymezených jako informace související s popisy atd. a individuálními identifikačními kódy, které byly vymazány z osobních informací použitých k vytváření anonymně zpracovávaných informací, a informace související s metodou zpracování použitou podle ustanovení čl. 36 odst. 1 zákona (omezeno na ty, které mohou obnovit osobní informace použitím těchto souvisejících informací)).

PŘÍLOHA 2

Její Excellence Věra Jourová, komisařka pro spravedlnost, spotřebitele a rovnost žen a mužů

Vaše Excellence,

velice vítám konstruktivní jednání mezi Japonskem a Evropskou komisí, jejichž cílem je vytvořit rámec pro vzájemné předávání osobních údajů mezi Japonskem a EU.

Na žádost Evropské komise, která byla určena vládě Japonska, Vám v příloze zasílám dokument, který obsahuje přehled o právním rámci pro přístup vlády Japonska k informacím.

Tento dokument se týká mnoha ministerstev a agentur vlády Japonska. Příslušná ministerstva a agentury (sekretariát kabinetu, Národní policejní agentura, Komise pro ochranu osobních informací, Ministerstvo vnitra a komunikací, Ministerstvo spravedlnosti, Zpravodajská služba pro veřejnou bezpečnost, Ministerstvo obrany) v rámci svých příslušných pravomocí obsahově odpovídají za pasáže tohoto dokumentu. Níže naleznete příslušná ministerstva a agentury a odpovídající podpisy.

Komise pro ochranu osobních informací přijímá veškeré dotazy k tomuto dokumentu a bude koordinovat nezbytné odpovědi u příslušných ministerstev a agentur.

Doufám, že tento dokument bude pro rozhodování v Evropské komisi přínosný.

Děkujeme Vám za cenný příspěvek, který jste v této záležitosti dosud poskytli.

S pozdravem

Yoko Kamikawa

ministryně spravedlnosti

Tento dokument byl vypracován Ministerstvem spravedlnosti a níže uvedenými ministerstvy a úřady.

Koichi Hamano

poradce, sekretariát kabinetu

Schunichi Kuryu

vrchní komisař Národní policejní agentury

Mari Sonoda

generální tajemnice, Komise pro ochranu osobních informací

Mitsuru Yasuda

náměstek ministra, Ministerstvo vnitra a komunikací

Seimei Nakagawa

Zpravodajská služba pro veřejnou bezpečnost

Kenichi Takahashi

administrativní náměstek ministra obrany

14. září 2018

Shromažďování a používání osobních informací japonskými orgány veřejné moci pro účely prosazování trestního práva a národní bezpečnosti

Následující dokument poskytuje přehled o právním rámci pro shromažďování a používání osobních (elektronických) informací japonskými orgány veřejné moci pro účely prosazování trestního práva a národní bezpečnosti (dále jen „přístup vlády“), zejména pokud jde o dostupné právní základy, platné podmínky (omezení) a záruky, včetně nezávislého dozoru a možností individuální ochrany. Toto prohlášení je určeno Evropské komisi s cílem vyjádřit závazek a poskytnout záruky, že přístup vlády k osobním informacím předávaným z EU do Japonska bude omezen na to, co je nezbytné a přiměřené, že přístup bude podléhat nezávislému doзору a že dotčené osoby se budou moci domáhat nápravy v případě jakéhokoli případného porušení jejich základního práva na soukromí a ochranu údajů. Tímto prohlášením se zároveň zavádí nový ochranný mechanismus spravovaný Komisí pro ochranu osobních informací, v jehož rámci budou vyřizovány stížnosti fyzických osob z EU na přístup vlády k jejich osobním údajům předávaným z EU do Japonska.

I. Obecné právní zásady týkající se přístupu vlády

V rámci výkonu veřejné moci musí být při přístupu vlády v plném rozsahu dodržovány právní předpisy (zásada zákonitosti). V Japonsku jsou osobní informace chráněny jak v soukromém, tak i veřejném sektoru víceúrovňovým mechanismem.

A. Ústavní rámec a výhrada právní zásady

Právo na soukromí a ochranu údajů se uznává v článku 13 Ústavy a v judikatuře jako ústavní právo. V tomto ohledu Nejvyšší soud konstatoval, že je přirozené, že si fyzické osoby nepřejí, aby ostatní bez dobrého důvodu znali jejich osobní informace, a že toto očekávání by mělo být chráněno⁽¹⁾. Další ochrana je zakotvena v čl. 21 odst. 2 Ústavy, který zajišťuje respektování důvěrnosti sdělení, a článek 35 Ústavy, který zaručuje právo nebyť předmětem prohlídky a zajištění věci bez soudního příkazu, což znamená, že shromažďování osobních informací, včetně přístupu, povinnými prostředky může být prováděno vždy jen na základě soudního příkazu. Takový příkaz může být vydán pouze pro vyšetřování již spáchaného trestného činu. Právní rámec Japonska proto shromažďování informací povinnými prostředky pro účely (nikoli trestního vyšetřování, ale) národní bezpečnosti nepovoluje.

Navíc musí být povinné shromažďování informací s výhradou právní zásady konkrétně podloženo právními předpisy. V případě nepovinného/dobrovolného shromažďování se informace získávají ze zdroje, k němuž má přístup kdokoli, nebo na základě žádosti o dobrovolné zpřístupnění, tedy žádosti, kterou nelze vymáhat od fyzické nebo právnické osoby, která je držitelem těchto informací. To je ovšem přípustné jen do té míry, do jaké je orgán veřejné moci příslušný k provádění vyšetřování, jelikož každý orgán veřejné moci může jednat pouze v rámci své správní příslušnosti stanovené zákonem (bez ohledu na to, zda jeho činnosti zasahují do práv a svobod fyzických osob). Tato zásada platí i pro schopnost orgánu shromažďovat osobní informace.

B. Zvláštní pravidla pro ochranu osobních informací

Zákon o ochraně osobních informací a zákon o ochraně osobních informací uchovávaných správními orgány, které jsou založeny na ústavních ustanoveních a dále je upřesňují, zaručují právo na osobní informace v soukromém i veřejném sektoru.

Podle článku 7 zákona o osobních informacích musí Komise pro ochranu osobních informací formulovat „Základní politiku ochrany osobních informací“ (základní politika). Tato základní politika, která je přijata na základě rozhodnutí kabinetu Japonska jako ústředního orgánu japonské vlády (předsedy vlády a ministrů), určuje směr pro ochranu osobních informací v Japonsku. Tímto způsobem funguje Komise pro ochranu osobních informací jako nezávislý orgán dozoru a slouží jako „velící středisko“ japonského systému ochrany osobních informací.

Kdykoli správní orgány shromažďují osobní informace a nezávisle na tom, zda tak činí povinnými nebo nepovinnými prostředky, musí v zásadě⁽²⁾ dodržovat požadavky zákona o ochraně osobních informací uchovávaných správními orgány. Zákon o ochraně osobních informací uchovávaných správními orgány je obecným zákonem, který se vztahuje na zpracování „uchovávaných osobních informací“⁽³⁾ „správními orgány“ (podle definice v čl. 2 odst. 1 uvedeného

⁽¹⁾ Rozsudek Nejvyššího soudu ze dne 12. září 2003 (2002 (Ju) č.1656).

⁽²⁾ Výjimky ve vztahu ke kapitole 4 zákona o ochraně osobních informací uchovávaných správními orgány viz s. 16 níže.

⁽³⁾ „Uchovávané osobní informace“ podle čl. 2 odst. 5 zákona o ochraně osobních informací uchovávaných správními orgány označují osobní informace, které zaměstnanec správního orgánu vypracoval nebo získal při výkonu svých povinností a které má tento správní orgán k dispozici pro organizační použití svými zaměstnanci.

zákona). Proto se vztahuje i na zpracování údajů v oblasti prosazování trestního práva a národní bezpečnosti. S výjimkou prefekturní policie se u všech orgánů veřejné moci, které mají oprávnění k vládnímu přístupu, jedná o státní orgány, které spadají pod definici „správních orgánů“. Nakládání s osobními informacemi ze strany prefekturní policie upravují prefekturní nařízení⁽⁴⁾, v nichž jsou stanoveny zásady ochrany osobních informací, práva a povinnosti, které jsou rovnocenné zásadám, právům a povinnostem uvedeným v zákoně o ochraně osobních informací uchovávaných správními orgány.

II. Vládní přístup pro účely prosazování trestního práva

A) Právní základy a omezení

1) Shromažďování osobních informací povinnými prostředky

a) Právní základ

Podle článku 35 Ústavy nesmí být porušeno právo všech osob na ochranu svobody domovní, písemností a majetku před přístupem, prohlídkami a zajištěním věci, s výjimkou případů, kdy byl vydán soudní příkaz na základě „přiměřeného důvodu“, v němž jsou zejména popsána místa, která je třeba prohledat, a věci, které mají být zajištěny. Proto smí orgán veřejné moci shromažďovat elektronické informace povinnými prostředky v rámci trestního vyšetřování pouze na základě soudního příkazu. To platí jak pro shromažďování elektronických záznamů obsahujících (osobní) informace, tak pro odposlech komunikací v reálném čase. Jedinou výjimkou z tohoto pravidla (která však není relevantní v souvislosti s elektronickým přenosem osobních údajů ze zahraničí) je čl. 220 odst. 1 trestního řádu⁽⁵⁾ podle něhož může státní zástupce, asistent státního zástupce nebo příslušník soudní policie, pokud zadrží podezřelého nebo „zjevného pachatele“ v případě potřeby provést prohlídku nebo zajištění věci „na místě při zadržení“.

V čl. 197 odst. 1 trestního řádu se stanoví, že povinná opatření pro vyšetřování se „nepoužijí, pokud trestní řád neobsahuje zvláštní ustanovení“. Pokud jde o povinné shromažďování elektronických informací, relevantním právním základem v tomto ohledu je čl. 218 odst. 1 trestního řádu (podle něhož může státní zástupce, asistent státního zástupce nebo příslušník soudní policie, pokud je to nezbytné pro vyšetřování trestného činu, provést prohlídku, zajištění věci nebo inspekci na základě příkazu vydaného soudcem) a článek 222-2 trestního řádu (podle něhož se povinná opatření pro odposlech elektronických komunikací bez souhlasu některé ze stran provádějí na základě jiných zákonů). V druhém z uvedených ustanovení se odkazuje na zákon o odposleších pro trestní vyšetřování (dále jen „zákon o odposleších“), který ve svém čl. 3 odst. 1 stanoví podmínky, za nichž lze odposlouchávat komunikaci týkající se určitých závažných trestných činů na základě příkazu k odposlechu vydaného soudcem⁽⁶⁾.

Pokud jde o policii, vyšetřujícím orgánem je ve všech případech prefekturní policie, zatímco Národní policejní agentura neprovádí žádná trestní vyšetřování na základě trestního řádu.

b) Omezení

Povinné shromažďování elektronických informací je omezené Ústavou a opravňujícím statutem, jak je vyloženo v judikatuře, kterými se zejména upravují kritéria, která mají soudy uplatňovat při vydávání soudních příkazů. Zákon o ochraně osobních informací uchovávaných správními orgány navíc ukládá řadu omezení, která se uplatňují jak na shromažďování informací, tak na nakládání s nimi (a místní vyhlášky v zásadě předepisují stejná kritéria pro prefekturní policii).

1) Omezení vyplývající z Ústavy a opravňujícího statutu

Podle čl. 197 odst. 1 trestního řádu se povinná opatření použijí jen tehdy, pokud trestní řád obsahuje zvláštní ustanovení. V čl. 218 odst. 1 trestního řádu se pak stanoví, že zajištění věci atd. lze provést na základě příkazu vydaného soudcem pouze v případě, „pokud je to nezbytné pro vyšetřování trestného činu“. Ačkoli kritéria pro posouzení nezbytnosti nejsou

⁽⁴⁾ Každá prefektura má své vlastní „prefekturní nařízení“ pro ochranu osobních informací prefekturní policií. Tato prefekturní nařízení nejsou k dispozici v anglickém překladu.

⁽⁵⁾ Podle čl. 220 odst. 1 trestního řádu může státní zástupce, asistent státního zástupce nebo příslušník soudní policie, pokud zadrží podezřelého, v případě potřeby přijmout následující opatření: a) vstup do sídla jiné osoby atd. za účelem pátrání po podezřelé osobě; b) prohlídka, zajištění věci nebo inspekce na místě při zadržení.

⁽⁶⁾ V tomto ustanovení se konkrétně stanoví, že „státní zástupce nebo soudní policie mohou v případech, které spadají pod některý z těchto bodů, pokud existuje situace dostatečná pro podezření, že se skuteční komunikace týkající se spáchání, příprav, spiknutí, pokud jde o následná opatření, jako je například utajování důkazů, pokyny a jinou vzájemnou komunikaci o trestném činu, které jsou uvedené v každém z uvedených bodů (v druhém a třetím bodě dále jen „sériová trestná činnost“), jakož i komunikace obsahující otázky týkající se uvedené trestné činnosti (v tomto odstavci dále jen „komunikace týkající se trestné činnosti“) a v případech, kdy je mimořádně obtížné identifikovat pachatele nebo objasnit situaci/podrobnosti spáchání trestného činu jiným způsobem, odposlouchávat komunikaci týkající se trestné činnosti na základě příkazu k odposlechu vydaného soudcem ohledně prostředků komunikace, které jsou určeny telefonním číslem a dalšími čísly/kódy pro identifikaci zdroje nebo místa, kde se nachází telefon, a používá je podezřelý na základě smlouvy s telekomunikačními operátory atd. (s výjimkou těch, které lze považovat za případy bez podezření, že se použijí jako „komunikace týkající se trestné činnosti“), nebo v případech, kdy existují důvody pro podezření, že se používají jako „komunikace týkající se trestné činnosti“, lze provést odposlech komunikace týkající se trestné činnosti tímto komunikačním prostředkem.“

v právních předpisech dále specifikována, Nejvyšší soud ⁽⁷⁾ rozhodl, že soudce by při posuzování nezbytnosti měl provést celkové posouzení a přitom vzít v úvahu zejména tyto prvky:

- a) závažnost trestného činu a způsob jeho spáchání;
- b) hodnotu a důležitost materiálů, které mají být zajištěny jako důkaz;
- c) pravděpodobnost zatajení nebo zničení zajištěných materiálů;
- d) míru znevýhodnění způsobeného zajištěním;
- e) další související podmínky.

Omezení vyplývají rovněž z požadavku „přiměřeného důvodu“ stanoveného v článku 35 Ústavy. Podle normy „přiměřeného důvodu“ mohou být vydány soudní příkazy, pokud: 1. je potřeba zahájit trestní vyšetřování (viz rozsudek Nejvyššího soudu ze dne 18. března 1969, (1968 (Shi) č.100) zmíněný výše), 2. existuje situace, kdy se má za to, že podezřelý (obviněný) spáchal trestný čin (čl. 156 odst. 1 trestního řádu) ⁽⁸⁾, 3. příkaz k vyšetřování osoby, předmětů, bydliště nebo jakéhokoli jiného místa osoby jiné, než je obviněná osoba, by měl být vydán pouze tehdy, pokud lze důvodně předpokládat, že existují předměty, které by měly být zajištěny (čl. 102 odst. 2 trestního řádu). Pokud se soudce domnívá, že listinné důkazy, které předložily vyšetřovací orgány, nepředstavují dostatečné důvody pro podezření na trestný čin, žádost o vydání soudního příkazu zamítne. V tomto ohledu je třeba poznamenat, že podle zákona o trestání organizovaného zločinu a o kontrole výnosů z trestné činnosti představují „přípravné úkony ke spáchání“ plánované trestné činnosti (např. příprava peněz na spáchání teroristického trestného činu) samy o sobě trestný čin, a mohou proto podléhat povinnému vyšetřování na základě soudního příkazu.

V neposlední řadě, pokud se soudní příkaz týká vyšetřování osoby, předmětů, bydliště nebo jakéhokoli jiného místa osoby jiné, než je podezřelá nebo obviněná osoba, je vydán pouze tehdy, pokud lze důvodně předpokládat, že existují předměty, které mají být zajištěny (čl. 102 odst. 2 a čl. 222 odst. 1 trestního řádu).

Pokud jde konkrétně o odposlech komunikace pro účely trestního vyšetřování na základě zákona o odposleších, může být prováděn pouze tehdy, jsou-li splněny přísné požadavky stanovené v čl. 3 odst. 1 uvedeného zákona. Podle uvedeného ustanovení se pro odposlech vždy předem vyžaduje soudní příkaz, který může být vydán pouze v omezených situacích ⁽⁹⁾.

2) Omezení vyplývající ze zákona o ochraně osobních informací uchovávaných správními orgány

Pokud jde o shromažďování ⁽¹⁰⁾ osobních informací a další nakládání s těmito informacemi (mimo jiné zejména jejich uchovávání, správu a používání) ze strany správních orgánů, stanoví zákon o ochraně osobních informací uchovávaných správními orgány především tato omezení:

- a) Podle čl. 3 odst. 1 zákona o ochraně osobních informací uchovávaných správními orgány mohou správní orgány uchovávat osobní informace, pouze pokud je uchovávání nezbytné k plnění povinností spadajících do jejich pravomoci stanovené právními předpisy. Při uchovávání se od nich rovněž požaduje, aby (v co největší míře) uváděly účel použití osobních informací. Podle čl. 3 odst. 2 a 3 zákona o ochraně osobních informací uchovávaných správními orgány nesmí správní orgány uchovávat osobní informace nad rámec toho, co je nezbytné pro dosažení takto určeného účelu použití, a nesmí změnit účel použití nad rámec toho, co lze přiměřeně považovat za relevantní pro původní účel.
- b) V článku 5 zákona o ochraně osobních informací uchovávaných správními orgány se stanoví, že vedoucí správního orgánu usiluje o to, aby uchovávané osobní informace zůstaly přesné a aktuální v rozsahu nezbytném pro dosažení účelu použití.
- c) V čl. 6 odst. 1 zákona o ochraně osobních informací uchovávaných správními orgány se stanoví, že vedoucí správního orgánu přijme opatření nezbytná k tomu, aby se zabránilo úniku, ztrátě nebo poškození, jakož i k řádné správě uchovávaných osobních informací.
- d) Podle článku 7 zákona o ochraně osobních informací uchovávaných správními orgány nesmí žádný (ani bývalý) zaměstnanec zpřístupnit získané osobní informace jiné osobě bez oprávněného důvodu, nebo takové informace používat k neoprávněnému účelu.

⁽⁷⁾ Rozsudek ze dne 18. března 1969 (1968 (Shi) č.100).

⁽⁸⁾ V čl. 156 odst. 1 trestního řádu se stanoví: „Při podání žádosti uvedené v odstavci 1 předchozího článku musí žadatel poskytnout materiály, na základě kterých se má za to, že podezřelý nebo obviněný spáchal trestný čin.“

⁽⁹⁾ Viz poznámka pod čarou 6.

⁽¹⁰⁾ Ustanovení čl. 3 odst. 1 a 2 zákona o ochraně osobních informací uchovávaných správními orgány omezuje rozsah uchovávání, a tím tedy i shromažďování osobních informací.

- e) Kromě toho se v čl. 8 odst. 1 zákona o ochraně osobních informací uchovávaných správními orgány stanoví, že pokud není v právních předpisech stanoveno jinak, nesmí vedoucí správního orgánu uchovávané osobní informace používat ani je poskytovat jiné osobě pro jiné účely, než je stanovený účel použití. I když čl. 8 odst. 2 obsahuje výjimky z tohoto pravidla v konkrétních situacích, uplatňují se pouze v případě, pokud takové výjimečné zpřístupnění pravděpodobně nezpůsobí „nespravedlivé“ poškození práv a zájmů subjektu údajů nebo třetí strany.
- f) Podle článku 9 zákona o ochraně osobních informací uchovávaných správními orgány vedoucí správního orgánu, pokud jsou uchovávané osobní informace poskytnuty jiné osobě, stanoví v případě potřeby omezení účelu nebo způsobu použití nebo jakákoli jiná nezbytná omezení; může rovněž od přijímající osoby požadovat, aby přijala opatření nezbytná k zamezení úniku a k řádné správě informací.
- g) V článku 48 zákona o ochraně osobních informací uchovávaných správními orgány se stanoví, že vedoucí správního orgánu se vynasnaží náležitě a urychleně vyřídit všechny stížnosti týkající se nakládání s osobními informacemi.

2) Shromažďování osobních informací prostřednictvím žádostí o dobrovolnou spolupráci (Dobrovolné vyšetřování)

a) Právní základ

Vedle použití povinných prostředků jsou osobní informace získávány buď z volně dostupných zdrojů, nebo na základě dobrovolného poskytnutí, například ze strany podnikatelských subjektů uchovávajících takové informace.

Pokud jde o poslední uvedenou možnost, zmocňuje čl. 197 odst. 2 trestního řádu státního zástupce a soudní policii k „písemným žádostem ve věcech vyšetřování“ (tzv. „žádosti o zpřístupnění informací“). V souladu s trestním řádem jsou dotázané osoby povinny vyšetřovací orgánům poskytnout informace. Neexistuje však žádný způsob, jak je k tomu přinutit, pokud veřejné instituce nebo veřejné a/nebo soukromé organizace, které žádost obdržely, odmítají vyhovět. Pokud na žádost neodpoví, nelze jim uložit žádný trest nebo jinou sankci. Považují-li vyšetřovací orgány požadované informace za nezbytné, musí je získat prostřednictvím prohlídky a zajištění věci na základě soudního příkazu.

S ohledem na narůstající povědomí fyzických osob, pokud jde o jejich právo na soukromí, a rovněž s ohledem na pracovní zátěž, kterou takové žádosti vytvářejí, jsou podnikatelské subjekty při reakci na tyto žádosti stále obezřetnější⁽¹⁾. Při rozhodování, zda budou spolupracovat, berou podnikatelské subjekty v úvahu zejména povahu požadovaných informací, svůj vztah k osobě, již se dané informace týkají, riziko pro jejich pověst, riziko soudního sporu atd.

b) Omezení

Pokud jde o povinné shromažďování elektronických informací, je dobrovolné vyšetřování omezeno Ústavou, jak je vykládána v judikatuře, a opravňujícím statutem. Kromě toho nejsou podnikatelské subjekty oprávněny poskytovat informace v určitých situacích. Také zákon o ochraně osobních informací uchovávaných správními orgány stanoví řadu omezení týkajících se shromažďování informací i nakládání s nimi (zatímco místní vyhlášky přebírají v zásadě tatáž kritéria pro prefekturní policii).

1) Omezení vyplývající z Ústavy a opravňujícího statutu

S ohledem na účel článku 13 Ústavy stanovil Nejvyšší soud ve dvou rozhodnutích z 24. prosince 1969 (1965 (A) č. 1187) a 15. dubna 2008 (2007 (A) č. 839) omezení pro dobrovolná vyšetřování vedená vyšetřovacími orgány. Ačkoli se uvedená rozhodnutí týkala případů, kdy byly osobní informace (ve formě obrazového materiálu) shromažďovány prostřednictvím fotografování/filmování, jsou tato zjištění relevantní pro dobrovolná (nepovinná) vyšetřování zasahující do soukromí jednotlivců v obecném smyslu. Proto platí a musí být dodržována také v souvislosti se shromažďováním osobních informací v rámci dobrovolného vyšetřování, přičemž je třeba brát v potaz zvláštní okolnosti každého případu.

V souladu s uvedenými rozhodnutími se zákonnost dobrovolného vyšetřování odvíjí od splnění tří kritérií, jimiž jsou:

— „podezření na trestný čin“ (tj. posouzení, zda byl spáchán trestný čin),

— „nezbytnost vyšetřování“ (tj. posouzení, zda žádost nepřesahuje rámec toho, co je pro účely vyšetřování nezbytné), a

⁽¹⁾ Viz rovněž oznámení vydané Národní policejní agenturou dne 7. prosince 1999 (viz str. 9), v němž se uvádí totéž.

— „vhodnost metod“ (tj. posouzení, zda je dobrovolné vyšetřování „vhodné“ nebo přiměřené pro dosažení cíle vyšetřování) ⁽¹²⁾.

Zákonnost dobrovolného vyšetřování se s ohledem na výše uvedená tři kritéria zpravidla posuzuje z hlediska toho, zda je lze považovat za přiměřené v souladu se společenskými konvencemi.

Požadavek na „nezbytnost“ vyšetřování rovněž přímo vyplývá z článku 197 trestního řádu a byl potvrzen v pokynech Národní policejní agentury (NPA) určených prefekturní policii a týkajících se využívání „žádosti o zpřístupnění informací“. Oznámení NPA ze dne 7. prosince 1999 stanoví řadu procesních omezení, včetně požadavku, aby „žádosti o zpřístupnění informací“ byly využívány pouze tehdy, je-li to pro účely šetření nezbytné. Mimo to je čl. 197 odst. 1 trestního řádu omezen na trestní vyšetřování, a může se tudíž použít pouze tehdy, existuje-li konkrétní podezření na již spáchaný trestný čin. Naproti tomu není tento právní základ použitelný pro shromažďování a použití osobních informací v případech, kdy dosud nedošlo k porušení právních předpisů.

2) Omezení s ohledem na některé podnikatelské subjekty

Na základě ochrany poskytované jinými právními předpisy se v určitých oblastech uplatňují další omezení.

V první řadě jsou vyšetřovací orgány a operátoři telekomunikačních sítí uchováající osobní informace povinni respektovat důvěrnost sdělení, kterou zaručuje čl. 21 odst. 2 Ústavy ⁽¹³⁾. Tutéž povinnost navíc pro provozovatele telekomunikačních sítí stanoví článek 4 zákona o telekomunikacích ⁽¹⁴⁾. Podle „pokynů k ochraně osobních informací v odvětví telekomunikací“ vydaných Ministerstvem vnitra a telekomunikací na základě Ústavy a zákona o telekomunikacích nesmí v případech dotýkajících se důvěrnosti sdělení provozovatelé telekomunikačních sítí zpřístupnit osobní informace související s důvěrností sdělení třetím stran, kromě případů, kdy získali souhlas dotčené osoby, nebo pokud se mohou dovolávat některého z „ospravedlnitelných důvodů“ pro nedodržení trestního zákoníku. Tyto důvody může představovat „ospravedlnitelné jednání“ (článek 35 trestního zákoníku), „sebeobrana“ (článek 36 trestního zákoníku) a „odvrácení bezprostředního nebezpečí“ (článek 37 trestního zákoníku). „Ospravedlnitelným jednáním“ podle trestního zákoníku je pouze jednání provozovatele telekomunikačních sítí, které je v souladu s povinnými opatřeními státu, což vylučuje dobrovolné vyšetřování. Pokud tedy vyšetřující orgány požadují osobní informace na základě „žádosti o zpřístupnění informací“ (čl. 197 odst. 2 trestního řádu), nesmí provozovatel telekomunikačních sítí tyto údaje zpřístupnit.

Za druhé jsou podnikatelské subjekty povinny odmítnout žádosti o dobrovolnou spolupráci, pokud jim zpřístupňování osobních informací zakazuje zákon. Spadají sem i případy, kdy má subjekt povinnost zachovávat důvěrnost informací, např. podle článku 134 trestního zákoníku ⁽¹⁵⁾.

3) Omezení vyplývající ze zákona o ochraně osobních informací uchovávaných správními orgány

Pokud jde o shromažďování osobních informací a další nakládání s těmito informacemi ze strany správních orgánů, stanoví zákon o ochraně osobních informací uchovávaných správními orgány určitá omezení, jak je vysvětleno výše v oddíle II.A.1 písm. b) bodě 2. Rovnocenná omezení vyplývají z prefekturních nařízení, jež se vztahují na prefekturní policii.

B) Dozor

1) Soudní dozor

Shromažďování osobních informací povinnými prostředky musí být založeno na soudním příkazu ⁽¹⁶⁾, a podléhá tudíž předchozímu posouzení ze strany soudce. Pokud bylo vyšetřování protiprávní, může soudce takové důkazy vyloučit z následného trestního řízení týkajícího se daného případu. Fyzická osoba může požadovat takové vyloučení v rámci svého trestního řízení na základě tvrzení, že vyšetřování bylo protiprávní.

⁽¹²⁾ Pro posouzení „vhodnosti metod“ jsou důležitými faktory závažnost trestného činu a naléhavost.

⁽¹³⁾ V čl. 21 odst. 2 Ústavy se stanoví: „Je zakázána jakákoli cenzura a jakékoli porušení důvěrnosti všech komunikačních prostředků.“

⁽¹⁴⁾ Článek 4 zákona o telekomunikacích stanoví: „1. Nesmí být porušena důvěrnost sdělení, s nimiž nakládá provozovatel telekomunikačních sítí. 2. Jakákoli osoba, která působí v odvětví telekomunikací, nesmí zpřístupnit důvěrné informace, které při výkonu funkce získá v souvislosti se sděleními, s nimiž nakládá provozovatel telekomunikačních sítí. Platí to i poté, kdy tato osoba přestane svou funkci vykonávat.“

⁽¹⁵⁾ Článek 134 trestního zákoníku stanoví: „1. Pokud lékař, lékárník, distributor léčivých přípravků, porodní asistentka, právní zástupce, obhájce, notář nebo jakákoli osoba dříve vykonávající některé z těchto povolání neodůvodněně zpřístupní důvěrné informace jiné osoby, se kterými se při výkonu tohoto povolání obeznámila, bude odsouzena k trestu odnětí svobody s nařízeným výkonem práce až na dobu šesti měsíců nebo k pokutě nepřevyšující 100 000 jenů. 2. Totéž platí v případě, kdy osoba, která vykonává či vykonávala církevní povolání, neodůvodněně zpřístupní důvěrné informace jiné osoby, s nimiž se v rámci náboženské činnosti obeznámila.“

⁽¹⁶⁾ Výjimka z tohoto pravidla viz poznámka pod čarou č. 5.

2) Dozor podle zákona o ochraně osobních informací uchovávaných správními orgány

Na základě zákona o ochraně osobních informací uchovávaných správními orgány má v Japonsku každý ministr nebo vedoucí každé agentury pravomoc k doзору a jeho prosazování, přičemž ministr vnitra a komunikací může vyšetřovat prosazování tohoto zákona všemi ostatními ministerstvy.

Domnívá-li se ministr vnitra a komunikací (např. na základě vyšetřování týkajícího se stavu prosazování zákona o ochraně osobních informací uchovávaných správními orgány ⁽¹⁷⁾), zpracování stížností či žádostí určených některému z jeho všeobecných informačních středisek), že je to pro účely uvedeného zákona nezbytné, může požádat vedoucího správního orgánu o předložení podkladů a vysvětlení týkajících se nakládání s osobními informacemi ze strany daného správního orgánu na základě článku 50 zákona o ochraně osobních informací uchovávaných správními orgány. Pokládá-li to ministr pro účely daného zákona za nezbytné, může vedoucímu správního orgánu zaslat stanoviska ohledně zpracování osobních informací příslušným správním orgánem. Vedle toho může ministr například požádat o revizi opatření prostřednictvím kroků, jež mu umožňují články 50 a 51 zákona, existuje-li podezření na jeho porušení či nesprávné provádění. To napomáhá k jednotnému uplatňování a souladu se zákonem o ochraně osobních informací uchovávaných správními orgány.

3) Dozor komisí pro veřejnou bezpečnost nad policií

V rámci policejní správy podléhá Národní policejní agentura doзору Národní komise pro veřejnou bezpečnost, zatímco nad prefekturní policií zajišťuje v každé prefektuře dozor prefekturní komise pro veřejnou bezpečnost. Každý z těchto dozorových úřadů zajišťuje demokratické řízení a politickou neutralitu policejní správy.

Národní komise pro veřejnou bezpečnost je zodpovědná za záležitosti spadající do její jurisdikce podle zákona o policii či jiných zákonů. Patří sem jmenování generálního komisaře Národní policejní agentury a vedoucích policejních úředníků na místní úrovni nebo též tvorba komplexních politik, které stanoví základní směrnice nebo opatření týkající se správy Národní policejní agentury.

Prefekturní komise pro veřejnou bezpečnost jsou složeny ze zástupců občanů v příslušné prefektuře v souladu se zákonem o policii a řídí prefekturní policii jako systém nezávislé rady. Členové jsou jmenováni guvernérem prefektury se souhlasem prefekturního shromáždění v souladu s článkem 39 zákona o policii. Jejich funkční období činí tři roky; odvolání proti své vůli mohou být pouze ze zvláštních důvodů uvedených v zákoně (např. nezpůsobilost k výkonu povinností, porušení povinností, profesní pochybení apod.), čímž je zaručena jejich nezávislost (viz články 40 a 41 zákona o policii). S cílem zaručit jejich politickou neutralitu dále článek 42 zákona o policii zakazuje členům komise, aby byli souběžně členy legislativního orgánu, stali se výkonnými členy politické strany nebo jiného politického subjektu nebo se aktivně účastnili politického hnutí. Ačkoli každá komise spadá do jurisdikce příslušného guvernéra prefektury, nemá guvernér žádnou pravomoc k vydávání pokynů týkajících se výkonu jejich funkcí.

Podle čl. 38 odst. 3 ve spojení s článkem 2 a čl. 36 odst. 2 zákona o policii jsou prefekturní komise pro veřejnou bezpečnost zodpovědné za „ochranu práv a svobody jednotlivce“. Za tímto účelem přijímají od velitelů prefekturní policie zprávy o činnostech v rámci jejich jurisdikce, a to rovněž na pravidelných setkáních konaných třikrát nebo čtyřikrát za měsíc. Komise poskytují v daných záležitostech pokyny prostřednictvím vypracování komplexních politik.

V rámci své dozorové funkce mohou navíc prefekturní komise pro veřejnou bezpečnost vydávat v konkrétních individuálních případech pokyny pro prefekturní policii, pokud to v souvislosti s inspekci činnosti prefekturní policie nebo zneužitím pravomoci jejich příslušníků považují za nezbytné. Komise také mohou v případě potřeby pověřit některého ze svých členů přezkumem stavu provádění vydaných pokynů (viz čl. 43 odst. 2 zákona o policii).

⁽¹⁷⁾ V zájmu transparentnosti a snadnějšího doзору ze strany ministerstva vnitra a telekomunikací je vedoucí správního orgánu v souladu s článkem 11 zákona o ochraně osobních informací uchovávaných správními orgány povinen zaznamenávat všechny údaje stanovené v čl. 10 odst. 1 uvedeného zákona, jako je např. název správního orgánu uchovávajícího určitý soubor, účel použití souboru, metoda shromažďování osobních informací atd. (tzv. „registr souborů osobních informací“). Souborů osobních informací, na které se vztahuje čl. 10 odst. 2 uvedeného zákona, např. které byly sestaveny nebo získány v rámci trestního vyšetřování nebo které se týkají záležitostí souvisejících s národní bezpečností, se však povinnost oznamovat je ministerstvu vnitra a telekomunikací a zařadit je do veřejného registru netýká. Podle článku 7 zákona o správě veřejných rejstříků a archivů je nicméně vedoucí správního orgánu vždy povinen zaznamenávat údaje o klasifikaci, názvu, době uchovávání, místě uložení atd. v případě správních dokumentů („registr souborů správních dokumentů“). Indexované informace z obou registrů jsou zveřejněny na internetu, takže fyzické osoby si mohou ověřit, jaký druh osobních informací soubor obsahuje a který správní orgán tyto informace uchovává.

4) Dozor parlamentu

Parlament může vést vyšetřování týkající se činnosti orgánů veřejné moci, a za tímto účelem může požadovat předložení dokumentů a výpověď svědků (článek 62 Ústavy). V tomto ohledu může příslušný výbor parlamentu posuzovat vhodnost shromažďování informací ze strany policie.

Tyto pravomoci jsou dále upřesněny v zákoně o parlamentu. Podle článku 104 uvedeného zákona může parlament požádat kabinet a veřejnoprávní subjekty o předložení zpráv a záznamů nezbytných pro jeho vyšetřování. Členové parlamentu mohou rovněž v souladu s článkem 74 zákona o parlamentu předkládat „písemné dotazy“. Takové dotazy musí schválit předseda komory a kabinet na ně musí zpravidla písemně odpovědět do sedmi dnů (není-li možné odpovědět v uvedené lhůtě, musí to být odůvodněno a být stanovena nová lhůta, viz článek 75 zákona o parlamentu). V minulosti se písemné dotazy parlamentu týkaly rovněž nakládání s osobními informacemi státní správou⁽¹⁸⁾.

C) Individuální ochrana

Podle článku 32 Ústavy Japonska nesmí být nikomu odepřeno právo na přístup k soudům. Kromě toho článek 17 Ústavy zaručuje každé osobě právo žalovat stát nebo veřejný subjekt o náhradu škody (jak stanoví zákon) v případě, kdy dané osobě vznikne škoda protiprávním jednáním úřední osoby.

1) Soudní ochrana před povinným shromažďováním informací na základě soudního příkazu (článek 430 trestního řádu)

Podle čl. 430 odst. 2 trestního řádu může fyzická osoba, která má námitky vůči krokům policejního úředníka v souvislosti se zajištěním věcí (rovněž pokud obsahují osobní informace) na základě soudního příkazu, předložit u příslušného soudu žádost (tzv. „kvazi-stížnost“), aby tato opatření byla „zrušena nebo změněna“.

Toto napadení lze provést, aniž by fyzická osoba musela čekat na uzavření případu. Shledá-li soud, že zajištění nebylo zapotřebí, nebo že existují jiné důvody považovat toto zajištění za protiprávní, může nařídít, aby byla daná opatření zrušena nebo změněna.

2) Soudní ochrana podle občanského soudního řádu a zákona o státní ochraně

Pokud se fyzické osoby domnívají, že bylo porušeno jejich právo na soukromí podle článku 13 Ústavy, mohou podat občanskoprávní žalobu požadující, aby osobní informace shromážděné během trestního vyšetřování byly vymazány.

Fyzická osoba může rovněž podat žalobu o náhradu škody na základě zákona o státní ochraně ve spojení s příslušnými články občanského zákoníku, pokud se domnívá, že v důsledku shromažďování jejích osobních informací nebo sledování bylo porušeno její právo na soukromí a utrpěla újmu⁽¹⁹⁾. Jelikož se „škoda“, jež je předmětem žádosti o náhradu, neomezuje pouze na škodu na majetku (článek 710 občanského zákoníku), může zahrnovat rovněž „psychickou újmu“. Výši náhrady za takovou morální újmu posoudí soudce na základě „volného hodnocení při uvážení jednotlivých faktorů každého případu“⁽²⁰⁾.

Ustanovení čl. 1 odst. 1 zákona o státní ochraně přiznává právo na náhradu, pokud i) státní úředník, který vykonává veřejnou moc státu nebo veřejného subjektu, ii) při plnění svých povinností iii) úmyslně nebo z nedbalosti iv) protiprávně v) způsobil jiné osobě škodu.

Dotčená osoba musí podat žalobu v souladu s občanským soudním řádem. Podle platných pravidel tak může učinit u soudu, do jehož jurisdikce spadá místo, kde k deliktu došlo.

⁽¹⁸⁾ Viz např. písemný dotaz Sněmovny radních č. 92 ze dne 27. března 2009 týkající se nakládání s informacemi shromážděnými v rámci trestního vyšetřování, včetně případů porušení povinnosti mlčenlivosti ze strany policie a orgánů pověřených stíháním.

⁽¹⁹⁾ Příkladem takové žaloby je „případ seznamu obranné agentury“ (rozsudek okresního soudu v Niigatě ze dne 11. května 2006, 2002 (Wa) č. 514) V tomto případě jeden z úředníků obranné agentury vyhotovil, uchovával a šířil seznam fyzických osob, které u obrané agentury podaly žádost o zpřístupnění správních dokumentů. Tento seznam obsahoval osobní informace žalobce. Žalobce tvrdil, že bylo porušeno jeho soukromí a právo na to, aby byl informován, a žádal od žalovaného náhradu škody podle čl. 1 odst. 1 zákona o státní ochraně. Soud žádosti částečně vyhověl a přiznal žalobci částečnou náhradu.

⁽²⁰⁾ Rozhodnutí Nejvyššího soudu ze dne 5. dubna 1910 (1910 (O) č. 71).

- 3) Ochrana fyzických osob před protiprávním/nepatřičným policejním šetřením: stížnost k prefekturní komisi pro veřejnou bezpečnost (článek 79 zákona o policii)

Podle článku 79 zákona o policii⁽²¹⁾, který je blíže objasněn v pokynech ředitele Národní policejní agentury určených prefekturní policii a prefekturním komisím pro veřejnou bezpečnost⁽²²⁾, mohou fyzické osoby předložit příslušné prefekturní komisi pro veřejnou bezpečnost písemnou stížnost⁽²³⁾ týkající se protiprávního nebo nepatřičného jednání policejního úředníka při výkonu jeho povinností, včetně povinností týkajících se shromažďování a používání osobních informací. Komise tyto stížnosti vyřizují svědomitě v souladu s právními předpisy a místními vyhláškami a stěžovatele o výsledku šetření informují písemně.

Na základě své dozorovací pravomoci podle čl. 38 odst. 3 zákona o policii vydá prefekturní komise pro veřejnou bezpečnost prefekturní policii pokyn, aby prošetřila skutečnosti, podle výsledku přezkoumání zavedla potřebná opatření a o výsledcích podala komisi zprávu. Tam, kde to považuje za nutné, může komise rovněž vydat pokyn k vyřízení stížnosti, například domnívá-li se, že šetření ze strany policie nebylo dostatečné. Tento postup je popsán ve sdělení Národní policejní agentury určeném velitelům prefekturní policie.

Při informování stěžovatele o výsledcích šetření jsou rovněž zohledněny policejní zprávy týkající se daného šetření a opatření přijatá na žádost komise.

- 4) Individuální ochrana podle zákona o ochraně osobních informací uchovávaných správními orgány a trestního řádu

a) Zákon o ochraně osobních informací uchovávaných správními orgány

Podle článku 48 zákona o ochraně osobních informací uchovávaných správními orgány musí správní orgány usilovat o řádné a rychlé vyřízení jakékoli stížnosti týkající se nakládání s osobními informacemi. Za účelem poskytování konsolidovaných informací fyzickým osobám (např. o dostupných právech na zpřístupnění, opravu a přerušení používání informací podle zákona o ochraně osobních informací uchovávaných správními orgány) a jako kontaktní místo, na které je možné se obracet s dotazy, zřídilo Ministerstvo vnitra a komunikací v každé prefektuře na základě čl. 47 odst. 2 zákona o ochraně osobních informací uchovávaných správními orgány všeobecná informační střediska pro zpřístupnění informací / ochranu osobních informací. Dotazy mohou pokládat i nerezidenti. Kupříkladu v rozpočtovém roce 2017 (duben 2017 až březen 2018) všeobecná informační střediska odpověděla na dotazy apod. u celkového počtu 5186 případů.

Články 12 a 27 zákona o ochraně osobních informací uchovávaných správními orgány udělují fyzickým osobám právo žádat o zpřístupnění a opravu uchovávaných osobních informací. Dále mohou fyzické osoby podle článku 36 zákona o ochraně osobních informací uchovávaných správními orgány požádat o přerušení používání nebo o výmaz jejich uchovávaných osobních informací v případě, že správní orgán nezískal uchovávané osobní informace zákonně nebo tyto informace uchovává či používá v rozporu s právními předpisy.

Pokud však jde o osobní informace shromažďované (buď na základě příkazu, nebo prostřednictvím „žádosti o zpřístupnění informací“) a uchovávané pro potřeby trestního vyšetřování⁽²⁴⁾, takové informace obecně spadají do kategorie „osobních informací zaznamenaných v dokumentech týkajících se soudních řízení a zajištěných předmětů“. Takové osobní informace jsou proto vyloučeny z oblasti působnosti individuálních práv v kapitole 4 zákona o ochraně osobních informací uchovávaných správními orgány podle článku 53-2 trestního řádu⁽²⁵⁾. Zpracovávání těchto osobních informací a práva fyzických osob na přístup a opravu místo toho podléhají zvláštním pravidlům podle trestního řádu a zákona

⁽²¹⁾ Výňatek z článku 79 zákona o policii:

1. Osoby mající námitky vůči výkonu povinností příslušníků prefekturní policie mohou prefekturní komisi pro veřejnou bezpečnost předložit písemnou stížnost postupem stanoveným ve vyhlášce o Národní komisi pro veřejnou bezpečnost.
2. Prefekturní komise pro veřejnou bezpečnost, která obdržela stížnost uvedenou v předchozím odstavci, ji vyřídí svědomitě v souladu s právními předpisy a místními vyhláškami a písemně informuje stěžovatele o výsledku šetření, s výjimkou následujících případů:
 - 1) stížnost byla podána za účelem zabránění v zákonném výkonu povinností prefekturní policie;
 - 2) není známo současné místo bydliště stěžovatele;
 - 3) stěžovatel je ve spojení s jinými stěžovateli, kteří již byli o výsledku společné stížnosti informováni.

⁽²²⁾ Národní policejní agentura, Sdělení o řádném vyřizování stížností týkajících se výkonu povinností policejních úředníků ze dne 13. dubna 2001, příloha 1 „Standardy pro výklad/provádění článku 79 zákona o policii“.

⁽²³⁾ V souladu se sdělením Národní policejní agentury (viz předchozí poznámka pod čarou) mají osoby, pro něž je sepsání stížnosti obtížné, nárok na pomoc. To výslovně zahrnuje případ cizinců.

⁽²⁴⁾ Na druhé straně se vyskytují dokumenty, které nejsou klasifikovány jako „dokumenty týkající se soudních řízení“, jelikož samy o sobě nejsou informacemi získanými prostřednictvím příkazu nebo písemných žádostí ve věcech vyšetřování, ale byly na základě takových dokumentů vytvořeny. V takovém případě by soukromé informace nepodléhaly čl. 45 odst. 1 zákona o ochraně osobních informací uchovávaných správními orgány, a tudíž by nebyly z působnosti kapitoly 4 zákona o ochraně osobních informací uchovávaných správními orgány vyloučeny.

⁽²⁵⁾ V čl. 53-2 odst. 2 trestního řádu je stanoveno, že ustanovení kapitoly IV zákona o ochraně osobních informací uchovávaných správními orgány se nepoužijí na osobní informace zaznamenané v dokumentech týkajících se soudních řízení a zajištěných předmětů.

o konečném trestním spise (viz níže) ⁽²⁶⁾. Toto vyloučení je odůvodněno různými faktory, jako je ochrana soukromí dotčených osob, utajení vyšetřování a řádný průběh trestního řízení. Nadále jsou přitom použitelná ustanovení kapitoly 2 zákona o ochraně osobních informací uchovávaných správními orgány, která upravují zásady nakládání s těmito informacemi.

b) Trestní řád

Podle trestního řádu závisí možnosti přístupu k osobním informacím shromažďovaným pro účely trestního vyšetřování jak na fázi řízení, tak i na roli fyzické osoby v daném vyšetřování (podezřelý, obviněný, oběť atd.).

Z pravidla uvedeného v článku 47 trestního řádu, podle něhož se dokumenty týkající se soudního řízení nesmí před začátkem řízení zveřejňovat (neboť by to mohlo poškodit čest a/nebo soukromí dotčených osob a bránit vyšetřování / soudnímu řízení) existuje výjimka, která v zásadě povoluje, aby do těchto informací mohla nahlížet oběť trestného činu, a to v rozsahu, jaký se považuje za přiměřený s ohledem na účel ustanovení článku 47 trestního řádu ⁽²⁷⁾.

Pokud jde o podezřelého, ti se o tom, že se jich týká trestní vyšetřování, zpravidla dozví při výsledku prováděném soudní policií nebo státním zástupcem. V případě, že se státní zástupce následně rozhodne trestní stíhání nezačít, ihned o této skutečnosti podezřelého na jeho žádost informuje (článek 259 trestního řádu).

Po zahájení trestního stíhání navíc státní zástupce poskytne obviněnému nebo jeho právnímu zástupci příležitost nahlédnout do důkazů před tím, než požádá o jejich posouzení soudem (článek 299 trestního řádu). To obviněnému umožňuje, aby zkontroloval své osobní informace shromážděné v průběhu trestního vyšetřování.

Ochrana osobních informací shromážděných v souvislosti s trestním vyšetřováním, ať již jde o podezřelého, obviněného nebo jakoukoli jinou osobu (např. oběť trestného činu), je zaručena povinností mlčenlivosti (článek 100 zákona o národních veřejných službách) a prostřednictvím trestu hrozícího v případě úniku důvěrných informací v průběhu plnění úkolů veřejné služby (čl. 109 bod xii) zákona o národních veřejných službách).

5) Individuální ochrana proti protiprávnímu/nepatřičnému vyšetřování ze strany orgánů veřejné moci: stížnost ke Komisi pro ochranu osobních informací

Podle článku 6 zákona o ochraně osobních informací přijme vláda ve spolupráci s vládami třetích zemí nezbytná opatření za účelem vybudování mezinárodně uzpůsobeného systému týkajícího se osobních informací prostřednictvím podpory spolupráce s mezinárodními organizacemi a dalšími mezinárodními rámci. Na základě tohoto ustanovení přenáší základní politika týkající se ochrany osobních informací (přijata rozhodnutím kabinetu) na Komisi pro ochranu osobních informací, jakožto orgán příslušný pro celkovou správu zákona o ochraně osobních informací, pravomoc přijímat nezbytná opatření k překlenutí rozdílu mezi systémy a operacemi Japonska a dotyčné cizí země s cílem zajistit vhodné nakládání s osobními informacemi přijatými z takové země.

Dále, jak je stanoveno v čl. 61 bodech i) a ii) zákona o ochraně osobních informací, je Komisi pro ochranu osobních informací svěřen úkol vypracovat a prosazovat základní politiku a také jí byla svěřena mediace stížností podaných proti podnikatelským subjektům. Správní orgány spolu rovněž úzce komunikují a vzájemně spolupracují (článek 80 zákona o ochraně osobních informací).

Na základě těchto ustanovení se bude Komise pro ochranu osobních informací zabývat stížnostmi podanými fyzickými osobami tímto způsobem:

- a) Fyzická osoba, která má podezření, že její údaje předané z EU byly shromážděny nebo použity orgány veřejné moci v Japonsku, včetně orgánů odpovědných za činnosti uvedené v kapitolách II a III tohoto prohlášení, v rozporu s použitelnými pravidly, včetně těch, na něž se vztahuje toto prohlášení, může podat stížnost ke Komisi pro ochranu osobních informací (individuálně nebo prostřednictvím svého úřadu pro ochranu osobních údajů).
- b) Komise pro ochranu osobních údajů danou stížnost vyřizuje, mimo jiné s využitím svých pravomocí podle článku 6, čl. 61 bodu ii) a článku 80 zákona o ochraně osobních informací, a o stížnosti informuje příslušné orgány veřejné moci, včetně příslušných dozorových úřadů.

⁽²⁶⁾ Podle trestního řádu a zákona o konečném trestním spise podléhají přístup k zajištěným předmětům a jejich oprava, jakož i dokumenty / osobní informace týkající se trestních řízení, jedinečnému a specifickému systému pravidel, jehož cílem je ochrana soukromí dotčených osob, utajení vyšetřování, řádný průběh trestního řízení atd.

⁽²⁷⁾ Konkrétněji – obětem trestného činu je v zásadě povoleno nahlížet do informací týkajících se objektivních důkazů, pokud jde o záznamy, které se netýkají stíhání, u případů s výhradou účasti oběti podle článku 316-33 a dalších trestního řádu, a to za účelem zajištění adekvátnější ochrany obětí trestného činu.

Podle článku 80 zákona o ochraně osobních informací musí tyto orgány s Komisí pro ochranu osobních informací spolupracovat, mimo jiné tím, že poskytnou nezbytné informace a příslušné materiály, tak aby Komise pro ochranu osobních informací mohla posoudit, zda shromažďování nebo následné použití osobních informací proběhlo v souladu s použitelnými pravidly. Při provádění tohoto posouzení bude Komise pro ochranu osobních informací spolupracovat s Ministerstvem vnitra a komunikací.

- c) Pokud posouzení ukáže, že došlo k porušení použitelných pravidel, zahrnuje spolupráce dotčených orgánů veřejné moci s Komisí pro ochranu osobních informací povinnost toto porušení napravit.

V případě protiprávního shromažďování osobních informací to podle použitelných pravidel zahrnuje výmaz osobních informací, které byly shromažďovány.

V případě, že došlo k porušení použitelných pravidel, Komise pro ochranu osobních informací před uzavřením posouzení rovněž potvrdí, že porušení bylo v plném rozsahu napraveno.

- d) Jakmile je posouzení uzavřeno, Komise pro ochranu osobních informací o jeho výsledku v přiměřené lhůtě uvědomí danou fyzickou osobu s uvedením případně přijatých nápravných opatření. Prostřednictvím tohoto oznámení Komise pro ochranu osobních informací rovněž informuje danou fyzickou osobu o možnosti vyžádat si od příslušného orgánu veřejné moci potvrzení výsledku a o tom, ke kterému úřadu takovou žádost o potvrzení podat.

Podrobné informace o výsledku posouzení lze omezit, pokud existují přiměřené důvody se domnívat, že sdělení takových informací pravděpodobně ohrozí probíhající vyšetřování.

Pokud se stížnost týká shromažďování nebo používání osobních údajů v oblasti prosazování trestního práva a posouzení odhalí, že bylo zahájeno řízení ve věci zahrnující osobní informace dané fyzické osoby a že toto řízení je ukončeno, Komise pro ochranu osobních informací bude fyzickou osobu informovat o tom, že lze nahlédnout do spisu podle článku 53 trestního řádu a článku 4 zákona o konečném trestním spise.

Pokud posouzení odhalí, že fyzická osoba je podezřelá v trestní věci, informuje Komise pro ochranu osobních informací danou fyzickou osobu o této skutečnosti a o možnosti podat žádost podle článku 259 trestního řádu.

- e) V případě, že fyzická osoba stále není spokojena s výsledkem řízení, může se obrátit na Komisi pro ochranu osobních informací, která danou fyzickou osobu informuje o různých možnostech a detailních postupech pro dosažení právní ochrany podle japonských právních předpisů. Komise pro ochranu osobních informací poskytne dané fyzické osobě podporu, včetně poradenství a pomoci ohledně jakýchkoli dalších kroků ve vztahu k příslušnému správnímu nebo soudnímu orgánu.

III. Přístup vlády pro účely národní bezpečnosti

A. Právní základ a omezení pro shromažďování osobních informací

1) Právní základ pro shromažďování informací příslušnými ministerstvy/agenturami

Jak je uvedeno výše, musí být shromažďování osobních informací správními orgány pro účely národní bezpečnosti v rozsahu jejich správní pravomoci.

V Japonsku neexistuje žádný právní předpis, který by umožňoval shromažďování informací povinnými prostředky pouze pro účely národní bezpečnosti. Podle článku 35 Ústavy je možné shromažďovat osobní informace nuceně pouze na základě příkazu vydaného soudem za účelem vyšetřování trestného činu. Takový příkaz lze tudíž vydat pouze pro účely trestního vyšetřování. To znamená, že v japonském právním systému není povoleno shromažďování informací nebo přístup k nim povinnými prostředky z důvodů národní bezpečnosti. V oblasti národní bezpečnosti místo toho mohou dotčená ministerstva nebo agentury získat informace pouze z volně přístupných zdrojů nebo je mohou získat od podnikatelských subjektů či fyzických osob, které je dobrovolně zpřístupní. Podnikatelské subjekty, které obdrží žádost o dobrovolnou spolupráci, nejsou ze zákona povinny tyto informace poskytnout, a pokud spolupráci odmítnou, neplynou z toho pro ně žádné negativní důsledky.

Odpovědnost v oblasti národní bezpečnosti má řada různých odborů ministerstev a agentur.

1) Sekretariát kabinetu

Sekretariát kabinetu provádí shromažďování a výzkum informací v souvislosti s důležitými politikami kabinetu⁽²⁸⁾ podle článku 12-2 zákona o kabinetu⁽²⁹⁾. Sekretariát kabinetu však nemá pravomoc shromažďovat osobní informace přímo od podnikatelských subjektů. Shromažďuje, zpracovává, analyzuje a posuzuje informace z veřejně dostupných materiálů, od dalších orgánů veřejné moci atd.

2) Národní policejní agentura / prefekturní policie

V každé prefektuře je prefekturní policie oprávněna shromažďovat informace v rozsahu své pravomoci podle článku 2 zákona o policii. Může se stát, že v rozsahu své pravomoci podle zákona o policii bude informace shromažďovat přímo Národní policejní agentura. To se týká zejména činností Bezpečnostního úřadu Národní policejní agentury a Odboru zahraničních věcí a zpravodajství. Podle článku 24 zákona o policii je Bezpečnostní úřad odpovědný za záležitosti týkající se bezpečnostní policie⁽³⁰⁾ a Odbor zahraničních věcí a zpravodajství odpovídá za záležitosti týkající se cizích státních příslušníků, jakož i japonských státních příslušníků, jejichž sídlo činnosti se nachází v zahraničí.

3) Zpravodajská služba pro veřejnou bezpečnost

Uplatňování zákona o předcházení podvratným činnostem a zákona o kontrole organizací, které se dopouštějí bezohledného masového vraždění, spadá zejména do kompetence Zpravodajské služby pro veřejnou bezpečnost. Tato zpravodajská služba je agenturou Ministerstva spravedlnosti.

Zákon o předcházení podvratným činnostem a zákon o kontrole organizací, které se dopouštějí bezohledného masového vraždění, stanoví, že správní rozhodnutí (tj. opatření, jimiž se nařizuje omezení činnosti těchto organizací, jejich rozpuštění atd.) lze za přísných podmínek přijmout vůči organizacím, které se dopouštějí některých závažných činů („teroristická podvratná činnost“ nebo „případ bezohledného masového vraždění“) v rozporu s „veřejnou bezpečností“ nebo „základním systémem společnosti“ podle Ústavy. „Teroristické podvratné činnosti“ spadají do oblasti působnosti zákona o předcházení podvratným činnostem (viz článek 4 zahrnující takové činnosti, jako je například vzpoura, podněcování k zahraniční agresi, zabití s politickým záměrem atd.), zatímco zákon o kontrole organizací, které se dopouštějí bezohledného masového vraždění, se zabývá „případy bezohledného masového vraždění“ (viz článek 4 tohoto zákona). Rozhodnutí podle zákona o předcházení podvratným činnostem nebo zákona o kontrole organizací, které se dopouštějí bezohledného masového vraždění, mohou být přijata pouze proti přesně určeným organizacím, které představují konkrétní vnitřní nebo vnější hrozbu pro veřejnou bezpečnost.

Zákon o předcházení podvratným činnostem a zákon o kontrole organizací, které se dopouštějí bezohledného masového vraždění, za tímto účelem poskytují zákonnou pravomoc provádět vyšetřování. Základní vyšetřovací pravomoci důstojníků Zpravodajské služby pro veřejnou bezpečnost jsou stanoveny v článku 27 zákona o předcházení podvratným činnostem a v článku 29 zákona o kontrole organizací, které se dopouštějí bezohledného masového vraždění. Vyšetřování vedená podle těchto ustanovení Zpravodajskou službou pro veřejnou bezpečnost jsou prováděna v rozsahu, v jakém jsou nezbytná, pokud jde o rozhodnutí týkající se kontroly výše uvedených organizací (v minulosti byly vyšetřovány např. radikální levicové skupiny, sekta Óm Šinrikjó / Aum Šinrikjó a některé domácí skupiny úzce spojené se Severní Koreou). Tato vyšetřování se však nemohou opírat o povinné prostředky, a organizace uchovávající osobní informace tak nemůže být nucena takové informace poskytnout.

Shromažďování a používání informací, které byly Zpravodajské službě pro veřejnou bezpečnost zpřístupněny dobrovolně, podléhá příslušným zárukám a omezením stanoveným právními předpisy, jako je mimo jiné důvěrnost sdělení zaručená Ústavou a pravidla pro nakládání s osobními informacemi podle zákona o ochraně osobních informací uchovávaných správními orgány.

4) Ministerstvo obrany

Pokud jde o sběr informací prováděný Ministerstvem obrany, toto ministerstvo shromažďuje informace na základě článků 3 a 4 zákona o zřízení Ministerstva obrany, a to v rozsahu nezbytném pro provádění záležitostí spadajících do jeho správní pravomoci, mimo jiné s ohledem na obranu a stráž, akce uskutečňované obrannými silami, jakož i rozmisťování pozemních, námořních a vzdušných obranných sil. Ministerstvo obrany může shromažďovat informace pro tyto účely pouze prostřednictvím dobrovolné spolupráce a z volně přístupných zdrojů. Neshromažďuje informace o široké veřejnosti.

2) Omezení a záruky

a) Zákonem stanovená omezení

1) Obecná omezení vyplývající ze zákona o ochraně osobních informací uchovávaných správními orgány

Zákon o ochraně osobních informací uchovávaných správními orgány je všeobecným právním předpisem, který se vztahuje na shromažďování a uchovávání osobních informací správními orgány v jakékoli oblasti činnosti těchto orgánů. Omezení a záruky popsané v oddíle II.A.1 písm. b) bodě 2 se proto vztahují také na uchovávání, uložení, použití atd. osobních informací v oblasti národní bezpečnosti.

⁽²⁸⁾ Provádí je Zpravodajská a vyšetřovací služba kabinetu na základě článku 4 nařízení o organizaci sekretariátu kabinetu (Cabinet Secretariat Organization Order).

⁽²⁹⁾ To zahrnuje „shromažďování a výzkum informací v souvislosti s důležitými politikami kabinetu“.

⁽³⁰⁾ Bezpečnostní policie je odpovědná za činnosti v oblasti boje proti trestné činnosti, které se týkají veřejné bezpečnosti a zájmu národa. To zahrnuje boj proti trestné činnosti a shromažďování informací o protiprávním jednání týkajícím se extrémních levicových skupin, pravicových skupin a škodlivých aktivit namířených proti Japonsku.

2) Zvláštní omezení použitelná na policii (Národní policejní agenturu i prefekturní policii)

Jak je uvedeno výše v oddíle týkajícím se shromažďování informací pro účely prosazování práva, policie může shromažďovat informace pouze v rámci své pravomoci a při této činnosti může podle čl. 2 odst. 2 zákona o policii jednat pouze v rozsahu „přísně omezeném“ na plnění svých povinností a způsobem, který je „nezaujatý, nestranný, nepředpojatý a spravedlivý“. Kromě toho „nikdy nezneužívá svých pravomocí způsobem, který by zasahoval do práv a svobod fyzických osob zaručených Ústavou Japonska“.

3) Zvláštní omezení použitelná na Zpravodajskou službu pro veřejnou bezpečnost

Jak článek 3 zákona o předcházení podvratným činnostem, tak i článek 3 zákona o kontrole organizací, které se dopouštějí bezohledného masového vraždění, stanoví, že vyšetřování vedená podle těchto zákonů se provádějí pouze v minimálním rozsahu nezbytném pro dosažení sledovaného účelu a nesmějí být prováděna tak, aby nepřiměřeně omezovala základní lidská práva. Navíc článek 45 zákona o předcházení podvratným činnostem a článek 42 zákona o kontrole organizací, které se dopouštějí bezohledného masového vraždění, stanoví, že pokud důstojník Zpravodajské služby pro veřejnou bezpečnost zneužije své pravomoci, dopustí se tak trestného činu, který lze postihnout těžšími trestními sankcemi, než „obecná“ zneužití pravomoci v jiných oblastech veřejného sektoru.

4) Zvláštní omezení použitelná na Ministerstvo obrany

Pokud jde o shromažďování/organizaci informací Ministerstvem obrany, jak je uvedeno v článku 4 zákona o zřízení Ministerstva obrany, omezuje se tato činnost ministerstva za účelem shromažďování informací na to, co je „nezbytné“ k plnění jeho povinností týkajících se 1) obrany a stráže, 2) akcí uskutečňovaných obrannými silami, 3) organizace, počtu pracovníků, struktury, vybavení a rozmisťování pozemních, námořních a vzdušných obranných sil.

b) Jiná omezení

Jak je vysvětleno výše v oddíle II.A.2 písm. b) bodě 1 v souvislosti s trestním vyšetřováním, z judikatury Nejvyššího soudu vyplývá, že na to, aby orgány mohly hospodářskému subjektu zaslat žádost o dobrovolnou spolupráci, musí být tato žádost nezbytná pro vyšetřování podezření z trestné činnosti a musí být přiměřená, pokud jde o dosažení účelu vyšetřování.

Ačkoli se vyšetřování prováděná vyšetřovacími orgány v oblasti národní bezpečnosti liší od vyšetřování prováděných vyšetřovacími orgány v oblasti prosazování práva, pokud jde o právní základ i účel, ústřední zásady „nutnosti vyšetřování“ a „vhodnosti metody“ se v oblasti národní bezpečnosti použijí obdobně a musí být dodrženy s náležitým přihlédnutím ke konkrétním okolnostem každého případu.

Kombinace výše uvedených omezení zajišťuje, že shromažďování a zpracovávání informací probíhá pouze v míře nezbytné pro plnění konkrétních povinností příslušného orgánu veřejné moci, jakož i na základě konkrétních hrozeb. Je tak vyloučen masový a neselektivní sběr osobních informací nebo přístup k těmto osobním informacím z důvodu národní bezpečnosti.

B. Dozor

1) Dozor podle zákona o ochraně osobních informací uchovávaných správními orgány

Jak je vysvětleno výše v oddíle II.B.2, v japonském veřejném sektoru je pravomoc dohlížet v rámci každého ministerstva nebo agentury na dodržování zákona o ochraně osobních informací uchovávaných správními orgány a toto dodržování vymáhat svěřena ministroví nebo vedoucímu daného ministerstva nebo agentury. Ministr vnitra a komunikací navíc může prošetřovat stav vymáhání tohoto zákona, požadovat po jednotlivých ministrech předložení materiálů a vysvětlení na základě článků 49 a 50 zákona a zasílat jednotlivým ministrům stanoviska na základě článku 51 zákona. Může například požádat o přezkum opatření prostřednictvím kroků podle článků 50 a 51 zákona.

2) Dozor nad policií vykonávaný komisemi pro veřejnou bezpečnost

Jak je vysvětleno výše v oddíle „II. Shromažďování informací pro účely prosazování trestního práva“, dozor nad činnostmi prefekturní policie provádí nezávislé prefekturní komise pro veřejnou bezpečnost.

Pokud jde o Národní policejní agenturu, funkce dozoru vykonává Národní komise pro veřejnou bezpečnost. Podle článku 5 zákona o policii je tato komise odpovědná především za „ochranu práv a svobody jednotlivce“. Za tímto účelem vytvoří komplexní politiky, které stanoví předpisy pro správu záležitostí předepsaných v jednotlivých položkách čl. 5 odst. 4 zákona o policii a další základní pokyny či opatření, podle nichž by se mělo při výkonu uvedených činností postupovat. Národní komise pro veřejnou bezpečnost požívá stejné míry nezávislosti jako prefekturní komise pro veřejnou bezpečnost.

3) Dozor nad Ministerstvem obrany vykonávaný kanceláří generálního inspektora pro dodržování právních předpisů
Kancelář generálního inspektora pro dodržování právních předpisů je nezávislý úřad Ministerstva obrany, který podle článku 29 zákona o zřízení Ministerstva obrany podléhá přímému dohledu ministra obrany. Kancelář generálního inspektora pro dodržování právních předpisů může provádět inspekce zaměřené na to, zda úředníci Ministerstva vnitra dodržují právní předpisy. Tyto inspekce se nazývají „inspekce obrany“.

Kancelář generálního inspektora pro dodržování právních předpisů provádí inspekce z pohledu nezávislého úřadu, aby tak zajistila dodržování právních předpisů v celém ministerstvu, včetně obranných sil. Své úkoly vykonává nezávisle na provozních útvech Ministerstva obrany. V návaznosti na inspekci podá kancelář generálního inspektora pro dodržování právních předpisů neprodleně zprávu o svých zjištěních společně s nezbytnými opatřeními ke zlepšení přímo ministroví obrany. Na základě této zprávy může ministr obrany vydat příkazy za účelem provedení opatření nezbytných k nápravě situace. Za provedení těchto opatření odpovídá náměstek ministra, který musí o stavu provádění ministra obrany informovat.

Jako dobrovolné opatření pro zajištění transparentnosti jsou nyní zjištění inspekci obrany zveřejňována na internetových stránkách Ministerstva obrany (ačkoli to zákon nevyžaduje).

Inspekce obrany se dělí do tří kategorií:

- i) pravidelné inspekce obrany, které se provádějí periodicky ⁽³¹⁾;
- ii) kontrolní inspekce obrany, které se provádějí s cílem ověřit, zda byla opatření ke zlepšení účinně provedena, a
- iii) zvláštní inspekce obrany, které jsou prováděny u konkrétních záležitostech z příkazu ministra obrany.

V souvislosti s těmito inspekcemi může generální inspektor požadovat zprávy od dotčeného úřadu a předložení dokumentů, může za účelem inspekce vstupovat do prostor, požadovat vysvětlení náměstka ministra atd. Vzhledem k povaze úkolů kanceláře generálního inspektora pro dodržování právních předpisů v oblasti inspekce tento úřad vedou právní odborníci na velmi vysoké úrovni (bývalý vrchní státní zástupce).

4) Dozor Zpravodajské služby pro veřejnou bezpečnost

Zpravodajská služba pro veřejnou bezpečnost provádí pravidelné i zvláštní inspekce činnosti svých jednotlivých úřadů a kanceláří (úřad Zpravodajské služby pro veřejnou bezpečnost, kanceláře a pobočky Zpravodajské služby pro veřejnou bezpečnost atd.) Pro účely pravidelných inspekci je inspektorem (inspektory) určen některý náměstek generálního ředitele a/nebo ředitel. Tyto inspekce se rovněž týkají správy osobních informací.

5) Dozor vykonávaný parlamentem

Pokud jde o shromažďování informací pro účely vymáhání práva, může parlament prostřednictvím svého příslušného výboru přezkoumávat zákonnost činností shromažďování informací v oblasti národní bezpečnosti. Pravomoci parlamentu v oblasti vyšetřování se zakládají na článku 62 Ústavy a článcích 74 a 104 zákona o parlamentu.

C. Individuální ochrana

Individuální ochranu lze uplatňovat stejnými způsoby jako v oblasti prosazování trestního práva. To zahrnuje také nový mechanismus právní ochrany pro vyřizování a řešení stížností podaných fyzickými osobami z EU, který spravuje a dozoruje Komise pro ochranu osobních informací. V tomto ohledu viz příslušné pasáže oddílu II.C.

V oblasti národní bezpečnosti jsou navíc dostupné zvláštní možnosti individuální ochrany.

Na osobní informace shromážděné správním orgánem pro účely národní bezpečnosti se vztahují ustanovení kapitoly 4 zákona o ochraně osobních informací uchovávaných správními orgány. To zahrnuje právo žádat o zpřístupnění (článek 12) a opravu (včetně doplnění nebo výmaz) (článek 27) osobních informací uchovávaných o fyzické osobě, jakož i právo žádat o přerušování používání osobních informací v případě, že správní orgán získal dotčené informace protiprávně (článek 36). V oblasti národní bezpečnosti výkon těchto práv nicméně podléhá určitým omezením: žádostem

⁽³¹⁾ Jako příklad inspekce relevantní pro záležitosti obsažené v tomto prohlášení lze uvést pravidelnou inspekci obrany v roce 2016, která se týkala „informovanosti / připravenosti na dodržování právních předpisů“, neboť jedním ústředních bodů inspekce byla ochrana osobních informací. Konkrétněji se inspekce zabývala stavem správy, uložení atd. osobních informací. Kancelář generálního inspektora pro dodržování právních předpisů ve své zprávě uvedla několik nedostatků ve správě osobních informací, které by měly být zlepšeny, jako například skutečnost, že údaje nebyly chráněny heslem. Zpráva je dostupná na internetových stránkách Ministerstva obrany.

o zpřístupnění, opravu nebo přerušení používání nebude vyhověno, pokud se týkají „informací, u kterých existují přiměřené důvody, aby se vedoucí správního orgánu domníval, že zpřístupnění pravděpodobně naruší národní bezpečnost, poškodí vztah vzájemné důvěry s jinou zemí nebo mezinárodní organizací nebo povede k nevýhodě při vyjednávání s jinou zemí nebo mezinárodní organizací“ (čl. 14 bod iv)). Do této výjimky proto nespadá veškeré dobrovolné shromažďování informací týkajících se národní bezpečnosti, neboť tato výjimka vždy vyžaduje konkrétní posouzení rizik spojených se zpřístupněním informací.

Navíc, pokud je žádost fyzické osoby zamítnuta z toho důvodu, že se dotčené informace považují za nepřístupitelné ve smyslu čl. 14 bodu iv), může fyzická osoba za účelem přezkumu tohoto rozhodnutí podat správní opravný prostředek, v němž například uvádí, že v předmětném případě nejsou podmínky stanovené v čl. 14 bodě iv) splněny. V takovém případě vedoucí příslušného správního orgánu vede před přijetím rozhodnutí konzultace s Radou pro přezkum ochrany osobních informací a zpřístupnění informací. Tato rada daný opravný prostředek přezkoumá z nezávislého úhlu pohledu. Rada je vysoce specializovaný a nezávislý subjekt, jehož členy, vybírané z řad vynikajících odborníků, jmenuje předseda vlády se souhlasem obou komor parlamentu⁽³²⁾. Rada disponuje silnými pravomocemi v oblasti vyšetřování, včetně možnosti žádat o dokumenty a zpřístupnění dotčených osobních informací, vést neveřejné debaty a použít tzv. postup Vaughnova indexu⁽³³⁾. Rada následně vyhotoví písemnou zprávu, jež je předána dotčené fyzické osobě⁽³⁴⁾. Zjištění obsažená ve zprávě se zveřejní. Přestože zpráva není po formální stránce právně závazná, dotčené správní orgány se zprávami téměř vždy řídí⁽³⁵⁾.

Podle čl. 3 odst. 3 zákona o správních sporech může fyzická osoba předložit věc soudu a žádat o zrušení rozhodnutí správního orgánu osobní informace nepřístupnit.

IV. Pravidelný přezkum

V rámci pravidelného přezkumu rozhodnutí o odpovídající ochraně si budou Komise pro ochranu osobních informací a Evropská komise vyměňovat informace o zpracování údajů za podmínek zjištění o odpovídající úrovni ochrany, včetně podmínek stanovených v tomto prohlášení.

⁽³²⁾ Viz článek 4 zákona o zřízení Rady pro přezkum ochrany osobních informací a zpřístupnění informací.

⁽³³⁾ Viz článek 9 zákona o zřízení Rady pro přezkum ochrany osobních informací a zpřístupnění informací.

⁽³⁴⁾ Viz článek 16 zákona o zřízení Rady pro přezkum ochrany osobních informací a zpřístupnění informací.

⁽³⁵⁾ Za poslední tři roky neexistuje žádný precedent, kdy by dotčený správní orgán přijal rozhodnutí, které by se lišilo od závěrů rady. V minulosti se takové případy vyskytly jen velmi zřídka: pouze ve dvou z celkem 2 000 případů od roku 2005 (rok vstupu zákona o ochraně osobních informací uchovávaných správními orgány v platnost). Pokud správní orgán přijme rozhodnutí, které se liší od závěrů rady, musí to jasně odůvodnit podle čl. 50 odst. 1 položky 4 zákona o přezkumu správních stížností, jak se použije ve spojení s nahrazením čl. 42 odst. 2 zákona o ochraně osobních informací uchovávaných správními orgány.