

II

(Acte fără caracter legislativ)

DECIZII

DECIZIA DE PUNERE ÎN APLICARE (UE) 2019/419 A COMISIEI

din 23 ianuarie 2019

în temeiul Regulamentului (UE) 2016/679 al Parlamentului European și al Consiliului privind protecția adecvată a datelor cu caracter personal de către Japonia în temeiul Legii privind protecția informațiilor cu caracter personal

[notificată cu numărul C(2019) 304]

(Text cu relevanță pentru SEE)

COMISIA EUROPEANĂ,

având în vedere Tratatul privind funcționarea Uniunii Europene,

având în vedere Regulamentul (UE) 2016/679 al Parlamentului European și al Consiliului din 27 aprilie 2016 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date și de abrogare a Directivei 95/46/CE (Regulamentul general privind protecția datelor) (RGDP) ⁽¹⁾, în special articolul 45 alineatul (3),

după consultarea Autorității Europene pentru Protecția Datelor,

1. INTRODUCERE

- (1) Regulamentul (UE) 2016/679 stabilește normele pentru transferul de date cu caracter personal de la operatori sau persoane împuternicite de către operatori din Uniunea Europeană către țări terțe și organizații internaționale, în măsura în care astfel de transferuri intră în domeniul său de aplicare. Normele privind transferurile internaționale de date cu caracter personal sunt prevăzute în capitolul V din regulamentul menționat, mai precis la articolele 44-50. Fluxurile de date cu caracter personal către și dinspre țări situate în afara Uniunii Europene sunt necesare pentru extinderea cooperării internaționale și a comerțului internațional, garantând, în același timp, că nivelul de protecție conferit datelor cu caracter personal din Uniunea Europeană nu este subminat.
- (2) În temeiul articolului 45 alineatul (3) din Regulamentul (UE) 2016/679, Comisia poate decide, prin intermediul unui act de punere în aplicare, că o țară terță, un teritoriu sau unul ori mai multe sectoare specificate dintr-o țară terță sau o organizație internațională asigură un nivel de protecție adecvat. În astfel de condiții, transferurile de date cu caracter personal către țara terță, teritoriul, sectorul sau organizația internațională pot avea loc fără a fi necesar să se obțină autorizări suplimentare, astfel cum se prevede la articolul 45 alineatul (1) și în considerentul 103 din regulament.
- (3) În conformitate cu articolul 45 alineatul (2) din Regulamentul (UE) 2016/679, adoptarea unei decizii privind caracterul adecvat al nivelului de protecție trebuie să se bazeze pe o analiză cuprinzătoare a ordinii juridice a țării terțe, în ceea ce privește atât normele aplicabile importatorilor de date, cât și limitările și garanțiile referitoare la accesul autorităților publice la datele cu caracter personal. Evaluarea trebuie să stabilească dacă țara terță în cauză garantează un nivel de protecție „echivalent în esență” cu cel garantat în cadrul Uniunii Europene [considerentul 104 din Regulamentul (UE) 2016/679]. Conform clarificărilor aduse de Curtea de Justiție a Uniunii Europene, aceasta nu necesită un nivel identic de protecție ⁽²⁾. În special, mijloacele la care țara terță în cauză recurge pot fi diferite de cele utilizate în cadrul Uniunii Europene, cu condiția ca acestea să se dovedească, în practică, eficace pentru asigurarea unui nivel adecvat de protecție ⁽³⁾. Prin urmare, standardul caracterului adecvat nu necesită o

⁽¹⁾ JO L 119, 4.5.2016, p. 1.

⁽²⁾ Cauza C-362/14, Maximilian Schrems/Data Protection Commissioner („Schrems”), ECLI:EU:C:2015:650, punctul 73.

⁽³⁾ Schrems, punctul 74.

reproducere punct cu punct a normelor Uniunii. Mai curând, testul constă în a stabili dacă, prin esența drepturilor la viață privată și punerea în aplicare efectivă, supravegherea și exercitarea acestora, sistemul străin în cauză, în ansamblul său, oferă nivelul de protecție necesar ⁽⁴⁾.

- (4) Comisia a analizat cu atenție legislația și practica din Japonia. Pe baza constatărilor prezentate în considerentele 6-175, Comisia concluzionează că Japonia asigură un nivel adecvat de protecție pentru datele cu caracter personal transferate către organizații care intră în domeniul de aplicare al Legii privind protecția informațiilor cu caracter personal ⁽⁵⁾ și sub rezerva condițiilor suplimentare menționate în prezenta decizie. Aceste condiții sunt prevăzute în normele suplimentare (anexa I), adoptate de Comisia pentru protecția informațiilor cu caracter personal (PPC) ⁽⁶⁾ și în expunerile, asigurările și angajamentele oficiale transmise de guvernul japonez Comisiei Europene (anexa II).
- (5) Prezenta decizie are drept efect faptul că transferurile de la un operator sau de la o persoană împuternicită de către un operator din Spațiul Economic European (SEE) ⁽⁷⁾ către astfel de organizații din Japonia pot avea loc fără a fi necesar să se obțină autorizări suplimentare. Prezenta decizie nu aduce atingere aplicării directe a Regulamentului (UE) 2016/679 pentru astfel de organizații, atunci când sunt îndeplinite condițiile prevăzute la articolul 3.

2. NORMELE APLICABILE PRELUCRĂRII DATELOR DE CĂTRE OPERATORII ECONOMICI

2.1. Cadrul de protecție a datelor din Japonia

- (6) Regimul juridic care reglementează viața privată și protecția datelor în Japonia își are rădăcinile în Constituția promulgată în 1946.
- (7) Articolul 13 din Constituție prevede:

„Toți oamenii sunt respectați în calitate de indivizi. Dreptul la viață, la libertate și la căutarea fericirii, în măsura în care acesta nu aduce atingere bunăstării publice, sunt considerenți supremi în legislație, precum și în alte afaceri guvernamentale.”

- (8) Pe baza acestui articol, Curtea Supremă din Japonia a clarificat drepturile persoanelor fizice în ceea ce privește protecția informațiilor cu caracter personal. Într-o decizie din 1969, aceasta a recunoscut dreptul la protecția vieții private și la protecția datelor ca drept constituțional ⁽⁸⁾. În special, Curtea a statuat că „orice persoană are libertatea de a-și proteja propriile informații cu caracter personal de la a fi divulgate unei părți terțe sau de la a fi făcute publice fără un motiv întemeiat.” În plus, într-o decizie din 6 martie 2008 („Juki-Net”) ⁽⁹⁾, Curtea Supremă a statuat că „libertatea cetățenilor în viața lor privată este protejată împotriva exercitării autorității publice și se poate considera că orice persoană are, printre alte libertăți legate de viața privată, libertatea de a-și proteja propriile informații cu caracter personal de la a fi divulgate unei părți terțe sau de la a fi făcute publice fără un motiv întemeiat” ⁽¹⁰⁾.
- (9) La 30 mai 2003, Japonia a adoptat o serie de legi în domeniul protecției datelor:

— Legea privind protecția informațiilor cu caracter personal (APPI);

— Legea privind protecția informațiilor cu caracter personal deținute de organele administrative (APPIHAO);

— Legea privind protecția informațiilor cu caracter personal deținute de agențiile administrative constituite (APPI-IAA).

⁽⁴⁾ A se vedea Comunicarea Comisiei către Parlamentul European și Consiliu, „Schimbul de date cu caracter personal și protecția acestora într-o lume globalizată”, COM(2017) 7 din 10 ianuarie 2017, secțiunea 3.1, p. 6-7.

⁽⁵⁾ Legea privind protecția informațiilor cu caracter personal (Legea nr. 57/2003).

⁽⁶⁾ Mai multe informații privind PPC sunt disponibile la următoarea adresă: <https://www.ppc.go.jp/en/> (inclusiv datele de contact pentru întrebări și plângeri: <https://www.ppc.go.jp/en/contactus/access/>).

⁽⁷⁾ Prezenta decizie are relevanță pentru SEE. Acordul privind Spațiul Economic European (Acordul privind SEE) prevede extinderea pieței interne a Uniunii Europene la cele trei state SEE, și anume Islanda, Liechtenstein și Norvegia. Decizia Comitetului mixt care încorporează Regulamentul (UE) 2016/679 în anexa XI la Acordul privind SEE a fost adoptată de Comitetul mixt al SEE la 6 iulie 2018 și a intrat în vigoare la 20 iulie 2018. Regulamentul este, prin urmare, reglementat de acordul respectiv.

⁽⁸⁾ Curtea Supremă, Hotărârea Marelui complet din 24 decembrie 1969, Keishu Vol. 23, nr. 12, p. 1625.

⁽⁹⁾ Curtea Supremă, Hotărârea din 6 martie 2008, Minshu Vol. 62, nr. 3, p. 665.

⁽¹⁰⁾ Curtea Supremă, Hotărârea din 6 martie 2008, Minshu Vol. 62, nr. 3, p. 665.

- (10) Ultimele două legi menționate (modificate în 2016) conțin dispoziții aplicabile în materie de protecție a informațiilor cu caracter personal de către entități din sectorul public. Prelucrarea datelor care intră în domeniul de aplicare al acestor legi nu constituie obiectul constatării caracterului adecvat cuprinse în prezenta decizie, care se limitează la protecția informațiilor cu caracter personal de către „operatorii economici care gestionează informații cu caracter personal” în sensul APPI.
- (11) APPI a fost reformată în ultimii ani. APPI modificată a fost promulgată la 9 septembrie 2015 și a intrat în vigoare la 30 mai 2017. Modificarea a introdus o serie de noi garanții și, de asemenea, a consolidat garanțiile existente, sistemul de protecție a datelor din Japonia apropiindu-se astfel de cel european. Printre acestea, se numără, de exemplu, un set de drepturi individuale exercitabile sau instituirea unei autorități de supraveghere independente (PPC), însărcinată cu supravegherea și asigurarea respectării APPI.
- (12) Pe lângă APPI, prelucrarea informațiilor cu caracter personal care se încadrează în domeniul de aplicare al prezentei decizii este supusă normelor de punere în aplicare emise pe baza APPI. Printre acestea se numără un amendament la Ordinul Cabinetului de aplicare a Legii privind protecția informațiilor cu caracter personal din 5 octombrie 2016 și așa-numitele norme de punere în aplicare a Legii privind protecția informațiilor cu caracter personal adoptate de PPC ⁽¹¹⁾. Ambele seturi de norme au caracter juridic obligatoriu și executoriu și au intrat în vigoare în același timp ca APPI modificată.
- (13) În plus, la 28 octombrie 2016, Cabinetul Japoniei (constând din prim-ministru și miniștrii care formează guvernul său) a emis o „politică de bază” de a „promova în mod cuprinzător și integral măsurile privind protecția informațiilor cu caracter personal”. În temeiul articolului 7 din APPI, „politica de bază”, este elaborată sub forma unei decizii a Cabinetului și include orientări de politică referitoare la punerea în aplicare a APPI, care vizează atât administrația centrală, cât și administrațiile locale.
- (14) Recent, prin decizia Cabinetului adoptată la 12 iunie 2018, Guvernul Japoniei a modificat „politica de bază”. Cu scopul de a facilita transferurile internaționale de date, decizia respectivă a Cabinetului conferă PPC, în calitate de autoritate competentă cu administrarea și punerea în aplicare a APPI, „competența de a lua măsurile necesare pentru a remedia diferențele legate de sisteme și operațiuni dintre Japonia și țara străină în cauză pe baza articolului 6 din lege pentru a asigura tratarea corespunzătoare a informațiilor cu caracter personal primite din partea acestei țări”. Decizia Cabinetului prevede că este vorba în special de competența de a stabili o mai bună protecție prin adoptarea de către PPC a unor norme mai stricte care să le completeze și să le depășească pe cele prevăzute în APPI și în Ordinul Cabinetului. În temeiul respectivei decizii, aceste norme mai stricte sunt obligatorii și executorii pentru operatorii economici japonezi.
- (15) Pe baza articolului 6 din APPI și a respectivei decizii a Cabinetului, PPC a adoptat la 15 iunie 2018 „Normele suplimentare în conformitate cu Legea privind protecția informațiilor cu caracter personal pentru gestionarea datelor cu caracter personal transferate din UE pe baza unei decizii privind caracterul adecvat al nivelului de protecție” („normele suplimentare”), cu scopul de a spori protecția informațiilor cu caracter personal transferate din Uniunea Europeană în Japonia pe baza prezentei decizii privind caracterul adecvat al nivelului de protecție. Aceste norme suplimentare sunt obligatorii din punct de vedere juridic pentru operatorii economici din Japonia și sunt executorii, atât de către PPC, cât și de către instanțe, la fel ca dispozițiile APPI pe care normele le completează cu norme mai stricte și/sau mai detaliate ⁽¹²⁾. Întrucât operatorii economici din Japonia care primesc și/sau prelucrează ulterior date cu caracter personal din Uniunea Europeană vor avea obligația legală de a se conforma normelor suplimentare, aceștia vor trebui să se asigure [de exemplu, prin mijloace tehnice („marcare”) sau organizaționale (stocarea într-o bază de date specială)] că pot identifica astfel de date cu caracter personal pe parcursul „ciclului de viață” al acestora ⁽¹³⁾. În secțiunile următoare, conținutul fiecărei norme suplimentare este analizat ca parte a evaluării articolelor din APPI pe care le completează.
- (16) Spre deosebire de modificarea din 2015, când răspunderea a aparținut diverselor ministere din Japonia din sectoare specifice, APPI împuternicește PPC să adopte „orientări”, „pentru a asigura punerea în aplicare corespunzătoare și eficientă a acțiunilor care trebuie întreprinse de un operator economic” conform normelor de protecție a datelor. Prin intermediul orientărilor sale, PPC oferă o interpretare cu valoare de autoritate a acestor norme, în special a

⁽¹¹⁾ Disponibil la adresa: https://www.ppc.go.jp/files/pdf/PPC_rules.pdf

⁽¹²⁾ A se vedea normele suplimentare (secțiunea introductivă).

⁽¹³⁾ Acest lucru nu este pus sub semnul întrebării de obligația generală de a păstra o evidență (doar) pentru o anumită perioadă de timp. Deși originea datelor se numără printre informațiile pe care operatorul economic care gestionează informații cu caracter personal trebuie să le confirme în conformitate cu articolul 26 alineatul (1) din APPI, cerința prevăzută la articolul 26 alineatul (4) din APPI, coroborat cu articolul 18 din normele PPC, se referă numai la o anumită formă de înregistrare (a se vedea articolul 16 din normele PPC) și nu împiedică un operator economic care gestionează informații cu caracter personal să asigure identificarea datelor pentru perioade mai lungi. PPC a confirmat acest lucru și a afirmat că „informațiile cu privire la originea datelor din UE trebuie să fie păstrate de către operatorul economic care gestionează informații cu caracter personal atâta timp cât este necesar pentru a putea respecta normele suplimentare”.

APPI. Conform informațiilor primite din partea PPC, aceste orientări fac parte integrantă din cadrul juridic, trebuie interpretate prin coroborare cu textul APPI, Ordinul Cabinetului, normele PPC și un set de întrebări și răspunsuri⁽¹⁴⁾ elaborat de PPC. Prin urmare, acestea sunt „obligatorii pentru operatorii economici”. În cazul în care orientările prevăd că un operator economic „trebuie” sau „nu ar trebui” să acționeze într-un anumit mod, PPC va considera că nerespectarea dispozițiilor relevante echivalează cu o încălcare a legii⁽¹⁵⁾.

2.2. Domeniul de aplicare material și personal

- (17) Domeniul de aplicare al APPI este determinat de conceptele definite: „informații cu caracter personal”, „date cu caracter personal” și „operator economic care gestionează informații cu caracter personal”. În același timp, APPI prevede unele derogări importante de la domeniul său de aplicare, în special pentru datele cu caracter personal prelucrate în mod anonim și pentru tipurile specifice de prelucrare de către anumiți operatori. Deși APPI nu utilizează termenul de „prelucrare”, acesta se bazează pe conceptul echivalent de „gestionare”, care, în conformitate cu informațiile primite de la PPC, include „orice act privind datele cu caracter personal”, inclusiv achiziționarea, introducerea, acumularea, organizarea, stocarea, editarea/prelucrarea, reînnoirea, ștergerea, extragerea, utilizarea sau furnizarea de informații cu caracter personal.

2.2.1. Definiția informațiilor cu caracter personal

- (18) În primul rând, în ceea ce privește domeniul său de aplicare material, APPI distinge între informațiile cu caracter personal și datele cu caracter personal, doar anumite dispoziții ale legii fiind aplicabile primei categorii. În conformitate cu articolul 2 alineatul (1) din APPI, conceptul de „informație cu caracter personal” include orice informație referitoare la o persoană în viață care permite identificarea persoanei respective. Definiția distinge între două categorii de informații cu caracter personal: (i) coduri individuale de identificare; și (ii) alte informații cu caracter personal prin care poate fi identificată o anumită persoană. Această ultimă categorie include și informații care, în sine, nu permit identificarea, dar care, atunci când sunt „ușor de compilat” cu alte informații, permit identificarea unei anumite persoane. În conformitate cu Orientările PPC⁽¹⁶⁾, se apreciază, de la caz la caz, dacă informațiile pot fi considerate „ușor de compilat”, luând în considerare situația reală („condiția”) a operatorului economic. Se va presupune astfel dacă o astfel de compilare este (sau poate fi) efectuată de un operator economic mediu („normal”), utilizând mijloacele de care dispune operatorul respectiv. De exemplu, informațiile nu sunt „ușor de compilat” cu alte informații în cazul în care un operator economic trebuie să depună eforturi neobișnuite sau să comită acte ilegale pentru a obține informațiile care urmează să fie compilate de la unul sau mai mulți operatori economici.

2.2.2. Definiția datelor cu caracter personal

- (19) Numai anumite forme de informații cu caracter personal intră sub incidența noțiunii de „date cu caracter personal” în conformitate cu APPI. De fapt, „datele cu caracter personal” sunt definite drept „informații cu caracter personal care constituie o bază de date cu informații cu caracter personal”, și anume „un corpus colectiv de informații” care conține informații cu caracter personal „organizate în mod sistematic pentru a permite căutarea de informații cu caracter personal specifice cu ajutorul unui calculator”⁽¹⁷⁾ sau „prevăzute prin ordin al Cabinetului ca fiind organizate sistematic pentru a putea căuta cu ușurință anumite informații cu caracter personal” (dar „cu excepția celor prevăzute prin ordin al Cabinetului ca având puține posibilități de a aduce atingere drepturilor și intereselor unei persoane fizice, având în vedere metoda de utilizare”)⁽¹⁸⁾.
- (20) Această excepție este specificată mai în detaliu la articolul 3 alineatul (1) din Ordinul Cabinetului, conform căruia trebuie să fie îndeplinite următoarele trei condiții cumulative: (i) corpusul colectiv de informații trebuie să fi fost „emis pentru a fi vândut unui număr mare de persoane nespecificate, iar emiterea sa să nu fi fost efectuată prin încălcarea dispozițiilor unei legi sau a unui ordin care se bazează pe acesta”; (ii) corpusul trebuie să poată fi „achiziționat în orice moment de un număr mare de persoane nespecificate”; și (iii) datele cu caracter personal pe

⁽¹⁴⁾ PPC, „Întrebări și răspunsuri”, 16 februarie 2017 (modificate la 30 mai 2017), disponibile la următoarea adresă: <https://www.ppc.go.jp/files/pdf/kojohouQA.pdf>. În documentul „Întrebări și răspunsuri” se discută o serie de aspecte abordate în orientări prin oferirea unor exemple practice, cum ar fi ce înseamnă date cu caracter personal sensibile, interpretarea consimțământului individual, transferurile către terți în contextul tehnologiei de tip cloud computing sau obligația deținere a evidențelor aplicată transferurilor transfrontaliere. Documentul „Întrebări și răspunsuri” este disponibil numai în limba japoneză.

⁽¹⁵⁾ În urma unei întrebări specifice, PPC a informat Comitetul european pentru protecția datelor (CEPD) cu privire la faptul că „instanțele din Japonia își bazează interpretarea pe orientări atunci când aplică APPI/normele PPC în cauzele individuale aflate pe rolul lor și, prin urmare, au făcut trimitere în mod direct la textul orientărilor PPC în hotărârile lor. Așadar, și din acest punct de vedere, orientările PPC sunt obligatorii pentru operatorii economici. PPC nu are cunoștință de faptul că instanța s-ar fi îndepărtat vreodată de orientări.” În acest sens, PPC a transmis Comisiei o hotărâre în domeniul protecției datelor în care instanța s-a bazat în mod explicit pe aceste orientări pentru soluția sa (a se vedea Instanța districtuală din Osaka, decizia din 19 mai 2006, Hanrei Jiho, Vol. 1948, p. 122, în care instanța a hotărât că operatorul economic are obligația de a lua o măsură de control de securitate pe baza acestor orientări).

⁽¹⁶⁾ Orientările PPC (Ediția cu normele generale), p. 6.

⁽¹⁷⁾ Acestea se referă la orice sistem de înregistrare electronică. Orientările PPC (Ediția generală, p. 17) oferă exemple specifice în acest sens, de exemplu o listă de adrese de e-mail stocate în software-ul client pentru e-mailuri.

⁽¹⁸⁾ Articolul 2 alineatele (4) și (6) din APPI.

care le conține acest corpus trebuie să fie „furnizate în scopul lor inițial fără a adăuga alte informații referitoare la o persoană în viață”. În conformitate cu explicațiile primite din partea PPC, această excepție restrânsă a fost introdusă cu scopul de a exclude cărțile de telefon sau tipurile similare de liste de abonați.

- (21) Pentru datele colectate în Japonia, această distincție între „informațiile cu caracter personal” și „datele cu caracter personal” este relevantă deoarece informațiile respective nu pot face întotdeauna parte dintr-o „bază de date cu informații cu caracter personal” (de exemplu, un set unic de date colectate și prelucrate manual) și, prin urmare, nu se vor aplica acele dispoziții din APPI care se referă exclusiv la datele cu caracter personal⁽¹⁹⁾.
- (22) În schimb, această distincție nu va fi relevantă pentru datele cu caracter personal importate din Uniunea Europeană în Japonia pe baza unei decizii privind caracterul adecvat al nivelului de protecție. Întrucât astfel de date vor fi, de regulă, transferate prin mijloace electronice (având în vedere că în era digitală aceasta este modalitatea obișnuită de a face schimb de date, în special pe o distanță mare, precum între UE și Japonia) și, prin urmare, vor deveni parte a sistemului electronic de înregistrare a datelor deținut de importator, potrivit APPI aceste date ale UE vor intra în categoria „date cu caracter personal”. Dacă datele cu caracter personal ar fi transferate din UE prin alte mijloace (de exemplu, pe suport de hârtie), această situație excepțională va intra în continuare sub incidența APPI în cazul în care, în urma transferului, acestea vor deveni parte a unui „corpus colectiv de informații” organizat sistematic, astfel încât să faciliteze căutarea cu ușurință a unor informații specifice [articolul 2 alineatul (4) punctul (ii) din APPI]. În conformitate cu articolul 3 alineatul (2) din Ordinul Cabinetului, acest lucru se va întâmpla în cazul în care informațiile sunt aranjate „conform unei anumite reguli”, iar baza de date dispune de instrumente, cum ar fi un cuprins sau index, pentru facilitarea căutării. Aceasta corespunde definiției unui „sistem de înregistrare” în sensul articolului 2 alineatul (1) din RGPD.

2.2.3. Definiția datelor cu caracter personal păstrate

- (23) Anumite dispoziții ale APPI, în special articolele 27-30 referitoare la drepturile individuale, se aplică doar unei categorii specifice de date cu caracter personal, și anume „datelor cu caracter personal păstrate”. Acestea sunt definite la articolul 2 alineatul (7) din APPI ca date cu caracter personal, altele decât cele care sunt fie: (i) „prevăzute prin ordin al Cabinetului ca fiind de natură să aducă atingere intereselor publice sau de altă natură, în cazul în care prezența sau absența lor este adusă la cunoștință”; fie (ii) „trebuie șterse în termen de maximum un an care este prevăzut prin ordin al Cabinetului”.
- (24) În ceea ce privește prima dintre cele două categorii, aceasta este explicată la articolul 4 din Ordinul Cabinetului și cuprinde patru tipuri de excepții⁽²⁰⁾. Aceste derogări urmăresc obiective similare celor enumerate la articolul 23 alineatul (1) din Regulamentul (UE) 2016/679, în special protecția persoanei vizate („persoana principală” în terminologia APPI) și libertatea celorlalți, securitatea națională, securitatea publică, aplicarea dreptului penal sau alte obiective importante de interes public general. În plus, din formularea de la articolul 4 alineatul (1) punctele (i)-(iv) din Ordinul Cabinetului rezultă că aplicarea lor presupune întotdeauna un risc specific pentru unul dintre interesele protejate importante⁽²¹⁾.
- (25) A doua categorie a fost specificată suplimentar la articolul 5 din Ordinul Cabinetului. Coroborat cu articolul 2 alineatul (7) din APPI, acesta exclude din domeniul de aplicare al noțiunii de date cu caracter personal păstrate și, prin urmare, al drepturilor individuale în conformitate cu APPI, datele cu caracter personal „care urmează să fie șterse” în termen de șase luni. PPC a explicat că această derogare vizează stimularea operatorilor economici să păstreze și să prelucreză datele pentru cea mai scurtă perioadă posibilă. Totuși, acest lucru ar însemna că persoanele vizate din UE nu ar putea beneficia de drepturi importante din alte motive decât durata păstrării datelor lor de către operatorul economic în cauză.
- (26) Pentru a remedia această situație, norma suplimentară (2) prevede că datele cu caracter personal transferate din Uniunea Europeană să fie „prelucrate ca date cu caracter personal păstrate, în sensul articolului 2 alineatul (7) din lege, indiferent de perioada în care se prevede ștergerea acestora”. Prin urmare, perioada de păstrare nu va avea niciun impact asupra drepturilor acordate persoanelor vizate din UE.

⁽¹⁹⁾ De exemplu, articolul 23 din APPI privind condițiile de partajare cu părți terțe a datelor cu caracter personal.

⁽²⁰⁾ Și anume, datele cu caracter personal: (i) „în legătură cu care există posibilitatea, în cazul în care se face cunoscută prezența sau absența datelor cu caracter personal menționate, să dăuneze vieții, integrității fizice sau bunurilor unei persoane principale sau unei părți terțe”; (ii) datele „în legătură cu care există posibilitatea, în cazul în care se face cunoscută prezența sau absența datelor cu caracter personal menționate, să încurajeze sau să inducă un act ilegal sau nedrept”; (iii) datele „în legătură cu care există posibilitatea, în cazul în care se face cunoscută prezența sau absența datelor cu caracter personal menționate, să submineze securitatea națională, să distrugă o relație de încredere cu o țară străină ori cu o organizație internațională sau să cauzeze un prejudiciu în negocierile cu o țară străină sau cu o organizație internațională”; și (iv) cele „în legătură cu care există posibilitatea, în cazul în care se face cunoscută prezența sau absența datelor cu caracter personal menționate, să împiedice menținerea siguranței și a ordinii publice, cum ar fi prevenirea, reprimarea sau investigarea unei infracțiuni”.

⁽²¹⁾ În aceste condiții, nu este necesară notificarea persoanei. Acest lucru este în conformitate cu articolul 23 alineatul (2) litera (h) din RGPD, care prevede că nu este necesar ca persoanele vizate să fie informate cu privire la restricție în cazul în care aceasta „poate aduce atingere scopului restricției”.

2.2.4. Definiția datelor cu caracter personal prelucrate în mod anonim

- (27) Cerințele aplicabile informațiilor cu caracter personal prelucrate în mod anonim, astfel cum sunt definite la articolul 2 alineatul (9) din APPI, sunt prevăzute în capitolul 4 secțiunea 2 din lege („Obligațiile operatorului economic care gestionează informații prelucrate în mod anonim”). În schimb, aceste informații nu sunt reglementate de dispozițiile capitolului IV secțiunea 1 din APPI, care include articolele ce prevăd garanțiile de protecție a datelor și drepturile care se aplică prelucrării datelor cu caracter personal în temeiul legii respective. În consecință, deși „informațiile cu caracter personal prelucrate în mod anonim” nu fac obiectul normelor „standard” de protecție a datelor (specificate în capitolul IV secțiunea 1 și la articolul 42 din APPI), acestea se încadrează în domeniul de aplicare al APPI, în special articolele 36-39.
- (28) În conformitate cu articolul 2 alineatul (9) din APPI, „informațiile cu caracter personal prelucrate în mod anonim” sunt informațiile referitoare la o persoană care au fost „ produse prin prelucrarea informațiilor cu caracter personal” prin intermediul măsurilor prevăzute în APPI [articolul 36 alineatul (1)] și specificate în normele PPC (articolul 19), astfel încât a devenit imposibilă identificarea unei anumite persoane sau restabilirea informațiilor cu caracter personal.
- (29) Din aceste dispoziții, astfel cum a fost confirmat și de către PPC, rezultă că prelucrarea informațiilor cu caracter personal care sunt „anonime” nu trebuie să fie ireversibilă din punct de vedere tehnic. În temeiul articolului 36 alineatul (2) din APPI, operatorii economici care gestionează „informații cu caracter personal prelucrate în mod anonim” au doar obligația de a preveni reidentificarea prin luarea unor măsuri de asigurare a securității „descrierilor etc. și a codurilor individuale de identificare șterse din informațiile cu caracter personal utilizate pentru a obține informații prelucrate în mod anonim, precum și informații referitoare la o metodă de prelucrare aplicată”.
- (30) Având în vedere faptul că „informațiile cu caracter personal prelucrate în mod anonim”, astfel cum sunt definite în APPI, includ date pentru care este încă posibilă reidentificarea persoanei, acest lucru ar putea însemna că datele cu caracter personal transferate din Uniunea Europeană ar putea pierde o parte din măsurile de protecție disponibile prin intermediul unui proces care, în conformitate cu Regulamentul (UE) 2016/679, ar fi considerat mai degrabă o formă de „pseudonimizare” decât de „anonimizare” (prin urmare, fără a li se schimba natura de date cu caracter personal).
- (31) Pentru a remedia această situație, normele suplimentare prevăd cerințe suplimentare aplicabile numai datelor cu caracter personal transferate din Uniunea Europeană în temeiul prezentei decizii. În conformitate cu norma (5) din Normele suplimentare, aceste informații cu caracter personal sunt considerate ca fiind „informații cu caracter personal prelucrate în mod anonim” numai în sensul APPI „în cazul în care operatorul economic care gestionează informații cu caracter personal ia măsuri care fac ca eliminarea datelor de identificare a persoanei să fie ireversibilă pentru oricine, inclusiv prin ștergerea informațiilor legate de metoda de prelucrare etc.” Acestea din urmă au fost specificate în normele suplimentare ca informații referitoare la descrieri și la codurile individuale de identificare care au fost șterse din informațiile cu caracter personal utilizate pentru a produce „informații cu caracter personal prelucrate în mod anonim”, precum și informații referitoare la o metodă de prelucrare aplicată, eliminând în același timp aceste descrieri și coduri de identificare individuale. Cu alte cuvinte, normele suplimentare prevăd obligația operatorului economic care produce „informații cu caracter personal prelucrate în mod anonim” să distrugă „cheia” care permite identificarea din nou a datelor. Acest lucru înseamnă că datele cu caracter personal originare din Uniunea Europeană vor intra sub incidența dispozițiilor APPI cu privire la „informațiile cu caracter personal prelucrate în mod anonim” numai în cazurile în care ar fi, de asemenea, considerate informații anonime în temeiul Regulamentului (UE) 2016/679 ⁽²²⁾.

2.2.5. Definiția operatorului economic care gestionează informații cu caracter personal

- (32) În ceea ce privește domeniul său de aplicare personal, APPI se aplică numai în cazul operatorilor economici care gestionează informații cu caracter personal. Conform definiției de la articolul 2 alineatul (5) din APPI, un operator economic care gestionează informații cu caracter personal este definit drept „o persoană care furnizează o bază de date cu informații cu caracter personal etc. pentru utilizare în cadrul activității sale”, cu excepția guvernului și a agențiilor administrative, atât la nivel central, cât și la nivel local.
- (33) Conform Orientărilor PPC, „activitate” înseamnă orice „comportament care are ca scop exercitarea, pentru un anumit obiectiv, independent de obținerea sau nu de profit, în mod repetat și continuu, a unei întreprinderi recunoscute din punct de vedere social”. Organizațiile fără personalitate juridică (cum ar fi asociațiile *de facto*) sau persoanele fizice sunt considerate drept operatori economici care gestionează informații cu caracter personal dacă furnizează (utilizează) o bază de date cu informații cu caracter personal etc. pentru activitățile lor ⁽²³⁾. Prin urmare, noțiunea de „activitate” în cadrul APPI este foarte largă, în sensul că include nu numai activități cu scop lucrativ, ci și activități fără scop lucrativ exercitate de toate tipurile de organizații și de persoane fizice. În plus, „utilizarea în cadrul activității” cuprinde, de asemenea, informații cu caracter personal care nu sunt utilizate în relațiile comerciale (externe) ale operatorului, ci intern, de exemplu, pentru prelucrarea datelor angajaților.

⁽²²⁾ A se vedea Regulamentul (UE) 2016/679, considerentul 26.

⁽²³⁾ Orientările PPC (Ediția cu normele generale), p. 18.

- (34) În ceea ce privește beneficiarii măsurilor de protecție prevăzute în APPI, legea nu face nicio distincție în funcție de cetățenia, reședința sau situația geografică a unei persoane. Același lucru este valabil și în ceea ce privește posibilitățile persoanelor fizice de a introduce căi de atac, fie la PPC, fie la o instanță judecătorească.

2.2.6. Conceptele de operator și de persoană împuternicită de către operator

- (35) În cadrul APPI, nu se face nicio distincție specifică între obligațiile impuse operatorilor și persoanelor împuternicite de către operatori. Absența acestei distincții nu afectează nivelul de protecție, întrucât toți operatorii economici care gestionează informații cu caracter personal intră sub incidența tuturor dispozițiilor legii. Un operator economic care gestionează informații cu caracter personal și care încredințează gestionarea datelor cu caracter personal unui mandatar (echivalentul unei persoane împuternicite de către operator în temeiul RGPD) rămâne supus obligațiilor care îi revin în temeiul APPI și al normelor suplimentare în ceea ce privește datele pe care le-a încredințat. În plus, în conformitate cu articolul 22 din APPI, operatorul respectiv este obligat să „exercite supravegherea necesară și adecvată” asupra mandatarului. La rândul său, astfel cum a confirmat PPC, mandatarul se supune el însuși tuturor obligațiilor prevăzute în APPI și în normele suplimentare.

2.2.7. Excluderi sectoriale

- (36) Articolul 76 din APPI exclude anumite tipuri de prelucrare a datelor de la aplicarea capitolului IV din lege, care conține principalele dispoziții privind protecția datelor (principii de bază, obligații ale operatorilor economici, drepturi individuale, supravegherea exercitată de PPC). Prelucrarea vizată de excluderea sectorială prevăzută la articolul 76 este exceptată, de asemenea, drept una dintre competențele de executare ale PPC, în temeiul articolului 43 alineatul (2) din APPI ⁽²⁴⁾.
- (37) Categoriile relevante pentru excluderea sectorială prevăzută la articolul 76 din APPI sunt definite prin utilizarea unui dublu criteriu bazat pe tipul de operator economic care gestionează informații cu caracter personal și prelucrează astfel de informații, precum și pe scopul prelucrării. Mai precis, excluderea se aplică: (i) instituțiilor de radiodifuziune, editorilor de ziare, agențiilor de comunicare sau altor organizații de presă (inclusiv oricărei persoane fizice care desfășoară activități de presă ca activitate profesională), în măsura în care prelucrează informații cu caracter personal în scopuri jurnalistice; (ii) persoanelor implicate într-o activitate profesională legată de scris, în măsura în care activitatea respectivă implică informații cu caracter personal; (iii) universităților și oricăror alte organizații sau grupuri care au drept scop studiile universitare sau oricărei persoane care aparține unei astfel de organizații, în măsura în care prelucrează informații cu caracter personal în scopul studiilor universitare; (iv) instituțiilor religioase în măsura în care prelucrează informații cu caracter personal în scopul desfășurării unei activități religioase (inclusiv a tuturor activităților conexe); și (v) organismelor politice în măsura în care prelucrează informații cu caracter personal în scopul desfășurării activității lor politice (inclusiv a tuturor activităților conexe). Prelucrarea informațiilor cu caracter personal pentru unul dintre scopurile enumerate la articolul 76 de către alte tipuri de operatori economici care gestionează informații cu caracter personal, precum și prelucrarea de informații cu caracter personal de către unul dintre operatorii economici care gestionează astfel de informații în alte scopuri, de exemplu în contextul ocupării forței de muncă, rămân reglementate de dispozițiile capitolului IV.
- (38) Pentru a asigura un nivel adecvat de protecție a datelor cu caracter personal transferate din Uniunea Europeană către operatorii economici din Japonia, sub incidența prezentei decizii ar trebui să intre numai prelucrarea informațiilor cu caracter personal care intră în domeniul de aplicare al capitolului IV din APPI – și anume, de către un operator economic care gestionează informații cu caracter personal în măsura în care situația de prelucrare nu corespunde niciuneia dintre excluderile sectoriale. Prin urmare, domeniul său de aplicare ar trebui aliniat cu cel al APPI. Potrivit informațiilor primite din partea PPC, în cazul în care un operator economic care gestionează informații cu caracter personal și care face obiectul prezentei decizii modifică ulterior scopul utilizării (în măsura în care acest lucru este permis), iar ulterior ar fi vizat de una dintre excluderile sectoriale prevăzute la articolul 76 din APPI, această situație ar fi considerată drept transfer internațional (având în vedere că, în astfel de cazuri, prelucrarea informațiilor cu caracter personal nu ar mai fi reglementată de capitolul IV din APPI și, prin urmare, nu ar intra în domeniul său de aplicare). Același lucru s-ar aplica în cazul în care un operator economic care gestionează informații cu caracter personal oferă astfel de informații unei entități care intră sub incidența articolului 76 din APPI în vederea utilizării pentru unul dintre scopurile de prelucrare indicate în dispoziția respectivă. În ceea ce privește datele cu caracter personal transferate din Uniunea Europeană, acesta ar constitui, prin urmare, un transfer ulterior sub rezerva garanțiilor relevante [în special cele menționate la articolul 24 din APPI și în norma suplimentară (4)]. În cazul în care operatorul economic care gestionează informații cu caracter personal se bazează pe consimțământul persoanei vizate ⁽²⁵⁾, acesta va trebui să îi furnizeze toate informațiile necesare, inclusiv cu privire la faptul că informațiile cu caracter personal nu vor mai fi protejate de APPI.

⁽²⁴⁾ În ceea ce privește alți operatori, PPC, în exercitarea competențelor sale de investigare și de executare, nu îi împiedică să își exercite dreptul la libertatea de exprimare, la libertatea de învățare, la libertatea religioasă și la libertatea de activitate politică [articolul 43 alineatul (1) din APPI].

⁽²⁵⁾ Astfel cum a explicat PPC, consimțământul este interpretat în Orientările PPC ca fiind o „expresie a intenției persoanei principale, în sensul că aceasta acceptă ca datele sale cu caracter personal să poată fi prelucrate printr-o metodă indicată de un operator economic care gestionează informații cu caracter personal”. Orientările PPC (Ediția cu normele generale, p. 24) enumeră modalitățile prin care consimțământul este considerat ca făcând parte din „practicile comerciale obișnuite în Japonia”, și anume acordul oral, returnarea de formulare sau alte documente, acordul prin e-mail, bifarea unei casete pe o pagină internet, efectuarea unui clic pe o pagină de start (*home page*), utilizarea unui ecran tactil etc. Toate aceste metode constituie o formă de exprimare expresă a consimțământului.

2.3. Garanții, drepturi și obligații

2.3.1. Limitarea scopului

- (39) Datele cu caracter personal ar trebui să fie prelucrate într-un scop anume și să fie utilizate ulterior numai în măsura în care acest lucru nu este incompatibil cu scopul prelucrării. Acest principiu al protecției datelor este garantat în temeiul articolelor 15 și 16 din APPI.
- (40) APPI se bazează pe principiul care prevede că un operator economic trebuie să specifice scopul utilizării „cât mai explicit posibil” [articolul 15 alineatul (1)] și că, atunci când prelucrează datele, îi revin obligații în acest sens.
- (41) În această privință, articolul 15 alineatul (2) din APPI prevede că scopul inițial nu poate fi modificat de către operatorul economic care gestionează informații cu caracter personal „în afară de domeniul de aplicare recunoscut ca fiind relevant în mod rezonabil în scopul de utilizare premodificat”, care este interpretat în orientările PPC drept echivalent cu ceea ce poate fi anticipat în mod obiectiv de către persoana vizată, pe baza „convențiilor sociale normale” ⁽²⁶⁾.
- (42) În plus, în conformitate cu articolul 16 alineatul (1) din APPI, operatorilor economici care gestionează informații cu caracter personal le este interzis să prelucreze astfel de informații dincolo de „domeniul de aplicare necesar pentru a atinge un scop de utilizare” specificat la articolul 15 fără a obține în prealabil consimțământul persoanei vizate, cu excepția cazului în care se aplică una dintre derogările prevăzute la articolul 16 alineatul (3) ⁽²⁷⁾.
- (43) În ceea ce privește informațiile cu caracter personal obținute de la un alt operator economic, operatorul economic care gestionează informații cu caracter personal este, în principiu, liber să stabilească un nou scop de utilizare ⁽²⁸⁾. Pentru a se asigura că, în cazul unui transfer din Uniunea Europeană, un astfel de destinatar este obligat să respecte scopul în care au fost transferate datele, norma suplimentară (3) impune ca, în cazurile în care un [operator economic care gestionează informații cu caracter personal] primește date cu caracter personal din UE pe baza unei decizii privind caracterul adecvat al nivelului de protecție” sau un astfel de operator „primește de la un alt [operator economic care gestionează informații cu caracter personal] date cu caracter personal transferate anterior din UE pe baza unei decizii privind caracterul adecvat al nivelului de protecție” (transmitere mai departe), destinatarul trebuie „să precizeze scopul utilizării datelor cu caracter personal menționate în sfera scopului de utilizare pentru care datele au fost primite inițial sau ulterior”. Cu alte cuvinte, regula garantează că, în contextul unui transfer, scopul specificat în temeiul Regulamentului (UE) 2016/679 continuă să determine prelucrarea și că o modificare a acestui scop în orice etapă a lanțului de prelucrare din Japonia ar necesita consimțământul persoanei vizate din UE. Deși obținerea acestui consimțământ impune operatorului economic care gestionează informații cu caracter personal să contacteze persoana vizată, în cazul în care acest lucru nu este posibil, rezultă pur și simplu că scopul inițial trebuie să fie menținut.

2.3.2. Legalitatea și corectitudinea prelucrării

- (44) Protecția suplimentară menționată în considerentul 43 este cu atât mai relevantă cu cât, cu ajutorul principiului limitării scopului, sistemul japonez garantează, de asemenea, că datele cu caracter personal sunt prelucrate în mod legal și corect.
- (45) În conformitate cu APPI, atunci când un operator economic care gestionează informații cu caracter personal colectează astfel de informații, este necesar să se precizeze în mod detaliat scopul utilizării informațiilor cu caracter personal ⁽²⁹⁾ și să se informeze cu promptitudine persoana vizată cu privire la utilizarea informațiilor cu caracter personal (sau la divulgarea către publicul larg) în acest scop ⁽³⁰⁾. În plus, articolul 17 din APPI prevede că un operator economic care gestionează informații cu caracter personal nu poate achiziționa astfel de informații prin înșelăciune sau prin alte mijloace neadecvate. În ceea ce privește anumite categorii de date, cum ar fi informațiile cu caracter personal care implică o atenție specială, achiziționarea lor necesită consimțământul persoanei vizate [articolul 17 alineatul (2) din APPI].

⁽²⁶⁾ Documentul „Întrebări și răspunsuri” emis de PPC conține o serie de exemple pentru a ilustra această noțiune. Printre exemplele de situații în care modificarea rămâne într-un domeniu de aplicare relevant în mod rezonabil se numără în special utilizarea informațiilor cu caracter personal obținute de la cumpărători de bunuri sau servicii în contextul unei tranzacții comerciale, în scopul informării cumpărătorilor respectivi cu privire la alte bunuri sau servicii relevante disponibile (de exemplu, un operator al unui club de fitness care înregistrează adresele de e-mail ale membrilor pentru a-i informa cu privire la cursuri și programe și pentru a utiliza adresele respective pentru a-și informa membrii cu privire la un nou serviciu de orientare nutrițională furnizat de club). În același timp, documentul „Întrebări și răspunsuri” include, de asemenea, un exemplu de situație în care nu se permite modificarea scopului de utilizare, și anume dacă o societate transmite informații cu privire la bunurile și serviciile sale la adresele de e-mail pe care le-a colectat în scopul avertizării cu privire la fraudarea sau furtul unui card de membru.

⁽²⁷⁾ Aceste derogări pot rezulta din alte acte cu putere de lege și norme administrative sau se referă la situații în care prelucrarea informațiilor cu caracter personal este necesară: (i) pentru „protecția vieții umane, a integrității fizice sau a bunurilor”; (ii) pentru „a îmbunătăți igiena publică sau a încuraja creșterea de copii sănătoși”; sau (iii) pentru „a coopera cu agențiile sau organismele guvernamentale ori cu reprezentanții acestora” în îndeplinirea atribuțiilor lor statutare. În plus, categoriile (i) și (ii) se aplică numai dacă este dificil să se obțină consimțământul persoanei vizate, iar categoria (iii) numai dacă există riscul ca obținerea consimțământului persoanei vizate să interfereze cu îndeplinirea unor astfel de sarcini.

⁽²⁸⁾ Acestea fiind spuse, în temeiul articolului 23 alineatul (1) din APPI, consimțământul persoanei fizice este, în principiu, necesar pentru divulgarea datelor către o terță parte. În acest mod, persoana fizică poate exercita un anumit control asupra utilizării datelor sale de către un alt operator economic.

⁽²⁹⁾ În conformitate cu articolul 15 alineatul (1) din APPI, o astfel de specificație trebuie să fie „cât mai explicită posibil”.

⁽³⁰⁾ Articolul 18 alineatul (1) din APPI.

- (46) În consecință, astfel cum s-a explicat în considerentele 41 și 42, operatorul economic care gestionează informațiile cu caracter personal nu este autorizat să prelucreză astfel de informații în alte scopuri, cu excepția cazului în care persoana vizată își dă consimțământul pentru o astfel de prelucrare sau în cazul în care se aplică una dintre derogările prevăzute la articolul 16 alineatul (3) din APPI.
- (47) În cele din urmă, în ceea ce privește furnizarea suplimentară de informații cu caracter personal unei părți terțe ⁽³¹⁾, articolul 23 alineatul (1) din APPI limitează divulgarea acestora la cazuri specifice, cu consimțământul prealabil al persoanei vizate, ca regulă generală ⁽³²⁾. Articolul 23 alineatele (2), (3) și (4) din APPI prevede excepții de la cerința de obținere a consimțământului. Totuși, aceste excepții se aplică numai în cazul datelor care nu sunt sensibile și necesită ca operatorul economic să informeze în prealabil persoanele vizate cu privire la intenția de a divulga informațiile cu caracter personal ale acestora către o parte terță și cu privire la posibilitatea de a se opune oricărei alte divulgări ulterioare ⁽³³⁾.
- (48) În ceea ce privește transferurile din Uniunea Europeană, datele cu caracter personal vor trebui, în mod necesar, să fie mai întâi colectate și prelucrate în UE în conformitate cu Regulamentul (UE) 2016/679. Acest lucru va implica întotdeauna, pe de o parte, colectarea și prelucrarea, inclusiv pentru transferul din Uniunea Europeană în Japonia, pe baza unuia dintre temeiurile juridice enumerate la articolul 6 alineatul (1) din regulamentul și, pe de altă parte, colectarea într-un scop specific, explicit și legitim, precum și interzicerea prelucrării ulterioare, inclusiv prin transfer, într-un mod incompatibil cu acest scop, astfel cum se prevede la articolul 5 alineatul (1) litera (b) și la articolul 6 alineatul (4) din regulamentul.
- (49) În urma transferului, conform normei suplimentare (3), operatorul economic care gestionează informații cu caracter personal și care va primi datele va trebui să „confirme” scopul (scopurile) specific(e) care stă (stau) la baza transferului [și anume, scopul specificat în temeiul Regulamentului (UE) 2016/679] și să prelucreză ulterior aceste date în conformitate cu scopul (scopurile) respectiv(e) ⁽³⁴⁾. Aceasta înseamnă nu numai că dobânditorul inițial al acestor date cu caracter personal din Japonia, ci și orice viitor destinatar al datelor (inclusiv un mandatar) trebuie să respecte scopul (scopurile) specificat(e) în regulamentul.
- (50) În plus, în cazul în care operatorul economic care gestionează informații cu caracter personal ar dori să schimbe scopul specificat anterior în conformitate cu Regulamentul (UE) 2016/679, în temeiul articolului 16 alineatul (1) din APPI acesta ar trebui să obțină, în principiu, consimțământul persoanei vizate. În absența acestui consimțământ, orice prelucrare a datelor care depășește domeniul de aplicare necesar pentru atingerea scopului său de utilizare ar constitui o încălcare a articolului 16 alineatul (1), care ar putea fi invocată de PPC și de instanțele judecătorești.
- (51) Prin urmare, având în vedere faptul că, în conformitate cu Regulamentul (UE) 2016/679, un transfer necesită un temei juridic valabil și un scop specific, care se reflectă în scopul utilizării „confirmat” în conformitate cu APPI, combinația dintre dispozițiile relevante ale APPI și ale normei suplimentare (3) oferă asigurarea că prelucrarea datelor UE în Japonia va continua să fie legală.

2.3.3. Exactitatea și reducerea la minimum a datelor

- (52) Datele ar trebui să fie exacte și, dacă este necesar, actualizate. De asemenea, ar trebui să fie adecvate, relevante și neexcesive în raport cu scopurile în care sunt prelucrate.
- (53) Aceste principii sunt asigurate în legislația japoneză de articolul 16 alineatul (1) din APPI, care interzice gestionarea informațiilor cu caracter personal dincolo de „domeniul de aplicare necesar pentru a atinge un scop de utilizare”. Astfel cum a explicat PPC, acest lucru nu doar exclude utilizarea datelor care nu sunt exacte și utilizarea excesivă a datelor (dincolo de ceea ce este necesar pentru atingerea scopului de utilizare), ci implică, de asemenea, interdicția de a trata datele care nu sunt relevante pentru realizarea scopului de utilizare.

⁽³¹⁾ Deși mandatarii sunt excluși din noțiunea de „parte terță” în sensul aplicării articolului 23 (a se vedea punctul 5), această excludere se aplică numai în măsura în care mandatarii gestionează datele cu caracter personal în limitele prevăzute în atribuire („în limitele domeniului de aplicare necesar pentru unul dintre scopurile utilizării”), și anume acționează ca persoană împuternicită de către operator.

⁽³²⁾ Celelalte motive (excepționale) sunt: (i) furnizarea de informații cu caracter personal „pe baza actelor cu putere de lege și a normelor administrative”; (ii) cazurile „în care este necesar să se protejeze viața, integritatea fizică sau bunurile unei persoane și în cazul în care este dificil să se obțină consimțământul persoanei principale”; (iii) cazurile „în care există o nevoie specială să se îmbunătățească igiena publică sau să se încurajeze creșterea de copii sănătoși și în care este dificil să se obțină consimțământul persoanei principale” și (iv) cazurile „în care este necesar să se coopereze cu o organizație guvernamentală centrală sau cu o administrație locală ori o persoană căreia acestea îi încredințează activități prevăzute în acte cu putere de lege și norme administrative și atunci când există posibilitatea ca obținerea consimțământului persoanei principale să interfereze cu desfășurarea activităților în cauză”.

⁽³³⁾ Printre informațiile care trebuie furnizate se numără, în special, categoriile de date cu caracter personal care urmează să fie partajate cu o parte terță și metoda de transmitere. În plus, operatorul economic care gestionează informații cu caracter personal trebuie să informeze persoana vizată cu privire la posibilitatea de a se opune transmiterii și cu privire la modul în care poate face o astfel de cerere.

⁽³⁴⁾ În conformitate cu articolul 26 alineatul (1) punctul (ii) din APPI, atunci când primește date cu caracter personal de la o parte terță, un operator economic care gestionează informații cu caracter personal este obligat să „confirme” (să verifice) „detaliile privind dobândirea de către partea terță a datelor cu caracter personal”, inclusiv scopul acestei dobândiri. Deși articolul 26 nu specifică în mod expres faptul că operatorul economic care gestionează informații cu caracter personal trebuie să respecte scopul respectiv, acest lucru este prevăzut în mod explicit în norma suplimentară (3).

- (54) În ceea ce privește obligația de a păstra datele exacte și actualizate, articolul 19 din APPI prevede obligația operatorului economic care gestionează informații cu caracter personal de a „depune eforturi pentru a păstra datele cu caracter personal exacte și actualizate în domeniul de aplicare necesar pentru a atinge scopul utilizării”. Această dispoziție ar trebui citită împreună cu articolul 16 alineatul (1) din APPI: conform explicațiilor primite din partea PPC, în cazul în care un operator economic care gestionează informații cu caracter personal nu îndeplinește standardele de acuratețe prevăzute, prelucrarea informațiilor cu caracter personal nu va fi considerată ca îndeplinind scopul de utilizare și, prin urmare, gestionarea acestora va deveni ilegală în temeiul articolului 16 alineatul (1).

2.3.4. Limitarea stocării

- (55) În principiu, datele nu ar trebui să fie păstrate pentru o perioadă mai îndelungată decât este necesar în vederea atingerii scopurilor în care sunt prelucrate datele cu caracter personal.
- (56) În conformitate cu articolul 19 din APPI, operatorii economici care gestionează informații cu caracter personal au obligația de a „depune eforturi [...] pentru a șterge fără întârziere datele cu caracter personal atunci când o astfel de utilizare a devenit inutilă”. Această dispoziție trebuie interpretată în coroborare cu articolul 16 alineatul (1) din APPI, care interzice gestionarea informațiilor cu caracter personal dincolo de „domeniul de aplicare necesar pentru a atinge un scop de utilizare”. Odată ce scopul utilizării a fost atins, prelucrarea informațiilor cu caracter personal nu mai poate fi considerată necesară și, prin urmare, nu poate continua (cu excepția cazului în care operatorul economic care gestionează informații cu caracter personal obține în acest sens consimțământul persoanei vizate).

2.3.5. Securitatea datelor

- (57) Datele cu caracter personal ar trebui prelucrate într-un mod care să le asigure securitatea, inclusiv protecția împotriva prelucrării neautorizate sau ilegale și împotriva pierderii, a distrugerii sau a deteriorării accidentale. În acest scop, operatorii economici ar trebui să ia măsurile tehnice sau organizatorice adecvate pentru a proteja datele cu caracter personal împotriva eventualelor amenințări. Aceste măsuri ar trebui să fie evaluate luând în considerare cunoștințele actuale și costurile aferente.
- (58) Acest principiu este pus în aplicare în legislația japoneză prin articolul 20 din APPI, care prevede ca un operator economic ce gestionează informații cu caracter personal „să ia măsurile necesare și adecvate pentru controlul securității datelor cu caracter personal, inclusiv pentru prevenirea scurgerii, pierderii sau deteriorării datelor sale cu caracter personal pe care le gestionează.” Orientările PPC explică măsurile care trebuie luate, inclusiv metodele de stabilire a politicilor de bază, a normelor de gestionare a datelor și a diferitelor „acțiuni de control” (în ceea ce privește siguranța organizațională, precum și securitatea umană, fizică și tehnologică) ⁽³⁵⁾. În plus, orientările PPC și o comunicare specifică (apendicele 8 privind „conținutul măsurilor de gestionare a siguranței care trebuie luate”), publicate de PPC, furnizează mai multe detalii privind măsurile referitoare la incidentele de securitate care implică, de exemplu, scurgerile de informații cu caracter personal, ca parte a măsurilor de gestionare a securității ce urmează să fie luate de către operatorii economici care gestionează informații cu caracter personal ⁽³⁶⁾.
- (59) În plus, ori de câte ori angajații sau subcontractanții gestionează informații cu caracter personal, trebuie să se asigure „supravegherea necesară și corespunzătoare” în conformitate cu articolele 20 și 21 din APPI în ceea ce privește controlul de securitate. În fine, în conformitate cu articolul 83 din APPI, scurgerea intenționată sau furtul de informații cu caracter personal este pasibil de o sancțiune de până la un an de închisoare.

2.3.6. Transparență

- (60) Persoanele vizate ar trebui să fie informate cu privire la principalele caracteristici ale prelucrării datelor lor cu caracter personal.
- (61) Articolul 18 alineatul (1) din APPI prevede că operatorul economic care gestionează informații cu caracter personal are obligația de a informa persoana vizată cu privire la scopul utilizării informațiilor cu caracter personal disponibile, cu excepția „cazurilor în care un scop de utilizare a fost divulgat în prealabil publicului”. Aceeași obligație se aplică în cazul unei modificări admisibile a scopului [articolul 18 alineatul (3)]. Se garantează astfel că persoana vizată este informată cu privire la faptul că datele sale au fost colectate. Cu toate că APPI nu solicită, în general, operatorului economic care gestionează informații cu caracter personal să informeze persoana vizată cu privire la destinarii prevăzuți ai informațiilor cu caracter personal în etapa colectării, aceste informații reprezintă o condiție necesară pentru orice divulgare ulterioară de informații către o parte terță (destinatar) în temeiul articolului 23 alineatul (2), prin urmare, în cazul în care acest lucru se realizează fără consimțământul prealabil al persoanei vizate.

⁽³⁵⁾ Orientările PPC (Ediția cu normele generale), p. 41 și p. 86-98.

⁽³⁶⁾ În conformitate cu secțiunea 3-3-2 din orientările PPC, în cazul unor astfel de scurgeri, daune sau pierderi, operatorul economic care gestionează informații cu caracter personal are obligația de a efectua investigațiile necesare și, în special, de a evalua amploarea încălcării drepturilor și a intereselor persoanei fizice respective, precum și natura și cantitatea de informații cu caracter personal în cauză.

- (62) În ceea ce privește „datele cu caracter personal păstrate”, articolul 27 din APPI prevede că operatorul economic care gestionează informații cu caracter personal informează persoana vizată cu privire la identitatea sa (detaliile de contact), la scopul utilizării și la procedurile de răspuns la o cerere privind drepturile individuale ale persoanei vizate în temeiul articolelor 28, 29 și 30 din APPI.
- (63) În conformitate cu normele suplimentare, datele cu caracter personal transferate din Uniunea Europeană vor fi considerate „date cu caracter personal păstrate”, indiferent de perioada lor de păstrare (cu excepția cazului în care acestea fac obiectul unor derogări); acestea vor fi întotdeauna supuse cerințelor de transparență prevăzute în ambele dispoziții menționate anterior.
- (64) Atât cerințele articolului 18, cât și obligația de a informa cu privire la scopul utilizării, în conformitate cu articolul 27 din APPI sunt supuse aceluiași set de derogări, bazate în principal pe considerente de interes public și pe protecția drepturilor și a intereselor persoanei vizate, ale părților terțe și ale operatorului ⁽³⁷⁾. În conformitate cu interpretarea formulată în orientările PPC, aceste excepții se aplică în situații foarte specifice, cum ar fi cazurile în care informațiile privind scopul utilizării ar risca să submineze măsurile legitime luate de operatorul economic pentru a proteja anumite interese (de exemplu, lupta împotriva fraudei, spionajului industrial, sabotajului).

2.3.7. Categorii speciale de date

- (65) Ar trebui să existe garanții specifice în cazul în care sunt prelucrate „categorii speciale de date”.
- (66) „Informațiile cu caracter personal care implică o atenție specială” sunt definite la articolul 2 alineatul (3) din APPI. Dispoziția menționată anterior se referă la „informații cu caracter personal care conțin rasa, crezul, statutul social, istoricul medical, cazierul judiciar, prejudiciile suferite în urma unei infracțiuni sau alte descrieri etc. ale persoanei principale, prevăzute în Ordinul Cabinetului ca fiind cele a căror gestionare necesită o atenție specială, pentru a nu cauza discriminare injustă, prejudecăți sau alte dezavantaje pentru persoana principală”. Aceste categorii corespund în mare parte listei de date sensibile în temeiul articolelor 9 și 10 din Regulamentul (UE) 2016/679. În special, „istoricul medical” corespunde datelor medicale, iar „cazierul judiciar și prejudiciile suferite în urma unei infracțiuni” sunt în esență aceleași ca și categoriile menționate la articolul 10 din Regulamentul (UE) 2016/679. Categoriile menționate la articolul 2 alineatul (3) din APPI sunt supuse unei interpretări ulterioare în Ordinul Cabinetului și în orientările PPC. În conformitate cu secțiunea 2.3 punctul (8) din orientările PPC, subcategoriile de „istoric medical” detaliate la articolul 2 punctele (ii) și (iii) din Ordinul Cabinetului sunt interpretate ca incluzând date genetice și biometrice. De asemenea, deși lista nu include în mod expres termenii „origine etnică” și „opinie politică”, aceasta cuprinde trimiteri la „rasă” și „crez”. Astfel cum s-a explicat în secțiunea 2.3 punctele 1 și 2 din orientările PPC, trimiterea la „rasă” include „legăturile etnice sau legăturile cu o anumită parte a lumii”, iar prin „crez” se înțeleg atât opiniile religioase, cât și cele politice.
- (67) Astfel cum reiese în mod clar din formularea dispoziției, aceasta nu este o listă închisă, întrucât alte categorii de date pot fi adăugate în măsura în care prelucrarea lor creează un risc de „discriminare injustă, prejudecăți sau alte dezavantaje pentru persoana principală”.
- (68) Deși conceptul de date „sensibile” este inherent o construcție socială în sensul că se bazează pe tradițiile culturale și juridice, pe considerentele de ordin moral și pe opțiunile de politică etc. ale unei anumite societăți, având în vedere importanța furnizării unor garanții adecvate pentru datele sensibile atunci când sunt transferate către operatorii economici din Japonia, Comisia a obținut ca protecția specială acordată „informațiilor cu caracter personal care necesită o atenție specială” în temeiul dreptului japonez să fie extinsă la toate categoriile recunoscute ca „date sensibile” în Regulamentul (UE) 2016/679. În acest scop, norma suplimentară (1) prevede că datele transferate din Uniunea Europeană privind viața sexuală, orientarea sexuală sau apartenența la un sindicat a unei persoane fizice se prelucrează de către operatorii economici care gestionează informații cu caracter personal „în același mod ca informațiile cu caracter personal care necesită o atenție specială în sensul articolului 2 alineatul (3) din [APPI]”.

⁽³⁷⁾ Acestea sunt: (i) cazuri în care există posibilitatea ca informarea persoanei vizate cu privire la scopul utilizării sau pentru a face publice datele ar „dăuna vieții, integrității fizice, bunurilor sau altor drepturi și interese ale unei persoane principale sau ale unei părți terțe” ori „drepturilor sau intereselor legitime ale [...] operatorului economic care gestionează informații cu caracter personal”; (ii) cazuri în care „este necesar să se coopereze cu o organizație guvernamentală centrală sau cu o administrație locală” în îndeplinirea sarcinilor statutare ale acestora și dacă astfel de informații sau divulgarea ar interfera cu asemenea „chestiuni”; (iii) cazurile în care scopul utilizării este clar, în funcție de situația în care au fost obținute datele.

- (69) În ceea ce privește garanțiile materiale suplimentare care se aplică în cazul informațiilor cu caracter personal ce necesită o atenție specială, în conformitate cu articolul 17 alineatul (2) din APPI, operatorii economici care gestionează informații cu caracter personal nu sunt autorizați să achiziționeze astfel de date fără consimțământul prealabil al persoanei fizice în cauză, fiind supuși doar unor excepții limitate⁽³⁸⁾. În plus, această categorie de informații cu caracter personal este exclusă de la posibilitatea unei divulgări către părți terțe pe baza procedurii prevăzute la articolul 23 alineatul (2) din APPI (care permite transmiterea datelor către părți terțe fără consimțământul prealabil al persoanei în cauză).

2.3.8. Responsabilitate

- (70) Conform principiului responsabilității, entităților care prelucreează date li se solicită să pună în aplicare măsuri tehnice și organizatorice adecvate pentru a-și respecta în mod efectiv obligațiile în materie de protecție a datelor și pentru a putea demonstra această conformitate, în special autorității de supraveghere competente.
- (71) Astfel cum s-a menționat în nota de subsol 34 (considerentul 49), operatorii economici care gestionează informații cu caracter personal sunt obligați, în conformitate cu articolul 26 alineatul (1) din APPI, să verifice identitatea părții terțe care le furnizează date cu caracter personal și „circumstanțele” în care aceste date au fost dobândite de partea terță [în cazul datelor cu caracter personal reglementate de prezenta decizie, în conformitate cu APPI și cu norma suplimentară (3), printre aceste circumstanțe se numără faptul că datele provin din Uniunea Europeană, precum și scopul transferului inițial de date]. Printre altele, această măsură vizează asigurarea legalității prelucrării datelor de-a lungul întregului lanț de gestionare a datelor cu caracter personal de către operatorii economici care gestionează informații cu caracter personal. În plus, în temeiul articolului 26 alineatul (3) din APPI, operatorii economici care gestionează informații cu caracter personal au obligația de a ține o evidență a datei de primire și a informațiilor (obligatorii) primite de la partea terță în temeiul alineatului (1), precum și a numelui persoanei în cauză (al persoanei vizate), a categoriilor de date prelucrate și, în măsura în care este relevant, a faptului că persoana vizată și-a dat consimțământul pentru partajarea datelor sale cu caracter personal. Astfel cum se prevede la articolul 18 din normele PPC, aceste evidențe trebuie păstrate pentru o perioadă de cel puțin unu până la trei ani, în funcție de circumstanțe. În exercitarea atribuțiilor sale, PPC poate solicita prezentarea unor astfel de evidențe⁽³⁹⁾.
- (72) Operatorii economici care gestionează informații cu caracter personal trebuie să trateze cu promptitudine și în mod corespunzător plângerile primite de la persoanele vizate cu privire la prelucrarea informațiilor lor cu caracter personal. Pentru a facilita tratarea plângerilor, aceștia stabilesc un „sistem necesar pentru atingerea scopului [în cauză]”, ceea ce înseamnă că ar trebui să instituie proceduri adecvate în cadrul organizației lor (de exemplu, să atribuie responsabilități sau să pună la dispoziție un punct de contact).
- (73) În cele din urmă, APPI creează un cadru pentru participarea organizațiilor sectoriale la asigurarea unui nivel ridicat de conformitate (a se vedea capitolul IV secțiunea 4). Rolul unor astfel de organizații acreditate de protecție a informațiilor cu caracter personal⁽⁴⁰⁾ este de a promova protecția acestor informații prin sprijinirea întreprinderilor prin expertiza lor, dar și de a contribui la punerea în aplicare a garanțiilor, în special prin tratarea plângerilor individuale și prin contribuția la soluționarea conflictelor legate de acestea. În acest scop, ele pot solicita, după caz, operatorilor economici participanți care gestionează informații cu caracter personal să adopte măsurile necesare⁽⁴¹⁾. În plus, în cazul încălcării securității datelor sau al altor incidente de securitate, operatorii economici care gestionează informații cu caracter personal informează, în principiu, PPC, precum și persoana vizată (sau publicul larg) și iau măsurile necesare, inclusiv măsuri pentru a reduce la minimum orice daune și pentru a preveni repetarea unor incidente similare⁽⁴²⁾. Deși acestea sunt sisteme voluntare, la 10 august 2017, PPC a întocmit o listă cu 44 de organizații, dintre care cea mai mare, Centrul pentru prelucrarea și dezvoltarea informațiilor din

⁽³⁸⁾ Excepțiile sunt următoarele: (i) „cazurile bazate pe acte cu putere de lege și norme administrative”; (ii) „cazurile în care este necesar să se protejeze viața, integritatea fizică sau bunurile unei persoane și cele în care este dificil să se obțină consimțământul persoanei principale”; (iii) „cazurile în care există o nevoie specială să se îmbunătățească igiena publică sau să se încurajeze creșterea de copii sănătoși și în care este dificil să se obțină consimțământul persoanei principale”; (iv) „cazurile în care este necesar să se coopereze cu o organizație guvernamentală centrală sau cu o administrație locală ori o persoană căreia acestea îi încredințează activități prevăzute în acte cu putere de lege și norme administrative și atunci când există posibilitatea ca obținerea consimțământului persoanei principale să interfereze cu desfășurarea activităților în cauză” și (v) cazurile în care informațiile cu caracter personal ce necesită o atenție specială sunt comunicate publicului de către o persoană vizată, o organizație guvernamentală, o administrație locală, o persoană care se încadrează într-una din categoriile prevăzute la articolul 76 alineatul (1) sau de către alte persoane prevăzute în normele PPC. O altă categorie se referă „alte cazuri prevăzute în Ordinul Cabinetului ca fiind echivalente cu cele menționate la fiecare element precedent” și, în conformitate cu actualul ordin al Cabinetului, se referă în special la caracteristicile clare ale unei persoane (de exemplu, o problemă de sănătate vizibilă) dacă datele sensibile au fost obținute (neintenționat) prin observarea vizuală, filmarea sau fotografierea persoanei vizate, de exemplu prin camere CCTV.

⁽³⁹⁾ În conformitate cu articolul 40 alineatul (1) din APPI, PPC poate, în măsura în care este necesar pentru punerea în aplicare a dispozițiilor relevante din APPI, să solicite unui operator economic care gestionează informații cu caracter personal să prezinte informațiile sau materialele necesare privind prelucrarea informațiilor cu caracter personal.

⁽⁴⁰⁾ APPI prevede, printre altele, norme privind acreditarea unor astfel de organizații; a se vedea articolele 47-50 din APPI.

⁽⁴¹⁾ Articolul 52 din APPI.

⁽⁴²⁾ Notificarea nr. 1/2017 a PPC privind măsurile care trebuie luate în astfel de cazuri în care a avut loc o încălcare a securității datelor cu caracter personal sau un alt incident.

Japonia (*Japan Information Processing and Development Center – JIPDEC*), reprezintă 15 436 de operatori economici participanți ⁽⁴³⁾. Printre sistemele acreditate se numără asociații sectoriale cum ar fi Asociația japoneză a dealerilor de titluri de valoare, Asociația japoneză a școlilor de șoferi sau Asociația organizatorilor de nunți ⁽⁴⁴⁾.

- (74) Organizațiile acreditate de protecție a informațiilor cu caracter personal prezintă rapoarte anuale cu privire la operațiunile lor. Conform documentului „Prezentare generală a stadiului punerii în aplicare a APPI în exercițiul financiar 2015”, publicat de PPC, organizațiile acreditate de protecție a informațiilor cu caracter personal au primit în total 442 de plângeri, au solicitat 123 de explicații din partea operatorilor economici aflați în jurisdicția lor, au solicitat documente de la acești operatori în 41 de cazuri, au oferit 181 de instrucțiuni și au formulat două recomandări ⁽⁴⁵⁾.

2.3.9. Restricții privind transferurile ulterioare de date

- (75) Nivelul de protecție oferit datelor cu caracter personal transferate din Uniunea Europeană către operatori economici din Japonia nu trebuie să fie subminat de transferul suplimentar al acestor date către destinatari dintr-o altă țară terță decât Japonia. Astfel de „transferuri ulterioare”, care, din perspectiva operatorului economic din Japonia, constituie transferuri internaționale din Japonia, ar trebui să fie permise numai în cazul în care destinatarul suplimentar din afara Japoniei intră el însuși sub incidența unor norme care asigură un nivel de protecție similar cu cel garantat în cadrul ordinii juridice japoneze.
- (76) O primă protecție este consacrată la articolul 24 din APPI, care interzice, în general, transferul de date cu caracter personal către o parte terță din afara teritoriului Japoniei fără acordul prealabil al persoanei în cauză. Norma suplimentară (4) garantează că, în cazul transferurilor de date din Uniunea Europeană, acest consimțământ va fi acordat în plină cunoștință de cauză, întrucât impune ca persoanei în cauză să îi fie „furnizate informații privind circumstanțele transferului necesare astfel încât persoana principală să ia o decizie cu privire la consimțământul său”. Având în vedere aceste elemente, persoana vizată va fi informată cu privire la faptul că datele vor fi transferate în străinătate (în afara domeniului de aplicare a APPI) și cu privire la țara de destinație specifică. Acest lucru îi va permite să evalueze riscul pe care îl implică transferul pentru respectarea vieții private. De asemenea, astfel cum se poate deduce din articolul 23 din APPI (a se vedea considerentul 47), informațiile furnizate persoanei principale ar trebui să cuprindă elementele obligatorii menționate la alineatul (2), și anume categoriile de date cu caracter personal furnizate unei părți terțe și metoda de divulgare.
- (77) Articolul 24 din APPI, aplicat împreună cu articolul 11 alineatul (2) din normele PPC, prevede câteva excepții de la această normă bazată pe consimțământ. În plus, în temeiul articolului 24, aceleași derogări precum cele aplicabile în conformitate cu articolul 23 alineatul (1) din APPI se aplică și transferurilor internaționale de date ⁽⁴⁶⁾.
- (78) Pentru a asigura continuitatea protecției în cazul datelor cu caracter personal transferate din Uniunea Europeană în Japonia în temeiul prezentei decizii, norma suplimentară (4) sporește nivelul de protecție pentru transferurile ulterioare de astfel de date de către operatorul economic care gestionează informații cu caracter personal către un destinatar din țara terță. Acest lucru se realizează prin limitarea și definirea bazelor pentru transferurile internaționale care pot fi utilizate de către operatorul economic care gestionează informații cu caracter personal ca alternativă la consimțământ. Mai precis și fără a aduce atingere derogărilor prevăzute la articolul 23 alineatul (1) din APPI, datele cu caracter personal transferate în temeiul prezentei decizii nu pot face obiectul transferurilor (ulterioare) fără consimțământ decât în două cazuri: (i) în cazul în care datele sunt transmise unei țări terțe care a fost recunoscută de PPC în temeiul articolului 24 din APPI ca oferind un nivel de protecție echivalent celui garantat în Japonia ⁽⁴⁷⁾; sau (ii) în cazul în care operatorul economic care gestionează informații cu caracter personal și partea terță destinatară au pus în aplicare împreună măsuri de asigurare a unui nivel de protecție echivalent cu cel prevăzut în APPI, lege coroborată cu normele suplimentare, prin intermediul unui contract, al altor forme de acorduri obligatorii sau al unor acorduri obligatorii în cadrul unui grup de întreprinderi. A doua categorie corespunde instrumentelor utilizate în temeiul Regulamentului (UE) 2016/679 pentru a se asigura garanții adecvate (în special, clauze contractuale și reguli corporatiste obligatorii). În plus, astfel cum a fost confirmat de către PPC, chiar și în aceste cazuri, transferul rămâne sub incidența normelor generale aplicabile oricărei furnizări de date cu caracter personal către o parte terță în conformitate cu APPI [adică sub incidența cerinței de obținere a consimțământului în temeiul articolului 23 alineatul (1) sau, alternativ, sub incidența cerinței privind informațiile, cu posibilitatea de a opta pentru neparticipare în temeiul articolului 23 alineatul (2) din APPI]. În cazul în care nu

⁽⁴³⁾ Potrivit cifrelor publicate pe site-ul PrivacyMark al JIPDEC, din 2 octombrie 2017.

⁽⁴⁴⁾ PPC, Lista organizațiilor acreditate de protecție a informațiilor cu caracter personal, disponibilă pe internet la adresa: <https://www.ppc.go.jp/personal/nintei/list/> sau https://www.ppc.go.jp/files/pdf/nintei_list.pdf

⁽⁴⁵⁾ PPC, Prezentare generală a stadiului punerii în aplicare a APPI în exercițiul financiar 2015 (octombrie 2016), disponibilă (numai în limba japoneză) pe internet la adresa: https://www.ppc.go.jp/files/pdf/personal_sekougaiyou_27ppc.pdf

⁽⁴⁶⁾ A se vedea nota de subsol 32.

⁽⁴⁷⁾ În conformitate cu articolul 11 din normele PPC, acest lucru necesită nu numai standarde materiale echivalente cu cele prevăzute în APPI care să fie supravegheate în mod eficace de o autoritate independentă de asigurare a respectării legii, ci și să se asigure punerea în aplicare a normelor relevante în țara terță.

este posibil ca persoanei vizate să i se transmită o cerere de consimțământ sau o cerere de comunicare a informațiilor prealabile solicitate în conformitate cu articolul 23 alineatul (2) din APPI, transferul nu poate avea loc.

- (79) Prin urmare, în afara cazurilor în care PPC a constatat că țara terță în cauză asigură un nivel de protecție echivalent cu cel garantat de către APPI ⁽⁴⁸⁾, cerințele prevăzute în norma suplimentară (4) exclud utilizarea unor instrumente de transfer care nu creează o relație obligatorie între exportatorul de date din Japonia și importatorul de date din țara terță și care nu garantează nivelul de protecție cerut. Acesta va fi cazul, de exemplu, al Sistemului de norme transfrontaliere privind protecția vieții private (CBPR) din cadrul APEC, la care Japonia este o economie participantă ⁽⁴⁹⁾, întrucât, în acest sistem, măsurile de protecție nu rezultă dintr-un acord care obligă exportatorul și importatorul în contextul relației lor bilaterale și sunt, în mod evident, la un nivel mai scăzut decât cel garantat de combinația dintre APPI și normele suplimentare ⁽⁵⁰⁾.
- (80) În cele din urmă, o garanție suplimentară în cazul transferurilor (ulterioare) rezultă din articolele 20 și 22 din APPI. În conformitate cu aceste dispoziții, în cazul în care un operator dintr-o țară terță (importator de date) acționează în numele operatorului economic care gestionează informații cu caracter personal (exportator de date), și anume în calitate de (subcontractant), acesta din urmă trebuie să asigure supravegherea celui dintâi în ceea ce privește securitatea prelucrării datelor.

2.3.10. Drepturi individuale

- (81) La fel ca legislația UE privind protecția datelor, APPI le acordă persoanelor fizice o serie de drepturi garantate. Printre acestea se numără dreptul de acces („divulgare”), rectificarea și ștergerea, precum și dreptul la opoziție („încetarea utilizării”).
- (82) În primul rând, în temeiul articolului 28 alineatele (1) și (2) din APPI, o persoană vizată are dreptul de a solicita unui operator economic care gestionează informații cu caracter personal să „divulge date cu caracter personal păstrate care îl pot identifica” și, la primirea unei astfel de cereri, operatorul respectiv „comunică datele cu caracter personal păstrate” persoanei vizate. Articolele 29 (dreptul de rectificare) și 30 (dreptul la încetarea utilizării) au aceeași structură ca articolul 28.
- (83) Articolul 9 din Ordinul Cabinetului precizează că divulgarea informațiilor cu caracter personal menționată la articolul 28 alineatul (2) din APPI se face în scris, cu excepția cazului în care operatorul economic care gestionează informații cu caracter personal și persoana vizată au convenit altfel.
- (84) Aceste drepturi fac obiectul a trei tipuri de restricții, referitoare la drepturile și interesele individuale ale persoanei sau ale părților terțe ⁽⁵¹⁾, la afectarea gravă a operațiunilor comerciale ale operatorului economic care gestionează informații cu caracter personal ⁽⁵²⁾, precum și la cazurile în care divulgarea ar încălca alte acte cu putere de lege sau norme administrative ⁽⁵³⁾. Situațiile în care s-ar aplica aceste restricții sunt similare cu unele dintre excepțiile aplicabile în temeiul articolului 23 alineatul (1) din Regulamentul (UE) 2016/679, care permite limitarea drepturilor persoanelor din motive legate de „protecția persoanei vizate sau a drepturilor și libertăților altora” sau de „alte obiective importante de interes public general”. Deși categoria de cazuri în care divulgarea ar încălca „alte acte cu

⁽⁴⁸⁾ Până în prezent, PPC nu a adoptat nicio decizie în temeiul articolului 24 din APPI prin care să recunoască faptul că o țară terță oferă un nivel de protecție echivalent celui garantat în Japonia. Singura decizie pe care o analizează în prezent în vederea adoptării se referă la SEE. În ceea ce privește alte decizii posibile în viitor, Comisia va monitoriza îndeaproape situația și, dacă este necesar, va lua măsurile adecvate pentru a aborda posibilele efecte negative asupra continuității protecției [a se vedea mai jos, considerentele 176, 177, 184 și articolul 3 alineatul (1)].

⁽⁴⁹⁾ Deși numai două societăți japoneze sunt certificate în conformitate cu sistemul CBPR al APEC (a se vedea https://english.jipdec.or.jp/sp/protection_org/cbpr/list.html). În afara Japoniei, singurii operatori economici certificați în conformitate cu acest sistem sunt un număr restrâns (23) de societăți din SUA (a se vedea <https://www.trustarc.com/consumer-resources/trusted-directory/#apec-list>).

⁽⁵⁰⁾ De exemplu, nicio definiție și nicio protecție specifică a datelor sensibile, nicio obligație de păstrare limitată a datelor. A se vedea, de asemenea, Avizul nr. 02/2014 al Grupului de lucru „Articolul 29” privind criteriile de referință referitoare la cerințele pentru regulile corporatiste obligatorii prezentate autorităților naționale de protecție a datelor din UE și pentru normele transfrontaliere privind protecția vieții private transmise către agenții de responsabilitate din cadrul CBPR al APEC, 6 martie 2014.

⁽⁵¹⁾ Conform PPC, numai astfel de interese pot justifica o restricție potrivit căreia acestea „merită să fie protejate legal”. Această evaluare trebuie efectuată de la caz la caz, „luând în considerare interferența cu dreptul fundamental la viață privată, inclusiv protecția datelor, astfel cum este recunoscută în Constituție și precedentele jurisprudențiale.” Printre interesele protejate se pot număra, de exemplu, comerțul sau alte secrete comerciale.

⁽⁵²⁾ Conceptul de „interferență gravă cu desfășurarea adecvată a activității operatorului” este ilustrat în orientările PPC prin diferite exemple, cum ar fi cererile complexe repetate și identice formulate de aceeași persoană, în cazul în care astfel de cereri implică, pentru operatorul economic, o sarcină semnificativă care ar putea compromite capacitatea acestuia de a răspunde altor cereri [Orientările PPC (Ediția cu normele generale), p. 62]. În termeni mai generali, PPC a confirmat că această categorie se limitează la cazuri excepționale care depășesc un simplu inconvenient. În special, un operator economic care gestionează informații cu caracter personal nu poate refuza divulgarea pur și simplu pentru că a fost solicitată o cantitate mare de date.

⁽⁵³⁾ După cum a confirmat PPC, aceste legi trebuie să respecte dreptul la viață privată, astfel cum este asigurat în Constituție și, prin urmare, „să reflecte o restricție necesară și rezonabilă”.

putere de lege sau norme administrative" poate părea generală, actele cu putere de lege sau normele administrative care prevăd limitări în această privință trebuie să respecte dreptul constituțional la viață privată și pot impune restricții numai în măsura în care exercitarea acestui drept ar „interferă cu bunăstarea publică”⁽⁵⁴⁾. Acest lucru necesită o echilibrare a intereselor în cauză.

- (85) În conformitate cu articolul 28 alineatul (3) din APPI, în cazul în care nu există date solicitate sau în cazul în care operatorul economic în cauză ce gestionează informații cu caracter personal decide să nu acorde acces la datele păstrate, este necesar ca persoana în cauză să fie informată fără întârziere.
- (86) În al doilea rând, în temeiul articolului 29 alineatele (1) și (2) din APPI, o persoană vizată are dreptul de a solicita rectificarea, adăugarea sau ștergerea datelor sale cu caracter personal păstrate, în cazul în care datele sunt inexacte. La primirea unei astfel de cereri, operatorul economic care gestionează informații cu caracter personal „efectuează [...] o investigație necesară” și, pe baza rezultatelor unei astfel de investigații, „face o rectificare etc. privind conținutul datelor păstrate”.
- (87) În al treilea rând, în temeiul articolului 30 alineatele (1) și (2) din APPI, o persoană vizată are dreptul de a solicita unui operator economic care gestionează informații cu caracter personal să întrerupă utilizarea acestui tip de informații sau să șteargă aceste informații, atunci când sunt tratate cu încălcarea articolului 16 (în ceea ce privește limitarea scopului) sau au fost dobândite în mod necorespunzător prin încălcarea articolului 17 din APPI (în ceea ce privește achiziția prin înșelăciune, alte mijloace necorespunzătoare sau, în cazul unor date sensibile, fără consimțământ). De asemenea, în conformitate cu articolul 30 alineatele (3) și (4) din APPI, persoana are dreptul de a solicita operatorului economic care gestionează informații cu caracter personal să înceteze furnizarea de informații unei părți terțe în cazul în care astfel s-ar încălca dispozițiile articolului 23 alineatul (1) sau ale articolului 24 din APPI (în ceea ce privește dispoziția referitoare la părțile terțe, inclusiv la transferurile internaționale).
- (88) Atunci când cererea este întemeiată, operatorul economic care gestionează informații cu caracter personal întrerupe fără întârziere utilizarea datelor sau transmiterea către o parte terță, în măsura necesară pentru a remedia încălcarea sau, în cazul în care situația respectivă face obiectul unei derogări (în special dacă încetarea utilizării ar cauza costuri deosebit de ridicate)⁽⁵⁵⁾, pune în aplicare măsurile alternative necesare pentru a proteja drepturile și interesele persoanei în cauză.
- (89) Spre deosebire de legislația UE, APPI și normele juridice de rang inferior relevante nu conțin dispoziții legale care să abordeze în mod specific posibilitatea de a se opune prelucrării în scopuri de marketing direct. Cu toate acestea, o astfel de prelucrare, în temeiul prezentei decizii, va avea loc în contextul unui transfer de date cu caracter personal care au fost colectate anterior în Uniunea Europeană. În conformitate cu articolul 21 alineatul (2) din Regulamentul (UE) 2016/679, persoana vizată are întotdeauna posibilitatea de a se opune unui transfer de date pentru a fi prelucrate în scopuri de marketing direct. În plus, astfel cum se explică în considerentul 43, în temeiul normei suplimentare (3), un operator economic care gestionează informații cu caracter personal este obligat să prelucreze datele primite în temeiul deciziei în același scop precum cel pentru care datele au fost transferate din Uniunea Europeană, cu excepția cazului în care persoana vizată consimte să modifice scopul utilizării. Prin urmare, în cazul în care transferul a fost efectuat în orice alt scop decât cel de marketing direct, unui operator economic din Japonia care gestionează informații cu caracter personal i se va interzice să prelucreze datele în scopul marketingului direct fără consimțământul persoanei vizate din UE.
- (90) În toate cazurile menționate la articolele 28 și 29 din APPI, operatorul economic care gestionează informații cu caracter personal are obligația de a informa persoana cu privire la rezultatul cererii sale fără întârziere și, în plus, trebuie să explice orice refuz (parțial) bazat pe excepțiile statutare prevăzute la articolele 27-30 (articolul 31 din APPI).

⁽⁵⁴⁾ Articolul 13 din Constituție a fost interpretat de Curtea Supremă ca oferind un drept la viață privată (a se vedea mai sus considerentele 7 și 8). Deși acest drept poate fi restricționat în cazurile în care „interferează cu bunăstarea publică”, în hotărârea sa din 6 martie 2008 (a se vedea considerentul 8), Curtea Supremă a precizat că orice restricție (care permite, în acest caz, unei autorități publice să colecteze și să prelucreze date cu caracter personal) trebuie să fie echilibrată în raport cu dreptul la viață privată, luând în considerare factori precum natura datelor în cauză, riscurile pe care le creează prelucrarea acestor date pentru persoanele fizice, garanțiile aplicabile și beneficiile de interes public rezultate din prelucrare. Acest lucru este foarte similar cu tipul de echilibrare impus de legislația UE, pe baza principiilor necesității și proporționalității, pentru autorizarea oricărei restricții asupra drepturilor și garanțiilor în materie de protecție a datelor.

⁽⁵⁵⁾ Pentru explicații suplimentare cu privire la aceste derogări, a se vedea comentariul articol cu articol al profesorului Katsuya Uga, referitor la Legea revizuită privind protecția informațiilor cu caracter personal, 2015, p. 217. De pildă, un exemplu de cerere care generează „cheltuieli foarte ridicate” este cazul în care numai unele nume aflate pe o listă lungă (de exemplu, într-o listă de abonați) sunt prelucrate cu încălcarea principiului limitării scopului, iar lista de abonați este deja în vânzare, ceea ce ar avea ca efect faptul că retragerea acestor exemplare și înlocuirea lor cu altele noi ar fi foarte costisitoare. În același exemplu, în cazul în care au fost deja vândute exemplare ale listei de abonați unui număr mare de persoane și este imposibil ca acestea să fie colectate în integralitate, ar fi, de asemenea, „difícil să se pună capăt unei utilizări”. În aceste scenarii, printre „măsurile alternative necesare” s-ar putea număra, de exemplu, publicarea sau distribuirea unei decizii de rectificare. O astfel de acțiune nu exclude alte forme de căi de atac (judiciare), pentru încălcarea drepturilor la viață privată, prejudiciile aduse reputației (calomnie) cauzate de publicarea sau încălcarea altor interese.

- (91) În ceea ce privește condițiile pentru depunerea unei cereri, articolul 32 din APPI (împreună cu Ordinul Cabinetului) permite operatorului economic care gestionează informații cu caracter personal să stabilească proceduri rezonabile, inclusiv în ceea ce privește informațiile necesare pentru identificarea datelor cu caracter personal păstrate. Cu toate acestea, în conformitate cu alineatul (4) din prezentul articol, operatorii economici care gestionează informații cu caracter personal nu trebuie să impună o „sarcină excesivă asupra unei persoane principale”. În anumite cazuri, operatorii respectivi pot impune taxe atât timp cât cuantumul acestora se înscrie „la un nivel considerat rezonabil în raport cu costurile actuale” (articolul 33 din APPI).
- (92) În cele din urmă, persoana poate obiecta față de furnizarea către o parte terță a informațiilor sale cu caracter personal, în conformitate cu articolul 23 alineatul (2) din APPI, sau poate refuza să își dea consimțământul în temeiul articolului 23 alineatul (1) (împiedicând astfel divulgarea în cazul în care nu ar fi disponibil niciun alt temei juridic). De asemenea, persoana în cauză poate opri prelucrarea datelor în alt scop, refuzând să își dea consimțământul în temeiul articolului 16 alineatul (1) din APPI.
- (93) Spre deosebire de legislația UE, APPI și normele juridice de rang inferior relevante nu conțin dispoziții generale care să abordeze chestiunea deciziilor care afectează persoana vizată și care se bazează exclusiv pe prelucrarea automată a datelor cu caracter personal. Cu toate acestea, chestiunea este abordată în anumite norme sectoriale aplicabile în Japonia care sunt deosebit de relevante pentru acest tip de prelucrare. Printre acestea se numără sectoarele în care întreprinderile recurg cel mai probabil la prelucrarea automată a datelor cu caracter personal pentru a lua decizii care afectează persoanele fizice (de exemplu, sectorul financiar). De exemplu, „Orientările generale pentru supravegherea băncilor importante”, astfel cum au fost revizuite în iunie 2017, prevăd ca persoanei în cauză să i se furnizeze explicații specifice privind motivele respingerii unei cereri de încheiere a unui acord de împrumut. Astfel, aceste norme oferă măsuri de protecție în ceea ce privește numărul probabil destul de limitat de cazuri în care deciziile automatizate ar fi luate de însoși operatorul economic „importator” din Japonia (mai degrabă decât de operatorul de date „exportator” din UE).
- (94) În orice caz, în ceea ce privește datele cu caracter personal care au fost colectate în Uniunea Europeană, orice decizie bazată pe prelucrarea automată va fi luată de regulă de către operatorul de date din Uniune (care are o relație directă cu persoana vizată în cauză) și, prin urmare, intră sub incidența Regulamentului (UE) 2016/679 ⁽⁵⁶⁾. Aceasta include scenarii de transfer în care prelucrarea este efectuată de un operator economic din străinătate (de exemplu, din Japonia) care acționează ca agent (operator) în numele operatorului din UE (sau în calitate de subcontractant care acționează în numele persoanei împuternicite de către operator din UE, care a primit datele de la un operator din UE care le-a colectat), care, pe această bază, ia decizia respectivă. Prin urmare, este puțin probabil ca lipsa din APPI a unor norme specifice privind procesul decizional automatizat să afecteze nivelul de protecție a datelor cu caracter personal transferate în temeiul prezentei decizii.

2.4. Supraveghere și asigurarea respectării normelor

2.4.1. Supravegherea independentă

- (95) Pentru a garanta și în practică un nivel adecvat de protecție a datelor, ar trebui instituită o autoritate de supraveghere independentă care să aibă competența de a monitoriza și de a asigura respectarea normelor de protecție a datelor. Această autoritate ar trebui să acționeze cu deplină independență și imparțialitate în îndeplinirea sarcinilor sale și în exercitarea competențelor sale.
- (96) În Japonia, autoritatea responsabilă cu monitorizarea și aplicarea APPI este PPC, care este compusă dintr-un președinte și opt comisari numiți de prim-ministru, cu acordul ambelor camere ale Dietei. Mandatul președintelui și al fiecăruia dintre comisari este de cinci ani, cu posibilitatea reînnoirii acestuia (articolul 64 din APPI). Comisarii pot fi demisi doar din motive întemeiate, într-o serie limitată de circumstanțe excepționale ⁽⁵⁷⁾ și nu trebuie să participe în mod activ la activități politice. În plus, în temeiul APPI, comisarii cu normă întreagă trebuie să se abțină de la orice alte activități remunerate sau de la activități economice. De asemenea, toți comisarii fac obiectul normelor interne care îi împiedică să participe la deliberări în cazul unui posibil conflict de interese. PPC este asistată de un secretariat, condus de un secretar general, care a fost înființat în scopul îndeplinirii sarcinilor atribuite PPC (articolul 70 din APPI). Atât comisarii, cât și toți funcționarii secretariatului sunt supuși unor norme stricte de confidențialitate (articolele 72 și 82 din APPI).

⁽⁵⁶⁾ În schimb, în cazul excepțional în care operatorul japonez are o relație directă cu persoana vizată din UE, aceasta va fi, de regulă, o consecință a faptului că se adresează persoanei din Uniunea Europeană prin oferirea de bunuri sau servicii ori prin monitorizarea comportamentului său. În acest scenariu, operatorul japonez se va încadra în domeniul de aplicare al Regulamentului (UE) 2016/679 [articolul 3 alineatul (2)] și, prin urmare, trebuie să respecte în mod direct legislația UE privind protecția datelor.

⁽⁵⁷⁾ În conformitate cu articolul 65 din APPI, concedierea împotriva voinței comisarului respectiv este posibilă numai din unul dintre următoarele motive: (i) deschiderea procedurii de faliment; (ii) condamnarea pentru încălcarea APPI sau a Legii privind utilizarea numerelor; (iii) condamnarea la o pedeapsă cu închisoarea fără regim de muncă sau la o pedeapsă și mai gravă; (iv) incapacitatea de a executa sarcini din cauza unei tulburări psihice sau fizice ori a unei abateri.

- (97) Competențele PPC, pe care autoritatea le exercită în deplină independență⁽⁵⁸⁾, sunt prevăzute, în principal, la articolele 40, 41 și 42 din APPI. În temeiul articolului 40, PPC poate solicita operatorilor economici care gestionează informații cu caracter personal să raporteze sau să transmită documente privind operațiunile de prelucrare și, de asemenea, poate să efectueze inspecții, atât la fața locului, cât și la nivelul cărților sau al altor documente. În măsura în care este necesar pentru a pune în aplicare APPI, PPC poate furniza, de asemenea, orientare sau consiliere operatorilor economici care gestionează informații cu caracter personal privind gestionarea acestui tip de informații. PPC a făcut deja uz de această competență în temeiul articolului 41 din APPI, emițând orientări adresate Facebook, în urma dezvăluirilor legate de Facebook/ Cambridge Analytica.
- (98) Cel mai important, PPC are competența – acționând în urma unei plângeri sau din proprie inițiativă – să emită recomandări și ordine pentru a asigura respectarea APPI și a altor norme obligatorii (inclusiv în ceea ce privește normele suplimentare), în cazuri individuale. Aceste competențe sunt prevăzute la articolul 42 din APPI. În timp ce alineatele (1) și (2) prevăd un mecanism în două etape prin care PPC poate emite un ordin (numai) ca urmare a unei recomandări prealabile, alineatul (3) permite adoptarea directă a unui ordin în cazuri de urgență.
- (99) Deși nu toate dispozițiile secțiunii 1 capitolul IV din APPI sunt enumerate la articolul 42 alineatul (1) – care stabilește, de asemenea, domeniul de aplicare al articolului 42 alineatul (2) – acest lucru poate fi explicat prin faptul că unele dintre dispozițiile respective nu se referă la obligațiile operatorului economic care gestionează informații cu caracter personal⁽⁵⁹⁾ și că toate măsurile de protecție esențiale sunt deja prevăzute de alte dispoziții care sunt incluse în lista respectivă. De exemplu, deși articolul 15 (care impune operatorului economic ce gestionează informații cu caracter personal să stabilească scopul și procesul de utilizare a informațiilor cu caracter personal relevante exclusiv în domeniul său de aplicare) nu este menționat, nerespectarea acestei cerințe poate constitui un temei pentru formularea unei recomandări bazate pe o încălcare a articolului 16 alineatul (1) (interdicția adresată operatorului economic care gestionează informații cu caracter personal de a prelucra astfel de informații dincolo de ceea ce este necesar pentru a atinge scopul utilizării, cu excepția cazului în care obține consimțământul persoanei vizate)⁽⁶⁰⁾. O altă dispoziție care nu este menționată la articolul 42 alineatul (1) este articolul 19 din APPI cu privire la exactitatea și păstrarea datelor. Nerespectarea acestei dispoziții poate fi consta într-o încălcare a articolului 16 alineatul (1), fie decurge dintr-o încălcare a articolului 29 alineatul (2), în cazul în care persoana în cauză solicită rectificarea sau ștergerea unor date eronate sau excesive, iar operatorul economic care gestionează informații cu caracter personal refuză să răspundă solicitării. În ceea ce privește drepturile persoanei vizate în conformitate cu articolul 28 alineatul (1), cu articolul 29 alineatul (1) și cu articolul 30 alineatul (1), supravegherea prin intermediul PPC este asigurată prin conferirea de competențe de executare în ceea ce privește obligațiile corespunzătoare prevăzute la articolele respective ce îi revin operatorului economic care gestionează informații cu caracter personal.
- (100) În temeiul articolului 42 alineatul (1) din APPI, PPC poate, atunci când recunoaște că există o „nevoie de protejare a drepturilor și intereselor unei persoane în cazurile în care un [operator economic care gestionează informații cu caracter personal] a încălcat” anumite dispoziții ale APPI, să emită o recomandare de a „suspenda acțiunea de încălcare sau de a lua alte măsuri necesare rectificării încălcării”. O astfel de recomandare nu este obligatorie, dar deschide calea pentru un ordin cu caracter obligatoriu în temeiul articolului 42 alineatul (2) din APPI. Pe baza acestei dispoziții, în cazul în care recomandarea nu este urmată de formularea „fără motive legitime”, iar PPC „recunoaște că este iminentă o încălcare gravă a drepturilor și intereselor unei persoane”, PPC poate cere operatorului economic care gestionează informații cu caracter personal să ia măsuri în conformitate cu recomandarea.
- (101) Normele suplimentare clarifică și consolidează în continuare competențele PPC de asigurare a respectării legii. Mai precis, în cazurile în care sunt implicate date importate din Uniunea Europeană, PPC va considera întotdeauna faptul că operatorul economic care gestionează informații cu caracter personal nu a adoptat, fără motive legitime, măsuri în vederea aplicării unei recomandări emise în baza APPI [articolul 42 alineatul (1)], ca o încălcare gravă a unui caracter iminent al drepturilor și intereselor unei persoane fizice în sensul articolului 42 alineatul (2) și, prin urmare, ca o încălcare care justifică emiterea unui ordin obligatoriu. În plus, ca un „motiv legitim” pentru nerespectarea unei recomandări, PPC va accepta doar „un eveniment de natură extraordinară [care împiedică asigurarea conformității] în afara controlului [operatorului economic ce gestionează informații cu caracter personal] care nu poate fi prevăzut în mod rezonabil (de exemplu, dezastre naturale)” sau cazurile în care necesitatea de a lua măsuri cu privire la o recomandare „a dispărut deoarece [operatorul economic ce gestionează informații cu caracter personal] a întreprins acțiuni alternative care remediază pe deplin încălcarea”.

⁽⁵⁸⁾ A se vedea articolul 62 din APPI.

⁽⁵⁹⁾ De exemplu, anumite dispoziții se referă la acțiunile operatorului economic ce gestionează informații cu caracter personal care sunt obligații opționale (articolele 32 și 33 din APPI) sau obligații privind „cele mai bune eforturi” care, ca atare, nu au caracter executiv [articolele 31 și 35, articolul 36 alineatul (6) și articolul 39 din APPI]. Anumite dispoziții nu se adresează operatorului economic care gestionează informații cu caracter personal, ci altor actori. Acesta este cazul, de exemplu, în ceea ce privește articolul 23 alineatul (4), articolul 26 alineatul (2) și articolul 34 din APPI [cu toate acestea, respectarea articolului 26 alineatul (2) din APPI este asigurată prin posibilitatea unor sancțiuni penale, în temeiul articolului 88 punctul (i) din APPI].

⁽⁶⁰⁾ În plus, astfel cum s-a explicat mai sus în considerentul 48, în contextul unui transfer, „scopul utilizării” va fi specificat de exportatorul de date din UE, care are această obligație în temeiul articolului 5 alineatul (1) litera (b) din Regulamentul (UE) 2016/679. Obligația respectivă trebuie respectată de către autoritatea pentru protecția datelor competentă din Uniunea Europeană.

- (102) Nerespectarea unui ordin al PPC este considerată infracțiune în temeiul articolului 84 din APPI, iar un operator economic ce gestionează informații cu caracter personal găsit vinovat poate fi pedepsit cu o pedeapsă privativă de libertate în regim de muncă de cel mult șase luni sau cu o amendă de maximum 300 000 de yen. În plus, în temeiul articolului 85 litera (i) din APPI, lipsa de cooperare cu PPC sau obstrucționarea investigațiilor sale se pedepsește cu amendă de până la 300 000 de yen. Aceste sancțiuni penale se aplică în plus față de cele care pot fi impuse pentru încălcări de fond ale APPI (a se vedea considerentul 108).

2.4.2. Căi de atac judiciare

- (103) Pentru a asigura o protecție adecvată și, în special, asigurarea respectării drepturilor individuale, persoanei vizate ar trebui să i se ofere căi de atac administrative și judiciare eficace, inclusiv despăgubiri pentru prejudiciile suferite.
- (104) Înainte sau în loc să urmeze o cale de atac administrativă sau judiciară, o persoană poate decide să înainteze operatorului însuși o plângere cu privire la prelucrarea datelor sale cu caracter personal. Pe baza articolului 35 din APPI, operatorii economici care gestionează informații cu caracter personal depun toate eforturile pentru a soluționa aceste plângeri „în mod adecvat și prompt” și pentru a institui sisteme interne de soluționare a plângerilor în vederea atingerii acestui obiectiv. În plus, în temeiul articolului 61 punctul (ii) din APPI, PPC este responsabilă cu „medierea necesară privind plângerile depuse și cu cooperarea oferită operatorului economic care se ocupă de plângerea respectivă”, în ambele cazuri, fiind incluse plângerile depuse de străini. În acest sens, legiuitorul japonez a încredințat totodată administrației centrale sarcina de a lua „măsurile necesare” pentru a permite și a facilita soluționarea plângerilor de către operatorii economici care gestionează informații cu caracter personal (articolul 9), iar administrațiile locale depun eforturi pentru a asigura medierea în astfel de cazuri (articolul 13). În acest sens, persoanele fizice pot depune o plângere la una dintre cele peste 1 700 de centre de protecție a consumatorilor înființate de administrațiile locale pe baza Legii privind siguranța consumatorilor ⁽⁶¹⁾, pe lângă posibilitatea de a depune o plângere la Centrul național pentru probleme de protecție a consumatorilor din Japonia. Astfel de plângeri pot fi, de asemenea, formulate cu privire la o încălcare a APPI. În temeiul articolului 19 din Legea de bază privind protecția consumatorilor ⁽⁶²⁾, autoritățile locale depun eforturi pentru a găsi soluții de mediere în ceea ce privește plângerile și pentru a le furniza părților expertiza necesară. Aceste mecanisme de soluționare a litigiilor par a fi destul de eficace, cu o rată de soluționare de 91,2 % în cazul a peste 75 000 de plângeri în 2015.
- (105) Încălcările dispozițiilor APPI de către un operator economic care gestionează informații cu caracter personal pot da naștere la acțiuni civile, precum și la proceduri și sancțiuni penale. În primul rând, în cazul în care consideră că drepturile sale în temeiul articolelor 28, 29 și 30 din APPI au fost încălcate, o persoană poate solicita instanței să emită o ordonanță președințială în care să solicite unui operator economic care gestionează informații cu caracter personal să răspundă cererii sale în temeiul uneia dintre aceste dispoziții, și anume să comunice datele cu caracter personal păstrate (articolul 28), să rectifice datele cu caracter personal păstrate care sunt incorecte (articolul 29) sau să înceteze prelucrarea ilegală sau furnizarea datelor către o parte terță (articolul 30). O astfel de acțiune poate fi introdusă fără a fi nevoie să se recurgă la articolul 709 din Codul civil ⁽⁶³⁾ sau la dreptul răspunderii civile ⁽⁶⁴⁾. În special, aceasta înseamnă că persoana nu trebuie să dovedească existența unui prejudiciu.
- (106) În al doilea rând, în cazul în care o presupusă încălcare nu vizează drepturile individuale în temeiul articolelor 28, 29 și 30, ci principiile generale de protecție a datelor sau obligațiile operatorului economic care gestionează informații cu caracter personal, persoana în cauză poate introduce o acțiune civilă împotriva operatorului economic, pe baza dispozițiilor privind răspunderea civilă delictuală prevăzute în Codul civil japonez, în special la articolul 709. În timp ce un proces în conformitate cu articolul 709 impune, pe lângă existența unei culpe (cu intenție sau din neglijență), demonstrarea unui prejudiciu, în conformitate cu articolul 710 din Codul civil, astfel de prejudicii pot fi atât materiale, cât și imateriale. Nu se impune nicio limitare cu privire la cuantumul compensației.
- (107) În ceea ce privește căile de atac disponibile, articolul 709 din Codul civil japonez se referă la compensarea bănească. Cu toate acestea, jurisprudența japoneză a interpretat acest articol ca oferind și dreptul de a obține o ordonanță președințială ⁽⁶⁵⁾. Prin urmare, în cazul în care o persoană vizată introduce o acțiune în temeiul articolului 709 din Codul civil și susține că drepturile sau interesele sale au fost lezate de o încălcare a unei dispoziții APPI de către persoana chemată în judecată, această cerere poate include, pe lângă despăgubirile pentru prejudiciile cauzate, o cerere de ordonanță președințială, vizând în special încetarea oricărei prelucrări ilegale.

⁽⁶¹⁾ Legea nr. 50 din 5 iunie 2009.

⁽⁶²⁾ Legea nr. 60 din 22 august 2012.

⁽⁶³⁾ Articolul 709 din Codul civil reprezintă principalul fundament pentru soluționarea litigiilor în materie civilă. În conformitate cu această dispoziție, „o persoană care a încălcat, în mod intenționat sau din neglijență, orice drept al altor persoane ori alte interese protejate din punct de vedere legal ale altora este obligată să ofere despăgubiri pentru orice daune care rezultă în consecință”.

⁽⁶⁴⁾ Înalta Curte din Tokyo, hotărârea din 20 mai 2015 (nepublicată); Tribunalul districtual din Tokyo, hotărârea din 8 septembrie 2014, Westlaw Japan 2014WLJPCA09088002. A se vedea articolul 34 alineatele (1) și (3) din APPI.

⁽⁶⁵⁾ A se vedea hotărârea Curții Supreme din 24 septembrie 2002 (Hanrei Times vol. 1106, p. 72).

- (108) În al treilea rând, în afară de căile de atac de drept civil (răspunderea civilă), persoana vizată poate adresa o plângere unui procuror sau unui agent al poliției judiciare cu privire la încălcările APPI, plângere care poate duce la sancțiuni penale. Capitolul VII din APPI conține o serie de dispoziții penale. Cea mai importantă dispoziție de acest fel (articolul 84) se referă la nerespectarea de către operatorul economic care gestionează informații cu caracter personal a ordinelor emise de PPC în temeiul articolului 42 alineatele (2) și (3). În cazul în care un operator economic nu respectă un ordin emis de PPC, președintele PPC (precum și orice alt funcționar public) ⁽⁶⁶⁾ poate transmite cazul către parchet sau către un agent al poliției judiciare și declanșa astfel deschiderea unei proceduri penale. Încălcarea unui ordin al PPC se pedepsește cu pedepse privative de libertate în regim de muncă cu durată de cel mult șase luni sau cu o amendă care se poate ridica la 300 000 de yeni. Printre celelalte dispoziții ale APPI care prevăd sancțiuni în cazul unor încălcări ale APPI care afectează drepturile și interesele persoanelor vizate se numără articolul 83 din APPI (referitor la „furnizarea sau utilizarea deturnată” a unei baze de date cu informații personale „în scopul de a încerca obținerea [...] de profituri ilegale”) și articolul 88 litera (i) din APPI [referitor la nerespectarea de către o parte terță a obligației de a informa în mod corect operatorul economic care gestionează informații cu caracter personal atunci când acesta din urmă primește date cu caracter personal în conformitate cu articolul 26 alineatul (1) din APPI, în special cu privire la detaliile achiziționării anterioare de către partea terță a acestor date]. Sancțiunile aplicabile pentru acest tip de încălcări ale APPI sunt, respectiv, pedeapsa cu închisoarea în regim de muncă pentru o perioadă maximă de un an sau o amendă care se poate ridica la 500 000 de yeni (în cazul încălcării articolului 83) sau o amendă administrativă care se poate ridica la 100 000 de yeni [în cazul încălcării articolului 88 litera (i)]. Deși este foarte probabil ca amenințarea cu aplicarea de sancțiuni penale să aibă deja un puternic efect de descurajare atât asupra organelor de conducere ale întreprinderii care coordonează operațiunile de prelucrare ale operatorilor economici care gestionează informații cu caracter personal, cât și asupra persoanelor care gestionează datele, în articolul 87 din APPI se precizează că, atunci când un reprezentant, un angajat sau un alt lucrător al unei persoane juridice a comis o încălcare în temeiul articolelor 83-85 din APPI, „actorul respectiv este pedepsit, iar persoanei juridice în cauză i se impune o amendă prevăzută la articolele respective”. În acest caz, atât angajatului, cât și societății li se pot aplica sancțiuni în limita sumei integrale maxime.
- (109) În cele din urmă, persoanele fizice pot, de asemenea, introduce căi de atac împotriva acțiunilor PPC sau împotriva inacțiunii PPC. În acest sens, legislația japoneză prevede mai multe căi de atac administrative și judiciare.
- (110) În cazul în care o persoană nu este mulțumită de o acțiune întreprinsă de PPC, aceasta poate introduce o cale de atac administrativă în temeiul Legii privind examinarea reclamațiilor administrative ⁽⁶⁷⁾. Invers, în cazul în care o persoană consideră că PPC ar fi trebuit să acționeze, dar nu a făcut acest lucru, aceasta îi poate solicita PPC, în temeiul articolului 36-3 din legea menționată, să ia o dispoziție sau să furnizeze orientări administrative în cazul în care persoana consideră că „nu a fost luată o dispoziție sau nu au fost impuse orientările administrative necesare pentru corectarea încălcării”.
- (111) În ceea ce privește căile de atac judiciare, în temeiul Legii privind contenciosul administrativ, o persoană care nu este mulțumită de o dispoziție administrativă adoptată de PPC poate introduce în justiție o acțiune *mandamus* ⁽⁶⁸⁾, prin care să solicite instanței să impună PPC luarea unor noi măsuri ⁽⁶⁹⁾. În anumite cazuri, instanța poate, de asemenea, să emită o hotărâre provizorie *mandamus* pentru a preveni un prejudiciu ireversibil ⁽⁷⁰⁾. În plus, în temeiul aceleiași legi, o persoană poate solicita revocarea unei decizii a PPC ⁽⁷¹⁾.
- (112) În fine, o persoană poate iniția, de asemenea, o acțiune împotriva PPC pentru obținerea unei despăgubiri din partea statului, în temeiul articolului 1 alineatul (1) din Legea privind măsurile reparatorii acordate de stat dacă persoana respectivă a suferit daune din cauza faptului că un ordin emis de PPC și adresat unui operator economic a fost ilegal sau din cauza faptului că PPC nu și-a exercitat autoritatea.

3. ACCESAREA ȘI UTILIZAREA DE CĂTRE AUTORITĂȚILE PUBLICE DIN JAPONIA A DATELOR CU CARACTER PERSONAL TRANSFERATE DIN UNIUNEA EUROPEANĂ

- (113) Comisia a evaluat, de asemenea, limitările și garanțiile, inclusiv supravegherea și mecanismele de reparație individuală, care sunt prevăzute în legislația japoneză în ceea ce privește colectarea și utilizarea ulterioară a datelor cu caracter personal transferate operatorilor economici din Japonia de către autoritățile publice din motive de interes public, în special în scopul asigurării respectării dreptului penal și în scopuri de asigurare a securității naționale („accesul administrației publice”). În acest sens, guvernul japonez a furnizat Comisiei expuneri, asigurări și angajamente oficiale semnate la cel mai înalt nivel ministerial și la nivel de agenții, acestea fiind incluse în anexa II la prezenta decizie.

⁽⁶⁶⁾ Articolul 239 alineatul (2) din Codul de procedură civilă.

⁽⁶⁷⁾ Legea nr. 160 din 2014.

⁽⁶⁸⁾ Articolul 37-2 din Legea privind contenciosul administrativ.

⁽⁶⁹⁾ În conformitate cu articolul 3 alineatul (6) din Legea privind contenciosul administrativ, termenul „acțiune *mandamus*” se referă la o acțiune vizând obținerea unei hotărâri judecătorești care să oblige o agenție administrativă să adopte o dispoziție administrativă inițială pe care „ar fi trebuit” să o adopte, dar pe care nu a adoptat-o.

⁽⁷⁰⁾ Articolul 37-5 din Legea privind contenciosul administrativ.

⁽⁷¹⁾ Capitolul II secțiunea 1 din Legea privind contenciosul administrativ.

3.1. Cadrul juridic general

- (114) Ca exercițiu de autoritate publică, accesul administrației publice japoneze trebuie să se realizeze cu respectarea deplină a legii (principiul legalității). În acest sens, Constituția Japoniei conține dispoziții de limitare și de încadrare a colectării datelor cu caracter personal de către autoritățile publice. După cum s-a menționat deja în ceea ce privește prelucrarea datelor de către operatorii economici, Curtea Supremă a Japoniei, bazându-se pe articolul 13 din Constituție, care protejează, printre altele, dreptul la libertate, a recunoscut dreptul la viață privată și la protecția datelor ⁽⁷²⁾. Un aspect important al acestui drept este libertatea oricărei persoane ca informațiile sale cu caracter personal să nu fie dezvăluite unui terț fără permisiunea persoanei în cauză ⁽⁷³⁾. Acest lucru implică dreptul la protecția efectivă a datelor cu caracter personal împotriva abuzurilor și (mai precis) împotriva accesului ilegal. O protecție suplimentară este asigurată de articolul 35 din Constituție referitor la dreptul tuturor persoanelor de a fi în siguranță la domiciliu, în documentele și în efectele personale, care impune autorităților publice obligația de a obține un mandat din partea unei instanțe, emis pentru o „cauză adecvată” ⁽⁷⁴⁾, în toate cazurile de „percheziție și punere sub sechestru”. În hotărârea sa din 15 martie 2017 (cauza GPS), Curtea Supremă a clarificat faptul că această cerință privind mandatul de arestare se aplică ori de câte ori guvernul invadează („intră în”) sfera privată într-un mod care suprimă voința persoanei în cauză și, prin urmare, prin intermediul unei „investigații obligatorii”. Un judecător nu poate emite un astfel de mandat decât pe baza unei suspiciuni concrete privind săvârșirea unei infracțiuni, și anume atunci când îi sunt furnizate documente justificative pe baza cărora se poate considera că persoana care face obiectul investigației a comis o infracțiune ⁽⁷⁵⁾. Prin urmare, autoritățile japoneze nu au competența juridică de a colecta informații cu caracter personal prin mijloace obligatorii în situațiile în care nu a avut loc încă nicio încălcare a legii ⁽⁷⁶⁾, de exemplu pentru a preveni o infracțiune sau o altă amenințare la adresa securității (ca în cazul investigațiilor efectuate din motive de securitate națională).
- (115) În temeiul principiului rezervei legii, orice colectare de date care se desfășoară în cadrul unei investigații coercitive trebuie să fie autorizată în mod explicit prin lege [astfel cum se reflectă, de exemplu, în articolul 197 alineatul (1) din Codul de procedură penală („CPP”) referitor la colectarea obligatorie de informații în scopul unei anchete penale]. Această cerință se aplică și în cazul accesului la informațiile electronice.
- (116) Este important de notat faptul că articolul 21 alineatul (2) din Constituție garantează confidențialitatea tuturor mijloacelor de comunicare, impunerea de limitări fiind permisă numai pe cale legislativă, din motive de interes public. Articolul 4 din Legea privind activitățile de telecomunicații, conform căruia secretul comunicațiilor gestionate de o societate de telecomunicații nu trebuie să fie încălcat, pune în aplicare această cerință de confidențialitate la nivelul dreptului material. Această dispoziție a fost interpretată ca o interdicție de a divulga informații despre comunicații, cu excepția cazului în care utilizatorii își dau consimțământul sau dacă divulgarea informațiilor se face pe baza uneia dintre derogările explicite de la răspunderea penală prevăzute în Codul penal ⁽⁷⁷⁾.
- (117) Constituția garantează, de asemenea, dreptul de a avea acces la justiție (articolul 32) și dreptul de a intenta o acțiune în justiție împotriva statului în vederea obținerii de măsuri reparatorii în cazul în care o persoană a suferit prejudicii din cauza unui act ilegal al unui funcționar public (articolul 17).
- (118) În ceea ce privește, în mod specific, dreptul la protecția datelor, în capitolul III secțiunile 1, 2 și 3 din APPI sunt prevăzute principiile generale care reglementează toate sectoarele, inclusiv sectorul public. Mai precis, articolul 3 din APPI prevede că toate informațiile cu caracter personal trebuie să fie gestionate în conformitate cu principiul respectării personalității indivizilor. Odată ce informațiile cu caracter personal au fost colectate („obținute”) de autoritățile publice ⁽⁷⁸⁾, inclusiv în cadrul înregistrărilor electronice, gestionarea acestora este reglementată prin

⁽⁷²⁾ A se vedea, de exemplu, hotărârea Curții Supreme din 12 septembrie 2003 în cauza nr. 1656 [2002 (Ju)]. În special, Curtea Supremă a statuat că „orice persoană are libertatea de a-și proteja propriile informații cu caracter personal de la a fi divulgate unui terț sau de la a fi făcute publice fără un motiv întemeiat.”

⁽⁷³⁾ Hotărârea Curții Supreme din 6 martie 2008 (Juki-net).

⁽⁷⁴⁾ „Cauza adecvată” există doar în cazul în care se consideră că persoana în cauză (persoana suspectată sau persoana acuzată) a comis o infracțiune, iar percheziția și punerea sub sechestru sunt necesare pentru desfășurarea unei anchete penale. A se vedea hotărârea Curții Supreme din 18 martie 1969 în cauza nr. 100 [1968 (Shi)].

⁽⁷⁵⁾ A se vedea articolul 156 alineatul (1) din Codul de procedură penală.

⁽⁷⁶⁾ Cu toate acestea, ar trebui remarcat faptul că Legea privind pedepsirea criminalității organizate și controlul produselor provenite din săvârșirea de infracțiuni din 15 iunie 2017 creează o nouă infracțiune care transferă în domeniul penal pregătirea unor acte de terorism și a altor forme de criminalitate organizată. Investigațiile pot fi inițiate numai dacă există o suspiciune concretă, bazată pe dovezi, că sunt întrunite toate cele trei condiții necesare care constituie infracțiunea (și anume, implicarea unui grup de criminalitate organizată, „actul de planificare” a infracțiunii și „actul de pregătire pentru săvârșirea” infracțiunii). A se vedea, de exemplu, și articolele 38-40 din Legea privind prevenirea activităților subversive (Legea nr. 240 din 21 iulie 1952).

⁽⁷⁷⁾ Articolul 15 alineatul (8) din Orientările privind protecția informațiilor cu caracter personal în sectorul telecomunicațiilor.

⁽⁷⁸⁾ Organele administrative, astfel cum sunt definite la articolul 2 alineatul (1) din APPIHAO. Potrivit informațiilor primite de la guvernul japonez, toate autoritățile publice, cu excepția poliției prefectorale, se încadrează în domeniul de aplicare al definiției „organelor administrative”. În același timp, poliția prefectorală își desfășoară activitatea în cadrul juridic stabilit prin ordonanțele prefectorale de protecție a informațiilor cu caracter personal (a se vedea articolul 11 din APPI și politica de bază), care prevăd dispoziții pentru protecția informațiilor cu caracter personal echivalente cu APPIHAO. A se vedea anexa II secțiunea I.B. Astfel cum a explicat PPC, în conformitate cu „politica de bază”, aceste ordonanțe trebuie să fie adoptate pe baza conținutului APPIHAO, iar MIC emite comunicări pentru a oferi autorităților locale îndrumările necesare în această privință. Așa cum a subliniat PPC, „[i]n aceste limite, în fiecare prefectură trebuie să se stabilească ordonanța de protecție a informațiilor cu caracter personal [...] pe baza politicii de bază și a conținutului comunicărilor.”

Legea privind protecția informațiilor cu caracter personal deținute de organele administrative („APPIHAO”) ⁽⁷⁹⁾. Această lege se referă, în principiu ⁽⁸⁰⁾, și la prelucrarea informațiilor cu caracter personal în scopul asigurării respectării dreptului penal sau al asigurării securității naționale. APPIHAO prevede, printre altele, că autoritățile publice: (i) pot păstra informațiile cu caracter personal numai în măsura în care acest lucru este necesar pentru îndeplinirea atribuțiilor care le revin; (ii) nu utilizează aceste informații în scopuri „nedrepte”, nici nu le comunică unui terț fără justificare; (iii) specifică scopul și nu schimbă scopul respectiv dincolo de ceea ce poate fi considerat în mod rezonabil ca fiind relevant pentru scopul inițial (limitarea scopului); (iv) în principiu, nu utilizează în alte scopuri informațiile cu caracter personal păstrate, nici nu le furnizează unui terț, iar în cazul în care consideră că acest lucru este necesar, impun restricții în ceea ce privește scopul sau metoda de utilizare de către terți; (v) se străduiesc să asigure corectitudinea informațiilor (calitatea datelor); (vi) iau măsurile necesare pentru gestionarea adecvată a informațiilor și pentru prevenirea scurgerii, pierderii sau deteriorării informațiilor (securitatea datelor); și (vii) depun eforturi pentru a prelucra în mod adecvat și rapid orice plângere referitoare la prelucrarea informațiilor ⁽⁸¹⁾.

3.2. Accesul și utilizarea de către autoritățile publice japoneze în scopuri de asigurare a respectării dreptului penal

- (119) Legislația japoneză conține o serie de limitări în ceea ce privește accesul la datele cu caracter personal și utilizarea acestora în scopul asigurării respectării dreptului penal, precum și o serie de mecanisme de supraveghere și de reparație care oferă garanții suficiente că datele respective sunt protejate în mod eficace împotriva ingerințelor ilegale și a riscului de abuz.

3.2.1. Temeiul juridic și limitările/garanțiile aplicabile

- (120) În cadrul juridic japonez, colectarea informațiilor electronice în scopul asigurării respectării dreptului penal este permisă pe baza unui mandat (colectare obligatorie) sau pe baza unei cereri de divulgare voluntară.

3.2.1.1. Investigație obligatorie bazată pe un mandat emis de o instanță

- (121) Astfel cum este indicat în considerentul 115, orice colectare de date în cadrul unei investigații coercitive trebuie să fie autorizată în mod specific prin lege și nu poate fi efectuată decât pe baza unui mandat din partea unei instanțe „emis pentru o cauză adecvată” (articolul 35 din Constituție). În ceea ce privește investigarea infracțiunilor, această cerință este reflectată în dispozițiile Codului de procedură penală („CPP”). În conformitate cu articolul 197 alineatul (1) din CPP, măsurile obligatorii „nu se aplică decât dacă au fost prevăzute dispoziții speciale în prezentul cod”. În ceea ce privește colectarea informațiilor electronice, singurele temeuri juridice relevante ⁽⁸²⁾ în această privință sunt articolul 218 din CPP (percheziția și punerea sub sechestru) și articolul 222-2 din CPP, conform căruia măsurile obligatorii pentru interceptarea comunicațiilor electronice fără consimțământul uneia sau altelea dintre părți se execută pe baza altor acte legislative, și anume pe baza Legii privind interceptarea comunicațiilor pentru investigarea infracțiunilor („Legea privind interceptarea comunicațiilor”). În ambele cazuri se aplică cerința existenței mandatului.
- (122) Mai precis, în temeiul articolului 218 alineatul (1) din CPP, un procuror, un procuror-asistent sau un agent al poliției judiciare poate, dacă acest lucru este necesar pentru investigarea unei infracțiuni, să efectueze o percheziție sau o punere sub sechestru (inclusiv să solicite înregistrări) pe baza unui mandat emis în prealabil de un judecător ⁽⁸³⁾. Printre altele, un astfel de mandat trebuie să conțină numele persoanei suspectate sau acuzate, infracțiunea imputată ⁽⁸⁴⁾, înregistrările electromagnetice care trebuie să fie puse sub sechestru și „locul sau articolele” care trebuie inspectate [articolul 219 alineatul (1) din CPP].

⁽⁷⁹⁾ Informațiile cu caracter personal obținute de funcționarii unui organ administrativ în cursul exercitării atribuțiilor și care sunt păstrate de respectivul organ administrativ pentru utilizarea la nivel de organizație se încadrează în definiția „informațiilor cu caracter personal păstrate” în sensul articolului 2 alineatul (3) din APPIHAO, atât timp cât acestea sunt înregistrate în „documente administrative”. Printre acestea se numără și informațiile electronice colectate și apoi prelucrate de aceste organisme, având în vedere faptul că definiția „documentelor administrative” de la articolul 2 alineatul (2) din Legea privind accesul la informațiile deținute de către organele administrative (Legea nr. 42 din 1999) cuprinde și înregistrările electromagnetice.

⁽⁸⁰⁾ Cu toate acestea, conform articolului 53-2 din Codul de procedură penală, capitolul IV din APPIHAO se exclude pentru „documentele referitoare la procese”, care, potrivit informațiilor primite, includ informațiile electronice obținute pe baza unui mandat sau a unei cereri de cooperare voluntară în cadrul unei anchete penale. În mod similar, în ceea ce privește informațiile colectate în domeniul securității naționale, persoanele fizice nu vor putea să își invoce cu succes drepturile în temeiul APPIHAO dacă directorul autorității publice are „motive rezonabile” de a considera că divulgarea informațiilor „poate aduce prejudicii securității naționale” [a se vedea articolul 14 punctul (iv)]. Acestea fiind spuse, autoritățile publice au obligația de a acorda cel puțin divulgarea parțială ori de câte ori este posibil (articolul 15).

⁽⁸¹⁾ A se vedea trimiterile specifice la APPIHAO din anexa II secțiunea IIA.1(b)(2).

⁽⁸²⁾ În timp ce articolul 220 din CPP autorizează percheziția și punerea sub sechestru „la fața locului”, fără mandat, în cazul în care un procuror, un procuror-asistent sau un agent al poliției judiciare arestează o persoană suspectată/un infractor surprins în flagrant delict, acest lucru nu este relevant în contextul unui transfer și, prin urmare, în scopul prezentei decizii.

⁽⁸³⁾ În conformitate cu articolul 222 alineatul (1) coroborat cu articolul 110 din CPP, mandatul de percheziție/punere sub sechestru pentru înregistrări trebuie prezentat persoanei care urmează să fie supusă acestei măsuri.

⁽⁸⁴⁾ A se vedea, de asemenea, articolul 189 alineatul (2) din CPP, conform căruia un agent al poliției judiciare trebuie să investigheze cu privire la infractor și la dovezile referitoare la infractor „atunci când acesta consideră că a fost comisă o infracțiune.” De asemenea, articolul 155 alineatul (1) din Codul de procedură penală impune obligația ca o cerere de mandat adresată în scris să conțină, printre altele, „infracțiunea imputată” și „un rezumat al faptelor care constituie infracțiunea”.

- (123) În ceea ce privește interceptarea comunicațiilor, articolul 3 din Legea privind interceptarea comunicațiilor autorizează astfel de măsuri numai cu îndeplinirea unor cerințe stricte. Mai precis, autoritățile publice trebuie să obțină un mandat prealabil din partea unei instanțe care poate fi emis numai pentru investigarea unor infracțiuni grave specifice (enumerare în anexa la legea menționată) ⁽⁸⁵⁾ și atunci când este „extrem de dificil să se identifice infractorul sau să se clarifice situațiile/detaliile săvârșirii infracțiunii prin alte căi” ⁽⁸⁶⁾. În temeiul articolului 5 din Legea privind interceptarea comunicațiilor, mandatul este emis pentru o perioadă limitată de timp și judecătorul poate impune condiții suplimentare. De asemenea, Legea privind interceptarea comunicațiilor prevede o serie de garanții suplimentare, cum ar fi, de exemplu, necesitatea prezenței martorilor (articolele 12 și 20), interdicția de a intercepta comunicațiile anumitor grupuri privilegiate (de exemplu, medicii, avocații) (articolul 15), obligația de a pune capăt interceptării comunicațiilor dacă aceasta nu mai este justificată, chiar și în cursul perioadei de valabilitate a mandatului (articolul 18) sau cerința generală de a transmite o notificare persoanei în cauză și de a permite accesul la înregistrări în termen de treizeci de zile de la încheierea interceptării (articolele 23 și 24).
- (124) Pentru toate măsurile obligatorii bazate pe un mandat, se poate efectua doar o examinare „limitată la ceea ce este necesar pentru atingerea obiectivului examinării respective”, cu alte cuvinte examinarea se efectuează numai în cazul în care obiectivele urmărite de investigație nu pot fi realizate în alt mod [articolul 197 alineatul (1) din CPP]. Deși criteriile pentru determinarea necesității nu sunt detaliate în dreptul material, Curtea Supremă a Japoniei a hotărât că judecătorul care emite un mandat ar trebui să facă o evaluare globală luând în considerare în special (i) gravitatea infracțiunii și modul în care a fost săvârșită; (ii) valoarea și importanța materialelor care urmează să fie puse sub sechestru ca probe; (iii) probabilitatea (riscul) ca probele să fie ascunse sau distruse; și (iv) măsura în care punerea sub sechestru poate cauza prejudicii persoanei în cauză ⁽⁸⁷⁾.

3.2.1.2. Cererea de divulgare voluntară bazată pe o „fișă de solicitare de informații”

- (125) În limitele competenței lor, autoritățile publice pot colecta informații electronice și pe baza cererilor de divulgare voluntară. Este vorba de o formă de cooperare fără caracter obligatoriu în cadrul căreia nu se poate impune formularea unui răspuns la cererea respectivă ⁽⁸⁸⁾, scutind astfel autoritățile publice de obligația de a obține un mandat din partea unei instanțe.
- (126) În măsura în care o astfel de cerere vizează un operator economic și are ca obiect informații cu caracter personal, operatorul economic trebuie să respecte cerințele prevăzute în APPI. În conformitate cu articolul 23 alineatul (1) din APPI, operatorii economici pot divulga informații cu caracter personal unor terți fără consimțământul persoanei fizice în cauză numai în anumite cazuri, inclusiv în cazul în care divulgarea informațiilor respective se „bazează pe acte cu putere de lege și norme administrative” ⁽⁸⁹⁾. În domeniul asigurării respectării dreptului penal, temeiul legal pentru aceste cereri îl constituie articolul 197 alineatul (2) din CPP, conform căruia „se poate solicita organizațiilor private să raporteze cu privire la chestiuni necesare pentru investigație”. Întrucât o astfel de „fișă de solicitare de informații” nu este autorizată decât în cadrul unei anchete penale, aceasta presupune întotdeauna existența unei suspiciuni concrete privind o infracțiune care a fost deja comisă ⁽⁹⁰⁾. În plus, întrucât astfel de investigații sunt, în general, efectuate de către poliția prefecturală, se aplică limitările prevăzute la articolul 2 alineatul (2) din Legea privind poliția ⁽⁹¹⁾. Conform acestei dispoziții, activitățile poliției sunt „strict limitate” la îndeplinirea responsabilităților și sarcinilor care îi revin (și anume prevenirea, eliminarea și investigarea infracțiunilor). În plus, în îndeplinirea sarcinilor sale, poliția trebuie să acționeze în mod imparțial, nepărtinitor și echitabil și nu trebuie să abuzeze în nicio circumstanță de competențele sale „într-un mod care să aducă atingere drepturilor și libertăților unei persoane fizice garantate în Constituția Japoniei” (care includ, după cum s-a indicat, dreptul la viață privată și la protecția datelor) ⁽⁹²⁾.
- (127) În mod specific, în ceea ce privește articolul 197 alineatul (2) din CPP, Agenția Națională de Poliție (ANP), în calitate de autoritate federală însărcinată, printre altele, cu toate chestiunile legate de poliția criminală, a emis

⁽⁸⁵⁾ Anexa se referă la 9 tipuri de infracțiuni, de exemplu, infracțiunile legate de droguri și de arme de foc, traficul de persoane și asasinat. Este de remarcat faptul că infracțiunea introdusă recent de „pregătire a unor acte de terorism și a altor acte de criminalitate organizată” (a se vedea nota de subsol 76) nu este inclusă în această listă restrictivă.

⁽⁸⁶⁾ Mai mult, în conformitate cu articolul 23 din Legea privind interceptarea comunicațiilor, autoritatea de investigare trebuie să îi notifice în scris persoanei vizate că i-au fost interceptate comunicațiile (și că, prin urmare, acestea au fost incluse în registrul de interceptare).

⁽⁸⁷⁾ A se vedea anexa II secțiunea II.A.1)(b)(1).

⁽⁸⁸⁾ Conform informațiilor primite, operatorii economici care nu își îndeplinesc obligația de a coopera nu au de suferit consecințe negative (de exemplu, nu li s-a aplicat sancțiuni) în temeiul niciunei legi. A se vedea anexa II secțiunea II.A.2)(a).

⁽⁸⁹⁾ Conform Orientărilor PPC (Ediția cu normele generale), articolul 23 alineatul (1) litera (i) constituie temeiul juridic pentru divulgarea informațiilor cu caracter personal ca răspuns atât la un mandat (articolul 218 din CPP), cât și la o „fișă de solicitare de informații” [articolul 197 alineatul (2) din CPP].

⁽⁹⁰⁾ Acest lucru înseamnă că „fișa de solicitare de informații” poate fi utilizată doar pentru a colecta informații în cazuri individuale, și nu pentru o colectare pe scară largă a datelor cu caracter personal. A se vedea, de asemenea, anexa II secțiunea I.A.2)(b)(1).

⁽⁹¹⁾ Precum și regulamentele Comisiei prefecturale pentru siguranța publică, a se vedea articolul 189 alineatul (1) din CPP.

⁽⁹²⁾ A se vedea, de asemenea, articolul 3 din Legea privind poliția, conform căruia jurământul de intrare în serviciu pe care îl depun toți agenții de poliție este „de a fi fideli obligației de a apăra și de a respecta Constituția și legile Japoniei și de a își îndeplini atribuțiile în mod imparțial, echitabil, corect și obiectiv.”

instrucțiuni adresate poliției prefecturale⁽⁹³⁾ cu privire la „utilizarea adecvată a solicitărilor de informații scrise în materie de investigații”. În conformitate cu această notificare, solicitările trebuie introduse cu ajutorul unui formular prestabilit („Formularul nr. 49” sau așa numita „fișă de solicitare de informații”)⁽⁹⁴⁾, trebuie să se refere la înregistrări „legate de o investigație specifică”, iar informațiile solicitate trebuie să fie „necesare pentru [respectiv] investigație”. În fiecare caz, anchetatorul șef „examinează în mod aprofundat necesitatea, conținutul etc. ale cererii individuale” și trebuie să primească aprobarea internă din partea unui înalt funcționar.

- (128) În plus, în două hotărâri ale Curții Supreme a Japoniei, din 1969 și din 2008⁽⁹⁵⁾, s-au stabilit o serie de limitări cu privire la măsurile neobligatorii care aduc atingere dreptului la viață privată⁽⁹⁶⁾. Mai precis, curtea a considerat că acest tip de măsuri trebuie să fie „rezonabile” și să se mențină în „limitele general admise”, adică trebuie să fie necesare pentru investigarea unui suspect (colectarea de probe) și puse în aplicare „prin metode adecvate pentru îndeplinirea scopului investigației”⁽⁹⁷⁾. Hotărârile menționate arată că acest lucru presupune un test de proporționalitate, care să ia în considerare toate circumstanțele cazului (de exemplu, măsura în care se aduce atingere dreptului la viață privată, inclusiv așteptarea ca viața privată să fie respectată, gravitatea infracțiunii, probabilitatea de a obține probe utile, importanța probelor respective, posibile căi alternative de investigare etc.)⁽⁹⁸⁾.
- (129) În afară de aceste limitări privind exercitarea autorității publice, se așteaptă din partea operatorilor economici ca aceștia să verifice („să confirme”) necesitatea și „raționalitatea” furnizării de date către un terț⁽⁹⁹⁾. Aici se încadrează și întrebarea dacă aceștia sunt împiedicați prin lege să coopereze. Astfel de obligații legale contradictorii pot decurge, în special, din obligațiile de confidențialitate, cum ar fi articolul 134 din Codul penal (referitor la relația dintre un medic, un avocat, un preot etc. și clientul său). De asemenea, „orice persoană care desfășoară activități în domeniul telecomunicațiilor păstrează, atât timp cât este în funcție, secretele terților pe care le-a aflat prin intermediul comunicațiilor gestionate de societatea de telecomunicații” [articolul 4 alineatul (2) din Legea privind activitățile de telecomunicații]. Această obligație este completată prin sancțiunea prevăzută la articolul 179 din Legea privind activitățile de telecomunicații, conform căruia orice persoană care a încălcat secretul comunicațiilor care sunt gestionate de o societate de telecomunicații se face vinovată de o infracțiune și este pedepsită cu închisoarea în regim de muncă pentru o perioadă de maxim doi ani sau cu o amendă de cel mult un milion de yeni⁽¹⁰⁰⁾. Deși această cerință nu este absolută și, mai precis, autorizează măsuri prin care se încalcă secretul comunicațiilor, dar care constituie „acte justificabile” în sensul articolului 35 din Codul penal⁽¹⁰¹⁾, această excepție nu acoperă răspunsul la cererile neobligatorii ale autorităților publice de divulgare a informațiilor electronice în temeiul articolului 197 alineatul (2) al CPP.

3.2.1.3. Utilizarea ulterioară a informațiilor colectate

- (130) Din momentul în care sunt colectate de către autoritățile publice japoneze, informațiile cu caracter personal intră în domeniul de aplicare al APPIHAO. Această lege reglementează gestionarea (prelucrarea) „informațiilor cu caracter

⁽⁹³⁾ În conformitate cu articolul 30 alineatul (1) și cu articolul 31 alineatul (2) din Legea privind poliția, directorul general al Birourilor regionale de poliție (care sunt sucursalele locale ale ANP) „conduce și supraveghează” poliția prefecturală.

⁽⁹⁴⁾ În fișa de solicitare de informații trebuie să se indice, de asemenea, datele de contact ale „gestionarului” („denumirea secțiunii [funcția], numele gestionarului, numărul de telefon al biroului, numărul extensiei etc.”).

⁽⁹⁵⁾ Curtea Supremă, hotărârea din 24 decembrie 1969 [1965(A) 1187]; hotărârea din 15 aprilie 2008 [2007(A) 839].

⁽⁹⁶⁾ Deși aceste hotărâri nu au vizat colectarea de informații electronice, guvernul japonez a precizat că aplicarea criteriilor stabilite de Curtea Supremă se extinde la orice atingere adusă de autoritățile publice dreptului la viață privată, inclusiv la toate „investigațiile voluntare” și, prin urmare, criteriile respective reprezintă o obligație pentru autoritățile japoneze și atunci când solicită divulgarea voluntară de informații. A se vedea anexa II secțiunea II.A.2)(b)(1).

⁽⁹⁷⁾ Potrivit informațiilor primite, acești factori trebuie să fie considerați „rezonabili în conformitate cu convențiile acceptate de societate.” A se vedea anexa II secțiunea II.A.2)(b)(1).

⁽⁹⁸⁾ Pentru considerații similare în contextul investigațiilor obligatorii („interceptarea comunicațiilor”), a se vedea și hotărârea Curții Supreme din 16 decembrie 1999, 1997 (A) 636.

⁽⁹⁹⁾ În această privință, autoritățile japoneze au atras atenția asupra Orientărilor PPC (Ediția cu normele generale) și a punctului 5/14 din documentul „Întrebări și răspunsuri” pregătit de PPC pentru aplicarea APPI. Potrivit autorităților japoneze, „având în vedere gradul de conștientizare din ce în ce mai ridicat cu privire la drepturile la viață privată, precum și volumul de muncă generat de astfel de solicitări, operatorii economici sunt din ce în ce mai precauți în răspunsurile pe care le oferă în cazul acestor solicitări”. A se vedea anexa II secțiunea II.A.2) și în ceea ce privește Notificarea din 1999 a ANP. Conform informațiilor primite, au existat într-adevăr cazuri în care operatorii economici au refuzat să coopereze. De exemplu, în raportul său de transparență din 2017, LINE (cea mai populară aplicație de mesagerie din Japonia) declară următoarele: „După primirea unor solicitări din partea agențiilor de investigare etc., [...] verificăm dacă solicitările respective sunt adecvate în ceea ce privește legalitatea, protecția utilizatorilor etc. În urma acestei verificări, vom refuza cererea la momentul respectiv în cazul în care vom constata o lacună juridică. Dacă sfera de acoperire a cererii este prea extinsă în raport cu scopul investigației, atunci solicităm o explicație în acest sens din partea agenției de investigare. Dacă explicația este neîntemeiată, nu răspundem la solicitarea respectivă.” Disponibil pe internet, la adresa: <https://linecorp.com/en/security/transparency/top>

⁽¹⁰⁰⁾ Sancțiunile sunt pedepsa cu închisoarea în regim de muncă pentru o perioadă de trei ani sau o amendă de cel mult 2 milioane de yeni pentru persoanele care „desfășoară activități de telecomunicații”.

⁽¹⁰¹⁾ „Actele justificabile” prevăzute în Codul penal sunt, în special, acele acte ale unei societăți de telecomunicații prin care aceasta respectă măsuri impuse de stat care au forță juridică (măsuri obligatorii), de exemplu, în cazul în care autoritățile de investigare iau măsuri pe baza unui mandat emis de un judecător. A se vedea anexa II secțiunea II.A.2)(b)(2), cu trimitere la Orientările privind protecția informațiilor cu caracter personal în sectorul telecomunicațiilor.

personal păstrate” și impune în acest sens o serie de limitări și de garanții (a se vedea considerentul 118) ⁽¹⁰²⁾. În plus, faptul că un organ administrativ poate păstra informații cu caracter personal „numai atunci când păstrarea acestor informații este necesară pentru desfășurarea activităților care intră în domeniul său de competență în temeiul actelor cu putere de lege și normelor administrative” [articolul 3 alineatul (1) din APPIHAO] impune, de asemenea, o serie de restricții, cel puțin indirect, în ceea ce privește colectarea inițială.

3.2.2. Supravegherea independentă

- (131) În Japonia, colectarea informațiilor electronice în domeniul asigurării respectării dreptului penal este, în principal ⁽¹⁰³⁾, de responsabilitatea poliției prefecturale ⁽¹⁰⁴⁾ care, în această privință, face obiectul mai multor niveluri de supraveghere.
- (132) În primul rând, în toate cazurile în care informațiile electronice sunt colectate prin mijloace obligatorii (percheziție și punere sub sechestru), poliția trebuie să obțină un mandat prealabil din partea unei instanțe (a se vedea considerentul 121). Prin urmare, colectarea informațiilor în acele cazuri va fi verificată *ex ante* de un judecător, pe baza unui standard strict de „cauză adecvată”.
- (133) Deși în cazul cererilor de divulgare voluntară nu există un control *ex ante* efectuat de un judecător, operatorii economici cărora li se adresează astfel de cereri se pot opune acestor cereri fără a risca să aibă de suferit consecințe negative (și vor trebui să țină seama de impactul pe care îl poate avea orice divulgare asupra vieții private). În plus, în conformitate cu articolul 192 alineatul (1) din CPP, agenții de poliție trebuie să coopereze întotdeauna cu procurorul (și cu Comisia prefecturală pentru siguranța publică) ⁽¹⁰⁵⁾ și să își coordoneze acțiunile cu acesta (aceasta). La rândul său, procurorul poate da instrucțiunile generale necesare pentru stabilirea unor standarde pentru desfășurarea unei investigații corecte și/sau poate emite ordine specifice cu privire la o investigație individuală (articolul 193 din CPP). În cazul în care astfel de instrucțiuni și/sau ordine nu sunt respectate, ministerul public poate introduce o procedură vizând luarea de măsuri disciplinare (articolul 194 din CPP). Așadar, poliția prefecturală își desfășoară activitatea sub supravegherea procurorului.
- (134) În al doilea rând, în conformitate cu articolul 62 din Constituție, fiecare cameră a parlamentului japonez („Dieta Națională a Japoniei”) poate desfășura investigații cu privire la administrația publică, inclusiv în ceea ce privește legalitatea colectării de informații de către poliție. În acest scop, Dieta poate solicita prezența și audierea unor martori și/sau furnizarea de înregistrări. Aceste competențe de anchetă sunt precizate mai detaliat în Regulamentul de procedură al Dietei Naționale, în special la capitolul XII. Mai precis, în conformitate cu articolul 104 din Regulamentul de procedură al Dietei, Cabinetul, agențiile publice și alte părți ale administrației publice „trebuie să răspundă solicitărilor venite din partea unei camere a Dietei sau din partea oricărei comisii a camerei respective de a prezenta rapoartele și înregistrările necesare spre examinare în cadrul unei investigații.” Refuzul de a se conforma solicitării nu este permis decât dacă administrația publică își justifică refuzul oferind un motiv plauzibil, care trebuie să fie considerat acceptabil de către Dietă, ori în cazul în care, printr-o declarație oficială, se arată că furnizarea rapoartelor sau a înregistrărilor respective ar aduce „prejudicii grave interesului național” ⁽¹⁰⁶⁾. În plus, membrii Dietei pot adresa întrebări scrise Cabinetului (articolele 74 și 75 din Regulamentul de procedură al Dietei) și, în trecut, unele dintre aceste „întrebări scrise” au abordat și chestiunea gestionării informațiilor cu caracter personal de către administrația publică ⁽¹⁰⁷⁾. Rolul exercitat de Dietă în supravegherea puterii executive este susținut printr-o serie de obligații de raportare, de exemplu, în temeiul articolului 29 din Legea privind interceptarea comunicațiilor.
- (135) În al treilea rând, tot în cadrul puterii executive, poliția prefecturală este supusă supravegherii independente. Această supraveghere este exercitată, în special, de comisiile prefecturale pentru siguranța publică instituite la nivel de prefectură pentru a asigura administrarea democratică și neutralitatea politică a poliției ⁽¹⁰⁸⁾. Aceste comisii sunt alcătuite din membri numiți de guvernatorul prefectural, cu consimțământul Adunării Prefecturale (aleși din rândul cetățenilor care nu au ocupat în ultimii cinci ani un post de funcționar public în cadrul poliției), iar mandatul lor este garantat (mai precis, revocarea nu este posibilă decât din motive întemeiate) ⁽¹⁰⁹⁾. Potrivit informațiilor primite, comisiile nu primesc instrucțiuni de la nimeni și, prin urmare, pot fi considerate complet independente ⁽¹¹⁰⁾. În ceea ce privește sarcinile și competențele comisiilor prefecturale pentru siguranța publică, în

⁽¹⁰²⁾ În ceea ce privește drepturile persoanelor vizate, a se vedea secțiunea 3.1.

⁽¹⁰³⁾ În principiu, un procuror (sau un procuror-asistent aflat sub ordinele procurorului) poate, în cazul în care consideră că acest lucru este necesar, să investigheze o infracțiune [articolul 191 alineatul (1) din CPP].

⁽¹⁰⁴⁾ Conform informațiilor primite, Agenția Națională de Poliție nu desfășoară investigații individuale. A se vedea anexa II secțiunea II.A.1)(a).

⁽¹⁰⁵⁾ A se vedea, de asemenea, articolul 246 din CPP, conform căruia poliția judiciară are obligația de a transmite procurorului dosarul cazului, după ce a efectuat investigația cu privire la o infracțiune („principiul transmiterii în toate cazurile”).

⁽¹⁰⁶⁾ Dieta dispune de alternativa de a solicita Consiliului de supraveghere și de examinare a secretelor desemnate în mod specific să efectueze o investigație cu privire la refuzul de a răspunde. A se vedea articolul 104-II din Regulamentul de procedură al Dietei.

⁽¹⁰⁷⁾ A se vedea anexa II secțiunea II.B.4).

⁽¹⁰⁸⁾ În plus, în conformitate cu dispozițiile articolului 100 din Legea privind autonomia locală, adunarea locală are autoritatea de a investiga activitățile autorităților de aplicare a legii instituite la nivel de prefectură, inclusiv activitățile poliției prefecturale.

⁽¹⁰⁹⁾ A se vedea articolele 39-41 din Legea privind poliția. În ceea ce privește neutralitatea politică, a se vedea, de asemenea, articolul 42 din Legea privind poliția.

⁽¹¹⁰⁾ A se vedea anexa II secțiunea II.B.3) („sistem de consiliu independent”).

temeiul articolului 38 alineatul (3) coroborat cu articolul 2 și cu articolul 36 alineatul (2) din Legea privind poliția, aceste comisii sunt responsabile cu „protecția drepturilor și a libertății unei persoane”. În acest scop, comisiile respective sunt abilitate să „supervizeze”⁽¹¹¹⁾ toate activitățile de investigare ale poliției prefectorale, inclusiv colectarea de date cu caracter personal. În special, acestea „pot da indicații poliției prefectorale în detaliu sau într-un anumit caz individual de inspecție privind abaterile profesionale ale personalului din poliție, dacă este necesar”⁽¹¹²⁾. Atunci când șeful poliției prefectorale⁽¹¹³⁾ primește o astfel de indicație sau ia cunoștință în mod direct de un posibil caz de abatere profesională (inclusiv încălcarea unor legi sau alte tipuri de neglijări ale îndatoririlor), acesta trebuie să inspecteze cu promptitudine cazul respectiv și să raporteze rezultatul inspecției efectuate către Comisia prefectorală pentru siguranța publică [articolul 56 alineatul (3) din Legea privind poliția]. În cazul în care comisia consideră că este necesar, aceasta poate, de asemenea, să-l însărcineze pe unul dintre membrii săi cu examinarea stadiului punerii în aplicare. Procesul continuă până în momentul în care Comisia prefectorală pentru siguranța publică consideră că incidentul a fost soluționat în mod adecvat.

- (136) În plus, în ceea ce privește aplicarea corectă a APPIHAO, ministrul de resort sau directorul agenției cu competențe în domeniu (de exemplu, comisarul general al ANP) are autoritate de aplicare a legii, sub supravegherea Ministerului Afacerilor Interne și al Comunicațiilor (MIC). Conform articolului 49 din APPIHAO, MIC „poate colecta rapoarte cu privire la stadiul aplicării prezentei legi” de la șefii organelor administrative (miniștrii). Această funcție de supraveghere este sprijinită de contribuțiile celor 51 de „centre de informare generală” ale MIC (unul în fiecare prefectură din Japonia), care tratează anual mii de solicitări de la persoane fizice⁽¹¹⁴⁾ (și care pot, la rândul lor, scoate la iveală posibile încălcări ale legii). În cazul în care consideră că acest lucru este necesar pentru a asigura respectarea legii menționate, MIC poate solicita prezentarea de explicații și materiale și poate emite avize cu privire la gestionarea informațiilor cu caracter personal de către organul administrativ în cauză (articolele 50 și 51 din APPIHAO).

3.2.3. Măsuri reparatorii individuale

- (137) În plus față de supravegherea din oficiu, persoanele fizice dispun, de asemenea, de mai multe posibilități de a obține măsuri reparatorii individuale, atât prin intermediul unor autorități independente (cum ar fi comisiile prefectorale pentru siguranța publică sau PPC), cât și prin intermediul instanțelor japoneze.
- (138) În primul rând, în ceea ce privește informațiile cu caracter personal colectate de către organele administrative, acestea din urmă au obligația de a „depune eforturi pentru a trata în mod adecvat și cu promptitudine orice plângere” cu privire la prelucrarea ulterioară a acestor informații (articolul 48 din APPIHAO). Deși capitolul IV din APPIHAO privind drepturile individuale nu se aplică în ceea ce privește informațiile cu caracter personal înregistrate în „documente referitoare la procese și la articole puse sub sechestru” [articolul 53-2 alineatul (2) din CPP], care acoperă informațiile cu caracter personal colectate în cadrul anchetelor penale, persoanele fizice pot depune o plângere pentru a invoca principiile generale de protecție a datelor, cum ar fi, de exemplu, obligația de a păstra informațiile cu caracter personal doar „atunci când păstrarea este necesară pentru a îndeplini [funcții de aplicare a legii]” [articolul 3 alineatul (1) din APPIHAO].
- (139) În plus, articolul 79 din Legea privind poliția le garantează persoanelor fizice care au temeri cu privire la „executarea sarcinilor” de către personalul poliției dreptul de a depune o plângere la Comisia prefectorală independentă (competentă) pentru siguranța publică. Această comisie va trata astfel de plângeri „cu loialitate”, cu respectarea legii și a ordonanțelor locale, și va informa în scris reclamantul cu privire la rezultate. Pe baza autorității sale de a supraveghea și „de a da instrucțiuni” poliției prefectorale în ceea ce privește „abaterile profesionale ale personalului” [articolul 38 alineatul (3) și articolul 43-2 alineatul (1) din Legea privind poliția], aceasta poate solicita poliției prefectorale să investigheze faptele, să ia măsurile adecvate pe baza rezultatelor investigației respective și să raporteze rezultatele. În cazul în care consideră că investigația efectuată de poliție nu a fost adecvată, comisia poate furniza, de asemenea, instrucțiuni cu privire la tratarea plângerii.
- (140) Pentru a facilita gestionarea plângerilor, ANP a emis o „comunicare” adresată poliției și comisiilor prefectorale pentru siguranța publică cu privire la tratarea adecvată a plângerilor referitoare la executarea sarcinilor de către agenții de poliție. În acest document, ANP enunță o serie de standarde pentru interpretarea și punerea în aplicare a

⁽¹¹¹⁾ A se vedea articolul 5 alineatul (3) și articolul 38 alineatul (3) din Legea privind poliția.

⁽¹¹²⁾ A se vedea articolul 38 alineatul (3) și articolul 43-2 alineatul (1) din Legea privind poliția. În cazul în care aceasta „dă o instrucțiune” în sensul articolului 43-2 alineatul (1), Comisia prefectorală pentru siguranța publică poate dispune ca un comitet desemnat de comisie să monitorizeze punerea în aplicare a instrucțiunii respective [alineatul (2)]. De asemenea, comisia poate recomanda luarea de măsuri disciplinare sau demiterea șefului poliției prefectorale [articolul 50 alineatul (2)], precum și a altor agenți de poliție [articolul 55 alineatul (4) din Legea privind poliția].

⁽¹¹³⁾ Același lucru este valabil și pentru inspectorul general în cazul poliției metropolitane din Tokyo [a se vedea articolul 48 alineatul (1) din Legea privind poliția].

⁽¹¹⁴⁾ Potrivit informațiilor primite, în cursul exercițiului financiar 2017 (din aprilie 2017 până în martie 2018), „centrele de informare generală” au tratat un număr total de 5 186 de solicitări provenite de la persoane fizice.

articolului 79 din Legea privind poliția. Printre altele, aceasta solicită poliției prefecturale să stabilească un „sistem de gestionare a plângerilor” și să trateze și să raporteze „cu promptitudine” toate plângerile către Comisia prefecturală pentru siguranța publică competentă. Comunicarea definește plângerile ca fiind cereri de corectare „pentru orice dezavantaj specific care a fost cauzat în urma unui comportament ilegal sau inadecvat” ⁽¹¹⁵⁾ sau pentru „faptul că un agent de poliție, în executarea sarcinilor care îi revin, nu a întreprins o acțiune necesară” ⁽¹¹⁶⁾, precum și orice „plângere/nemulțumire legată de modul neadecvat de executare a sarcinilor de către un agent de poliție”. Domeniul de aplicare material al unei plângeri este așadar definit în linii mari, acoperind orice afirmație privind colectarea ilegală de date, iar reclamantul nu este obligat să aducă dovezi pentru a demonstra prejudiciul suferit ca urmare a acțiunilor unui agent de poliție. Un aspect important este acela că comunicarea prevede faptul că străinii (printre alții) primesc asistență pentru formularea unei plângeri. În urma unei plângeri, comisiile prefecturale pentru siguranța publică au obligația de a se asigura că poliția prefecturală examinează faptele, pune în aplicare măsurile „în funcție de rezultatul acestei examinări” și raportează rezultatele. În cazul în care comisia consideră că examinarea este insuficientă, aceasta emite instrucțiuni privind tratarea plângerii, pe care poliția prefecturală are obligația de a le urma. Pe baza rapoartelor primite și a măsurilor luate, comisia transmite o notificare persoanei fizice în cauză, precizând, printre altele, măsurile luate pentru soluționarea plângerii. Comunicarea ANP subliniază faptul că plângerile ar trebui tratate în „mod sincer” și că rezultatul ar trebui notificat „într-un termen [...] considerat adecvat în lumina normelor sociale și a bunului-simț”.

- (141) În al doilea rând, având în vedere faptul că măsurile reparatorii vor trebui să fie solicitate, în mod normal, în străinătate, adică într-un sistem străin și într-o limbă străină, pentru a facilita obținerea de reparații pentru persoanele fizice din UE ale căror date cu caracter personal sunt transferate către operatori economici din Japonia și, ulterior, accesate de autoritățile publice, guvernul japonez a recurs la competențele sale pentru a crea un mecanism specific, administrat și supravegheat de PPC, care să gestioneze și să soluționeze plângerile din acest domeniu. Acest mecanism se bazează pe obligația de cooperare impusă autorităților publice japoneze în temeiul APPI și pe rolul special al PPC în ceea ce privește transferurile internaționale de date dinspre țări terțe în temeiul articolului 6 din APPI și al politicii de bază (astfel cum a fost stabilit de către administrația japoneză prin ordin al Cabinetului). Detaliile acestui mecanism sunt prezentate în expunerile, asigurările și angajamentele oficiale primite din partea autorităților japoneze și anexate la prezenta decizie ca anexa II. Mecanismul nu este supus niciunei cerințe în vigoare și este deschis tuturor persoanelor, indiferent dacă sunt suspectate sau nu ori acuzate sau nu de înfăptuirea unei infracțiuni.
- (142) În cadrul acestui mecanism, o persoană care are suspiciuni că datele sale transferate din Uniunea Europeană au fost colectate sau utilizate de autoritățile publice din Japonia (inclusiv de autoritățile responsabile de asigurarea respectării dreptului penal) cu încălcarea normelor aplicabile poate depune o plângere la PPC (individual sau prin intermediul autorității pentru protecția datelor din țara sa în sensul articolului 51 din RGPD). PPC va avea obligația de a trata plângerea și, într-o primă etapă, va informa autoritățile publice competente, inclusiv organismele de supraveghere relevante, cu privire la aceasta. Autoritățile menționate au obligația de a coopera cu PPC, „inclusiv prin furnizarea informațiilor necesare și a materialelor relevante, astfel încât PPC să poată evalua dacă colectarea sau utilizarea ulterioară a informațiilor cu caracter personal a avut loc în conformitate cu normele aplicabile” ⁽¹¹⁷⁾. Această obligație, care derivă din articolul 80 din APPI (acesta impunând autorităților publice japoneze obligația de a coopera cu PPC), se aplică în general și deci acoperă și reexaminarea oricărei măsuri de investigare luate de autoritățile respective, care, în plus, s-au angajat să coopereze prin intermediul unor asigurări scrise oferite de ministerele și directorii de agenții care au competențe în domeniul respectiv, astfel cum este indicat în anexa II.
- (143) În cazul în care evaluarea arată că a avut loc o încălcare a normelor aplicabile, „cooperarea autorităților publice în cauză cu PPC include și obligația de a remedia încălcarea respectivă”, ceea ce, în cazul colectării ilegale de informații cu caracter personal, acoperă și ștergerea datelor respective. Este important de remarcat faptul că această obligație este îndeplinită sub supravegherea PPC, care va „confirma, înainte de încheierea evaluării, că încălcarea a fost remediată pe deplin.”
- (144) După încheierea evaluării, PPC îi comunică persoanei fizice într-un termen rezonabil rezultatul evaluării, inclusiv orice măsură corectivă întreprinsă, dacă este cazul. În același timp, PPC informează, de asemenea, persoana fizică cu privire la posibilitatea de a obține o confirmare a rezultatului de la autoritatea publică competentă și îi comunică denumirea autorității căreia trebuie să i se adreseze o astfel de cerere de confirmare. Posibilitatea de

⁽¹¹⁵⁾ Condiția existenței unui „dezavantaj specific” sugerează doar faptul că reclamantul trebuie să fie afectat el însuși de comportamentul poliției (sau de inacțiunea acesteia), nu că reclamantul trebuie să demonstreze prejudiciul cauzat.

⁽¹¹⁶⁾ Respectarea legislației, inclusiv a cerințelor legale privind colectarea și utilizarea datelor cu caracter personal, face parte din aceste îndatoriri. A se vedea articolul 2 alineatul (2) și articolul 3 din Legea privind poliția.

⁽¹¹⁷⁾ Pentru a realiza această evaluare, PPC va colabora cu MIC care, astfel cum se precizează în considerentul 136, poate solicita prezentarea de explicații și materiale și poate emite avize cu privire la gestionarea informațiilor cu caracter personal de către organul administrativ în cauză (articolele 50 și 51 din APPIHAO).

a primi o astfel de confirmare, care să includă motivele care stau la baza deciziei autorității competente, este utilă persoanei în cauză în eventualitatea unor demersuri ulterioare, inclusiv atunci când introduce o cale de atac judiciară. Accesul la informații detaliate cu privire la rezultatul evaluării poate fi restricționat, atât timp cât există motive întemeiate de a considera că prin comunicarea acestor informații investigația în curs este expusă unui risc.

- (145) În al treilea rând, o persoană care nu este de acord cu o decizie (un mandat) de punere sub sechestru ⁽¹¹⁸⁾ privind datele sale cu caracter personal luate (emis) de un judecător sau cu măsurile luate de poliție sau de organele de urmărire penală care aplică o astfel de decizie poate solicita anularea sau modificarea deciziei ori măsurilor respective [articolul 429 alineatul (1) și articolul 430 alineatele (1) și (2) din CPP, precum și articolul 26 din Legea privind interceptarea comunicațiilor] ⁽¹¹⁹⁾. În cazul în care instanța de control judiciar consideră că fie mandatul în sine, fie executarea acestuia („procedura de punere sub sechestru”) este ilegal(ă), aceasta va da curs cererii și va dispune returnarea articolelor puse sub sechestru ⁽¹²⁰⁾.
- (146) În al patrulea rând, ca o formă mai indirectă de control judiciar, o persoană care consideră că colectarea informațiilor sale cu caracter personal în cadrul investigației unei infracțiuni a fost ilegală poate, în faza de judecată a procesului său penal, să invoce această ilegalitate. În cazul în care instanța este de acord, acest lucru va duce la excluderea elementelor de probă pe motiv de inadmisibilitate.
- (147) În fine, în temeiul articolului 1 alineatul (1) din Legea privind măsurile reparatorii acordate de stat, o instanță poate hotărî acordarea unei despăgubiri în cazul în care un funcționar public care exercită autoritatea publică a statului a cauzat persoanei în cauză prejudicii, în cursul exercitării atribuțiilor sale, în mod ilegal și din culpă (intenționat sau din neglijență). În conformitate cu articolul 4 din Legea privind măsurile reparatorii acordate de stat, răspunderea statului pentru daune se întemeiază pe dispozițiile Codului civil. În acest sens, articolul 710 din Codul civil prevede că răspunderea acoperă, de asemenea, și alte daune decât daunele materiale, deci și daunele morale (de exemplu, sub formă de „prejudiciu psihologic”). Aceasta include cazurile în care viața privată a unei persoane a fost invadată de o supraveghere ilicită și/sau de colectarea informațiilor sale cu caracter personal (de exemplu, executarea ilegală a unui mandat) ⁽¹²¹⁾.
- (148) În plus față de compensațiile bănești, persoanele pot beneficia, în anumite condiții, și de o ordonanță președințială (de exemplu, ștergerea datelor cu caracter personal colectate de autoritățile publice) pe baza drepturilor lor la viață privată în temeiul articolului 13 din Constituție ⁽¹²²⁾.
- (149) În ceea ce privește toate căile de atac menționate, mecanismul de soluționare a litigiilor creat de guvernul japonez prevede că o persoană care este în continuare nemulțumită de rezultatul procedurii se poate adresa PPC „care informează persoana în cauză cu privire la diferitele posibilități și proceduri detaliate pentru obținerea de reparații în temeiul actelor cu putere de lege și normelor administrative japoneze.” În plus, PPC „va oferi persoanei în cauză sprijin, inclusiv consiliere și asistență în ceea ce privește introducerea unei eventuale căi de atac ulterioare pe lângă instanța administrativă sau judecătorească relevantă.”
- (150) Aceasta include recurgerea la drepturile procedurale prevăzute în Codul de procedură penală. De exemplu, „[î]n cazul în care evaluarea arată că o persoană este suspectată în cadrul unui dosar penal, PPC va informa persoana respectivă în legătură cu acest lucru” ⁽¹²³⁾, precum și în legătură cu posibilitatea pe care o are, în temeiul articolului 259 din CPP, de a solicita ministerului public să o informeze atunci când acesta din urmă ia decizia de a nu iniția o procedură penală. De asemenea, în cazul în care evaluarea arată că informațiile cu caracter personal ale persoanei respective au fost utilizate în cadrul unui caz și că acel caz a fost închis, PPC va informa persoana în cauză că dosarul poate fi consultat în temeiul articolului 53 din CPP (și al articolului 4 din Legea privind dosarele penale

⁽¹¹⁸⁾ Aceasta include un mandat privind interceptarea comunicațiilor, pentru care în Legea privind interceptarea comunicațiilor este prevăzută o cerință de notificare specifică (articolul 23). Conform dispoziției respective, autoritatea de investigare trebuie să le notifice în scris persoanelor în cauză faptul că le-au fost interceptate comunicațiile (și că, prin urmare, acestea au fost incluse în registrul de interceptare). Un alt exemplu este articolul 100 alineatul (3) din CPP conform căruia instanța, atunci când pune sub sechestru trimiteri poștale sau telegrame expediate învinutului sau de către acesta, trebuie să notifice acest lucru expeditorului sau destinatarului, cu excepția cazului în care există riscul ca o astfel de notificare să obstrucționeze procedurile judiciare. Articolul 222 alineatul (1) din CPP face trimitere la această dispoziție pentru perchezițiile și punerile sub sechestru efectuate de o autoritate de investigare.

⁽¹¹⁹⁾ Deși o astfel de cerere nu are ca efect automat suspendarea executării deciziei de punere sub sechestru, instanța de control judiciar poate dispune suspendarea până la adoptarea unei decizii pe fond. A se vedea articolul 429 alineatul (2) și articolul 432 coroborate cu articolul 424 din CPP.

⁽¹²⁰⁾ A se vedea anexa II secțiunea II.C(1).

⁽¹²¹⁾ A se vedea anexa II secțiunea II.C(2).

⁽¹²²⁾ A se vedea, de exemplu, hotărârea instanței districtuale din Tokyo din 24 martie 1988 (nr. 2925); hotărârea instanței districtuale din Osaka din 26 aprilie 2007 (nr. 2925). Potrivit instanței districtuale din Osaka, va trebui să fie găsit un echilibru între o serie de factori, cum ar fi, de exemplu: (i) natura și conținutul informațiilor cu caracter personal în cauză; (ii) modul în care aceste informații au fost colectate; (iii) dezavantajele pentru persoana în cauză, în cazul în care informațiile nu sunt șterse; și (iv) interesul public, inclusiv dezavantajele pentru autoritatea publică, în cazul în care informațiile sunt șterse.

⁽¹²³⁾ În orice caz, după inițierea procedurii penale, ministerul public îi oferă învinutului posibilitatea de a consulta probele respective (a se vedea articolele 298-299 din CPP). În ceea ce privește victimele infracțiunilor, a se vedea articolele 316-333 din CPP.

închise). Este important ca o persoană să aibă acces la dosarul său, deoarece acest lucru o va ajuta să înțeleagă mai bine investigația efectuată împotriva sa și, astfel, să pregătească o eventuală acțiune în instanță (de exemplu, o acțiune în despăgubiri) în cazul în care consideră că datele sale au fost colectate sau utilizate în mod ilegal.

3.3. Accesul și utilizarea de către autoritățile publice japoneze în scopuri de securitate națională

- (151) Potrivit autorităților japoneze, în Japonia nu există nicio lege care să permită solicitările obligatorii de informații sau „interceptarea administrativă a comunicațiilor” în afara anchetelor penale. Prin urmare, din motive de securitate națională, informațiile pot fi obținute numai de la o sursă de informații care poate fi accesată liber de oricine sau prin divulgare voluntară. Operatorii economici care primesc o cerere de cooperare voluntară (sub formă de divulgare a unor informații electronice) nu au nicio obligație legală de a furniza informațiile respective ⁽¹²⁴⁾.
- (152) De asemenea, potrivit informațiilor primite, numai patru entități guvernamentale sunt împuternicite să colecteze informații electronice deținute de operatorii economici japonezi din motive de securitate națională, și anume: (i) biroul de informații operative și cercetare al Cabinetului (*Cabinet Intelligence & Research Office* – CIRO); (ii) Ministerul Apărării; (iii) poliția [atât Agenția Națională de Poliție (ANP) ⁽¹²⁵⁾, cât și poliția prefecturală]; și (iv) Agenția de Informații pentru Securitate Publică (*Public Security Intelligence Agency* – PSIA). Cu toate acestea, CIRO nu colectează niciodată informații direct de la operatorii economici, nici prin interceptarea comunicațiilor. În cazul în care primește informații de la alte autorități publice pentru a furniza documente de analiză Cabinetului, aceste autorități, la rândul lor, trebuie să respecte legea, inclusiv limitările și garanțiile analizate în prezenta decizie. Prin urmare, activitățile sale nu sunt relevante în contextul unui transfer.

3.3.1. Temeiul juridic și limitările/garanțiile aplicabile

- (153) Conform informațiilor primite, Ministerul Apărării colectează informații (electronice) pe baza Legii privind instituirea Ministerului Apărării. În temeiul articolului 3 al legii respective, misiunea Ministerului Apărării este de a gestiona și de a comanda forțele militare și „de a desfășura activități legate de acestea în scopul asigurării păcii și independenței naționale, precum și a siguranței națiunii”. Articolul 4 alineatul (4) prevede că Ministerul Apărării are în competența sa „apărarea și protecția”, acțiunile care trebuie întreprinse de Forțele de autoapărare, precum și desfășurarea forțelor militare, inclusiv colectarea informațiilor necesare pentru realizarea acestor activități. Prerogativele deținute permit Ministerului Apărării să colecteze informații (electronice) de la operatorii economici doar prin intermediul cooperării voluntare.
- (154) Ca și în cazul poliției prefecturale, responsabilitățile și îndatoririle acestuia includ „menținerea siguranței și ordinii publice” [articolul 35 alineatul (2) coroborat cu articolul 2 alineatul (1) din Legea privind poliția]. În cadrul acestor competențe, poliția poate colecta informații, dar numai pe bază de voluntariat, fără obligație juridică. În plus, activitățile poliției sunt „strict limitate” la ceea ce este necesar pentru îndeplinirea sarcinilor sale. De asemenea, poliția acționează într-un mod „împărtial, nepărtinitor, obiectiv și echitabil” și nu abuzează niciodată de competențele sale „în niciun mod care să aducă atingere drepturilor și libertăților unei persoane care sunt garantate prin Constituția Japoniei” (articolul 2 din Legea privind poliția).
- (155) În fine, PSIA poate efectua investigații în conformitate cu Legea privind prevenirea activităților subversive („SAPA”) și cu Legea privind controlul organizațiilor care au săvârșit acte de ucidere în masă arbitrar („ACO”) în cazul în care astfel de investigații sunt necesare pentru pregătirea adoptării unor măsuri de control împotriva anumitor organizații ⁽¹²⁶⁾. În temeiul acestor două legi, la cererea directorului general al PSIA, Comisia de examinare a securității publice poate emite anumite „dispoziții” [supraveghere/interdicții în cazul ACO ⁽¹²⁷⁾, dizolvare/interdicții în cazul SAPA ⁽¹²⁸⁾] și, în acest context, PSIA poate efectua investigații ⁽¹²⁹⁾. Conform informațiilor primite, aceste

⁽¹²⁴⁾ Prin urmare, operatorii economici pot alege în mod liber să nu coopereze, fără a se expune niciunui risc de sancțiuni sau altor consecințe negative. A se vedea anexa II secțiunea III.A.1).

⁽¹²⁵⁾ Cu toate acestea, în conformitate cu informațiile primite, rolul principal al ANP este de a coordona investigațiile efectuate de diferitele departamente ale poliției prefecturale și de a face schimb de informații cu autoritățile străine. Chiar și în cadrul acestui rol, ANP este supusă supravegherii de către Comisia națională pentru siguranța publică, care este responsabilă, printre altele, de protecția drepturilor și libertăților persoanelor fizice [articolul 5 alineatul (1) din Legea privind poliția].

⁽¹²⁶⁾ A se vedea anexa II secțiunea III.A.1)(3). Domeniul de aplicare respectiv al acestor două acte legislative este limitat, SAPA referindu-se la „activitățile teroriste subversive” și ACO la „actul de ucidere în masă arbitrar” (ceea ce înseamnă o „activitate teroristă subversivă” în temeiul SAPA „prin care un număr mare de persoane sunt asasinat în mod arbitrar”).

⁽¹²⁷⁾ A se vedea articolele 5 și 8 din ACO. O dispoziție privind supravegherea implică și o obligație de raportare pentru organizația vizată de măsură. Pentru garanțiile procedurale, în special cerințele de transparență și autorizarea prealabilă a Comisiei de examinare a securității publice, a se vedea articolele 12, 13 și 15-27 din ACO.

⁽¹²⁸⁾ A se vedea articolele 5 și 7 din SAPA. Pentru garanțiile procedurale, în special cerințele de transparență și autorizarea prealabilă a Comisiei de examinare a securității publice, a se vedea articolele 11-25 din SAPA.

⁽¹²⁹⁾ A se vedea articolul 27 din SAPA și articolele 29 și 30 din ACO.

investigații sunt întotdeauna efectuate cu titlu voluntar, ceea ce înseamnă că PSIA nu îl poate obliga pe deținătorul informațiilor cu caracter personal să furnizeze informațiile respective⁽¹³⁰⁾. De fiecare dată, controalele și investigațiile se limitează la strictul necesar pentru a atinge scopul controlului și, în niciun caz, nu trebuie să fie efectuate pentru a se restrânge „în mod nejustificat” drepturile și libertățile garantate prin Constituția Japoniei [articolul 3 alineatul (1) din SAPA/ACO]. În plus, în conformitate cu articolul 3 alineatul (2) din SAPA/ACO, PSIA nu trebuie în niciun caz să facă abuz de aceste controale sau de investigațiile desfășurate pentru a pregăti aceste controale. În cazul în care un agent al PSIA și-a utilizat în mod abuziv autoritatea pe care i-o conferă legea respectivă obligând o persoană să facă orice lucru pe care persoana respectivă nu este obligată să îl facă sau interferând în exercitarea drepturilor persoanei respective, acesta este pasibil de sancțiuni penale în temeiul articolului 45 din SAPA sau al articolului 42 din ACO. În cele din urmă, cele două legi prevăd în mod explicit că dispozițiile lor, inclusiv competențele pe care le conferă, „nu fac în nicio circumstanță obiectul unei interpretări extinse” (articolul 2 din SAPA/ACO).

- (156) În toate cazurile referitoare la accesul administrației publice din motive de securitate națională descrise în prezenta secțiune, se aplică limitările stabilite de Curtea Supremă a Japoniei pentru investigațiile voluntare, ceea ce înseamnă că colectarea informațiilor (electronice) trebuie să fie conformă cu principiile necesității și proporționalității („metoda adecvată”) ⁽¹³¹⁾. Astfel cum s-a confirmat în mod explicit de către autoritățile japoneze, „operațiunea de colectare și prelucrare a informațiilor are loc numai în măsura în care acest lucru este necesar pentru îndeplinirea unor sarcini specifice ale autorității publice competente, precum și pe baza unor amenințări specifice”. Prin urmare, „sunt excluse colectarea în masă și arbitrară sau accesul la informații cu caracter personal din motive de securitate națională” ⁽¹³²⁾.
- (157) De asemenea, odată colectate, informațiile cu caracter personal păstrate de autoritățile publice în scopuri de securitate națională vor intra sub incidența măsurilor de protecție prevăzute de APPHIO și, prin urmare, vor beneficia de această protecție, care se va aplica în ceea ce privește stocarea, utilizarea și divulgarea ulterioare ale acestora (a se vedea considerentul 118).

3.3.2. Supravegherea independentă

- (158) Colectarea de informații cu caracter personal în scopuri de securitate națională face obiectul unei supravegheri pe mai multe niveluri din partea celor trei ramuri ale puterii de stat.
- (159) În primul rând, Dieta Națională a Japoniei, prin intermediul comisiilor sale specializate în domeniu, poate examina legalitatea investigațiilor în baza competențelor sale de control parlamentar (articolul 62 din Constituție, articolul 104 din Regulamentul de procedură al Dietei; a se vedea considerentul 134). Această funcție de supraveghere este sprijinită de obligațiile de raportare specifice privind activitățile desfășurate în baza unora dintre temeiurile juridice menționate mai sus ⁽¹³³⁾.
- (160) În al doilea rând, în cadrul puterii executive există mai multe mecanisme de supraveghere.
- (161) În ceea ce privește Ministerul Apărării, supravegherea este exercitată de Biroul inspectorului general (IGO) de a cărui competență ține conformitatea juridică ⁽¹³⁴⁾; acest birou a fost înființat în baza articolului 29 din Legea privind instituirea Ministerului Apărării ca birou în cadrul acestui minister, sub supravegherea ministrului apărării (cărui birou îi raportează), dar care este independent de departamentele operaționale ale ministerului. IGO are sarcina de a asigura atât respectarea actelor cu putere de lege și a normelor administrative, cât și îndeplinirea în mod corespunzător de către funcționarii din cadrul Ministerului Apărării a atribuțiilor care le revin. IGO are, printre altele, autoritatea de a efectua așa-numitele „inspecții în domeniul apărării”, atât la intervale regulate („inspecții regulate în domeniul apărării”), cât și în cazuri individuale („inspecții speciale în domeniul apărării”), care, în trecut, vizau și gestionarea adecvată a informațiilor cu caracter personal ⁽¹³⁵⁾. În contextul acestor inspecții, IGO poate intra în sedii (birouri) și poate solicita prezentarea de documente sau informații, inclusiv furnizarea de

⁽¹³⁰⁾ A se vedea anexa II secțiunea III.A.1)(3).

⁽¹³¹⁾ A se vedea anexa II secțiunea III.A.2)(b): „Din jurisprudența Curții Supreme rezultă că, pentru a putea adresa o cerere de cooperare voluntară unui operator economic, cererea respectivă trebuie să fie necesară pentru investigarea unei infracțiuni suspectate și trebuie să fie rezonabilă pentru a atinge scopul investigației. Deși investigațiile efectuate de autoritățile de investigare în domeniul securității naționale sunt diferite, atât din punctul de vedere al temeiului juridic, cât și din punctul de vedere al scopului, de investigațiile efectuate de autoritățile de investigare în domeniul asigurării respectării legii, principiile centrale ale «necesității investigației» și «caracterului adecvat al metodei» se aplică în mod similar în domeniul securității naționale și trebuie respectate ținând seama în mod corespunzător de circumstanțele specifice fiecărui caz.”

⁽¹³²⁾ A se vedea anexa II secțiunea III.A.2)(b).

⁽¹³³⁾ A se vedea, de exemplu, articolul 36 din SAPA/articolul 31 din ACO (pentru PSIA).

⁽¹³⁴⁾ Șeful IGO este un fost procuror. A se vedea anexa II secțiunea III.B.3).

⁽¹³⁵⁾ A se vedea anexa II secțiunea III.B.3. Conform exemplului oferit, inspecția regulată în domeniul apărării din 2016, având drept obiect „sensibilizarea/pregătirea pentru conformitatea juridică” a vizat, printre altele, „situația protecției informațiilor cu caracter personal” (gestionare, stocare etc.). În raportul rezultat s-au constatat cazuri de gestionare necorespunzătoare a datelor și s-au solicitat îmbunătățiri în această privință. Ministerul Apărării a publicat raportul pe site-ului său web.

explicații de către viceministrul adjunct al ministrului apărării. Inspecția se încheie cu un raport adresat ministrului apărării, în care se prezintă constatările și măsurile de îmbunătățire (a căror punere în aplicare poate fi verificată din nou prin inspecții suplimentare). Raportul, la rândul său, constituie baza pentru instrucțiunile emise de ministrul apărării în vederea punerii în aplicare a măsurilor necesare pentru soluționarea situației; viceministrul adjunct are sarcina de a pune în aplicare aceste măsuri și trebuie să raporteze cu privire la acțiunile subsecvente.

- (162) În ceea ce privește poliția prefectorală, supravegherea este asigurată de către comisiile prefectorale independente pentru siguranța publică, astfel cum este explicat în considerentul 135 în ceea ce privește asigurarea respectării dreptului penal.
- (163) În cele din urmă, după cum s-a indicat, PSIA poate efectua investigații numai în măsura în care acest lucru este necesar pentru adoptarea unei interdicții, a unei dizolvări sau a unei dispoziții de supraveghere în temeiul SAPA/ACO, iar pentru aceste dispoziții, Comisia de examinare a securității publice, care este independentă ⁽¹³⁶⁾, exercită o supraveghere *ex ante*. În plus, se efectuează, de către inspectori desemnați în mod specific, inspecții regulate/periodice (care examinează în mod exhaustiv operațiile PSIA) ⁽¹³⁷⁾ și inspecții interne speciale ⁽¹³⁸⁾ cu privire la activitățile anumitor departamente/birouri etc.; aceste inspecții pot conduce la formularea de instrucțiuni adresate șefilor departamentelor relevante etc. de a lua măsuri corective sau măsuri de îmbunătățire.
- (164) Aceste mecanisme de supraveghere, care sunt consolidate și mai mult prin posibilitatea ca persoanele fizice să declanșeze intervenția PPC ca autoritate independentă de supraveghere (a se vedea considerentul 168 de mai jos), oferă garanțiile adecvate împotriva riscului de abuz de putere din partea autorităților japoneze în domeniul securității naționale și împotriva oricărei colectări ilegale de informații electronice.

3.3.3. Măsuri reparatorii individuale

- (165) În ceea ce privește măsurile reparatorii individuale în legătură cu informațiile cu caracter personal colectate și deci „păstrate” de către organe administrative, acestea din urmă au obligația de a „depune eforturi pentru a trata în mod adecvat și cu promptitudine orice plângere” cu privire la prelucrarea datelor (articolul 48 din APPIHAO).
- (166) În plus, spre deosebire de ceea ce este prevăzut în cazul anchetelor penale, persoanele fizice (inclusiv cetățenii străini care locuiesc în străinătate) au, în principiu, dreptul de divulgare ⁽¹³⁹⁾, de rectificare (inclusiv de ștergere) și de suspendare a utilizării/furnizării în temeiul APPIHAO. Acestea fiind spuse, șeful organului administrativ poate refuza divulgarea în ceea ce privește informațiile „pentru care există motive întemeiate [...] de a considera că divulgarea lor este de natură să dăuneze securității naționale” [articolul 14 punctul (iv) din APPIHAO] și poate chiar refuza divulgarea fără a fi obligat să reveleze existența informațiilor respective (articolul 17 din APPIHAO). De asemenea, cu toate că o persoană fizică poate solicita suspendarea utilizării sau ștergerea în temeiul articolului 36 alineatul (1) litera (i) din APPIHAO în cazul în care organul administrativ a obținut informațiile în cauză în mod ilegal sau le păstrează/utilizează într-un mod care depășește ceea ce este necesar pentru a atinge scopul specificat, autoritatea poate respinge cererea în cazul în care constată că suspendarea utilizării „este susceptibilă să împiedice executarea corespunzătoare a activităților care țin de scopul în care sunt utilizate informațiile cu caracter personal păstrate având în vedere natura activităților respective” (articolul 38 din APPIHAO). Totuși, atunci când este posibil să se separe cu ușurință informațiile și să se excludă acele porțiuni de informații care fac obiectul unei excepții, organele administrative au obligația să acorde cel puțin o divulgare parțială [a se vedea, de exemplu, articolul 15 alineatul (1) din APPIHAO] ⁽¹⁴⁰⁾.

⁽¹³⁶⁾ În conformitate cu Legea privind instituirea Comisiei de examinare a securității publice, președintele și membrii comisiei „își exercită în mod independent autoritatea” (articolul 3). Aceștia sunt numiți de către prim-ministru, cu acordul ambelor camere ale Dietei, și pot fi demisi doar „din motive întemeiate” (de exemplu, pedeapsă cu închisoarea, abuz în serviciu, tulburare psihică sau fizică, inițierea unei proceduri de faliment).

⁽¹³⁷⁾ Regulamentul privind inspecțiile periodice ale Agenției de Informații pentru Securitate Publică (Directorul general al PSIA, instrucțiunea nr. 4, 1986).

⁽¹³⁸⁾ Regulamentul privind inspecțiile speciale ale Agenției de Informații pentru Securitate Publică (Directorul general al PSIA, instrucțiunea nr. 11, 2008). Atunci când directorul general al PSIA consideră că acest lucru este necesar, vor fi desfășurate inspecții speciale.

⁽¹³⁹⁾ Acest drept corespunde dreptului de a primi o copie a „informațiilor cu caracter personal păstrate”.

⁽¹⁴⁰⁾ A se vedea, de asemenea, posibilitatea „divulgării discreționare” chiar și în cazul în care „informațiile a căror divulgare este interzisă” sunt incluse în „informațiile cu caracter personal păstrate” a căror divulgare este solicitată (articolul 16 din APPIHAO).

- (167) În orice caz, organul administrativ trebuie să emită o decizie scrisă într-un termen dat (30 de zile, care în anumite condiții poate fi prelungit cu încă 30 de zile). În cazul în care cererea este respinsă sau aprobată doar parțial ori în cazul în care persoana în cauză consideră, din alte motive, că organul administrativ a dat dovadă de un comportament „illegal sau nedrept”, persoana respectivă poate solicita examinarea administrativă pe baza Legii privind examinarea reclamațiilor administrative⁽¹⁴¹⁾. În acest caz, șeful organului administrativ care are sarcina de a lua o decizie cu privire la calea de atac consultă Comitetul de reexaminare a divulgării informațiilor și a protecției informațiilor cu caracter personal (articolele 42 și 43 din APPIHAO), un comitet specializat și independent, ai cărui membri sunt numiți de primul ministru cu acordul ambelor camere ale Dietei. Potrivit informațiilor primite, Comitetul de reexaminare poate realiza o examinare⁽¹⁴²⁾ și, în această privință, poate solicita organului administrativ să furnizeze atât informațiile cu caracter personal păstrate, inclusiv orice conținut clasificat, cât și alte informații și documente. Deși raportul final trimis reclamantului și organului administrativ, care este de asemenea publicat, nu are forță juridică obligatorie, constatările din raportul respectiv sunt urmate în aproape toate cazurile⁽¹⁴³⁾. Mai mult, persoana în cauză are posibilitatea de a introduce o cale de atac în instanță împotriva deciziei luate cu privire la contestație, în baza Legii privind contenciosul administrativ. Acest demers deschide calea către exercitarea controlului judiciar asupra utilizării excepției (excepțiilor) din motive de securitate națională, inclusiv pentru a determina dacă excepția respectivă a fost utilizată în mod abuziv sau dacă este în continuare justificată.
- (168) Pentru a facilita exercitarea drepturilor menționate mai sus în temeiul APPIHAO, MIC a înființat 51 de „centre de informare generală” care furnizează informații consolidate cu privire la aceste drepturi, la procedurile aplicabile pentru a adresa o cerere și la căile de atac posibile⁽¹⁴⁴⁾. În ceea ce privește organele administrative, acestea au obligația să furnizeze „informații care să contribuie la precizarea informațiilor cu caracter personal păstrate”⁽¹⁴⁵⁾ și să ia „alte măsuri adecvate, ținând cont de ceea ce este potrivit pentru persoana care intenționează să depună cererea” [articolul 47 alineatul (1) din APPIHAO].
- (169) La fel ca în cazul investigațiilor din domeniul asigurării respectării dreptului penal, și în domeniul securității naționale persoanele fizice pot obține măsuri reparatorii individuale prin contactarea directă a PPC. Acest demers va declanșa procedura specifică de soluționare a litigiilor pe care guvernul japonez a creat-o pentru persoanele fizice din UE ale căror date cu caracter personal sunt transferate în temeiul prezentei decizii (a se vedea explicațiile detaliate din considerentele 141-144 și considerentul 149).
- (170) În plus, persoanele fizice pot recurge la căi de atac judiciare sub forma unei acțiuni în despăgubiri în temeiul Legii privind măsurile reparatorii acordate de stat, care acoperă și prejudiciile morale și, în anumite condiții, ștergerea datelor colectate (a se vedea considerentul 147).

4. CONCLUZIE: NIVEL ADECVAT DE PROTECȚIE A DATELOR CU CARACTER PERSONAL TRANSFERATE DIN UNIUNEA EUROPEANĂ CĂTRE OPERATORI ECONOMICI DIN JAPONIA

- (171) Comisia consideră că APPI, astfel cum a fost completată prin normele suplimentare cuprinse în anexa I, împreună cu expunerile, asigurările și angajamentele oficiale cuprinse în anexa II, asigură un nivel de protecție a datelor cu caracter personal transferate din Uniunea Europeană care este, în esență, echivalent cu cel garantat prin Regulamentul (UE) 2016/679.
- (172) În plus, Comisia consideră că, în ansamblu, mecanismele de supraveghere și căile de atac prevăzute în legislația japoneză permit detectarea și pedepsirea în practică a încălcărilor comise de operatorii economici care gestionează informații cu caracter personal și pun la dispoziția persoanelor vizate căile de atac juridice necesare pentru a obține accesul la datele cu caracter personal care le privesc și, în cele din urmă, rectificarea sau ștergerea datelor respective.

⁽¹⁴¹⁾ Legea privind examinarea reclamațiilor administrative (Legea nr. 160 din 2014), în special articolul 1 alineatul (1).

⁽¹⁴²⁾ A se vedea articolul 9 din Legea de instituire a Comitetului de reexaminare a divulgării informațiilor și a protecției informațiilor cu caracter personal (Legea nr. 60 din 2003).

⁽¹⁴³⁾ Conform informațiilor primite, în cei 13 ani care au trecut din 2005 (anul în care a intrat în vigoare APPIHAO), în numai două din peste 2000 de cazuri organul administrativ nu a urmat recomandările din raport, în ciuda faptului că deciziile administrative au fost contrazise de câteva ori de Comitetul de reexaminare. În plus, în cazul în care organul administrativ ia o decizie care se abate de la constatările din raport, acesta trebuie să indice în mod clar motivele pentru care a acționat astfel. A se vedea anexa II secțiunea III.C, cu trimitere la articolul 50 alineatul (1) punctul (iv) din Legea privind examinarea reclamațiilor administrative.

⁽¹⁴⁴⁾ Centrele de informare generală – câte unul în fiecare prefectură – oferă cetățenilor explicații privind informațiile cu caracter personal colectate de autoritățile publice (de exemplu, bazele de date existente) și normele aplicabile privind protecția datelor (APPIHAO), inclusiv privind modul de exercitare a drepturilor de divulgare, de rectificare sau de suspendare a utilizării. În același timp, centrele funcționează ca punct de contact pentru solicitările/plângerile din partea cetățenilor. A se vedea anexa II secțiunea II.C.4(a).

⁽¹⁴⁵⁾ A se vedea, de asemenea, articolele 10 și 11 din APPIHO privind Registrul dosarelor cu informații cu caracter personal, care conțin însă excepții extinse în ceea ce privește „dosarele cu informații cu caracter personal” pregătite sau obținute pentru desfășurarea de anchete penale sau care conțin aspecte privind securitatea și alte interese importante ale statului [a se vedea articolul 10 alineatul (2) punctele (i) și (ii) din APPIHAO].

- (173) În cele din urmă, pe baza informațiilor disponibile cu privire la ordinea juridică japoneză, inclusiv pe baza expunerilor, asigurărilor și angajamentelor formulate de guvernul japonez și cuprinse în anexa II, Comisia consideră atât că orice atingere adusă, în scopuri de interes public, în special în scopul asigurării respectării dreptului penal și în scopul securității naționale, de autoritățile publice japoneze drepturilor fundamentale ale persoanelor fizice ale căror date cu caracter personal sunt transferate din Uniunea Europeană către Japonia se va limita la ceea ce este strict necesar pentru îndeplinirea obiectivului legitim în cauză, cât și că există o protecție juridică eficace împotriva unor astfel de atingeri.
- (174) Prin urmare, având în vedere constatările cuprinse în prezenta decizie, Comisia consideră că Japonia asigură un nivel adecvat de protecție a datelor cu caracter personal transferate din Uniunea Europeană către operatorii economici care gestionează informații cu caracter personal din Japonia și care fac obiectul APPI, cu excepția cazurilor în care destinatarul se încadrează într-una dintre categoriile enumerate la articolul 76 alineatul (1) din APPI, iar scopurile prelucrării corespund, în totalitate sau parțial, unuia dintre scopurile prevăzute în dispoziția respectivă.
- (175) Pe această bază, Comisia concluzionează că se respectă standardul caracterului adecvat prevăzut la articolul 45 din Regulamentul (UE) 2016/679, interpretat în lumina Cartei drepturilor fundamentale a Uniunii Europene, în special în hotărârea din cauza Schrems ⁽¹⁴⁶⁾.

5. ACȚIUNILE AUTORITĂȚILOR PENTRU PROTECȚIA DATELOR ȘI INFORMAȚIILE TRANSMISE COMISIEI

- (176) În conformitate cu jurisprudența Curții de Justiție ⁽¹⁴⁷⁾ și astfel cum se prevede la articolul 45 alineatul (4) din Regulamentul (UE) 2016/679, Comisia ar trebui să monitorizeze continuu evoluțiile relevante din țara terță după adoptarea unei decizii privind caracterul adecvat al nivelului de protecție, pentru a evalua dacă Japonia continuă să asigure un nivel de protecție echivalent în esență. O astfel de verificare este necesară, în orice caz, atunci când Comisia primește orice informație care dă naștere unor îndoieli justificate în această privință.
- (177) Prin urmare, Comisia ar trebui să monitorizeze în permanență situația în ceea ce privește cadrul juridic și practica propriu-zisă de prelucrare a datelor cu caracter personal, astfel cum sunt evaluate în prezenta decizie, inclusiv respectarea de către autoritățile japoneze a expunerilor, asigurărilor și angajamentelor cuprinse în anexa II. Pentru a facilita acest proces, se așteaptă din partea autorităților japoneze să informeze Comisia cu privire la evoluțiile semnificative relevante pentru prezenta decizie, atât în ceea ce privește prelucrarea datelor cu caracter personal de către operatorii economici, cât și limitările și garanțiile aplicabile accesului autorităților publice la datele cu caracter personal. Aceasta ar trebui să includă orice decizie adoptată de PPC în temeiul articolului 24 din APPI prin care se recunoaște că o țară terță oferă un nivel de protecție echivalent celui garantat în Japonia.
- (178) În plus, pentru a permite Comisiei să își exercite în mod eficace funcția de monitorizare, statele membre ar trebui să informeze Comisia cu privire la orice acțiune relevantă întreprinsă de autoritățile naționale de protecție a datelor („APD”), în special în ceea ce privește solicitările sau plângerile formulate de persoanele vizate din UE cu privire la transferul de date cu caracter personal din Uniunea Europeană către operatori economici din Japonia. De asemenea, Comisia ar trebui să fie informată cu privire la orice indiciu potrivit căruia acțiunile autorităților publice japoneze responsabile cu prevenirea, investigarea, detectarea sau aducerea în fața instanței a infracțiunilor sau cu securitatea națională, inclusiv acțiunile oricărui organism de supraveghere, nu asigură nivelul de protecție necesar.
- (179) Statele membre și organele acestora au obligația de a lua măsurile necesare pentru a se conforma actelor instituțiilor Uniunii, întrucât se presupune că aceste acte sunt legale și, prin urmare, produc efecte juridice atât timp cât nu sunt retrase, înclucate în cadrul unei acțiuni în anulare sau declarate nule ca urmare a unei trimiteri preliminare sau a unei excepții de nelegalitate. În consecință, o decizie a Comisiei privind caracterul adecvat al nivelului de protecție, adoptată în temeiul articolului 45 alineatul (3) din Regulamentul (UE) 2016/679, este obligatorie pentru toate organele statelor membre cărora li se adresează, inclusiv pentru autoritățile de supraveghere independente ale acestora. În același timp, astfel cum este explicat de Curtea de Justiție în hotărârea pronunțată în cauza Schrems ⁽¹⁴⁸⁾ și astfel cum este prevăzut la articolul 58 alineatul (5) din regulament, în cazul în care o autoritate națională de protecție a datelor pune sub semnul întrebării, inclusiv în urma primirii unei plângeri, compatibilitatea unei decizii a Comisiei privind caracterul adecvat al nivelului de protecție cu dreptul fundamental al unei persoane la viață privată și la protecția datelor, legislația națională trebuie să prevadă o cale de atac pentru a prezenta obiecțiile respective în fața unei instanțe naționale, care, în caz de îndoieli, trebuie să suspende procedurile și să efectueze o trimitere preliminară către Curtea de Justiție ⁽¹⁴⁹⁾.

⁽¹⁴⁶⁾ A se vedea mai sus nota de subsol 3.

⁽¹⁴⁷⁾ Hotărârea pronunțată în cauza Schrems, punctul 76.

⁽¹⁴⁸⁾ Hotărârea pronunțată în cauza Schrems, punctul 65.

⁽¹⁴⁹⁾ Hotărârea pronunțată în cauza Schrems, punctul 65: „În această privință, revine legiuitorului național sarcina de a prevedea căi de atac care să permită autorității naționale de supraveghere în cauză să invoce motivele pe care le consideră întemeiate în fața instanțelor naționale, astfel încât acestea din urmă să efectueze, dacă împărtășesc îndoielile acestei autorități în ceea ce privește validitatea deciziei Comisiei, o trimitere preliminară în vederea examinării validității acestei decizii”.

6. REVIZUIREA PERIODICĂ A CONSTATĂRII REFERITOARE LA CARACTERUL ADECVAT

- (180) În conformitate cu articolul 45 alineatul (3) din Regulamentul (UE) 2016/679 ⁽¹⁵⁰⁾ și având în vedere faptul că nivelul de protecție asigurat de ordinea juridică japoneză poate suferi modificări, Comisia, în urma adoptării prezentei decizii, ar trebui să verifice periodic dacă constatările referitoare la caracterul adecvat al nivelului de protecție asigurat de Japonia sunt în continuare justificate în fapt și în drept.
- (181) În acest scop, prezenta decizie ar trebui să facă obiectul unei prime revizuii în termen de doi ani de la intrarea sa în vigoare. În urma acestei prime revizuii și în funcție de rezultatul acesteia, Comisia va decide, consultându-se îndeaproape cu comitetul instituit în temeiul articolului 93 alineatul (1) din RGPD, dacă ciclul de doi ani trebuie menținut. În orice caz, revizuirile ulterioare ar trebui să aibă loc cel puțin o dată la patru ani ⁽¹⁵¹⁾. Revizuirea ar trebui să se refere la toate aspectele legate de funcționarea prezentei decizii și, în special, la aplicarea normelor suplimentare (acordându-se o atenție deosebită protecției oferite în caz de transferuri ulterioare), la aplicarea normelor privind consimțământul, inclusiv în cazul retragerii, la eficacitatea exercitării drepturilor individuale, precum și la limitările și garanțiile privind accesul administrației publice, inclusiv mecanismul de reparație, astfel cum este prevăzut în anexa II la prezenta decizie. Revizuirea ar trebui să acopere, de asemenea, eficacitatea supravegherii și a asigurării respectării legislației, atât în ceea ce privește normele aplicabile operatorilor economici care gestionează informații cu caracter personal, cât și normele aplicabile în domeniul asigurării respectării dreptului penal și în domeniul securității naționale.
- (182) Pentru a efectua această revizuire, Comisia ar trebui să se reunească cu PPC, însoțit, dacă este cazul, de alte autorități japoneze responsabile cu accesul administrației publice, inclusiv organismele de supraveghere competente. Participarea la această reuniune ar trebui să fie deschisă reprezentanților membrilor Comitetului european pentru protecția datelor (EDPB). În cadrul revizuirii comune, Comisia ar trebui să solicite PPC să furnizeze informații cuprinzătoare cu privire la toate aspectele relevante pentru constatarea referitoare la caracterul adecvat, inclusiv cu privire la limitările și garanțiile referitoare la accesul administrației publice la date ⁽¹⁵²⁾. Comisia ar trebui, de asemenea, să solicite explicații atât cu privire la orice informație relevantă pentru prezenta decizie pe care a primit-o, inclusiv cu privire la rapoartele publice întocmite de autoritățile japoneze sau de alte părți interesate din Japonia, de Comitetul european pentru protecția datelor, de diferite autorități naționale de protecție a datelor, de grupuri ale societății civile, cât și cu privire la informațiile transmise de mass-media sau de orice altă sursă de informații disponibilă.
- (183) Pe baza revizuirii comune, Comisia ar trebui să pregătească un raport public care trebuie să fie prezentat Parlamentului European și Consiliului.

7. SUSPENDAREA DECIZIEI PRIVIND CARACTERUL ADECVAT

- (184) În cazul în care, pe baza verificărilor periodice și ad-hoc sau a oricăror alte informații disponibile, Comisia ajunge la concluzia că nivelul de protecție oferit de ordinea juridică japoneză nu mai poate fi considerat echivalent în esență cu nivelul de protecție din Uniunea Europeană, aceasta ar trebui să informeze în acest sens autoritățile competente din Japonia și să solicite luarea măsurilor corespunzătoare într-un interval de timp bine definit și rezonabil. Printre acestea se numără normele aplicabile atât operatorilor economici, cât și autorităților publice japoneze responsabile cu asigurarea respectării dreptului penal sau cu securitatea națională. De exemplu, o astfel de procedură ar fi declanșată în cazurile în care transferurile ulterioare, inclusiv cele efectuate pe baza unor decizii adoptate de PPC în temeiul articolului 24 din APPI prin care se recunoaște că o țară terță oferă un nivel echivalent de protecție celui garantat în Japonia, nu vor mai fi efectuate cu aplicarea unor garanții care să asigure continuitatea protecției în sensul articolului 44 din RGPD.
- (185) În cazul în care, după perioada de timp stabilită, autoritățile competente din Japonia nu demonstrează în mod satisfăcător că prezenta decizie continuă să se bazeze pe un nivel adecvat de protecție, Comisia ar trebui, în temeiul articolului 45 alineatul (5) din Regulamentul (UE) 2016/679, să inițieze procedura care conduce la suspendarea parțială sau totală a prezentei decizii sau la abrogarea acesteia. Ca alternativă, Comisia ar trebui să inițieze procedura de modificare a prezentei decizii, în special prin aplicarea unor condiții suplimentare transferurilor de date sau prin limitarea domeniului de aplicare al constatării referitoare la caracterul adecvat numai la transferurile de date pentru care se asigură continuitatea protecției în sensul articolului 44 din RGPD.

⁽¹⁵⁰⁾ În conformitate cu articolul 45 alineatul (3) din Regulamentul (UE) 2016/679, „[a]ctul de punere în aplicare prevede un mecanism de revizuire periodică, cel puțin o dată la patru ani, care ia în considerare toate evoluțiile relevante din țara terță sau organizația internațională”.

⁽¹⁵¹⁾ Articolul 45 alineatul (3) din Regulamentul (UE) 2016/679 prevede că trebuie să se efectueze o revizuire periodică cel puțin o dată la patru ani. A se vedea, de asemenea, Comitetul european pentru protecția datelor (EDPB), Criterii de referință privind caracterul adecvat al nivelului de protecție (*Adequacy Referential*), WP 254 rev. 01.

⁽¹⁵²⁾ A se vedea, de asemenea, anexa II secțiunea IV: „În cadrul revizuirii periodice a deciziei privind caracterul adecvat al nivelului de protecție, PPC și Comisia Europeană vor face schimb de informații privind prelucrarea datelor în condițiile definite în constatarea referitoare la caracterul adecvat, inclusiv cele stabilite în prezenta expunere.”

- (186) Mai precis, Comisia ar trebui să inițieze procedura de suspendare sau de abrogare în cazul în care există indicii potrivit cărora normele suplimentare cuprinse în anexa I nu sunt respectate de către operatorii economici care primesc date cu caracter personal în temeiul prezentei decizii și/sau nu sunt aplicate în mod eficace sau că autoritățile japoneze nu respectă expunerile, asigurările și angajamentele cuprinse în anexa II la prezenta decizie.
- (187) De asemenea, Comisia ar trebui să aibă în vedere inițierea procedurii care conduce la modificarea, suspendarea sau abrogarea prezentei decizii în cazul în care, în contextul revizuirii comune sau într-un alt context, autoritățile japoneze competente nu furnizează informațiile sau clarificările necesare pentru evaluarea nivelului de protecție acordat datelor cu caracter personal transferate din Uniunea Europeană către Japonia sau pentru evaluarea respectării prezentei decizii. În această privință, Comisia ar trebui să ia în considerare măsura în care informațiile relevante pot fi obținute din alte surse.
- (188) Din motive de urgență justificate în mod corespunzător, cum ar fi riscul de încălcare gravă a drepturilor persoanelor vizate, Comisia ar trebui să ia în considerare posibilitatea adoptării unei decizii de suspendare sau de abrogare a prezentei decizii cu aplicare imediată, în temeiul articolului 93 alineatul (3) din Regulamentul (UE) 2016/679, coroborat cu articolul 8 din Regulamentul (UE) nr. 182/2011 al Parlamentului European și al Consiliului ⁽¹⁵³⁾.

8. CONSIDERAȚII FINALE

- (189) Comitetul european pentru protecția datelor și-a publicat avizul ⁽¹⁵⁴⁾, care a fost luat în considerare la pregătirea prezentei decizii.
- (190) Parlamentul European a adoptat o rezoluție privind o strategie în domeniul comerțului digital care invită Comisia să acorde prioritate și să accelereze adoptarea deciziilor privind caracterul adecvat al nivelului de protecție cu partenerii comerciali importanți în condițiile prevăzute în Regulamentul (UE) 2016/679, ca mecanism important de protecție a transferurilor de date cu caracter personal din Uniunea Europeană ⁽¹⁵⁵⁾. Parlamentul European a adoptat, de asemenea, o rezoluție privind caracterul adecvat al protecției datelor cu caracter personal asigurate de Japonia ⁽¹⁵⁶⁾.
- (191) Măsurile prevăzute în prezenta decizie sunt conforme cu avizul comitetului instituit în temeiul articolului 93 alineatul (1) din RGPD,

ADOPTĂ PREZENTA DECIZIE:

Articolul 1

1. În sensul articolului 45 din Regulamentul (UE) 2016/679, Japonia asigură un nivel adecvat de protecție a datelor cu caracter personal transferate din Uniunea Europeană către operatorii economici din Japonia care gestionează informații cu caracter personal și care fac obiectul Legii privind protecția informațiilor cu caracter personal, astfel cum a fost completată prin normele suplimentare din anexa I, precum și prin expunerile, asigurările și angajamentele oficiale cuprinse în anexa II.

⁽¹⁵³⁾ Regulamentul (UE) nr. 182/2011 al Parlamentului European și al Consiliului din 27 aprilie 2016 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date și de abrogare a Directivei 95/46/CE (Regulamentul general privind protecția datelor) (JO L 55, 28.2.2011, p. 13).

⁽¹⁵⁴⁾ Avizul 28/2018 referitor la Proiectul de decizie de punere în aplicare a Comisiei privind protecția adecvată a datelor cu caracter personal în Japonia, adoptat la 5 decembrie 2018.

⁽¹⁵⁵⁾ Rezoluția Parlamentului European din 12 decembrie 2017 intitulată „Către o strategie în domeniul comerțului digital” [2017/2065(INI)]. A se vedea, în special, punctul 8 („[...] reamintește că datele cu caracter personal pot fi transferate către țări terțe fără a utiliza dispoziții generale în acorduri comerciale atunci când sunt îndeplinite – atât în prezent, cât și în viitor – cerințele consfințite în [...] capitolul V din Regulamentul (UE) 2016/679 privind protecția datelor; recunoaște că deciziile privind caracterul adecvat al nivelului de protecție, inclusiv cele parțiale și sectoriale, reprezintă un mecanism fundamental în ceea ce privește protecția transferului datelor cu caracter personal din UE către o țară terță; observă că UE a adoptat decizii privind caracterul adecvat al nivelului de protecție cu doar patru din primii săi 20 de parteneri comerciali [...]”) și punctul 9 („invită Comisia să acorde prioritate și să accelereze adoptarea deciziilor privind caracterul adecvat al nivelului de protecție, cu condiția ca țările terțe să asigure, în temeiul legislației lor interne sau al angajamentelor lor internaționale, un nivel de protecție «în esență echivalent» cu cel garantat în UE [...]”).

⁽¹⁵⁶⁾ Rezoluția Parlamentului European din 13 decembrie 2018 referitoare la protecția adecvată a datelor cu caracter personal asigurate de Japonia [2018/2979(RSP)].

2. Prezenta decizie nu se referă la datele cu caracter personal transferate unor destinatari care se încadrează într-una dintre următoarele categorii, în măsura în care scopurile prelucrării datelor cu caracter personal corespund, în întregime sau în parte, unuia dintre scopurile enumerate, respectiv:

- (a) instituțiile de radiodifuziune, editorii de ziare, agențiile de comunicare sau alte organizații de presă (inclusiv orice persoană fizică care desfășoară activități de presă ca activitate profesională), în măsura în care prelucrează date cu caracter personal în scopuri jurnalistice;
- (b) persoanele implicate într-o activitate profesională legată de redactare, în măsura în care activitatea respectivă implică date cu caracter personal;
- (c) universitățile și orice alte organizații sau grupuri care au ca finalitate studiile universitare sau orice persoană care aparține unei astfel de organizații sau unui astfel de grup, în măsura în care prelucrează date cu caracter personal în scopul studiilor universitare;
- (d) organismele religioase, în măsura în care prelucrează date cu caracter personal în scopul desfășurării unei activități religioase (inclusiv a tuturor activităților conexe); și
- (e) organismele politice, în măsura în care prelucrează date cu caracter personal în scopul desfășurării activității lor politice (inclusiv a tuturor activităților conexe).

Articolul 2

Ori de câte ori autoritățile competente din statele membre, pentru a proteja persoanele fizice în ceea ce privește prelucrarea datelor cu caracter personal, își exercită competențele în temeiul articolului 58 din Regulamentul (UE) 2016/679, ceea ce duce la suspendarea sau la interdicția definitivă a fluxurilor de date către un anumit operator economic din Japonia care intră în domeniul de aplicare prevăzut la articolul 1, statul membru în cauză informează fără întârziere Comisia.

Articolul 3

1. Comisia monitorizează în permanență aplicarea cadrului juridic pe care se bazează prezenta decizie, inclusiv condițiile în care se efectuează transferurile ulterioare, în scopul de a evalua dacă Japonia continuă să asigure un nivel adecvat de protecție în sensul articolului 1.

2. Statele membre și Comisia se informează reciproc cu privire la cazurile în care Comisia pentru protecția informațiilor cu caracter personal sau orice altă autoritate japoneză competentă nu asigură respectarea cadrului juridic pe care se bazează prezenta decizie.

3. Statele membre și Comisia se informează reciproc atât cu privire la orice indiciu potrivit căruia atingerile aduse de autoritățile publice din Japonia dreptului persoanelor fizice la protecția datelor cu caracter personal depășesc ceea ce este strict necesar, cât și cu privire la faptul că nu există o protecție juridică eficace împotriva unor astfel de atingeri.

4. În termen de doi ani de la data notificării prezentei decizii către statele membre și ulterior cel puțin o dată la patru ani, Comisia evaluează constatarea menționată la articolul 1 alineatul (1) pe baza tuturor informațiilor disponibile, inclusiv a informațiilor primite în cadrul revizuirii comune realizate împreună cu autoritățile japoneze relevante.

5. În cazul în care Comisia dispune de indicii că nu mai este asigurat un nivel adecvat de protecție, aceasta informează autoritățile competente din Japonia. Dacă este necesar, Comisia poate decide să suspende, să modifice sau să abroge prezenta decizie ori poate limita domeniul de aplicare al acesteia, în special în cazul în care există indicii că:

- (a) operatorii economici din Japonia care au primit date cu caracter personal din Uniunea Europeană în temeiul prezentei decizii nu respectă garanțiile suplimentare prevăzute în normele suplimentare cuprinse în anexa I la prezenta decizie sau supravegherea și asigurarea respectării legislației în această privință sunt insuficiente;
- (b) autoritățile publice japoneze nu respectă expunerile, asigurările și angajamentele cuprinse în anexa II la prezenta decizie, inclusiv în ceea ce privește condițiile și limitările privind colectarea datelor cu caracter personal transferate în temeiul prezentei decizii și accesul autorităților publice japoneze la aceste date în scopuri de asigurare a respectării dreptului penal sau de securitate națională.

Comisia poate, de asemenea, să prezinte un proiect de măsuri care să fie luate în cazul în care lipsa de cooperare a autorităților japoneze împiedică Comisia să stabilească dacă este afectată constatarea de la articolul 1 alineatul (1) din prezenta decizie.

Articolul 4

Prezenta decizie se adresează statelor membre.

Adoptată la Bruxelles, 23 ianuarie 2019.

Pentru Comisie
Věra JOUROVÁ
Membru al Comisiei

ANEXA 1

**NORMELE SUPLIMENTARE ÎN TEMEIUL LEGII PRIVIND PROTECȚIA INFORMAȚIILOR CU CARACTER PERSONAL
PENTRU GESTIONAREA DATELOR CU CARACTER PERSONAL TRANSFERATE DIN UE PE BAZA UNEI DECIZII
PRIVIND CARACTERUL ADECVAT AL NIVELULUI DE PROTECȚIE**

Cuprins

1. Informațiile cu caracter personal care necesită o atenție specială [articolul 2 alineatul (3) din lege]	38
2. Datele cu caracter personal păstrate [articolul 2 alineatul (7) din lege]	39
3. Specificarea unui scop al utilizării, a unei restricții ca urmare a utilizării [articolul 15 alineatul (1), articolul 16 alineatul (1) și articolul 26 alineatele (1) și (3) din lege]	40
4. Restricții privind furnizarea către o parte terță într-o țară străină (articolul 24 din lege; articolul 11-2 din norme)	41
5. Informații prelucrate anonim [articolul 2 alineatul (9) și articolul 36 alineatele (1) și (2) din lege]	41

[Termeni]

„lege”	Legea privind protecția informațiilor cu caracter personal (Legea nr. 57/2003)
„ordinul Cabinetului”	Ordinul Cabinetului de aplicare a Legii privind protecția informațiilor cu caracter personal (Ordinul Cabinetului nr. 507/2003)
„norme”	Normele de punere în aplicare a Legii privind protecția informațiilor cu caracter personal (Normele nr. 3/2016 ale Comisiei pentru protecția informațiilor cu caracter personal)
„orientările privind normele generale”	Orientările referitoare la Legea privind protecția informațiilor cu caracter personal (volumul cu normele generale) (Comunicarea nr. 65/2015 a Comisiei pentru protecția informațiilor cu caracter personal)
„UE”	Uniunea Europeană, inclusiv statele sale membre și, având în vedere Acordul privind SEE, Islanda, Liechtenstein și Norvegia
„RGPD”	Regulamentul Parlamentului European și al Consiliului privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date și de abrogare a Directivei 95/46/CE (Regulamentul general privind protecția datelor)

„decizia privind caracterul adecvat al nivelului de protecție”
decizia Comisiei Europene potrivit căreia o țară terță sau un teritoriu din țara terță respectivă etc. asigură un nivel adecvat de protecție a datelor cu caracter personal în conformitate cu articolul 45 din RGPD

În scopul de a efectua un transfer reciproc și fără probleme al datelor cu caracter personal între Japonia și UE, Comisia pentru protecția informațiilor cu caracter personal a desemnat UE ca fiind o țară străină care a instituit un sistem de protecție a informațiilor cu caracter personal recunoscut ca având standarde echivalente celor din Japonia cu privire la protecția drepturilor și intereselor persoanelor în temeiul articolului 24 din lege, iar Comisia Europeană a decis în același timp că Japonia asigură un nivel adecvat de protecție a datelor cu caracter personal în temeiul articolului 45 din RGPD.

Astfel, se va realiza un transfer reciproc și fără probleme al datelor cu caracter personal între Japonia și UE, într-un mod care să asigure un nivel ridicat de protecție a drepturilor și intereselor persoanelor. Pentru a asigura un nivel ridicat de protecție a informațiilor cu caracter personal primite din UE pe baza unei decizii privind caracterul adecvat al nivelului de protecție și având în vedere că, în pofida unui grad ridicat de convergență între cele două sisteme, există diferențe relevante, Comisia pentru protecția informațiilor cu caracter personal a adoptat prezentele norme suplimentare pe baza dispozițiilor legii privind punerea în aplicare etc. a cooperării cu guvernele altor țări și în vederea asigurării tratării corespunzătoare a informațiilor cu caracter personal primite din UE pe baza unei decizii privind caracterul adecvat al nivelului de protecție de către un operator economic care gestionează informații cu caracter personal, precum și în scopul unei puneri în aplicare adecvate și eficiente a obligațiilor prevăzute de aceste norme ⁽¹⁾.

⁽¹⁾ Articolul 4, articolul 6, articolul 8, articolul 24, articolul 60 și articolul 78 din lege și articolul 11 din norme.

În special, articolul 6 din lege prevede competența de a lua măsuri legislative și alte măsuri necesare pentru a asigura o protecție sporită a informațiilor cu caracter personal și pentru a construi un sistem privind informațiile cu caracter personal care să respecte standardele internaționale prin norme mai stricte care completează și depășesc normele prevăzute în lege și în ordinul Cabinetului. Prin urmare, Comisia pentru protecția informațiilor cu caracter personal, în calitate de autoritate competentă pentru gestionarea generală a aplicării legii, are competența de a stabili, în temeiul articolului 6 din lege, reglementări mai stricte prin formularea prezentelor norme suplimentare care prevăd un nivel mai ridicat de protecție a drepturilor și intereselor persoanelor în ceea ce privește gestionarea datelor cu caracter personal primite din UE pe baza unei decizii privind caracterul adecvat al nivelului de protecție, inclusiv în ceea ce privește definirea informațiilor cu caracter personal care necesită o atenție specială în sensul articolului 2 alineatul (3) din lege și a datelor cu caracter personal păstrate în sensul articolului 2 alineatul (7) din lege (inclusiv referitor la perioada de păstrare relevantă).

Pe această bază, normele suplimentare sunt obligatorii pentru un operator economic care gestionează informații cu caracter personal și care primește date cu caracter personal transferate din UE pe baza unei decizii privind caracterul adecvat al nivelului de protecție, acesta fiind, așadar, obligat să le respecte. Dat fiind că aceste norme sunt obligatorii din punct de vedere juridic, respectarea drepturilor și obligațiilor este asigurată de Comisia pentru protecția informațiilor cu caracter personal în același mod ca și în cazul dispozițiilor din lege pe care normele suplimentare le completează cu norme mai stricte și/sau mai detaliate. În cazul încălcării drepturilor și obligațiilor care decurg din normele suplimentare, persoanele pot obține, de asemenea, reparație din partea instanțelor în același mod ca și în cazul dispozițiilor din lege pe care normele suplimentare le completează cu norme mai stricte și/sau mai detaliate.

În ceea ce privește asigurarea respectării de către Comisia pentru protecția datelor cu caracter personal, în cazul în care un operator economic care gestionează informații cu caracter personal nu respectă una sau mai multe obligații prevăzute de normele suplimentare, Comisia pentru protecția informațiilor cu caracter personal are competența de a adopta măsuri în temeiul articolului 42 din lege. În ceea ce privește, în general, informațiile cu caracter personal primite din UE pe baza unei decizii privind caracterul adecvat al nivelului de protecție, se consideră că, dacă un operator economic care gestionează informații cu caracter personal nu ia măsuri în conformitate cu o recomandare primită în temeiul articolului 42 alineatul (1) din lege, fără a avea un motiv legitim⁽²⁾, aceasta reprezintă o încălcare gravă a naturii iminente a drepturilor și intereselor persoanelor în sensul articolului 42 alineatul (2) din lege.

1. Informațiile cu caracter personal care necesită o atenție specială [articolul 2 alineatul (3) din lege]

Articolul 2 alineatul (3) din lege

- (3) „Informațiile cu caracter personal care necesită o atenție specială”, în sensul prezentei legi, înseamnă informațiile cu caracter personal care conțin rasa, crezul, statutul social, istoricul medical, cazierul judiciar, prejudiciile suferite în urma unei infracțiuni sau alte descrieri etc. ale persoanei principale, prevăzute în ordinul Cabinetului ca fiind cele a căror gestionare necesită o atenție specială, pentru a nu cauza discriminare injustă, prejudecăți sau alte dezavantaje pentru persoana principală.

Articolul 2 din ordinul Cabinetului

Aceste descrieri etc. prevăzute în ordinul Cabinetului în temeiul articolului 2 alineatul (3) din lege sunt descrierile etc. care conțin oricare dintre aspectele prevăzute în continuare (cu excepția celor care țin de istoricul medical sau de antecedentele penale ale persoanei principale):

- (i) faptul de a avea dizabilități fizice, intelectuale, mintale (inclusiv dizabilități de dezvoltare) sau orice alte dizabilități fizice și mintale funcționale menționate de normele Comisiei pentru protecția informațiilor cu caracter personal;
- (ii) rezultatele unui control medical sau ale unei alte examinări (denumit în continuare „control medical etc.” la punctul următor) pentru prevenirea și depistarea precoce a unei boli, efectuat asupra persoanei principale de către un medic sau de o altă persoană cu atribuții legate de medicină [denumit(ă) în continuare „medic etc.” la punctul următor];
- (iii) faptul că persoana principală a primit îndrumări, asistență medicală sau rețete de la un medic etc. pentru îmbunătățirea stării mintale și fizice, pe baza rezultatelor unui control medical etc. sau din motive de boală, vătămare sau alte evoluții mintale și fizice;
- (iv) faptul că persoana principală a făcut obiectul unei arestări, al unei percheziții, al unui sechestru, al unei rețineri, al începerii urmăririi penale sau al altor proceduri legate de o cauză penală, în calitate de suspect sau pârât;

⁽²⁾ Prin motiv legitim se înțelege un eveniment de natură extraordinară în afara controlului operatorului economic care gestionează informații cu caracter personal, care nu poate fi prevăzut în mod rezonabil (de exemplu, dezastre naturale) sau cazurile în care necesitatea de a lua măsuri cu privire la o recomandare emisă de Comisia pentru protecția informațiilor cu caracter personal în temeiul articolului 42 alineatul (1) din lege a dispărut deoarece operatorul economic care gestionează informații cu caracter personal a întreprins acțiuni alternative care remediază pe deplin încălcarea.

- (v) faptul că persoana principală a făcut obiectul unei investigații, al unei măsuri de observare și protecție, al unei audieri și al unei decizii, al unei măsuri de protecție sau al altor proceduri legate de o cauză de protecție a minorilor, în calitate de delincvent juvenil sau de persoană suspectată în temeiul articolului 3 alineatul (1) din Legea privind minorii.

Articolul 5 din norme

Dizabilitățile fizice și mintale funcționale menționate de normele Comisiei pentru protecția informațiilor cu caracter personal în temeiul articolului 2 punctul (i) din ordin sunt următoarele:

- (i) dizabilitățile fizice menționate în tabelul anexat la Legea privind bunăstarea persoanelor cu dizabilități fizice (Legea nr. 283 din 1949);
- (ii) dizabilitățile intelectuale menționate în Legea privind bunăstarea persoanelor cu dizabilități intelectuale (Legea nr. 37 din 1960);
- (iii) dizabilitățile mintale menționate în Legea privind sănătatea mintală și bunăstarea persoanelor cu dizabilități mintale (Legea nr. 123 din 1950) [inclusiv dizabilitățile de dezvoltare prevăzute la articolul 2 alineatul (1) din Legea privind sprijinirea persoanelor cu dizabilități de dezvoltare, cu excepția dizabilităților intelectuale prevăzute de Legea privind bunăstarea persoanelor cu dizabilități intelectuale];
- (iv) o boală pentru care nu există metode de tratament stabilite sau alte boli rare a căror gravitate, stabilită prin ordinul Cabinetului la articolul 4 alineatul (1) din Legea privind sprijinul cuprinzător pentru viața cotidiană și socială a persoanelor cu dizabilități (Legea nr. 123 din 2005), este echivalentă cu cea prevăzută de Ministerul Sănătății, Muncii și Bunăstării la alineatul respectiv.

În cazul în care datele cu caracter personal primite din UE pe baza unei decizii privind caracterul adecvat al nivelului de protecție conțin date privind viața sexuală sau orientarea sexuală sau apartenența la un sindicat a unei persoane fizice, care sunt definite drept categorii speciale de date cu caracter personal în temeiul RGPD, un operator economic care gestionează informații cu caracter personal are obligația de a gestiona aceste date cu caracter personal în același mod prevăzut pentru informațiile cu caracter personal care necesită o atenție specială în sensul articolului 2 alineatul (3) din lege.

2. Datele cu caracter personal păstrate [articolul 2 alineatul (7) din lege]

Articolul 2 alineatul (7) din lege

- (7) „Datele cu caracter personal păstrate”, în sensul prezentei legi, înseamnă datele cu caracter personal pe care un operator economic care gestionează informații cu caracter personal are autoritatea de a le divulga, corecta, adăuga sau șterge, pe care acesta poate înceta să le utilizeze, le poate elimina sau pe care poate înceta să le furnizeze terților și care nu fac parte din datele considerate de ordinul Cabinetului ca fiind de natură să aducă atingere intereselor publice sau de alt tip în cazul în care se face cunoscută prezența sau absența acestor date, nici datele a căror ștergere se efectuează în termen de maximum un an, astfel cum se prevede în ordinul Cabinetului.

Articolul 4 din ordinul Cabinetului

Datele prevăzute prin ordinul Cabinetului la articolul 2 alineatul (7) sunt următoarele:

- (i) datele în legătură cu care există posibilitatea, în cazul în care se face cunoscută prezența sau absența datelor cu caracter personal menționate, să dăuneze vieții, integrității fizice sau bunurilor unei persoane principale sau unei părți terțe;
- (ii) datele în legătură cu care există posibilitatea, în cazul în care se face cunoscută prezența sau absența datelor cu caracter personal menționate, să încurajeze sau să inducă un act ilegal sau nedrept;
- (iii) datele în legătură cu care există posibilitatea, în cazul în care se face cunoscută prezența sau absența datelor cu caracter personal menționate, să submineze securitatea națională, să distrugă o relație de încredere cu o țară străină ori cu o organizație internațională sau să cauzeze un prejudiciu în negocierile cu o țară străină sau cu o organizație internațională;
- (iv) datele în legătură cu care există posibilitatea, în cazul în care se face cunoscută prezența sau absența datelor cu caracter personal menționate, să împiedice menținerea siguranței și a ordinii publice, cum ar fi prevenirea, reprimarea sau investigarea unei infracțiuni.

Articolul 5 din ordinul Cabinetului

Perioada prevăzută prin ordinul Cabinetului la articolul 2 alineatul (7) din lege este de șase luni.

Datele cu caracter personal primite din UE pe baza unei decizii privind caracterul adecvat al nivelului de protecție trebuie gestionate ca date cu caracter personal păstrate în sensul articolului 2 alineatul (7) din lege, indiferent de perioada în care se prevede ștergerea acestora.

În cazul în care datele cu caracter personal primite din UE pe baza unei decizii privind caracterul adecvat al nivelului de protecție se încadrează în domeniul de aplicare al datelor cu caracter personal prevăzute de ordinul Cabinetului ca fiind „de natură să aducă atingere intereselor publice sau de alt tip în cazul în care se face cunoscută prezența sau absența acestor date”, nu se impune gestionarea datelor respective drept date cu caracter personal păstrate (a se vedea articolul 4 din ordinul Cabinetului; orientările privind normele generale, „2-7. Datele cu caracter personal păstrate”).

3. Specificarea unui scop al utilizării, a unei restricții ca urmare a utilizării [articolul 15 alineatul (1), articolul 16 alineatul (1) și articolul 26 alineatele (1) și (3) din lege]

Articolul 15 alineatul (1) din lege

- (1) Atunci când prelucrează informații cu caracter personal, un operator economic care gestionează informații cu caracter personal specifică scopul utilizării informațiilor cu caracter personal (denumit în continuare „scopul utilizării”), cât mai explicit posibil.

Articolul 16 alineatul (1) din lege

- (1) Un operator economic care gestionează informații cu caracter personal nu gestionează informații cu caracter personal fără a obține în avans, din partea persoanei principale, un consimțământ care să depășească ceea ce este necesar pentru a atinge un scop al utilizării specificat în temeiul dispozițiilor de la articolul precedent.

Articolul 26 alineatele (1) și (3) din lege

- (1) Atunci când primește date cu caracter personal de la o parte terță, un operator economic care gestionează informații cu caracter personal confirmă aspectele expuse în cele ce urmează, în conformitate cu normele Comisiei pentru protecția informațiilor cu caracter personal: (text omis)

(i) (text omis);

(ii) circumstanțele în care respectivele date cu caracter personal au fost dobândite de către partea terță menționată anterior.

- (3) Atunci când a efectuat confirmarea în temeiul dispozițiilor alineatului (1), un operator economic care gestionează informații cu caracter personal păstrează, în temeiul normelor Comisiei pentru protecția informațiilor cu caracter personal, un registru cu data la care a primit datele cu caracter personal, un element referitor la respectiva confirmare, precum și alte aspecte prevăzute de normele Comisiei pentru protecția informațiilor cu caracter personal.

În cazul în care un operator economic care gestionează informații cu caracter personal gestionează informații cu caracter personal depășind ceea ce este necesar pentru a atinge unul dintre obiectivele utilizării specificate la articolul 15 alineatul (1) din lege, acesta trebuie să obțină în prealabil consimțământul relevant al persoanei principale [articolul 16 alineatul (1) din lege]. Atunci când primește date cu caracter personal de la o parte terță, un operator economic care gestionează informații cu caracter personal confirmă, în temeiul normelor, aspecte precum circumstanțele în care aceste date cu caracter personal au fost dobândite de către partea terță respectivă, și ține o evidență a acestor aspecte [articolul 26 alineatele (1) și (3) din lege].

În cazul în care un operator economic care gestionează informații cu caracter personal primește date cu caracter personal din UE pe baza unei decizii privind caracterul adecvat al nivelului de protecție, circumstanțele dobândirii acestor date cu caracter personal, care trebuie confirmate și luate în evidență în conformitate cu articolul 26 alineatele (1) și (3), includ scopul utilizării pentru care au fost primite din UE.

În mod similar, în cazul în care un operator economic care gestionează informații cu caracter personal primește de la un alt operator economic care gestionează informații cu caracter personal date cu caracter personal transferate anterior din UE pe baza unei decizii privind caracterul adecvat al nivelului de protecție, circumstanțele dobândirii acestor date cu caracter personal, care trebuie confirmate și luate în evidență în conformitate cu articolul 26 alineatele (1) și (3), includ scopul utilizării pentru care au fost primite datele.

În cazurile menționate mai sus, operatorul economic care gestionează informații cu caracter personal trebuie să specifice scopul utilizării acestor date cu caracter personal în cadrul domeniului de aplicare al scopului utilizării pentru care datele au fost primite inițial sau ulterior, astfel cum au fost confirmate și luate în evidență în temeiul articolului 26 alineatele (1) și (3), și să utilizeze aceste date în limitele domeniului de aplicare respectiv [în conformitate cu articolul 15 alineatul (1) și cu articolul 16 alineatul (1) din lege].

4. Restricții privind furnizarea către o parte terță într-o țară străină (articolul 24 din lege; articolul 11-2 din norme)

Articolul 24 din lege

Un operator economic care gestionează informații cu caracter personal, cu excepția cazurilor prevăzute la fiecare dintre punctele de la alineatul (1) din articolul precedent, are obligația, în cazul în care furnizează date cu caracter personal unei părți terțe (cu excepția unei persoane care instituie un sistem ce respectă standardele prevăzute de normele Comisiei pentru protecția informațiilor cu caracter personal ca fiind necesare pentru adoptarea continuă de măsuri echivalente cu cele pe care le adoptă un operator economic care gestionează informații cu caracter personal în ceea ce privește gestionarea de date cu caracter personal în temeiul dispozițiilor din prezenta secțiune; denumită în continuare în același fel în prezentul articol) într-o țară străină (însemnând o țară sau o regiune situată în afara teritoriului Japoniei; denumită în continuare în același fel) (cu excepția celor pe care normele Comisiei pentru protecția informațiilor cu caracter personal le definesc drept o țară străină care a instituit un sistem de protecție a informațiilor cu caracter personal recunoscut ca având standarde echivalente cu cele din Japonia în ceea ce privește protecția drepturilor și intereselor persoanelor fizice; denumită în continuare în același fel în prezentul articol), să obțină în prealabil consimțământul persoanei principale potrivit căruia aceasta aprobă furnizarea către o parte terță într-o țară străină. În acest caz, dispozițiile articolului precedent nu se aplică.

Articolul 11-2 din norme

Standardele prevăzute de normele Comisiei pentru protecția informațiilor cu caracter personal în temeiul articolului 24 din lege se încadrează la unul dintre următoarele puncte:

- (i) un operator economic care gestionează informații cu caracter personal și o persoană căreia îi sunt furnizate date cu caracter personal au pus în aplicare, în ceea ce privește gestionarea datelor cu caracter personal de către persoana căreia îi sunt furnizate datele, măsuri conforme cu dispozițiile prevăzute în capitolul IV secțiunea 1 din lege, utilizând o metodă adecvată și rezonabilă;
- (ii) o persoană căreia îi sunt furnizate date cu caracter personal a obținut, sub o formă sau alta, o recunoaștere în baza unui cadru internațional privind gestionarea informațiilor cu caracter personal.

În cazul în care furnizează unei părți terțe dintr-o țară străină datele cu caracter personal pe care le-a primit din UE pe baza unei decizii privind caracterul adecvat al nivelului de protecție, un operator economic care gestionează informații cu caracter personal obține în prealabil consimțământul persoanei principale potrivit căruia aceasta aprobă furnizarea către o parte terță dintr-o țară străină în temeiul articolului 24 din lege, după ce persoana principală a primit informații privind circumstanțele transferului necesare pentru ca aceasta să ia o decizie cu privire la consimțământul său, cu excepția cazurilor care se încadrează la unul din următoarele puncte (i)-(iii):

- (i) în cazul în care partea terță se află într-o țară care, conform normelor, este o țară străină care a instituit un sistem de protecție a informațiilor cu caracter personal recunoscut ca având standarde echivalente cu cele din Japonia în ceea ce privește protecția drepturilor și intereselor persoanelor fizice;
- (ii) în cazul în care un operator economic care gestionează informații cu caracter personal și partea terță căreia îi sunt furnizate datele cu caracter personal au pus împreună în aplicare, în ceea ce privește gestionarea datelor cu caracter personal de către partea terță, măsuri care să asigure un nivel de protecție echivalent cu cel prevăzut de lege, în coroborare cu prezentele norme, utilizând o metodă adecvată și rezonabilă (adică prin încheierea unui contract, a altor forme de acord cu caracter obligatoriu sau a unor acorduri cu caracter obligatoriu în cadrul unui grup de întreprinderi);
- (iii) în cazurile care se încadrează la oricare punct de la alineatul (1) al articolului 23 din lege.

5. Informații prelucrate anonim [articolul 2 alineatul (9) și articolul 36 alineatele (1) și (2) din lege]

Articolul 2 alineatul (9) din lege

- (9) „Informații prelucrate anonim”, în sensul prezentei legi, înseamnă informațiile referitoare la o persoană care pot fi produse în urma prelucrării informațiilor cu caracter personal, astfel încât să fie imposibilă identificarea unei anumite persoane prin măsurile prevăzute la oricare dintre punctele următoare, în conformitate cu repartizarea informațiilor cu caracter personal prevăzută la fiecare din punctele menționate anterior, și să fie imposibilă restabilirea informațiilor cu caracter personal:

- (i) informațiile cu caracter personal care se încadrează la alineatul (1) punctul (i); ștergerea unei părți a descrierilor etc. conținute în informațiile cu caracter personal respective (inclusiv înlocuirea acelei părți a descrierilor etc. cu alte descrieri etc. cu ajutorul unei metode fără regularitate care să permită restabilirea acelei părți a descrierilor etc.);
- (ii) informațiile cu caracter personal care se încadrează la alineatul (1) punctul (ii); ștergerea tuturor codurilor individuale de identificare conținute în informațiile cu caracter personal respective (inclusiv înlocuirea acelor coduri individuale de identificare cu alte descrieri etc. cu ajutorul unei metode fără regularitate care să permită restabilirea acelor coduri individuale de identificare).

Articolul 36 alineatul (1) din lege

- (1) Un operator economic care gestionează informații cu caracter personal, atunci când produce informații prelucrate anonim (care se limitează la cele care constituie o bază de date cu informații prelucrate anonim etc.; denumite în continuare în același fel), prelucrează informațiile cu caracter personal în conformitate cu standardele prevăzute de normele Comisiei pentru protecția informațiilor cu caracter personal ca fiind necesare pentru a face imposibilă identificarea unei anumite persoane și restabilirea informațiilor cu caracter personal utilizate pentru producție.

Articolul 19 din norme

Standardele prevăzute de normele Comisiei pentru protecția informațiilor cu caracter personal în temeiul articolului 36 alineatul (1) din lege sunt următoarele:

- (i) ștergerea integrală sau a unei părți a acelor descrieri etc. care pot identifica o anumită persoană conținute în informațiile cu caracter personal (inclusiv înlocuirea acelor descrieri etc. cu alte descrieri etc. cu ajutorul unei metode fără regularitate care să permită restabilirea integrală sau a unei părți a descrierilor etc.);
- (ii) ștergerea tuturor codurilor individuale de identificare conținute în informațiile cu caracter personal (inclusiv înlocuirea acelor coduri cu alte descrieri etc. cu ajutorul unei metode fără regularitate care să permită restabilirea codurilor individuale de identificare);
- (iii) ștergerea acestor coduri (care se limitează la codurile care corelează reciproc informațiile multiple gestionate efectiv de către un operator economic care gestionează informații cu caracter personal) care corelează informațiile cu caracter personal și informațiile obținute prin luarea unor măsuri privind informațiile cu caracter personal (inclusiv înlocuirea acestor coduri cu alte coduri care nu pot corela informațiile cu caracter personal respective și informațiile obținute prin luarea de măsuri privind informațiile cu caracter personal respective, utilizând o metodă fără regularitate care să permită restabilirea codurilor în cauză);
- (iv) ștergerea descrierilor idiosincratice etc. (inclusiv înlocuirea acestor descrieri etc. cu alte descrieri etc., utilizând o metodă fără regularitate care să permită restabilirea descrierilor idiosincratice etc.);
- (v) pe lângă măsurile prevăzute la fiecare dintre punctele precedente, luarea de măsuri corespunzătoare pe baza rezultatelor obținute în urma examinării caracteristicilor etc. bazei de date cu caracter personal etc., cum ar fi o diferență între descrierile etc. conținute în informațiile cu caracter personal și descrierile etc. conținute în alte informații cu caracter personal care constituie o bază de date cu caracter personal etc. cuprinzând informațiile cu caracter personal respective.

Articolul 36 alineatul (2) din lege

- (2) Atunci când produce informații care au fost prelucrate anonim, un operator economic care gestionează informații cu caracter personal trebuie să ia măsurile necesare pentru controlul de securitate al respectivelor informații, în conformitate cu standardele care au fost prevăzute de normele Comisiei pentru protecția informațiilor cu caracter personal ca fiind necesare pentru a preveni scurgerea de informații referitoare la descrierile respective etc. și a codurilor individuale de identificare eliminate din informațiile cu caracter personal utilizate pentru a produce informațiile prelucrate în mod anonim, precum și scurgerea de informații referitoare la metoda de prelucrare utilizată în conformitate cu dispozițiile alineatului precedent.

Articolul 20 din Norme

Standardele prevăzute de normele Comisiei pentru protecția informațiilor cu caracter personal în temeiul articolului 36 alineatul (2) din lege sunt următoarele:

- (i) definirea clară a autorității și a responsabilității persoanelor care gestionează informații cu privire la acele descrieri etc. și la codurile individuale de identificare care au fost șterse din informațiile cu caracter personal utilizate pentru a produce informații prelucrate anonim, precum și informații cu privire la metoda de prelucrare utilizată în temeiul dispozițiilor articolului 36 alineatul (1) (este vorba doar de acele informații care pot restabili informațiile cu caracter personal prin utilizarea unor astfel de informații conexe) (denumite în continuare, în acest articol, „informații referitoare la metoda de prelucrare etc.”);
- (ii) stabilirea de norme și proceduri privind gestionarea informațiilor referitoare la metoda de prelucrare etc., gestionarea corespunzătoare a informațiilor referitoare la metoda de prelucrare etc., în conformitate cu normele și procedurile, evaluarea situației gestionării și, pe baza rezultatelor evaluării, luarea măsurilor necesare pentru a aduce îmbunătățiri;
- (iii) luarea măsurilor necesare și adecvate pentru a împiedica o persoană care are autoritatea legitimă de a gestiona informații referitoare la metoda de prelucrare etc. să gestioneze informații referitoare la metoda de prelucrare etc.

Informațiile cu caracter personal primite din UE pe baza unei decizii privind caracterul adecvat al nivelului de protecție sunt considerate informații prelucrate anonim în sensul articolului 2 alineatul (9) din lege numai în cazul în care operatorul economic care gestionează informații cu caracter personal ia măsuri care fac ca imposibilitatea de a identifica persoana să fie ireversibilă pentru oricine, procedând astfel inclusiv prin ștergerea informațiilor referitoare la metoda de prelucrare etc. [este vorba de informațiile referitoare la descrierile respective etc. și la codurile individuale de identificare care au fost șterse din informațiile cu caracter personal utilizate pentru a produce informații prelucrate în mod anonim, precum și de informațiile privind metoda de prelucrare utilizată în temeiul dispozițiilor articolului 36 alineatul (1) din lege (limitate doar la acele informații care pot restabili informațiile cu caracter personal prin utilizarea unor astfel de informații conexe)].

ANEXA 2

Excelenței sale doamna Věra Jourová, comisar pentru justiție, consumatori și egalitate de gen a Comisiei Europene

Excelență,

Salut discuțiile constructive dintre Japonia și Comisia Europeană care vizează crearea cadrului pentru transferul reciproc de date cu caracter personal între Japonia și UE.

La cererea Comisiei Europene adresată guvernului Japoniei, trimit un document anexat, care oferă o imagine de ansamblu a cadrului juridic privind accesul la informații al guvernului Japoniei.

Acest document se referă la numeroase ministere și agenții ale Guvernului Japoniei, iar în ceea ce privește conținutul documentului, fiecare minister și agenție relevantă (Secretariatul Cabinetului, Agenția Națională de Poliție, Comisia pentru protecția informațiilor cu caracter personal, Ministerul Afacerilor Interne și al Comunicațiilor, Ministerul Justiției, Agenția de Informații pentru Securitate Publică, Ministerul Apărării) este responsabilă de pasajele din propria sferă de competență. Mai jos găsiți ministerele și agențiile relevante, precum și semnăturile aferente.

Comisia pentru protecția informațiilor cu caracter personal acceptă toate întrebările privind acest document și va coordona răspunsurile necesare în rândul ministerelor și al agențiilor relevante.

Sper ca acest document să fie util pentru luarea deciziilor la nivelul Comisiei Europene.

Apreciez contribuția importantă pe care ați adus-o până în prezent în acest domeniu.

Cu stimă,

Yoko Kamikawa

Ministrul Justiției

Acest document a fost elaborat de Ministerul Justiției și de următoarele ministere și agenții:

Koichi Hamano

Consilier, Secretariatul Cabinetului

Schunichi Kuryu

Comisarul general al Agenției Naționale de Poliție

Mari Sonoda

Secretarul general al Comisiei pentru protecția informațiilor cu caracter personal

Mitsuru Yasuda

Viceministru, Ministerul Afacerilor Interne și al Comunicațiilor

Seimei Nakagawa

Agenția de Informații pentru Securitate Publică

Kenichi Takahashi

Viceministru administrativ al Apărării

14 septembrie 2018

Colectarea și utilizarea informațiilor cu caracter personal de către autoritățile publice japoneze pentru aplicarea legii penale și în scopuri de securitate națională

Următorul document oferă o imagine de ansamblu asupra cadrului juridic privind colectarea și utilizarea informațiilor cu caracter personal (în format electronic) de către autoritățile publice japoneze pentru aplicarea legii penale și în scopuri de securitate națională (denumit în continuare „accesul administrației publice”), în special în ceea ce privește temeiurile juridice disponibile, condițiile (limitările) și garanțiile aplicabile, inclusiv supravegherea independentă și posibilitățile de a recurge la căi de atac individuale. Această expunere este adresată Comisiei Europene cu scopul de a exprima un angajament și de a furniza asigurări cu privire la faptul că accesul administrației publice la informațiile cu caracter personal transferate din UE în Japonia se va limita la ceea ce este necesar și proporțional, sub rezerva unei supravegheri independente, și la faptul că persoanele vizate vor putea obține reparații în cazul oricărei posibile încălcări a dreptului lor fundamental la viață privată și la protecția datelor. Această expunere prevede, de asemenea, crearea unui nou mecanism de reparație individuală, administrat de Comisia pentru protecția informațiilor cu caracter personal (PPC), care să trateze plângerile cetățenilor din UE cu privire la accesul administrației publice la datele lor cu caracter personal transferate din UE în Japonia.

I. Principiile juridice generale relevante pentru accesul administrației publice

Ca exercițiu de autoritate publică, accesul administrației publice trebuie să se realizeze cu respectarea deplină a legii (principiul legalității). În Japonia, informațiile cu caracter personal sunt protejate atât în sectorul privat, cât și în sectorul public printr-un mecanism organizat pe mai multe niveluri.

A. Cadrul constituțional și principiul rezervei legii

Articolul 13 din Constituție și jurisprudența recunosc dreptul la viață privată ca drept constituțional. În acest sens, Curtea Supremă a statuat că este normal ca persoanele să nu dorească ca informațiile lor cu caracter personal să fie cunoscute de alte persoane fără un motiv întemeiat și că această așteptare trebuie protejată⁽¹⁾. Alte măsuri de protecție sunt consacrate la articolul 21 alineatul (2) din Constituție, care asigură respectarea secretului comunicațiilor, și la articolul 35 din Constituție, care garantează dreptul de a nu face obiectul perchezițiilor și al punerii sub sechestru fără mandat, ceea ce înseamnă că pentru colectarea informațiilor cu caracter personal prin mijloace obligatorii, inclusiv pentru accesul la aceste informații, este întotdeauna necesar un mandat judecătoresc. Un astfel de mandat poate fi emis numai pentru cercetarea unei infracțiuni deja comise. Prin urmare, în cadrul juridic japonez, colectarea informațiilor prin mijloace obligatorii în scopul securității naționale (și nu al unei anchete penale) nu este permisă.

În plus, în conformitate cu principiul rezervei legii, colectarea obligatorie a informațiilor trebuie să fie autorizată în mod specific prin lege. În cazul colectării neobligatorii/voluntare, informațiile se obțin dintr-o sursă care poate fi accesată în mod liber sau primită pe baza unei cereri de divulgare voluntară, adică a unei cereri care nu poate fi executată împotriva entității fizice sau juridice care deține informațiile. Cu toate acestea, acest lucru poate fi permis doar în măsura în care autoritatea publică este competentă să efectueze investigația, având în vedere faptul că fiecare autoritate publică poate acționa numai în limitele competenței sale administrative prevăzute de lege (indiferent dacă activitățile sale aduc sau nu atingere drepturilor și libertăților persoanelor). Acest principiu se aplică competenței autorității de a colecta informații cu caracter personal.

B. Norme specifice privind protecția informațiilor cu caracter personal

Legea privind protecția informațiilor cu caracter personal (APPI) și Legea privind protecția informațiilor cu caracter personal deținute de organele administrative (APPIHAO), care se bazează pe dispozițiile constituționale, detaliindu-le, garantează dreptul la informații cu caracter personal atât în sectorul privat, cât și în cel public.

Articolul 7 din APPI stipulează că PPC formulează „politica de bază privind protecția informațiilor cu caracter personal” („politica de bază”). Politica de bază, care este adoptată prin decizia Cabinetului Japoniei [ca organ central al guvernului japonez (primul-ministru și miniștrii de stat)], stabilește direcția privind protecția informațiilor cu caracter personal în Japonia. Astfel, PPC, în calitate de autoritate de supraveghere independentă, servește drept „centru de comandă” al sistemului japonez de protecție a informațiilor cu caracter personal.

Ori de câte ori colectează informații cu caracter personal și indiferent dacă fac sau nu acest lucru prin mijloace obligatorii, organele administrative trebuie, în principiu⁽²⁾, să respecte cerințele APPIHAO. APPIHAO este o lege generală aplicabilă prelucrării „informațiilor cu caracter personal păstrate”⁽³⁾ de „organele administrative” [astfel cum sunt definite la

⁽¹⁾ Curtea Supremă, Hotărârea din 12 septembrie 2003 [2002 (Ju) nr. 1656].

⁽²⁾ În ceea ce privește excepțiile referitoare la capitolul 4 din APPIHAO, a se vedea mai jos, pagina 16.

⁽³⁾ La articolul 2 alineatul (5) din APPIHAO «informații cu caracter personal păstrate» înseamnă informațiile cu caracter personal pregătite sau obținute de către un angajat al unui organ administrativ în exercitarea funcțiilor sale și păstrate de organul administrativ respectiv pentru uzul organizațional al angajaților săi.

articolul 2 alineatul (1) din APPIHAO]. Prin urmare, aceasta acoperă și prelucrarea datelor în domeniul aplicării legii penale și al securității naționale. Printre autoritățile publice care sunt autorizate să pună în aplicare accesul administrației publice, toate autoritățile, cu excepția poliției prefecturale, sunt autorități publice naționale care se încadrează în definiția „organelor administrative”. Prelucrarea informațiilor cu caracter personal de către poliția prefecturală este reglementată de ordonanțele prefecturale ⁽⁴⁾, care prevăd principii pentru protecția informațiilor cu caracter personal și drepturi și obligații echivalente cu cele prevăzute de APPIHAO.

II. Accesul administrației publice în scopul aplicării legii penale

A) Temeiuri juridice și limitări

1) Colectarea informațiilor cu caracter personal prin mijloace obligatorii

(a) Temeiuri juridice

În conformitate cu articolul 35 din Constituție, dreptul oricărei persoane la inviolabilitatea domiciliului, documentelor și efectelor (împotriva descinderilor, a perchezițiilor și a sechestrelor) nu poate fi afectat, cu excepția unui mandat care este emis pentru o „cauză adecvată” și în care se descrie în mod specific locul care urmează a fi percheziționat și obiectele care urmează a fi puse sub sechestru. Prin urmare, colectarea obligatorie a informațiilor electronice de către autoritățile publice în contextul unei anchete penale nu poate avea loc decât pe baza unui mandat. Acest lucru este valabil atât pentru colectarea de înregistrări electronice care conțin informații (cu caracter personal), cât și pentru interceptarea în timp real a comunicațiilor (denumită „interceptare a comunicațiilor”). Singura excepție de la această regulă (care însă nu este relevantă în contextul unui transfer electronic de informații cu caracter personal din străinătate) este articolul 220 alineatul (1) din Codul de procedură penală ⁽⁵⁾, potrivit căruia un procuror, un procuror-asistent sau un agent al poliției judiciare poate, atunci când arestează o persoană suspectată sau un infractor surprins în flagrant delict, să efectueze o percheziție și o punere sub sechestru „la fața locului în momentul arestării”, dacă acest lucru este necesar.

Articolul 197 alineatul (1) din Codul de procedură penală prevede că măsurile obligatorii de investigare „nu se aplică decât dacă au fost prevăzute dispoziții speciale în prezentul cod”. În ceea ce privește colectarea obligatorie a informațiilor electronice, temeiurile juridice relevante în această privință sunt articolul 218 alineatul (1) din Codul de procedură penală (conform căruia un procuror, un procuror-asistent sau un agent al poliției judiciare poate să efectueze percheziții, puneri sub sechestru sau inspecții, în cazul în care acest lucru este necesar pentru investigarea unei infracțiuni, pe baza unui mandat emis de un judecător) și articolul 222-2 din Codul de procedură penală (conform căruia măsurile obligatorii pentru interceptarea comunicațiilor electronice fără consimțământul uneia sau altelea dintre părți se execută pe baza altor acte legislative). Această din urmă dispoziție se referă la Legea privind interceptarea comunicațiilor pentru investigarea infracțiunilor („Legea privind interceptarea comunicațiilor”), care, la articolul 3 alineatul (1), prevede condițiile în care comunicațiile legate de anumite infracțiuni grave pot fi interceptate în baza unui mandat de interceptare a comunicațiilor emis de un judecător ⁽⁶⁾.

În ceea ce privește poliția, competența de investigare îi revine în toate cazurile poliției prefecturale, în timp ce Agenția Națională de Poliție (ANP) nu desfășoară anchete penale bazate pe Codul de procedură penală.

(b) Limitări

Colectarea obligatorie de informații în format electronic este limitată prin Constituție și legea de abilitare, astfel cum sunt interpretate în jurisprudență, care prevede, în special, criteriile pe care trebuie să le îndeplinească instanțele atunci când eliberează un mandat. În plus, APPIHAO impune o serie de limitări atât în ceea ce privește colectarea, cât și în ceea ce privește gestionarea informațiilor (în timp ce ordonanțele locale reproduc în esență aceleași criterii pentru poliția prefecturală).

(1) Limitări care decurg din Constituție și din legea de abilitare

În conformitate cu articolul 197 alineatul (1) din Codul de procedură penală, măsurile obligatorii nu se aplică decât dacă au fost prevăzute dispoziții speciale în respectivul cod. Articolul 218 alineatul (1) din Codul de procedură penală prevede

⁽⁴⁾ Fiecare prefectură are propria „ordonanță prefecturală” care se aplică protecției informațiilor cu caracter personal de către poliția prefecturală. Nu există traduceri în engleză pentru aceste ordonanțe prefecturale.

⁽⁵⁾ Articolul 220 alineatul (1) din Codul de procedură penală prevede că, atunci când un procuror, un procuror-asistent sau un agent al poliției judiciare arestează o persoană suspectată, acesta poate, dacă este necesar, să ia următoarele măsuri: (a) să intre în reședința unei alte persoane etc. pentru a căuta persoana suspectată; (b) să efectueze percheziții, puneri sub sechestru sau inspecții la fața locului în momentul arestării.

⁽⁶⁾ Mai precis, această dispoziție prevede că „procurorul sau poliția judiciară poate – în cazurile care intră sub incidența oricăruia dintre următoarele litere, dacă există o situație care oferă suficiente motive pentru a suspecta că vor avea loc comunicații referitoare la angajamente, pregătiri, conspirații privind unele acțiuni subsecvente, precum suprimarea dovezilor etc., instrucțiuni și alte tipuri de comunicare reciprocă a infracțiunilor prevăzute la fiecare dintre literele menționate (denumite în continuare «o serie de infracțiuni» la a doua și a treia literă), precum și comunicații care se referă la chestiuni legate de respectivele infracțiuni (denumite «comunicații legate de infracțiuni» în prezentul paragraf), și în cazurile în care este extrem de dificil să se identifice infractorul sau să se clarifice situațiile/detaliile săvârșirii infracțiunii prin alte căi – să intercepteze comunicațiile legate de infracțiuni, pe baza unui mandat de interceptare a comunicațiilor emis de un judecător, cu privire la un mijloc de comunicare, care este specificat prin numărul de telefon și prin alte numere/coduri de identificare a sursei sau destinației telefonului respectiv și care este utilizat de persoana suspectată în baza contractului cu societățile de telecomunicații etc. (cu excepția comunicațiilor care nu sunt suspectate drept «comunicații legate de infracțiuni»), precum și cu privire la mijloacele de comunicare care sunt suspectate a fi utilizate pentru «comunicații legate de infracțiuni», iar interceptarea comunicațiilor legate de infracțiuni poate fi realizată prin respectivul mijloc de comunicare.”

că punerea sub sechestru etc. poate fi efectuată pe baza unui mandat emis de un judecător numai „dacă acest lucru este necesar pentru investigarea unei infracțiuni”. Deși criteriile pentru evaluarea necesității nu sunt specificate mai detaliat în dreptul material, Curtea Supremă ⁽⁷⁾ a hotărât că, atunci când evaluează necesitatea dispozițiilor, judecătorul ar trebui să efectueze o evaluare globală, luând în considerare, în special, următoarele elemente:

- (a) gravitatea infracțiunii și modul în care a fost comisă;
- (b) valoarea și importanța materialelor puse sub sechestru pentru a servi drept dovezi;
- (c) probabilitatea de ascundere sau distrugere a materialelor puse sub sechestru;
- (d) amploarea dezavantajelor cauzate de o punere sub sechestru;
- (e) alte condiții conexe.

Limitările decurg, de asemenea, din cerința de la articolul 35 din Constituție de a prezenta „cauza adecvată”. În temeiul criteriului „cauzei adecvate” se pot emite mandate în cazul în care: [1] este necesară o anchetă penală (a se vedea Hotărârea Curții Supreme din 18 martie 1969 [1968 (Shi) nr. 100] menționată mai sus), [2] există o situație în care se consideră că persoana suspectată (persoana acuzată) a comis o infracțiune [articolul 156 alineatul (1) din normele de procedură penală] ⁽⁸⁾, [3] mandatul de investigare corporală sau de investigare a efectelor, a reședinței unei persoane, alta decât persoana acuzată, sau a oricărui alt loc în care se află aceasta ar trebui emis numai în cazul în care există motive rezonabile de a presupune că există obiecte care ar trebui puse sub sechestru [articolul 102 alineatul (2) din Codul de procedură penală]. În cazul în care un judecător consideră că documentele justificative prezentate de autoritățile de investigare nu prezintă motive suficiente pentru a suspecta săvârșirea unei infracțiuni, acesta va respinge cererea de obținere a unui mandat. În această privință, ar trebui remarcat faptul că, în conformitate cu Legea privind pedepsirea criminalității organizate și controlul produselor provenite din săvârșirea de infracțiuni, „actele pregătitoare înainte de săvârșirea” unei infracțiuni planificate (de exemplu, pregătirea banilor pentru comiterea unei infracțiuni de terorism) constituie ele însele o infracțiune și, prin urmare, pot face obiectul unei anchete obligatorii bazate pe un mandat.

În fine, în cazul în care mandatul se referă la o investigare corporală sau la investigarea efectelor și reședinței unei persoane, alta decât persoana suspectată sau persoana acuzată, sau a oricărui alt loc în care se află aceasta, mandatul respectiv se eliberează numai atunci când există motive rezonabile de a presupune că obiectele care vor fi confiscate există [articolul 102 alineatul (2) și articolul 222 alineatul (1) din Codul de procedură penală].

În ceea ce privește în mod specific interceptarea comunicațiilor în scopul anchetelor penale pe baza Legii privind interceptarea comunicațiilor, această interceptare poate fi efectuată numai atunci când sunt îndeplinite cerințele stricte prevăzute la articolul 3 alineatul (1) din legea menționată. În conformitate cu respectiva dispoziție, interceptarea necesită întotdeauna obținerea în prealabil a unui mandat judecătoresc, care poate fi emis numai în situații limitate ⁽⁹⁾.

(2) Limitări care decurg din APPIHAO

În ceea ce privește colectarea ⁽¹⁰⁾ și gestionarea ulterioară a informațiilor cu caracter personal (inclusiv, în special, păstrarea, gestionarea și utilizarea) de către organele administrative, APPIHAO prevede următoarele limitări:

- (a) În conformitate cu articolul 3 alineatul (1) din APPIHAO, organele administrative pot păstra informații cu caracter personal numai în cazul în care păstrarea este necesară pentru desfășurarea activităților care intră în domeniul lor de competență în temeiul actelor cu putere de lege și al normelor administrative. În cazul păstrării informațiilor, organelor respective li se solicită, de asemenea, să specifice (cât mai mult posibil) scopul utilizării informațiilor cu caracter personal. În conformitate cu articolul 3 alineatele (2) și (3) din APPIHAO, organele administrative nu păstrează informații cu caracter personal dincolo de ceea ce este necesar pentru îndeplinirea scopului de utilizare specificat și nu modifică scopul utilizării dincolo de ceea ce poate fi considerat în mod rezonabil ca fiind relevant pentru scopul inițial.
- (b) Articolul 5 din APPIHAO prevede că șeful unui organ administrativ depune eforturi pentru a se asigura că informațiile cu caracter personal păstrate sunt exacte și actualizate, în măsura necesară pentru realizarea scopului utilizării.
- (c) Articolul 6 alineatul (1) din APPIHAO prevede că șeful unui organ administrativ ia măsurile necesare pentru a preveni scurgerile, pierderile sau daunele, precum și pentru a gestiona în mod corespunzător informațiile cu caracter personal păstrate.
- (d) În conformitate cu articolul 7 din APPIHAO, niciun angajat (inclusiv fost angajat) nu comunică unei alte persoane, fără motive întemeiate, informațiile cu caracter personal obținute și nici nu utilizează aceste informații în scopuri nedrepte.

⁽⁷⁾ Hotărârea din 18 martie 1969 [1968 (Shi) nr. 100].

⁽⁸⁾ Articolul 156 alineatul (1) din normele de procedură penală prevede următoarele: „La depunerea cererii prevăzute la alineatul (1) de la articolul precedent, solicitantul furnizează materiale pe baza cărora ar trebui să se considere că persoana suspectată sau persoana acuzată a comis o infracțiune.”

⁽⁹⁾ A se vedea nota de subsol 6.

⁽¹⁰⁾ Articolul 3 alineatele (1) și (2) din APPIHAO limitează gradul de păstrare și, prin urmare, de colectare a informațiilor cu caracter personal.

- (e) În plus, articolul 8 alineatul (1) din APPPHAO prevede că șeful unui organ administrativ nu poate utiliza sau pune la dispoziția unei alte persoane, în alte scopuri decât scopul specificat de utilizare, informații cu caracter personal păstrate, decât dacă există dispoziții contrare prevăzute de acte cu putere de lege și acte administrative. Deși articolul 8 alineatul (2) conține excepții de la această regulă în situații specifice, acestea se aplică numai dacă o astfel de divulgare excepțională nu este susceptibilă de a provoca un prejudiciu „nedrept” drepturilor și intereselor persoanei vizate sau ale unei părți terțe.
- (f) În conformitate cu articolul 9 din APPHIAO, în cazul în care informațiile cu caracter personal păstrate sunt furnizate unei alte persoane, șeful unui organ administrativ impune, dacă este necesar, restricții privind scopul utilizării sau modalitatea de utilizare, precum și orice alte restricții necesare; de asemenea, acesta poate solicita persoanei destinatar să ia măsurile necesare pentru prevenirea scurgerilor și pentru buna gestionare a informațiilor.
- (g) Articolul 48 din APPHIAO prevede că șeful unui organ administrativ depune eforturi pentru a prelucra în mod corespunzător și rapid orice plângere referitoare la gestionarea informațiilor cu caracter personal.

2) Colectarea de informații cu caracter personal prin cereri de cooperare voluntară (investigație voluntară)

(a) *Temei juridic*

În afara utilizării mijloacelor obligatorii, informațiile cu caracter personal sunt obținute fie dintr-o sursă care poate fi accesată în mod liber, fie pe baza divulgării voluntare, efectuate inclusiv de către operatorii economici care dețin astfel de informații.

În ceea ce privește ultima modalitate, articolul 197 alineatul (2) din Codul de procedură penală abilitază organele de urmărire penală și poliția judiciară să efectueze „solicitări de informații scrise în materie de investigații” (așa-numitele „fișe de solicitare de informații”). În conformitate cu Codul de procedură penală, persoanele cărora li se adresează solicitările trebuie să raporteze acest lucru autorităților de investigare. Cu toate acestea, în cazul în care funcționarii publici sau organizațiile publice și/sau private care au primit solicitările refuză să raporteze, nu există nicio posibilitate de a îi obliga să se conformeze acestei cerințe. În cazul în care aceștia nu raportează solicitările, nu se pot impune sancțiuni penale sau alte sancțiuni. În cazul în care consideră că informațiile solicitate sunt indispensabile, autoritățile de investigare vor trebui să obțină informațiile prin percheziții și puneri sub sechestru efectuate pe baza unui mandat judecătoresc.

Având în vedere gradul de conștientizare din ce în ce mai ridicat cu privire la drepturile la viață privată, precum și volumul de muncă generat de astfel de solicitări, operatorii economici sunt din ce în ce mai precauți în răspunsurile pe care le oferă în cazul acestor solicitări ⁽¹¹⁾. Pentru a decide dacă să coopereze, operatorii economici (mai ales) țin seama de natura informațiilor solicitate, de relația lor cu persoana ale cărei informații sunt vizate, de riscurile pentru reputație, de riscurile de litigiu etc.

(b) *Limitări*

În ceea ce privește colectarea obligatorie a informațiilor în format electronic, investigațiile voluntare sunt limitate de Constituție, astfel cum este interpretată în jurisprudență, precum și de legea de abilitare. În plus, operatorii economici nu au dreptul legal de a divulga informații în anumite situații. În fine, APPHIAO prevede o serie de limitări atât în ceea ce privește colectarea, cât și în ceea ce privește gestionarea informațiilor (în timp ce ordonanțele locale reproduc în esență aceleași criterii pentru poliția prefectorală).

(1) Limitări care decurg din Constituție și din legea de abilitare

Luând în considerare scopul articolului 13 din Constituție, în două decizii din 24 decembrie 1969 [1965 (A) nr. 1187] și, respectiv, din 15 aprilie 2008 [2007 (A) nr. 839], Curtea Supremă a impus limite în ceea ce privește investigațiile voluntare efectuate de autoritățile de investigare. Deși aceste decizii au vizat cazuri în care s-au colectat informații cu caracter personal (sub formă de imagini) prin fotografiere/filmare, constatările sunt relevante pentru investigațiile voluntare (neobligatorii) care interferează cu viața privată a unei persoane în general. Prin urmare, aceste limitări se aplică și trebuie să fie respectate în ceea ce privește colectarea de informații cu caracter personal prin investigații voluntare, ținând seama de circumstanțele specifice fiecărui caz.

În conformitate cu deciziile respective, legalitatea investigației voluntare depinde de îndeplinirea a trei criterii, și anume:

- „existența unei suspiciuni privind săvârșirea unei infracțiuni” (trebuie să se evalueze dacă s-a comis o infracțiune);
- „necesitatea investigației” (trebuie să se evalueze dacă solicitarea rămâne în sfera a ceea ce este necesar în scopul investigației); și

⁽¹¹⁾ A se vedea, de asemenea, notificarea emisă de Agenția Națională de Poliție la 7 decembrie 1999 (la punctul 9 de mai jos) care furnizează aceeași indicație.

— „caracterul adecvat al metodelor” (trebuie să se evalueze dacă investigația voluntară este „adecvată” sau rezonabilă pentru a atinge scopul investigației) ⁽¹²⁾.

În general, ținând seama de cele trei criterii de mai sus, legalitatea investigației voluntare este evaluată din perspectiva necesității de a se stabili dacă aceasta poate fi considerată rezonabilă în conformitate cu convențiile acceptate de societate.

Cerința ca investigația să fie „necesară” decurge, de asemenea, direct din articolul 197 din Codul de procedură penală și a fost confirmată în instrucțiunile adresate de Agenția Națională de Poliție (ANP) poliției prefectorale în ceea ce privește utilizarea „fișelor de solicitare de informații”. Notificarea ANP din 7 decembrie 1999 prevede o serie de limitări procedurale, inclusiv cerința de a utiliza „fișele de solicitare de informații” numai în cazul în care acest lucru este necesar în scopul investigației. În plus, articolul 197 alineatul (1) din Codul de procedură penală se limitează la anchetele penale și, prin urmare, poate fi aplicat numai în cazul în care există o suspiciune concretă privind o infracțiune care a fost deja comisă. În schimb, acest temei juridic nu este valabil pentru colectarea și utilizarea informațiilor cu caracter personal în cazul în care nu s-a produs încă nicio încălcare a legii.

(2) Limitări referitoare la anumiți operatori economici

În anumite domenii se aplică limitări suplimentare, pe baza măsurilor de protecție prevăzute în alte legi.

În primul rând, autoritățile de investigare, precum și societățile de telecomunicații care dețin informații cu caracter personal au obligația de a respecta secretul comunicațiilor, astfel cum este garantat de articolul 21 alineatul (2) din Constituție ⁽¹³⁾. În plus, la articolul 4 din Legea privind activitățile de telecomunicații este prevăzută aceeași obligație pentru societățile de telecomunicații ⁽¹⁴⁾. În conformitate cu „Orientările privind protecția informațiilor cu caracter personal în sectorul telecomunicațiilor”, emise de Ministerul Afacerilor Interne și al Comunicațiilor (MIC) în temeiul Constituției și al Legii privind activitățile de telecomunicații, în cazurile în care secretul comunicațiilor este în joc, societățile de telecomunicații nu trebuie să divulge terților informații cu caracter personal privind secretul comunicării, cu excepția cazului în care au obținut consimțământul persoanei în cauză sau dacă se pot baza pe una dintre „cauzele justificabile” pentru nerespectarea Codului penal. Acestea din urmă se referă la „acte justificabile” (articolul 35 din Codul penal), „autoapărare” (articolul 36 din Codul penal) și „evitarea unui pericol imediat” (articolul 37 din Codul penal). „Actele justificabile” prevăzute în Codul penal sunt doar acele acte ale unei societăți de telecomunicații prin care aceasta respectă măsurile obligatorii ale statului, din care investigația voluntară nu face parte. Prin urmare, dacă autoritățile de investigare solicită informații cu caracter personal pe baza unei „fișe de solicitare de informații” [articolul 197 alineatul (2) din Codul de procedură penală], divulgarea datelor de către o societate de telecomunicații este interzisă.

În al doilea rând, operatorii economici au obligația de a refuza cererile de cooperare voluntară în cazul în care legea le interzice să divulge informații cu caracter personal. Sunt incluse cazurile în care operatorul are obligația de a respecta confidențialitatea informațiilor, de exemplu în temeiul articolului 134 din Codul penal ⁽¹⁵⁾.

(3) Limitări bazate pe APPIHAO

În ceea ce privește colectarea și prelucrarea ulterioară a informațiilor cu caracter personal de către organele administrative, APPIHAO prevede limitări, astfel cum se explică mai sus în secțiunea II partea A punctul 1 litera (b) subpunctul 2. Limitări echivalente rezultă și din ordonanțele prefectorale aplicabile poliției prefectorale.

B) Supraveghere

1) Supravegherea judiciară

În ceea ce privește colectarea informațiilor cu caracter personal prin mijloace obligatorii, aceasta trebuie să se bazeze pe un mandat ⁽¹⁶⁾ și, prin urmare, face obiectul unei examinări prealabile de către un judecător. În cazul în care investigația a fost ilegală, judecătorul poate exclude aceste probe în judecata ulterioară a cauzei. O persoană fizică poate solicita o astfel de excludere în cadrul judecății cauzei sale penale dacă susține că investigația a fost ilegală.

⁽¹²⁾ Printre factorii relevanți în vederea evaluării „caracterului adecvat al metodelor” se află gravitatea infracțiunii și urgența.

⁽¹³⁾ Articolul 21 alineatul (2) din Constituție prevede următoarele: „Nu se aplică nicio cenzură și nu se încalcă secretul mijloacelor de comunicare.”

⁽¹⁴⁾ Articolul 4 din Legea privind activitățile de telecomunicații prevede următoarele: „(1) Nu se încalcă secretul comunicațiilor gestionate de o societate de telecomunicații. (2) Nicio persoană care desfășoară activități în domeniul telecomunicațiilor nu divulgă secretele pe care le-a aflat, în cursul exercitării funcției, prin intermediul comunicațiilor gestionate de către o societate de telecomunicații. Aceeași obligație se aplică și după ce a părăsit funcția în cauză.”

⁽¹⁵⁾ Articolul 134 din Codul penal prevede următoarele: „(1) Atunci când un medic, un farmacist, un distribuitor de produse farmaceutice, o moașă, un avocat, un avocat al apărării, un notar public sau orice altă persoană care a exercitat anterior o astfel de profesie divulgă, fără motive justificate, informațiile confidențiale ale unei alte persoane pe care le-a aflat în cursul exercitării profesiei respective, acest lucru se pedepsește cu închisoarea în regim de muncă pentru o perioadă maximă de 6 luni sau cu o amendă de cel mult 100 000 de yen. (2) Se aplică aceeași dispoziție în cazul în care o persoană care exercită sau a exercitat o profesie religioasă divulgă, fără motive justificate, informațiile confidențiale ale unei alte persoane pe care le-a aflat în cursul unor astfel de activități religioase.”

⁽¹⁶⁾ În ceea ce privește excepția de la această regulă, a se vedea nota de subsol 5.

2) Supravegherea bazată pe APPIHAO

În Japonia, ministrul sau șeful fiecărui minister sau al fiecărei agenții are autoritatea de supraveghere și de asigurare a respectării legii pe baza APPIHAO, în timp ce ministrul afacerilor interne și al comunicațiilor poate investiga asigurarea respectării APPIHAO de către toate celelalte ministere.

În cazul în care consideră că este necesar pentru realizarea scopului APPIHAO, de exemplu pe baza investigației privind situația asigurării respectării APPIHAO ⁽¹⁷⁾, a prelucrării plângerilor sau a întrebărilor adresate unuia dintre centrele sale de informare generală, ministrul afacerilor interne și al comunicațiilor poate solicita șefului unui organ administrativ să prezinte materiale și explicații privind gestionarea informațiilor cu caracter personal de către organul administrativ în cauză în temeiul articolului 50 din APPIHAO. Ministrul poate adresa opinii șefului organului administrativ cu privire la prelucrarea informațiilor cu caracter personal în cadrul organului administrativ în cazul în care consideră că acest lucru este necesar pentru realizarea scopului legii menționate. În plus, ministrul poate, de exemplu, să solicite o revizuire a măsurilor prin intermediul acțiunilor pe care le poate întreprinde în temeiul articolelor 50 și 51 din lege atunci când se suspectează că a avut loc o încălcare sau o aplicare necorespunzătoare a legii. Acest lucru contribuie la asigurarea aplicării și respectării uniforme a APPIHAO.

3) Supravegherea de către comisiile pentru siguranța publică în ceea ce privește poliția

În ceea ce privește administrația poliției, ANP face obiectul supravegherii de către Comisia națională pentru siguranța publică, iar poliția prefectorală face obiectul supravegherii de către una dintre comisiile prefectorale pentru siguranța publică instituite în fiecare prefectură. Fiecare dintre aceste organisme de supraveghere asigură gestionarea democratică și neutralitatea politică a administrației poliției.

Aspectele care sunt de competența Comisiei naționale pentru siguranța publică sunt prevăzute în Legea privind poliția și în alte legi. Acestea includ numirea comisarului general al ANP și a agenților locali de poliție cu rang înalt, precum și stabilirea unor politici cuprinzătoare care să prevadă direcțiile sau măsurile de bază referitoare la administrarea ANP.

Comisiile prefectorale pentru siguranța publică sunt formate din membri care reprezintă cetățenii din prefectura respectivă, pe baza Legii poliției, și gestionează poliția prefectorală în calitate de consiliu independent. Membrii sunt numiți de către guvernatorul prefectural cu consimțământul Adunării Prefectorale, în temeiul articolului 39 din Legea privind poliția. Mandatul lor este de trei ani și aceștia pot fi demisi împotriva voinței lor numai din motive specifice enumerate în legislație (cum ar fi incapacitatea de a-și îndeplini obligațiile, încălcarea obligațiilor, abateri etc.), asigurându-li-se astfel independența (a se vedea articolele 40 și 41 din Legea privind poliția). De asemenea, pentru a garanta neutralitatea lor politică, articolul 42 din Legea privind poliția le interzice membrilor comisiei să dețină în același timp funcția de membru al unui organ legislativ, să devină membru executiv al unui partid politic sau al oricărui alt organism politic și să participe activ la mișcări politice. Deși fiecare comisie se află sub jurisdicția guvernatorului prefectural respectiv, acest lucru nu îi conferă guvernatorului autoritatea de a emite instrucțiuni privind exercitarea funcțiilor acesteia.

În temeiul articolului 38 alineatul (3) coroborat cu articolul 2 și cu articolul 36 alineatul (2) din Legea privind poliția, comisiile prefectorale pentru siguranța publică sunt responsabile cu „protecția drepturilor și a libertății unei persoane”. În acest scop, acestea primesc rapoarte din partea șefilor poliției prefectorale privind activitățile din jurisdicția lor, inclusiv în cadrul unor reuniuni periodice desfășurate de trei sau patru ori pe lună. Comisiile oferă orientări cu privire la aceste aspecte prin stabilirea unor politici cuprinzătoare.

În plus, în cadrul funcției lor de supraveghere, comisiile prefectorale pentru siguranța publică pot să emită instrucțiuni adresate poliției prefectorale în cazuri individuale concrete, atunci când consideră că acest lucru este necesar în contextul unei inspecții a activităților poliției prefectorale sau al unor abateri ale personalului său. De asemenea, atunci când consideră necesar, comisiile pot încredința unui membru desemnat din cadrul lor sarcina de a examina stadiul punerii în aplicare a instrucțiunilor emise (articolul 43-2 din Legea privind poliția).

⁽¹⁷⁾ Pentru a asigura transparența și a facilita supravegherea de către MIC, în temeiul articolului 11 din APPIHAO, șeful unui organ administrativ are obligația de a păstra o evidență a fiecărui element prevăzut la articolul 10 alineatul (1) din APPIHAO, cum ar fi denumirea organului administrativ care păstrează dosarul, scopul utilizării dosarului, metoda de colectare a informațiilor cu caracter personal etc. (așa-numitul „Registru al dosarelor cu informații cu caracter personal”). Cu toate acestea, dosarele cu informații cu caracter personal care intră sub incidența articolului 10 alineatul (2) din APPIHAO, cum ar fi cele întocmite sau obținute în cadrul unei anchete penale sau cele referitoare la chestiuni relevante pentru securitatea națională, sunt exceptate de la obligația de a fi notificate MIC și de a fi incluse în registrul public. Totuși, în temeiul articolului 7 din Legea privind gestionarea registrelor și a arhivelor publice, șeful unui organ administrativ are obligația de a înregistra întotdeauna clasificarea, titlul, perioada de păstrare și locul de depozitare etc. ale documentelor administrative („Registru de gestionare a dosarelor cu documente administrative”). Indexul informațiilor pentru ambele registre este publicat pe internet și permite persoanelor fizice să verifice ce tip de informații cu caracter personal conține dosarul și care organ administrativ păstrează informațiile.

4) Supravegherea de către Dietă

Dieta poate desfășura investigații în legătură cu activitățile autorităților publice și, în acest scop, poate solicita prezentarea unor documente și audierea unor martori (articolul 62 din Constituție). În acest context, comisia competentă din cadrul Dietei poate examina caracterul adecvat al activităților de colectare de informații desfășurate de poliție.

Aceste competențe sunt specificate mai detaliat în cadrul Regulamentului de procedură al Dietei. În temeiul articolului 104 din Regulamentul de procedură, Dieta poate solicita Cabinetului și agențiilor publice să îi prezinte rapoartele și evidențele necesare pentru desfășurarea investigației sale. În plus, membrii Dietei pot adresa „întrebări scrise” în temeiul articolului 74 din Regulamentul de procedură al Dietei. Aceste întrebări trebuie să fie aprobate de președintele Camerei și, în principiu, trebuie să primească un răspuns scris din partea Cabinetului în termen de șapte zile (atunci când este imposibil să se răspundă în termenul respectiv, acest lucru trebuie justificat și trebuie să se stabilească un nou termen, a se vedea articolul 75 din Regulamentul de procedură al Dietei). În trecut, întrebările scrise adresate de Dietă au abordat și chestiunea gestionării informațiilor cu caracter personal de către administrația publică ⁽¹⁸⁾.

C) Măsuri reparatorii individuale

În conformitate cu articolul 32 din Constituția Japoniei, nicio persoană nu poate fi lipsită de dreptul de acces la justiție. În plus, articolul 17 din Constituție garantează fiecărei persoane dreptul de a intenta o acțiune în justiție împotriva statului sau a unei entități publice în vederea obținerii de măsuri reparatorii (astfel cum sunt prevăzute de lege) în cazul în care persoana în cauză a suferit prejudicii din cauza unui act ilegal al unui funcționar public.

1) Căile de atac judiciare împotriva colectării obligatorii de informații pe baza unui mandat (articolul 430 din Codul de procedură penală)

În conformitate cu articolul 430 alineatul (2) din Codul de procedură penală, o persoană care este nemulțumită de măsurile întreprinse de un agent de poliție cu privire la punerea sub sechestru a unor articole (inclusiv dacă acestea conțin informații cu caracter personal) pe baza unui mandat poate depune o cerere (așa-numita „cvasiplângere”) la instanța judecătorească competentă pentru ca aceste măsuri să fie „anulate sau modificate”.

O astfel de acțiune poate fi intentată fără ca persoana în cauză să trebuiască să aștepte închiderea cauzei. În cazul în care constată că punerea sub sechestru nu a fost necesară sau că există alte motive pentru a considera că punerea sub sechestru este ilegală, instanța judecătorească poate dispune anularea sau modificarea măsurilor respective.

2) Căile de atac judiciare prevăzute în Codul de procedură civilă și în Legea privind măsurile reparatorii acordate de stat

În cazul în care consideră că dreptul lor la viață privată prevăzut la articolul 13 din Constituție a fost încălcat, persoanele fizice pot introduce o acțiune civilă pentru a solicita ștergerea informațiilor cu caracter personal colectate în cadrul unei anchete penale.

De asemenea, în cazul în care consideră că dreptul său la viață privată a fost încălcat și că a suferit un prejudiciu ca urmare a colectării informațiilor sale cu caracter personal sau a supravegherii sale, o persoană fizică poate introduce o acțiune în vederea obținerii de despăgubiri pentru prejudiciile suferite, în temeiul Legii privind măsurile reparatorii acordate de stat, coroborată cu articolele relevante din Codul civil ⁽¹⁹⁾. Având în vedere că „prejudiciul” care face obiectul unei acțiuni în despăgubiri nu se limitează la prejudiciile materiale (articolul 710 din Codul civil), acțiunea respectivă poate viza și „prejudiciile psihologice”. Valoarea despăgubirilor pentru un astfel de prejudiciu moral va fi stabilită de către judecător pe baza unei „evaluări libere care ține seama de diverși factori în fiecare cauză” ⁽²⁰⁾.

La articolul 1 alineatul (1) din Legea privind măsurile reparatorii acordate de stat se prevede acordarea unei despăgubiri în cazul în care (i) un funcționar public care exercită autoritatea publică a statului sau a unei entități publice, (ii) în cursul exercitării atribuțiilor sale, (iii) intenționat sau din neglijență, (iv) în mod ilegal, (v) a cauzat prejudicii unei alte persoane.

Persoana respectivă trebuie să intenteze un proces în conformitate cu Codul de procedură civilă. În conformitate cu normele aplicabile, aceasta poate intenta procesul la instanța competentă pentru locul în care s-a comis delictul.

⁽¹⁸⁾ A se vedea, de exemplu, întrebarea scrisă nr. 92 a Camerei Consilierilor din 27 martie 2009 privind gestionarea informațiilor colectate în contextul anchetelor penale, inclusiv cazurile de încălcare a obligațiilor de confidențialitate de către autoritățile de poliție și de urmărire penală.

⁽¹⁹⁾ Un exemplu de astfel de acțiune este „Cauza referitoare la lista Agenției de Apărare” [Tribunalul districtual din Niigata, hotărârea din 11 mai 2006 [2002 (Wa) nr. 514]. În această cauză, un funcționar al Agenției de Apărare a întocmit, a păstrat și a distribuit o listă a persoanelor care au depus la Agenția de Apărare cereri de divulgare a documentelor administrative. Lista conținea informații cu caracter personal ale reclamantului. Insistând asupra faptului că i s-au încălcat dreptul la viață privată, dreptul de a cunoaște etc., reclamantul a solicitat ca pârâtul să plătească despăgubiri pentru prejudicii în temeiul articolului 1 alineatul (1) din Legea privind măsurile reparatorii acordate de stat. Această cerere a fost acceptată parțial de instanță, care i-a acordat reclamantului o despăgubire parțială.

⁽²⁰⁾ Curtea Supremă, hotărârea din 5 aprilie 1910 [1910 (O) nr. 71].

- 3) Căile de atac individuale împotriva investigațiilor ilegale/necorespunzătoare ale poliției: plângerea adresată Comisiei prefecturale pentru siguranța publică (articolul 79 din Legea privind poliția)

În conformitate cu articolul 79 din Legea privind poliția ⁽²¹⁾, astfel cum a fost clarificat într-o instrucțiune emisă de către șeful ANP și adresată poliției prefecturale și comisiilor prefecturale pentru siguranța publică ⁽²²⁾, persoanele fizice pot depune, la comisia prefecturală pentru siguranța publică competentă, o plângere scrisă ⁽²³⁾ împotriva oricărui comportament ilegal sau necorespunzător al unui agent de poliție în exercitarea sarcinilor sale, fiind incluse și sarcinile legate de colectarea și utilizarea informațiilor cu caracter personal. Comisia va trata astfel de plângeri cu loialitate, cu respectarea legii și a ordonanțelor locale, și va informa în scris reclamantul cu privire la rezultatul investigației.

Pe baza autorității sale de supraveghere, în conformitate cu articolul 38 alineatul (3) din Legea privind poliția, Comisia prefecturală pentru siguranța publică emite instrucțiuni adresate poliției prefecturale pentru ca aceasta să investigheze faptele, să pună în aplicare măsurile necesare în funcție de rezultatul examinării și să raporteze comisiei rezultatele. În cazul în care consideră necesar, Comisia poate, de asemenea, să emită instrucțiuni cu privire la tratarea plângerii, de exemplu în cazul în care consideră că investigația desfășurată de poliție este insuficientă. Această punere în aplicare este descrisă în Comunicarea emisă de ANP și adresată șefilor poliției prefecturale.

Informarea reclamantului cu privire la rezultatul investigației se face, de asemenea, ținând seama de rapoartele poliției privind investigația și măsurile luate la cererea comisiei.

- 4) Măsurile reparatorii individuale prevăzute în APPIHAO și în Codul de procedură penală

(a) APPIHAO

În conformitate cu articolul 48 din APPIHAO, organele administrative trebuie să depună eforturi pentru a trata în mod adecvat și cu promptitudine orice plângere referitoare la gestionarea informațiilor cu caracter personal. Pentru a furniza informații consolidate persoanelor fizice (de exemplu, cu privire la drepturile disponibile de divulgare, de rectificare și de suspendare a utilizării în temeiul APPIHAO) și ca punct de contact pentru întrebări, MIC a instituit în fiecare prefectură centre de informare generală privind divulgarea informațiilor/protecția informațiilor cu caracter personal, în temeiul articolului 47 alineatul (2) din APPIHAO. Nerezidenții pot, de asemenea, adresa întrebări. De exemplu, în exercițiul financiar 2017 (din aprilie 2017 până în martie 2018), numărul total de cazuri în care centrele de informare generală au răspuns la întrebări etc. a fost de 5 186.

Articolele 12 și 27 din APPIHAO acordă persoanelor fizice dreptul de a solicita divulgarea și rectificarea informațiilor cu caracter personal păstrate. În plus, în conformitate cu articolul 36 din APPIHAO, persoanele fizice pot solicita suspendarea utilizării sau ștergerea informațiilor cu caracter personal păstrate, în cazul în care organul administrativ nu a obținut în mod legal informațiile cu caracter personal păstrate ori le păstrează sau le utilizează cu încălcarea legii.

Cu toate acestea, în ceea ce privește informațiile cu caracter personal colectate (fie pe baza unui mandat, fie prin intermediul unei „fișe de solicitare de informații”) și păstrate pentru anchete penale ⁽²⁴⁾, acestea intră în general în categoria „informațiilor cu caracter personal înregistrate în documente referitoare la procese și la articole puse sub sechestru”. Astfel de informații cu caracter personal sunt, prin urmare, excluse din domeniul de aplicare al drepturilor individuale prevăzute în capitolul 4 din APPIHAO în temeiul articolului 53-2 din Codul de procedură penală ⁽²⁵⁾. Prelucrarea unor astfel de informații cu caracter personal și drepturile persoanei de acces și de rectificare fac, în

⁽²¹⁾ Articolul 79 din Legea privind poliția (extras):

- (1) Oricine are o plângere împotriva executării sarcinilor de către personalul poliției prefecturale poate depune o plângere în scris la Comisia prefecturală pentru siguranța publică, prin procedura prevăzută în Ordonanța Comisiei naționale pentru siguranța publică.
- (2) Comisia prefecturală pentru siguranța publică care a primit o plângere prevăzută la alineatul precedent o tratează cu loialitate, cu respectarea legii și a ordonanțelor locale, și informează în scris reclamantul cu privire la rezultat, cu excepția următoarelor cazuri:
 1. se constată că plângerea a fost introdusă pentru a împiedica executarea legală a sarcinilor poliției prefecturale;
 2. reședința actuală a reclamantului nu este cunoscută;
 3. se constată că plângerea a fost depusă în comun cu alți reclamanți, iar alți reclamanți au fost informați deja cu privire la rezultatul plângerii comune.

⁽²²⁾ ANP, Comunicare privind tratarea corespunzătoare a plângerilor referitoare la executarea sarcinilor de către agenții de poliție, 13 aprilie 2001, cu anexa 1 intitulată „Standarde privind interpretarea/punerea în aplicare a articolului 79 din Legea privind poliția”.

⁽²³⁾ În conformitate cu comunicarea ANP (a se vedea nota de subsol precedentă), persoanele care au dificultăți în ceea ce privește formularea unei plângeri în scris trebuie să primească asistență. Această categorie include în mod expres cazul străinilor.

⁽²⁴⁾ Pe de altă parte, ar putea exista documente care nu sunt clasificate ca „documente referitoare la procese”, deoarece acestea nu constituie, în sine, informații obținute pe baza unui mandat sau a unor solicitări de informații scrise în materie de investigații, ci au fost create pe baza unor astfel de documente. În acest caz, informațiile private nu fac obiectul articolului 45 alineatul (1) din APPIHAO și, prin urmare, astfel de informații nu ar fi excluse de la aplicarea capitolului 4 din APPIHAO.

⁽²⁵⁾ Articolul 53-2 alineatul (2) din Codul de procedură penală prevede că dispozițiile capitolului IV din APPIHAO nu se aplică informațiilor cu caracter personal înregistrate în documentele referitoare la procese și la articole puse sub sechestru.

schimb, obiectul unor norme speciale prevăzute în Codul de procedură penală și în Legea privind dosarele penale închise (a se vedea mai jos) ⁽²⁶⁾. Această excludere este justificată de diverși factori, cum ar fi protecția vieții private a persoanelor în cauză, secretul investigațiilor și desfășurarea corespunzătoare a judecării. Acestea fiind spuse, dispozițiile capitolului 2 din APPIHAO care reglementează principiile de gestionare a acestor informații rămân aplicabile.

(b) Codul de procedură penală

În temeiul Codului de procedură penală, posibilitățile de acces la informațiile cu caracter personal colectate în scopul anchetelor penale depind atât de stadiul procedurii, cât și de rolul persoanei în cadrul anchetei (suspect, acuzat, victimă etc.).

Ca excepție de la regula prevăzută la articolul 47 din Codul de procedură penală, și anume că documentele referitoare la proces nu se fac publice înainte de începerea procesului (deoarece acest lucru ar putea aduce atingere onoarei și/sau dreptului la viață privată al persoanelor în cauză și ar putea împiedica ancheta/procesul), examinarea acestor informații de către victima unei infracțiuni este, în principiu, permisă în măsura în care aceasta este considerată rezonabilă, ținând seama de scopul dispoziției prevăzute la articolul 47 din Codul de procedură penală ⁽²⁷⁾.

În cazul suspectilor, aceștia află de obicei că fac obiectul unei anchete penale în cursul unui interogatoriu efectuat fie de către poliția judiciară, fie de către procuror. În cazul în care, ulterior, procurorul decide să nu inițieze urmărirea penală, acesta informează prompt persoana suspectată în legătură cu acest fapt la cererea sa (articolul 259 din Codul de procedură penală).

În plus, după inițierea urmăririi penale, procurorul dă persoanei acuzate sau avocatului său posibilitatea de a examina probele înainte de a solicita examinarea acestora de către instanță (articolul 299 din Codul de procedură penală). Acest lucru permite persoanei acuzate să verifice informațiile cu caracter personal care au fost colectate în cursul anchetei penale.

În fine, protecția informațiilor cu caracter personal colectate în cadrul unei anchete penale, fie că este vorba de o persoană suspectată, de o persoană acuzată sau de orice altă persoană (de exemplu victima unei infracțiuni), este garantată prin obligația de confidențialitate (articolul 100 din Legea privind serviciul public național) și prin riscul de sancționare în cazul scurgerii de informații confidențiale în cursul exercitării atribuțiilor de serviciu public [articolul 109 punctul (xii) din Legea privind serviciul public național].

5) Căi de atac individuale împotriva investigațiilor ilegale/neadecvate efectuate de autoritățile publice: plângerea adresată PPC

În conformitate cu articolul 6 din APPI, guvernul, în colaborare cu guvernele țărilor terțe, ia măsurile necesare pentru a elabora un sistem de informații cu caracter personal care este conform la nivel internațional, prin promovarea cooperării cu organizațiile internaționale și cu alte cadre internaționale. În temeiul acestei dispoziții, politica de bază privind protecția informațiilor cu caracter personal (adoptată prin decizie a Cabinetului) delegă către PPC, în calitatea sa de autoritate competentă pentru administrarea generală a APPI, competența de a lua măsurile necesare pentru soluționarea diferențelor de sistem și de operare dintre Japonia și țara străină în cauză, cu scopul de a asigura tratarea corespunzătoare a informațiilor cu caracter personal primite din partea țării respective.

În plus, după cum prevede articolul 61 punctele (i) și (ii) din APPI, PPC are sarcina de a formula și a promova politica de bază, precum și de a media în cazul plângerilor depuse împotriva operatorilor economici. În sfârșit, organele administrative comunică și cooperează strâns unele cu altele (articolul 80 din APPI).

Pe baza acestor dispoziții, PPC va trata plângerile depuse de persoanele fizice după cum urmează:

- a) O persoană fizică ce suspectează că datele sale transferate din UE au fost colectate sau utilizate de autoritățile publice din Japonia, inclusiv de autoritățile responsabile cu activitățile menționate în capitolele II și III din prezenta „expunere”, cu încălcarea normelor aplicabile, inclusiv a celor care fac obiectul prezentei „expuneri”, poate depune o plângere la PPC (în mod individual sau prin intermediul autorității pentru protecția datelor din țara sa).
- b) PPC tratează plângerea, recurgând inclusiv la competențele sale prevăzute la articolul 6, articolul 61 punctul (ii) și articolul 80 din APPI, și informează autoritățile publice competente, inclusiv organismele de supraveghere relevante, cu privire la plângere.

⁽²⁶⁾ În Codul de procedură penală și în Legea privind dosarele penale închise se prevede că accesul la articolele puse sub sechestru și la documentele/informațiile cu caracter personal referitoare la procesele penale, precum și rectificarea acestora fac obiectul unui sistem unic și distinct de norme care vizează protejarea vieții private a persoanelor în cauză, a secretului investigațiilor și a desfășurării corespunzătoare a procesului penal etc.

⁽²⁷⁾ Mai precis, victimele infracțiunilor pot, în principiu, să examineze informațiile referitoare la probele obiective din dosarele în care s-a decis neînceperea urmăririi penale în cazurile în care se permite participarea victimelor, prevăzute la articolul 316-33 din Codul de procedură penală, pentru a asigura o protecție mai bună a victimelor infracțiunilor.

Articolul 80 din APPI prevede că aceste autorități au obligația de a coopera cu PPC, inclusiv prin furnizarea informațiilor necesare și a materialelor relevante, astfel încât PPC să poată evalua dacă colectarea sau utilizarea ulterioară a informațiilor cu caracter personal a avut loc în conformitate cu normele aplicabile. Pentru efectuarea evaluării sale, PPC va coopera cu MIC.

- c) Dacă evaluarea arată că a avut loc o încălcare a normelor aplicabile, cooperarea autorităților publice în cauză cu PPC include și obligația de a remedia încălcarea respectivă.

În cazul colectării ilegale de informații cu caracter personal în temeiul normelor aplicabile, aceasta include ștergerea informațiilor cu caracter personal colectate.

În cazul încălcării normelor aplicabile, PPC va confirma, de asemenea, înainte de încheierea evaluării, că încălcarea a fost remediată pe deplin.

- d) După încheierea evaluării, PPC comunică persoanei fizice, într-un termen rezonabil, rezultatul evaluării, inclusiv orice măsură corectivă întreprinsă, dacă este cazul. Prin această comunicare, PPC informează, de asemenea, persoana fizică despre posibilitatea de a obține o confirmare a rezultatului de la autoritatea publică competentă și precizează cărei autorități trebuie să i se adreseze o astfel de cerere de confirmare.

Accesul la informații detaliate despre rezultatul evaluării poate fi restricționat, atât timp cât există motive întemeiate de a se considera că prin comunicarea unor astfel de informații investigația în curs poate fi expusă unui risc.

Dacă plângerea se referă la colectarea sau utilizarea de informații cu caracter personal în domeniul aplicării legii penale, în situația în care evaluarea arată că a fost deschisă o cauză care implică informațiile cu caracter personal ale persoanei respective și că această cauză a fost închisă, PPC va informa persoana respectivă că dosarul cauzei poate fi consultat în temeiul articolului 53 din Codul de procedură penală și al articolului 4 din Legea privind dosarele penale închise.

Dacă evaluarea arată că o persoană este suspectă într-o cauză penală, PPC va informa persoana respectivă cu privire la acest fapt și cu privire la posibilitatea de a introduce o cerere în temeiul articolului 259 din Codul de procedură penală.

- e) Dacă este în continuare nemulțumită de rezultatul acestei proceduri, persoana în cauză se poate adresa PPC, care o va informa cu privire la diferitele posibilități și proceduri detaliate pentru obținerea de reparații în temeiul legilor și reglementărilor japoneze. PPC va asigura persoanei sprijin, inclusiv consiliere și asistență, în vederea introducerii unei eventuale acțiuni ulterioare la instanța administrativă sau judecătorească relevantă.

III. Accesul guvernului în scopuri de securitate națională

A. Temeiuri juridice și limitări ale colectării de informații cu caracter personal

1) Temeiuri juridice pentru colectarea de informații de către ministerul/agenția interesate

După cum s-a arătat mai sus, colectarea de informații cu caracter personal în scopuri de securitate națională de către organele administrative trebuie să se încadreze în domeniul de competență administrativă al acestora.

În Japonia nu există nicio lege care să permită, numai din motive de securitate națională, colectarea de informații prin mijloace obligatorii. În conformitate cu articolul 35 din Constituție, informațiile cu caracter personal pot fi colectate prin coerciție numai pe baza unui mandat emis de o instanță pentru investigarea unei infracțiuni. Prin urmare, un astfel de mandat poate fi emis numai în scopul unei anchete penale. Aceasta înseamnă că în sistemul juridic japonez nu sunt permise colectarea/accesul la informații prin mijloace obligatorii în scopuri de securitate națională. În schimb, în domeniul securității naționale, ministerele sau agențiile interesate pot obține informații numai din surse care pot fi accesate în mod liber sau pot primi informații de la operatori economici sau de la persoane fizice, prin divulgare voluntară. Operatorii economici care primesc o cerere de cooperare voluntară nu au obligația legală de a furniza astfel de informații și, prin urmare, nu se confruntă cu consecințe negative dacă refuză să coopereze.

Mai multe departamente și agenții ministeriale au responsabilități în domeniul securității naționale.

(1) Secretariatul Cabinetului

Secretariatul Cabinetului desfășoară activități de colectare și cercetare de informații privind politicile importante ale Cabinetului⁽²⁸⁾, prevăzute la articolul 12-2 din Legea privind Cabinetul⁽²⁹⁾. Cu toate acestea, Secretariatul Cabinetului nu are competența de a colecta informații cu caracter personal direct de la operatorii economici. Acesta colectează, compilează, analizează și evaluează informațiile provenite din materialele cu sursă deschisă, de la alte autorități publice etc.

(2) ANP/Poliția prefectorală

În fiecare prefectură, poliția prefectorală este abilitată să colecteze informații care țin de competența sa în temeiul articolului 2 din Legea privind poliția. Se poate întâmpla ca ANP să colecteze în mod direct informații din domeniul său de competență în temeiul Legii privind poliția. Este vorba, în special, de activitățile Biroului de Securitate al ANP și ale Departamentului pentru Afaceri Externe și Informații. În temeiul articolului 24 din Legea privind poliția, Biroul de Securitate este responsabil cu chestiunile care privesc poliția de securitate⁽³⁰⁾, iar Departamentul pentru Afaceri Externe și Informații este responsabil cu chestiunile care privesc cetățenii străini, precum și cetățenii japonezi care desfășoară activități în țări străine.

(3) Agenția de Informații pentru Securitate Publică (PSIA)

Aplicarea Legii privind prevenirea activităților subversive (SAPA) și a Legii privind controlul organizațiilor care au săvârșit acte de ucidere în masă arbitrară (ACO) intră, în principal, în competența Agenției de Informații pentru Securitate Publică (PSIA). Aceasta este o agenție a Ministerului Justiției.

Conform SAPA și ACO pot fi adoptate, în condiții stricte, dispoziții administrative (și anume, măsuri care impun limitarea activităților unor astfel de organizații, dizolvarea acestora etc.) împotriva organizațiilor care comit anumite acte grave („activitate teroristă subversivă” sau „act de ucidere în masă arbitrară”) încălcând „securitatea publică” sau „sistemul fundamental al societății” prevăzute de Constituție. „Activitățile teroriste subversive” intră în domeniul SAPA (a se vedea articolul 4 care acoperă activități precum insurecția, instigarea la agresiune împotriva străinilor, omorul cu intenție politică etc.), în timp ce ACO se referă la „actele de ucidere în masă arbitrară” (a se vedea articolul 4 din ACO). Numai organizațiile identificate în mod precis și care reprezintă amenințări interne sau externe specifice la adresa securității publice pot face obiectul dispozițiilor SAPA sau ACO.

În acest scop, SAPA și ACO asigură autoritate juridică pentru desfășurarea de investigații. Competențele fundamentale de investigare ale funcționarilor PSIA (PSIO) sunt prevăzute la articolul 27 din SAPA și la articolul 29 din ACO. Investigațiile efectuate de PSIA în temeiul acestor dispoziții sunt desfășurate în măsura în care sunt necesare din perspectiva dispozițiilor sus-menționate de control al organizațiilor (grupurile de stânga radicale, secta *Aum Shinrikyo* și anumite grupuri interne care au legături strânse cu Coreea de Nord au fost menționate ca exemple de organizații supuse investigațiilor în trecut). Cu toate acestea, pentru investigațiile respective nu se poate recurge la mijloace obligatorii și, prin urmare, o organizație care deține informații cu caracter personal nu poate fi obligată să furnizeze aceste informații.

Colectarea și utilizarea informațiilor dezvăluite PSIA în mod voluntar fac obiectul garanțiilor și limitărilor relevante prevăzute de lege, cum ar fi, printre altele, secretul comunicării garantat de Constituție și normele privind prelucrarea informațiilor cu caracter personal în temeiul APPIHAO.

(4) Ministerul Apărării (MOD)

Ministerul Apărării colectează informații pe baza articolelor 3 și 4 din Legea de constituire a MOD, în măsura în care acest lucru este necesar pentru exercitarea competenței sale administrative, inclusiv în ceea ce privește apărarea și protecția, acțiunile care trebuie întreprinse de Forțele de autoapărare, precum și desfășurarea Forțelor de autoapărare terestre, maritime și aeriene. MOD poate colecta informații în acest scop numai prin cooperare voluntară și din surse accesibile în mod liber. MOD nu colectează informații cu privire la publicul larg.

2) Limitări și garanții

a) Limitări în temeiul legii

(1) Limitări generale în baza APPIHAO

APPIHAO este o lege cu caracter general care se aplică colectării și prelucrării informațiilor cu caracter personal de către organele administrative în orice domeniu de activitate al acestor organe. Prin urmare, limitările și garanțiile descrise în secțiunea II partea A punctul 1) litera (b) subpunctul (2) se aplică și în cazul păstrării, stocării, utilizării etc. a informațiilor cu caracter personal din domeniul securității naționale.

⁽²⁸⁾ Aceste activități sunt desfășurate de Oficiul de Informații și Cercetări al Cabinetului, în temeiul articolului 4 din Ordinul de organizare a Secretariatului Cabinetului.

⁽²⁹⁾ Acesta include „colectarea și cercetarea de informații privind politicile importante ale Cabinetului”.

⁽³⁰⁾ Poliția de securitate este responsabilă cu activitățile de control al criminalității legate de siguranța publică și de interesul națiunii. Printre acestea se numără controlul infracțiunilor și colectarea de informații privind actele ilegale ale grupurilor de extremă stângă sau extremă dreaptă și privind activitățile antijaponeze.

(2) Limitări specifice aplicabile poliției (atât ANP, cât și Poliției prefectorale)

După cum se specifică mai sus în secțiunea referitoare la colectarea de informații în scopuri de aplicare a legii, poliția poate colecta numai informații din domeniul său de competență și, în acest scop, poate acționa, în temeiul articolului 2 alineatul (2) din Legea privind poliția, numai într-o măsură „limitată strict” la îndeplinirea sarcinilor sale și într-un mod „imparțial, nepărtinitor, obiectiv și echitabil”. În plus, competențele sale „nu vor fi niciodată utilizate abuziv, într-un mod care să interfereze cu drepturile și libertățile persoanelor, garantate prin Constituția Japoniei”.

(3) Limitări specifice aplicabile PSIA

Atât articolul 3 din SAPA, cât și articolul 3 din ACO prevăd faptul că investigațiile efectuate în temeiul acestor legi sunt desfășurate numai în măsura necesară pentru atingerea scopului urmărit și nu se derulează într-un mod care restricționează nerezonabil drepturile fundamentale ale omului. În plus, în conformitate cu articolul 45 din SAPA și cu articolul 42 din ACO, dacă un funcționar al PSIA abuzează de autoritatea sa, acest fapt constituie o infracțiune pasibilă de sancțiuni penale mai severe decât în cazul abuzurilor „generale” de autoritate în alte domenii ale sectorului public.

(4) Limitări specifice aplicabile MOD

În ceea ce privește activitățile de colectare/organizare de către MOD a informațiilor, menționate la articolul 4 din Legea de constituire a MOD, activitatea de colectare a informațiilor desfășurată de acest minister se limitează la ceea ce este „necesar” pentru îndeplinirea atribuțiilor sale privind: 1. apărarea și protecția; 2. acțiunile care trebuie întreprinse de Forțele de autoapărare, (3) organizarea, efectivele, structura, echipamentele și desfășurarea Forțelor de autoapărare terestre, maritime și aeriene.

b) Alte limitări

După cum s-a arătat mai sus, în secțiunea II partea A punctul 2) litera (b) subpunctul (1), în cazul anchetelor penale, din jurisprudența Curții Supreme reiese că, pentru a putea adresa unui operator economic o cerere de cooperare voluntară, cererea respectivă trebuie să fie necesară pentru investigarea unei suspiciuni de infracțiune și trebuie să fie rezonabilă pentru atingerea scopul investigației.

Deși investigațiile efectuate de autoritățile de investigare în domeniul securității naționale diferă, în ceea ce privește atât temeiul juridic, cât și scopul, de investigațiile efectuate de autoritățile de investigare în domeniul aplicării legii, principiile centrale ale „necesității investigației” și „adecvării metodei” se aplică în mod similar în domeniul securității naționale și trebuie respectate, ținând seama în mod corespunzător de circumstanțele specifice ale fiecărui caz.

Combinarea limitărilor menționate mai sus asigură faptul că operațiunile de colectare și prelucrare a informațiilor au loc numai în măsura în care sunt necesare pentru îndeplinirea sarcinilor specifice ale autorității publice competente și numai în temeiul unor amenințări specifice. Acest lucru exclude colectarea în masă și arbitrară de informații cu caracter personal sau accesul în masă și arbitrar la acestea din motive de securitate națională.

B. Supraveghere

1. Supravegherea pe baza APPIHAO

După cum s-a arătat mai sus, în secțiunea II partea B punctul 2), în sectorul public japonez, ministrul sau șeful fiecărui minister sau al fiecărei agenții are competența de a supraveghea și a asigura conformitatea cu APPIHAO în ministerul sau agenția sa. În plus, ministrul Afacerilor Interne și Comunicațiilor poate investiga situația aplicării legii, poate solicita fiecărui ministru să transmită materiale și explicații în temeiul articolelor 49 și 50 din lege și poate trimite opinii fiecărui ministru în temeiul articolului 51 din lege. De exemplu, acesta poate solicita o revizuire a măsurilor prin acțiunile prevăzute la articolele 50 și 51 din lege.

2. Supravegherea poliției de către comisiile pentru siguranță publică

După cum s-a arătat în secțiunea II de mai sus „Colectarea de informații în scopuri de aplicare a legii penale”, comisiile independente prefectorale pentru siguranță publică supraveghează activitățile poliției prefectorale.

În ceea ce privește Agenția Națională de Poliție (ANP), funcțiile de supraveghere sunt exercitate de Comisia națională pentru siguranță publică. În temeiul articolului 5 din Legea privind poliția, comisia respectivă este responsabilă, în special, cu „protecția drepturilor și a libertății persoanelor”. În acest scop, comisia menționată instituie politici cuprinzătoare, care stabilesc regulile de administrare a cazurilor prevăzute la fiecare punct al articolului 5 alineatul (4) din Legea privind poliția, precum și alte instrucțiuni sau măsuri de bază pe care ar trebui să se întemeieze desfășurarea activităților menționate. Comisia națională pentru siguranță publică (NPSC) are același grad de independență ca și comisiile prefectorale pentru siguranță publică (PPSC).

3) Supravegherea MOD de către Biroul Inspectorului General pentru conformitate juridică

Biroul Inspectorului General pentru conformitate juridică (IGO) este un birou independent al Ministerului Apărării (MOD), aflat sub supravegherea directă a ministrului Apărării în temeiul articolului 29 din Legea de constituire a Ministerului Apărării. IGO poate efectua inspecții pentru verificarea respectării legilor și a reglementărilor de către funcționarii MOD. Aceste inspecții sunt denumite „inspecții în domeniul apărării”.

IGO efectuează inspecții în calitate de birou independent, pentru a asigura respectarea legislației de către întregul minister, inclusiv de către Forțele de autoapărare (SDF). Acesta își îndeplinește sarcinile independent de departamentele operaționale ale MOD. După inspecție, IGO prezintă direct ministrului Apărării, fără întârziere, un raport conținând constatările sale și măsurile de ameliorare necesare. Pe baza raportului IGO, ministrul Apărării poate emite ordine pentru punerea în aplicare a măsurilor necesare în vederea remedierii situației. Viceministrul adjunct răspunde de punerea în aplicare a acestor măsuri și trebuie să prezinte ministrului Apărării un raport privind stadiul punerii în aplicare.

Ca măsură voluntară de asigurare a transparenței, constatările inspecțiilor în domeniul apărării sunt publicate în prezent pe site-ul web al MOD (deși acest lucru nu este impus prin lege).

Există trei categorii de inspecții în domeniul apărării:

- (i) inspecții reglementare în domeniul apărării, care se efectuează periodic ⁽³¹⁾;
- (ii) inspecții în domeniul apărării pentru verificări, care sunt efectuate pentru a verifica dacă măsurile de ameliorare au fost luate efectiv; și
- (iii) inspecții speciale în domeniul apărării, care sunt efectuate în legătură cu aspecte specifice dispuse de ministrul Apărării.

În contextul acestor inspecții, Inspectorul General poate solicita rapoarte birourilor în cauză, poate solicita transmiterea de documente, poate intra în sedii pentru a efectua inspecția, poate solicita explicații viceministrului adjunct etc. Având în vedere natura sarcinilor de inspecție ale IGO, acest birou este condus de experți juridici de rang înalt (foști procurori șefi).

4) Supravegherea de către PSIA

PSIA efectuează atât inspecții reglementare, cât și inspecții speciale asupra operațiunilor birourilor și oficiilor sale (Biroul de Informații de Securitate Publică, oficiile și suboficiile de informații de securitate publică etc.). Pentru inspecțiile reglementare este (sunt) desemnat (desemnați) un director general adjunct și/sau un director în calitate de inspector(i). Aceste inspecții privesc, de asemenea, gestionarea informațiilor cu caracter personal.

5) Supravegherea de către Dieta

În ceea ce privește colectarea de informații în scopuri de aplicare a legii, Dieta, prin comisia sa competentă, poate examina legalitatea activităților de colectare de informații în domeniul securității naționale. Competențele de investigare ale Dietei se bazează pe articolul 62 din Constituție și pe articolele 74 și 104 din Legea privind Dieta.

C. Căile de atac individuale

Căile de atac individuale pot fi exercitate prin aceleași mijloace care sunt utilizate și în domeniul aplicării legii penale. Acestea includ și noul mecanism de recurs, administrat și supravegheat de PPC, pentru tratarea și soluționarea plângerilor depuse de persoanele fizice din UE. În acest sens, a se vedea pasajele relevante din secțiunea II partea C.

În plus, în domeniul securității naționale, există căi de atac individuale specifice.

Informațiile cu caracter personal colectate de un organ administrativ în scopuri de securitate națională sunt supuse dispozițiilor capitolului 4 din APPIHAO. Acestea includ dreptul de a solicita divulgarea (articolul 12) sau corectarea (inclusiv adăugarea sau ștergerea) (articolul 27) a informațiilor cu caracter personal reținute, precum și dreptul de a solicita suspendarea utilizării informațiilor cu caracter personal, dacă organul administrativ a obținut aceste informații

⁽³¹⁾ Ca exemplu de inspecție relevantă pentru aspectele la care se referă prezenta expunere, se poate cita Inspecția reglementară din 2016 în domeniul apărării privind „Conștientizarea/pregătirea pentru conformitatea juridică”, întrucât protecția informațiilor cu caracter personal a fost unul dintre punctele centrale ale inspecției. Mai precis, inspecția a vizat situația gestionării, a stocării etc. a informațiilor cu caracter personal. În raportul său, IGO a identificat mai multe aspecte neadecvate ale gestionării informațiilor cu caracter personal care ar trebui îmbunătățite, cum ar fi incapacitatea de a proteja datele cu ajutorul unei parole. Raportul este disponibil pe site-ul web al MOD.

în mod ilegal (articolul 36). Acestea fiind spuse, în domeniul securității naționale, exercitarea drepturilor respective este supusă anumitor restricții: cererile de divulgare, corectare sau suspendare nu vor fi aprobate dacă acestea se referă la „informații a căror divulgare șeful unui organ administrativ are motive întemeiate să o considere ca fiind susceptibilă să aducă prejudicii securității naționale, să afecteze relația de încredere reciprocă cu o altă țară sau cu o organizație internațională sau să cauzeze un dezavantaj în negocierile cu o altă țară sau cu o organizație internațională” [articolul 14 punctul (iv)]. Prin urmare, nu orice colectare voluntară de informații legate de securitatea națională intră sub incidența excepției respective, deoarece aceasta din urmă impune o evaluare concretă a riscurilor pe care le implică divulgarea informațiilor în cauză.

În plus, dacă cererea unei persoane este respinsă pe motiv că informațiile în cauză sunt considerate nedivulgabile în sensul articolului 14 punctul (iv), persoana respectivă poate introduce un recurs administrativ pentru a obține revizuirea unei astfel de decizii, susținând, de exemplu, că în cazul său nu sunt îndeplinite condițiile stabilite la articolul 14 punctul (iv). În această situație, înainte de a lua o decizie, șeful organului administrativ în cauză consultă Comitetul de reexaminare a divulgării informațiilor și a protecției informațiilor cu caracter personal. Acest comitet va examina recursul în mod independent. Comitetul este un organism foarte specializat și independent, ai cărui membri sunt numiți de primul ministru, cu acordul celor două camere ale Dietei, din rândul persoanelor cu competențe și experiență excepționale ⁽³²⁾. Comitetul dispune de competențe de investigare solide, inclusiv de posibilitatea de a solicita documente și divulgarea informațiilor cu caracter personal în cauză, de a organiza o dezbatere cu ușile închise și de a aplica procedura indicelui Vaughn ⁽³³⁾. Comitetul întocmește ulterior un raport scris, care se comunică persoanei în cauză ⁽³⁴⁾. Constatările cuprinse în raport sunt făcute publice. Deși, în mod oficial, raportul nu este obligatoriu din punct de vedere juridic, organul administrativ în cauză respectă aproape întotdeauna concluziile rapoartelor ⁽³⁵⁾.

În sfârșit, în conformitate cu articolul 3 alineatul (3) din Legea privind litigiile administrative, o persoană poate introduce o acțiune în instanță pentru a obține revocarea deciziei luate de organul administrativ de a nu divulga informațiile cu caracter personal.

IV. Reexaminarea periodică

În cadrul reexaminării periodice a deciziei privind caracterul adecvat, PPC și Comisia Europeană vor face schimb de informații privind prelucrarea datelor în condițiile menționate în constatarea adecvării, inclusiv în cele stabilite în prezenta expunere.

⁽³²⁾ A se vedea articolul 4 din Legea de constituire a Comitetului de reexaminare a divulgării informațiilor și a protecției informațiilor cu caracter personal.

⁽³³⁾ A se vedea articolul 9 din Legea de constituire a Comitetului de reexaminare a divulgării informațiilor și a protecției informațiilor cu caracter personal.

⁽³⁴⁾ A se vedea articolul 16 din Legea de constituire a Comitetului de reexaminare a divulgării informațiilor și a protecției informațiilor cu caracter personal.

⁽³⁵⁾ În ultimii trei ani, nu a existat niciun precedent în care organul administrativ în cauză să fi luat o decizie diferită de concluziile Comitetului. În trecutul mai îndepărtat, există foarte puține cazuri în care s-a întâmplat acest lucru: numai două cazuri dintr-un total de 2 000 de cazuri începând din anul 2005 (anul în care a intrat în vigoare APPIHAO). Dacă adoptă o decizie care diferă de concluziile Comitetului, organul administrativ indică în mod clar motivele acestei decizii, în conformitate cu articolul 50 alineatul (1) punctul 4 din Legea de reexaminare a plângerilor administrative, aplicată cu înlocuirea articolului 42 alineatul (2) din APPIHAO.