II

(Acte fără caracter legislativ)

DECIZII

DECIZIA DE PUNERE ÎN APLICARE (UE) 2022/254 A COMISIEI

din 17 decembrie 2021

de constatare, în temeiul Regulamentului (UE) 2016/679 al Parlamentului European și al Consiliului, a nivelului adecvat de protecție a datelor cu caracter personal asigurat de Republica Coreea în baza Legii privind protecția informațiilor cu caracter personal

[notificată cu numărul C(2021) 9316]

(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) ([1]), în special articolul 45 alineatul (3),

întrucât:

1. INTRODUCERE

(1) Regulamentul (UE) 2016/679 stabilește normele pentru transferul de date cu caracter personal de la operatori sau persoane împuternicite de operatori din Uniune 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 sunt prevăzute în capitolul V (articolele 44-50) din regulamentul respectiv. Deși fluxul de date cu caracter personal către și dinspre țări situate în afara Uniunii Europene este esențial pentru dezvoltarea comerțului transfrontalier și a cooperării internaționale, nivelul de protecție conferit datelor cu caracter personal din Uniune nu trebuie să fie subminat de transferurile către țări terțe ([2]).

(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 o țară terță 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 Regulamentul (UE) 2016/679.

(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. În evaluare, Comisia 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]. Această situație trebuie evaluată în raport cu legislația Uniunii, în special cu Regulamentul (UE) 2016/679, precum și cu jurisprudența Curții de Justiție a Uniunii Europene ([3]).

([1]) JO L 119, 4.5.2016, p. 1.
([2]) A se vedea considerentul 101 din Regulamentul (UE) 2016/679.
([3]) A se vedea, cel mai recent, cauza C-311/18, Facebook Ireland și Schrems („Schrems II”), ECLI:EU:C:2020:559.

(4) Conform clarificărilor aduse de Curtea de Justiție a Uniunii Europene, aceasta nu necesită găsirea unui nivel identic de protecție ([4]). În special, mijloacele la care țara terță în cauză recurge pentru protecția datelor cu caracter personal pot fi diferite de cele utilizate în cadrul Uniunii, cu condiția ca acestea să se dovedească, în practică, eficace pentru asigurarea unui nivel adecvat de protecție ([5]). Prin urmare, standardul caracterului adecvat nu necesită o 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 ([6]). Criteriile de referință privind caracterul adecvat al nivelului de protecție ale Comitetului european pentru protecția datelor, care urmăresc să ofere clarificări suplimentare cu privire la acest standard, oferă, de asemenea, orientări în acest sens ([7]).

(5) Comisia a analizat cu atenție legislația și practica din Republica Coreea. Pe baza constatărilor prezentate în considerentele 8-208, Comisia concluzionează că Republica Coreea asigură un nivel adecvat de protecție a datelor cu caracter personal transferate de la un operator sau de la o persoană împuternicită de un operator din Uniune ([8]) către entități (de exemplu, persoane fizice sau juridice, organizații, instituții publice) din Coreea care intră în domeniul de aplicare al Legii privind protecția informațiilor cu caracter personal (Legea nr. 10465 din 29 martie 2011, astfel cum a fost modificată ultima dată prin Legea nr. 16930 din 4 februarie 2020). Acestea includ atât operatorii, cât și persoanele împuternicite de operatori (numiți „destinatari ai externalizării” ([9])) în sensul Regulamentului (UE) 2016/679. Constatările privind caracterul adecvat nu acoperă prelucrarea datelor cu caracter personal pentru activități misionare ale organizațiilor religioase și pentru numirea candidaților de către partidele politice sau prelucrarea informațiilor cu caracter personal privind creditele în conformitate cu Legea privind informațiile referitoare la credite de către operatorii care sunt supravegheați de Comisia pentru servicii financiare.

(6) Această concluzie ține seama de garanțiile suplimentare prevăzute în Notificarea nr. 2021-5 (anexa I) și de expunerile, asigurările și angajamentele oficiale ale guvernului coreean față de Comisie (anexa II).

(7) Prezenta decizie are drept efect posibilitatea ca transferurile către operatorii și persoanele împuternicite de operatori din Republica Coreea să aibă loc fără a fi necesară obținerea unei autorizări suplimentare. Aceasta nu aduce atingere aplicării directe a Regulamentului (UE) 2016/679 pentru astfel de entități în cazul în care sunt îndeplinite condițiile privind domeniul de aplicare teritorial al regulamentului respectiv, astfel cum se prevede la articolul 3.

2. NORMELE APLICABILE PRELUCRĂRII DATELOR CU CARACTER PERSONAL

2.1 Cadrul privind protecția datelor din Republica Coreea

(8) Regimul juridic care reglementează viața privată și protecția datelor în Coreea este întemeiat pe Constituția coreeană, promulgată la 17 iulie 1948. Deși dreptul la protecția datelor cu caracter personal nu este prevăzut în mod expres în Constituție, acesta este totuși recunoscut ca un drept fundamental care derivă din drepturile constituționale la demnitate umană și la căutarea fericirii (articolul 10), la viața privată (articolul 17) și la confidențialitatea comunicațiilor (articolul 18). Acest lucru a fost confirmat atât de Curtea Supremă ([10]), cât și de Curtea Constituțională ([11]). Restricțiile privind drepturile și libertățile fundamentale (inclusiv dreptul la viață privată) pot fi impuse numai prin lege, atunci când este necesar pentru securitatea națională sau pentru menținerea legii și ordinii pentru bunăstarea publică, și nu pot afecta substanța dreptului sau libertății în cauză [articolul 37 alineatul (2)].

([4]) Cauza C-362/14, Maximillian Schrems/Data Protection Commissioner („Schrems”), ECLI:EU:C:2015:650, punctul 73.
([5]) Schrems, punctul 74.
([6]) 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.
([7]) Comitetul european pentru protecția datelor, Criterii de referință privind caracterul adecvat al nivelului de protecție, WP 254 rev. 01., disponibile la următoarea adresă: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=614108.
([8]) 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 care fac parte din 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. În sensul deciziei, trimiterile la UE și la statele membre ale UE ar trebui, prin urmare, să fie înțelese ca incluzând și statele SEE.
([9]) A se vedea secțiunea 2.2.3 din prezenta decizie.
([10]) A se vedea, de exemplu, Hotărârea Curții Supreme 2014Da77970 din 15 octombrie 2015 (rezumat în limba engleză disponibil la linkul către „Prezentarea de către legiuitor a cauzei privind profesorii sindicaliști”, la adresa https://www.privacy.go.kr/eng/enforcement_01.do) și jurisprudența citată în aceasta, inclusiv Decizia 2012Da49933 din 24 iulie 2014.
([11]) A se vedea, în special, Hotărârea Curții Constituționale 99Hun-ma513 din 26 mai 2005 (rezumat în limba engleză disponibil la adresa http://www.koreanlii.or.kr/w/index.php/99Hun-Ma513?ckattempt=2) și Hotărârea 2014JHun-ma449 2013 Hun-Ba68 (consolidată) din 23 decembrie 2015 (rezumat în limba engleză disponibil la linkul către „Cauza privind modificarea numărului de înregistrare al rezidenților” la adresa https://www.privacy.go.kr/eng/enforcement_01.do).

(9) Deși Constituția face trimitere în mai multe rânduri la drepturile cetățenilor coreeni, Curtea Constituțională a hotărât că și cetățenii străini au anumite drepturi fundamentale ([12]). În special, Curtea a statuat că protecția demnității și a valorii ca ființă umană, precum și dreptul de a căuta fericirea sunt drepturi ale oricărei ființe umane, nu doar ale cetățenilor ([13]). În plus, potrivit expunerilor oficiale ale guvernului coreean ([14]), este general recunoscut faptul că articolele 12-22 din Constituție (care includ drepturile la viață privată) prevăd drepturi fundamentale ale omului ([15]). Deși până în prezent nu există o jurisprudență specifică în ceea ce privește dreptul la viață privată al cetățenilor străini, fundamentarea acestuia pe protejarea demnității umane și căutarea fericirii sprijină această concluzie ([16]).

(10) În plus, Coreea a adoptat o serie de legi în domeniul protecției datelor care oferă garanții pentru toate persoanele, indiferent de cetățenia acestora ([17]). În sensul prezentei decizii, legile relevante sunt:

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

— Legea privind utilizarea și protecția informațiilor privind creditele ([18]);

— Legea privind protecția confidențialității comunicațiilor.

(11) PIPA prevede cadrul juridic general pentru protecția datelor în Republica Coreea. Aceasta este completată de un decret de punere în aplicare (Decretul prezidențial nr. 23169 din 29 septembrie 2011, modificat ultima dată prin Decretul prezidențial nr. 30892 din 4 august 2020) (Decretul de punere în aplicare a PIPA), care, la fel ca PIPA, este obligatoriu din punct de vedere juridic și executoriu.

(12) În plus, „notificările" de reglementare adoptate de Comisia pentru protecția informațiilor cu caracter personal (PIPC) prevăd norme suplimentare privind interpretarea și aplicarea PIPA. Pe baza articolului 5 (Obligații ale statului) și a articolului 14 din PIPA (Cooperare internațională), PIPC a adoptat Notificarea nr. 2021-5 din 1 septembrie 2020 (astfel cum a fost modificată prin Notificarea nr. 2021-1 din 21 ianuarie 2021 și Notificarea nr. 2021-5 din 16 noiembrie 2021, Notificarea nr. 2021-5) privind interpretarea, aplicarea și punerea în aplicare a anumitor dispoziții ale PIPA. Această notificare oferă clarificări care se aplică oricărei prelucrări de date cu caracter personal în temeiul PIPA, precum și garanții suplimentare pentru datele cu caracter personal transferate către Coreea în temeiul prezentei decizii. Notificarea este obligatorie din punct de vedere juridic pentru operatorii de informații cu caracter personal și executorie atât pentru PIPC, cât și pentru instanțe ([19]). O încălcare a normelor prevăzute în notificare implică o încălcare a dispozițiilor relevante din PIPA pe care le completează. Prin urmare, conținutul garanțiilor suplimentare este analizat în cadrul evaluării articolelor relevante din PIPA. În cele din urmă, în Manualul și Orientările PIPA adoptate de PIPC ([20]) sunt prevăzute orientări suplimentare privind PIPA și decretul de punere în aplicare corespunzător, care stau la baza aplicării și a asigurării respectării normelor de protecție a datelor de către PIPC.

([12]) Hotărârea Curții Constituționale 93 Hun-MA120 din 29 decembrie 1994.
([13]) Hotărârea Curții Constituționale 99HeonMa494 din 29 noiembrie 2001.
([14]) A se vedea secțiunea 1.1 din anexa II.
([15]) A se vedea, de asemenea, articolul 1 din Legea privind protecția informațiilor cu caracter personal, care se referă în mod expres la „libertățile și drepturile persoanelor". Mai precis, acesta arată că scopul unei astfel de legi este „să asigure prelucrarea și protecția informațiilor cu caracter personal în scopul protejării libertății și drepturilor persoanelor, precum și respectarea în continuare a demnității și a valorii persoanelor". De asemenea, articolul 5 alineatul (1) din Legea privind protecția informațiilor cu caracter personal stabilește responsabilitatea statului de a „formula politici pentru a preveni consecințele negative ale colectării în afara scopului, utilizarea abuzivă și necorespunzătoare a informațiilor cu caracter personal, supravegherea și urmărirea indiscretă etc., precum și de a îmbunătăți gradul de respectare a demnității ființelor umane și a vieții private."
([16]) În plus, articolul 6 alineatul (2) din Constituție prevede că statutul cetățenilor străini este garantat astfel cum se prevede în dreptul internațional și în tratate. Coreea este parte la mai multe acorduri internaționale care garantează dreptul la viață privată, cum ar fi Pactul internațional cu privire la drepturile civile și politice (articolul 17), Convenția privind drepturile persoanelor cu handicap (articolul 22) și Convenția cu privire la drepturile copilului (articolul 16).
([17]) Acestea includ norme relevante pentru protecția datelor cu caracter personal, dar nu se aplică într-o situație în care datele cu caracter personal sunt colectate în Uniune și transferate către Coreea în temeiul Regulamentului (UE) 2016/679, de exemplu în Legea privind protecția, utilizarea etc. a informațiilor de localizare.
([18]) Scopul acestei legi este de a promova o activitate solidă de informare cu privire la credite, de a promova utilizarea eficientă și gestionarea sistematică a informațiilor privind creditele și de a proteja confidențialitatea acestora împotriva utilizării necorespunzătoare și abuzive a informațiilor privind creditele (articolul 1 din lege).
([19]) De exemplu, instanțele coreene s-au pronunțat cu privire la conformitatea cu notificările de reglementare într-un număr de cazuri, inclusiv prin tragerea la răspundere a operatorilor coreeni pentru încălcarea unei notificări (a se vedea, de exemplu, Hotărârea Curții Supreme 2018Da219406, 25 octombrie 2018, în care Curtea a dispus ca operatorul să plătească despăgubiri persoanelor fizice pentru prejudiciile suferite din cauza încălcării „Notificării pentru standardul privind măsurile de asigurare a securității informațiilor cu caracter personal"; a se vedea, de asemenea, Hotărârea Curții Supreme nr. 2018Da219352 din 25 octombrie 2018; Hotărârea Curții Supreme nr. 2011Da24555 din 16 mai 2016; Hotărârea Tribunalului districtual central din Seul 2014Gahap511956 din 13 octombrie 2016; Hotărârea Tribunalului districtual central din Seul 2009Gahap43176 din 26 ianuarie 2010).
([20]) Articolul 12 alineatul (1) din PIPA.

(13) În plus, Legea privind utilizarea și protecția informațiilor privind creditele (CIA) stabilește norme specifice care se aplică atât operatorilor comerciali „obișnuiți”, cât și entităților specializate din sectorul financiar atunci când prelucrează informații cu caracter personal privind creditele, și anume informații care sunt necesare pentru a determina bonitatea părților la tranzacții financiare sau comerciale. Printre acestea se numără, în special, numele, datele de contact, tranzacțiile financiare, ratingul de credit, statutul de asigurat sau soldul creditelor, atunci când astfel de informații sunt utilizate pentru a stabili bonitatea unei persoane ([21]). În schimb, în cazul în care astfel de informații sunt utilizate în alte scopuri (cum ar fi, resursele umane), PIPA se aplică integral. În ceea ce privește dispozițiile specifice privind protecția datelor ale CIA, conformitatea este supravegheată parțial de PIPC (pentru organizațiile comerciale; a se vedea articolul 45-3 din CIA) și parțial de Comisia pentru servicii financiare ([22]) [pentru sectorul financiar, inclusiv agențiile de rating de credit, bănci, companii de asigurări, case de economii de ajutor reciproc, societăți financiare de credit specializate, societăți de servicii de investiții financiare, societăți de finanțare a valorilor mobiliare, cooperative de credit etc.; a se vedea articolul 45 alineatul (1) din CIA coroborat cu articolul 36-2 din Decretul de punere în aplicare a CIA și articolul 38 din Legea privind Comisia pentru servicii financiare]. În acest sens, domeniul de aplicare al prezentei decizii se limitează la operatorii comerciali care sunt supravegheați de PIPC ([23]). Normele specifice ale CIA care se aplică în acest context (normele generale PIPA se aplică în cazul în care nu există norme specifice) sunt descrise în secțiunea 2.3.11.

2.2 **Domeniul de aplicare material și personal al PIPA**

(14) Cu excepția cazului în care există dispoziții contrare specifice în alte legi, protecția datelor cu caracter personal este reglementată de PIPA (articolul 6). Domeniul său de aplicare material și personal este determinat de conceptele definite de „informații cu caracter personal”, „prelucrare” și „operator de informații cu caracter personal”.

2.2.1 *Definiția datelor cu caracter personal*

(15) Articolul 2 alineatul (1) din PIPA definește informațiile cu caracter personal ca fiind informații referitoare la o persoană în viață care permit identificarea persoanei respective în mod direct, de exemplu cu ajutorul numelui, al numărului de înregistrare pentru rezidenți sau al imaginii sale, ori în mod indirect, și anume atunci când informațiile care nu permit în sine identificarea unei anumite persoane pot fi combinate cu ușurință cu alte informații. Posibilitatea ca informațiile să poată fi combinate „cu ușurință” depinde de probabilitatea rezonabilă a unei astfel de combinări, ținând seama de posibilitatea de a obține alte informații, precum și de timpul, costul și tehnologia necesare pentru identificarea unei persoane.

(16) În plus, informațiile pseudonimizate – și anume, informații care nu pot conduce la identificarea unei anumite persoane fără a fi utilizate sau combinate cu informații suplimentare pentru a le readuce la starea inițială – sunt considerate date cu caracter personal în temeiul PIPA [articolul 2 alineatul (1) litera (c) din PIPA]. În schimb, informațiile care sunt complet „anonimizate” sunt excluse din domeniul de aplicare al PIPA (articolul 58-2 din PIPA). Acesta este cazul informațiilor care nu pot conduce la identificarea unei anumite persoane, chiar dacă sunt combinate cu alte informații, ținând seama de timpul, costul și tehnologia necesare în mod rezonabil pentru identificare.

(17) Aceasta corespunde domeniului de aplicare material al Regulamentului (UE) 2016/679 și noțiunilor de „date cu caracter personal”, „pseudonimizare” ([24]) și „informații anonimizate” ([25]) prevăzute de acesta.

([21]) Articolul 2 alineatul (1) din CIA.

([22]) Comisia pentru servicii financiare este autoritatea de supraveghere pentru sectorul financiar din Coreea și, în această calitate, asigură, de asemenea, executarea CIA.

([23]) În cazul în care acest lucru s-ar schimba în viitor, de exemplu prin extinderea jurisdicției PIPC la toate prelucrările de informații cu caracter personal privind creditele în temeiul CIA, s-ar putea lua în considerare modificarea deciziei privind caracterul adecvat al nivelului de protecție pentru a include și entitățile care fac în prezent obiectul supravegherii Comisiei pentru servicii financiare.

([24]) În cadrul PIPA, „prelucrarea pseudonimizată” este considerată o prelucrare prin metode cum ar fi ștergerea parțială a datelor cu caracter personal sau înlocuirea parțială sau integrală a datelor cu caracter personal, astfel încât nicio persoană să nu poată fi recunoscută fără informații suplimentare [articolul 2 alineatele (1)-(2) din PIPA]. Aceasta corespunde definiției noțiunii de „pseudonimizare” de la articolul 4 punctul 5 din Regulamentul (UE) 2016/679, care se referă la „prelucrarea datelor cu caracter personal într-un asemenea mod încât acestea să nu mai poată fi atribuite unei anume persoane vizate fără a se utiliza informații suplimentare, cu condiția ca aceste informații suplimentare să fie stocate separat și să facă obiectul unor măsuri de natură tehnică și organizatorică care să asigure neatribuirea respectivelor date cu caracter personal unei persoane fizice identificate sau identificabile”.

([25]) În special, considerentul 26 din Regulamentul (UE) 2016/679 clarifică faptul că regulamentul nu se aplică informațiilor anonimizate, și anume informațiilor care nu se referă la o persoană fizică identificată sau identificabilă. Acest lucru depinde, la rândul său, de toate mijloacele care pot fi utilizate în mod rezonabil, fie de către operator, fie de o altă persoană, pentru a identifica persoana fizică în mod direct sau indirect. Pentru a se stabili dacă este probabil, în mod rezonabil, să fie utilizate astfel de mijloace, trebuie luați în considerare toți factorii obiectivi, precum costurile și intervalul de timp necesare pentru identificare, ținându-se seama atât de tehnologia disponibilă la momentul prelucrării, cât și de dezvoltarea tehnologică.

2.2.2 *Definiția prelucrării*

(18) Noțiunea de „prelucrare” este definită pe larg în PIPA ca acoperind „colectarea, generarea, conectarea, centralizarea, înregistrarea, stocarea, păstrarea, prelucrarea cu valoare adăugată, editarea, extragerea, producerea, rectificarea, recuperarea, utilizarea, furnizarea și divulgarea, distrugerea informațiilor cu caracter personal și alte activități similare” ([26]). Deși anumite dispoziții din PIPA se referă numai la anumite tipuri de prelucrare, cum ar fi „utilizarea”, „furnizarea” sau „colectarea” ([27]), noțiunea de „utilizare” se interpretează ca incluzând orice tip de prelucrare cu excepția „colectării” sau „furnizării (către terți)”. Această interpretare largă a noțiunii de „utilizare” garantează astfel că nu există lacune în materie de protecție în legătură cu anumite activități de prelucrare. Prin urmare, conceptul de „prelucrare” corespunde aceleiași noțiuni din Regulamentul (UE) 2016/679.

2.2.3 *Operatorul de informații cu caracter personal și „destinatarul externalizării”*

(19) PIPA se aplică „operatorilor de informații cu caracter personal” (operator). Similar Regulamentului (UE) 2016/679, PIPA include orice instituție publică, persoană juridică, organizație sau persoană fizică care prelucrează date cu caracter personal în mod direct sau indirect pentru a gestiona fișiere de date cu caracter personal în cadrul activităților lor ([28]). În acest context, „dosar cu informații cu caracter personal” înseamnă orice „set sau seturi de informații cu caracter personal dispuse sau organizate în mod sistematic pe baza unei anumite reguli pentru facilitarea accesului la informațiile cu caracter personal” [articolul 2 alineatul (4) din PIPA] ([29]). Pe plan intern, operatorul are obligația de a forma persoanele implicate în prelucrare aflate în subordinea sa, cum ar fi agenții sau angajații societății, și de a exercita controlul și supravegherea corespunzătoare [articolul 28 alineatul (1) din PIPA].

(20) Atunci când un operator („entitatea care efectuează externalizarea”) externalizează prelucrarea datelor cu caracter personal către o parte terță („destinatarul externalizării”) se aplică obligații specifice. În special, externalizarea trebuie să fie reglementată de un acord obligatoriu din punct de vedere juridic (de regulă, un contract) ([30]) care să stabilească domeniul de aplicare al activității externalizate, scopul prelucrării, garanțiile tehnice și de gestionare care trebuie aplicate, supravegherea de către operator, răspunderea (cum ar fi despăgubirile pentru daunele cauzate de o încălcare a obligațiilor contractuale), precum și limitările oricărei subcontractări a serviciilor de prelucrare a datelor ([31]) [articolul 26 alineatele (1) și (2) din PIPA coroborate cu articolul 28 alineatul (1) din Decretul de punere în aplicare] ([32]).

(21) În plus, operatorul trebuie să publice și să actualizeze în permanență detaliile privind activitatea externalizată și identitatea destinatarului externalizării sau, în măsura în care prelucrarea externalizată se referă la activități de marketing direct, să notifice direct persoanelor în cauză informațiile relevante [articolul 26 alineatele (2) și (3) din PIPA coroborate cu articolul 28 alineatele (2)-(5) din Decretul de punere în aplicare] ([33]).

(22) În plus, în conformitate cu articolul 26 alineatul (4) din PIPA coroborat cu articolul 28 alineatul (6) din Decretul de punere în aplicare, operatorul are obligația de a-l „educa” pe destinatarul externalizării cu privire la măsurile de securitate necesare și de a supraveghea, inclusiv prin inspecții, dacă acesta respectă toate obligațiile operatorului în temeiul PIPA ([34]), precum și în temeiul contractului de externalizare. În cazul în care destinatarul externalizării cauzează prejudicii ca urmare a unei încălcări a PIPA, acțiunile sale sau abținerea sa de a acționa vor fi atribuite operatorului în scopuri legate de răspundere, precum în cazul unui angajat [articolul 26 alineatul (6) din PIPA].

([26]) Articolul 2 alineatul (2) din PIPA.

([27]) De exemplu, articolele 15-19 din PIPA fac trimitere numai la colectarea, utilizarea și furnizarea de informații cu caracter personal.

([28]) Articolul 2 alineatul (5) din PIPA. Instituțiile publice în sensul PIPA includ toate departamentele sau agențiile administrative centrale și organismele afiliate acestora, administrațiile locale, școlile și corporațiile publice cu investiții ale administrațiilor locale, organismele administrative ale Adunării Naționale și sistemul judiciar (inclusiv Curtea Constituțională) [articolul 2 alineatul (6) din PIPA coroborat cu articolul 2 din Decretul de punere în aplicare a PIPA].

([29]) Aceasta corespunde domeniului de aplicare material al Regulamentului (UE) 2016/679. În conformitate cu articolul 2 alineatul (1) din Regulamentul (UE) 2016/679, regulamentul se aplică „prelucrării datelor cu caracter personal, efectuată total sau parțial prin mijloace automatizate, precum și prelucrării prin alte mijloace decât cele automatizate a datelor cu caracter personal care fac parte dintr-un sistem de evidență a datelor sau care sunt destinate să facă parte dintr-un sistem de evidență a datelor”. Articolul 4 punctul 6 din Regulamentul (UE) 2016/679 definește „sistemul de evidență a datelor” ca fiind „orice set structurat de date cu caracter personal accesibile conform unor criterii specifice”. În acest sens, în considerentul 15 se explică faptul că protecția persoanelor fizice ar trebui să se aplice „prelucrării datelor cu caracter personal prin mijloace automatizate, precum și prelucrării manuale, în cazul în care datele cu caracter personal sunt cuprinse sau destinate să fie cuprinse într-un sistem de evidență. Dosarele sau seturile de dosare, precum și copertele acestora, care nu sunt structurate în conformitate cu criterii specifice nu ar trebui să intre în domeniul de aplicare al prezentului regulament”.

([30]) A se vedea Manualul PIPA, capitolul III secțiunea 2 privind articolul 26 (p. 203-212), care explică faptul că articolul 26 alineatul (1) din PIPA se referă la acorduri obligatorii, cum ar fi contracte sau acorduri similare.

([31]) În conformitate cu articolul 26 alineatul (5) din PIPA, persoanei împuternicite de operator îi este interzis să utilizeze orice informație cu caracter personal în afara domeniului de aplicare al activității externalizate sau să furnizeze informații cu caracter personal unei părți terțe. Nerespectarea acestei cerințe poate conduce la impunerea unei sancțiuni penale în temeiul articolului 71 punctul 2 din PIPA.

([32]) Nerespectarea acestei cerințe poate conduce la aplicarea unei amenzi; a se vedea articolul 75 alineatul (4) punctul 4 din PIPA.

([33]) Nerespectarea acestei cerințe poate conduce la impunerea unei amenzi; a se vedea articolul 75 alineatul (2) punctul 1 și alineatul (4) punctul 5 din PIPA.

([34]) A se vedea, de asemenea, articolul 26 alineatul (7) din PIPA, conform căruia articolele 15-25, 27-31, 33-38 și 50 se aplică *mutatis mutandis* persoanei împuternicite de operator.

(23) Deși PIPA nu utilizează, prin urmare, concepte diferite pentru „operatori” și „persoane împuternicite de operatori”, normele privind externalizarea prevăd, în esență, obligații și garanții echivalente cu cele care reglementează relația dintre operatori și persoanele împuternicite de operatori în temeiul Regulamentului (UE) 2016/679.

2.2.4 *Dispoziții speciale pentru furnizorii de servicii din domeniul informațiilor și comunicațiilor*

(24) Deși PIPA se aplică prelucrării datelor cu caracter personal de către orice operator, anumite dispoziții conțin norme specifice (drept *lex specialis*) pentru prelucrarea datelor cu caracter personal ale „utilizatorilor” de către „furnizorii de servicii din domeniul informațiilor și comunicațiilor” ([35]). Noțiunea de „utilizatori” cuprinde persoanele fizice care utilizează servicii de informații și comunicații (articolul 2 alineatul (1) paragraful 4 din Legea privind promovarea utilizării rețelelor de informații și comunicații și protecția datelor, Legea privind rețelele). Pentru aceasta, este necesar ca persoana respectivă fie să utilizeze în mod direct serviciile de telecomunicații furnizate de un operator coreean de telecomunicații, fie să utilizeze serviciile de informații ([36]) furnizate în scop comercial (adică în scop lucrativ) de către o entitate care, la rândul său, se bazează pe serviciile unui operator de telecomunicații autorizat/înregistrat în Coreea ([37]). În ambele cazuri, entitatea care are obligații în temeiul dispozițiilor PIPA specifice este una care oferă un serviciu online direct unei persoane (adică unui utilizator).

(25) În schimb, o constatare a caracterului adecvat se referă exclusiv la nivelul de protecție conferit datelor cu caracter personal transferate de la un operator/o persoană împuternicită de operator din Uniune către o entitate dintr-o țară terță (în acest caz: Republica Coreea). În scenariul din urmă, persoanele fizice din Uniune vor avea, în mod normal, o relație directă numai cu „exportatorul de date” din Uniune, dar nu și cu un furnizor coreean de servicii din domeniul informațiilor și comunicațiilor ([38]). Prin urmare, dispozițiile specifice ale PIPA cu privire la datele cu caracter personal ale utilizatorilor de servicii din domeniul informațiilor și comunicațiilor se vor aplica, cel mult, numai în situații limitate, datelor cu caracter personal transferate în temeiul prezentei decizii.

2.2.5 *Exceptarea de la anumite dispoziții ale PIPA*

(26) Articolul 58 alineatul (1) din PIPA exclude aplicarea unei părți din PIPA (și anume a articolelor 15-57) în ceea ce privește patru categorii de prelucrare a datelor ([39]). În special, părțile din PIPA care tratează motivele specifice ale prelucrării, anumite obligații în materie de protecție a datelor, normele detaliate de exercitare a drepturilor individuale, precum și normele care reglementează soluționarea litigiilor de către Comitetul pentru medierea litigiilor în materie de informații cu caracter personal nu se aplică. Alte dispoziții de bază ale PIPA rămân aplicabile, în special dispozițiile generale referitoare la principiile privind protecția datelor (articolul 3 din PIPA) – inclusiv, de exemplu, principiile legalității, specificării scopului și limitării scopului, reducerea la minimum a datelor, exactitatea și securitatea datelor – și drepturile individuale (de acces, rectificare, ștergere și suspendare; a se vedea articolul 4 din PIPA). În plus, articolul 58 alineatul (4) din PIPA impune obligații specifice pentru aceste activități de prelucrare, și anume în ceea ce privește reducerea la minimum a datelor, păstrarea limitată a datelor, măsurile de securitate și tratarea plângerilor ([40]). În consecință, persoanele fizice pot depune în continuare o plângere la PIPC în cazul nerespectării acestor principii și obligații, iar PIPC are competența de a lua măsuri de asigurare a respectării legislației în caz de neconformitate.

([35]) A se vedea în special articolul 18 alineatul (2) și capitolul VI din PIPA.

([36]) Serviciile de informații cuprind atât furnizarea de informații, cât și furnizarea de servicii de intermediere pentru furnizarea de informații.

([37]) A se vedea articolul 2 alineatul (1) punctul 3 [coroborat cu articolul 2 alineatul (1) punctele 2 și 4] din Legea privind rețelele și articolul 2 alineatele (6) și (8) din Legea privind activitățile de telecomunicații.

([38]) În măsura în care furnizorii coreeni de servicii din domeniul informațiilor și comunicațiilor ar avea o relație directă cu persoane din UE (prin oferirea de servicii online), acest lucru ar putea atrage aplicarea directă a Regulamentului (UE) 2016/679, în temeiul articolului 3 alineatul (2) litera (a) din acesta.

([39]) Articolul 58 alineatul (2) din PIPA prevede, de asemenea, că articolele 15 și 22, articolul 27 alineatele (1)-(2), articolele 34 și 37 nu se aplică informațiilor cu caracter personal prelucrate prin intermediul dispozitivelor de prelucrare vizuală a datelor instalate și exploatate în locuri deschise. Întrucât această dispoziție se referă la utilizarea supravegherii video în Coreea, și anume colectarea directă de informații cu caracter personal de la persoane din Coreea, aceasta nu este relevantă în sensul prezentei decizii, care se referă la transferurile de date cu caracter personal de la operatori/persoane împuternicite de operatori din UE către entități din Coreea. În plus, în conformitate cu articolul 58 alineatul (3) din PIPA, articolul 15 (colectarea și utilizarea informațiilor cu caracter personal), articolul 30 (obligația de a institui o politică publică în materie de confidențialitate) și articolul 31 (obligația de a numi un responsabil cu protecția vieții private) nu se aplică informațiilor cu caracter personal care sunt prelucrate pentru a gestiona grupuri sau asociații bazate pe relații de prietenie (de exemplu, cluburi de hobby-uri). Deoarece astfel de grupuri sunt considerate a fi de natură personală, fără legătură cu o activitate profesională sau comercială, nu este necesar niciun temei juridic specific (cum ar fi consimțământul persoanelor în cauză) pentru a colecta și utiliza informațiile lor în acest context. Cu toate acestea, continuă să se aplice toate celelalte dispoziții ale PIPA (de exemplu, reducerea la minimum a datelor, limitarea scopului, legalitatea prelucrării, securitatea și drepturile individuale). În plus, orice prelucrare a informațiilor cu caracter personal în afara scopului înființării unui grup social nu ar beneficia de exceptare.

([40]) Mai precis, articolul 58 alineatul (4) din PIPA prevede obligația de a prelucra informațiile cu caracter personal în măsura minimă necesară pentru atingerea scopului preconizat, de a le prelucra pe durata minimă și de a lua măsurile necesare pentru gestionarea în condiții de siguranță și prelucrarea adecvată a acestor informații cu caracter personal. Aceasta din urmă include garanții tehnice, de gestionare și fizice, precum și măsuri de asigurare a tratării corespunzătoare a fiecărei plângeri în parte.

(27) În primul rând, exceptarea parțială vizează datele cu caracter personal colectate în temeiul Legii privind statisticile pentru prelucrarea de către instituțiile publice. Conform clarificărilor primite din partea guvernului coreean, datele cu caracter personal prelucrate în acest context se referă în mod normal la cetățenii coreeni și ar putea include numai în mod excepțional informații privind străinii, și anume în cazul statisticilor privind intrarea pe teritoriu și ieșirea de pe teritoriu sau privind investițiile străine. Cu toate acestea, chiar și în aceste situații, astfel de date nu sunt în mod normal transferate de la operatori/persoane împuternicite de operatori din Uniune, ci, mai degrabă, ar fi colectate direct de autoritățile publice din Coreea ([41]). În plus, în mod similar cu ceea ce prevede considerentul 162 din Regulamentul (UE) 2016/679, prelucrarea datelor în temeiul Legii privind statisticile face obiectul mai multor condiții și garanții. În special, Legea privind statisticile impune obligații specifice, cum ar fi aceea de a asigura exactitatea, consecvența și imparțialitatea; a garanta confidențialitatea persoanelor fizice; a proteja informațiile respondenților care participă la sondaje statistice, inclusiv cu scopul de a preveni utilizarea acestor informații în orice alt scop decât cel de elaborare a statisticilor și de a impune angajaților anumite cerințe de confidențialitate ([42]). Autoritățile publice care prelucrează statisticile trebuie, de asemenea, să respecte, printre altele, principiile reducerii la minimum a datelor, limitării scopului și securității [articolul 3 și articolul 58 alineatul (4) din PIPA] și să le permită persoanelor fizice să își exercite drepturile (de acces, rectificare, ștergere și suspendare; a se vedea articolul 4 din PIPA). În cele din urmă, datele trebuie prelucrate într-o formă anonimizată sau pseudonimizată dacă aceasta permite îndeplinirea scopului prelucrării [articolul 3 alineatul (7) din PIPA].

(28) În al doilea rând, articolul 58 alineatul (1) din PIPA se referă la datele cu caracter personal colectate sau solicitate pentru analiza informațiilor legate de securitatea națională. Domeniul de aplicare și consecințele acestei exceptări parțiale sunt descrise mai detaliat în considerentul 149.

(29) În al treilea rând, exceptarea parțială se aplică prelucrării temporare a datelor cu caracter personal atunci când acest lucru este necesar de urgență din motive de siguranță sau de securitate publică, inclusiv de sănătate publică. Această categorie este interpretată strict de PIPC și, conform informațiilor primite, nu a fost utilizată niciodată. Aceasta se aplică numai în situații de urgență care necesită acțiuni urgente, de exemplu pentru monitorizarea agenților infecțioși sau pentru salvarea și ajutorarea victimelor dezastrelor naturale ([43]). Chiar și în aceste situații, exceptarea parțială vizează numai prelucrarea datelor cu caracter personal pe o perioadă limitată de timp pentru realizarea unei astfel de acțiuni. Situațiile în care acest lucru s-ar putea aplica transferurilor de date care fac obiectul prezentei decizii sunt și mai limitate, având în vedere probabilitatea redusă ca datele cu caracter personal transferate din Uniune către operatorii coreeni să fie de tipul celor care ar putea face ca prelucrarea ulterioară a acestora să fie „necesară de urgență” pentru astfel de situații de urgență.

(30) În cele din urmă, exceptarea parțială se aplică datelor cu caracter personal colectate sau utilizate de presă, pentru activități misionare ale organizațiilor religioase sau pentru numirea candidaților de către partidele politice. Exceptarea se aplică numai în cazul în care datele cu caracter personal sunt prelucrate de către presă, organizații religioase sau partide politice în aceste scopuri specifice (și anume, activități jurnalistice, activități misionare și numirea candidaților politici). În cazul în care entitățile respective prelucrează date cu caracter personal în alte scopuri, cum ar fi gestionarea resurselor umane sau administrarea internă, PIPA se aplică integral.

(31) În ceea ce privește prelucrarea datelor cu caracter personal de către presă pentru activități jurnalistice, echilibrul dintre libertatea de exprimare și alte drepturi (inclusiv dreptul la viață privată) este prevăzut în Legea privind arbitrajul și măsurile reparatorii etc. pentru daunele cauzate de articolele de presă (Legea presei) ([44]). În special, articolul 5 din Legea presei prevede că presa (și anume, orice organizație de radiodifuziune și televiziune, ziar,

([41]) În acest sens, articolul 33 din Legea privind statisticile impune instituțiilor publice obligația de a proteja informațiile respondenților care participă la sondaje statistice, inclusiv cu scopul de a împiedica utilizarea acestor informații în orice alt scop decât cel de elaborare a statisticilor.

([42]) Articolul 2 alineatele (2)-(3), articolul 30 alineatul (2), articolele 33 și 34 din Legea privind statisticile.

([43]) Manualul PIPA, secțiunea privind articolul 58.

([44]) De exemplu, articolul 4 din Legea presei prevede că articolele de presă trebuie să fie imparțiale și obiective, să servească interesului public, să respecte demnitatea și valoarea umană și să nu defăimeze alte persoane și să nu încalce drepturile acestora, moralitatea publică sau etica socială.

publicație periodică sau ziar online), serviciile de știri online și organizațiile de radiodifuziune și televiziune multimedia online nu pot încălca dreptul persoanelor fizice la viață privată. Cu toate acestea, în cazul în care are loc o încălcare a dreptului la viață privată, aceasta trebuie remediată cu promptitudine, în conformitate cu procedurile specifice prevăzute în lege. În acest sens, legea le acordă persoanelor fizice care suferă prejudicii ca urmare a unui articol de presă o serie de drepturi, cum ar fi obținerea publicării unei corectări a unei declarații false, a unei rectificări prin intermediul unei declarații contradictorii sau a unui alt articol (în cazul în care un articol de presă se referă la acuzații privind infracțiuni de care persoana este achitată ulterior) ([45]). Plângerile formulate de persoanele fizice pot fi soluționate de organele de presă în mod direct (prin intermediul unui ombudsman) ([46]), prin conciliere sau arbitraj (în fața unei comisii specializate de arbitraj pentru presă) ([47]) sau în fața instanțelor judecătorești. De asemenea, persoanele fizice pot obține despăgubiri atunci când suferă daune financiare, încălcarea unui drept referitor la personalitate sau orice alte suferințe emoționale cauzate de un act ilegal al presei (intenționat sau din neglijență) ([48]). Presa este exonerată de răspundere în temeiul legii în măsura în care un articol de presă care aduce atingere drepturilor unei persoane nu este contrar valorilor sociale și este publicat fie cu consimțământul persoanei în cauză, fie în interes public (și există suficiente motive pentru a considera că articolul prezintă adevărul) ([49]).

(32) Întrucât prelucrarea datelor cu caracter personal de către presă în scopul desfășurării activităților jurnalistice face, prin urmare, obiectul unor garanții specifice care decurg din Legea presei, nu există astfel de garanții suplimentare care să încadreze utilizarea excepțiilor pentru activitățile de prelucrare desfășurate de organizațiile religioase și de partidele politice într-un mod comparabil cu dispozițiile articolelor 85, 89 și 91 din Regulamentul (UE) 2016/679. Prin urmare, Comisia consideră oportun să excludă din domeniul de aplicare al prezentei decizii organizațiile religioase, în măsura în care acestea prelucrează date cu caracter personal pentru activitățile lor misionare, și partidele politice, în măsura în care acestea prelucrează date cu caracter personal în contextul numirii candidaților.

2.3 **Garanții, drepturi și obligații**

2.3.1 *Legalitatea și echitatea prelucrării*

(33) Datele cu caracter personal ar trebui prelucrate în mod legal și echitabil.

(34) Acest principiu este prevăzut la articolul 3 alineatele (1) și (2) din PIPA și este consolidat de articolul 59 din PIPA, care interzice prelucrarea datelor cu caracter personal „prin fraudă, mijloace necorespunzătoare sau nedrepte”, „fără autoritate juridică” sau „în afara autorității juridice corespunzătoare” ([50]). Aceste principii generale ale prelucrării legale sunt elaborate la articolele 15-19 din PIPA, care stabilesc diferitele temeiuri juridice pentru prelucrare (colectare, utilizare și furnizare către terți), inclusiv circumstanțele în care aceasta poate implica o modificare a scopului (articolul 18 din PIPA).

([45]) Articolele 15-17 din Legea presei.

([46]) Fiecare canal de presă sau mass-media trebuie să aibă propriul ombudsman pentru a preveni și a remedia eventualele prejudicii cauzate de presă (de exemplu, prin recomandarea corectării articolelor de presă care sunt false sau aduc atingere reputației altora); articolul 6 din Legea presei.

([47]) Comisia este formată din 40 până la 90 de comisari de arbitraj, numiți de ministrul culturii, sportului și turismului din rândul persoanelor calificate drept judecători, avocați, persoane implicate în colectarea de știri sau realizarea de reportaje timp de cel puțin 10 ani sau alte persoane cu expertiză în domeniul presei. Comisarii de arbitraj nu pot fi, în același timp, funcționari publici, membri ai partidelor politice sau jurnaliști. În conformitate cu articolul 8 din Legea presei, comisarii de arbitraj trebuie să își îndeplinească sarcinile în mod independent și nu pot primi indicații sau instrucțiuni în legătură cu aceste sarcini. În plus, sunt în vigoare norme specifice pentru a preveni conflictele de interese, de exemplu excluderea comisarilor individuali de la examinarea cazurilor individuale în care soțul/soția sau rudele acestora sunt părți în cauză (articolul 10 din Legea presei). Comisia poate soluționa litigii prin conciliere sau arbitraj, dar poate, de asemenea, să prevadă recomandări pentru remedierea încălcărilor (secțiunea 5 din Legea presei).

([48]) Articolul 30 din Legea presei.

([49]) Articolul 5 din Legea presei.

([50]) Articolul 59 din PIPA interzice oricărei persoane „care prelucrează sau a prelucrat vreodată informații cu caracter personal” „să obțină informații cu caracter personal sau să obțină consimțământul pentru prelucrarea informațiilor cu caracter personal prin fraudă, prin mijloace necorespunzătoare sau nedrepte”, „să divulge informațiile cu caracter personal dobândite în cadrul activității sau să le furnizeze pentru a fi utilizate de către orice terț fără autoritate” sau „să deterioreze, să distrugă, să modifice, să falsifice sau să divulge alte informații cu caracter personal fără a avea autoritate juridică sau în afara unei autorități juridice corespunzătoare”. O încălcare a acestei interdicții poate conduce impunerea de sancțiuni penale; a se vedea articolul 71 alineatele (5) și (6) și articolul 72 alineatul (2) din PIPA. În plus, articolul 70 alineatul (2) din PIPA permite impunerea unei sancțiuni penale pentru obținerea de informații cu caracter personal prelucrate de terți prin fraudă sau alte mijloace sau metode nedrepte ori pentru furnizarea acestora către un terț în scopuri lucrative sau nedrepte, precum și pentru încurajarea sau organizarea unui astfel de comportament.

(35) În conformitate cu articolul 15 alineatul (1) din PIPA, un operator poate colecta date cu caracter personal (în domeniul de aplicare al colectării) numai pe baza unui număr limitat de temeiuri juridice. Acestea sunt (1) consimțământul persoanei vizate ([51]) (punctul 1); (2) necesitatea de a executa și de a duce la îndeplinire un contract cu persoana vizată (punctul 4); (3) o autorizație specială prevăzută de lege sau necesitatea respectării unei obligații legale (punctul 2); necesitatea ([52]) ca o instituție publică să îndeplinească sarcinile în jurisdicția sa, astfel cum prevede legea; (4) necesitatea evidentă de a proteja viața, integritatea fizică sau drepturile de proprietate ale persoanei vizate sau ale unei părți terțe împotriva unui pericol iminent (numai în cazul în care persoana vizată nu este în măsură să își exprime intenția sau nu poate obține consimțământul prealabil) (punctul 5); (5) necesitatea de a asigura „interesul justificabil" al operatorului dacă acesta este „în mod evident superior" intereselor persoanei vizate (și numai în cazul în care prelucrarea are o „legătură substanțială" cu interesul legitim și nu depășește ceea ce este rezonabil) (punctul 6) ([53]). Aceste motive de prelucrare sunt în esență echivalente cu cele prevăzute la articolul 6 din Regulamentul (UE) 2016/679, inclusiv motivul privind „interesul justificabil" care este echivalent cu motivul „interesului legitim" de la articolul 6 alineatul (1) litera (f) din Regulamentul (UE) 2016/679.

(36) Odată colectate, datele cu caracter personal pot fi utilizate în scopul colectării [articolul 15 alineatul (1) din PIPA] sau „în domeniul de aplicare legat în mod rezonabil" de scopul colectării, luând în considerare posibilele dezavantaje create pentru persoana vizată și cu condiția să fi fost adoptate măsurile de securitate necesare (de exemplu criptarea) [articolul 15 alineatul (3) din PIPA]. Pentru a stabili dacă scopul utilizării este „legat în mod rezonabil" de scopul inițial al colectării, decretul de punere în aplicare stabilește criterii specifice, care sunt similare cu cele prevăzute la articolul 6 alineatul (4) din Regulamentul (UE) 2016/679. În special, trebuie să existe o relevanță considerabilă pentru scopul inițial; utilizarea suplimentară trebuie să fie previzibilă (de exemplu, având în vedere circumstanțele în care au fost colectate informațiile); și, dacă este posibil, datele trebuie să fie pseudonimizate ([54]). Criteriile specifice utilizate de un operator în această evaluare trebuie să fie dezvăluite în prealabil în politica de confidențialitate ([55]). În plus, responsabilul de protecția vieții private (a se vedea considerentul 94) trebuie să verifice în mod specific dacă utilizarea ulterioară are loc în parametrii respectivi.

([51]) Consimțământul trebuie să fie exprimat în mod liber, în cunoștință de cauză, specific și exprimat într-unul din modurile prevăzute de lege. În orice caz, consimțământul nu poate fi obținut prin fraudă, prin mijloace necorespunzătoare sau nedrepte [articolul 59 alineatul (1) din PIPA]. În primul rând, în conformitate cu articolul 4 punctul 2 din PIPA, persoanele vizate au dreptul „de a-și da sau nu consimțământul" și „de a alege domeniul de aplicare al consimțământului" și ar trebui să fie informate în acest sens [articolul 15 alineatul (2), articolul 16 alineatele (2) și (3), articolul 17 alineatul (2) și articolul 18 alineatul (3) din PIPA]. Articolul 22 alineatul (5) din PIPA conține o garanție suplimentară prin care se interzice unui operator să refuze furnizarea de bunuri sau servicii în cazul în care acest lucru ar putea submina libertatea de alegere a persoanei respective în ceea ce privește acordarea consimțământului. Aceasta include situațiile în care numai anumite tipuri de prelucrare necesită consimțământul (în timp ce altele se bazează pe un contract) și include, de asemenea, prelucrarea ulterioară a datelor cu caracter personal colectate în contextul furnizării de bunuri sau servicii. În al doilea rând, în conformitate cu articolul 15 alineatul (2), articolul 17 alineatele (2) și (3) și articolul 18 alineatul (3) din PIPA, atunci când solicită consimțământul, operatorul trebuie să transmită persoanei vizate „detalii" privind datele cu caracter personal în cauză [de exemplu, că este vorba despre date sensibile; a se vedea articolul 17 alineatul (2) punctul 2 litera (a) din Decretul de punere în aplicare a PIPA], scopul prelucrării, perioada de păstrare și orice destinatar al datelor. Orice astfel de solicitare se face „într-un mod care poate fi recunoscut în mod explicit", care diferențiază aspectele ce necesită consimțământul de alte aspecte [articolul 22 alineatele (1)-(4) din PIPA]. În al treilea rând, articolul 17 alineatul (1) punctele 1-6 din Decretul de punere în aplicare a PIPA prevede modalitățile specifice prin care un operator trebuie să obțină consimțământul, cum ar fi consimțământul scris cu semnătura persoanei vizate sau consimțământul prin e-mail (cu confirmare de primire). Deși PIPA nu conferă în mod specific persoanelor fizice un drept general de a-și retrage consimțământul, persoanele fizice au în schimb dreptul de a obține suspendarea prelucrării datelor care le privesc, care, atunci când este exercitat, va duce la încetarea prelucrării și la ștergerea datelor (a se vedea considerentul 78 privind dreptul la suspendare).

([52]) Conform informațiilor primite de la PIPC, instituțiile publice pot invoca acest motiv numai dacă prelucrarea informațiilor cu caracter personal este inevitabilă, cu alte cuvinte trebuie să fie imposibil sau nerezonabil de dificil pentru instituție să își îndeplinească funcțiile fără a prelucra datele.

([53]) Articolul 39-3 din PIPA impune obligații specifice (mai stricte) furnizorilor de servicii din domeniul informațiilor și comunicațiilor în ceea ce privește colectarea și utilizarea informațiilor cu caracter personal ale utilizatorilor lor. În special, aceasta impune furnizorului să obțină consimțământul utilizatorului, după furnizarea de informații privind scopul colectării/utilizării, categoriile de informații cu caracter personal care urmează să fie colectate și perioada pentru care vor fi prelucrate informațiile [articolul 39-3 alineatul (1) din PIPA]. Același lucru este valabil și atunci când se modifică oricare dintre aceste aspecte. Neobținerea consimțământului pentru colectarea de informații face obiectul unor sancțiuni penale [articolul 71 alineatele (4)-(5) din PIPA]. În mod excepțional, informațiile cu caracter personal ale utilizatorilor pot fi colectate sau utilizate de către furnizorii de servicii din domeniul informațiilor și comunicațiilor fără obținerea consimțământului în prealabil. Acesta este cazul (1) atunci când este în mod clar dificil să se obțină consimțământul normal pentru informațiile cu caracter personal necesare pentru executarea contractului care reglementează furnizarea de servicii din domeniul informațiilor și comunicațiilor, din motive economice și tehnologice (de exemplu, atunci când datele cu caracter personal sunt create în mod inevitabil în procesul de executare a unui contract, cum ar fi informațiile privind facturarea, jurnalele de acces și evidențele de plată); (2) atunci când acest lucru este necesar pentru achitarea tarifelor ca urmare a furnizării serviciilor din domeniul informațiilor și comunicațiilor; sau (3) dacă este permis de alte legi [de exemplu, articolul 21 alineatul (1) punctul 6 din Legea privind protecția consumatorilor în comerțul electronic prevede că operatorii economici pot colecta informații cu caracter personal cu privire la tutorii legali ai unui minor pentru a confirma dacă a fost obținut consimțământul valabil în numele minorului] [articolul 39-3 alineatul (2) din PIPA]. În toate cazurile, furnizorii de servicii din domeniul informațiilor și comunicațiilor nu pot refuza să furnizeze servicii pentru simplul motiv că utilizatorul nu furnizează mai multe informații cu caracter personal decât minimul necesar (și anume, informațiile necesare pentru realizarea elementelor esențiale ale serviciului în cauză); a se vedea articolul 39-3 alineatul (3) din PIPA.

([54]) A se vedea articolul 14-2 din Decretul de punere în aplicare a PIPA.

([55]) Articolul 14-2 alineatul (2) din Decretul de punere în aplicare a PIPA.

(37) Norme similare (dar oarecum mai stricte) se aplică și furnizării de date către un terț. În conformitate cu articolul 17 alineatul (1) din PIPA, furnizarea de date cu caracter personal către un terț este permisă pe baza consimțământului ([56]) sau, în scopul colectării, în cazul în care informațiile au fost colectate pe baza unuia dintre temeiurile juridice prevăzute la articolul 15 alineatul (1) punctele 2, 3 și 5 din PIPA. Aceasta exclude în special orice divulgare întemeiată pe „interesul justificabil" al operatorului. În plus, articolul 17 alineatul (4) din PIPA permite furnizarea către terți „în domeniul de aplicare legat în mod rezonabil" de scopul colectării, luând din nou în considerare posibilele dezavantaje create pentru persoana vizată și cu condiția să fi fost adoptate măsurile de securitate necesare (cum ar fi criptarea). Trebuie luați în considerare aceiași factori ca cei descriși în considerentul 36 pentru a evalua dacă furnizarea se încadrează în domeniul de aplicare în mod rezonabil legat de scopul colectării și se aplică aceleași garanții (și anume, în ceea ce privește transparența prin politica de confidențialitate și implicarea responsabilului cu protecția vieții private).

(38) Primirea datelor cu caracter personal de către un operator de date coreean din Uniune este considerată o „colectare" în sensul articolului 15 din PIPA. Notificarea nr. 2021-5 (secțiunea I din anexa I la prezenta decizie) clarifică faptul că scopul pentru care datele au fost transferate de entitatea în cauză din UE constituie scopul colectării pentru operatorul coreean de date. În consecință, operatorii de date coreeni care primesc date cu caracter personal din Uniune sunt, în principiu, obligați să prelucreze astfel de informații în domeniul de aplicare al transferului, în conformitate cu articolul 17 din PIPA.

(39) Se aplică limitări speciale în cazul în care operatorul dorește să utilizeze datele cu caracter personal sau să le furnizeze unui terț într-un alt scop decât scopul colectării ([57]). În conformitate cu articolul 18 alineatul (2) din PIPA, un operator privat poate, în mod excepțional ([58]), să utilizeze date cu caracter personal sau să le furnizeze unui terț într-un alt scop: (1) pe baza consimțământului suplimentar (adică separat) al persoanei vizate; (2) în cazul în care acest lucru este prevăzut de dispoziții legale speciale; sau (3) în cazul în care acest lucru este în mod evident necesar pentru protecția vieții, a integrității fizice sau a drepturilor de proprietate ale persoanei vizate sau ale unei părți terțe împotriva unui pericol iminent (numai dacă persoana vizată nu este în măsură să își exprime intenția, iar consimțământul prealabil nu se poate obține) ([59]).

(40) Instituțiile publice pot, de asemenea, să utilizeze date cu caracter personal sau să le furnizeze unui terț în scopuri diferite în anumite situații. Acestea includ cazurile în care, în caz contrar, instituțiilor publice le-ar fi imposibil să își îndeplinească obligațiile statutare prevăzute de lege, sub rezerva autorizării de către PIPC. În plus, instituțiile publice pot furniza date cu caracter personal unei alte autorități sau instanțe, dacă acest lucru este necesar pentru investigarea și urmărirea penală a infracțiunilor sau pentru o punere sub acuzare; pentru ca o instanță să își îndeplinească funcțiile legate de procedurile judiciare în curs; sau pentru executarea unei sancțiuni penale ori a unei hotărâri de încredințare sau de îngrijire ([60]). De asemenea, acestea pot furniza date cu caracter personal unui guvern străin sau unei organizații internaționale pentru a se conforma unei obligații legale care decurge dintr-un tratat sau dintr-o convenție internațională, caz în care trebuie, de asemenea, să respecte cerințele privind transferurile transfrontaliere de date (a se vedea considerentul 90).

(41) Prin urmare, principiile legalității și echității prelucrării sunt puse în aplicare în cadrul juridic coreean într-un mod în esență echivalent cu Regulamentul (UE) 2016/679, permițând prelucrarea numai în baza unor temeiuri legitime și clar definite. În plus, în toate cazurile menționate, prelucrarea este permisă numai dacă nu este de natură să „aducă atingere în mod abuziv" intereselor persoanei vizate sau ale unui terț, ceea ce necesită o echilibrare a intereselor. În plus, articolul 18 alineatul (5) din PIPA prevede garanții suplimentare atunci când operatorul furnizează date cu caracter personal unui terț, care pot include o cerere de restricționare a scopului și a metodei de utilizare sau punerea în aplicare a unor măsuri de securitate specifice. Partea terță este, la rândul său, obligată să pună în aplicare măsurile solicitate.

([56]) Încălcarea articolului 17 alineatul (1) punctul 1 din PIPA poate conduce la impunerea de sancțiuni penale [articolul 71 alineatul (1) din PIPA].

([57]) „Scopul preconizat" este scopul pentru care au fost colectate informațiile. De exemplu, atunci când informațiile sunt colectate pe baza consimțământului persoanei în cauză, scopul preconizat este scopul comunicat persoanei respective în temeiul articolului 15 alineatul (2) din PIPA.

([58]) În conformitate cu articolul 18 alineatul (1) din PIPA. Încălcarea articolului 18 alineatele (1) și (2) poate conduce la impunerea de sancțiuni penale [articolul 71 alineatul (2) din PIPA].

([59]) Utilizarea informațiilor cu caracter personal sau furnizarea acestora către un terț de către furnizorii de servicii din domeniul informațiilor și comunicațiilor în alt scop decât cel inițial poate avea loc numai în baza motivelor prevăzute la articolul 18 alineatul (2) punctele 1 și 2 din PIPA (și anume, în cazul în care se obține consimțământul suplimentar sau în cazul în care legislația prevede dispoziții speciale). A se vedea articolul 18 alineatul (2) din PIPA.

([60]) Cu excepția cazului în care prelucrarea este necesară pentru investigarea infracțiunilor, punerea sub acuzare și urmărirea penală, instituțiile publice care utilizează informații cu caracter personal sau le furnizează unui terț în alt scop decât cel al colectării (de exemplu, atunci când acest lucru este permis în mod expres de lege sau necesar pentru a executa un tratat) au obligația de a publica temeiurile juridice ale prelucrării, scopul și domeniul de aplicare al acesteia pe site-ul lor web sau în Monitorul Oficial și de a ține evidențe în acest sens [articolul 18 alineatul (4) din PIPA și articolul 15 din Decretul de punere în aplicare a PIPA].

(42) În cele din urmă, articolul 28-2 din PIPA permite prelucrarea (ulterioară) a informațiilor pseudonimizate fără consimțământul persoanei în cauză în scopuri statistice, de cercetare științifică ([61]) și de arhivare în interes public, sub rezerva unor garanții specifice. Ca și Regulamentul (UE) 2016/679 ([62]), PIPA facilitează, prin urmare, prelucrarea (ulterioară) a datelor cu caracter personal în astfel de scopuri într-un cadru care să prevadă garanții adecvate pentru protejarea drepturilor persoanelor fizice. În loc să se bazeze pe pseudonimizare ca o posibilă garanție, PIPA o impune ca o condiție prealabilă pentru desfășurarea anumitor activități de prelucrare în scopuri statistice, de cercetare științifică și de arhivare în interes public (cum ar fi posibilitatea de a prelucra datele fără consimțământ sau de a combina seturi de date diferite).

(43) În plus, PIPA impune o serie de garanții specifice, în special în ceea ce privește măsurile tehnice și organizatorice necesare, ținerea evidențelor, limitări privind schimbul de date și abordarea posibilelor riscuri de reidentificare. Combinarea diferitelor garanții descrise în considerentele 44-48 asigură faptul că prelucrarea datelor cu caracter personal în acest context face obiectul unor măsuri de protecție în esență echivalente cu cele care ar fi necesare în conformitate cu Regulamentul (UE) 2016/679.

(44) În primul rând și cel mai important, articolul 28-5 alineatul (1) din PIPA interzice prelucrarea informațiilor pseudonimizate în scopul identificării unei anumite persoane. Dacă informațiile care ar putea identifica o persoană ar fi totuși generate în timpul prelucrării informațiilor pseudonimizate, operatorul trebuie să suspende imediat prelucrarea și să distrugă aceste informații [articolul 28-5 alineatul (2) din PIPA]. Nerespectarea acestor dispoziții face obiectul unor amenzi administrative și constituie o infracțiune ([63]). Aceasta înseamnă că, chiar și în situațiile în care ar fi *practic* posibil să se reidentifice persoana, o astfel de reidentificare este interzisă din punct de vedere *juridic*.

(45) În al doilea rând, atunci când prelucrează (ulterior) informații pseudonimizate în astfel de scopuri, operatorul trebuie să instituie măsuri tehnologice, de gestionare și fizice specifice pentru a asigura securitatea informațiilor (inclusiv stocarea și gestionarea separată a informațiilor care sunt necesare pentru a readuce informațiile pseudonimizate la starea lor inițială) ([64]). În plus, trebuie să se țină evidențe ale informațiilor pseudonimizate prelucrate, ale scopului prelucrării, ale istoricului utilizării și ale eventualilor terți beneficiari [articolul 29-5 alineatul (2) din Decretul de punere în aplicare a PIPA].

(46) În al treilea și ultimul rând, PIPA prevede garanții specifice pentru a împiedica identificarea persoanelor fizice de către terți în cazul în care informațiile sunt partajate. În special, atunci când furnizează informații pseudonimizate unui terț în scopuri statistice, de cercetare științifică sau de arhivare în interes public, operatorii nu pot include informații care ar putea fi utilizate pentru a identifica o anumită persoană [articolul 28-2 alineatul (2) din PIPA] ([65]).

(47) Mai precis, deși PIPA permite combinarea informațiilor pseudonimizate (prelucrate de diferiți operatori) în scopuri statistice, de cercetare științifică sau de arhivare în interes public, rezervă această competență instituțiilor specializate dotate cu mecanisme de securitate specifice [articolul 28-3 alineatul (1) din PIPA] ([66]). Atunci când solicită o combinare de date pseudonimizate, operatorul trebuie să prezinte documentația privind, printre altele, datele care urmează să fie combinate, scopul combinării, precum și măsurile de securitate propuse pentru prelucrarea datelor

([61]) Cercetarea științifică este definită la articolul 2 alineatul (8) din PIPA ca fiind „cercetarea care aplică metode științifice, cum ar fi dezvoltarea tehnologică și demonstrarea, cercetarea fundamentală, cercetarea aplicată și cercetarea finanțată din fonduri private". Aceste categorii corespund celor stabilite în considerentul 159 din Regulamentul (UE) 2016/679.

([62]) A se vedea articolul 5 alineatul (1) litera (b) și articolul 89 alineatele (1)-(2), precum și considerentele 50 și 157 din Regulamentul (UE) 2016/679.

([63]) A se vedea articolul 28-6 alineatul (1), articolul 71 punctul 4-3 și articolul 75 alineatul (2) punctul 4-4 din PIPA.

([64]) Articolul 28-4 din PIPA și articolul 29-5 din Decretul de punere în aplicare a PIPA. Nerespectarea acestei obligații face obiectul unor sancțiuni administrative și penale; a se vedea articolul 73 alineatul (1) și articolul 75 alineatul (2) punctul 6 din PIPA.

([65]) Încălcarea acestor cerințe poate conduce la impunerea de sancțiuni penale [articolul 71 alineatul (2) din PIPA]. PIPC a început imediat să pună în aplicare aceste noi norme, de exemplu prin decizia sa din 28 aprilie 2021, prin care a impus o amendă și măsuri de remediere împotriva unei societăți care, printre alte încălcări ale PIPA, nu a respectat cerința de la articolul 28-2 alineatul (2) din PIPA; a se vedea https://www.pipc.go.kr/np/cop/bbs/selectBoardArticle.do?bbsId=BS074&mCode=C020010000&nttId=7298&fbclid=IwAR3SKcMQi6G5pR9k4I7j6GNXtc8aBVDOwcUReVvzQtYI7AS40UKYXoOXo8.

([66]) Pentru a fi desemnată drept instituție specializată (o „agenție specializată în combinarea datelor"), trebuie depusă la PIPC o cerere însoțită de documente justificative care să detalieze, printre altele, mecanismele și echipamentele existente pentru combinarea în siguranță a datelor pseudonimizate și care să confirme că solicitantul are cel puțin trei angajați cu normă întreagă cu calificări sau experiență în domeniul protecției datelor cu caracter personal [articolul 29-2 alineatele (1)-(2) din Decretul de punere în aplicare a PIPA]. Cerințele detaliate, de exemplu în ceea ce privește calificările personalului, mecanismele disponibile, măsurile de securitate, politicile și procedurile interne, precum și cerințele financiare, sunt prevăzute în Notificarea nr. 2020-9 a PIPC privind combinarea și difuzarea informațiilor pseudonimizate (graficul I). Desemnarea drept agenție specializată în combinarea datelor poate fi revocată de PIPC (după organizarea unei audieri) din anumite motive, de exemplu, în cazul în care agenția nu mai îndeplinește standardele de securitate necesare pentru desemnare sau în cazul în care a avut loc o încălcare a securității datelor în contextul combinării datelor [articolul 29-2 alineatele (5)-(6) din Decretul de punere în aplicare a PIPA]. PIPC trebuie să publice fiecare desemnare (sau revocare a desemnării) a unei agenții specializate în combinarea datelor [articolul 29-2 alineatul (7) din Decretul de punere în aplicare a PIPA].

combinate ([67]). Pentru a permite combinarea datelor, operatorul trebuie să trimită datele care urmează să fie combinate către instituția specializată și să furnizeze o „cheie de combinare” (și anume, informațiile care au fost utilizate pentru pseudonimizare) către Agenția coreeană pentru internet și securitate ([68]). Aceasta din urmă generează „date de legătură între cheile de combinare” (care permit corelarea cheilor de combinare ale diferiților solicitanți pentru a realiza combinarea seturilor de date) și le furnizează instituției specializate ([69]).

(48) Operatorul care solicită combinarea poate analiza informațiile combinate la sediul instituției specializate, într-un spațiu în care se aplică măsuri de securitate tehnice, fizice și administrative specifice (articolul 29-3 din Decretul de punere în aplicare a PIPA). Operatorii care contribuie cu un set de date pentru o astfel de combinare pot scoate datele combinate în afara instituției specializate numai după pseudonimizarea sau anonimizarea ulterioară a datelor combinate și cu aprobarea instituției respective [articolul 28-3 alineatul (2) din PIPA] ([70]). Atunci când analizează dacă să acorde sau să nu acorde o astfel de aprobare, instituția va evalua legătura dintre datele combinate și scopul prelucrării și dacă a fost elaborat un plan de securitate specific pentru utilizarea acestor date ([71]). Exportarea informațiilor combinate în afara instituției nu va fi permisă dacă informațiile conțin date care ar permite identificarea unei persoane ([72]). În cele din urmă, combinarea și difuzarea datelor pseudonimizate de către instituția specializată sunt supravegheate de PIPC [articolul 29-4 alineatul (3) din Decretul de punere în aplicare a PIPA].

2.3.2 *Prelucrarea de categorii speciale de date cu caracter personal*

(49) În cazul în care sunt prelucrate „categorii speciale” de date, ar trebui să existe garanții specifice.

(50) PIPA conține norme specifice în ceea ce privește prelucrarea datelor sensibile ([73]), care sunt definite drept date cu caracter personal care dezvăluie informații despre ideologia, convingerile, înscrierea sau retragerea dintr-un sindicat sau partid politic, opinii politice, informații despre starea de sănătate și viața sexuală a unei persoane, precum și alte informații cu caracter personal care ar putea amenința „în mod evident” viața privată a persoanei vizate și care au fost indicate ca informații sensibile prin decret prezidențial ([74]). Conform clarificărilor primite din partea PIPC, viața sexuală este interpretată ca acoperind, de asemenea, orientarea sau preferințele sexuale ale unei persoane ([75]). În plus, articolul 18 din decretul de punere în aplicare adaugă categorii suplimentare la domeniul de aplicare al datelor sensibile, în special informațiile referitoare la ADN obținute în urma testelor genetice și datele care constituie cazierul judiciar. Modificarea recentă a Decretului de punere în aplicare a PIPA a extins suplimentar noțiunea de date sensibile, incluzând, de asemenea, datele cu caracter personal care dezvăluie originea rasială sau etnică și informațiile biometrice ([76]). În urma acestei modificări, noțiunea de date sensibile din cadrul PIPA este, în esență, echivalentă cu cea de la articolul 9 din Regulamentul (UE) 2016/679.

(51) În conformitate cu articolul 23 alineatul (1) din PIPA și în mod similar cu ceea ce se prevede la articolul 9 alineatul (1) din Regulamentul (UE) 2016/679, prelucrarea datelor sensibile este, în general, interzisă, cu excepția cazului în care se aplică una dintre excepțiile enumerate ([77]). Acestea limitează prelucrarea la cazurile în care operatorul informează persoana vizată în conformitate cu articolele 15 și 17 din PIPA și obține un consimțământ separat (și anume, separat de consimțământul pentru prelucrarea altor date cu caracter

([67]) Articolul 8 alineatele (1)-(2) din Notificarea nr. 2020-9 privind combinarea și difuzarea informațiilor pseudonimizate.
([68]) Articolul 2 alineatele (3) și (6) și articolul 9 alineatul (1) din Notificarea nr. 2020-9 privind combinarea și difuzarea informațiilor pseudonimizate.
([69]) Articolul 2 alineatul (4) și articolul 9 alineatele (2)-(3) din Notificarea nr. 2020-9 privind combinarea și difuzarea informațiilor pseudonimizate. Instituția specializată trebuie să distrugă imediat datele de legătură între cheile de combinare după combinare [articolul 9 alineatul (4) din notificare].
([70]) Încălcarea cerințelor privind combinarea seturilor de date poate duce la impunerea de sancțiuni penale (articolul 71 punctul 4-2 din PIPA). A se vedea, de asemenea, articolul 29-2 alineatul (4) din Decretul de punere în aplicare a PIPA.
([71]) Procedura de aprobare a difuzării datelor combinate este prevăzută la articolul 11 din Notificarea nr. 2020-9 privind combinarea și difuzarea informațiilor pseudonimizate. În special, instituția specializată trebuie să înființeze un „comitet de revizuire a difuzărilor”, format din angajați cu cunoștințe și experiență temeinice în domeniul protecției datelor.
([72]) Articolul 29-2 alineatul (4) din Decretul de punere în aplicare a PIPA și Notificarea nr. 2020-9, articolul 11.
([73]) Necesitatea de a oferi măsuri de protecție specifice pentru prelucrarea datelor sensibile, cum ar fi datele privind sănătatea sau comportamentul sexual, a fost, de asemenea, recunoscută de Curtea Constituțională coreeană; a se vedea Decizia Curții Constituționale în cauza HunMa 1139 din 31 mai 2007.
([74]) Articolul 23 alineatul (1) din PIPA.
([75]) A se vedea, de asemenea, Manualul PIPA, capitolul III secțiunea 2 privind articolul 23 (p. 157-164).
([76]) Și anume, informațiile cu caracter personal care rezultă din prelucrarea tehnică specifică a datelor referitoare la caracteristicile fizice, fiziologice sau comportamentale ale unei persoane în scopul identificării unice a persoanei respective.
([77]) Nerespectarea acestor cerințe poate conduce la sancțiuni în temeiul articolului 71 punctul 3 din PIPA.

personal) sau atunci când prelucrarea este necesară sau permisă prin lege. Autoritățile publice pot prelucra, de asemenea, informații biometrice, informații referitoare la ADN obținute din teste genetice, informații cu caracter personal care dezvăluie originea rasială sau etnică și date care constituie cazierul judiciar pe baza acelor temeiuri de care dispun în mod exclusiv (de exemplu, atunci când acest lucru este necesar pentru investigarea infracțiunilor sau atunci când este necesar pentru ca o instanță să examineze o cauză) ([78]). Ca atare, temeiurile juridice disponibile pentru prelucrarea datelor sensibile sunt mai limitate decât pentru alte tipuri de date cu caracter personal și chiar mai restrictive în legislația coreeană decât cele prevăzute la articolul 9 alineatul (2) din Regulamentul (UE) 2016/679.

(52) În plus, articolul 23 alineatul (2) din PIPA – a cărui nerespectare poate conduce la impunerea de sancțiuni ([79]) – subliniază importanța deosebită a asigurării unor măsuri de securitate adecvate la prelucrarea datelor sensibile, astfel încât acestea „să nu poată fi pierdute, furate, divulgate, falsificate, modificate sau deteriorate.” Deși aceasta este o cerință generală în temeiul articolului 29 din PIPA, articolul 3 alineatul (4) precizează că nivelul de securitate trebuie adaptat tipului de date cu caracter personal care sunt prelucrate, ceea ce înseamnă că trebuie să se țină seama de riscurile specifice implicate în prelucrarea datelor sensibile. În plus, prelucrarea datelor se efectuează întotdeauna „într-un mod care să reducă la minimum posibilitatea de a se încălca” dreptul la viața privată al persoanei vizate și, dacă este posibil, „cu caracter anonim” [articolul 3 alineatele (6) și (7) din PIPA]. Aceste cerințe sunt deosebit de relevante în cazul în care prelucrarea se referă la date sensibile.

2.3.3 *Limitarea scopului*

(53) Datele cu caracter personal ar trebui să fie colectate într-un scop anume și într-un mod care să nu fie incompatibil cu scopul prelucrării.

(54) Acest principiu este asigurat de articolul 3 alineatele (1) și (2) din PIPA, conform cărora operatorul „specifică și precizează” scopul prelucrării, prelucrează datele cu caracter personal într-un mod adecvat și necesar scopului și nu le utilizează în afara acestui scop. Principiul general al limitării scopului este confirmat, de asemenea, la articolul 15 alineatul (1), articolul 18 alineatul (1), articolul 19 și – pentru persoanele împuternicite de către operator (așa-numiții „destinatari ai externalizării”) – la articolul 26 alineatul (1) punctul 1, alineatul (5) și alineatul (7) din PIPA. În special, datele cu caracter personal pot fi, în principiu, utilizate și furnizate terților numai în scopul pentru care au fost colectate [articolul 15 alineatul (1) și articolul 17 alineatul (1) punctul 2]. Prelucrarea într-un scop compatibil, și anume „în domeniul de aplicare legat în mod rezonabil de scopul inițial al colectării”, poate avea loc numai dacă nu afectează în mod negativ persoanele vizate și dacă sunt adoptate măsurile de securitate necesare (cum ar fi criptarea) [articolul 15 alineatul (3) și articolul 17 alineatul (4) din PIPA]. Pentru a stabili dacă prelucrarea ulterioară are un scop compatibil, Decretul de punere în aplicare a PIPA enumeră criterii specifice care sunt similare cu cele prevăzute la articolul 6 alineatul (4) din Regulamentul (UE) 2016/679; a se vedea considerentul 36.

(55) Astfel cum se explică în considerentul 38, scopul colectării în cazul operatorilor coreeni care primesc date cu caracter personal din Uniune este scopul pentru care sunt transferate datele. Modificarea scopului de către operator este permisă numai în mod excepțional, în cazuri specifice (enumerate) [articolul 18 alineatul (2) punctul 1-3 din PIPA; a se vedea, de asemenea, considerentul 39]. În măsura în care modificarea scopului este autorizată prin lege, aceste legi, la rândul lor, trebuie să respecte dreptul fundamental la viață privată și la protecția datelor, precum și principiile necesității și proporționalității prevăzute de Constituția coreeană. În plus, la articolul 18 alineatele (2) și (5) din PIPA sunt prevăzute garanții suplimentare, în special cerința ca o astfel de modificare a scopului să nu „aducă atingere în mod abuziv interesului unei persoane vizate”, astfel, fiind necesară întotdeauna o echilibrare a intereselor. Aceasta prevede un nivel de protecție în esență echivalent cu cel prevăzut la articolul 5 alineatul (1) litera (b) și la articolul 6 coroborate cu considerentul 50 din Regulamentul (UE) 2016/679.

2.3.4 *Exactitatea și reducerea la minimum a datelor*

(56) Datele cu caracter personal ar trebui să fie exacte și, dacă este necesar, actualizate. De asemenea, ar trebui să fie adecvate, relevante și limitate la ceea ce este necesar în raport cu scopurile în care sunt prelucrate.

([78]) În conformitate cu articolul 18 din Decretul de punere în aplicare a PIPA, categoriile de date enumerate în acesta sunt excluse de la furnizarea prevăzută la articolul 23 alineatul (1) din lege atunci când sunt prelucrate de o instituție publică în temeiul articolului 18 alineatul (2) punctul 5-9 din PIPA.

([79]) A se vedea articolul 73 punctul 1 și articolul 75 alineatul (2) punctul 6 din PIPA.

(57) Principiul exactității este, de asemenea, recunoscut la articolul 3 alineatul (3) din PIPA, care prevede că datele cu caracter personal sunt „exacte, complete și actualizate în măsura necesară în raport cu scopurile" pentru care sunt prelucrate datele. Reducerea la minimum a datelor este necesară în temeiul articolului 3 alineatele (1) și (6) și al articolului 16 alineatul (1) din PIPA, care prevăd că operatorul colectează date cu caracter personal (numai) „în măsura minimă necesară" pentru scopul preconizat și că acestuia îi revine sarcina probei în acest sens. Dacă este posibil să se îndeplinească scopul colectării prin prelucrarea informațiilor în formă anonimizată, operatorii ar trebui să depună eforturi în acest sens [articolul 3 alineatul (7) din PIPA].

2.3.5 *Limitarea stocării*

(58) În principiu, datele cu caracter personal 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.

(59) Principiul limitării stocării este prevăzut, de asemenea, la articolul 21 alineatul (1) din PIPA ([80]), care impune operatorului să „distrugă" ([81]) datele cu caracter personal fără întârziere la îndeplinirea scopului prelucrării sau la expirarea perioadei de păstrare (luându-se în considerare data care survine mai întâi), cu excepția cazului în care păstrarea ulterioară este impusă de lege ([82]). În cazul din urmă, datele cu caracter personal relevante „sunt stocate și gestionate separat de alte informații cu caracter personal" [articolul 21 alineatul (3) din PIPA].

(60) Articolul 21 alineatul (1) din PIPA nu se aplică atunci când datele pseudonimizate sunt prelucrate în scopuri statistice, de cercetare științifică sau de arhivare în interes public ([83]). Pentru a asigura principiul păstrării limitate a datelor și în acest caz, Notificarea nr. 2021-5 impune operatorilor să anonimizeze informațiile în conformitate cu articolul 58-2 din PIPA în cazul în care datele nu au fost distruse în momentul îndeplinirii scopului specific al prelucrării ([84]).

2.3.6 *Securitatea datelor*

(61) 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 evaluate luând în considerare stadiul actual al tehnologiei, costurile aferente și natura, domeniul de aplicare, contextul și scopurile prelucrării, precum și riscurile la adresa drepturilor persoanelor fizice.

(62) Un principiu similar al securității este prevăzut la articolul 3 alineatul (4) din PIPA, care impune operatorilor să „gestioneze informațiile cu caracter personal în condiții de siguranță, în conformitate cu metodele, tipurile etc. de prelucrare a informațiilor cu caracter personal, ținând seama de posibilitatea încălcării drepturilor persoanelor vizate și de gravitatea riscurilor relevante". În plus, operatorul „prelucrează informațiile cu caracter personal într-un mod care să reducă la minimum posibilitatea de a încălca dreptul la viață privată al unei persoane vizate" și, în acest context, depune eforturi pentru a prelucra datele cu caracter personal în mod anonim sau pseudonimizat, dacă este posibil [articolul 3 alineatele (6) și (7) din PIPA].

(63) Aceste cerințe generale sunt detaliate suplimentar la articolul 29 din PIPA, conform căruia fiecare operator „ia măsuri tehnice, de gestionare și fizice, precum stabilirea unui plan intern de gestionare și păstrarea de înregistrări ale autentificărilor etc., care sunt necesare pentru a asigura siguranța, astfel cum prevede decretul prezidențial, în

([80]) Articolul 8 [coroborat cu articolul 8-2 din Decretul de punere în aplicare], articolul 11 [coroborat cu articolul 12 alineatul (2) din Decretul de punere în aplicare].

([81]) În ceea ce privește metodele de distrugere a informațiilor cu caracter personal, a se vedea articolul 16 din Decretul de punere în aplicare a PIPA. Articolul 21 alineatul (2) din PIPA clarifică faptul că aceasta include „măsurile necesare pentru a bloca recuperarea și reconstituirea".

([82]) Nerespectarea acestor cerințe poate conduce la impunerea de sancțiuni penale [articolul 73 alineatele (1)-(2) din PIPA]. Articolul 39-6 din PIPA impune furnizorilor de servicii din domeniul informațiilor și comunicațiilor o cerință suplimentară de a șterge informațiile cu caracter personal ale utilizatorilor care nu au utilizat serviciile din domeniul informațiilor și comunicațiilor oferite timp de cel puțin un an (cu excepția cazului în care păstrarea ulterioară este impusă de lege sau la cererea persoanei respective). Persoanele fizice trebuie informate cu privire la intenția de ștergere a informațiilor lor cu 30 de zile înainte de expirarea termenului de un an [articolul 39-6 alineatul (2) din PIPA și articolul 48-5 alineatul (3) din Decretul de punere în aplicare a PIPA]. În cazul în care legea impune păstrarea ulterioară, datele păstrate trebuie stocate separat de alte informații ale utilizatorilor și pot fi utilizate sau divulgate numai în conformitate cu legea respectivă [articolul 48-5 alineatele (1)-(2) din Decretul de punere în aplicare a PIPA].

([83]) Articolul 28-7 din PIPA.

([84]) Notificarea nr. 2021-5 (anexa I), secțiunea 4.

așa fel încât informațiile cu caracter personal să nu poată fi pierdute, furate, divulgate, falsificate, modificate sau deteriorate." Articolul 30 alineatul (1) din Decretul de punere în aplicare a PIPA specifică acele măsuri referindu-se la (1) formularea și punerea în aplicare a unui plan intern de gestionare pentru prelucrarea în condiții de siguranță a datelor cu caracter personal, (2) controale și restricții ale accesului, (3) adoptarea tehnologiei de criptare pentru stocarea și transmiterea în siguranță a datelor personale, (4) înregistrări ale autentificărilor (5) programe de securitate și (6) măsuri fizice, cum ar fi un sistem de stocare sau blocare sigur ([85]).

(64) În plus, în cazul în care are loc o încălcare a securității datelor se aplică obligații specifice (articolul 34 din PIPA coroborat cu articolele 39 și 40 din Decretul de punere în aplicare a PIPA) ([86]). În special, operatorul are obligația de a notifica fără întârziere persoanelor vizate prejudiciate detaliile încălcării ([87]), inclusiv informații cu privire la contramăsurile (obligatorii) luate de operator și la măsurile pe care persoanele vizate le pot lua pentru a reduce la minimum riscul de prejudiciu [articolul 34 alineatele (1) și (2) din PIPA] ([88]). În cazul în care încălcarea securității datelor vizează cel puțin 1 000 de persoane vizate, operatorul raportează fără întârziere încălcarea securității datelor și contramăsurile luate și către PIPC, și către Agenția coreeană pentru internet și securitate, care pot oferi asistență tehnică [articolul 34 alineatul (3) din PIPA coroborat cu articolul 39 din Decretul de punere în aplicare a PIPA]. Operatorii sunt răspunzători pentru prejudiciile cauzate de încălcarea securității datelor, în conformitate cu dispozițiile Legii civile privind răspunderea delictuală (a se vedea, de asemenea, secțiunea 2.5 privind măsurile reparatorii) ([89]).

(65) În îndeplinirea obligațiilor sale în materie de securitate, operatorul trebuie să fie asistat de un responsabil cu protecția vieții private, ale cărui sarcini includ, printre altele, dezvoltarea unui sistem de control intern „pentru a preveni divulgarea, utilizarea abuzivă și necorespunzătoare a informațiilor cu caracter personal" [articolul 31 alineatul (2) punctul 4 din PIPA]. În plus, operatorul are datoria de a-și „controla și supraveghea corespunzător" angajații care prelucrează date cu caracter personal, inclusiv în ceea ce privește gestionarea în condiții de siguranță a acestora; este astfel inclusă formarea („educarea") necesară a angajaților [articolul 28 alineatele (1) și (2) din PIPA]. În cele din urmă, în cazul subcontractării serviciilor de prelucrare a datelor, operatorul trebuie să impună cerințe „destinatarului externalizării", printre altele, în ceea ce privește gestionarea în condiții de siguranță a datelor cu caracter personal („garanții tehnice și de gestionare") și trebuie să supravegheze modul în care acestea sunt puse în aplicare prin inspecții [articolul 26 alineatele (1) și (4) din PIPA coroborate cu articolul 28 alineatul (1) punctele 3 și 4 și alineatul (6) din Decretul de punere în aplicare a PIPA].

2.3.7 *Transparența*

(66) Persoanele vizate ar trebui să fie informate cu privire la principalele caracteristici ale prelucrării datelor lor cu caracter personal.

([85]) În ceea ce privește prelucrarea datelor cu caracter personal de către furnizorii de servicii din domeniul informațiilor și comunicațiilor, articolul 39-5 din PIPA prevede în mod explicit că numărul de persoane care prelucrează informații cu caracter personal ale utilizatorilor trebuie limitat la minimum. În plus, furnizorii de servicii din domeniul informațiilor și comunicațiilor se asigură că informațiile cu caracter personal ale utilizatorilor nu sunt expuse publicului prin intermediul rețelei de informații și comunicații [articolul 39-10 alineatul (1) din PIPA]. Informațiile expuse trebuie șterse sau blocate la solicitarea PIPC [articolul 39-10 alineatul (2) din PIPA]. La un nivel mai general, furnizorii de servicii din domeniul informațiilor și comunicațiilor (și părțile terțe care primesc date cu caracter personal ale utilizatorilor) fac obiectul unor obligații suplimentare în materie de securitate, specificate la articolul 48-2 din Decretul de punere în aplicare a PIPA, de exemplu elaborarea și punerea în aplicare a unui plan intern de gestionare în ceea ce privește măsurile de securitate, măsurile de asigurare a controlului accesului, criptarea, utilizarea aplicațiilor software pentru detectarea programelor malware etc.

([86]) În plus, există o interdicție generală de a deteriora, distruge, modifica, falsifica sau permite scurgerea de informații cu caracter personal fără a avea autoritate juridică; a se vedea articolul 59 punctul 3 din PIPA.

([87]) Cerința de notificare a persoanei în cauză nu se aplică în măsura în care are loc o încălcare a securității datelor în ceea ce privește informațiile pseudonimizate prelucrate în scopuri statistice, de cercetare științifică sau de arhivare în interes public [articolul 28-7 din PIPA, care prevede o exceptare de la articolul 34 alineatul (1) și articolul 39-4 din PIPA]. Pentru a asigura notificarea persoanelor fizice, operatorul în cauză ar trebui să identifice persoanele din setul de date pseudonimizate, acțiune care este interzisă în mod expres în temeiul articolului 28-5 din PIPA. Cu toate acestea, cerința generală de notificare a încălcării securității datelor (către PIPC) se aplică în continuare.

([88]) Cerințele de notificare, inclusiv termenul și posibilitatea unei notificări „în etape", sunt precizate mai detaliat la articolul 40 din Decretul de punere în aplicare a PIPA. În cazul furnizorilor de servicii din domeniul informațiilor și comunicațiilor care au obligația de a transmite o notificare persoanei vizate și PIPC în termen de 24 de ore de la momentul la care au luat cunoștință de faptul că informațiile cu caracter personal au fost pierdute, furate sau divulgate [articolul 39-4 alineatul (1) din PIPA] se aplică norme mai stricte. Această notificare trebuie să includă detalii privind informațiile cu caracter personal care au fost divulgate, momentul în care s-a produs scurgerea, măsurile care pot fi luate de utilizator, măsurile adoptate de furnizor ca răspuns și datele de contact ale departamentului căruia utilizatorul îi poate adresa întrebări [articolul 39-4 alineatul (1) punctele 1-5 din PIPA]. În cazul în care există un motiv justificat, de exemplu lipsa datelor de contact ale utilizatorului, se pot folosi alte mijloace de notificare, de exemplu publicarea informațiilor pe un site internet [articolul 39-4 alineatul (1) din PIPA coroborat cu articolul 48-4 alineatul (4) și următoarele din Decretul de punere în aplicare a PIPA]. În acest caz, PIPC trebuie să fie informată cu privire la motive [articolul 34-4 alineatul (3) din PIPA].

([89]) A se vedea, de exemplu, hotărârile Curții Supreme 2011Da59834, 2011Da59858 și 2011Da59841 din 26 decembrie 2012. Un rezumat în limba engleză este disponibil la adresa: http://library.scourt.go.kr/SCLIB_data/decision/9-69%202012.12.26.2011Da59834.htm.

(67) Acest lucru este asigurat în diferite moduri în sistemul coreean. În afară de dreptul la informare prevăzut la articolul 4 punctul 1 (în general) și articolul 20 alineatul (1) din PIPA (pentru datele cu caracter personal colectate de la terți), precum și dreptul de acces în temeiul articolului 35 din PIPA, PIPA include o cerință generală de transparență în ceea ce privește scopul prelucrării [articolul 3 alineatul (1) din PIPA] și cerințe specifice de transparență în cazul în care prelucrarea se bazează pe consimțământ [articolele 15 alineatul (2), articolul 17 alineatul (2) și articolul 18 alineatul (3) din PIPA] ([90]). În plus, articolul 20 alineatul (2) din PIPA impune anumitor operatori – celor pentru care prelucrarea depășește anumite praguri ([91]) – obligația de a notifica persoanei vizate ale cărei date cu caracter personal au fost primite de la un terț sursa informațiilor, scopul prelucrării și dreptul persoanei vizate de a solicita suspendarea prelucrării, cu excepția cazului în care o astfel de notificare se dovedește imposibilă din cauza lipsei oricăror informații de contact. Se aplică excepții pentru anumite dosare de date cu caracter personal deținute de autoritățile publice, în special dosarele care conțin date prelucrate în scopuri legate de securitatea națională, alte interese naționale deosebit de importante („grave") sau în scopuri de asigurare a respectării dreptului penal sau în cazul în care notificarea este de natură să aducă prejudicii vieții sau integrității fizice a unei alte persoane sau să prejudicieze în mod abuziv drepturile de proprietate și interesele unei alte persoane, cu toate acestea, numai în cazul în care interesele publice sau private în cauză sunt „în mod evident superioare" drepturilor persoanelor vizate [articolul 20 alineatul (4) din PIPA]. Acest lucru necesită o echilibrare a intereselor.

(68) În plus, articolul 3 alineatul (5) din PIPA prevede că operatorii fac publică politica lor de confidențialitate (și alte aspecte legate de prelucrarea datelor cu caracter personal). Această cerință este detaliată la articolul 30 din PIPA coroborat cu articolul 31 din Decretul de punere în aplicare a PIPA. Potrivit acestor dispoziții, politica publică în materie de confidențialitate trebuie să includă, printre altele (1) tipurile de date cu caracter personal prelucrate, (2) scopul prelucrării, (3) perioada de păstrare, (4) dacă datele cu caracter personal sunt furnizate unui terț ([92]), (5) orice subcontractare a serviciilor de prelucrare a datelor, (6) informații privind drepturile persoanei vizate și modul de exercitare a acestora și (7) datele de contact (inclusiv numele responsabilului cu protecția vieții private sau al departamentului intern responsabil cu asigurarea respectării normelor privind protecția datelor și tratarea plângerilor). Politica de confidențialitate trebuie să fie pusă la dispoziția publicului astfel încât persoanele vizate „să o poată recunoaște cu ușurință" [articolul 30 alineatul (2) din PIPA] ([93]) și să fie actualizată în permanență [articolul 31 alineatul (2) din Decretul de punere în aplicare a PIPA].

(69) Instituțiile publice sunt supuse unei obligații suplimentare de a înregistra, în special, următoarele informații la PIPC: (1) denumirea instituției publice, (2) motivele și scopurile prelucrării dosarelor de date cu caracter personal, (3) detaliile privind datele cu caracter personal care sunt înregistrate, (4) metoda de prelucrare, (5) perioada de păstrare, (6) numărul persoanelor vizate ale căror date cu caracter personal sunt păstrate, (7) departamentul care tratează cererile persoanelor vizate și (8) destinatarii datelor cu caracter personal, atunci când datele sunt furnizate în mod regulat sau repetat [articolul 32 alineatul (1) din PIPA] ([94]). Dosarele de date cu caracter personal înregistrate sunt făcute publice de PIPC și trebuie, de asemenea, să fie menționate de instituțiile publice în politica lor de confidențialitate [articolul 30 alineatul (1) și articolul 32 alineatul (4) din PIPA].

(70) Pentru a spori transparența pentru persoanele vizate din Uniune ale căror date cu caracter personal sunt transferate către Coreea pe baza prezentei decizii, secțiunea 3 punctele (i) și (ii) din Notificarea nr. 2021-5 (anexa I) impune cerințe suplimentare în materie de transparență. În primul rând, atunci când primesc date cu caracter personal din Uniune în temeiul prezentei decizii, operatorii coreeni trebuie să notifice persoanelor vizate fără întârzieri nejustificate (și, în orice caz, în termen de cel mult o lună de data transferului) numele și datele de contact ale entităților care transferă și primesc informațiile, datele cu caracter personal (sau categoriile de date cu caracter personal) transferate, scopul colectării de către operatorul coreean, perioada de păstrare și drepturile de care beneficiază în temeiul PIPA. În al doilea rând, atunci când furnizează terților date cu caracter personal

([90]) În special, atunci când informațiile cu caracter personal sunt prelucrate cu consimțământul unei persoane, operatorul trebuie să informeze persoana în cauză cu privire la scopul prelucrării, detaliile cu privire la informațiile care urmează să fie prelucrate, destinatarul informațiilor, perioada de păstrare și utilizare a informațiilor cu caracter personal, precum și faptul că persoana în cauză are dreptul de a refuza consimțământul (și orice dezavantaj care ar putea rezulta din aceasta).

([91]) În conformitate cu articolul 15-2 alineatul (1) din Decretul de punere în aplicare a PIPA, aceasta privește operatorii care prelucrează informații sensibile referitoare la cel puțin 50 000 de persoane vizate sau informații cu caracter personal „normale" referitoare la cel puțin 1 milion de persoane vizate. Articolul 15-2 alineatul (2) din Decretul de punere în aplicare a PIPA stabilește modalitățile și termenele notificării, iar articolul 15-2 alineatul (3), cerința de a ține anumite evidențe. În plus, pentru anumite categorii de furnizori de servicii din domeniul informațiilor și comunicațiilor (cei care au generat venituri din vânzări de cel puțin 10 miliarde de woni în cursul anului precedent sau cei care stochează/gestionează date cu caracter personal pentru cel puțin un milion de utilizatori pe zi, în medie, în cursul celor trei luni anterioare sfârșitului anului precedent), care au obligația de a informa în mod regulat utilizatorii cu privire la istoricul utilizării informațiilor lor cu caracter personal, cu excepția cazului în care acest lucru se dovedește imposibil din cauza lipsei oricăror informații de contact (articolul 39-8 din PIPA și articolul 48-6 din Decretul de punere în aplicare a PIPA), se aplică norme specifice.

([92]) Conform informațiilor primite de la guvernul coreean, acest lucru implică obligația de a enumera destinatarii în politica publică în materie de confidențialitate în mod individual.

([93]) Alte modalități sunt prevăzute la articolul 31 alineatul (3) din Decretul de punere în aplicare a PIPA.

([94]) Cerința de înregistrare nu se aplică anumitor tipuri de dosare cu informații cu caracter personal, de exemplu celor în care se înregistrează aspecte legate de securitatea națională, secrete diplomatice, anchete penale, urmăriri penale, pedepse, anchetarea infracțiunilor fiscale sau dosare care se referă exclusiv la activitatea profesională internă [articolul 32 alineatul (2) din PIPA].

primite din Uniune în temeiul prezentei decizii, persoanele vizate trebuie să fie informate, printre altele, cu privire la destinatar, la datele cu caracter personal sau la categoriile de date cu caracter personal care urmează să fie furnizate, la țara căreia îi sunt furnizate datele (dacă este cazul), precum și cu privire la drepturile de care beneficiază în temeiul PIPA ([95]). În acest mod, prin notificare se asigură informarea continuă a persoanelor din UE cu privire la operatorii specifici care prelucrează informațiile lor și posibilitatea acestora de a-și exercita drepturile în fața entităților relevante.

(71) Secțiunea 3 punctul (iii) din notificare (anexa I) permite anumite excepții limitate și calificate de la aceste obligații suplimentare de transparență care sunt în esență echivalente cu cele prevăzute în Regulamentul (UE) 2016/679. În special, notificarea persoanelor vizate în Uniune nu este necesară (1) atunci când și atât timp cât este necesar să se restricționeze notificarea din anumite motive de interes public (de exemplu, în cazul în care informațiile sunt prelucrate în scopuri legate de securitatea națională sau de anchete penale în curs), în măsura în care aceste obiective de interes public sunt în mod evident superioare drepturilor persoanei vizate; (2) atunci când persoana vizată deține deja informațiile; (3) atunci când și atât timp cât notificarea este susceptibilă să aducă prejudicii vieții sau integrității fizice a persoanei în cauză sau a unei alte persoane sau să prejudicieze în mod abuziv drepturile de proprietate ale altei persoane, în cazul în care aceste drepturi sau interese sunt în mod evident superioare drepturilor persoanei vizate; sau (4) atunci când nu există date de contact pentru persoanele în cauză sau ar fi necesar un efort disproporționat pentru a le transmite o notificare. Pentru a stabili dacă este sau nu este posibil să se contacteze persoana vizată sau dacă acest lucru implică eforturi excesive, se va lua în considerare posibilitatea de a coopera cu exportatorul de date din Uniune.

(72) Prin urmare, normele din considerentele 67-71 asigură un nivel de protecție în esență echivalent în ceea ce privește transparența cu ceea ce este prevăzut în Regulamentul (UE) 2016/679.

2.3.8 *Drepturi individuale*

(73) Persoanele vizate ar trebui să aibă anumite drepturi care pot fi impuse operatorului sau persoanei împuternicite de operator, în special dreptul de acces la date, dreptul de rectificare, dreptul de a se opune prelucrării și dreptul la ștergerea datelor. În același timp, aceste drepturi pot face obiectul unor restricții, în măsura în care acestea sunt necesare și proporționale pentru a proteja obiectivele importante de interes public general.

(74) În conformitate cu articolul 3 alineatul (5) din PIPA, operatorul garantează drepturile persoanelor vizate enumerate la articolul 4 din PIPA și specificate mai detaliat la articolele 35-37, 39 și 39-2 din PIPA.

(75) În primul rând, persoanele fizice au dreptul la informare și dreptul de acces. Atunci când operatorul a colectat date cu caracter personal de la un terț – astfel cum se va întâmpla întotdeauna când datele sunt transferate din Uniune – persoanele vizate au, în general, dreptul de a primi informații privind (1) „sursa" datelor cu caracter personal colectate (și anume, entitatea care efectuează transferul), (2) scopul prelucrării și (3) faptul că persoana vizată are dreptul de a solicita suspendarea prelucrării [articolul 20 alineatul (1) din PIPA]. Se aplică excepții limitate, și anume în cazul în care o astfel de notificare este de natură să aducă prejudicii vieții sau integrității fizice a unei alte persoane sau „să prejudicieze în mod abuziv drepturile de proprietate și alte interese" ale altei persoane, dar numai în cazul în care aceste interese ale terților sunt „superioare în mod explicit" drepturilor persoanei vizate [articolul 20 alineatul (4) punctul 2 din PIPA].

(76) În plus, articolul 35 alineatele (1) și (3) din PIPA coroborate cu articolul 41 alineatul (4) din Decretul de punere în aplicare a PIPA conferă persoanelor vizate dreptul de acces la informațiile lor cu caracter personal ([96]). Dreptul de acces include confirmarea prelucrării, informații privind tipul de date prelucrate, scopul prelucrării, perioada de păstrare, precum și orice divulgare către un terț, precum și furnizarea unei copii a informațiilor cu caracter personal prelucrate [articolul 4 punctul 3 din PIPA coroborat cu articolul 41 alineatul (1) din Decretul de aplicare

([95]) Notificarea nr. 2021-5, secțiunea 3 punctul (ii) (anexa I).

([96]) În conformitate cu articolul 35 alineatul (3) din PIPA coroborat cu articolul 42 alineatul (2) din Decretul de punere în aplicare a PIPA, operatorul poate amâna accesul din „motive întemeiate" (și anume, din motive justificate, de exemplu, dacă este nevoie de mai mult timp pentru a evalua posibilitatea de a permite accesul), dar trebuie să notifice persoanei vizate o astfel de justificare în termen de 10 zile și să furnizeze informații cu privire la căile de atac împotriva acestei decizii; de îndată ce motivul amânării nu mai există, trebuie să se permită accesul.

a PIPA] ([97]). Accesul poate fi limitat (acces parțial) ([98]) sau refuzat numai în cazul în care acest lucru este prevăzut de lege ([99]), în cazul în care acest lucru ar putea aduce prejudicii vieții sau integrității fizice a unui terț sau o încălcare nejustificată a drepturilor de proprietate și a altor interese ale unei alte persoane [articolul 35 alineatul (4) din PIPA] ([100]). Aceasta din urmă implică faptul că ar trebui să existe o echilibrare între drepturile și libertățile protejate prin Constituție ale persoanei în cauză, pe de o parte, și ale altor persoane, pe de altă parte. În cazul în care accesul este limitat sau refuzat, operatorul trebuie să informeze persoana vizată cu privire la motivele limitării sau refuzului și la modalitățile de contestare a deciziei [articolul 41 alineatul (5) și articolul 42 alineatul (2) din Decretul de punere în aplicare a PIPA].

(77) În al doilea rând, persoanele vizate au dreptul la rectificarea sau ștergerea ([101]) datelor lor cu caracter personal, „cu excepția cazului în care se prevede altfel în alte legi" [articolul 36 alineatele (1) și (2) din PIPA] ([102]). La primirea unei cereri, operatorul trebuie să investigheze chestiunea fără întârziere, să ia măsurile necesare ([103]) și să informeze persoana vizată în acest sens în termen de 10 zile; în cazul în care nu se poate da curs cererii, această cerință de notificare va acoperi motivele refuzului și modalitățile de exercitare a unei căi de atac [a se vedea articolul 36 alineatul (4) din PIPA coroborat cu articolul 43 alineatul (3) din Decretul de punerea în aplicare a PIPA] ([104]).

(78) În cele din urmă, persoanele vizate au dreptul la suspendarea prelucrării datelor lor cu caracter personal, fără întârziere ([105]), cu excepția cazului în care se aplică una dintre excepțiile enumerate [articolul 37 alineatele (1) și (2) din PIPA] ([106]). Operatorul poate refuza cererea (1) în cazul în care acest lucru este autorizat în mod expres prin lege sau este necesar („inevitabil") pentru a se conforma obligațiilor legale, (2) în cazul în care suspendarea ar putea aduce prejudicii vieții sau integrității fizice a unei terțe părți ori o încălcare nejustificată a drepturilor de proprietate și a altor interese ale unei alte persoane, (3) în cazul în care unei instituții publice i-ar fi imposibil să își îndeplinească funcția prevăzută de lege fără prelucrarea informațiilor sau (4) în cazul în care persoana vizată nu reziliază în mod expres contractul de bază cu operatorul, chiar dacă executarea contractului ar fi imposibilă fără prelucrarea datelor respective. În acest caz, operatorul trebuie să informeze fără întârziere persoana vizată cu privire la motivele refuzului și la căile de atac [articolul 37 alineatul (2) din PIPA coroborat cu articolul 44 alineatul (2) din decretul PIPA]. În conformitate cu articolul 37 alineatul (4) din PIPA, operatorul trebuie, fără întârziere, „să ia măsurile necesare, inclusiv distrugerea informațiilor cu caracter personal relevante" atunci când se conformează cererii de suspendare ([107]).

(79) Dreptul la suspendare se aplică, de asemenea, în cazul în care datele cu caracter personal sunt utilizate în scopuri de marketing direct, și anume pentru a promova bunuri sau servicii ori pentru a solicita achiziționarea acestora. În plus, o astfel de prelucrare ulterioară necesită, în general, consimțământul specific (suplimentar) al persoanei vizate [a se vedea articolul 15 alineatul (1) punctul 1 și articolul 17 alineatul (2) punctul 1 din PIPA] ([108]). Atunci când solicită acest consimțământ, operatorul trebuie să informeze persoana vizată în special cu privire la utilizarea

([97]) Accesul la informațiile cu caracter personal prelucrate de o instituție publică poate fi obținut direct de la instituție sau indirect prin depunerea unei cereri la PIPC, care va transmite cererea fără întârziere [articolul 35 alineatul (2) din PIPA și articolul 41 alineatul (3) din Decretul de punere în aplicare a PIPA].

([98]) În conformitate cu articolul 42 alineatul (1) din Decretul de punere în aplicare a PIPA, operatorul are obligația de a acorda acces parțial în cazul în care cel puțin o parte din informații nu sunt vizate de motivele de refuz.

([99]) Aceste legi trebuie, la rândul lor, să respecte dreptul fundamental la viață privată și la protecția datelor, precum și principiile necesității și proporționalității prevăzute de Constituția coreeană.

([100]) În plus, instituțiile publice pot refuza acordarea accesului în cazul în care acest lucru ar cauza dificultăți grave în îndeplinirea anumitor funcții, inclusiv privind desfășurarea auditurilor în curs sau impunerea, colectarea sau rambursarea impozitelor [articolul 35 alineatul (4) din PIPA].

([101]) În acest caz, operatorul trebuie să ia măsuri de prevenire a recuperării informațiilor cu caracter personal; a se vedea articolul 36 alineatul (3) din PIPA.

([102]) Aceste legi trebuie să respecte cerințele prevăzute de Constituție conform cărora un drept fundamental poate fi restricționat numai când acest lucru este necesar din motive legate de securitatea națională sau de menținerea ordinii publice pentru bunăstarea publică și nu poate afecta esența libertății sau a dreptului [articolul 37 alineatul (2) din Constituție].

([103]) Articolul 43 alineatul (2) din Decretul de punere în aplicare a PIPA prevede o procedură specială în cazul în care operatorul prelucrează dosare de informații cu caracter personal furnizate de un alt operator.

([104]) Neluarea măsurilor necesare pentru corectarea sau ștergerea informațiilor cu caracter personal și utilizarea sau furnizarea continuă a acestor informații către un terț pot conduce la impunerea de sancțiuni penale [articolul 73 alineatul (2) din PIPA].

([105]) În conformitate cu articolul 44 alineatul (2) din Decretul de punere în aplicare a PIPA, operatorul informează persoana vizată cu privire la faptul că a suspendat în mod corespunzător prelucrarea în termen de 10 zile de la primirea cererii.

([106]) În ceea ce privește instituțiile publice, dreptul la suspendarea prelucrării poate fi exercitat în ceea ce privește informațiile din dosarele cu informații cu caracter personal înregistrate (articolul 37 coroborat cu articolul 32 din PIPA). O astfel de înregistrare nu este necesară într-un număr limitat de situații, de exemplu în cazul în care dosarele cu informații cu caracter personal se referă la securitatea națională, anchete penale, relații diplomatice etc. [articolul 32 alineatul (2) din PIPA].

([107]) Nesuspendarea prelucrării poate conduce la impunerea de sancțiuni penale [articolul 73 alineatul (3) din PIPA].

([108]) Comitetul de mediere a litigiilor (a se vedea considerentul 133) a tratat mai multe cazuri în care persoanele s-au plâns de utilizarea datelor lor în scopuri de marketing direct fără consimțământ, ceea ce a condus, de exemplu, la plata unei compensații și la ștergerea datelor cu caracter personal de către operatorul relevant [a se vedea, de exemplu, Comitetul de mediere a litigiilor 20R10-024(2020.11.18), 20R08-015(2020.8.28), 20R07-031(2020.9.1)].

preconizată a datelor în scopuri de marketing direct – și anume faptul că poate fi contactată pentru a promova bunuri sau servicii sau pentru a solicita achiziționarea acestora – într-un „mod care poate fi recunoscut în mod explicit" [articolul 22 alineatele (2) și (4) din PIPA coroborat cu articolul 17 alineatul (2) punctul 1 din Decretul de punere în aplicare a PIPA].

(80) Pentru a facilita exercitarea drepturilor individuale, operatorul trebuie să stabilească proceduri specifice și să le facă publice [articolul 38 alineatul (4) din PIPA] ([109]). Acestea includ proceduri pentru formularea de obiecții împotriva refuzului unei cereri [articolul 38 alineatul (5) din PIPA]. Operatorul trebuie să se asigure că procedura de exercitare a drepturilor este „ușor de utilizat de către persoanele vizate" și nu este mai dificilă decât cea pentru colectarea datelor cu caracter personal; aceasta include, de asemenea, obligația de a furniza informații cu privire la procedură pe site-ul său internet [articolul 41 alineatul (2), articolul 43 alineatul (1) și articolul 44 alineatul (1) din Decretul de punere în aplicare a PIPA] ([110]). Persoanele fizice pot autoriza un reprezentant să depună o astfel de cerere [articolul 38 alineatul (1) din PIPA coroborat cu articolul 45 din Decretul de punere în aplicare a PIPA]. Deși operatorul are dreptul de a impune o taxă (și, în cazul unei cereri de transmitere a unor copii ale datelor cu caracter personal, o taxă poștală), suma trebuie să fie stabilită „în cadrul cheltuielilor efective necesare pentru prelucrarea [cererii]"; nu se poate impune nicio taxă (sau taxă poștală) în cazul în care necesitatea depunerii cererii este atribuită operatorului [articolul 38 alineatul (3) din PIPA coroborat cu articolul 47 din Decretul de punere în aplicare a PIPA].

(81) PIPA și decretul de punere în aplicare a sa nu conțin dispoziții generale care abordează chestiunea deciziilor care afectează persoana vizată și sunt bazate exclusiv pe prelucrarea automată a datelor cu caracter personal. Cu toate acestea, în ceea ce privește datele cu caracter personal care au fost colectate în Uniune, orice decizie bazată pe prelucrarea automată va fi luată de regulă de către operatorul din Uniune (care are o relație directă cu persoana vizată în cauză) și, prin urmare, intră sub incidența Regulamentului (UE) 2016/679 ([111]). Aceasta include scenarii de transfer în care prelucrarea este efectuată de un operator economic din străinătate (de exemplu, din Coreea) care acționează ca agent (operator) în numele operatorului din Uniune (sau în calitate de subcontractant care acționează în numele persoanei împuternicite de operator din Uniune, care a primit datele de la un operator din Uniune care le-a colectat), care, pe această bază, ia decizia respectivă. Prin urmare, este puțin probabil ca lipsa din PIPA a unor norme specifice privind procesul decizional automatizat să afecteze nivelul de protecție a datelor cu caracter personal transferate în temeiul prezentei decizii.

(82) În mod excepțional, dispozițiile privind transparența la cerere (articolul 20) și drepturile individuale (articolele 35-37), precum și cerința de notificare individuală pentru furnizorii de servicii din domeniul informațiilor și comunicațiilor (articolul 39-8 din PIPA) nu se aplică în ceea ce privește informațiile pseudonimizate, atunci când acestea sunt prelucrate în scopuri statistice, de cercetare științifică sau de arhivare în interes public (articolul 28-7 din PIPA) ([112]). În conformitate cu abordarea de la articolul 11 alineatul (2) (coroborat cu considerentul 57) din Regulamentul (UE) 2016/679, acest lucru este justificat de faptul că, pentru a asigura transparența sau pentru a acorda drepturi individuale, operatorul ar trebui să identifice dacă datele (și, în caz afirmativ, care anume) sunt legate de persoana fizică ce formulează cererea, fapt care este interzis în mod expres în temeiul PIPA [articolul 28-5 alineatul (1) din PIPA]. În plus, în cazul în care o astfel de reidentificare implică anularea pseudonimizării pentru întregul set de date (pseudonimizate), aceasta ar expune informațiile cu caracter personal ale tuturor celorlalte persoane în cauză la riscuri crescute. Deși Regulamentul (UE) 2016/679 se referă la situațiile în care reidentificarea este practic imposibilă, PIPA adoptă o abordare mai strictă, interzicând în mod expres reidentificarea în toate situațiile în care sunt prelucrate informații pseudonimizate.

(83) Sistemul coreean, astfel cum este descris în considerentele 74-82, conține, prin urmare, norme privind drepturile persoanelor vizate care oferă un nivel de protecție în esență echivalent cu cel prevăzut în Regulamentul (UE) 2016/679.

([109]) A se vedea, de asemenea, articolul 30 alineatul (1) punctul 5 din PIPA privind politica de confidențialitate, care conține, printre altele, informații privind drepturile persoanelor și modul de exercitare a acestora.

([110]) A se vedea, de asemenea, articolul 39-7 alineatul (2) din PIPA în ceea ce privește furnizorii de servicii din domeniul informațiilor și comunicațiilor.

([111]) În schimb, în cazul excepțional în care operatorul economic coreean 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 economic coreean 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.

([112]) A se vedea, de asemenea, Notificarea nr. 2021-5, care confirmă faptul că secțiunea III din PIPA (inclusiv articolul 28-7) se aplică numai atunci când informațiile pseudonimizate sunt prelucrate în scopuri de cercetare științifică, de statistică sau arhivare în interes public; a se vedea secțiunea 4 din anexa I la prezenta decizie.

2.3.9 *Transferuri ulterioare*

(84) Nivelul de protecție conferit datelor cu caracter personal transferate din Uniune către operatorii din Republica Coreea nu trebuie să fie subminat de transferul suplimentar al acestor date către destinatari dintr-o țară terță.

(85) Astfel de „transferuri ulterioare” constituie transferuri internaționale din Republica Coreea din perspectiva operatorului coreean. În acest sens, PIPA face distincție între externalizarea prelucrării către un destinatar al externalizării (și anume o persoană împuternicită de operator) și furnizarea de date cu caracter personal către terți ([113]).

(86) În primul rând, atunci când prelucrarea datelor cu caracter personal este externalizată către o entitate situată într-o țară terță, operatorul coreean trebuie să asigure conformitatea cu dispozițiile PIPA privind externalizarea (articolul 26 din PIPA). Aceasta include instituirea unui instrument obligatoriu din punct de vedere juridic care, printre altele, să limiteze prelucrarea de către destinatarul externalizării la scopul activității externalizate, să impună garanții tehnice și de gestionare și să limiteze subcontractarea serviciilor de prelucrare a datelor [a se vedea articolul 26 alineatul (1) din PIPA]; și publicarea de informații privind activitățile externalizate. În plus, operatorul are obligația de a-l „educa” pe destinatarul externalizării cu privire la măsurile de securitate necesare și de a supraveghea, inclusiv prin inspecții, respectarea tuturor obligațiilor operatorului în temeiul PIPA ([114]), precum și a contractului de externalizare.

(87) În cazul în care destinatarul externalizării cauzează prejudicii prin prelucrarea datelor cu caracter personal cu încălcarea PIPA, acest lucru va fi atribuit operatorului în scopuri legate de răspundere, cum ar fi cazul angajaților operatorului [articolul 26 alineatul (6) din PIPA]. Prin urmare, operatorul coreean rămâne responsabil pentru datele cu caracter personal care au fost externalizate și trebuie să se asigure că persoana împuternicită de operator din străinătate prelucrează informațiile în conformitate cu PIPA. În cazul în care destinatarul externalizării prelucrează informațiile cu încălcarea PIPA, operatorul coreean poate fi tras la răspundere pentru nerespectarea obligației sale de a asigura respectarea PIPA, de exemplu prin supravegherea destinatarului externalizării. Garanțiile incluse în contractul de externalizare și responsabilitatea operatorului coreean pentru acțiunile destinatarului externalizării asigură continuitatea protecției atunci când prelucrarea datelor cu caracter personal este externalizată către o entitate din afara Coreei.

(88) În al doilea rând, operatorii coreeni pot furniza date cu caracter personal unui terț situat în afara Coreei. Deși PIPA include o serie de temeiuri juridice care permit furnizarea către terți în general, în cazul în care terțul se află în afara Coreei, operatorul trebuie, în principiu ([115]), să obțină consimțământul persoanei vizate ([116]) după ce a furnizat persoanei vizate informații privind (1) tipul de date cu caracter personal, (2) destinatarul datelor cu caracter personal, (3) scopul transferului în sensul scopului prelucrării urmărit de destinatar, (4) perioada de păstrare pentru prelucrarea de către destinatar, precum și (5) faptul că persoana vizată poate refuza consimțământul [articolul 17 alineatele (2) și (3) din PIPA]. Notificarea nr. 2021-5, în secțiunea sa privind transparența (a se vedea considerentul 70), impune ca persoanele fizice să fie informate cu privire la țara terță în care vor fi furnizate datele lor. Acest lucru asigură faptul că persoanele vizate din Uniune vor putea lua o decizie în deplină cunoștință de cauză cu privire la acordarea sau neacordarea consimțământului pentru o furnizare în străinătate. În plus, operatorul nu trebuie să încheie un contract cu beneficiarul terț cu încălcarea PIPA și, prin urmare, contractul nu trebuie să conțină obligații care ar contrazice cerințele impuse de PIPA operatorului ([117]).

([113]) Furnizorilor de servicii din domeniul informațiilor și comunicațiilor li se aplică norme specifice. În conformitate cu articolul 39-12 din PIPA, furnizorii de servicii din domeniul informațiilor și comunicațiilor trebuie, în principiu, să obțină consimțământul utilizatorului pentru orice transfer de informații cu caracter personal în străinătate. În cazul în care informațiile cu caracter personal sunt transferate ca parte a externalizării operațiunilor de prelucrare, inclusiv pentru stocare, consimțământul nu este necesar dacă persoanele în cauză au fost informate în prealabil, direct sau prin intermediul unui anunț public, într-un mod care să permită accesul facil, cu privire la (1) detalii privind informațiile care urmează să fie transferate, (2) țara către care vor fi transferate informațiile (precum și data și metoda transferului), (3) numele destinatarului și (4) scopul utilizării și păstrării de către destinatar [articolul 39-12 alineatul (3) din PIPA]. În plus, în acest caz se vor aplica cerințele generale privind externalizarea. Pentru fiecare transfer, trebuie instituite garanții specifice în ceea ce privește securitatea, tratarea plângerilor și a litigiilor, precum și alte măsuri necesare pentru protecția informațiilor utilizatorilor (articolul 48-10 din Decretul de punere în aplicare a PIPA).

([114]) A se vedea, de asemenea, articolul 26 alineatul (7) din PIPA, conform căruia articolele 25-15, 27-31, 33-38 și 50 se aplică *mutatis mutandis* persoanei împuternicite de operator.

([115]) În cazul furnizării către terți a informațiilor cu caracter personal ale utilizatorilor de către furnizorii de servicii din domeniul informațiilor și comunicațiilor, este necesar întotdeauna consimțământul utilizatorului [articolul 39-12 alineatul (2) din PIPA].

([116]) Astfel cum se explică în detaliu în nota de subsol 51, pentru ca un astfel de consimțământ să fie valabil, acesta trebuie să fie acordat în mod liber, în cunoștință de cauză și specific.

([117]) A se vedea, de asemenea, articolul 39-12 alineatul (1) din PIPA în ceea ce privește furnizorii de servicii din domeniul informațiilor și comunicațiilor.

(89) Fără consimțământul persoanei în cauză, datele cu caracter personal pot fi furnizate unui terț (în străinătate) dacă scopul divulgării rămâne „în domeniul de aplicare asociat în mod rezonabil" scopului inițial al colectării [articolul 17 alineatul (4) din PIPA; a se vedea considerentul 36]. Cu toate acestea, atunci când decide dacă să divulge (sau să nu divulge) date cu caracter personal pentru un scop „asociat", operatorul trebuie să ia în considerare dacă divulgarea generează dezavantaje pentru persoana în cauză și dacă au fost luate măsurile de securitate necesare (cum ar fi criptarea). Având în vedere că țara terță către care sunt transferate datele cu caracter personal nu poate oferi măsuri de protecție similare celor prevăzute în temeiul PIPA, secțiunea 2 din Notificarea nr. 2021-5 recunoaște că astfel de dezavantaje pot apărea și pot fi evitate numai dacă operatorul coreean și destinatarul din străinătate, prin intermediul unui instrument obligatoriu din punct de vedere juridic (cum ar fi un contract), asigură un nivel de protecție echivalent cu PIPA, inclusiv în ceea ce privește drepturile persoanelor vizate.

(90) În cazul divulgării „în afara scopului", și anume al furnizării de date unui terț cu un scop nou (fără legătură cu cel inițial), care poate avea loc numai pe baza unuia dintre motivele prevăzute la articolul 18 alineatul (2) din PIPA, astfel cum se descrie în considerentul 39, se aplică norme speciale. Totuși, chiar și în aceste condiții, furnizarea către terți este exclusă în cazul în care este de natură să „aducă atingere în mod abuziv" intereselor persoanei vizate sau ale unui terț, ceea ce necesită o echilibrare a intereselor. În plus, în temeiul articolului 18 alineatul (5) din PIPA, operatorul trebuie să aplice garanții suplimentare, care pot include o solicitare adresată terțului de a restricționa scopul și metoda de prelucrare sau de a institui măsuri de securitate specifice. Totodată, având în vedere că țara terță către care sunt transferate datele cu caracter personal nu poate oferi măsuri de protecție similare celor prevăzute în temeiul PIPA, secțiunea 2 din Notificarea nr. 2021-5 recunoaște că o asemenea „încălcare neloială" a intereselor persoanei fizice în cauză sau ale unui terț poate surveni și poate fi evitată numai dacă operatorul coreean și destinatarul din străinătate, prin intermediul unui instrument obligatoriu din punct de vedere juridic (cum ar fi un contract), asigură un nivel de protecție echivalent cu PIPA, inclusiv în ceea ce privește drepturile persoanelor vizate.

(91) Prin urmare, normele din considerentele 86-90 asigură continuitatea protecției atunci când datele cu caracter personal sunt transferate ulterior (către un „destinatar al exernalizării" sau către un terț) din Republica Coreea într-un mod care este în esență echivalent cu dispozițiile Regulamentului (UE) 2016/679.

2.3.10 *Responsabilitatea*

(92) Conform principiului responsabilității, entităților care prelucrează 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.

(93) În conformitate cu articolul 3 alineatele (6) și (8) din PIPA, operatorul trebuie să prelucreze datele cu caracter personal „într-un mod care să reducă la minimum posibilitatea de a se încălca" dreptul la viață privată al persoanei vizate și va depune eforturi pentru a obține încrederea persoanei vizate prin respectarea și îndeplinirea sarcinilor și a responsabilităților prevăzute în PIPA și în alte legi conexe. Aceasta include stabilirea unui plan de gestionare intern (articolul 29 din PIPA), precum și formarea și supravegherea corespunzătoare a personalului (articolul 28 din PIPA).

(94) Ca mijloc de asigurare a responsabilității, articolul 31 din PIPA coroborat cu articolul 32 din Decretul de punere în aplicare a PIPA creează obligația operatorilor de a desemna un responsabil cu protecția vieții private care „preia în mod cuprinzător sarcina prelucrării informațiilor cu caracter personal". În special, un astfel de responsabil cu protecția vieții private are sarcina de a îndeplini următoarele funcții: (1) stabilirea și punerea în aplicare a unui plan de protecție a datelor cu caracter personal și elaborarea politicii de confidențialitate, (2) efectuarea de anchete periodice privind stadiul și practicile de prelucrare a datelor cu caracter personal, în vederea remedierii oricăror deficiențe, (3) tratarea plângerilor și compensarea daunelor, (4) instituirea unui sistem de control intern pentru a preveni divulgarea, abuzul sau utilizarea necorespunzătoare a datelor cu caracter personal, (5) pregătirea și punerea în aplicare a unui program educațional, (6) protejarea, controlul și gestionarea dosarelor cu date cu caracter personal și (7) distrugerea datelor cu caracter personal după ce scopul prelucrării a fost atins sau perioada de păstrare a datelor a expirat. În îndeplinirea acestor sarcini, responsabilul cu protecția vieții private poate verifica stadiul prelucrării datelor cu caracter personal și sistemele conexe și poate solicita informații în acest sens [articolul 31 alineatul (3) din PIPA]. Dacă responsabilul cu protecția vieții private ia cunoștință de o încălcare a PIPA sau a altor legi relevante privind protecția datelor, acesta va lua imediat măsuri de remediere și va raporta aceste măsuri conducerii („șefului") operatorului, dacă este cazul [articolul 31 alineatul (4) din PIPA]. În conformitate cu articolul 31 alineatul (5) din PIPA, responsabilul cu protecția vieții private nu trebuie să se confrunte cu dezavantaje nejustificate ca urmare a exercitării acestor funcții.

(95) În plus, operatorii trebuie să depună eforturi în mod proactiv pentru a efectua o evaluare a impactului asupra vieții private în cazul în care operarea dosarelor cu date cu caracter personal implică un risc la adresa vieții private [articolul 33 alineatul (8) din PIPA]. În temeiul articolului 33 alineatele (1) și (2) din PIPA coroborate cu articolele 35, 36 și 38 din Decretul de punere în aplicare a PIPA, factori precum tipul și natura datelor prelucrate (în special dacă acestea constituie informații sensibile), volumul acestora, perioada de păstrare și probabilitatea încălcării securității datelor vor fi relevanți pentru evaluarea gradului de risc pentru drepturile persoanelor vizate. Scopul evaluării impactului asupra vieții private este de a asigura analizarea factorilor de risc pentru viața privată, precum și a oricăror măsuri de siguranță sau a altor contramăsuri, precum și de a indica aspectele care necesită îmbunătățiri [a se vedea articolul 33 alineatul (1) din PIPA coroborat cu articolul 38 din Decretul de punere în aplicare a PIPA].

(96) Instituțiile publice au obligația de a efectua o evaluare a impactului atunci când prelucrează anumite dosare cu date cu caracter personal care prezintă un risc mai ridicat de posibile încălcări ale vieții private [articolul 33 alineatul (1) din PIPA]. În conformitate cu articolul 35 din Decretul de punere în aplicare a PIPA, acest lucru este valabil, printre altele, pentru dosarele care conțin informații sensibile privind cel puțin 50 000 de persoane vizate, dosarele care vor fi corelate cu alte dosare și care, ca urmare a acestui fapt, vor conține informații privind cel puțin 500 000 de persoane vizate sau dosarele care conțin informații privind cel puțin un milion de persoane vizate. Rezultatul unei evaluări a impactului efectuate de o instituție publică trebuie comunicat PIPC [articolul 33 alineatul (1) din PIPA], care poate emite un aviz [articolul 33 alineatul (3) din PIPA].

(97) În cele din urmă, articolul 13 din PIPA prevede că PIPC stabilește politicile necesare pentru promovarea și sprijinirea „activităților de autoreglementare a protecției datelor" de către operatori, printre altele prin educația privind protecția datelor, promovarea și sprijinirea organizațiilor implicate în protecția datelor, precum și prin sprijinirea operatorilor în stabilirea și punerea în aplicare a normelor de autoreglementare. În plus, acesta introduce și facilitează sistemul de marcare cu ePRIVACY. În acest sens, articolul 32-2 din PIPA coroborat cu articolele 34-2 - 34-8 din Decretul de punere în aplicare a PIPA prevede posibilitatea de a certifica faptul că sistemul (sistemele) de prelucrare și protecție a datelor cu caracter personal al(e) unui operator respectă cerințele PIPA. În conformitate cu aceste norme, se poate acorda o certificare ([118]) (pentru o perioadă de 3 ani) dacă operatorul îndeplinește criteriile de certificare stabilite de PIPC, inclusiv instituirea unor garanții de gestionare, tehnice și fizice pentru protecția datelor cu caracter personal ([119]). PIPC trebuie să examineze sistemele operatorului care sunt relevante pentru certificare cel puțin o dată pe an, pentru menținerea eficacității, ceea ce poate duce la revocarea certificării [articolul 32 alineatul (4) din PIPA coroborat cu articolul 34-5 din Decretul de punere în aplicare a PIPA; așa-numita „gestionare subsecventă"].

(98) Prin urmare, cadrul coreean pune în aplicare principiul responsabilității într-un mod care asigură un nivel de protecție în esență echivalent cu cel prevăzut în Regulamentul (UE) 2016/679, inclusiv prin prevederea unor mecanisme diferite pentru a asigura și a demonstra conformitatea cu PIPA.

2.3.11 *Norme speciale pentru prelucrarea informațiilor cu caracter personal privind creditele*

(99) Astfel cum se descrie în considerentul 13, CIA stabilește norme specifice pentru prelucrarea informațiilor cu caracter personal privind creditele de către operatorii comerciali. Prin urmare, atunci când prelucrează informații cu caracter personal privind creditele, operatorii comerciali trebuie să respecte cerințele generale ale PIPA, cu excepția cazului în care CIA conține norme mai specifice. Acesta va fi cazul, de exemplu, atunci când prelucrează informații referitoare la un card de credit sau la un cont bancar în contextul unei tranzacții comerciale cu o persoană fizică. Fiind o lege sectorială ce vizează prelucrarea informațiilor privind creditele (atât cu caracter personal, cât și fără caracter personal), CIA nu numai că impune garanții specifice în materie de protecție a datelor (de exemplu în ceea ce privește transparența și securitatea), dar și reglementează într-un mod mai general, circumstanțele specifice în care pot fi prelucrate informațiile cu caracter personal privind creditele. Acest lucru se reflectă, în special, în cerințele detaliate privind utilizarea, furnizarea de date către un terț și păstrarea unor astfel de date.

(100) La fel ca PIPA, CIA reflectă principiile legalității și proporționalității. În primul rând, ca cerință generală, articolul 15 alineatul (1) din CIA permite colectarea de informații cu caracter personal privind creditele numai prin mijloace rezonabile și echitabile și în cea mai mică măsură necesară pentru a servi unui scop determinat, în conformitate cu articolul 3 alineatele (1)-(2) din PIPA. În al doilea rând, CIA reglementează în mod specific legalitatea prelucrării informațiilor cu caracter personal privind creditele, limitând colectarea, utilizarea și furnizarea acestora unui terț și asociind în general aceste activități de prelucrare de cerința consimțământului persoanei în cauză.

([118]) În plus, în cazul în care operatorul intenționează să facă referire la certificare sau să promoveze certificarea în cadrul operațiunilor sale comerciale, acesta poate utiliza marcajul privind protecția informațiilor cu caracter personal stabilit de PIPC. A se vedea articolul 34-7 din Decretul de punere în aplicare a PIPA.

([119]) Începând din noiembrie 2018, a fost dezvoltat „Sistemul privind informațiile cu caracter personal și de management al securității informațiilor" (ISMS-P), care certifică faptul că operatorii utilizează un sistem de gestionare cuprinzător.

(101) Informațiile cu caracter personal privind creditele pot fi colectate pe baza unuia dintre motivele furnizate de PIPA sau pe baza unor motive specifice enunțate în CIA. Având în vedere că articolul 45 din Regulamentul (UE) 2016/679 presupune un transfer de date cu caracter personal de către un operator sau o persoană împuternicită de operator din Uniune, dar nu se referă la colectarea directă (de exemplu de la persoana fizică sau de pe un site web) de către un operator din Coreea, numai consimțământul și motivele prevăzute de PIPA sunt relevante pentru prezenta decizie. Printre aceste motive se numără, în special, situațiile în care transferul este necesar pentru executarea unui contract cu persoana în cauză sau pentru interesele legitime ale operatorului coreean [articolul 15 alineatul (1) punctele 4 și 6 din PIPA] ([120]).

(102) Odată colectate, informațiile cu caracter personal privind creditele pot fi utilizate (1) în scopul inițial pentru care au fost furnizate (direct) de către persoana respectivă ([121]); (2) într-un scop compatibil cu scopul inițial al colectării ([122]); (3) pentru a stabili dacă să stabilească sau să mențină o relație comercială solicitată de persoana respectivă ([123]); (4) în scopuri statistice, de cercetare și arhivare în interes public ([124]), dacă informațiile sunt pseudonimizate ([125]); (5) în cazul în care se obține un nou consimțământ sau (6) în conformitate cu legea.

(103) În cazul în care un operator comercial intenționează să divulge unui terț informații cu caracter personal privind creditele, acesta trebuie să obțină consimțământul persoanei în cauză ([126]) după ce a informat-o cu privire la destinatarul datelor, la scopul prelucrării de către destinatar, la detaliile privind datele care urmează a fi furnizate, la perioada de stocare de către destinatar și la dreptul de a refuza consimțământul [articolul 32 alineatul (1) din CIA și articolul 28 alineatul (2) din Decretul de punere în aplicare a CIA] ([127]). Această cerință privind consimțământul nu se aplică în situații specifice, și anume în cazul în care informațiile cu caracter personal privind creditele sunt divulgate ([128]): (1) unui destinatar al externalizării în scopuri de externalizare ([129]); (2) unui terț în cazul unui transfer, al unei divizări sau fuziuni de întreprinderi; (3) în scopuri statistice, de cercetare și arhivare în interes public, dacă informațiile sunt pseudonimizate; (4) într-un scop compatibil cu scopul inițial al colectării; (5) unui terț care utilizează informațiile pentru a încasa o datorie a persoanei în cauză ([130]); (6) pentru a se conforma unei hotărâri judecătorești; (7) unui procuror/agent de poliție judiciară într-o situație de urgență în care viața persoanei este în pericol sau în care este de așteptat să sufere vătămări corporale și nu este timp pentru

([120]) CIA conține și alte temeiuri juridice pentru colectare, și anume atunci când acest lucru este cerut de lege, atunci când informațiile sunt făcute publice de o instituție publică în temeiul legislației privind libertatea de informare sau atunci când informațiile sunt disponibile pe o rețea socială. Pentru ca operatorul comercial să poată invoca ultimul motiv, acesta trebuie să fie în măsură să demonstreze încadrarea colectării în domeniul de aplicare al consimțământului persoanei vizate, pe baza unei interpretări rezonabile („obiective") și ținând seama de natura datelor, de intenția și de scopul de a le pune la dispoziție în cadrul rețelei sociale, în cazul în care caracterul colectării este „foarte relevant" pentru scopul respectiv etc. (articolul 13 din Decretul de punere în aplicare a CIA). Cu toate acestea, astfel cum se explică în considerentul 101, aceste motive nu vor fi, în principiu, relevante într-un scenariu de transfer.

([121]) De exemplu, atunci când informațiile privind creditele sunt generate/furnizate în contextul unei tranzacții comerciale cu persoana în cauză. Totuși, acest motiv nu poate fi invocat pentru a utiliza informațiile cu caracter personal privind creditele în scopuri de marketing direct [a se vedea articolul 33 alineatul (1) punctul 3 din CIA].

([122]) Pentru a stabili dacă scopul utilizării este compatibil cu scopul inițial al colectării, trebuie luați în considerare următorii factori: (1) relația („relevanța") dintre cele două scopuri; (2) modul în care au fost colectate informațiile; (3) impactul utilizării asupra persoanei în cauză și (4) dacă au fost puse în aplicare măsuri de securitate adecvate, cum ar fi pseudonimizarea [a se vedea articolul 32 alineatul (6) punctul 9-4 din CIA].

([123]) De exemplu, un operator ar putea fi nevoit să ia în considerare informațiile cu caracter personal privind creditele pe care le-a primit de la o persoană fizică pentru a decide dacă să extindă durata unui împrumut acordat persoanei respective.

([124]) Articolul 33 din CIA coroborat cu articolul 32 alineatul (6) punctele 9-2, 9-4 și 10 din CIA.

([125]) Pseudonimizarea este definită la articolul 2 alineatul (15) din CIA ca o prelucrare a informațiilor cu caracter personal privind creditele care să nu mai permită identificarea persoanelor fizice din informațiile respective decât în combinație cu informații suplimentare. Deși CIA conține garanții specifice pentru prelucrarea informațiilor pseudonimizate în scopuri statistice, de cercetare și de arhivare în interes public (articolul 40-2 din CIA), aceste norme nu se aplică organizațiilor comerciale. În schimb, acestea din urmă fac în continuare obiectul cerințelor specifice din secțiunea III din PIPA, astfel cum se descrie în considerentele 42-48. Articolul 40-3 din CIA exonerează, de asemenea, prelucrarea informațiilor pseudonimizate privind creditele – atunci când aceasta are loc în scopuri statistice, de cercetare științifică sau de arhivare în interes public – de la cerințele privind transparența și drepturile individuale, în mod similar cu excepția prevăzută la articolul 28-7 din PIPA și sub rezerva garanțiilor prevăzute în secțiunea III din PIPA, astfel cum sunt descrise mai detaliat în considerentele 42-48.

([126]) Acest lucru nu este valabil în cazul se furnizează informații unui terț pentru a menține informațiile cu caracter personal privind creditele exacte și actualizate, atât timp cât furnizarea rămâne în scopul inițial al prelucrării [articolul 32 alineatul (1) din CIA]. Aceasta poate avea loc, de exemplu, atunci când agenției de rating de credit îi sunt furnizate informații actualizate pentru a se asigura că evidențele sale sunt corecte.

([127]) În cazul în care nu este practic să se furnizeze informațiile menționate mai sus, poate fi suficient ca persoana respectivă să fie îndrumată către destinatarul terț pentru informațiile solicitate.

([128]) Având în vedere că CIA nu reglementează în mod specific divulgarea în străinătate a informațiilor cu caracter personal privind creditele, aceste divulgări trebuie să respecte garanțiile pentru transferurile ulterioare impuse de secțiunea 2 din Notificarea nr. 2021-5.

([129]) Externalizarea prelucrării informațiilor cu caracter personal privind creditele poate avea loc numai pe baza unui contract scris și în conformitate cu cerințele de la articolul 26 alineatele (1)-(3) și (5) din PIPA, astfel cum se descrie în considerentul 20 (articolul 17 din CIA și articolul 14 din Decretul de punere în aplicare a CIA). Destinatarul externalizării nu poate utiliza informații care depășesc domeniul de aplicare al sarcinilor externalizate, iar societatea care efectuează externalizarea trebuie să instituie cerințe de securitate specifice (de exemplu, criptarea) și să-l educe pe destinatarul externalizării cu privire la modul de prevenire a pierderii, furtului, divulgării, modificării sau compromiterii informațiilor privind creditele.

([130]) A se vedea, de asemenea, articolul 28 alineatul (10) punctele 1, 2 și 6 din Decretul de punere în aplicare a CIA.

emiterea unui mandat judecătoresc ([131]); (8) autorităților fiscale competente în vederea respectării legislației fiscale; sau (9) în conformitate cu alte legi. În cazul divulgării bazate pe unul dintre aceste motive, persoana vizată trebuie să fie informată în prealabil în acest sens [articolul 32 alineatul (7) din CIA].

(104) De asemenea, CIA reglementează în mod specific durata prelucrării informațiilor cu caracter personal privind creditele pe baza unuia dintre aceste motive de utilizare sau furnizare către un terț după încetarea relației comerciale cu persoana respectivă ([132]). Numai informațiile necesare pentru a stabili sau a menține această relație pot fi păstrate, sub rezerva unor garanții suplimentare (acestea trebuie să fie păstrate separat de informațiile privind creditele care se referă la persoane cu care există o relație comercială în curs, protejate prin măsuri de securitate specifice și accesibile numai persoanelor autorizate) ([133]). Toate celelalte date trebuie șterse [articolul 17-2 alineatul (1) punctul 2 din Decretul de punere în aplicare a CIA]. Pentru a stabili care date au fost necesare pentru relația comercială, trebuie luați în considerare diferiți factori, inclusiv dacă ar fi fost posibil ca relația să se stabilească fără datele respective și dacă aceasta privește în mod direct bunurile sau serviciile furnizate persoanei respective [articolul 17-2 alineatul (2) din Decretul de punere în aplicare a CIA].

(105) Chiar și în cazurile în care informațiile cu caracter personal privind creditele pot fi păstrate, în principiu, după încheierea relației comerciale, acestea trebuie șterse în termen de trei luni de la atingerea scopului ulterior al prelucrării ([134]) sau, în orice caz, după cinci ani (articolul 20-2 din CIA). Într-un număr limitat de situații, informațiile cu caracter personal privind creditele pot fi păstrate pentru o perioadă mai mare de cinci ani, în special dacă acest lucru este necesar pentru a se conforma unei obligații legale; atunci când sunt necesare pentru interesele vitale privind viața, integritatea fizică sau bunurile unei persoane; pentru arhivarea informațiilor pseudonimizate (care au fost utilizate în scopuri de cercetare științifică, statistici sau arhivare în interes public); sau în scopuri legate de asigurări (în special pentru plata asigurărilor sau pentru prevenirea fraudei în domeniul asigurărilor) ([135]). În aceste cazuri excepționale, se aplică garanții specifice [cum ar fi notificarea persoanei cu privire la utilizarea ulterioară, separarea informațiilor păstrate de informațiile care se referă la persoane cu care există încă o relație comercială, limitarea drepturilor de acces; a se vedea articolul 17-2 alineatele (1)-(2) din Decretul de punere în aplicare a CIA].

(106) De asemenea, CIA specifică principiile exactității și calității datelor, impunând ca informațiile cu caracter personal privind creditele să fie „înregistrate, modificate și gestionate" pentru a le menține exacte și actualizate [articolul 18 alineatul (1) CIA și articolul 15 alineatul (3) din Decretul de punere în aplicare a CIA] ([136]). Atunci când furnizează informații cu privire la credite altor entități (cum ar fi agențiile de rating de credit), operatorii comerciali au, de asemenea, obligația specifică să verifice exactitatea informațiilor, pentru a se asigura că destinatarul înregistrează și gestionează numai informații exacte [articolul 15 alineatul (1) din Decretul de punere în aplicare a CIA, coroborat cu articolul 18 alineatul (1) din CIA]. La un nivel mai general, CIA prevede obligația de păstrare a unor evidențe privind colectarea, utilizarea, divulgarea de către terți și distrugerea informațiilor cu caracter personal privind creditele [articolul 20 alineatul (2) din CIA] ([137]).

(107) În plus, prelucrarea informațiilor cu caracter personal privind creditele face obiectul unor cerințe specifice în ceea ce privește securitatea datelor. În special, CIA impune punerea în aplicare a unor măsuri tehnologice, fizice și organizatorice pentru a preveni accesul ilegal la sistemele informatice, precum și modificarea, distrugerea sau orice alt risc pentru datele prelucrate (de exemplu, prin intermediul controalelor de acces; a se vedea articolul 19 din CIA și articolul 16 din Decretul de punere în aplicare a CIA). În plus, atunci când are loc un schimb de informații cu caracter personal privind creditele cu un terț, trebuie încheiat un acord care să prevadă măsuri de securitate specifice [articolul 19 alineatul (2) din CIA]. În cazul în care are loc o încălcare a informațiilor cu caracter personal privind creditele, trebuie luate măsuri pentru a reduce la minimum orice prejudiciu, iar persoanele în cauză trebuie informate fără întârziere [articolul 39-4 alineatele (1)-(2) din CIA]. În plus, PIPC trebuie să fie informat cu privire la notificarea transmisă persoanelor fizice și la măsurile care au fost puse în aplicare [articolul 39-4 alineatul (4) din CIA].

([131]) În acest caz, trebuie solicitat fără întârziere un mandat. În cazul în care mandatul nu este emis în termen de 36 de ore, datele primite trebuie șterse fără întârziere [articolul 32 alineatul (6) punctul 6 din CIA].

([132]) De exemplu, întrucât obligațiile contractuale au fost îndeplinite, una dintre părți și-a exercitat dreptul de reziliere etc.; a se vedea articolul 17-2 alineatul (5) din Decretul de punere în aplicare a CIA.

([133]) Articolul 20-2 alineatul (1) din CIA și articolul 17-2 alineatul (1) punctul 1 din Decretul de punere în aplicare a CIA.

([134]) Această perioadă ține seama de faptul că, adesea, ștergerea nu va fi posibilă imediat, ci, de regulă, va necesita anumite etape (de exemplu, separarea datelor care urmează să fie șterse de alte date și efectuarea ștergerii fără a afecta stabilitatea sistemelor informatice) care necesită o anumită perioadă de timp pentru punerea în aplicare.

([135]) Articolul 20-2 alineatul (2) din CIA.

([136]) Articolul 18 alineatul (2) din CIA și articolul 15 alineatul (4) din Decretul de punere în aplicare a CIA stabilesc norme mai specifice în ceea ce privește această cerință de ținere a evidențelor, de exemplu pentru înregistrările referitoare la informații care pot dezavantaja o persoană, cum ar fi informațiile privind delincvența și falimentul.

([137]) În ceea ce privește alte mecanisme de responsabilizare, CIA solicită anumitor organizații [de exemplu, cooperativele și corporațiile publice, a se vedea articolul 21 alineatul (2) din Decretul de punere în aplicare a CIA] să numească un „administrator/tutore al informațiilor privind creditele" care este responsabil cu monitorizarea respectării CIA și îndeplinește sarcinile „responsabilului cu protecția vieții private" în temeiul PIPA [articolul 20 alineatele (3) și (4) din CIA].

(108) De asemenea, CIA prevede obligații specifice de transparență la obținerea consimțământului pentru utilizarea sau furnizarea de informații cu caracter personal privind creditele [articolul 32 alineatul (4) și articolul 34-2 din CIA și articolul 30-3 din Decretul de punere în aplicare a CIA] și, mai general, înainte de a furniza informații unui terț [articolul 32 alineatul (7) din CIA] ([138]). În plus, persoanele fizice au dreptul de a obține, la cerere, informații cu privire la utilizarea și furnizarea informațiilor lor privind creditele către terți în cei trei ani anteriori cererii (inclusiv scopul și datele unei astfel de utilizări/furnizări) ([139]).

(109) În temeiul CIA, persoanele fizice au, de asemenea, drept de acces la informațiile lor personale privind creditele [articolul 38 alineatul (1) din CIA] și de a obține rectificarea datelor inexacte [articolul 38 alineatele (2)-(3) din CIA] ([140]). În plus, pe lângă dreptul general la ștergerea datelor în temeiul PIPA (a se vedea considerentul 77), CIA prevede un drept specific la ștergerea informațiilor cu caracter personal privind creditele care au fost păstrate un timp mai îndelungat decât perioadele de păstrare menționate în considerentul 104, și anume cinci ani (pentru informațiile cu caracter personal privind creditele care au fost necesare pentru stabilirea sau menținerea unei relații comerciale) sau trei luni (pentru alte tipuri de informații cu caracter personal privind creditele) ([141]). În mod excepțional, o cerere de ștergere poate fi refuzată în cazul în care este necesară o păstrare ulterioară în circumstanțele descrise în considerentul 105. În cazul în care o persoană solicită ștergerea, dar se aplică una dintre excepții, trebuie aplicate garanții specifice informațiilor privind creditele în cauză [articolul 38-3 alineatul (3) din CIA și articolul 33-3 din Decretul de punere în aplicare a CIA]. De exemplu, informațiile trebuie păstrate separat de alte informații, pot fi accesate numai de către o persoană autorizată și trebuie să facă obiectul unor măsuri de securitate specifice.

(110) În plus față de drepturile menționate în considerentul 109, CIA le garantează persoanelor fizice dreptul de a solicita unui operator să înceteze să le contacteze în scopuri de marketing direct [articolul 37 alineatul (2) din lege] și dreptul la portabilitatea datelor. În privința acestuia din urmă, CIA le permite persoanelor fizice să solicite transmiterea informațiilor lor cu caracter personal privind creditele către ele însele sau către anumiți terți (cum ar fi instituțiile financiare și societățile de rating de credit). Informațiile cu caracter personal privind creditele trebuie prelucrate și transmise părții terțe într-un format care poate fi prelucrat de un dispozitiv de prelucrare a informațiilor (cum ar fi un calculator).

(111) În măsura în care CIA conține norme specifice în comparație cu PIPA, Comisia consideră, prin urmare, că și aceste norme asigură un nivel de protecție în esență echivalent cu cel oferit de Regulamentul (UE) 2016/679.

2.4 **Supravegherea și asigurarea respectării normelor**

(112) Pentru a garanta 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.

2.4.1 *Supravegherea independentă*

(113) În Republica Coreea, autoritatea independentă însărcinată cu monitorizarea și punerea în aplicare a PIPA este PIPC. PIPC este alcătuită dintr-un președinte, un vicepreședinte și șapte comisari. Președintele și vicepreședintele sunt numiți de președintele statului la recomandarea prim-ministrului. Dintre comisari, doi sunt numiți de președintele statului la recomandarea președintelui comisiei, și cinci, la recomandarea Adunării Naționale [dintre care doi la recomandarea partidului politic din care face parte președintele statului și trei la recomandarea altor partide politice [articolul 7-2 alineatul (2) din PIPA], ceea ce ajută la evitarea unei situații de părtinire în

([138]) Aceasta include o cerință generală de notificare [articolul 32 alineatul (7) din CIA] și o obligație specifică de transparență în cazul în care informațiile prin care se poate stabili bonitatea unei persoane sunt furnizate anumitor entități, cum ar fi agențiile de rating de credit și agențiile de colectare a informațiilor privind creditele (articolul 35-3 din CIA și articolul 30-3 din Decretul de punere în aplicare a CIA) ori în cazul refuzării sau încetării unei relații comerciale pe baza informațiilor cu caracter personal privind creditele primite de la un terț (articolul 36 din CIA și articolul 31 din Decretul de punere în aplicare a CIA).

([139]) Articolul 35 din CIA. Anumite organizații comerciale, de exemplu cooperativele și corporațiile publice [articolul 21 alineatul (2) din Decretul de punere în aplicare a CIA], fac obiectul unor cerințe suplimentare în materie de transparență, de exemplu, de a pune anumite informații la dispoziția publicului (articolul 31 din CIA) și de a informa persoanele fizice cu privire la posibilele dezavantaje ale scorului lor de rating de credit atunci când se angajează în tranzacții financiare care prezintă riscuri de credit (articolul 35-2 din CIA).

([140]) În ceea ce privește condițiile și excepțiile de la drepturile de acces și de rectificare, se aplică normele PIPA (descrise în considerentele 76-77). În plus, la articolul 38 alineatele (4)-(8) din CIA și la articolul 33 din Decretul de punere în aplicare a CIA sunt prevăzute alte modalități. În special, un operator comercial care a corectat sau a șters informațiile inexacte referitoare la credite trebuie să transmită persoanei în cauză o notificare în acest sens. În plus, orice terț căruia i-au fost dezvăluite aceste informații în cursul ultimelor șase luni trebuie să fie înștiințat, iar persoana în cauză trebuie să fie informată în acest sens. În cazul în care o persoană nu este mulțumită de modul în care a fost tratată o cerere de rectificare, aceasta poate depune o cerere la PIPC, care verifică acțiunile operatorului și poate impune măsuri de remediere.

([141]) Articolul 38-3 din CIA.

procesul de numire) ([142]). Această procedură este în concordanță cu cerințele aplicabile numirii membrilor autorităților de protecție a datelor din Uniune [articolul 53 alineatul (1) din Regulamentul (UE) 2016/679]. În plus, toți comisarii trebuie să se abțină de la implicarea în orice activitate comercială care generează profit, de la activități politice și de la deținerea de funcții în administrația publică sau în Adunarea Națională [articolele 7-6 și 7-7 alineatul (1) punctul 3 din PIPA] ([143]). Toți comisarii fac obiectul unor norme specifice menite să împiedice participarea lor la deliberări în cazul unui posibil conflict de interese (articolul 7-11 din PIPA). PIPC este asistat de un secretariat (articolul 7-13) și poate înființa subcomisii (formate din trei comisari) pentru a trata încălcările minore și chestiunile recurente (articolul 7-12 din PIPA).

(114) Fiecare membru al PIPC este numit pe trei ani și poate fi numit din nou o singură dată [articolul 7-4 alineatul (1) din PIPA]. Comisarii pot fi demiși numai în anumite circumstanțe, și anume dacă nu mai sunt în măsură să își exercite atribuțiile din cauza unei dizabilități mintale sau fizice pe termen lung, dacă încalcă legea sau în cazul unuia dintre motivele de revocare din funcție ([144]) (articolul 7-5 din PIPA). Acest lucru le oferă protecție instituțională în exercitarea funcțiilor lor.

(115) La un nivel mai general, articolul 7 alineatul (1) din PIPA garantează în mod explicit independența PIPC, iar articolul 7-5 alineatul (2) din PIPA prevede obligația comisarilor de a-și îndeplini atribuțiile în mod independent, în conformitate cu legea și cu propria lor conștiință ([145]). Garanțiile instituționale și procedurale descrise, inclusiv în ceea ce privește numirea și demiterea membrilor săi, asigură faptul că PIPC acționează în deplină independență, fără influențe sau instrucțiuni externe. În plus, în calitate de agenție administrativă centrală, PIPC își propune anual propriul buget (care este revizuit de Ministerul Finanțelor ca parte a bugetului național general înainte de adoptarea de către Adunarea Națională) și este responsabilă cu gestionarea personalului propriu. PIPC are un buget curent de circa 35 de milioane EUR și are 154 de angajați (inclusiv 40 de angajați specializați în tehnologia informației și comunicațiilor, 32 de angajați specializați în investigații și 40 de experți juridici).

(116) Sarcinile și competențele PIPC sunt prevăzute în principal la articolele 7-8 și 7-9, precum și la articolele 61-66 din PIPA ([146]). În special, sarcinile PIPC includ consilierea cu privire la actele cu putere de lege și normele administrative referitoare la protecția datelor, elaborarea de politici și orientări în materie de protecție a datelor, investigarea încălcărilor drepturilor individuale, tratarea plângerilor și medierea litigiilor, asigurarea respectării PIPA, asigurarea educării și a promovării în domeniul protecției datelor, precum și schimbul de informații și cooperarea cu autoritățile de protecție a datelor din țările terțe ([147]).

(117) În temeiul articolului 68 din PIPA coroborat cu articolul 62 din Decretul de punere în aplicare a PIPA, anumite sarcini ale PIPC au fost delegate Agenției coreene pentru internet și securitate, și anume: (1) educația și relațiile publice, (2) formarea specialiștilor și elaborarea de criterii pentru evaluările impactului asupra vieții private, (3) tratarea cererilor de desemnare a unei așa-numite instituții de evaluare a impactului asupra vieții private, (4) tratarea cererilor de acces indirect la datele cu caracter personal deținute de autoritățile publice [articolul 35 alineatul (2) din PIPA] și (5) sarcina de a solicita materiale și de a efectua inspecții cu privire la plângerile primite prin așa-numitul Centru de intermediere telefonică pentru protecția vieții private. În contextul tratării plângerilor prin intermediul Centrului de intermediere telefonică pentru protecția vieții private, Agenția coreeană pentru

([142]) Numai persoanele care îndeplinesc următoarele criterii pot fi numite drept comisari PIPC: înalți funcționari publici responsabili cu gestionarea informațiilor cu caracter personal; foști judecători, procurori sau avocați care și-au exercitat profesia timp de cel puțin 10 ani; foști manageri cu experiență în domeniul protecției datelor care au lucrat într-o instituție sau organizație publică mai mult de trei ani sau care au fost recomandați de o astfel de instituție sau organizație; și foști conferențiari cu cunoștințe de specialitate în domeniul protecției datelor, care au lucrat cel puțin cinci ani într-o instituție academică (articolul 7-2 din PIPA).

([143]) A se vedea, de asemenea, articolul 4-2 din Decretul de punere în aplicare a PIPA.

([144]) A se vedea articolul 7-7 din PIPA, conform căruia cetățenii și membrii partidelor politice de altă cetățenie decât cea coreeană nu pot deveni membri ai PIPC. Același lucru este valabil și în cazul persoanelor pentru care s-au impus anumite tipuri de sancțiuni penale, au fost revocate din funcție prin măsuri disciplinare în ultimii cinci ani etc. (articolul 7-7 din PIPA coroborat cu articolul 33 din Legea privind funcționarii publici).

([145]) Deși articolul 7 alineatul (2) din PIPA se referă la competența generală a prim-ministrului în temeiul articolului 18 din Legea privind organizațiile guvernamentale de a suspenda sau de a revoca – cu aprobarea președintelui statului – orice dispoziție ilegală sau injustă a unei agenții administrative centrale, nu se acordă o astfel de competență în ceea ce privește competențele de investigare sau de executare ale PIPC [a se vedea articolul 7 alineatul (2) punctele 1 și 2 din PIPA]. Conform explicațiilor primite de la guvernul coreean, articolul 18 din Legea privind organizațiile guvernamentale are rolul de a oferi prim-ministrului posibilitatea de a acționa în circumstanțe extraordinare, de exemplu pentru a media un dezacord între diferite agenții guvernamentale. Cu toate acestea, prim-ministrul nu a făcut niciodată uz de această competență de la adoptarea acestei dispoziții în 1963.

([146]) Atunci când este necesar pentru îndeplinirea sarcinilor prevăzute la articolul 7-9 alineatul (1) din PIPA, PIPC poate solicita avize de la funcționarii publici relevanți, experții din domeniul protecției datelor, organizații civice și operatorii economici relevanți. În plus, PIPC poate solicita materiale relevante, poate emite recomandări de îmbunătățire și poate verifica dacă acestea sunt puse în aplicare [articolul 7-9 alineatele (2)-(5) din PIPA].

([147]) A se vedea, de asemenea, articolul 9 din PIPA (Planul general trienal pentru protecția informațiilor cu caracter personal), articolul 12 din PIPA (Orientări standard privind protecția informațiilor cu caracter personal), articolul 13 din PIPA (Politici pentru promovarea și sprijinirea autoreglementării).

internet și securitate transmite cazul către PIPC sau către parchet, în cazul în care constată că a avut loc o încălcare a legii. Posibilitatea de a depune o plângere la Centrul de intermediere telefonică pentru protecția vieții private nu împiedică persoanele fizice să depună în mod direct o plângere la PIPC sau să se adreseze PIPC în cazul în care consideră că plângerea lor nu a fost tratată în mod satisfăcător de către Agenția coreeană pentru internet și securitate.

2.4.2 *Asigurarea respectării normelor, inclusiv sancțiuni*

(118) În vederea asigurării conformității cu PIPA, legiuitorul a acordat PIPC atât competențe de investigare, cât și competențe de executare, variind de la recomandări la amenzi administrative. Aceste competențe sunt completate și de un regim de sancțiuni penale.

(119) În ceea ce privește competențele de investigare, în cazul în care se suspectează sau s-a raportat o încălcare a PIPA ori în cazul în care este necesar pentru protecția drepturilor persoanelor vizate împotriva încălcărilor, PIPC poate efectua inspecții la fața locului și poate solicita toate materialele relevante (cum ar fi articole și documente) de la operatorii de date cu caracter personal (articolul 63 din PIPA coroborat cu articolul 60 din Decretul de punere în aplicare a PIPA) ([148]).

(120) În ceea ce privește punerea în aplicare, în temeiul articolului 61 alineatul (2) din PIPA, PIPC poate oferi recomandări operatorilor de date cu privire la modalitățile în care pot îmbunătăți nivelul de protecție a datelor cu caracter personal pentru anumite activități de prelucrare. Operatorii de date trebuie să depună eforturi de bună credință pentru a pune în aplicare astfel de recomandări și au obligația de a informa PIPC cu privire la rezultat. În plus, în cazul în care există motive întemeiate să se creadă că a avut loc o încălcare a PIPA și că neluarea de măsuri este de natură să cauzeze prejudicii dificil de remediat, PIPC poate impune măsuri de remediere [articolul 64 alineatul (1) din PIPA] ([149]). Secțiunea 5 din Notificarea 2021-5 (anexa I) clarifică, cu efect obligatoriu, faptul că aceste condiții sunt îndeplinite în ceea ce privește încălcarea oricărei dispoziții PIPA care protejează drepturile la viață privată ale persoanelor fizice în ceea ce privește informațiile cu caracter personal ([150]). Printre măsurile pe care PIPC este abilitată să le ia se numără dispunerea încetării comportamentului care a cauzat încălcarea, suspendarea temporară a prelucrării datelor sau orice alte măsuri necesare. Nerespectarea unei măsuri de remediere poate conduce la impunerea unei sancțiuni sub unei forma unei amenzi cu o valoare maximă de 50 de milioane de woni [articolul 75 alineatul (2) punctul 13 din PIPA].

(121) În ceea ce privește anumite autorități publice (cum ar fi Adunarea Națională, agențiile administrative centrale, organismele administrației locale și instanțele), articolul 64 alineatul (4) din PIPA prevede că PIPC poate „recomanda" oricare dintre măsurile de remediere menționate în considerentul 120 și că aceste autorități sunt obligate să respecte o astfel de recomandare, cu excepția cazului în care există circumstanțe extraordinare. În conformitate cu secțiunea 5 din Notificarea nr. 2021-5, aceasta se referă la circumstanțe de fapt sau de drept extraordinare de care PIPC nu a avut cunoștință atunci când a formulat recomandarea. Autoritatea publică în cauză poate invoca astfel de circumstanțe extraordinare numai dacă demonstrează în mod clar că nu a avut loc nicio încălcare, iar PIPC stabilește că situația nu este, într-adevăr, aceasta. În caz contrar, autoritatea publică trebuie să urmeze recomandarea PIPC și „să ia o măsură de remediere, inclusiv să oprească imediat acțiunea, și să compenseze daunele în cazul excepțional în care a fost totuși săvârșită o faptă ilegală".

(122) PIPC poate solicita, de asemenea, altor agenții administrative cu competențe specifice în temeiul legislației sectoriale (de exemplu în domeniul sănătății, al educației) să efectueze o investigație – pe cont propriu sau împreună cu PIPC – cu privire la (suspiciunile de) încălcări ale confidențialității de către operatorii care activează în aceste sectoare sub jurisdicția lor și să impună măsuri de remediere [articolul 63 alineatele (4)-(5) din PIPA]. În acest caz, PIPC stabilește temeiul, obiectul și domeniul de aplicare al investigației ([151]). La rândul său, agenția administrativă competentă trebuie să prezinte PIPC un plan de inspecție și să transmită PIPC rezultatul inspecției. PIPC poate recomanda luarea unei măsuri de remediere specifice, agenția competentă trebuind să depună toate eforturile pentru a o pune în aplicare. În orice caz, o astfel de solicitare nu limitează competența PIPC de a efectua propria investigație sau de a impune sancțiuni.

([148]) În plus, PIPC are acces la sediile operatorului pentru a inspecta situația operațiunilor comerciale, a înregistrărilor, a documentelor etc. [articolul 63 alineatul (2) din PIPA]. A se vedea, de asemenea, articolul 45-3 din CIA și articolul 36-4 din Decretul de punere în aplicare a CIA în ceea ce privește competențele PIPC în temeiul legii respective.

([149]) A se vedea, de asemenea, articolul 45-4 din CIA în ceea ce privește competențele PIPC prevăzute de CIA.

([150]) Secțiunea 5 din notificare prevede că „un motiv întemeiat pentru a considera că a avut loc o încălcare în ceea ce privește informațiile cu caracter personal și că lipsa de acțiune este de natură să cauzeze prejudicii dificil de remediat în sensul articolului 64 alineatele (1) și (2) din PIPA se referă la o încălcare a oricăruia dintre principiile, drepturile și obligațiile prevăzute de lege pentru a proteja drepturile persoanelor fizice la informații cu caracter personal." Acest lucru este valabil și în cazul competențelor PIPC prevăzute la articolul 45-4 din CIA.

([151]) Articolul 60 din Decretul de punere în aplicare a PIPA.

(123) Pe lângă competențele sale de remediere, PIPC poate impune amenzi administrative cu valori cuprinse între 10 și 50 de milioane de woni pentru încălcări ale diferitelor cerințe ale PIPA (articolul 75 din PIPA) ([152]). Printre altele, aceasta include nerespectarea cerințelor privind legalitatea prelucrării, neluarea măsurilor de securitate necesare, nerespectarea obligației de a transmite o notificare persoanelor vizate în cazul unei încălcări a securității datelor, nerespectarea cerințelor privind subcontractarea serviciilor de prelucrare a datelor, neinstituirea și nepublicarea unei politici de confidențialitate, nedesemnarea unui responsabil cu protecția vieții private sau lipsa de acțiune la cererea persoanei vizate în exercitarea drepturilor sale individuale, precum și anumite încălcări procedurale (lipsa cooperării în cursul unei investigații). În cazul încălcării mai multor dispoziții ale PIPA de către același operator, se poate aplica o amendă pentru fiecare încălcare, iar la stabilirea nivelului amenzii se va lua în considerare numărul persoanelor afectate.

(124) În plus, în cazul în care există motive întemeiate pentru a suspecta o încălcare a PIPA sau a oricăror alte „legi privind protecția datelor", PIPC poate depune o plângere penală la agenția de investigare competentă [cum ar fi un procuror; a se vedea articolul 65 alineatul (1) din PIPA]. În plus, PIPC poate recomanda operatorului să ia măsuri disciplinare împotriva persoanei responsabile [inclusiv a managerului responsabil; a se vedea articolul 65 alineatul (2) din PIPA]. La primirea unei astfel de recomandări, operatorul trebuie să se conformeze ([153]) și să notifice PIPC în scris rezultatul (articolul 65 din PIPA coroborat cu articolul 58 din Decretul de punere în aplicare a PIPA).

(125) În ceea ce privește recomandarea prevăzută la articolul 61, măsurile de remediere prevăzute la articolul 64, acuzarea sau recomandarea unei măsuri disciplinare prevăzută la articolul 65 și impunerea de amenzi administrative prevăzută la articolul 75 din PIPA, PIPC poate face publice faptele – și anume încălcarea, entitatea care a încălcat legea și măsura (măsurile) impusă (impuse) – prin publicarea acestora pe site-ul său web sau într-un cotidian național [articolul 66 din PIPA coroborat cu articolul 61 alineatul (1) din Decretul de punere în aplicare a PIPA] ([154]).

(126) În cele din urmă, respectarea cerințelor privind protecția datelor din PIPA (precum și a altor „legi privind protecția datelor") este susținută de un regim de sancțiuni penale. În acest sens, articolele 70-73 din PIPA conțin dispoziții privind sancțiunile care pot conduce fie la aplicarea unei amenzi (între 20 și 100 de milioane de woni), fie a unei pedepse cu închisoarea (pedeapsa maximă variind între 2 și 10 ani). Încălcările relevante includ, printre altele, utilizarea datelor cu caracter personal sau furnizarea unor astfel de date către o terță parte fără consimțământul necesar, prelucrarea de informații sensibile care contravin interdicției de la articolul 23 alineatul (1) din PIPA, nerespectarea cerințelor de siguranță aplicabile care au ca rezultat pierderea, furtul, divulgarea, falsificarea, modificarea sau deteriorarea datelor cu caracter personal, neluarea măsurilor necesare pentru corectarea, ștergerea sau suspendarea datelor cu caracter personal sau transferul ilegal de date cu caracter personal către o țară terță ([155]). În conformitate cu articolul 74 din PIPA, în fiecare dintre aceste cazuri, angajatul, agentul sau reprezentantul operatorului, precum și operatorul însuși sunt răspunzători ([156]).

(127) Pe lângă sancțiunile penale prevăzute în PIPA, utilizarea abuzivă a datelor cu caracter personal poate constitui, de asemenea, o infracțiune în temeiul Codului penal. Acest lucru este valabil în special în ceea ce privește încălcarea secretului corespondenței, documentelor sau înregistrărilor electronice (articolul 316), divulgarea informațiilor care fac obiectul secretului profesional (articolul 317), frauda comisă cu ajutorul calculatoarelor (articolul 347-2), precum și deturnarea de fonduri și abuzul de încredere (articolul 355).

(128) Prin urmare, sistemul coreean combină diferite tipuri de sancțiuni, de la măsuri de remediere și amenzi administrative până la sancțiuni penale, care pot avea un efect disuasiv deosebit de puternic asupra operatorilor și a persoanelor care prelucrează datele. Imediat după înființarea sa în 2020, PIPC a început să facă uz de competențele sale. Raportul anual pe 2021 al PIPC arată că PIPC a emis deja o serie de recomandări, amenzi administrative și ordine de remediere, atât împotriva sectorului public (aproximativ 34 de autorități publice), cât și

([152]) În plus, în cazul în care sistemele de prelucrare și protecție a informațiilor cu caracter personal operate de un operator au fost certificate ca fiind conforme cu PIPA, dar criteriile de certificare prevăzute la articolul 34-2 alineatul (1) din Decretul de punere în aplicare a PIPA nu au fost îndeplinite în fapt sau în cazul unei încălcări grave a unei „legi privind protecția informațiilor [cu caracter personal]", PIPC poate revoca certificarea [articolul 32-2 alineatele (3) și (5) din PIPA]. PIPC notifică operatorului o astfel de revocare și o anunță public sau o publică pe site-ul său web ori în Monitorul Oficial (articolul 34-4 din Decretul de punere în aplicare a PIPA). De asemenea, pentru încălcările CIA sunt prevăzute amenzi administrative (articolul 52 din CIA) și sancțiuni penale (articolul 50 din CIA).

([153]) În conformitate cu articolul 58 alineatul (2) din Decretul de punere în aplicare a PIPA, în cazul în care există circumstanțe speciale care fac „imposibilă" respectarea recomandărilor, operatorul trebuie să furnizeze PIPC o justificare motivată.

([154]) Atunci când decide dacă să publice astfel de informații, PIPC ține seama de fondul și gravitatea încălcării, de durata și frecvența acesteia, precum și de consecințele acesteia (amploarea prejudiciului). Entitatea în cauză trebuie să fie notificată în prealabil și să aibă posibilitatea de a se apăra. A se vedea articolul 61 alineatele (2) și (3) din Decretul de punere în aplicare a PIPA.

([155]) A se vedea articolul 71 punctul 2 coroborat cu articolul 18 alineatul (1) din PIPA [nerespectarea condițiilor prevăzute la articolul 17 alineatul (3) din PIPA, la care face trimitere articolul 18 alineatul (1)]. A se vedea, de asemenea, articolul 75 alineatul (2) punctul 1 coroborat cu articolul 17 alineatul (2) din PIPA [nefurnizarea informațiilor necesare către persoana în cauză în temeiul articolului 17 alineatul (2) din PIPA, la care face trimitere articolul 17 alineatul (3)].

([156]) În plus, articolul 74-2 din PIPA permite confiscarea oricăror sume de bani, bunuri sau alte profituri obținute ca urmare a încălcării sau, în cazul în care confiscarea este imposibilă, „colectarea" beneficiului obținut în mod ilegal.

împotriva operatorilor privați (aproximativ 140 de societăți) ([157]). Printre cazurile remarcabile se numără, de exemplu, impunerea unei amenzi de 6,7 miliarde de woni în decembrie 2020 unei societăți pentru încălcarea diferitelor dispoziții ale PIPA (inclusiv ale cerințelor privind securitatea, consimțământul pentru furnizarea către terți și transparența) ([158]) și o amendă de 103,3 milioane de woni în aprilie 2021, unei societăți din domeniul tehnologiei IA (pentru încălcarea, printre alte dispoziții, a normelor privind legalitatea prelucrării, în special privind consimțământul, și prelucrarea informațiilor pseudonimizate) ([159]). În august 2021, PIPC a finalizat o altă investigație asupra activităților a trei societăți, care a dus la măsuri de remediere și la impunerea unor amenzi de până la 6,47 miliarde de woni (printre altele, pentru că nu au informat persoanele fizice cu privire la divulgarea datelor cu caracter personal către terți, inclusiv transferurile către țări terțe) ([160]). De asemenea, deja înainte de recenta reformă, Coreea de Sud avea un istoric solid în ceea ce privește aplicarea legii, autoritățile responsabile făcând uz de întreaga gamă de acțiuni de asigurare a respectării legislației, inclusiv amenzi administrative, măsuri de remediere și acțiuni de tipul denunțării și partajării („naming and sharing") în legătură cu numeroși operatori, inclusiv cu furnizori de servicii de comunicații (Comisia pentru comunicații din Coreea), precum și cu operatori comerciali, instituții financiare, autorități publice, universități și spitale (Ministerul Internelor și al Siguranței) ([161]). Din aceste motive, Comisia concluzionează că sistemul coreean asigură aplicarea efectivă a normelor privind protecția datelor în practică, garantând astfel un nivel de protecție în esență echivalent cu cel prevăzut în Regulamentul (UE) 2016/679.

2.5 **Măsuri reparatorii**

(129) 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 daunele suferite.

(130) Sistemul coreean le oferă persoanelor fizice diverse mecanisme pentru a-și exercita în mod efectiv drepturile și pentru a obține reparații (judiciare).

(131) Într-o primă etapă, persoanele care consideră că le-au fost încălcate drepturile sau interesele în materie de protecție a datelor pot apela la operatorul relevant. În conformitate cu articolul 30 alineatul (1) punctul 5 din PIPA, politica de confidențialitate a operatorului include, printre altele, informații privind drepturile persoanelor vizate și modul de exercitare a acestora. În plus, acesta furnizează informații de contact – cum ar fi numele și numărul de telefon al responsabilului cu protecția vieții private sau al departamentului responsabil cu protecția datelor – pentru a permite depunerea plângerilor („reclamații"). În cadrul organizației operatorului, responsabilului cu protecția vieții private îi revine sarcina de a trata plângerile, de a adopta măsuri de remediere în caz de încălcare a dreptului la viață privată și de compensare a daunelor [articolul 31 alineatul (2) punctul 3 și alineatul (4) din PIPA]. Acestea din urmă sunt relevante, de exemplu, în cazul unei încălcări a securității datelor, întrucât operatorul trebuie să informeze persoana vizată cu privire la punctul (punctele) de contact pentru raportarea oricăror daune, printre altele [articolul 34 alineatul (1) punctul 5 din PIPA].

(132) În plus, PIPA le oferă persoanelor fizice mai multe căi de atac împotriva operatorilor. În primul rând, orice persoană care consideră că drepturile sau interesele sale în materie de protecție a datelor au fost încălcate de către operator poate raporta o astfel de încălcare direct la PIPC și/sau una dintre instituțiile specializate desemnate de PIPC să primească și să trateze plângerile; printre acestea se numără Agenția coreeană pentru internet și securitate, care, în acest scop, gestionează un centru de intermediere telefonică privind informațiile cu caracter personal (așa-numitul „centru de intermediere telefonică privind protecția vieții private") [articolul 62 alineatele (1) și (2) din PIPA coroborat cu articolul 59 din Decretul de punere în aplicare a PIPA]. Centrul de intermediere telefonică privind protecția vieții private investighează și stabilește încălcările, oferă consiliere în legătură cu prelucrarea

([157]) A se vedea raportul anual al PIPC pe 2021, p. 50-55 (disponibil doar în limba coreeană), la adresa https://www.pipc.go.kr/np/cop/bbs/selectBoardArticle.do?bbsId=BS074&mCode=C020010000&nttId=7511#LINK.

([158]) A se vedea la adresa (disponibil doar în limba coreeană) https://www.pipc.go.kr/np/cop/bbs/selectBoardArticle.do?bbsId=BS074&mCode=C020010000&nttId=6954#LINK.

([159]) A se vedea la adresa (disponibil doar în limba coreeană) https://www.pipc.go.kr/np/cop/bbs/selectBoardArticle.do?bbsId=BS074&mCode=C020010000&nttId=7298&fbclid=IwAR3SKcMQi6G5pR9k4I7j6GNXtc8aBVDOwcURevvvzQtYI7AS40UKYXoOXo8.

([160]) A se vedea la adresa (disponibil doar în limba coreeană): https://www.pipc.go.kr/np/cop/bbs/selectBoardArticle.do?bbsId=BS074&mCode=C020010000&nttId=7497#LINK.

([161]) A se vedea, de exemplu, raportul anual pe 2020 la adresa (disponibil numai în limba coreeană) https://www.pipc.go.kr/np/cop/bbs/selectBoardList.do?bbsId=BS079&mCode=D070020000 și exemplele prezentate în limba engleză la adresa https://www.privacy.go.kr/eng/enforcement_02.do.

datelor cu caracter personal [articolul 62 alineatul (3) din PIPA] și poate raporta încălcările către PIPC (dar nu poate lua el însuși măsuri de executare). Centrul de intermediere telefonică privind protecția vieții private primește un număr mare de plângeri/cereri (de exemplu, 177 457 în 2020, 159 255 în 2019 și 164 497 în 2018) ([162]). Potrivit informațiilor primite de la PIPC, PIPC însăși a primit aproximativ 1 000 de plângeri în perioada august 2020-august 2021. Ca răspuns la o plângere, PIPC poate emite o recomandare de îmbunătățiri, măsuri de remediere, o „acuzație" transmisă agenției de investigare competente (inclusiv unui procuror) sau recomandări de măsuri disciplinare (a se vedea articolele 61, 64 și 65 din PIPA). Deciziile PIPC (cum ar fi refuzul de a trata o plângere sau respingerea pe fond a unei plângeri) pot fi contestate în temeiul Legii privind contenciosul administrativ ([163]).

(133) În al doilea rând, în conformitate cu articolele 40-50 din PIPA coroborate cu articolele 48-14 - 57 din Decretul de punere în aplicare a PIPA, persoanele vizate pot introduce acțiuni în fața unui așa-numit „comitet de mediere a litigiilor", care este format din reprezentanți numiți de președintele PIPC din rândul membrilor serviciului executiv superior al PIPC și din persoane numite pe baza experienței lor în domeniul protecției datelor din rândul anumitor grupuri eligibile [a se vedea articolul 40 alineatele (2), (3) și (7) din PIPA, articolul 48-14 din Decretul de punere în aplicare a PIPA] ([164]). Posibilitatea de a recurge la mediere în fața Comitetului de mediere a litigiilor oferă o cale alternativă pentru a obține despăgubiri, dar nu limitează dreptul unei persoane de a apela în schimb la PIPC sau la instanțe. Pentru a examina cazul, Comitetul poate solicita părților la litigiu să furnizeze materialele necesare și/sau să invite martorii relevanți să se prezinte în fața sa (articolul 45 din PIPA). După clarificarea chestiunii, Comitetul pregătește un proiect de decizie privind medierea ([165]), asupra căruia trebuie să fie de acord majoritatea membrilor săi. Proiectul de decizie privind medierea poate include suspendarea încălcării, căile de atac necesare (inclusiv restituirea sau despăgubirea), precum și orice măsuri necesare pentru a preveni repetarea aceleiași (aceloraași) încălcări sau a unei (unor) încălcări similare [articolul 47 alineatul (1) din PIPA]. În cazul în care ambele părți convin asupra deciziei de mediere, aceasta va avea același efect ca o soluționare judecătorească [articolul 47 alineatul (5) din PIPA]. Niciuna dintre părți nu este împiedicată să inițieze o acțiune în justiție în timp ce medierea este în curs, caz în care aceasta din urmă va fi suspendată [a se vedea articolul 48 alineatul (2) din PIPA] ([166]). Cifrele anuale emise de PIPC arată că persoanele fizice recurg în mod regulat la procedura în fața Comitetului de mediere a litigiilor, ceea ce duce adesea la un rezultat pozitiv. De exemplu, în 2020, Comitetul a tratat 126 de cazuri, dintre care 89 au fost soluționate în fața Comitetului (77 de cazuri în care părțile ajunseseră deja la un acord înainte de încheierea procesului de mediere și 12 cazuri în care părțile au acceptat propunerea de mediere), ceea ce a condus la o rată de mediere de 70,6 % ([167]). În mod similar, în 2019, Comitetul a tratat 139 de cazuri, dintre care 92 au fost soluționate, ceea ce a condus la o rată de mediere de 62,2 %.

(134) Mai mult, în cazul în care există cel puțin 50 de persoane care suferă prejudicii sau ale căror drepturi în materie de protecție a datelor au fost încălcate în același mod sau în mod similar ca urmare a aceluiași (tip de) incident ([168]), o persoană vizată sau o organizație de protecție a datelor poate solicita medierea colectivă a litigiilor în numele unei astfel de colectivități; alte persoane vizate pot solicita să participe la o astfel de mediere, care va fi anunțată public de către Comitetul de mediere a litigiilor [articolul 49 alineatele (1)-(3) din PIPA coroborat cu articolele 52-54 din Decretul de punere în aplicare a PIPA] ([169]). Comitetul de mediere a litigiilor poate selecta cel puțin o persoană care reprezintă în modul cel mai adecvat interesul comun în calitate de parte reprezentativă

([162]) A se vedea raportul anual al PIPC din 2021, p. 174. În 2020, astfel de plângeri au vizat, de exemplu, colectarea datelor fără consimțământ, nerespectarea obligațiilor de transparență, încălcări ale PIPA de către persoanele împuternicite de operatori, măsuri de securitate insuficiente, lipsa unui răspuns la solicitările persoanelor vizate, precum și întrebările generale.

([163]) În special, persoanele fizice pot contesta exercitarea sau refuzul de a exercita prerogative de autoritate publică de către o agenție administrativă [articolul 2 alineatul (1) punctul 1, articolul 3 punctul 1 din Legea privind contenciosul administrativ]. Informații mai detaliate privind aspectele procedurale, inclusiv cerințele de admisibilitate, sunt disponibile în considerentul 181.

([164]) Toți membrii au un mandat fix și pot fi revocați doar dintr-un motiv întemeiat [a se vedea articolul 40 alineatul (5) și articolul 41 din PIPA]. În plus, articolul 42 din PIPA conține garanții pentru protecția împotriva conflictelor de interese.

([165]) A se vedea articolul 44 din PIPA. În plus, poate propune un proiect de soluționare și poate recomanda soluționarea fără mediere (a se vedea articolul 46 din PIPA).

([166]) În plus, Comitetul poate respinge medierea în cazul în care consideră că este inadecvat să medieze litigiul având în vedere natura acestuia sau pentru că cererea de mediere a fost depusă în scopuri abuzive (articolul 48 din PIPA).

([167]) A se vedea raportul anual al PIPC din 2021, p. 179-180. Aceste cazuri au vizat, printre altele, încălcări ale cerinței de a obține consimțământul pentru colectarea datelor, principiul limitării scopului și drepturile persoanelor vizate.

([168]) A se vedea articolul 49 alineatul (1) din PIPA, conform căruia persoanele vizate trebuie să sufere un prejudiciu sau o încălcare a drepturilor lor „în mod identic sau similar" și articolul 52 punctul 2 din Decretul de punere în aplicare a PIPA care introduce cerința ca „aspectele grave ale incidentului să fie comune în fapt sau din punct de vedere juridic".

([169]) În plus, chiar și entitățile care nu sunt părți pot beneficia de pe urma unei decizii de mediere colective a litigiilor acceptate de operator, în sensul în care Comitetul de mediere a litigiilor poate recomanda operatorului să elaboreze și să prezinte un plan de despăgubire care să le vizeze (și) pe acestea [articolul 49 alineatul (5) din PIPA].

[articolul 49 alineatul (4) din PIPA]. În cazul în care operatorul respinge medierea colectivă a litigiilor sau nu acceptă decizia de mediere, anumite organizații ([170]) pot introduce o acțiune colectivă în justiție pentru a remedia încălcarea (articolele 51-57 din PIPA).

(135) În al treilea rând, în cazul unei încălcări a vieții private care aduce „prejudicii" persoanei în cauză, persoana vizată are dreptul la o cale de atac adecvată în cadrul unei „proceduri prompte și echitabile" (articolul 4 punctul 5 coroborat cu articolul 39 din PIPA) ([171]). Operatorul se poate dezincrimina dacă dovedește absența culpei (a „intenției frauduloase" sau a neglijenței). În cazul în care persoana vizată suferă prejudicii ca urmare a pierderii, furtului, divulgării, falsificării, modificării sau deteriorării datelor sale cu caracter personal, Curtea poate stabili o despăgubire de până la trei ori mai mare decât prejudiciul real, luând în considerare o serie de factori [articolul 39 alineatele (3) și (4) din PIPA]. În mod alternativ, persoana vizată poate solicita o „sumă rezonabilă" drept despăgubire, care să nu depășească 3 milioane de woni [articolul 39-2 alineatele (1) și (2) din PIPA]. În plus, în conformitate cu Codul civil, despăgubirea poate fi solicitată de la orice persoană „care cauzează pierderi sau provoacă vătămări unei alte persoane printr-o faptă ilicită, intenționată sau din neglijență" ([172]) sau de la o persoană „care a adus prejudicii persoanei, libertății sau reputației unei alte persoane sau care a cauzat suferințe psihice unei alte persoane" ([173]). O astfel de răspundere delictuală ca urmare a încălcării normelor de protecție a datelor a fost confirmată de Curtea Supremă ([174]). În cazul în care daunele au fost cauzate de o acțiune ilegală a unei autorități publice, se poate depune o cerere de despăgubire, de asemenea, în temeiul Legii privind despăgubirile acordate de stat ([175]). O cerere în temeiul Legii privind despăgubirile acordate de stat poate fi depusă la un „Consiliu pentru despăgubiri" specializat sau direct la instanțele coreene ([176]). Răspunderea statului acoperă, de asemenea, prejudiciile morale (cum ar fi suferința psihică) ([177]). În cazul în care victima este cetățean străin, Legea privind despăgubirile acordate de stat se aplică atât timp cât țara sa de origine asigură, de asemenea, despăgubiri din partea statului pentru cetățenii coreeni ([178]).

(136) În al patrulea rând, Curtea Supremă a recunoscut că persoanele fizice au dreptul de a solicita o ordonanță prezidențială pentru încălcarea drepturilor lor prevăzute de Constituție, inclusiv dreptul la protecția datelor cu caracter personal ([179]). În acest context, o instanță poate, de exemplu, să oblige operatorii să suspende sau să înceteze orice activitate ilegală. În plus, drepturile în materie de protecție a datelor, inclusiv drepturile protejate de PIPA, pot fi puse în aplicare prin acțiuni civile. Această aplicare orizontală a protecției constituționale a vieții private în relațiile dintre părți private a fost recunoscută de Curtea Supremă ([180]).

([170]) Și anume, grupuri de consumatori sau ONG-uri non-profit de o anumită dimensiune în ceea ce privește numărul membrilor, al căror scop declarat este protecția datelor [deși în cazul acestora din urmă, cu cerința suplimentară ca minimum 100 de persoane vizate care s-au confruntat cu aceeași încălcare (sau același de tip de încălcare) să fi depus o cerere de introducere a unei acțiuni colective]. A se vedea articolul 51 din PIPA.

([171]) Articolele 43 - 43-3 din CIA prevăd, de asemenea, răspunderea pentru compensarea prejudiciilor rezultate din încălcarea acestei legi.

([172]) Articolul 750 din Codul civil.

([173]) Articolul 751 alineatul (1) din Codul civil.

([174]) A se vedea, de exemplu, hotărârea Curții Supreme 2015Da251539, 251546, 251553, 251560, 251577 din 30 mai 2018. În plus, Curtea Supremă a confirmat că încălcarea securității datelor poate conduce la acordarea de despăgubiri în temeiul Codului civil; a se vedea hotărârea Curții Supreme 2011Da59834, 59858, 59841 din 26 decembrie 2012 (rezumat în limba engleză disponibil la adresa http://library.scourt.go.kr/SCLIB_data/decision/9-69%202012.12.26.2011Da59834.htm). În acest caz, Curtea Supremă a clarificat faptul că, pentru a evalua dacă o persoană s-a confruntat cu o suferință emoțională calificată drept prejudiciu reparabil, ar trebui luați în considerare mai mulți factori, cum ar fi tipul și caracteristicile informațiilor scurse, măsura în care persoana respectivă poate fi identificată ca urmare a încălcării, posibilitatea de acces la date de către terți, măsura în care informațiile cu caracter personal au fost difuzate, dacă acest lucru a condus la încălcări suplimentare ale drepturilor individuale, modul în care informațiile cu caracter personal au fost gestionate și protejate etc.

([175]) În baza Legii privind despăgubirile acordate de stat, persoanele fizice pot solicita despăgubiri pentru prejudiciile cauzate de funcționarii publici în exercitarea atribuțiilor lor oficiale cu încălcarea legii [articolul 2 alineatul (1) din lege].

([176]) Articolele 9 și 12 din Legea privind despăgubirile acordate de stat. Legea instituie consilii districtuale (prezidate de procurorul adjunct al parchetului corespunzător), un consiliu central (prezidat de ministrul adjunct al justiției) și un consiliu special (însărcinat cu cererile de despăgubire pentru prejudiciile cauzate de personalul militar sau de angajații civili ai armatei, prezidat de ministrul adjunct al apărării naționale). Cererile de despăgubire sunt tratate, în principiu, de consiliile districtuale, care, în anumite circumstanțe, trebuie să înainteze cazurile consiliului central/special, de exemplu, atunci când despăgubirea depășește o anumită sumă sau când o persoană solicită o nouă deliberare. Toate consiliile sunt formate din membri numiți de ministrul justiției (de exemplu, din rândul funcționarilor publici din cadrul Ministerului Justiției, al executorilor judecătorești, al avocaților și al persoanelor cu expertiză în materie de despăgubiri acordate de stat) și fac obiectul unor norme specifice privind conflictul de interese (a se vedea articolul 7 din Decretul de punere în aplicare a Legii privind despăgubirile acordate de stat).

([177]) A se vedea articolul 8 din Legea privind despăgubirile acordate de stat (care face trimitere la Codul civil), precum și articolul 751 din Codul civil.

([178]) Articolul 7 din Legea privind despăgubirile acordate de stat.

([179]) Hotărârea Curții Supreme 93Da40614 din 12 aprilie 1996 și Hotărârea 2008Da42430 din 2 septembrie 2011 (rezumat în limba engleză disponibil la adresa https://www.scourt.go.kr/eng/supreme/decisions/NewDecisionsView.work?seq=696&pageIndex=1&mode=6&searchWord=).

([180]) A se vedea, de exemplu, Hotărârea Curții Supreme 2008Da42430 din 2 septembrie 2011 (rezumat în limba engleză disponibil la adresa https://www.scourt.go.kr/eng/supreme/decisions/NewDecisionsView.work?seq=696&pageIndex=1&mode=6&searchWord=).

(137) În cele din urmă, persoanele fizice pot depune o plângere penală în temeiul Codului de procedură penală (articolul 223) la un procuror sau la un agent al poliției judiciare ([181]).

(138) Prin urmare, sistemul coreean oferă diverse căi de a obține despăgubiri, de la opțiuni ușor accesibile, cu costuri reduse [de exemplu, contactând Centrul de intermediere telefonică privind protecția vieții private sau prin mediere (colectivă)] până la căi administrative (în fața PIPC) și căi judiciare, inclusiv cu posibilitatea de a obține despăgubiri pentru daune.

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

(139) Comisia a evaluat, de asemenea, limitările și garanțiile, inclusiv supravegherea și mecanismele de reparație individuală, care sunt prevăzute în legislația coreeană în ceea ce privește colectarea și utilizarea ulterioară a datelor cu caracter personal transferate operatorilor economici din Coreea de către autoritățile publice coreene 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 coreean 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.

(140) Pentru a evalua dacă condițiile în care accesul administrației publice la datele transferate către Coreea în temeiul prezentei decizii îndeplinesc criteriul „echivalenței substanțiale" în temeiul articolului 45 alineatul (1) din Regulamentul (UE) 2016/679, astfel cum a fost interpretat de Curtea de Justiție a Uniunii Europene în lumina Cartei drepturilor fundamentale, Comisia a luat în considerare în special următoarele criterii.

(141) În primul rând, orice restrângere a dreptului la protecția datelor cu caracter personal trebuie să fie prevăzută de lege, iar temeiul juridic care permite ingerința în acest drept trebuie să definească el însuși întinderea restrângerii exercitării dreptului vizat ([182]).

(142) În al doilea rând, pentru a îndeplini cerința proporționalității potrivit căreia derogările de la protecția datelor cu caracter personal și restrângerile acesteia trebuie să fie efectuate în limitele strictului necesar într-o societate democratică pentru a îndeplini obiective specifice de interes general echivalente cu cele recunoscute de Uniune, legislația țării terțe în cauză care permite o ingerință trebuie să prevadă norme clare și precise care să reglementeze conținutul și aplicarea măsurilor respective și să impună o serie de cerințe minime, astfel încât persoanele ale căror date au fost transferate să dispună de garanții suficiente care să permită protejarea în mod eficient a datelor lor cu caracter personal împotriva riscurilor de abuz ([183]). Legislația trebuie în special să indice în ce împrejurări și în ce condiții poate fi luată o măsură care prevede prelucrarea unor asemenea date ([184]), precum și să supună îndeplinirea acestor cerințe unei supravegheri independente ([185]).

(143) În al treilea rând, legislația respectivă și cerințele sale trebuie să fie obligatorii din punct de vedere juridic în temeiul dreptului intern. Acest lucru se referă în primul rând la autoritățile din țara terță în cauză, dar aceste cerințe legale trebuie să aibă, de asemenea, caracter executoriu în fața instanțelor judecătorești ([186]). În special, persoanele vizate trebuie să dispună de posibilitatea de a exercita căi legale în fața unui tribunal independent și imparțial pentru a avea acces la date cu caracter personal care le privesc sau de a obține rectificarea sau ștergerea unor astfel de date ([187]).

3.1 **Cadrul juridic general**

(144) Limitările și garanțiile care se aplică colectării și utilizării ulterioare a datelor cu caracter personal de către autoritățile publice coreene decurg din cadrul constituțional general, din legile specifice care reglementează activitățile acestora în domeniul asigurării respectării dreptului penal și al securității naționale, precum și din normele care se aplică în mod specific prelucrării datelor cu caracter personal.

([181]) Astfel cum se explică în considerentul 127, utilizarea abuzivă a datelor poate constitui o infracțiune în temeiul Codului penal.
([182]) A se vedea Schrems II, punctele 174-175 și jurisprudența citată. A se vedea, de asemenea, în ceea ce privește accesul autorităților publice ale statelor membre, cauza C-623/17, Privacy International, ECLI:EU:C:2020:790, punctul 65; și cauzele conexate C-511/18, C-512/18 și C-520/18, La Quadrature du Net și alții, ECLI:EU:C:2020:791, punctul 175.
([183]) A se vedea Schrems II, punctele 176 și 181, precum și jurisprudența citată. A se vedea, de asemenea, în ceea ce privește accesul autorităților publice ale statelor membre, Privacy International, punctul 68; și La Quadrature du Net și alții, punctul 132.
([184]) A se vedea Schrems II, punctul 176. A se vedea, de asemenea, în ceea ce privește accesul autorităților publice ale statelor membre, Privacy International, punctul 68; și La Quadrature du Net și alții, punctul 132.
([185]) A se vedea Schrems II, punctul 179.
([186]) A se vedea Schrems II, punctele 181-182.
([187]) A se vedea Schrems I, punctul 95 și Schrems II, punctul 194. În acest sens, CJUE a subliniat în special faptul că respectarea articolului 47 din Carta drepturilor fundamentale, care garantează dreptul la o cale de atac eficientă în fața unei instanțe judecătorești independente și imparțiale, „participă de asemenea la nivelul de protecție impus în cadrul Uniunii [și] trebuie să fie constatată de Comisie înainte ca aceasta să adopte o decizie privind caracterul adecvat al nivelului de protecție în temeiul articolului 45 alineatul (1) din Regulamentul (UE) 2016/679" (Schrems II, punctul 186).

(145) În primul rând, accesul autorităților publice coreene la datele cu caracter personal este reglementat de principiile generale ale legalității, necesității și proporționalității care decurg din Constituția coreeană ([188]). În special, drepturile și libertățile fundamentale (inclusiv dreptul la viață privată și dreptul la confidențialitatea corespondenței) ([189]) pot fi restricționate numai prin lege și atunci când acest lucru este necesar pentru securitatea națională sau menținerea legii și ordinii pentru bunăstarea publică. Astfel de restricții nu pot afecta substanța dreptului sau a libertății în cauză. În special în ceea ce privește perchezițiile și punerile sub sechestru, Constituția prevede că acestea pot avea loc numai în condițiile prevăzute de lege, în baza unui mandat emis de un judecător și cu respectarea unui proces echitabil ([190]). În cele din urmă, persoanele fizice își pot invoca drepturile și libertățile în fața Curții Constituționale în cazul în care consideră că acestea au fost încălcate de autoritățile publice în exercitarea competențelor lor ([191]). În mod similar, persoanele fizice care au suferit daune ca urmare a unei nelegalități săvârșite de un funcționar public în exercitarea atribuțiilor sale au dreptul de a solicita despăgubiri ([192]).

(146) În al doilea rând, astfel cum se descrie mai detaliat în secțiunile 3.2.1 și 3.3.1, principiile generale menționate în considerentul 145 sunt reflectate, de asemenea, în legislația specifică ce reglementează competențele autorităților de aplicare a legii și ale autorităților naționale de securitate. De exemplu, în ceea ce privește anchetele penale, Codul de procedură penală (CPA) prevede că pot fi luate măsuri obligatorii numai în cazul în care acest lucru este prevăzut în mod explicit în CPA și în cea mai mică măsură necesară pentru atingerea scopului anchetei ([193]). În mod similar, articolul 3 din Legea privind protecția confidențialității comunicațiilor (CPPA) interzice accesul la comunicațiile private, cu excepția cazului în care acesta se întemeiază pe lege și intră sub rezerva limitărilor și a garanțiilor prevăzute de lege. În domeniul securității naționale, Legea privind Serviciul Național de Informații (Legea privind NIS) prevede că orice acces la comunicații sau informații de localizare trebuie să respecte legea și supune sancțiunilor penale abuzul de putere și încălcările legii ([194]).

(147) În al treilea rând, prelucrarea datelor cu caracter personal de către autoritățile publice, inclusiv în scopul aplicării legii și al securității naționale, face obiectul normelor privind protecția datelor în temeiul PIPA ([195]). Ca principiu general, articolul 5 alineatul (1) din PIPA prevede obligația autorităților publice de a elabora politici pentru a preveni „abuzul și utilizarea necorespunzătoare a informațiilor cu caracter personal, supravegherea și urmărirea indiscretă etc., precum și pentru a îmbunătăți gradul de respectare a demnității ființelor umane și a vieții private". În plus, orice operator trebuie să prelucreze datele cu caracter personal într-un mod care să reducă la minimum posibilitatea de a se încălca viața privată a persoanei vizate [articolul 3 alineatul (6) din PIPA].

(148) Toate cerințele prevăzute în PIPA, astfel cum sunt descrise în detaliu în secțiunea 2, se aplică prelucrării datelor cu caracter personal în scopul aplicării legii. Aceasta include principiile de bază (precum legalitatea și echitatea, limitarea scopului, exactitatea, reducerea la minimum a datelor, limitarea stocării, securitatea și transparența), obligații (de exemplu, în ceea ce privește notificarea încălcării securității datelor și datele sensibile) și drepturi (de a obține accesul, la rectificare, ștergere și suspendare).

(149) Deși prelucrarea datelor cu caracter personal în scopuri legate de securitatea națională face obiectul unui set mai limitat de dispoziții din PIPA, se aplică principiile de bază, precum și normele privind supravegherea, asigurarea respectării legii și căile de atac ([196]). Mai precis, articolele 3 și 4 din PIPA stabilesc principiile generale de protecție a datelor (principiile legalității și echității, limitării scopului, exactității, reducerii la minimum a datelor, securității și transparenței) și drepturile individuale (dreptul de a fi informat, dreptul de acces și dreptul la rectificare, ștergere și suspendare) ([197]). În plus, articolul 4 alineatul (5) din PIPA le oferă persoanelor fizice dreptul la despăgubiri adecvate pentru orice prejudiciu care rezultă din prelucrarea datelor lor cu caracter personal în cadrul unei proceduri prompte și echitabile. Acesta este completat de obligații mai specifice de prelucrare a datelor cu

([188]) A se vedea anexa II secțiunea 1.1.

([189]) Articolul 37 alineatul (2) din Constituție.

([190]) Articolul 16 și articolul 12 alineatul (3) din Constituție. Articolul 12 alineatul (3) din Constituție stabilește, de asemenea, circumstanțele excepționale în care pot avea loc percheziții sau puneri sub sechestru fără mandat (deși este necesar în continuare un mandat *ex post*), și anume în cazul unui flagrant delict sau, pentru infracțiuni care fac obiectul unei pedepse privative de libertate de cel puțin trei ani, dacă există riscul ca probele să fie distruse sau ca suspectul să dispară.

([191]) Articolul 68 alineatul (1) din Legea privind Curtea Constituțională.

([192]) Articolul 29 alineatul (1) din Constituție.

([193]) Articolul 199 alineatul (1) din CPA. La un nivel mai general, atunci când își exercită competențele în temeiul CPA, autoritățile publice trebuie să respecte drepturile fundamentale ale persoanelor suspectate de săvârșirea de infracțiuni și ale oricărei alte persoane vizate [articolul 198 alineatul (2) din CPA].

([194]) Articolul 14 din Legea privind NIS.

([195]) A se vedea anexa II secțiunea 1.2.

([196]) Articolul 58 alineatul (1) punctul 2 din PIPA. A se vedea, de asemenea, secțiunea 6 din Notificarea nr. 2021-5 (anexa I). Această exceptare de la anumite dispoziții ale PIPA se aplică numai atunci când datele cu caracter personal sunt prelucrate „în scopuri legate de securitatea națională". Odată ce situația de securitate națională care justifică prelucrarea datelor a încetat, exceptarea nu mai poate fi invocată, aplicându-se toate cerințele PIPA.

([197]) Astfel de drepturi pot fi restricționate numai în cazul în care acest lucru este prevăzut de lege, în măsura în care acest lucru este necesar și proporțional pentru a proteja un obiectiv important de interes public, sau în cazul în care acordarea dreptului poate aduce prejudicii vieții sau integrității fizice a unui terț sau încălcări nejustificate ale drepturilor de proprietate și ale altor interese ale unui terț. A se vedea secțiunea 6 din Notificarea nr. 2021-5.

caracter personal numai în măsura minimă necesară pentru atingerea scopului preconizat și pentru perioada minimă, de a institui măsurile necesare pentru a asigura gestionarea în condiții de siguranță a datelor și prelucrarea corespunzătoare (cum ar fi garanții tehnice, de gestionare și fizice), precum și de a institui măsuri pentru tratarea corespunzătoare a reclamațiilor individuale (plângeri) ([198]). În cele din urmă, principiile generale ale legalității, necesității și proporționalității prevăzute în Constituția Coreei (a se vedea considerentul 145) se aplică, de asemenea, prelucrării datelor cu caracter personal în scopuri legate de securitatea națională.

(150) Aceste limitări și garanții generale pot fi invocate de persoanele fizice în fața organismelor independente de supraveghere (de exemplu, PIPC și/sau Comisia națională pentru drepturile omului; a se vedea considerentele 177-178) și în fața instanțelor (a se vedea considerentele 179-183) pentru a obține despăgubiri.

3.2 **Accesul și utilizarea de către autoritățile publice coreene în scopuri de asigurare a respectării dreptului penal**

(151) Legislația Republicii Coreea impune o serie de limitări privind accesul la datele cu caracter personal și utilizarea acestora în scopul asigurării respectării dreptului penal și prevede mecanisme de supraveghere și de exercitare a unei căi de atac care sunt în concordanță cu cerințele menționate în considerentele 141-143 din prezenta decizie. Condițiile în care poate avea loc un astfel de acces și garanțiile aplicabile utilizării acestor competențe sunt evaluate în detaliu în secțiunile următoare.

3.2.1 *Temeiuri juridice, limitări și garanții*

(152) Datele cu caracter personal prelucrate de operatori coreeni care ar fi transferate din Uniune în temeiul prezentei decizii ([199]) pot fi colectate de autoritățile coreene în scopul asigurării respectării dreptului penal în contextul unei percheziții sau al unei puneri sub sechestru (pe baza CPA), prin accesarea informațiilor privind comunicațiile (pe baza CPPA) sau prin obținerea de date privind abonații prin intermediul unor cereri de divulgare voluntară (în temeiul Legii privind activitățile de telecomunicații, TBA) ([200]).

3.2.1.1 Percheziții și punerile sub sechestru

(153) CPA prevede că o percheziție sau o punere sub sechestru poate avea loc numai în cazul în care o persoană este suspectată de săvârșirea unei infracțiuni, când este necesară pentru investigație și când se stabilește o legătură între investigație și persoana care trebuie percheziționată sau obiectul care trebuie să fie inspectat sau sechestrat ([201]). În plus, o percheziție sau o punere sub sechestru (ca orice măsură obligatorie) poate fi autorizată/efectuată numai în cea mai mică măsură necesară ([202]). În cazul în care o percheziție vizează un CD sau alt suport de stocare a datelor, în principiu, vor fi confiscate numai datele necesare (prin copiere sau imprimare), mai degrabă decât întregul suport ([203]). Acesta din urmă poate fi confiscat numai atunci când se consideră că este aproape imposibil să se imprime sau să se copieze datele solicitate separat sau atunci când se consideră că este practic imposibil să se îndeplinească scopul percheziției ([204]). Prin urmare, CPA stabilește norme clare și precise privind domeniul de aplicare și aplicarea acestor măsuri, garantând astfel că interferența cu drepturile persoanelor fizice în cazul unei percheziții sau al unei puneri sub sechestru se va limita la ceea ce este necesar pentru o anchetă penală specifică și va fi proporțională cu scopul urmărit.

([198]) Articolul 58 alineatul (4) din PIPA.

([199]) A se vedea anexa II secțiunea 2.1. Expunerea oficială a guvernului coreean (secțiunea 2.1 din anexa II) se referă și la posibilitatea de a colecta informații privind tranzacțiile financiare în scopul prevenirii spălării banilor și a finanțării terorismului în temeiul Legii privind raportarea și utilizarea informațiilor specifice referitoare la tranzacțiile financiare (ARUSFTI). Cu toate acestea, ARUSFTI prevede obligații de divulgare numai pentru operatorii care prelucrează informații cu caracter personal privind creditele în temeiul CIA și care fac obiectul supravegherii FSC (a se vedea considerentul 13). Întrucât prelucrarea informațiilor cu caracter personal privind creditele de către acești operatori este exclusă din domeniul de aplicare al prezentei decizii, ARUSFTI nu este relevantă pentru prezenta evaluare.

([200]) Articolul 3 din CPPA menționează, de asemenea, Legea privind instanțele militare ca posibil temei juridic pentru colectarea datelor privind comunicațiile. Cu toate acestea, legea respectivă reglementează colectarea de informații privind personalul militar și se poate aplica civililor numai într-un număr limitat de cazuri (de exemplu, în cazul comiterii de infracțiuni de către personalul militar împreună cu civili sau în cazul unei infracțiuni îndreptate împotriva armatei comise de o persoană, pot fi inițiate proceduri în fața unei instanțe militare; a se vedea articolul 2 din Legea privind instanțele militare). În orice caz, această lege cuprinde dispoziții generale care reglementează perchezițiile și punerile sub sechestru care sunt similare celor prevăzute în CPA (a se vedea, de exemplu, articolele 146-149 și 153-156 din Legea privind instanțele militare) și, de exemplu, prevede posibilitatea de a colecta date poștale numai atunci când acestea sunt necesare pentru o investigație și în baza unui mandat emis de instanța militară. În măsura în care comunicațiile electronice ar fi colectate în temeiul acestei legi, s-ar aplica limitările și garanțiile prevăzute în CPPA. A se vedea anexa II secțiunea 2.2.2 și nota de subsol 50.

([201]) Articolul 215 alineatele (1) și (2) din CPA. A se vedea, de asemenea, articolul 106 alineatul (1), articolul 107 și articolul 109 din CPA, care prevăd că instanțele pot efectua percheziții și puneri sub sechestru atât timp cât se consideră că articolele sau persoanele în cauză au legătură cu un caz specific. A se vedea anexa II secțiunea 2.2.1.2.

([202]) Articolul 199 alineatul (1) din CPA.

([203]) Articolul 106 alineatul (3) din CPA.

([204]) Articolul 106 alineatul (3) din CPA.

(154) În ceea ce privește garanțiile procedurale, CPA prevede obligația de a se obține un mandat din partea unei instanțe pentru efectuarea unei percheziții sau a unei puneri sub sechestru ([205]). O percheziție sau o punere sub sechestru fără mandat este permisă numai în mod excepțional, și anume în situații de urgență ([206]), *in loco* în momentul arestării sau al reținerii unei persoane suspectate de săvârșirea de infracțiuni ([207]) sau în cazul în care un articol este înlăturat sau prezentat în mod voluntar de către o persoană suspectată de săvârșirea de infracțiuni sau de un terț (în ceea ce privește datele cu caracter personal, chiar de către persoana în cauză) ([208]). Perchezițiile și punerile sub sechestru ilegale fac obiectul unor sancțiuni penale ([209]), iar orice probă obținută cu încălcarea CPA este considerată inadmisibilă ([210]). În cele din urmă, persoanele în cauză trebuie să fie întotdeauna informate cu privire la o percheziție sau o punere sub sechestru (inclusiv o punere sub sechestru a datelor lor) fără întârziere ([211]), ceea ce, la rândul său, va facilita exercitarea drepturilor materiale ale persoanei respective și dreptul la reparații (a se vedea în special posibilitatea de a contesta executarea unui mandat de punere sub sechestru; a se vedea considerentul 180).

3.2.1.2 Accesul la informațiile privind comunicațiile

(155) În temeiul CPPA, autoritățile coreene de asigurare a respectării dreptului penal pot lua două tipuri de măsuri ([212]): pe de o parte, colectarea de „date de confirmare privind comunicațiile" ([213]), care includ data telecomunicațiilor, ora de începere și de încheiere, numărul de apeluri inițiate și primite, precum și numărul de abonat al celeilalte părți, frecvența utilizării, fișierele-jurnal privind utilizarea serviciilor de telecomunicații și informațiile de localizare (de exemplu, de la turnurile de transmisie unde se primesc semnalele); și, pe de altă parte, „măsurile de restricționare a comunicațiilor", care acoperă atât colectarea conținutului corespondenței tradiționale, cât și interceptarea directă a conținutului telecomunicațiilor ([214]).

(156) Datele de confirmare a comunicațiilor pot fi accesate numai atunci când acest lucru este necesar pentru desfășurarea unei anchete penale sau pentru executarea unei pedepse ([215]), pe baza unui mandat emis de o instanță ([216]). În acest sens, CPPA prevede furnizarea de informații detaliate atât în cererea de emitere a mandatului (de exemplu, cu privire la motivele cererii, relația cu ținta/abonatul și datele necesare), cât și în cadrul mandatului propriu-zis (de exemplu, cu privire la obiectivul, ținta și domeniul de aplicare al măsurii) ([217]). Colectarea fără mandat poate avea loc numai

([205]) Articolul 215 alineatele (1) și (2) din CPA, articolul 113 din CPA. Atunci când solicită un mandat, autoritatea în cauză trebuie să prezinte materiale care să demonstreze motivele pentru care o persoană este suspectată de comiterea unei infracțiuni, necesitatea efectuării unei percheziții, inspecții sau puneri sub sechestru și existența articolelor relevante care urmează să fie puse sub sechestru [articolul 108 alineatul (1) din Regulamentul de procedură penală]. Mandatul în sine trebuie să indice, printre altele, numele persoanei suspectate de săvârșirea de infracțiuni și infracțiunea; locul, persoana sau articolele care urmează să fie percheziționate sau articolele care urmează să fie puse sub sechestru; data emiterii; și perioada efectivă de aplicare [articolul 114 alineatul (1) coroborat cu articolul 219 din CPA]. A se vedea anexa II secțiunea 2.2.1.2.

([206]) Și anume, atunci când este imposibil să se obțină un mandat din cauza urgenței la locul comiterii unei infracțiuni [articolul 216 alineatul (3) din CPA], caz în care se menține obligativitatea obținerii mandatului, ulterior, fără întârziere [articolul 216 alineatul (3) din CPA].

([207]) Articolul 216 alineatele (1) și (2) din CPA.

([208]) Articolul 218 din CPA. În plus, astfel cum se explică în secțiunea 2.2.1.2 din anexa II, articolele prezentate în mod voluntar sunt admise ca probe în cadrul procedurilor judiciare numai dacă nu există nicio îndoială rezonabilă cu privire la caracterul voluntar al divulgării, aspect care trebuie demonstrat de procuror.

([209]) Articolul 321 din Codul penal.

([210]) Articolul 308-2 din CPA. În plus, o persoană (și avocatul acesteia) poate fi prezentă în momentul executării unui mandat de percheziție sau de punere sub sechestru și, prin urmare, poate ridica obiecții și în momentul executării mandatului (articolele 121 și 219 din CPA).

([211]) Articolele 121 și 122 din CPA (în ceea ce privește perchezițiile) și articolul 219 coroborat cu articolul 106 alineatul (4) din CPA (în ceea ce privește punerile sub sechestru).

([212]) A se vedea, de asemenea, anexa II secțiunea 2.2.2.1. Astfel de măsuri pot fi luate cu ajutorul obligatoriu al operatorilor de telecomunicații, după ce se acordă acestor operatori o autorizare scrisă obținută de la o instanță [articolul 9 alineatul (2) din CPPA], care trebuie păstrată de operatori (articolul 15-2 din CPPA și articolul 12 din Decretul de punere în aplicare a CPPA). Furnizorii de servicii de telecomunicații pot refuza cooperarea atunci când informațiile privind persoana vizată, astfel cum sunt indicate în autorizarea scrisă a instanței (de exemplu, numărul de telefon al persoanei), sunt incorecte și au interdicția, în orice circumstanțe, de a divulga parolele utilizate pentru telecomunicații [articolul 9 alineatul (4) din CPPA].

([213]) Articolul 2 alineatul (11) din CPPA.

([214]) A se vedea articolul 2 alineatul (6) din CPPA, care se referă la „cenzură" (deschiderea corespondenței fără consimțământul părții în cauză sau aflarea, înregistrarea sau reținerea conținutului său prin alte mijloace) și articolul 2 alineatul (7) din CPPA, care se referă la „interceptarea comunicațiilor" (dobândirea sau înregistrarea conținutului telecomunicațiilor prin ascultarea sau citirea în comun a sunetelor, cuvintelor, simbolurilor sau imaginilor comunicațiilor prin intermediul dispozitivelor electronice și mecanice fără consimțământul părții în cauză sau ingerința în transmiterea și recepția acestora).

([215]) Articolul 13 alineatul (1) din CPPA. A se vedea, de asemenea, anexa II secțiunea 2.2.2.3. În plus, datele de localizare în timp real și datele de confirmare a comunicațiilor referitoare la o anumită stație de bază pot fi colectate numai pentru investigarea infracțiunilor grave sau în cazul în care, în caz contrar, ar fi dificil să se prevină săvârșirea unei infracțiuni sau să se colecteze probe [articolul 13 alineatul (2) din CPPA]. Acest lucru reflectă necesitatea de a se prevedea garanții suplimentare în cazul unor măsuri deosebit de invazive pentru viața privată, în concordanță cu principiul proporționalității.

([216]) Articolele 13 și 6 din CPPA.

([217]) A se vedea articolul 13 alineatele (3) și (9) coroborate cu articolul 6 alineatele (4) și (6) din CPPA.

atunci când, din motive de urgență, este imposibil să se obțină o autorizare din partea instanței, caz în care mandatul trebuie să fie obținut și comunicat furnizorului de servicii de telecomunicații imediat după solicitarea datelor ([218]). În cazul în care instanța refuză să acorde autorizarea ulterioară, informațiile colectate trebuie distruse ([219]).

(157) În ceea ce privește garanțiile suplimentare legate de colectarea datelor de confirmare a comunicațiilor, CPPA impune cerințe specifice de ținere a evidențelor și de transparență ([220]). În special, atât autoritățile de asigurarea respectării dreptului penal ([221]), cât și furnizorii de servicii de telecomunicații ([222]) trebuie să țină evidența solicitărilor și a divulgărilor făcute. În plus, autoritățile de asigurare a respectării dreptului penal trebuie, în principiu, să informeze persoanele fizice cu privire la faptul că datele lor de confirmare a comunicațiilor au fost colectate ([223]). O astfel de notificare poate fi amânată numai în circumstanțe excepționale, pe baza unei autorizări din partea șefului unui parchet districtual competent ([224]). O astfel de autorizare poate fi acordată numai atunci când notificarea este de natură (1) să pună în pericol securitatea națională, siguranța și ordinea publică, (2) să provoace decesul sau vătămarea corporală, (3) să împiedice procedurile judiciare echitabile (de exemplu, ducând la distrugerea probelor sau amenințarea martorilor) sau (4) să defăimeze persoana suspectată de săvârșirea unei infracțiuni, victimele sau alte persoane care au legătură cu cazul sau să le invadeze viața privată. În aceste cazuri, notificarea trebuie transmisă în termen de 30 de zile de îndată ce motivul (motivele) amânării încetează să existe ([225]). În urma notificării, persoanele fizice au dreptul să obțină informații cu privire la motivele colectării datelor lor ([226]).

(158) Se aplică norme mai stricte în ceea ce privește măsurile de restricționare a comunicațiilor, care pot fi utilizate numai atunci când există motive întemeiate de a suspecta că anumite infracțiuni grave menționate în mod specific în CPPA sunt planificate, sunt în curs de săvârșire sau au fost săvârșite ([227]). În plus, măsurile de restricționare a comunicațiilor pot fi luate numai în ultimă instanță și în cazul în care este dificil să se prevină în alt mod săvârșirea unei infracțiuni, să se aresteze un infractor sau să se colecteze probe ([228]). Acestea trebuie întrerupte imediat după ce nu mai sunt necesare, pentru a se asigura că încălcarea confidențialității comunicațiilor este cât mai limitată posibil ([229]). Informațiile care au fost obținute în mod ilegal prin intermediul unor măsuri de restricționare a comunicațiilor nu sunt admise ca probe în cadrul procedurilor judiciare sau disciplinare ([230]).

(159) În ceea ce privește garanțiile procedurale, CPPA prevede obligația de obținere a unui mandat judecătoresc pentru a pune în aplicare măsuri de restricționare a comunicațiilor ([231]). Din nou, CPPA prevede obligația ca cererea de emitere a unui mandat și mandatul în sine să conțină informații detaliate ([232]), inclusiv cu privire la justificarea cererii, precum și la comunicațiile care trebuie colectate (care trebuie să fie cele ale persoanei suspectate de săvârșirea de infracțiuni care face obiectul investigației) ([233]). Astfel de măsuri pot fi luate fără mandat numai în cazul unei amenințări iminente de criminalitate organizată sau în cazul în care o altă infracțiune gravă care poate cauza în mod direct decesul sau vătămarea gravă este iminentă și există o situație de urgență care face imposibilă

([218]) Articolul 13 alineatul (2) din CPPA.
([219]) Articolul 13 alineatul (3) din CPPA.
([220]) A se vedea anexa II secțiunea 2.2.2.3.
([221]) Articolul 13 alineatele (5) și (6) din CPPA.
([222]) Articolul 13 alineatul (7) din CPPA. În plus, furnizorii de servicii de telecomunicații trebuie să prezinte de două ori pe an Ministerului Științei și TIC un raport cu privire la divulgarea datelor de confirmare a comunicațiilor.
([223]) A se vedea articolul 13-3 alineatul (7) coroborat cu articolul 9-2 din CPPA. În special, persoanele fizice trebuie informate în termen de 30 de zile de la luarea unei decizii de (ne)începere a urmăririi penale sau în termen de 30 de zile după un an de la luarea unei decizii de suspendare a punerii sub acuzare (deși notificarea trebuie, în orice caz, să fie transmisă în termen de 30 de zile de la colectarea informațiilor), a se vedea articolul 13-3 alineatul (1) din CPPA.
([224]) Articolul 13-3 alineatele (2)-(3) din CPPA.
([225]) Articolul 13-3 alineatul (4) din CPPA.
([226]) Articolul 13-3 alineatul (5) din CPPA. La cererea persoanei în cauză, procurorul sau agentul de poliție judiciară trebuie să prezinte motivele în scris, în termen de 30 de zile de la primirea cererii, cu excepția cazului în care se aplică una dintre excepțiile pentru amânarea notificării [articolul 13-3 alineatul (6) din CPPA].
([227]) De exemplu, infracțiuni precum insurecția, infracțiunile legate de droguri, infracțiunile care implică explozivi, precum și infracțiunile legate de securitatea națională, relațiile diplomatice sau bazele și instalațiile militare, a se vedea articolul 5 alineatul (1) din CPPA. A se vedea, de asemenea, anexa II secțiunea 2.2.2.2.
([228]) Articolul 3 alineatul (2) și articolul 5 alineatul (1) din CPPA.
([229]) Articolul 2 din Decretul de punere în aplicare a CPPA.
([230]) Articolul 4 din CPPA.
([231]) Articolul 6 alineatele (1), (2) și (5)-(6) din CPPA.
([232]) O cerere de emitere a unui mandat trebuie să descrie (1) motivele întemeiate pentru a suspecta (*prima facie*) că una dintre infracțiunile enumerate este planificată, este în curs de săvârșire sau a fost săvârșită, precum și orice materiale justificative; (2) măsurile de restricționare a comunicațiilor, precum și ținta, domeniul de aplicare, obiectivul și perioada lor efectivă; și (3) locul în care vor fi executate măsurile și modul în care acestea vor fi puse în aplicare [articolul 6 alineatul (4) din CPPA și articolul 4 alineatul (1) din Decretul de punere în aplicare a CPPA]. Mandatul în sine trebuie să specifice măsurile, precum și ținta, domeniul de aplicare, perioada efectivă, locul de executare și modul de punere în aplicare a acestora [articolul 6 alineatul (6) din CPPA].
([233]) Ținta unei măsuri de restricționare a comunicațiilor trebuie să fie obiectele de corespondență sau telecomunicațiile specifice expediate sau primite de suspect sau obiectele de corespondență sau telecomunicațiile expediate sau primite de suspect pe o perioadă determinată [articolul 5 alineatul (2) din CPPA].

parcurgerea procedurii obișnuite ([234]). Totuși, în acest caz, o cerere de emitere a unui mandat trebuie depusă imediat după luarea măsurii ([235]). Măsurile de restricționare a comunicațiilor pot fi puse în aplicare numai pentru o perioadă maximă de două luni ([236]), perioadă ce poate fi prelungită cu aprobarea instanței numai dacă sunt îndeplinite în continuare condițiile pentru punerea în aplicare a măsurilor ([237]). Perioada prelungită nu poate depăși în total un an, respectiv trei ani pentru anumite infracțiuni deosebit de grave (de exemplu, infracțiuni legate de insurecție, agresiune externă, securitate națională etc.) ([238]).

(160) La fel ca în cazul colectării datelor de confirmare a comunicațiilor, CPPA prevede obligația furnizorilor de servicii de telecomunicații ([239]) și a autorităților de aplicare a legii ([240]) să păstreze evidențe privind executarea măsurilor de restricționare a comunicațiilor și prevede obligația de notificare a persoanei în cauză, care poate fi amânată în mod excepțional, dacă este necesar, din motive importante de interes public ([241]).

(161) În cele din urmă, nerespectarea mai multor limitări și garanții prevăzute de CPPA (inclusiv, de exemplu, obligațiile de obținere a unui mandat, de ținere a evidenței și de notificare a persoanei), atât în ceea ce privește colectarea datelor de confirmare a comunicațiilor, cât și utilizarea măsurilor de restricționare a comunicațiilor, fac obiectul unor sancțiuni penale ([242]).

(162) Competențele autorităților de aplicare a dreptului penal de a colecta date privind comunicațiile în temeiul CPPA (atât conținutul comunicațiilor, cât și datele de confirmare a comunicațiilor) sunt, prin urmare, limitate de norme clare și precise și fac obiectul unei serii de garanții. Aceste garanții, în special, garantează supravegherea executării unor astfel de măsuri, atât *ex ante* (prin autorizare judiciară prealabilă), cât și *ex post* (prin cerințe de ținere a evidențelor și de raportare) și facilitează accesul persoanelor fizice la căi de atac eficace (prin asigurarea faptului că acestea sunt informate cu privire la colectarea datelor lor).

3.2.1.3 Cereri de divulgare voluntară a datelor privind abonații

(163) Pe lângă faptul că se bazează pe măsurile obligatorii descrise în considerentele 153-162, autoritățile coreene de aplicare a legii pot solicita furnizorilor de servicii de telecomunicații să transmită „date privind comunicațiile" în mod voluntar, în sprijinul unui proces penal, al investigării sau al executării unei pedepse [articolul 83 alineatul (3) din TBA]. Această posibilitate există numai pentru câteva seturi de date limitate, și anume numele, numărul de înregistrare pentru rezidenți, adresa și numărul de telefon al utilizatorilor, datele la care utilizatorii se abonează sau își reziliază abonamentul, precum și codurile de identificare a utilizatorului (și anume codurile utilizate pentru a identifica utilizatorul de drept al sistemelor informatice sau al rețelelor de comunicații) ([243]). Întrucât numai persoanele care contractează în mod direct servicii de la un furnizor coreean de telecomunicații sunt considerate „utilizatori" ([244]), persoanele din UE ale căror date au fost transferate către Republica Coreea nu ar intra, în mod normal, în această categorie ([245]).

(164) Unor astfel de divulgări voluntare li se aplică limitări diferite, atât în ceea ce privește exercitarea competențelor de către autoritatea de aplicare a legii, cât și în ceea ce privește răspunsul operatorului de telecomunicații. Ca o cerință generală, autoritățile de aplicare a legii trebuie să acționeze în conformitate cu principiile constituționale ale necesității și proporționalității [articolul 12 alineatul (1) și articolul 37 alineatul (2) din Constituție], inclusiv atunci când solicită informații în mod voluntar. În plus, acestea trebuie să respecte PIPA, în special să colecteze

([234]) Articolul 8 alineatul (1) din CPPA. Cu toate acestea, colectarea de informații în situații de urgență trebuie să aibă loc întotdeauna în conformitate cu o „declarație privind cenzura/interceptarea comunicațiilor de urgență", iar autoritatea care efectuează colectarea trebuie să țină un registru al tuturor măsurilor de urgență [articolul 8 alineatul (4) din CPPA].

([235]) Colectarea trebuie întreruptă imediat în cazul în care autoritatea de aplicare a legii nu obține autorizarea din partea instanței în termen de 36 de ore [articolul 8 alineatul (2) din CPPA], caz în care, astfel cum se explică în secțiunea 2.2.2.2 din anexa II, informațiile colectate vor fi, în principiu, distruse. Instanța trebuie, de asemenea, sesizată în cazul în care măsurile de urgență au încetat într-un interval de timp atât de scurt încât să se evite necesitatea unei autorizări [de exemplu, în cazul în care suspectul este arestat imediat după inițierea interceptării; a se vedea articolul 8 alineatul (5) din CPPA]. În acest caz, instanței trebuie să i se furnizeze informații privind obiectivul, ținta, domeniul de aplicare, perioada, locul de executare și metoda de colectare, precum și motivele pentru care nu a depus o cerere de autorizare din partea instanței [articolul 8 alineatele (6)-(7) din CPPA].

([236]) Articolul 6 alineatul (7) din CPPA. În cazul în care obiectivul măsurilor este atins mai devreme în perioada respectivă, măsurile trebuie să înceteze imediat.

([237]) Articolul 6 alineatele (7)-(8) din CPPA.

([238]) Articolul 6 alineatul (8) din CPPA.

([239]) Articolul 9 alineatul (3) din CPPA.

([240]) Articolul 18 alineatul (1) din Decretul de punere în aplicare a CPPA.

([241]) În special, procurorul trebuie să informeze persoana în cauză în termen de 30 de zile de la emiterea unei decizii de punere sub acuzare sau a unei dispoziții de a nu fi pusă sub acuzare sau de a nu fi arestată [articolul 9-2 alineatul (1) din CPPA]. Notificarea poate fi amânată cu aprobarea șefului parchetului districtual, în cazul în care aceasta ar reprezenta un pericol grav pentru securitatea națională sau ar afecta siguranța și ordinea publică sau ar putea prejudicia grav viața și integritatea fizică a altora [articolul 9-2 alineatele (4)-(6) din CPPA].

([242]) Articolele 16 și 17 din CPPA.

([243]) Articolul 83 alineatul (3) din TBA. A se vedea, de asemenea, anexa II secțiunea 2.2.3.

([244]) Articolul 2 alineatul (9) din TBA.

([245]) A se vedea, de asemenea, anexa II secțiunea 2.2.3.

doar volumul minim de date cu caracter personal, în măsura necesară atingerii unui scop legitim, într-un mod care să reducă la minimum impactul asupra vieții private a persoanelor fizice [cum ar fi articolul 3 alineatele (1) și (6) din PIPA]. Mai precis, cererile de obținere a datelor privind comunicațiile în temeiul TBA trebuie să fie formulate în scris și să indice motivele cererii, legătura cu utilizatorul relevant și domeniul de aplicare al datelor solicitate ([246]).

(165) Furnizorii de servicii de telecomunicații nu sunt obligați să dea curs acestor cereri și pot face acest lucru numai în conformitate cu PIPA. Aceasta înseamnă, în special, că trebuie să pună în balanță diferitele interese aflate în joc, neputând furniza datele în cazul în care acest lucru ar putea încălca în mod abuziv interesele persoanei respective sau ale unui terț ([247]). Se va proceda astfel, de exemplu, atunci când este clar că autoritatea solicitantă a abuzat de autoritatea sa ([248]). Operatorii de telecomunicații trebuie să țină evidența divulgărilor în temeiul TBA și să prezinte de două ori pe an ministrului științei și TIC un raport în acest sens ([249]).

(166) În plus, în conformitate cu secțiunea 3 din Notificarea nr. 2021-5 (anexa I), furnizorii de telecomunicații trebuie, în principiu, să transmită o notificare persoanei în cauză atunci când se conformează în mod voluntar unei cereri ([250]). La rândul său, acest lucru va permite persoanei în cauză să își exercite drepturile și, în cazul în care datele sale sunt divulgate în mod ilegal, să obțină reparații fie de la operator (de exemplu, fie pentru divulgarea datelor cu încălcarea PIPA, fie pentru că a dat curs unei cereri care era în mod clar disproporționată), fie de la autoritatea de aplicare a legii (de exemplu, pentru că acționează dincolo de limitele a ceea ce este necesar și proporțional sau pentru că nu respectă cerințele procedurale prevăzute în TBA).

3.2.2 *Utilizarea ulterioară a informațiilor colectate*

(167) Prelucrarea datelor cu caracter personal colectate de autoritățile coreene de asigurare a respectării dreptului penal face obiectul tuturor cerințelor PIPA, inclusiv în ceea ce privește limitarea scopului [articolul 3 alineatele (1)-(2) din PIPA], legalitatea utilizării și furnizarea către terți [articolele 15, 17 și 18 din PIPA], transferurile internaționale [articolele 17 și 18 din PIPA, coroborate cu secțiunea 2 din Notificarea nr. 2021-5] ([251]), proporționalitatea/reducerea la minimum a datelor [articolul 3 alineatele (1) și (6) din PIPA] și limitarea stocării (articolul 21 din PIPA) ([252]).

(168) În ceea ce privește conținutul comunicațiilor obținute prin executarea măsurilor de restricționare a comunicațiilor, CPPA limitează în mod specific posibila utilizare a acestora la investigarea, urmărirea penală sau prevenirea infracțiunilor grave ([253]); procedurile disciplinare pentru aceleași infracțiuni; cererile de despăgubire formulate de o parte la comunicații sau în cazul în care acest lucru este permis în mod expres de alte legi ([254]). În plus, conținutul colectat al telecomunicațiilor transmise prin internet poate fi păstrat numai cu aprobarea instanței care a autorizat măsurile de restricționare a comunicațiilor ([255]), în vederea utilizării acestuia pentru investigarea, urmărirea penală sau prevenirea infracțiunilor grave ([256]). La un nivel mai general, CPPA interzice divulgarea informațiilor confidențiale obținute prin măsuri de restricționare a comunicațiilor și utilizarea unor astfel de informații pentru a aduce atingere reputației celor care au făcut obiectul măsurilor ([257]).

3.2.3 *Supravegherea*

(169) În Coreea, activitățile autorităților de asigurarea respectării dreptului penal sunt supravegheate de diferite organisme ([258]).

([246]) Articolul 83 alineatul (4) din TBA. În cazul în care este imposibil să se prezinte o cerere scrisă din motive de urgență, cererea scrisă trebuie transmisă imediat ce motivul urgenței dispare [articolul 83 alineatul (4) din TBA].

([247]) Articolul 18 alineatul (2) din PIPA.

([248]) Hotărârea Curții Supreme nr. 2012Da105482 din 10 martie 2016. A se vedea, de asemenea, anexa II secțiunea 2.2.3 cu privire la această hotărâre a Curții Supreme.

([249]) Articolul 83 alineatele (5)-(6) din TBA.

([250]) Această cerință face obiectul unor excepții limitate și calificate, în special dacă și atât timp cât notificarea ar pune în pericol o anchetă penală în curs sau ar putea dăuna vieții sau integrității fizice a unei alte persoane, în cazul în care aceste drepturi sau interese sunt în mod evident superioare drepturilor persoanei vizate. A se vedea secțiunea 3 punctul (iii) subpunctul (1) din notificare.

([251]) În special, autorităților publice coreene li se cere să asigure, printr-un instrument obligatoriu din punct de vedere juridic, un nivel de protecție echivalent cu cel oferit de PIPA; a se vedea, de asemenea, considerentul 90.

([252]) A se vedea, de asemenea, anexa II secțiunea 1.2.

([253]) A se vedea considerentul 158.

([254]) Articolul 12 din CPPA. A se vedea anexa II secțiunea 2.2.2.2.

([255]) Procurorul sau agentul de poliție care execută măsurile de restricționare a comunicațiilor trebuie să selecteze telecomunicațiile care urmează să fie păstrate în termen de 14 zile de la încetarea măsurilor și să solicite aprobarea instanței (în cazul agentului de poliție, cererea trebuie înaintată unui procuror, care, la rândul său, transmite cererea instanței), a se vedea articolul 12-2 alineatele (1) și (2) din CPPA.

([256]) O cerere pentru o astfel de autorizare trebuie să conțină informații privind măsurile de restricționare a comunicațiilor, un rezumat al rezultatelor măsurilor, motivele reținerii (împreună cu materiale justificative) și telecomunicațiile care trebuie păstrate [articolul 12-2 alineatul (3) din CPPA]. În cazul în care nu se depune nicio cerere, datele obținute trebuie șterse în termen de 14 zile de la încetarea măsurii de restricționare a comunicațiilor [articolul 12-2 alineatul (5) din CPPA] și, în cazul în care cererea este respinsă, în termen de șapte zile [articolul 12-2 alineatul (5) din CPPA]. În ambele cazuri, în termen de șapte zile, trebuie depus un raport cu privire la ștergere la instanța care a autorizat colectarea.

([257]) Articolul 11 alineatul (2) din Decretul de punere în aplicare a CPPA.

([258]) A se vedea anexa II secțiunea 2.3.

(170) În primul rând, poliția este supusă supravegherii interne de către un inspector general ([259]), care efectuează controlul legalității, inclusiv în ceea ce privește posibilele încălcări ale drepturilor omului. Inspectorul general a fost instituit pentru a pune în aplicare Legea privind auditurile din sectorul public, care încurajează crearea de organisme de audit intern și stabilește cerințe specifice privind componența și sarcinile acestora. În special, legea prevede că șeful unui organism de audit intern este numit din afara autorității relevante (cum ar fi foști judecători, profesori) pentru o perioadă de doi până la cinci ani ([260]), poate fi demis numai din motive justificate (de exemplu, atunci când nu își poate îndeplini atribuțiile din motive de sănătate sau atunci când face obiectul unor măsuri disciplinare) ([261]), garantându-i-se independența în cea mai mare măsură posibilă ([262]). Obstrucționarea unui audit intern face obiectul unor amenzi administrative ([263]). Rapoartele de audit (care pot include recomandări, cereri de măsuri disciplinare și cereri de despăgubiri sau de corectare) sunt comunicate șefului autorității publice relevante, Comisiei de audit și inspecție (BAI) ([264]) și, în general, sunt făcute publice ([265]). Rezultatele punerii în aplicare a raportului trebuie, de asemenea, notificate BAI ([266]) (a se vedea considerentul 173 privind rolul și competențele de supraveghere ale BAI).

(171) În al doilea rând, PIPC supraveghează conformitatea prelucrării datelor de către autoritățile de asigurarea respectării dreptului penal cu PIPA și cu alte legi care protejează dreptul la viață privată al persoanelor fizice, inclusiv cu legile care reglementează colectarea de probe (electronice) în scopul asigurării respectării dreptului penal, astfel cum se descrie în secțiunea 3.2.1 ([267]). În special, întrucât supravegherea PIPC se extinde la legalitatea și echitatea colectării și prelucrării datelor [articolul 3 alineatul (1) din PIPA], care vor fi încălcate în cazul în care datele cu caracter personal sunt accesate și utilizate cu încălcarea acestor legi ([268]), PIPC poate, de asemenea, să investigheze și să asigure respectarea limitărilor și a garanțiilor descrise în secțiunea 3.2.1 ([269]). În exercitarea acestui rol de supraveghere, PIPC poate face uz de toate competențele sale de investigare și de remediere, astfel cum sunt descrise în detaliu în secțiunea 2.4.2. Deja dinainte de recenta reformă a PIPA (și anume, în cadrul rolului său anterior de supraveghere pentru sectorul public), PIPC a desfășurat mai multe activități de supraveghere a prelucrării datelor cu caracter personal de către autoritățile de asigurare a respectării dreptului penal, de exemplu în contextul interogării suspecților (cazul nr. 2013-16, 26 august 2013), în ceea ce privește transmiterea de notificări persoanelor fizice cu privire la impunerea de amenzi administrative (cazul nr. 2015-02-04, 26 ianuarie 2015), schimbul de date cu alte autorități (cazul nr. 2018-15-146, 9 iulie 2018, cazul nr. 2018-25-308, 10 decembrie 2018; cazul nr. 2019-02-015, 29 ianuarie 2019), colectarea amprentelor digitale sau a fotografiilor (cazul nr. 2019-17-273, 9 septembrie 2019), utilizarea dronelor (cazul nr. 2020-01-004, 13 ianuarie 2020). În aceste cazuri, PIPC a investigat respectarea mai multor dispoziții ale PIPA (de exemplu, legalitatea prelucrării, principiile limitării scopului și reducerii la minimum a datelor), dar și a dispozițiilor relevante ale altor legi, cum ar fi Codul de procedură penală, și, după caz, a emis recomandări pentru a alinia prelucrarea la cerințele privind protecția datelor.

(172) În al treilea rând, supravegherea independentă este asigurată de Comisia națională pentru drepturile omului (NHRC) ([270]), care poate investiga încălcări ale drepturilor la viață privată și la confidențialitatea corespondenței, ca parte a mandatului său general de a proteja drepturile fundamentale prevăzute la articolele 10-22 din Constituție. NHRC este alcătuită din 11 comisari care trebuie să dețină calificări specifice ([271]) și care sunt numiți de președintele statului în conformitate cu procedurile prevăzute în lege. Mai precis, patru comisari sunt desemnați de Adunarea Națională, patru, de către președintele statului, și trei, de către președintele Curții Supreme ([272]). Președintele comisiei este numit de președintele statului din rândul comisarilor și trebuie să fie confirmat de Adunarea Națională ([273]). Comisarii (inclusiv președintele Comisiei) sunt numiți pentru un mandat de trei ani, cu posibilitate de reînnoire, și pot fi demiși numai dacă sunt condamnați la închisoare sau când nu

([259]) A se vedea anexa II secțiunea 2.3.1. A se vedea, de asemenea, https://www.police.go.kr/eng/knpa/org/org01.jsp.
([260]) În mod similar, auditorii sunt numiți pe baza condițiilor specifice prevăzute în lege; a se vedea articolul 16 și următoarele din Legea privind auditurile din sectorul public.
([261]) Articolele 8-11 din Legea privind auditurile din sectorul public.
([262]) Articolul 7 din Legea privind auditurile din sectorul public.
([263]) Articolul 41 din Legea privind auditurile din sectorul public.
([264]) Articolul 23 alineatul (1) din Legea privind auditurile din sectorul public.
([265]) Articolul 26 din Legea privind auditurile din sectorul public.
([266]) Articolul 23 alineatul (3) din Legea privind auditurile din sectorul public.
([267]) A se vedea articolul 7-8 alineatele (3) și (4) și articolul 7-9 alineatul (5) din PIPA.
([268]) A se vedea Notificarea PIPC nr. 2021-5, secțiunea 6 (anexa I).
([269]) A se vedea, de asemenea, anexa II secțiunea 2.3.4.
([270]) Articolul 1 din Legea privind Comisia pentru drepturile omului (Legea NHRC).
([271]) Pentru a fi numit, un comisar trebuie (1) să fi lucrat timp de cel puțin zece ani în cadrul unei universități sau al unui institut de cercetare autorizat, cel puțin în calitate de conferențiar; (2) să fi ocupat funcția de judecător, procuror sau avocat cel puțin zece ani; (3) să fi fost implicat în activități privind drepturile omului timp de cel puțin zece ani (de exemplu, pentru o organizație non-profit, neguvernamentală sau internațională); sau (4) să fi fost recomandat de grupuri ale societății civile [articolul 5 alineatul (3) din Legea NHRC]. În plus, odată numiți, comisarilor li se interzice să dețină în același timp o funcție în cadrul Adunării Naționale, al consiliilor locale sau al oricărei administrații naționale ori locale (în calitate de funcționar public); a se vedea articolul 10 din Legea NHRC.
([272]) Articolul 5 alineatele (1) și (2) din Legea NHRC.
([273]) Articolul 5 alineatul (5) din Legea NHRC.

mai sunt capabili să își exercite atribuțiile din cauza unor deficiențe fizice sau psihice prelungite (caz în care două treimi dintre comisari trebuie să fie de acord cu demiterea) ([274]). În cadrul unei anchete, NHRC poate solicita prezentarea de materiale relevante, poate efectua inspecții și poate convoca diverse persoane să depună mărturie ([275]). În ceea ce privește competențele de remediere, NHRC poate emite recomandări (publice) de îmbunătățire sau corectare a politicilor și practicilor specifice, la care autoritățile publice trebuie să răspundă printr-un plan de punere în aplicare propus ([276]). Dacă autoritatea în cauză nu pune în aplicare recomandările, aceasta trebuie să informeze Comisia în acest sens ([277]), care, la rândul său, poate să dezvăluie această neîndeplinire Adunării Naționale și/sau să o facă publică. Potrivit expunerii oficiale a guvernului coreean (secțiunea 2.3.5 din anexa II), autoritățile coreene respectă, în general, recomandările NHRC și sunt puternic încurajate să facă acest lucru, întrucât punerea lor în aplicare a fost evaluată ca parte a unei evaluări generale continue sub autoritatea cabinetului prim-ministrului. Cifrele anuale privind activitățile sale arată că NHRC supraveghează în mod activ activitățile autorităților de asigurare a respectării dreptului penal, fie pe baza unor petiții individuale, fie prin anchete *ex officio* ([278]).

(173) În al patrulea rând, controlul general al legalității activităților autorităților publice este exercitat de BAI, care examinează veniturile și cheltuielile statului și, la un nivel mai general, supraveghează respectarea obligațiilor autorităților publice în vederea îmbunătățirii funcționării administrației publice ([279]). BAI este înființată în mod oficial sub conducerea președintelui Republicii Coreea, dar își menține un statut independent în ceea ce privește atribuțiile care îi revin ([280]). În plus, i se acordă independență deplină în ceea ce privește numirea, demiterea și organizarea personalului său, precum și întocmirea bugetului său ([281]). BAI este alcătuită dintr-un președinte de comisie (numit de președintele statului, cu acordul Adunării Naționale) ([282]) și șase comisari (numiți de președintele statului la recomandarea președintelui comisiei) ([283]), care trebuie să îndeplinească anumite calificări prevăzute de lege ([284]) și care pot fi revocați numai în caz de punere sub acuzare, condamnare la închisoare sau incapacitate de a-și îndeplini atribuțiile din cauza unor deficiențe psihice sau fizice pe termen lung ([285]). BAI efectuează anual un audit general, dar poate efectua, de asemenea, audituri specifice cu privire la chestiuni de interes special. La efectuarea unui audit sau a unei inspecții, BAI poate solicita prezentarea de documente și prezența unor persoane ([286]). BAI poate emite recomandări, poate solicita măsuri disciplinare sau poate depune o plângere penală ([287]).

(174) În cele din urmă, Adunarea Națională exercită controlul parlamentar asupra autorităților publice prin investigații și inspecții ([288]) ale activităților acestora ([289]). Adunarea Națională poate solicita divulgarea documentelor, poate impune înfățișarea martorilor ([290]), poate recomanda măsuri de remediere (dacă ajunge la concluzia că au avut loc

([274]) Articolul 7 alineatul (1) și articolul 8 din Legea NHRC.

([275]) Articolul 36 din Legea NHRC. În conformitate cu articolul 6 alineatul (7) din lege, prezentarea de materiale sau obiecte poate fi respinsă în cazul în care ar aduce atingere confidențialității statului care ar putea avea un efect major asupra securității statului sau a relațiilor diplomatice sau ar constitui un obstacol serios în calea unei anchete penale sau a unui proces în curs. În astfel de cazuri, Comisia poate solicita informații suplimentare din partea șefului agenției relevante (care trebuie să se conformeze cu bună-credință), dacă acest lucru este necesar pentru a permite să se verifice dacă refuzul de a furniza informațiile este justificat.

([276]) Articolul 25 alineatele (1) și (3) din Legea NHRC.

([277]) Articolul 25 alineatul (4) din Legea NHRC.

([278]) De exemplu, între 2015 și 2019, NHRC a primit anual între 1 380 și 1 699 de petiții împotriva autorităților de asigurare a respectării dreptului penal și a tratat un număr la fel de ridicat de solicitări (de exemplu, a tratat 1 546 de plângeri împotriva poliției în 2018 și 1 249, în 2019); de asemenea, Comisia a efectuat mai multe anchete *ex officio*, astfel cum se descrie mai detaliat în raportul anual pe 2018 al NHRC (disponibil la adresa https://www.humanrights.go.kr/site/program/board/basicboard/view?menuid=002003003001&pagesize=10&boardtypeid=7017&boardid=7602641) și în raportul anual pe 2019 (disponibil la adresa https://www.humanrights.go.kr/site/program/board/basicboard/view?menuid=002003003001&pagesize=10&boardtypeid=7017&boardid=7606217).

([279]) Articolele 20 și 24 din Legea privind Comisia de audit și inspecție (Legea BAI). A se vedea anexa II, secțiunea 2.3.2.

([280]) Articolul 2 alineatul (1) din Legea BAI.

([281]) Articolul 2 alineatul (2) din Legea BAI.

([282]) Articolul 4 alineatul (1) din Legea BAI.

([283]) Articolul 5 alineatul (1) și articolul 6 din Legea BAI.

([284]) De exemplu, să fi ocupat funcția de judecător, procuror sau avocat timp de cel puțin zece ani, să fi lucrat ca funcționar public, profesor sau să fi ocupat un post specific învățământului superior la o universitate timp de cel puțin opt ani sau să fi lucrat timp de cel puțin zece ani în cadrul unei societății cotate la bursă sau al unei instituții cu capital de stat (din care cel puțin cinci ani ca funcționar executiv); a se vedea articolul 7 din Legea BAI. În plus, comisarilor li se interzice să participe la activități politice și să dețină în același timp funcții în cadrul Adunării Naționale, al agențiilor administrative, al organizațiilor supuse auditului și inspecției de către BAI sau orice alt post sau funcție remunerat(ă) (articolul 9 din Legea BAI).

([285]) Articolul 8 din Legea BAI.

([286]) A se vedea, de exemplu, articolul 27 din Legea BAI.

([287]) Articolele 24 și 31-35 din Legea BAI.

([288]) Articolul 128 din Legea privind Adunarea Națională și articolele 2, 3 și 15 din Legea privind inspecția și investigarea administrației de stat. Aceasta include inspecții anuale ale afacerilor guvernamentale în ansamblu, dar și investigații cu privire la chestiuni specifice.

([289]) A se vedea anexa secțiunea 2.2.3.

([290]) Articolul 10 alineatul (1) din Legea privind inspecția și investigarea administrației de stat. A se vedea, de asemenea, articolele 128 și 129 din Legea privind Adunarea Națională.

activități ilegale sau necorespunzătoare) ([291]) și poate face publice rezultatele constatărilor sale ([292]). În cazul în care Adunarea Națională solicită luarea de măsuri de remediere – care pot include, de exemplu, acordarea de despăgubiri, luarea de măsuri disciplinare sau îmbunătățirea procedurilor interne – autoritatea publică în cauză are obligația de a acționa fără întârziere și de a prezenta Adunării Naționale un raport cu privire la rezultat ([293]).

3.2.4 *Măsuri reparatorii*

(175) Sistemul coreean oferă diferite căi (judiciare) pentru a obține despăgubiri, inclusiv despăgubiri pentru daune.

(176) În primul rând, PIPA le oferă persoanelor fizice dreptul de acces, rectificare, ștergere și suspendare în ceea ce privește datele cu caracter personal prelucrate în scopul asigurării respectării dreptului penal ([294]).

(177) În al doilea rând, persoanele fizice pot recurge la diferitele mecanisme de exercitare a unei căi de atac oferite de PIPA în cazul în care datele lor au fost prelucrate de o autoritate de asigurare a respectării dreptului penal cu încălcarea PIPA sau cu încălcarea limitărilor și garanțiilor care reglementează colectarea datelor cu caracter personal prevăzute în alte legi (de exemplu, CPA sau CPPA; a se vedea considerentul 171). În special, persoanele fizice pot depune o plângere la PIPC (inclusiv prin intermediul Centrului de intermediere telefonică privind protecția vieții private gestionat de Agenția coreeană pentru internet și securitate ([295])) sau la Comitetul de mediere a litigiilor privind informațiile cu caracter personal ([296]). Aceste posibilități de a recurge la căi de atac nu sunt supuse unor cerințe suplimentare de admisibilitate. În temeiul Legii privind contenciosul administrativ, persoanele fizice pot, de asemenea, să formuleze un recurs/să conteste deciziile sau lipsa de acțiune a PIPC (a se vedea considerentul 132).

(178) În al treilea rând, orice persoană ([297]) poate depune o plângere la NHRC cu privire la o încălcare a dreptului la viață privată și la protecția datelor de către o autoritate coreeană de asigurare a respectării dreptului penal. NHRC poate recomanda rectificarea sau îmbunătățirea oricărei legi, instituții, politici sau practici relevante ([298]) sau punerea în aplicare a unor căi de atac, cum ar fi medierea ([299]), încetarea încălcării drepturilor omului, despăgubiri pentru daune și măsuri de prevenire a repetării acelorași încălcări sau a unor încălcări similare ([300]). Potrivit expunerii oficiale a guvernului coreean (secțiunea 2.4.2 din anexa II), aceasta poate include, de asemenea, ștergerea datelor cu caracter personal colectate în mod ilegal. Deși NHRC nu are competența să emită decizii obligatorii, aceasta oferă o cale de atac mai informală, la costuri mai reduse și mai accesibilă, în special deoarece, astfel cum se explică în anexa II secțiunea 2.4.2, nu impune demonstrarea unui prejudiciu în fapt pentru ca plângerea să fie investigată ([301]). Acest lucru asigură că plângerile persoanelor fizice cu privire la colectarea datelor lor pot fi investigate, chiar dacă o persoană nu este în măsură să demonstreze că datele sale au fost într-adevăr colectate (de exemplu, deoarece nu a fost informată încă). Rapoartele anuale de activitate ale NHRC arată că persoanele fizice utilizează, de asemenea, această cale în practică pentru a contesta activitățile autorităților de asigurare a respectării dreptului penal, inclusiv în ceea ce privește prelucrarea datelor cu caracter personal ([302]). În cazul în care o persoană nu este satisfăcută de rezultatul unei proceduri în fața NHRC, aceasta poate contesta deciziile NHRC

([291]) Articolul 16 alineatul (2) din Legea privind inspecția și investigarea administrației de stat.
([292]) Articolul 12-2 din Legea privind inspecția și investigarea administrației de stat.
([293]) Articolul 16 alineatul (3) din Legea privind inspecția și investigarea administrației de stat.
([294]) Acest drept poate fi exercitat direct la autoritatea competentă sau indirect prin intermediul PIPC [articolul 35 alineatul (2) din PIPA]. Astfel cum se descrie mai detaliat în considerentele 76-78, excepțiile de la aceste drepturi se vor aplica numai atunci când este necesar pentru protejarea intereselor (publice) importante.
([295]) Articolul 62 din PIPA.
([296]) Articolele 40-50 din PIPA și articolele 48-2 - 57 din Decretul de punere în aplicare a PIPA. A se vedea, de asemenea, anexa II secțiunea 2.4.1.
([297]) Astfel cum se explică în anexa II secțiunea 2.4.2, deși articolul 4 din Legea NHRC se referă la cetățenii și străinii care își au reședința în Republica Coreea, termenul „reședință" reflectă mai degrabă conceptul de jurisdicție decât teritoriul. Prin urmare, dacă drepturile fundamentale ale unui străin din afara Coreei sunt încălcate de instituțiile naționale din Coreea, persoana respectivă poate depune o plângere la NHRC. Acesta ar fi cazul când autoritățile publice coreene accesează în mod ilegal datele cu caracter personal ale unui străin transferate în Coreea. A se vedea în special explicațiile furnizate la adresa https://www.humanrights.go.kr/site/program/board/basicboard/list?boardtypeid=7025&menuid=002004005001&pagesize=10&currentpage=2.
([298]) Articolul 44 din Legea NHRC.
([299]) O persoană fizică poate solicita, de asemenea, soluționarea plângerii prin mediere; a se vedea articolul 42 și următoarele din Legea NHRC.
([300]) Articolul 42 alineatul (4) din Legea NHRC. În plus, NHRC poate adopta măsuri urgente de remediere în cazul unei încălcări în curs care ar putea cauza prejudicii dificil de remediat dacă nu este tratată; a se vedea articolul 48 din Legea NHRC.
([301]) În principiu, o plângere trebuie depusă în termen de un an de la încălcare, dar NHRC poate decide în continuare să investigheze o plângere care este depusă și după această perioadă, atât timp cât termenul de prescripție prevăzut de dreptul penal sau civil nu a expirat [articolul 32 alineatul (1) punctul (4) din Legea NHRC].
([302]) De exemplu, NHRC a tratat în trecut plângeri și a emis recomandări cu privire la punerile sub sechestru ilegale și la încălcarea obligației de a informa persoanele fizice cu privire la o punere sub sechestru (a se vedea p. 80 și 91 din raportul anual pe 2018 al NHRC, disponibil la adresa https://www.humanrights.go.kr/site/program/board/basicboard/view?menuid=002003003001&pagesize=10&boardtypeid=7017&boardid=7604746), precum și la prelucrarea ilegală a informațiilor cu caracter personal de către poliție, parchete și instanțe (a se vedea p. 157-158 din Raportul anual pe 2019 al NHRC, disponibil la adresa https://www.humanrights.go.kr/site/program/board/basicboard/view?menuid=002003003001&pagesize=10&boardtypeid=7017&boardid=7603308, și p. 76 din raportul anual pe 2019, disponibil la adresa https://www.humanrights.go.kr/site/program/board/basicboard/view?menuid=002003003001&pagesize=10&boardtypeid=7017&boardid=7606217).

(cum ar fi o decizie de a nu continua investigarea unei plângeri ([303])) și recomandările în fața instanțelor coreene în temeiul Legii privind contenciosul administrativ (a se vedea considerentul 181) ([304]). În plus, o procedură în fața NHRC poate facilita și mai mult accesul la instanțe, deoarece o persoană fizică ar putea introduce căi de atac suplimentare împotriva autorității publice care a prelucrat în mod ilegal datele sale pe baza constatărilor NHRC, în conformitate cu procedurile descrise în considerentele 181-183.

(179) În cele din urmă, sunt disponibile diferite căi de atac judiciare, care le permit persoanelor fizice să invoce limitările și garanțiile descrise în secțiunea 3.2.1 pentru a obține reparații ([305]).

(180) În ceea ce privește punerile sub sechestru (inclusiv de date), CPA prevede posibilitatea de a formula obiecții cu privire la executarea unui mandat sau de a contesta executarea acestuia prin intermediul unei „cvasi-plângeri", adresând instanței competente o cerere de anulare sau modificare a unei dispoziții emise de un procuror sau de un ofițer de poliție ([306]).

(181) La un nivel mai general, persoanele fizice pot contesta acțiunile ([307]) sau omisiunile ([308]) autorităților publice (inclusiv ale autorităților de asigurare a asigurarea respectării dreptului penal) în temeiul Legii privind contenciosul administrativ ([309]). Acțiunea administrativă este considerată o „dispoziție atacabilă" dacă are un impact direct asupra drepturilor și obligațiilor civile ([310]), ceea ce, astfel cum a confirmat guvernul coreean (secțiunea 2.4.3 din anexa II), este cazul măsurilor de colectare a datelor cu caracter personal, fie direct (de exemplu, prin interceptarea comunicațiilor), prin intermediul unor cereri de divulgare cu caracter obligatoriu (de exemplu, către un furnizor de servicii) sau prin cereri de cooperare voluntară. Pentru ca o plângere în temeiul Legii privind contenciosul administrativ să fie admisibilă, o persoană fizică trebuie să aibă un interes juridic în continuarea cererii ([311]). În conformitate cu jurisprudența Curții Supreme, „interesul juridic" este interpretat ca un „interes protejat din punct de vedere juridic", și anume un interes direct și specific protejat prin acte cu putere de lege și norme administrative pe care se bazează dispozițiile administrative (nu interese generale, indirecte și abstracte ale publicului) ([312]). Persoanele fizice au un astfel de interes juridic în cazul oricărei încălcări a limitărilor și garanțiilor care se aplică colectării datelor lor cu caracter personal în scopul asigurării respectării dreptului penal (în temeiul unor legi specifice sau al PIPA). În temeiul Legii privind contenciosul administrativ, o instanță poate decide să revoce sau să modifice o dispoziție ilegală, să pronunțe o constatare a nulității (și anume, constatarea faptului că dispoziția nu are efect juridic sau inexistența sa în ordinea juridică) sau să pronunțe o constatare că omisiunea este ilegală ([313]). O hotărâre definitivă în temeiul Legii privind contenciosul administrativ este obligatorie pentru părți ([314]).

([303]) De exemplu, dacă, în mod excepțional, NHRC nu este în măsură să inspecteze anumite materiale sau instalații deoarece acestea se referă la secrete de stat care ar putea avea un efect semnificativ asupra securității statului sau a relațiilor diplomatice ori dacă inspecția ar reprezenta un obstacol major în calea unei anchete penale sau a unui proces în curs și dacă acest lucru împiedică NHRC să efectueze ancheta necesară pentru a evalua temeinicia petiției primite, va informa persoana în cauză cu privire la motivele pentru care plângerea a fost respinsă, în conformitate cu articolul 39 din Legea NHRC. În acest caz, persoana în cauză ar putea contesta decizia NHRC în temeiul Legii privind contenciosul administrativ.

([304]) A se vedea, de exemplu, Hotărârea Înaltei Curți de la Seul 2007Nu27259 din 18 aprilie 2008, confirmată prin Hotărârea Curții Supreme 2008Du7854 din 9 octombrie 2008; Hotărârea Înaltei Curți de la Seul 2017Nu69382 din 2 februarie 2018.

([305]) A se vedea anexa II secțiunea 2.4.3.

([306]) Articolul 417 din CPA coroborat cu articolul 414 alineatul (2) din CPA. A se vedea, de asemenea, Hotărârea Curții Supreme nr. 97Mo66 din 29 septembrie 1997.

([307]) Legea privind contenciosul administrativ se referă la o „dispoziție", și anume la exercitarea sau refuzul de a exercita prerogative de autoritate publică într-un caz specific.

([308]) În temeiul Legii privind contenciosul administrativ, aceasta se referă la incapacitatea prelungită a unei agenții administrative de a adopta o anumită dispoziție contrară unei obligații legale în acest sens.

([309]) O cale de atac administrativă poate fi introdusă mai întâi în fața comisiilor administrative de apel instituite în cadrul anumitor autorități publice (de exemplu, NIS, NHRC) sau în fața Comisiei administrative centrale de apel instituite în cadrul Comisiei pentru combaterea corupției și drepturile civile [articolul 6 din Legea privind căile de atac administrative și articolul 18 alineatul (1) din Legea privind contenciosul administrativ], ca o cale de atac mai informală. Cu toate acestea, o plângere poate fi introdusă direct în fața instanțelor coreene în temeiul Legii privind contenciosul administrativ.

([310]) Hotărârea Curții Supreme 98Du18435, 22 octombrie 1999, Hotărârea Curții Supreme 99Du1113, 8 septembrie 2000, și Hotărârea Curții Supreme 2010Du3541, 27 septembrie 2012.

([311]) Articolele 12, 35 și 36 din Legea privind contenciosul administrativ. În plus, o cerere de revocare/modificare a unei dispoziții și o cerere de declarare a ilegalității unei omisiuni trebuie depuse în termen de 90 de zile de la data la care persoana a luat cunoștință de dispoziție/omisiune și, în principiu, nu mai târziu de un an de la data emiterii dispoziției sau a apariției omisiunii, cu excepția cazului în care există motive justificabile [articolul 20 și articolul 38 alineatul (2) din Legea privind contenciosul administrativ]. Noțiunea de „motive justificabile" a fost interpretată în sens larg de Curtea Supremă și presupune să se evalueze dacă este acceptabil din punct de vedere social să se permită depunerea unei plângeri tardive, având în vedere toate circumstanțele cauzei (Hotărârea Curții Supreme 90Nu6521 din 28 iunie 1991). Astfel cum a confirmat guvernul coreean în secțiunea 2.4.3 din anexa II, aceasta include (dar nu se limitează la) motivele pentru care partea în cauză nu poate fi considerată răspunzătoare (și anume, situații care se află în afara controlului reclamantului, de exemplu în cazul în care nu i-a fost notificată colectarea informațiilor sale cu caracter personal) sau cazurile de forță majoră (de exemplu, un dezastru natural, război).

([312]) Hotărârea Curții Supreme nr. 2006Du330 din 26 martie 2006.

([313]) Articolele 2 și 4 din Legea privind contenciosul administrativ.

([314]) Articolul 30 alineatul (1) din Legea privind contenciosul administrativ.

(182) Pe lângă contestarea acțiunii guvernului prin intermediul litigiilor administrative, persoanele fizice pot, de asemenea, să depună o plângere constituțională la Curtea Constituțională cu privire la orice încălcare a drepturilor lor fundamentale ca urmare a exercitării sau neexercitării competenței guvernamentale (cu excepția hotărârilor instanțelor) ([315]). Dacă sunt disponibile alte căi de atac, acestea trebuie mai întâi epuizate. În conformitate cu jurisprudența Curții Constituționale, cetățenii străini pot depune o plângere constituțională în măsura în care drepturile lor fundamentale sunt recunoscute în temeiul Constituției coreene (a se vedea explicațiile de la secțiunea 1.1) ([316]). Curtea Constituțională poate invalida exercitarea competenței guvernamentale care a cauzat încălcarea sau poate confirma că o anumită omisiune de a acționa este neconstituțională ([317]). În acest caz, autoritatea competentă este obligată să ia măsuri pentru a se conforma hotărârii Curții.

(183) În plus, persoanele fizice pot obține despăgubiri pentru daune în fața instanțelor coreene. În primul rând, aceasta include posibilitatea de a solicita despăgubiri pentru încălcările PIPA comise de autoritățile de asigurare a respectării dreptului penal, în conformitate cu articolul 39 (a se vedea, de asemenea, considerentul 135). La un nivel mai general, persoanele fizice pot solicita despăgubiri pentru prejudiciile cauzate de funcționarii publici în exercitarea atribuțiilor lor oficiale cu încălcarea legii, în temeiul Legii privind despăgubirile acordate de stat (a se vedea, de asemenea, considerentul 135) ([318]).

(184) Mecanismele descrise în considerentele 176-183 le oferă persoanelor vizate căi de atac administrative și judiciare eficace, permițându-le în special să își exercite drepturile, inclusiv dreptul de a avea acces la datele lor cu caracter personal sau de a obține rectificarea sau ștergerea unor astfel de date.

3.3 **Accesul și utilizarea de către autoritățile publice coreene în scopuri legate de securitatea națională**

(185) Legislația Republicii Coreea conține o serie de limitări și garanții în ceea ce privește accesul la datele cu caracter personal și utilizarea acestora în scopuri legate de securitatea națională și prevede mecanisme de supraveghere și de exercitare a unei căi de atac care sunt în concordanță cu cerințele menționate în considerentele 141-143 din prezenta decizie. Condițiile în care poate avea loc un astfel de acces și garanțiile aplicabile utilizării acestor competențe sunt evaluate în detaliu în secțiunile următoare.

3.3.1 *Temeiuri juridice, limitări și garanții*

(186) În Republica Coreea, datele cu caracter personal pot fi accesate în scopuri de securitate națională pe baza CPPA, a TBA și a Legii privind combaterea terorismului pentru protecția cetățenilor și securitatea publică (Legea privind combaterea terorismului) ([319]). Principala autoritate ([320]) cu competențe în domeniul securității naționale este Serviciul Național de Informații (NIS) ([321]). Colectarea și utilizarea datelor cu caracter personal de către NIS

([315]) Articolul 68 alineatul (1) din Legea privind Curtea Constituțională. Plângerile constituționale trebuie depuse în termen de 90 de zile de la data la care persoana respectivă a luat cunoștință de încălcare și în termen de un an de la producerea acesteia. Astfel cum s-a explicat, de asemenea, în anexa II secțiunea 2.4.3, având în vedere că procedura din Legea privind contenciosul administrativ se aplică litigiilor în temeiul Legii privind Curtea Constituțională, respectiv al articolului 40 din Legea privind Curtea Constituțională, o plângere va fi în continuare admisibilă dacă există „motive justificabile", astfel cum a fost interpretat în conformitate cu jurisprudența Curții Supreme menționată în nota de subsol 312. Dacă trebuie epuizate mai întâi alte căi de atac, o plângere constituțională trebuie depusă în termen de 30 de zile de la hotărârea definitivă în legătură cu o astfel de cale de atac (articolul 69 din Legea privind Curtea Constituțională).

([316]) Hotărârea Curții Constituționale nr. 99HeonMa194 din 29 noiembrie 2001.

([317]) Articolul 75 alineatul (3) din Legea privind Curtea Constituțională.

([318]) Articolul 2 alineatul (1) din Legea privind despăgubirile acordate de stat.

([319]) A se vedea anexa II secțiunea 3.1.

([320]) În mod excepțional, poliția și organele de urmărire penală pot, de asemenea, să colecteze informații cu caracter personal în scopuri legate de securitatea națională (a se vedea nota de subsol 327 și anexa II secțiunea 3.2.1.2). În plus, serviciul coreean de informații militare (Comandamentul de sprijin pentru securitate în domeniul apărării, înființat în cadrul Ministerului Apărării) are competențe în domeniul securității naționale. Totuși, astfel cum se explică în anexa II secțiunea 3.1, acesta este responsabil cu informațiile militare și supraveghează civilii numai dacă acest lucru este necesar pentru îndeplinirea funcțiilor sale militare. În special, poate investiga doar personalul militar, angajații civili ai armatei, persoanele care urmează programe de instruire militară, cadrele militare trecute în rezervă sau persoanele din serviciul de recrutare a cadrelor militare și prizonierii de război (articolul 1 din Legea privind instanțele militare). Atunci când colectează informații privind comunicațiile în scopuri legate de securitatea națională, Comandamentul de sprijin pentru securitate în domeniul apărării face obiectul limitărilor și garanțiilor prevăzute în CPPA și în decretul de punere în aplicare a acesteia.

([321]) Mandatul NIS este de a colecta, compila și distribui informații privind țările străine (și anume, informații generale privind tendințele și evoluțiile legate de țările străine sau activitățile actorilor statali); informații privind combaterea spionajului (inclusiv a spionajului militar și industrial), a terorismului și a activităților organizațiilor infracționale internaționale; informații privind anumite tipuri de infracțiuni îndreptate împotriva securității publice și naționale (de exemplu, insurecție internă, agresiune externă) și informații referitoare la sarcina de asigurare a securității cibernetice și de prevenire sau combatere a atacurilor și amenințărilor cibernetice [articolul 4 alineatul (2) din Legea NIS]. A se vedea, de asemenea, anexa II secțiunea 3.1.

trebuie să respecte cerințele legale relevante (inclusiv PIPA și CPPA) ([322]) și orientările generale elaborate de președintele statului și revizuite de Adunarea Națională ([323]). Ca principiu general, NIS trebuie să mențină neutralitatea politică și să protejeze libertatea și drepturile persoanelor ([324]). În plus, personalul NIS nu trebuie să abuzeze de autoritatea sa oficială pentru a obliga vreo instituție, organizație sau persoană fizică să facă ceva ce nu este obligată să facă (în temeiul legii) și nici să obstrucționeze exercitarea de către orice persoană a drepturilor sale ([325]).

3.3.1.1 Accesul la informațiile privind comunicațiile

(187) Pe baza CPPA, autoritățile publice coreene ([326]) pot colecta date de confirmare a comunicațiilor (și anume, data telecomunicațiilor, ora inițială și finală, numărul de apeluri trimise și primite, precum și numărul de abonat al celeilalte părți, frecvența utilizării, fișierele-jurnal privind utilizarea serviciilor de telecomunicații și a informațiilor de localizare, a se vedea considerentul 155) și conținutul comunicațiilor (prin intermediul măsurilor de restricționare a comunicațiilor, a se vedea considerentul 155) în scopuri de securitate națională (astfel cum se stabilește prin mandatul NIS, a se vedea nota de subsol 322 de mai sus). Aceste competențe se extind la două tipuri de informații: (1) comunicațiile în cadrul cărora una sau ambele părți sunt cetățeni coreeni ([327]) și (2) comunicațiile a) țărilor ostile Republicii Coreea, b) agenților străine, grupurilor sau cetățenilor suspectați de implicare în activități anticoreene ([328]) sau c) membrilor grupurilor care operează în Peninsula Coreeană, dar care depășesc efectiv suveranitatea Republicii Coreea și grupurile lor umbrelă cu sediul în țări străine ([329]). Prin urmare, comunicațiile persoanelor din UE transferate din Uniune către Republica Coreea pe baza prezentei decizii pot fi colectate în temeiul CPPA numai în scopuri legate de securitatea națională (sub rezerva condițiilor prevăzute în considerentele 188-192) în cazul în care fie au loc între o persoană din UE și un cetățean coreean, fie, în cazul în care se referă exclusiv la comunicațiile dintre persoane de altă cetățenie decât cea coreeană, se încadrează în una dintre cele trei categorii menționate la punctele 2a), b) și c).

(188) În ambele scenarii, colectarea datelor de confirmare a comunicațiilor poate avea loc numai în scopul prevenirii amenințărilor la adresa securității naționale ([330]), în timp ce măsurile de restricționare a comunicațiilor pot fi luate numai atunci când există un risc major pentru securitatea națională, iar colectarea este necesară pentru a preveni acest risc ([331]). În plus, conținutul comunicațiilor poate fi accesat numai ca măsură de ultimă instanță și trebuie depuse eforturi pentru a reduce la minimum încălcarea confidențialității comunicațiilor ([332]), asigurându-se astfel că aceasta rămâne proporțională cu obiectivul de securitate națională urmărit. Colectarea atât a conținutului comunicațiilor, cât și a datelor de confirmare a comunicațiilor se poate desfășura numai pe o perioadă maximă de patru luni și trebuie întreruptă imediat dacă obiectivul urmărit este atins mai devreme ([333]). În cazul în care condițiile relevante continuă să fie îndeplinite, perioada poate fi prelungită, cu autorizarea prealabilă a unei instanțe (pentru măsurile descrise în considerentul 189) sau a președintelui statului (pentru măsurile descrise în considerentul 190) ([334]), cu până la patru luni.

(189) Aceleași garanții procedurale se aplică colectării datelor de confirmare a comunicațiilor și conținutului comunicațiilor ([335]). În special, în cazul în care cel puțin una dintre persoanele implicate în comunicații este cetățean coreean, serviciul de informații trebuie să depună o cerere scrisă la biroul procurorului general, care, la rândul său,

([322]) A se vedea, de asemenea, articolele 14, 22 și 23 din Legea NIS.
([323]) Articolul 4 alineatul (2) din Legea NIS.
([324]) Articolul 3 alineatul (1), articolul 6 alineatul (2), articolul 11 și articolul 21 din Legea NIS. A se vedea, de asemenea, normele privind conflictele de interese, în special articolele 10 și 12 din Legea NIS.
([325]) Articolul 13 din Legea privind NIS.
([326]) Printre acestea se numără serviciile de informații (și anume, NIS și Comandamentul de sprijin pentru securitate în domeniul apărării) și poliția/organele de urmărire penală.
([327]) Articolul 7 alineatul (1) punctul 1 din CPPA.
([328]) Astfel cum a explicat guvernul coreean în nota de subsol 244 din anexa II, aceasta se referă la activități care reprezintă o amenințare pentru existența și siguranța națiunii, ordinea democratică sau supraviețuirea și libertatea poporului.
([329]) Articolul 7 alineatul (1) punctul 2 din CPPA.
([330]) Articolul 13-4 din CPPA.
([331]) Articolul 7 alineatul (1) din CPPA.
([332]) Articolul 3 alineatul (2) din CPPA. În plus, măsurile de restricționare a comunicațiilor trebuie să înceteze imediat după ce nu mai sunt necesare, asigurându-se astfel că orice încălcare a secretelor comunicațiilor unei persoane este limitată la minimum (articolul 2 din Decretul de punere în aplicare a CPPA).
([333]) Articolul 7 alineatul (2) din CPPA.
([334]) Cererea de obținere a aprobării pentru extinderea măsurilor de supraveghere trebuie formulată în scris, precizând motivele pentru care se solicită prelungirea și furnizând materiale justificative [articolul 7 alineatul (2) din CPPA și articolul 5 din Decretul de punere în aplicare a CPPA].
([335]) A se vedea articolul 13-4 alineatul (2) din CPPA și articolul 37 alineatul (4) din Decretul de punere în aplicare a CPPA, conform cărora procedurile aplicabile colectării conținutului comunicațiilor se aplică și colectării datelor de confirmare a comunicațiilor. A se vedea, de asemenea, anexa II secțiunea 3.2.1.1.1.

trebuie să solicite un mandat din partea președintelui Înaltei Curți ([336]). CPPA enumeră informațiile care trebuie furnizate în cererea adresată procurorului, în cererea de mandat și în mandatul propriu-zis, care includ, în special, justificarea cererii și principalele motive de suspiciune, materiale justificative, precum și informații privind obiectivul, ținta [și anume persoana (persoanele) vizată (vizate)], domeniul de aplicare și durata măsurii propuse ([337]). Colectarea fără mandat poate avea loc numai dacă există un act de asociere infracțională care amenință securitatea națională și există o situație de urgență care face imposibilă parcurgerea procedurilor menționate anterior ([338]). Totuși, și în acest caz, o cerere de emitere a unui mandat trebuie depusă imediat după luarea măsurii ([339]). Prin urmare, CPPA definește în mod clar domeniul de aplicare și condițiile acestor tipuri de colectare și le supune unor garanții (procedurale) specifice (inclusiv autorizarea judiciară prealabilă), ceea ce asigură că utilizarea unor astfel de măsuri este limitată la ceea ce este necesar și proporțional. În plus, cerința de a furniza informații detaliate atât în cererea de mandat, cât și în mandatul propriu-zis exclude posibilitatea unui acces arbitrar.

(190) În cazul comunicațiilor dintre persoanele care au altă cetățenie decât cea coreeană care se încadrează în una dintre cele trei categorii specifice enumerate în considerentul 187, trebuie depusă o cerere la directorul NIS, care, după o examinare a caracterului adecvat al măsurilor propuse, trebuie să solicite aprobarea scrisă prealabilă din partea președintelui Republicii Coreea ([340]). Cererea pregătită de serviciul de informații trebuie să includă aceleași informații detaliate ca o cerere de emitere a unui mandat adresată unei instanțe (a se vedea considerentul 189), în special cu privire la justificarea cererii și la principalele motive de suspiciune, materiale justificative și informații privind obiectivele, persoana (persoanele) vizată (vizate), domeniul de aplicare și durata măsurilor propuse ([341]). În situații de urgență ([342]), trebuie obținută aprobarea prealabilă din partea ministrului în subordinea căruia se află serviciul de informații relevant, deși serviciul de informații trebuie să solicite aprobarea președintelui statului imediat după luarea măsurilor de urgență ([343]). Tot în ceea ce privește colectarea comunicațiilor exclusiv între persoane de altă cetățenie decât cea coreeană, CPPA limitează, prin urmare, utilizarea unor astfel de măsuri la ceea ce este necesar și proporțional, delimitând în mod clar categoriile limitate de persoane care pot face obiectul unor astfel de măsuri și stabilind criterii detaliate pe care serviciile de informații trebuie să le demonstreze pentru a justifica o cerere de colectare de informații. În plus, din nou, aceasta exclude posibilitatea unui acces arbitrar. Deși nu există o aprobare independentă prealabilă a unor astfel de măsuri, supravegherea independentă este asigurată *ex post*, în special de PIPC și NHRC (a se vedea, de exemplu, considerentele 199-200).

(191) În plus, CPPA impune mai multe garanții suplimentare care contribuie la supravegherea *ex post* și facilitează accesul persoanelor la căi de atac eficace. În primul rând, în ceea ce privește orice tip de colectare în scopuri legate de securitatea națională, CPPA prevede cerințe diferite de ținere a evidențelor și de raportare. În special, atunci când solicită cooperarea operatorilor privați, serviciile de informații trebuie să prezinte mandatul judecătoresc/autorizarea prezidențială sau o copie a copertei unei declarații privind cenzura de urgență, pe care entitatea obligată trebuie să o păstreze în dosarele sale ([344]). În cazul în care operatorii privați sunt obligați să coopereze,

([336]) Articolul 6 alineatele (5) și (8) și articolul 7 alineatul (1) punctul 1 și alineatul (3) din CPPA, coroborate cu articolul 7 alineatele (3)-(4) din Decretul de punere în aplicare a CPPA.

([337]) A se vedea articolul 7 alineatul (3) și articolul 6 alineatul (4) din CPPA (pentru cererea din partea serviciului de informații), articolul 4 din Decretul de punere în aplicare a CPPA (pentru cererea procurorului) și articolul 7 alineatul (3) și articolul 6 alineatul (6) din CPPA (pentru mandat).

([338]) Articolul 8 din CPPA.

([339]) Articolul 8 alineatele (2) și (8) din CPPA. Colectarea trebuie întreruptă imediat în cazul în care nu se obține autorizarea instanței în termen de 36 de ore de la momentul în care sunt luate măsurile. În cazurile în care supravegherea este finalizată într-un termen scurt, eliminând astfel necesitatea obținerii unei autorizări din partea instanței, șeful biroului procurorului general competent trebuie să trimită o notificare privind măsura de urgență pregătită de serviciul de informații președintelui instanței competente, care, pe această bază, poate examina legalitatea colectării [articolul 8 alineatele (5) și (7) din CPPA]. Această notificare trebuie să indice obiectivul, ținta, domeniul de aplicare, perioada, locul de executare și metoda de supraveghere, precum și motivele pentru care nu s-a depus o cerere înainte de luarea măsurii [articolul 8 alineatul (6) din CPPA]. La un nivel mai general, serviciile de informații pot lua măsuri de urgență numai în conformitate cu o „declarație privind cenzura/interceptarea comunicațiilor de urgență” și trebuie să țină evidența acestor măsuri [articolul 8 alineatul (4) din CPPA].

([340]) Articolul 8 alineatele (1) și (2) din Decretul de punere în aplicare a CPPA.

([341]) Articolul 8 alineatul (3) din Decretul de punere în aplicare a CPPA coroborat cu articolul 6 alineatul (4) din CPPA.

([342]) Și anume, atunci când, în cazurile în care măsura vizează un act de asociere infracțională care amenință securitatea națională, nu există suficient timp pentru a obține aprobarea președintelui statului, iar neadoptarea unor măsuri de urgență poate afecta securitatea națională [articolul 8 alineatul (8) din CPPA].

([343]) Articolul 8 alineatul (9) din CPPA. Colectarea trebuie întreruptă imediat dacă autorizarea nu se obține în termen de 36 de ore de la momentul depunerii cererii.

([344]) Articolul 9 alineatul (2) din CPPA și articolul 12 din Decretul de punere în aplicare a CPPA. A se vedea articolul 13 din Decretul de punere în aplicare a CPPA privind posibilitatea de a impune obligații privind asistența oficiilor poștale și a furnizorilor de servicii de telecomunicații. Operatorii privați cărora li se solicită să dezvăluie informații pot refuza acest lucru atunci când mandatul/autorizația sau declarația privind cenzura de urgență se referă la un identificator eronat (de exemplu, un număr de telefon ce aparține altei persoane decât cea identificată). În orice caz, acestora le este interzis să divulge parolele utilizate pentru comunicații [articolul 9 alineatul (4) din CPPA].

atât autoritatea publică solicitantă, cât și operatorul relevant trebuie să țină evidențe privind scopul și obiectul măsurilor, precum și data executării ([345]). În plus, serviciile de informații trebuie să prezinte directorului NIS un raport cu privire la informațiile pe care le-au colectat și la rezultatul activității de supraveghere ([346]).

(192) În al doilea rând, persoanele fizice trebuie să fie informate cu privire la colectarea datelor lor (date de confirmare a comunicațiilor sau conținutul comunicațiilor) în scopuri legate de securitatea națională atunci când se referă la comunicații în cadrul cărora cel puțin una dintre părți este cetățean coreean ([347]). Această notificare trebuie transmisă în scris în termen de 30 de zile de la data la care s-a încheiat colectarea (inclusiv în cazul în care datele au fost obținute în conformitate cu procedura de urgență) și poate fi amânată numai dacă și atât timp cât ar pune în pericol securitatea națională sau ar dăuna vieții și siguranței fizice a persoanelor respective ([348]). Indiferent de această notificare, persoanele fizice pot obține despăgubiri prin diferite căi, astfel cum se explică în detaliu în secțiunea 3.3.4.

3.3.1.2 Colectarea de informații privind persoanele suspectate de terorism

(193) Legea privind combaterea terorismului prevede că NIS poate colecta date privind persoanele suspectate de terorism ([349]) în conformitate cu limitările și garanțiile prevăzute în alte legi ([350]). În special, NIS poate obține date privind comunicațiile (în temeiul CPPA) și alte informații cu caracter personal (printr-o cerere de divulgare voluntară) ([351]). În ceea ce privește colectarea informațiilor privind comunicațiile (și anume, conținutul comunicațiilor sau datele de confirmare a comunicațiilor), se aplică limitările și garanțiile descrise în secțiunea 3.3.1.1, inclusiv cerința de a obține un mandat aprobat de instanță. În ceea ce privește cererile de divulgare voluntară a altor tipuri de date cu caracter personal ale persoanelor suspectate de terorism, NIS trebuie să respecte cerințele prevăzute în Constituție și în PIPA cu privire la necesitate și proporționalitate (a se vedea considerentul 164) ([352]). Operatorii care primesc astfel de cereri pot respecta în mod voluntar condițiile prevăzute în PIPA (de exemplu, în conformitate cu principiul reducerii la minimum a datelor și prin limitarea impactului asupra vieții private a persoanei) ([353]). În acest caz, ei trebuie, de asemenea, să respecte cerința de notificare a persoanei în cauză în urma Notificării nr. 2021-5 (a se vedea considerentul 166).

([345]) Pentru măsurile de restricționare a comunicațiilor, aceste evidențe trebuie păstrate timp de trei ani; a se vedea articolul 9 alineatul (3) din CPPA și articolul 17 alineatul (2) din Decretul de punere în aplicare a CPPA. În ceea ce privește datele de confirmare a comunicațiilor, serviciile de informații trebuie să țină evidența faptului că a fost depusă o cerere pentru astfel de date, precum și a cererii scrise în sine și a instituției care s-a bazat pe aceasta [articolul 13 alineatul (5) și articolul 13-4 alineatul (3) din CPPA]. Furnizorii de servicii de telecomunicații trebuie să păstreze evidențe timp de șapte ani și să prezinte de două ori pe an Ministerului Științei și TIC un raport cu privire la frecvența acestor divulgări [articolul 9 alineatul (3) din CPPA coroborat cu articolul 13 alineatul (7) din CPPA și cu articolul 37 alineatul (4) și articolul 39 din Decretul de punere în aplicare a CPPA].

([346]) Articolul 18 alineatul (3) din Decretul de punere în aplicare a CPPA.

([347]) Articolul 9-2 alineatul (3) și articolul 13-4 din CPPA. Notificarea trebuie să menționeze (1) faptul că informațiile au fost colectate, (2) agenția executantă și (3) perioada de executare.

([348]) Articolul 9-2 alineatul (4) din CPPA. În acest caz, notificarea trebuie transmisă în termen de 30 de zile de la încetarea motivelor de amânare; a se vedea articolul 13-4 alineatul (2) și articolul 9-2 alineatul (6) din CPPA.

([349]) Și anume, membri ai unei grupări teroriste [astfel cum au fost desemnați de Organizația Națiunilor Unite; a se vedea articolul 2 alineatul (2) din Legea privind combaterea terorismului]; persoane care promovează și difuzează idei sau tactici ale unei grupări teroriste, colectează sau contribuie la fonduri destinate terorismului sau se implică în alte activități de pregătire, asociere infracțională, propagandă sau instigare la terorism; sau persoane despre care există motive întemeiate să suspecteze că au desfășurat astfel de activități [articolul 2 alineatul (3) din Legea privind combaterea terorismului]. Termenul „terorism" este definit la articolul 2 alineatul (1) din Legea privind combaterea terorismului ca fiind un comportament menit să împiedice exercitarea autorității statului, a unei administrații locale sau a unui guvern străin (inclusiv, a unei organizații internaționale) sau menit să îl/o oblige să acționeze fără a avea o obligație juridică în acest sens ori să amenințe publicul. Un astfel de comportament poate include, de exemplu, uciderea, răpirea persoanelor sau luarea de ostatici; deturnarea/sechestrarea, distrugerea sau deteriorarea unei nave sau aeronave; utilizarea de arme biochimice, explozive sau incendiare cu intenția de a provoca moartea, vătămări grave sau daune; și utilizarea abuzivă a materialelor nucleare sau radioactive.

([350]) Articolul 9 alineatele (1) și (3) din Legea privind combaterea terorismului.

([351]) Deși Legea privind combaterea terorismului se referă, de asemenea, la posibilitatea de a colecta informații cu privire la intrarea și ieșirea din Republica Coreea în baza Legii privind imigrația și a Legii vamale, aceste legi nu prevăd în prezent o astfel de posibilitate (a se vedea secțiunea 3.2.2.1 din anexa II). În orice caz, acestea nu s-ar aplica, în principiu, datelor transferate în baza prezentei decizii, deoarece ar privi, de regulă, informațiile care ar fi colectate direct de către autoritățile coreene (mai degrabă decât accesul la datele care au fost transferate anterior din Uniune către operatori coreeni). În plus, Legea privind combaterea terorismului menționează ARUSFTI ca temei juridic pentru colectarea de informații privind tranzacțiile financiare. Cu toate acestea, astfel cum se explică în nota de subsol 200, tipurile de date care ar putea fi obținute în baza acestei legi nu intră în domeniul de aplicare al prezentei decizii. În cele din urmă, Legea privind combaterea terorismului prevede, de asemenea, că NIS poate colecta informații de localizare prin intermediul unor cereri fără caracter obligatoriu, caz în care furnizorii informațiilor de localizare ar putea divulga în mod voluntar astfel de informații în condițiile prevăzute în PIPA (astfel cum se descrie în considerentul 193) și în Legea privind informațiile de localizare. Cu toate acestea, astfel cum s-a explicat și în nota de subsol 17, informațiile de localizare nu ar fi transferate din Uniune către operatorii coreeni pe baza prezentei decizii, ci ar fi mai degrabă generate în interiorul Coreei.

([352]) A se vedea anexa II secțiunea 3.2.2.2.

([353]) A se vedea articolul 58 alineatul (4) din PIPA, care prevede că informațiile cu caracter personal sunt prelucrate în măsura minimă necesară pentru atingerea scopului preconizat, și articolul 3 alineatul (6) din PIPA, care prevede că informațiile cu caracter personal trebuie prelucrate într-un mod care să reducă la minimum posibilitatea de a se aduce atingere vieții private a persoanei. A se vedea, de asemenea articolul 59 punctele 2 și 3 din PIPA, potrivit cărora operatorilor le este interzis să divulge informații cu caracter personal unor terți fără autoritate.

3.3.1.3 Cereri de divulgare voluntară a datelor privind abonații

(194) În temeiul TBA, furnizorii de servicii de telecomunicații pot divulga în mod voluntar date privind abonații (a se vedea considerentul 163) la cererea unui serviciu de informații care intenționează să colecteze astfel de informații pentru a preveni o amenințare la adresa securității naționale ([354]). În ceea ce privește astfel de cereri din partea NIS, se aplică aceleași limitări (care decurg din Constituție, PIPA și TBA) ca și în domeniul asigurării respectării dreptului penal, astfel cum se prevede în considerentul 164 ([355]). Furnizorii de servicii de telecomunicații nu sunt obligați să se conformeze și pot face acest lucru numai în condițiile prevăzute în PIPA (în special în conformitate cu principiul reducerii la minimum a datelor și prin limitarea impactului asupra vieții private a persoanei; a se vedea, de asemenea, considerentul 193). Se aplică aceleași cerințe în ceea ce privește ținerea evidenței și notificarea persoanei în cauză ca și în domeniul asigurării respectării dreptului penal (a se vedea considerentele 165 și 166).

3.3.2 *Utilizarea ulterioară a informațiilor colectate*

(195) Prelucrarea datelor cu caracter personal colectate de autoritățile coreene în scopuri legate de securitatea națională se supune principiilor limitării scopului [articolul 3 alineatele (1)-(2) din PIPA], legalității și echității prelucrării [articolul 3 alineatul (1) din PIPA], proporționalității/reducerii la minimum a datelor [articolul 3 alineatele (1) și (6) și articolului 58 din PIPA], exactității [articolul 3 alineatul (3) din PIPA], transparenței [articolul 3 alineatul (5) din PIPA], securității [articolul 58 alineatul (4) din PIPA] și limitării stocării [articolul 58 alineatul (4) din PIPA] ([356]). O eventuală dezvăluire a datelor cu caracter personal către terți (inclusiv țări terțe) poate avea loc numai în conformitate cu aceste principii (în special limitarea scopului și reducerea la minimum a datelor), după ce s-a evaluat conformitatea cu principiile necesității și proporționalității [articolul 37 alineatul (2) din Constituție] și luând în considerare impactul asupra drepturilor persoanelor în cauză [articolul 3 alineatul (6) din PIPA].

(196) În ceea ce privește conținutul comunicațiilor și datele de confirmare a comunicațiilor, CPPA limitează și mai mult utilizarea acestor date la procedurile judiciare, în cazul în care o parte la comunicații le invocă în cadrul unei cereri de despăgubiri; sau utilizările permise în temeiul altor legi ([357]).

3.3.3 *Supravegherea*

(197) Activitățile autorităților naționale coreene de securitate sunt supravegheate de diferite organisme ([358]).

(198) În primul rând, Legea privind combaterea terorismului prevede mecanisme de supraveghere specifice pentru activitățile de combatere a terorismului, inclusiv colectarea de date privind persoanele suspectate de terorism. În special, la nivelul executivului, activitățile de combatere a terorismului sunt supravegheate de Comisia de combatere a terorismului ([359]), căreia directorul NIS trebuie să îi raporteze cu privire la investigațiile și urmărirea suspecților de terorism în vederea colectării de informații sau de materiale necesare pentru activitățile de combatere a terorismului ([360]). În plus, responsabilul cu protecția drepturilor omului (HRPO) supraveghează în mod specific conformitatea activităților de combatere a terorismului cu drepturile fundamentale ([361]). HRPO este numit de președintele Comisiei de combatere a terorismului din rândul persoanelor care îndeplinesc anumite calificări enumerate în Decretul de punere în aplicare a Legii privind combaterea terorismului ([362]) pentru un mandat de doi ani (cu posibilitate de reînnoire) și poate fi revocat din funcție doar din motive specifice, limitate și întemeiate ([363]). În exercitarea funcției sale de supraveghere, HRPO poate emite recomandări generale pentru

([354]) Articolul 83 alineatul (3) din TBA.
([355]) A se vedea, de asemenea, anexa II secțiunea 3.2.3.
([356]) A se vedea anexa II secțiunea 1.2.
([357]) Articolul 5 alineatele (1)-(2), articolul 12 și articolul 13-5 din CPPA.
([358]) A se vedea anexa II secțiunea 3.3.
([359]) Articolul 5 alineatul (3) din Legea privind combaterea terorismului. Comisia este prezidată de prim-ministru și este compusă din mai mulți miniștri și șefi ai agențiilor guvernamentale, cum ar fi miniștrii afacerilor externe, justiției, apărării naționale și internelor și siguranței, directorul NIS și comisarul general al Agenției Naționale de Poliție [articolul 3 alineatul (1) din Decretul de punere în aplicare a Legii privind combaterea terorismului].
([360]) Articolul 9 alineatul (4) din Legea privind combaterea terorismului.
([361]) Articolul 7 din Legea privind combaterea terorismului.
([362]) Și anume, orice persoană calificată drept avocat, cu experiență profesională de cel puțin zece ani sau cu cunoștințe de specialitate în domeniul drepturilor omului și care ocupă sau a ocupat (cel puțin) funcția de conferențiar timp de cel puțin zece ani sau care a ocupat funcția de înalt funcționar public în cadrul agențiilor de stat sau al administrațiilor locale sau care are cel puțin zece ani de experiență profesională în domeniul drepturilor omului, de exemplu într-o organizație neguvernamentală [articolul 7 alineatul (1) din Decretul de punere în aplicare a Legii privind combaterea terorismului].
([363]) De exemplu, atunci când este pus sub acuzare într-un dosar penal legat de îndatoririle sale, atunci când a divulgat informații confidențiale sau din cauza unei incapacități psihice sau fizice pe termen lung [articolul 7 alineatul (3) din Decretul de punere în aplicare a Legii privind combaterea terorismului].

îmbunătățirea protecției drepturilor omului ([364]) și recomandări specifice de măsuri de remediere în cazul în care s-a constatat o încălcare a drepturilor omului ([365]). Autoritățile publice au obligația de a informa HRPO cu privire la măsurile luate ca urmare a recomandărilor sale ([366]).

(199) În al doilea rând, PIPC supraveghează respectarea de către autoritățile naționale de securitate a normelor privind protecția datelor, care includ atât dispozițiile aplicabile ale PIPA (a se vedea considerentul 149), cât și limitările și garanțiile care se aplică în cazul colectării de date cu caracter personal în temeiul altor legi (CPPA, Legea privind combaterea terorismului și TBA, a se vedea, de asemenea, considerentul 171) ([367]). În exercitarea acestui rol de supraveghere, PIPC poate face uz de toate competențele sale de investigare și de remediere, astfel cum sunt descrise în detaliu în secțiunea 2.4.2.

(200) În al treilea rând, activitățile autorităților naționale de securitate fac obiectul supravegherii independente a NHRC, în conformitate cu procedurile descrise în considerentul 172 ([368]).

(201) În al patrulea rând, funcția de supraveghere a BAI se extinde și la autoritățile naționale de securitate, deși NIS poate, în circumstanțe excepționale, să refuze furnizarea anumitor informații sau materiale, și anume atunci când acestea constituie secrete de stat, iar publicarea lor ar avea un impact grav asupra securității naționale ([369]).

(202) În cele din urmă, supravegherea parlamentară a activităților NIS este asigurată de Adunarea Națională (prin intermediul unei comisii specializate pentru informații) ([370]). CPPA stabilește un rol specific de supraveghere pentru Adunarea Națională în ceea ce privește utilizarea măsurilor de restricționare a comunicațiilor în scopuri legate de securitatea națională ([371]). În special, Adunarea Națională poate efectua inspecții la fața locului ale echipamentelor de interceptare a comunicațiilor și poate solicita atât NIS, cât și operatorilor de telecomunicații care au dezvăluit conținutul comunicațiilor să prezinte un raport în acest sens. Adunarea Națională își poate îndeplini, de asemenea, funcțiile generale de supraveghere (în conformitate cu procedurile descrise în considerentul 174). Legea NIS prevede că directorul NIS trebuie să răspundă fără întârziere atunci când Comisia pentru informații solicită un raport privind o chestiune specifică ([372]), cu norme specifice pentru anumite informații deosebit de sensibile. În mod concret, directorul NIS poate refuza să răspundă sau să depună mărturie în fața Comisiei numai în circumstanțe excepționale, și anume dacă cererea se referă la secrete de stat care vizează chestiuni militare, diplomatice sau legate de Coreea de Nord, în cazul cărora cunoștințele publice ar putea avea un impact grav asupra „destinului național" al țării ([373]). În acest caz, Comisia pentru informații poate solicita o explicație din partea prim-ministrului și, dacă nu se oferă nicio explicație în termen de șapte zile, răspunsul sau mărturia nu poate fi refuzat(ă).

3.3.4 *Măsuri reparatorii*

(203) De asemenea, în domeniul securității naționale, sistemul coreean oferă diferite căi (judiciare) pentru a obține despăgubiri, inclusiv despăgubiri pentru daune. Aceste mecanisme le oferă persoanelor vizate căi de atac administrative și judiciare eficace care le permit, în special, să își exercite drepturile, inclusiv dreptul de a avea acces la datele lor cu caracter personal sau de a obține rectificarea sau ștergerea acestor date.

(204) În primul rând, în temeiul articolului 3 alineatul (5) și al articolului 4 alineatele (1), (3) și (4) din PIPA, persoanele fizice își pot exercita drepturile de acces, rectificare, ștergere și suspendare în fața autorităților naționale de securitate. Secțiunea 6 din Notificarea nr. 2021-5 (anexa I la prezenta decizie) clarifică și mai mult modul în care aceste drepturi se aplică în contextul prelucrării datelor în scopuri de securitate națională. În special, o autoritate națională de securitate poate limita sau refuza exercitarea dreptului numai în măsura în care și atât timp cât este necesar și proporțional pentru a proteja un obiectiv important de interes public (de exemplu, în măsura

([364]) Articolul 8 alineatul (1) din Decretul de punere în aplicare a Legii privind combaterea terorismului.
([365]) Articolul 9 alineatul (1) din Decretul de punere în aplicare a Legii privind combaterea terorismului. HRPO decide în mod autonom cu privire la adoptarea recomandărilor, dar trebuie să prezinte un raport cu aceste recomandări președintelui Comisiei pentru combaterea terorismului.
([366]) Articolul 9 alineatul (2) din Decretul de punere în aplicare a Legii privind combaterea terorismului. Potrivit expunerii oficiale a guvernului coreean, nepunerea în aplicare a unei recomandări a HRPO ar fi înaintată Comisiei de combatere a terorismului, inclusiv prim-ministrului, deși, până în prezent, nu au existat cazuri în care recomandările HRPO să nu fie puse în aplicare (a se vedea secțiunea 3.3.1 din anexa II).
([367]) Anexa II secțiunea 3.3.4.
([368]) În special în ceea ce privește NIS, NHRC a efectuat în trecut investigații *ex officio* și a gestionat o serie de plângeri individuale. A se vedea, de exemplu, raportul anual pe 2018 al NHRC, p. 128 (disponibil adresa https://www.humanrights.go.kr/site/program/board/basicboard/view?menuid=002003003001&pagesize=10&boardtypeid=7017&boardid=7604746) și raportul anual pe 2019 al NHRC, p. 70 (disponibil la adresa https://www.humanrights.go.kr/site/program/board/basicboard/view?menuid=002003003001&pagesize=10&boardtypeid=7017&boardid=7606217).
([369]) Articolul 13 alineatul (1) din Legea NIS.
([370]) Articolul 36 și articolul 37 alineatul (1) punctul 15 din Legea privind Adunarea Națională.
([371]) Articolul 15 din CPPA.
([372]) Articolul 15 alineatul (2) din Legea NIS.
([373]) Articolul 17 alineatul (2) din Legea NIS. „Secretele de stat" sunt definite ca fapte, bunuri sau cunoștințe (clasificate) care nu sunt divulgate niciunei alte țări sau organizații pentru a se evita orice dezavantaj grav pentru siguranța națională și la care se permite doar un acces limitat. A se vedea articolul 13 alineatul (4) din Legea NIS.

în care și atât timp cât acordarea dreptului ar pune în pericol o investigație în curs sau ar amenința securitatea națională) sau în cazul în care acordarea dreptului poate aduce atingere vieții sau integrității fizice a unui terț. Prin urmare, invocarea unei astfel de restricții necesită o echilibrare a drepturilor și intereselor individuale în raport cu interesul public relevant și nu poate, în niciun caz, să afecteze substanța dreptului [articolul 37 alineatul (2) din Constituție]. În cazul în care cererea este respinsă sau restricționată, persoanei în cauză trebuie să i se comunice motivele fără întârziere.

(205) În al doilea rând, persoanele fizice au dreptul de a obține reparații în temeiul PIPA în cazul în care datele lor au fost prelucrate de o autoritate națională de securitate cu încălcarea PIPA sau a limitărilor și garanțiilor prevăzute de alte legi care reglementează colectarea datelor cu caracter personal (în special CPPA; a se vedea considerentul 171) ([374]). Acest drept poate fi exercitat printr-o plângere adresată PIPC (inclusiv prin intermediul Centrului de intermediere telefonică privind protecția vieții private gestionat de Agenția coreeană pentru internet și securitate) ([375]). În plus, pentru a facilita accesul la căi de atac împotriva autorităților naționale coreene din domeniul securității, cetățenii UE pot depune o plângere la PIPC prin intermediul autorității lor naționale pentru protecția datelor ([376]). În acest caz, PIPC va informa persoana în cauză prin intermediul autorității naționale pentru protecția datelor după încheierea investigației (inclusiv, dacă este cazul, cu informații cu privire la măsurile de remediere impuse). În temeiul Legii privind contenciosul administrativ, persoanele fizice pot, de asemenea, să formuleze un recurs/să conteste deciziile sau lipsa de acțiune a PIPC (a se vedea considerentul 132).

(206) În al treilea rând, persoanele fizice pot depune o plângere la HRPO cu privire la încălcarea dreptului lor la viață privată/la protecția datelor în contextul activităților de combatere a terorismului (și anume, în temeiul Legii privind combaterea terorismului) ([377]), care poate recomanda măsuri de remediere. Întrucât nu există cerințe de admisibilitate în fața HRPO, o plângere va fi tratată chiar dacă persoana în cauză nu poate demonstra că a fost într-adevăr vătămată (de exemplu din cauza presupusei colectări ilegale a datelor sale de către o autoritate națională de securitate) ([378]). Autoritatea competentă trebuie să informeze HRPO cu privire la orice măsuri luate pentru punerea în aplicare a recomandărilor sale.

(207) În al patrulea rând, persoanele fizice pot depune o plângere la NHRC cu privire la colectarea datelor lor de către autoritățile naționale de securitate și pot obține reparații în conformitate cu procedura descrisă în considerentul 178 ([379]).

(208) În cele din urmă, sunt disponibile diferite căi de atac judiciare ([380]), care le permit persoanelor fizice să invoce limitările și garanțiile descrise în secțiunea 3.3.1 pentru a obține reparații. În special, persoanele fizice pot contesta legalitatea acțiunilor autorităților naționale de securitate în temeiul Legii privind contenciosul administrativ (în conformitate cu procedura descrisă în considerentul 181 sau cu Legea privind Curtea Constituțională (a se vedea considerentul 182). În plus, acestea pot obține despăgubiri pentru daune în temeiul Legii privind despăgubirile acordate de stat (astfel cum se descrie mai detaliat în considerentul 183).

4. **CONCLUZII**

(209) Comisia consideră că Republica Coreea – prin intermediul PIPA, al normelor speciale aplicabile anumitor sectoare (astfel cum sunt analizate în secțiunea 2) și al garanțiilor suplimentare prevăzute în Notificarea nr. 2021-5 (anexa I) – asigură un nivel de protecție a datelor cu caracter personal transferate din Uniunea Europeană care este în esență echivalent cu cel garantat de Regulamentul (UE) 2016/679.

(210) În plus, Comisia consideră că, în ansamblu, mecanismele de supraveghere și căile de atac prevăzute în legislația coreeană permit detectarea și abordarea în practică a încălcărilor normelor de protecție a datelor de către operatorii din Coreea 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.

([374]) Articolul 58 alineatul (4) și articolul 4 alineatul (5) din PIPA. A se vedea anexa II secțiunea 3.4.2.
([375]) Articolul 62 și articolul 63 alineatul (2) din PIPA.
([376]) Notificarea nr. 2021-5 (secțiunea 6 din anexa I).
([377]) Articolul 8 alineatul (1) punctul 2 din Decretul de punere în aplicare a Legii privind combaterea terorismului.
([378]) A se vedea anexa II secțiunea 3.4.1.
([379]) De exemplu, NHRC primește în mod regulat plângeri împotriva Serviciului Național de Informații; a se vedea cifrele din raportul anual pe 2019 al NHRC privind numărul de plângeri primite între 2015 și 2019, p. 70 (disponibil la adresa https://www.humanrights.go.kr/site/program/board/basicboard/view?menuid=002003003001&pagesize=10&boardtypeid=7017&boardid=7606217).
([380]) A se vedea anexa II secțiunea 3.4.4.

(211) În fine, pe baza informațiilor disponibile privind ordinea juridică coreeană, inclusiv expunerile, asigurările și angajamentele guvernului coreean cuprinse în anexa II, Comisia consideră că orice ingerință în interesul public, în special în scopuri de asigurare a respectării dreptului penal și de securitate națională, din partea autorităților publice coreene în drepturile fundamentale ale persoanelor ale căror date cu caracter personal sunt transferate din Uniunea Europeană către Republica Coreea se va limita la ceea ce este strict necesar pentru atingerea obiectivului legitim în cauză și că există o protecție juridică eficace împotriva unei astfel de ingerințe.

(212) Prin urmare, având în vedere constatările prezentei decizii, ar trebui să se decidă că Republica Coreea asigură un nivel adecvat de protecție în sensul articolului 45 din Regulamentul (UE) 2016/679, interpretat în lumina Cartei drepturilor fundamentale a Uniunii Europene, pentru datele cu caracter personal transferate din Uniunea Europeană către Republica Coreea, către operatori de date cu caracter personal din Republica Coreea care fac obiectul PIPA, cu excepția organizațiilor religioase, în măsura în care prelucrează date cu caracter personal pentru activitățile lor misionare; a partidelor politice, în măsura în care prelucrează date cu caracter personal în contextul numirii candidaților, și a operatorilor care fac obiectul supravegherii de către Comisia pentru servicii financiare în ceea ce privește prelucrarea informațiilor cu caracter personal privind creditele în temeiul Legii privind informațiile privind creditele, în măsura în care prelucrează astfel de informații.

5. EFECTELE PREZENTEI DECIZII ȘI ACȚIUNILE AUTORITĂȚILOR PENTRU PROTECȚIA DATELOR

(213) 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, anulate în cadrul unei acțiuni în anulare sau declarate nule ca urmare a unei trimiteri preliminare sau a unei excepții de nelegalitate.

(214) 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 special, transferurile de la un operator sau de la o persoană împuternicită de operator din Uniune către operatori din Republica Coreea pot avea loc fără a fi necesară obținerea unei autorizări suplimentare.

(215) Ar trebui reamintit faptul că, în temeiul articolului 58 alineatul (5) din Regulamentul (UE) 2016/679 și astfel cum este explicat de Curtea de Justiție în hotărârea pronunțată în cauza Schrems ([381]), 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 poate fi obligată să efectueze o trimitere preliminară către Curtea de Justiție ([382]).

6. MONITORIZAREA ȘI REVIZUIREA PREZENTEI DECIZII

(216) În conformitate cu jurisprudența Curții de Justiție ([383]) 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 țara terță 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.

(217) Prin urmare, Comisia ar trebui să monitorizeze în permanență situația din Republica Coreea 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 coreene a expunerilor, asigurărilor și angajamentelor cuprinse în anexa II. Pentru a facilita acest proces, autoritățile coreene sunt invitate să informeze cu promptitudine Comisia cu privire la evoluțiile semnificative relevante pentru prezenta decizie în ceea ce privește prelucrarea datelor cu caracter personal de către operatorii economici și autoritățile publice, precum și cu privire la limitările și garanțiile aplicabile accesului autorităților publice la datele cu caracter personal.

([381]) Schrems, punctul 65.

([382]) 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".

([383]) Schrems, punctul 76.

(218) 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, 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 de date din Republica Coreea. De asemenea, Comisia ar trebui să fie informată cu privire la orice indiciu potrivit căruia acțiunile autorităților publice coreene 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.

(219) În conformitate cu articolul 45 alineatul (3) din Regulamentul (UE) 2016/679 ([384]) și având în vedere faptul că nivelul de protecție asigurat de ordinea juridică coreeană 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 Republica Coreea sunt în continuare justificate în fapt și în drept.

(220) În acest scop, prezenta decizie ar trebui să facă obiectul unei prime revizuiri în termen de trei ani de la intrarea sa în vigoare. În urma acestei prime revizuiri și în funcție de rezultatul acesteia, Comisia va decide, consultându-se îndeaproape cu comitetul instituit în temeiul articolului 93 alineatul (1) din Regulamentul (UE) 2016/679, dacă ciclul de trei ani trebuie menținut. În orice caz, revizuirile ulterioare ar trebui să aibă loc cel puțin o dată la patru ani ([385]). Revizuirea ar trebui să acopere toate aspectele legate de funcționarea prezentei decizii, în special aplicarea garanțiilor suplimentare prevăzute în anexa I la prezenta decizie, acordând o atenție deosebită protecției aplicate în cazul transferurilor ulterioare; evoluțiile relevante ale jurisprudenței; normele privind prelucrarea informațiilor pseudonimizate în scopuri statistice, de cercetare științifică și de arhivare în interes public, precum și aplicarea excepțiilor prevăzute la articolul 28 alineatul (7) PIPA; eficacitatea exercitării drepturilor individuale, inclusiv înainte de recent reformata PIPC, și aplicarea excepțiilor de la aceste drepturi; aplicarea exceptărilor parțiale prevăzute de PIPA; precum și limitările și garanțiile în ceea ce privește accesul guvernului (astfel cum se prevede în anexa II la prezenta decizie), inclusiv cooperarea PIPC cu autoritățile UE din domeniul protecției datelor cu privire la plângerile depuse de persoanele fizice. Revizuirea ar trebui să acopere, de asemenea, eficacitatea supravegherii și a asigurării respectării legislației, în ceea ce privește PIPA și în domeniul asigurării respectării dreptului penal, precum și în domeniul securității naționale (în special de către PIPC și NHRC).

(221) Pentru a efectua această revizuire, Comisia ar trebui să se reunească cu PIPC, însoțit, dacă este cazul, de alte autorități coreene 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. În cadrul revizuirii, Comisia ar trebui să solicite PIPC 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 ([386]). 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 coreene sau de alte părți interesate din Coreea, de Comitetul european pentru protecția datelor, de diferite autorități 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.

(222) Pe baza revizuirii, Comisia ar trebui să pregătească un raport public care trebuie să fie prezentat Parlamentului European și Consiliului.

7. **SUSPENDAREA, ABROGAREA SAU MODIFICAREA PREZENTEI DECIZII**

(223) În cazul în care informațiile disponibile, în special informațiile care rezultă din monitorizarea prezentei decizii sau cele furnizate de autoritățile coreene sau ale statelor membre, arată că nivelul de protecție oferit de Republica Coreea ar putea să nu mai fie adecvat, Comisia ar trebui să informeze cu promptitudine autoritățile coreene competente în acest sens și să solicite luarea unor măsuri adecvate într-un termen rezonabil specificat.

(224) În cazul în care, la expirarea termenului specificat, autoritățile coreene competente nu iau măsura respectivă sau nu demonstrează în mod satisfăcător că prezenta decizie continuă să se bazeze pe un nivel adecvat de protecție, Comisia va iniția procedura menționată la articolul 93 alineatul (2) din Regulamentul (UE) 2016/679 în vederea suspendării sau abrogării parțiale sau integrale a prezentei decizii.

(225) Ca alternativă, Comisia va iniția această procedură în vederea modificării 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 în continuare un nivel adecvat de protecție.

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

([385]) 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.

([386]) A se vedea anexa II la prezenta decizie.

(226) Mai precis, Comisia ar trebui să inițieze procedura de suspendare sau de abrogare în cazul în care există indicii potrivit cărora garanțiile 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 coreene nu respectă expunerile, asigurările și angajamentele cuprinse în anexa II la prezenta decizie.

(227) 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 sau într-un alt context, autoritățile coreene competente nu furnizează informațiile sau clarificările necesare pentru evaluarea nivelului de protecție acordat datelor cu caracter personal transferate din Uniunea Europeană către Republica Coreea sau în ceea ce privește respectarea prezentei decizii. În această privință, Comisia ar trebui să ia în considerare măsura în care informațiile relevante pot fi obținute din alte surse.

(228) Din motive imperioase de urgență justificate corespunzător, Comisia va face uz de posibilitatea de a adopta, în conformitate cu procedura menționată la articolul 93 alineatul (3) din Regulamentul (UE) 2016/679, acte de punere în aplicare imediat aplicabile de suspendare, abrogare sau modificare a deciziei.

8. **CONSIDERAȚII FINALE**

(229) Comitetul european pentru protecția datelor și-a publicat avizul ([387]), care a fost luat în considerare la pregătirea prezentei decizii.

(230) Măsurile prevăzute în prezenta decizie sunt conforme cu avizul comitetului instituit în temeiul articolului 93 alineatul (1) din Regulamentul (UE) 2016/679,

ADOPTĂ PREZENTA DECIZIE:

Articolul 1

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

(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) organizații religioase, în măsura în care prelucrează date cu caracter personal pentru activitățile lor misionare;

(b) partide politice, în măsura în care prelucrează date cu caracter personal în contextul numirii candidaților;

(c) entități care fac obiectul supravegherii de către Comisia pentru servicii financiare în ceea ce privește prelucrarea informațiilor cu caracter personal privind creditele în temeiul Legii privind informațiile referitoare la credite, în măsura în care prelucrează astfel de informații.

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 în ceea ce privește transferurile de date care intră în domeniul de aplicare prevăzut la articolul 1 din prezenta decizie, 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 care se exercită drepturile individuale și în care autoritățile publice coreene au acces la datele transferate în temeiul prezentei decizii, pentru a evalua dacă Republica Coreea continuă să asigure un nivel adecvat de protecție în sensul articolului 1.

([387]) Avizul 32/2021 privind Proiectul de decizie de punere în aplicare a Comisiei Europene în temeiul Regulamentului (UE) 2016/679 privind protecția adecvată a datelor cu caracter personal în Republica Coreea, disponibil la următoarea adresă: https://edpb.europa.eu/our-work-tools/our-documents/opinion-art-70/opinion-322021-regarding-european-commission-draft_en.

(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 coreeană 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 coreene 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 trei 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 realizate împreună cu autoritățile coreene relevante.

(5) În cazul în care Comisia dispune de indicii potrivit cărora nu mai este asigurat un nivel adecvat de protecție, aceasta informează autoritățile competente din Coreea. Dacă este necesar, Comisia poate decide să suspende, să modifice sau să abroge prezenta decizie ori poate limita domeniul de aplicare al acesteia, în conformitate cu articolul 45 alineatul (5) din Regulamentul (UE) 2016/679, în special în cazul în care există indicii potrivit cărora:

(a) operatorii din Coreea care au primit date cu caracter personal din Uniunea Europeană în temeiul prezentei decizii nu respectă garanțiile suplimentare prevăzute în anexa I sau supravegherea și asigurarea respectării legislației în această privință sunt insuficiente;

(b) autoritățile publice coreene nu respectă expunerile, asigurările și angajamentele cuprinse în anexa II, inclusiv în ceea ce privește condițiile și limitările privind colectarea datelor cu caracter personal transferate în temeiul prezentei decizii și accesul autorităților publice coreene la aceste date în scopuri de asigurare a respectării dreptului penal sau de securitate națională.

Comisia poate, de asemenea, să adopte astfel de măsuri în cazul în care lipsa de cooperare a autorităților coreene împiedică Comisia să stabilească dacă Republica Coreea continuă să asigure un nivel adecvat de protecție.

Articolul 4

Prezenta decizie se adresează statelor membre.

Adoptată la Bruxelles, 17 decembrie 2021.

Pentru Comisie
Didier REYNDERS
Membru al Comisiei

ANEXA I

NORME SUPLIMENTARE PENTRU INTERPRETAREA ȘI APLICAREA LEGII PRIVIND PROTECȚIA INFORMAȚIILOR CU CARACTER PERSONAL REFERITOARE LA PRELUCRAREA DATELOR CU CARACTER PERSONAL TRANSFERATE CĂTRE COREEA

Cuprins

I. Prezentare generală 54

II. Definițiile termenilor 55

III. Norme suplimentare 55

1. Limitarea utilizării în afara scopului și furnizarea de informații cu caracter personal (articolele 3, 15 și 18 din lege) 55

2. Limitarea transferului ulterior de date cu caracter personal [articolul 17 alineatele (3) și (4), articolul 18 din lege] 57

3. Notificare privind datele în cazul în care datele cu caracter personal nu au fost obținute de la persoana vizată (articolul 20 din lege) 58

4. Domeniul de aplicare al exceptării speciale pentru prelucrarea informațiilor pseudonimizate (articolele 28-2, 28-3, 28-4, 28-5, 28-6 și 28-7, articolul 3 și articolul 58-2 din lege) 60

5. Măsuri de remediere etc. [articolul 64 alineatele (1), (2) și (4) din lege] 61

6. Aplicarea PIPA pentru prelucrarea datelor cu caracter personal în scopuri legate de securitatea națională, inclusiv investigarea încălcărilor și punerea în aplicare în conformitate cu PIPA (articolul 7-8, articolul 7-9, articolul 58, articolul 3, articolul 4 și articolul 62 din PIPA) 62

I. **Prezentare generală**

Coreea și Uniunea Europeană (denumită în continuare „UE") s-au angajat în discuții privind caracterul adecvat al nivelului de protecție, în urma cărora Comisia Europeană a stabilit că Coreea garantează un nivel adecvat de protecție a datelor cu caracter personal în conformitate cu articolul 45 din RGPD.

În acest context, Comisia pentru protecția informațiilor cu caracter personal a adoptat această notificare în baza articolului 5 (Obligațiile statului etc.) și a articolului 14 (Cooperarea internațională) ([1]) din Legea privind protecția informațiilor cu caracter personal pentru a clarifica interpretarea, aplicarea și asigurarea respectării anumitor dispoziții ale legii, inclusiv în ceea ce privește prelucrarea datelor cu caracter personal transferate către Coreea în baza deciziei UE privind caracterul adecvat al nivelului de protecție.

Întrucât această notificare are statutul de normă administrativă pe care agenția administrativă competentă o stabilește și o anunță pentru a clarifica standardele de interpretare, aplicare și executare a Legii privind protecția informațiilor cu caracter personal în sistemul juridic din Coreea, ea are forță juridică obligatorie pentru operatorul de informații cu caracter personal, în sensul că orice încălcare a notificării poate fi considerată o încălcare a dispozițiilor relevante ale PIPA. În plus, în cazul în care drepturile și interesele personale sunt încălcate ca urmare a nerespectării notificării, persoanele relevante au dreptul de a obține reparații de la Comisia pentru protecția informațiilor cu caracter personal sau în instanță.

În consecință, în cazul în care operatorul de informații cu caracter personal, care prelucrează informațiile cu caracter personal transferate către Coreea în conformitate cu decizia UE privind caracterul adecvat al nivelului de protecție, nu ia măsuri conforme cu această notificare, se va aprecia că „există motive temeinice pentru a considera că a avut loc o încălcare în ceea ce privește informațiile cu caracter personal, iar neluarea de măsuri poate cauza prejudicii dificil de remediat", în temeiul articolului 64 alineatele (1) și (2) din lege. În astfel de cazuri, Comisia pentru protecția informațiilor cu caracter personal sau agențiile administrative centrale asociate pot dispune ca operatorul relevant de informații cu

([1]) Articolul 14 din Legea privind protecția informațiilor cu caracter personal prevede autoritatea guvernului coreean de a institui politici de îmbunătățire a nivelului de protecție a informațiilor cu caracter personal în mediul internațional și de prevenire a încălcării drepturilor persoanelor vizate ca urmare a transferului transfrontalier de informații cu caracter personal.

caracter personal să ia măsuri de remediere etc. în conformitate cu autoritatea conferită de această dispoziție și, în funcție de anumite încălcări ale legii, pot fi impuse, de asemenea, sancțiuni corespunzătoare (sancțiuni, amenzi administrative etc.).

II. **Definițiile termenilor**

Definițiile termenilor utilizați în documentul de față sunt următoarele:

(i) Lege: Legea privind protecția informațiilor cu caracter personal (Legea nr. 16930, modificată la 4 februarie 2020 și pusă în aplicare la 5 august 2020).

(ii) Decret prezidențial: Decretul de punere în aplicare a Legii privind protecția informațiilor cu caracter personal (Decretul prezidențial nr. 30509, 3 martie 2020, de modificare a altor legi).

(iii) Persoană vizată: o persoană care poate fi identificată din informațiile prelucrate astfel încât să devină obiectul informațiilor respective.

(iv) Operator de informații cu caracter personal: o instituție publică, persoană juridică, organizație, persoană fizică etc. care prelucrează informații cu caracter personal în mod direct sau indirect, ca parte a activităților sale;

(v) UE: UE (la sfârșitul lunii februarie 2020, 27 de țări membre [2], inclusiv Belgia, Germania, Franța, Italia, Luxemburg, Țările de Jos, Danemarca, Irlanda, Grecia, Portugalia, Spania, Austria, Finlanda, Suedia, Cipru, Republica Cehă, Estonia, Ungaria, Letonia, Lituania, Malta, Polonia, Slovacia, Slovenia, România, Bulgaria și Croația), precum și țările asociate la UE prin Acordul privind SEE (Islanda, Liechtenstein, Norvegia).

(vi) RGPD: legislația generală a UE privind protecția informațiilor cu caracter personal, Regulamentul general privind protecția datelor [Regulamentul (UE) 2016/679].

(vii) Decizie privind caracterul adecvat al nivelului de protecție: în conformitate cu articolul 45 alineatul (3) din RGPD, Comisia Europeană a decis că o țară terță, un teritoriu al unei țări terțe, unul sau mai multe sectoare sau o organizație internațională asigură un nivel adecvat de protecție a informațiilor cu caracter personal.

III. **Norme suplimentare**

1. **Limitarea utilizării în afara scopului și furnizarea de informații cu caracter personal (articolele 3, 15 și 18 din lege)**

<Legea privind protecția informațiilor cu caracter personal

(Legea nr. 16930, modificată parțial la 4 februarie 2020)>

Articolul 3 (Principii privind protecția informațiilor cu caracter personal) (1) Operatorul de informații cu caracter personal specifică în mod explicit scopurile în care sunt prelucrate informațiile cu caracter personal și colectează informații cu caracter personal în mod legal și echitabil, în măsura minimă necesară în acest scop.

(2) Operatorul de informații cu caracter personal prelucrează informațiile cu caracter personal într-un mod adecvat, necesar scopurilor în care sunt prelucrate informațiile cu caracter personal și nu le utilizează în afara acestor scopuri.

Articolul 15 (Colectarea și utilizarea informațiilor cu caracter personal) (1) Un operator de informații cu caracter personal poate colecta informații cu caracter personal în oricare dintre următoarele situații și le poate utiliza în scopul colectării:

1. în cazul în care se obține consimțământul persoanei vizate;

2. în cazul în care există dispoziții speciale în legislație sau este inevitabil pentru respectarea obligațiilor legale;

3. în cazul în care este inevitabil pentru îndeplinirea de către o instituție publică a atribuțiilor care intră în domeniul său de competență, astfel cum prevede legea etc.;

4. în cazul în care este inevitabil necesar pentru executarea și îndeplinirea unui contract cu o persoană vizată;

[2] Până la încheierea perioadei de tranziție, aceasta include și Regatul Unit, astfel cum se prevede la articolele 126, 127 și 132 din Acordul privind retragerea Regatului Unit al Marii Britanii și Irlandei de Nord din Uniunea Europeană și din Comunitatea Europeană a Energiei Atomice (2019/C 384 I/01).

5. în cazul în care se consideră că este în mod evident necesar pentru protejarea vieții, a integrității fizice sau a intereselor patrimoniale ale persoanei vizate sau ale unui terț împotriva unui pericol iminent, atunci când persoana vizată sau reprezentantul său legal nu este în măsură să își exprime intenția sau nu se poate obține consimțământul prealabil din cauza unor adrese necunoscute etc.;

6. în cazul în care este necesar în interesul justificabil al unui operator de informații cu caracter personal, care este în mod evident superior drepturilor persoanei vizate. În astfel de cazuri, prelucrarea este permisă numai în măsura în care este legată în mod substanțial de interesul justificabil al operatorului de informații cu caracter personal și nu depășește un domeniu de aplicare rezonabil.

Articolul 18 (Limitarea utilizării în afara scopului și furnizarea informațiilor cu caracter personal) (1) Un operator de informații cu caracter personal nu va utiliza informațiile cu caracter personal în afara domeniului de aplicare prevăzut la articolul 15 alineatul (1) și la articolul 39-3 alineatele (1) și (2) și nu le va furniza niciunui terț în afara domeniului de aplicare prevăzut la articolul 17 alineatele (1) și (3).

(2) Fără a aduce atingere alineatului (1), în cazul în care se aplică oricare dintre următoarele paragrafe, un operator de informații cu caracter personal poate utiliza informațiile cu caracter personal sau le poate furniza unui terț în alte scopuri, cu excepția cazului în care acest lucru este de natură să încalce în mod abuziv interesele unei persoane vizate sau ale unui terț: furnizorii respectivi de servicii de informații și comunicații [astfel cum se prevede la articolul 2 alineatul (1) punctul 3 din Legea privind promovarea utilizării rețelelor de informații și comunicații și protecția informațiilor etc.; în continuare se aplică aceleași dispoziții] care prelucrează informații cu caracter personal ale utilizatorilor [astfel cum se prevede la articolul 2 alineatul (1) punctul 4 din Legea privind promovarea utilizării rețelelor de informații și comunicații și protecția informațiilor etc.; în continuare se aplică aceleași dispoziții] fac doar obiectul dispozițiilor de la paragrafele 1 și 2, iar paragrafele 5-9 se aplică numai instituțiilor publice:

1. în cazul în care se obține un consimțământ suplimentar din partea persoanei vizate;

2. în cazul în care există alte dispoziții speciale în legislație;

3. în cazul în care se consideră că este în mod evident necesar pentru protecția vieții, a integrității fizice sau a intereselor patrimoniale ale persoanei vizate sau ale unui terț împotriva unui pericol iminent, în cazul în care persoana vizată sau reprezentantul său legal nu este în măsură să își exprime intenția sau nu se poate obține consimțământul prealabil din cauza unor adrese necunoscute;

4. șters;<prin Legea nr. 16930, 4 februarie 2020>

5. în cazul în care este imposibil să îndeplinească atribuțiile care intră în domeniul său de competență, astfel cum prevede orice lege, cu excepția cazului în care operatorul de informații cu caracter personal utilizează informațiile cu caracter personal în alt scop decât cel preconizat sau le furnizează unui terț și face obiectul deliberării și rezoluției Comisiei;

6. în cazul în care este necesar să se furnizeze informații cu caracter personal unui guvern sau unei organizații internaționale străine în vederea executării unui tratat sau a unei alte convenții internaționale;

7. în cazul în care este necesar pentru investigarea unei infracțiuni, punerea sub acuzare și urmărirea penală;

8. în cazul în care este necesar pentru ca o instanță să își exercite atribuțiile în materie de proceduri judiciare;

9. în cazul în care este necesar pentru executarea pedepsei, eliberarea condiționată și reținere.

[alineatele (3)-(4) au fost omise]

(5) În cazul în care un operator de informații cu caracter personal furnizează informații cu caracter personal unui terț în alt scop decât cel prevăzut la alineatul (2), operatorul de informații cu caracter personal solicită destinatarului informațiilor cu caracter personal să limiteze scopul și metoda de utilizare și alte aspecte necesare sau să pregătească garanțiile necesare pentru a asigura siguranța informațiilor cu caracter personal. În astfel de cazuri, persoana care primește o astfel de solicitare ia măsurile necesare pentru a asigura siguranța informațiilor cu caracter personal.

(i) Alineatele (1) și (2) ale articolului 3 din lege prevăd principiul conform căruia un operator de informații cu caracter personal trebuie să colecteze numai informațiile cu caracter personal minime necesare în scopul prelucrării legale și legitime a informațiilor cu caracter personal și nu ar trebui să le utilizeze în alte scopuri decât cele preconizate ([3]).

(ii) În conformitate cu acest principiu, articolul 15 alineatul (1) din lege prevede că, atunci când un operator de informații cu caracter personal colectează informații cu caracter personal, acestea pot fi utilizate în scopul colectării, iar articolul 18 alineatul (1) prevede că informațiile cu caracter personal nu ar trebui utilizate în afara scopului colectării sau furnizate unui terț.

([3]) Întrucât aceste dispoziții stabilesc principii generale care se aplică oricărei prelucrări de informații cu caracter personal, inclusiv în cazul în care o astfel de prelucrare este reglementată în mod specific de alte legi, clarificările din această secțiune se aplică și în cazul în care datele cu caracter personal sunt prelucrate în temeiul altor legi [a se vedea, de exemplu, articolul 15 alineatul (1) din Legea privind informațiile referitoare la credite, care se referă în mod specific la aceste dispoziții].

(iii) De asemenea, chiar dacă informațiile cu caracter personal pot fi utilizate în alte scopuri decât cel preconizat sau pot fi furnizate unui terț în cazurile excepționale ([4]) descrise în paragrafele articolului 18 alineatul (2) din lege, trebuie să se solicite restricționarea scopului sau a metodei de utilizare, astfel încât informațiile cu caracter personal să poată fi prelucrate în condiții de siguranță, în conformitate cu alineatul (5), sau trebuie să se ia măsurile necesare pentru a asigura siguranța informațiilor cu caracter personal.

(iv) Dispozițiile de mai sus se aplică în mod egal prelucrării tuturor informațiilor cu caracter personal primite de la o țară terță în zona jurisdicției legale a Coreei, indiferent de cetățenia persoanei vizate.

(v) De exemplu, în cazul în care un operator de informații cu caracter personal din UE transferă informații cu caracter personal unui operator coreean de informații cu caracter personal în conformitate cu decizia Comisiei Europene privind caracterul adecvat al nivelului de protecție, scopul operatorului de informații cu caracter personal din UE de a transfera informațiile cu caracter personal este considerat a fi scopul operatorului coreean de informații cu caracter personal de a colecta informațiile cu caracter personal și, în astfel de cazuri, operatorul coreean de informații cu caracter personal poate utiliza aceste informații sau le poate furniza unui terț numai în scopul colectării, cu excepția cazurilor excepționale descrise la articolul 18 alineatul (2) din lege.

2. **Limitarea transferului ulterior de date cu caracter personal [articolul 17 alineatele (3) și (4), articolul 18 din lege]**

<Legea privind protecția informațiilor cu caracter personal

(Legea nr. 16930, modificată parțial la 4 februarie 2020)>

Articolul 17 (Furnizarea de informații cu caracter personal) (1) Text omis

(2) Un operator de informații cu caracter personal informează o persoană vizată cu privire la următoarele aspecte atunci când obține consimțământul prevăzut la alineatul (1) punctul 1. Aceleași dispoziții se aplică și în cazul în care se modifică oricare dintre următoarele:

1. destinatarul informațiilor cu caracter personal;
2. scopul în care destinatarul informațiilor cu caracter personal utilizează aceste informații;
3. detalii privind informațiile cu caracter personal care trebuie furnizate;
4. perioada în care destinatarul păstrează și utilizează informațiile cu caracter personal;
5. faptul că persoana vizată are dreptul de a refuza consimțământul și dezavantajele, dacă este cazul, care rezultă din refuzul consimțământului.

(3) Un operator de informații cu caracter personal informează o persoană vizată cu privire la aspectele prevăzute la alineatul (2) și obține consimțământul persoanei vizate pentru a furniza informațiile cu caracter personal unui terț în străinătate; și nu încheie un contract pentru transferul transfrontalier de informații cu caracter personal prin încălcarea legii.

(4) Un operator de informații cu caracter personal poate furniza informații cu caracter personal fără consimțământul unei persoane vizate în limitele domeniului de aplicare legate în mod rezonabil de scopurile în care au fost colectate inițial informațiile cu caracter personal, în conformitate cu aspectele prevăzute în decretul prezidențial, luând în considerare dacă se creează dezavantaje pentru persoana vizată, dacă au fost luate măsurile necesare pentru a asigura siguranța, cum ar fi criptarea etc.

※ Consultați paginile 3, 4 și 5 pentru articolul 18.

<Decretul de punere în aplicare a Legii privind protecția informațiilor cu caracter personal

([Data punerii în aplicare: 5 februarie 2021] [Decretul prezidențial nr. 30892, 4 august 2020, de modificare a altor legi])>

Articolul 14-2 (Standarde privind utilizarea/furnizarea suplimentară de informații cu caracter personal etc.)

(1) În cazul în care un operator de informații cu caracter personal utilizează sau furnizează informații cu caracter personal (acțiune denumită în continuare „utilizare sau furnizare suplimentară de informații cu caracter personal") fără consimțământul persoanei vizate în conformitate cu articolul 15 alineatul (3) din lege sau cu articolul 17 alineatul (4) din lege, operatorul de informații cu caracter personal ia în considerare următoarele aspecte:

1. dacă are legătură în mod rezonabil cu scopul inițial pentru care au fost colectate informațiile cu caracter personal;
2. dacă utilizarea sau furnizarea suplimentară de informații cu caracter personal este previzibilă având în vedere circumstanțele în care au fost colectate informațiile cu caracter personal și practicile de prelucrare;
3. dacă utilizarea sau furnizarea suplimentară de informații cu caracter personal nu aduce atingere în mod abuziv intereselor persoanei vizate; precum și
4. dacă au fost luate măsurile necesare pentru asigurarea securității, cum ar fi pseudonimizarea sau criptarea.

([4]) Furnizorii de servicii din domeniul informațiilor și comunicațiilor fac doar obiectul articolului 18 alineatul (2) paragrafele 1 și 2. Paragrafele 5-9 se aplică numai instituțiilor publice.

(2) Operatorul de informații cu caracter personal divulgă în prealabil criteriile de evaluare a aspectelor menționate la paragrafele de la alineatul (1) din politica de confidențialitate conform articolului 30 alineatul (1) din lege, iar responsabilul cu protecția vieții private, astfel cum se prevede la articolul 31 alineatul (1) din lege, verifică dacă operatorul de informații cu caracter personal utilizează sau furnizează informații cu caracter personal suplimentare în conformitate cu standardele relevante.

(i) În cazul în care operatorul de informații cu caracter personal furnizează informații cu caracter personal unui terț din străinătate, acesta trebuie să informeze în prealabil persoanele vizate cu privire la toate aspectele descrise la articolul 17 alineatul (2) din lege și să obțină consimțământul acestora, cu excepția cazurilor care intră sub incidența alineatului (1) sau (2). Nu ar trebui încheiat niciun contract cu privire la furnizarea transfrontalieră de date cu caracter personal cu încălcarea acestei legi.

(1) În cazul în care informațiile cu caracter personal sunt furnizate în limitele domeniului de aplicare legat în mod rezonabil de scopul inițial al colectării, în conformitate cu articolul 17 alineatul (4) din lege. Cu toate acestea, cazurile în care se poate aplica această dispoziție se limitează la situațiile în care sunt îndeplinite standardele privind utilizarea și furnizarea suplimentară de informații cu caracter personal, prevăzute la articolul 14-2 din decretul de punere în aplicare. În plus, operatorul de informații cu caracter personal trebuie să analizeze dacă furnizarea de informații cu caracter personal poate crea dezavantaje persoanelor vizate și dacă a luat măsurile necesare pentru asigurarea siguranței, cum ar fi criptarea.

(2) Dacă informațiile cu caracter personal pot fi furnizate unui terț în cazurile excepționale menționate la articolul 18 alineatul (2) din lege (a se vedea paginile 3~5). Cu toate acestea, chiar și în astfel de cazuri, dacă furnizarea unor astfel de informații cu caracter personal este de natură să încalce în mod abuziv interesele persoanei vizate sau ale unui terț, informațiile cu caracter personal nu pot fi furnizate unui terț. În plus, furnizorul de informații cu caracter personal trebuie să solicite destinatarului informațiilor cu caracter personal să limiteze scopul sau metoda de utilizare a informațiilor cu caracter personal sau să ia măsurile necesare pentru a asigura siguranța acestora, astfel încât informațiile cu caracter personal să poată fi prelucrate în condiții de siguranță.

(ii) În cazul în care informațiile cu caracter personal sunt furnizate unui terț din străinătate, este posibil ca acestea să nu beneficieze de nivelul de protecție garantat de Legea coreeană privind protecția informațiilor cu caracter personal din cauza diferențelor dintre sistemele de protecție a informațiilor cu caracter personal din diferite țări. În consecință, astfel de cazuri vor fi considerate „cazuri în care pot fi create dezavantaje pentru persoana vizată" menționate la articolul 17 alineatul (4) din lege sau „cazuri în care interesul unei persoane vizate sau al unui terț este încălcat în mod abuziv" menționate la articolul 18 alineatul (2) din lege și la articolul 14-2 din Decretul de punere în aplicare a aceleiași legi ([5]). Pentru a îndeplini cerințele acestor dispoziții, operatorul de informații cu caracter personal și terțul trebuie, prin urmare, să asigure în mod explicit un nivel de protecție echivalent cu cel oferit de lege, inclusiv să garanteze exercitarea de către persoana vizată a drepturilor sale în documente obligatorii din punct de vedere juridic, cum ar fi contracte, chiar și după ce informațiile cu caracter personal sunt transferate în străinătate.

3. **Notificare privind datele în cazul în care datele cu caracter personal nu au fost obținute de la persoana vizată (articolul 20 din lege)**

<Legea privind protecția informațiilor cu caracter personal

(Legea nr. 16930, modificată parțial la 4 februarie 2020)>

Articolul 20 (Notificarea privind sursele etc. informațiilor cu caracter personal colectate de la terți) (1) Atunci când un operator de informații cu caracter personal prelucrează informații cu caracter personal colectate de la terți, operatorul de informații cu caracter personal notifică imediat persoanei vizate următoarele aspecte, la cererea persoanei vizate:

1. sursa informațiilor cu caracter personal colectate;
2. scopul prelucrării informațiilor cu caracter personal;
3. faptul că persoana vizată are dreptul să solicite suspendarea prelucrării informațiilor cu caracter personal, astfel cum se prevede la articolul 37.

(2) Fără a aduce atingere alineatului (1), atunci când un operator de informații cu caracter personal care îndeplinește criteriile stabilite prin decretul prezidențial, ținând seama de tipul și cantitatea de informații cu caracter personal prelucrate, de numărul de angajați, de volumul vânzărilor etc., colectează informații cu caracter personal de la terți și le prelucrează în temeiul articolului 17 alineatul (1) punctul 1, operatorul de informații cu caracter personal notifică persoanei vizate aspectele menționate la alineatul (1): acest lucru nu se aplică în cazul în care informațiile colectate de operatorul de informații cu caracter personal nu conțin nicio informație cu caracter personal, cum ar fi datele de contact, prin care persoana vizată poate fi informată.

([5]) În temeiul articolului 18 alineatul (2) punctul 2 din PIPA, acest lucru este valabil și atunci când informațiile cu caracter personal sunt divulgate unor terți din străinătate pe baza dispozițiilor din alte legi (cum ar fi, de exemplu, Legea privind informațiile referitoare la credite).

(3) Aspectele necesare în ceea ce privește timpul, metoda și procedura de notificare a persoanei vizate în temeiul alineatului (2) teza principală sunt stabilite în decretul prezidențial.

(4) Alineatul (1) și teza principală de la alineatul (2) nu se aplică în niciuna dintre următoarele situații: acest lucru este valabil numai în cazul în care este vădit superior drepturilor persoanelor vizate în temeiul legii:

1. în cazul în care informațiile cu caracter personal care fac obiectul unei cereri de notificare sunt incluse în dosarele cu informații cu caracter personal menționate la oricare dintre paragrafele de la articolul 32 alineatul (2);
2. în cazul în care o astfel de notificare este de natură să afecteze viața sau integritatea fizică a oricărei alte persoane sau să prejudicieze în mod abuziv bunurile și alte interese ale oricărei alte persoane.

(i) Dacă operatorul de informații cu caracter personal primește informațiile cu caracter personal transferate din UE în baza deciziei sale privind caracterul adecvat al nivelului de protecție ([6]), acesta trebuie să notifice persoanei vizate următoarele informații, de la (1) la (5), fără întârzieri nejustificate și, în orice caz, în termen de cel mult o lună de la data transferului.

(1) Numele și datele de contact ale persoanelor care transferă și primesc informațiile cu caracter personal.

(2) Elementele sau categoriile de informații cu caracter personal transferate.

(3) Scopul colectării și utilizării informațiilor cu caracter personal (astfel cum au fost stabilite de exportatorul de date în conformitate cu punctul 1 din această notificare).

(4) Perioada de păstrare a informațiilor cu caracter personal.

(5) Informațiile privind drepturile persoanei vizate în ceea ce privește prelucrarea informațiilor cu caracter personal, metoda și procedura de exercitare a drepturilor și eventualele dezavantaje în cazul în care exercitarea acestora creează dezavantaje.

(ii) De asemenea, în cazul în care operatorul de informații cu caracter personal furnizează informațiile cu caracter personal de la punctul (i) unui terț din Republica Coreea sau din străinătate, acesta trebuie să notifice persoanei vizate informațiile de la (1) la (5) înainte ca acestea să fie furnizate.

(1) Numele și datele de contact ale persoanelor care furnizează și primesc informațiile cu caracter personal.

(2) Elementele sau categoriile de informații cu caracter personal furnizate.

(3) Țara în care sunt furnizate informațiile cu caracter personal, data preconizată și metoda de furnizare a acestora (limitate la cazurile în care informațiile cu caracter personal sunt furnizate unui terț în străinătate).

(4) Scopul și temeiul juridic al furnizorului de informații cu caracter personal pentru furnizarea informațiilor cu caracter personal.

(5) Informațiile privind drepturile persoanei vizate în ceea ce privește prelucrarea informațiilor cu caracter personal, metoda și procedura de exercitare a drepturilor și eventualele dezavantaje, dacă exercitarea acestora creează dezavantaje.

(iii) Operatorul de informații cu caracter personal nu poate aplica punctul (i) sau (ii) în niciunul dintre următoarele cazuri de la (1) la (4).

(1) Dacă informațiile cu caracter personal care trebuie notificate sunt incluse în oricare dintre următoarele dosare cu informații cu caracter personal menționate la articolul 32 alineatul (2) din lege, în măsura în care interesele protejate de această dispoziție sunt în mod evident superioare drepturilor persoanei vizate și numai atât timp cât notificarea ar amenința urmărirea intereselor în cauză, de exemplu periclitând anchetele penale în curs sau amenințând securitatea națională.

(2) Dacă și atât timp cât notificarea este de natură să dăuneze vieții sau integrității fizice a unei alte persoane sau să încalce în mod abuziv interesele patrimoniale ale unei alte persoane, în cazul în care aceste drepturi sau interese sunt în mod evident superioare drepturilor persoanei vizate.

(3) Dacă persoana vizată deține deja informațiile pe care operatorul de informații cu caracter personal trebuie să le comunice în conformitate cu (i) sau (ii).

(4) Dacă operatorul de informații cu caracter personal nu deține date de contact ale persoanei vizate sau dacă aceasta implică eforturi excesive pentru a contacta persoana vizată, inclusiv în contextul prelucrării, în condițiile prevăzute în secțiunea 3 din PIPA. Pentru a stabili dacă este sau nu este posibil să se contacteze persoana vizată sau dacă acest lucru implică eforturi excesive, ar trebui să se ia în considerare posibilitatea de a coopera cu exportatorul de date din UE.

([6]) Obligațiile prevăzute la punctele (i), (ii) și (iii) se aplică, de asemenea, atunci când operatorul care primește informații cu caracter personal din UE în baza deciziei privind caracterul adecvat al nivelului de protecție prelucrează astfel de informații în temeiul altor legi, cum ar fi, de exemplu, Legea privind informațiile referitoare la credite.

4. **Domeniul de aplicare al exceptării speciale pentru prelucrarea informațiilor pseudonimizate (articolele 28-2, 28-3, 28-4, 28-5, 28-6 și 28-7, articolul 3 și articolul 58-2 din lege)**

<Legea privind protecția informațiilor cu caracter personal

(Legea nr. 16930, modificată parțial la 4 februarie 2020)>

Capitolul III Prelucrarea informațiilor cu caracter personal

SECȚIUNEA 3 Cazuri speciale privind datele pseudonimizate

Articolul 28-2 (Prelucrarea datelor pseudonimizate) (1) Un operator de informații cu caracter personal poate prelucra informații pseudonimizate fără consimțământul persoanelor vizate în scopuri statistice, de cercetare științifică și de arhivare în interes public etc.

(2) Un operator de informații cu caracter personal nu include informații care pot fi utilizate pentru a identifica o anumită persoană atunci când furnizează informații pseudonimizate unui terț în conformitate cu alineatul (1).

Articolul 28-3 (Restricția privind combinarea datelor pseudonimizate) (1) Fără a aduce atingere articolului 28-2, combinarea informațiilor pseudonimizate prelucrate de diferiți operatori de informații cu caracter personal în scopuri statistice, de cercetare științifică și de păstrare a evidențelor în interes public etc. se efectuează de către o instituție specializată desemnată de Comisia pentru protecție sau de directorul agenției administrative centrale corespunzătoare.

(2) Un operator de informații cu caracter personal care intenționează să difuzeze informații combinate în afara organizației care a combinat informațiile trebuie să obțină aprobarea directorului instituției specializate după prelucrarea informațiilor în informații pseudonimizate sau în forma menționată la articolul 58-2.

(3) Aspectele necesare, inclusiv procedurile și metodele de combinare prevăzute la alineatul (1), standardele și procedurile de desemnare sau de anulare a desemnării unei instituții specializate de administrare și supraveghere, precum și standardele și procedurile de export și de aprobare în temeiul alineatului (2) sunt stabilite în decretul prezidențial.

Articolul 28-4 (Obligația de a lua măsuri de siguranță pentru datele pseudonimizate) (1) La prelucrarea informațiilor pseudonimizate, un operator de informații cu caracter personal ia măsurile tehnice, organizatorice și fizice necesare pentru stocarea și gestionarea separată a informațiilor suplimentare necesare pentru revenirea la starea inițială, după cum ar putea fi necesar pentru a asigura siguranța prevăzută în decretul prezidențial, astfel încât informațiile cu caracter personal să nu poată fi pierdute, furate, divulgate, falsificate, modificate sau deteriorate.

(2) Un operator de informații cu caracter personal care intenționează să prelucreze informațiile pseudonimizate întocmește și păstrează evidențe referitoare la aspectele prevăzute în decretul prezidențial, inclusiv la scopul prelucrării informațiilor pseudonimizate, precum și un destinatar terț atunci când sunt furnizate informații pseudonimizate, pentru a gestiona prelucrarea informațiilor pseudonimizate.

Articolul 28-5 (Interdicții privind prelucrarea informațiilor pseudonimizate) (1) Nimeni nu trebuie să prelucreze informațiile pseudonimizate în scopul identificării unei anumite persoane.

(2) Atunci când, în timpul prelucrării informațiilor pseudonimizate, sunt generate informații de identificare a unei anumite persoane, operatorul de informații cu caracter personal trebuie să înceteze prelucrarea informațiilor și să recupereze și să distrugă imediat informațiile.

Articolul 28-6 (Impunerea de suprataxe administrative pentru prelucrarea informațiilor pseudonimizate) (1) Comisia poate impune o amendă echivalentă cu mai puțin de trei sutimi din totalul vânzărilor operatorului de date care a prelucrat datele în scopul identificării unei anumite persoane cu încălcarea articolului 28-5 alineatul (1): cu condiția ca, în cazul în care nu există vânzări sau apar dificultăți în calcularea veniturilor din vânzări, operatorul de date să poată fi sancționat cu o amendă de maximum 400 de milioane de woni sau trei sutimi din valoarea capitalului, luându-se în considerare valoarea cea mai mare.

(2) Articolul 34-2 alineatele (3)-(5) se aplică *mutatis mutandis* aspectelor necesare pentru impunerea și colectarea suprataxelor administrative.

Articolul 28-7 (Domeniul de aplicare) Articolele 20, 21, 27, 34 alineatul (1), 35 - 37, 39-3, 39-4, 39-6 - 39-8 nu se aplică informațiilor pseudonimizate.

Capitolul I Dispoziții generale

Articolul 3 (Principii privind protecția informațiilor cu caracter personal) (1) Operatorul de informații cu caracter personal specifică în mod explicit scopurile în care sunt prelucrate informațiile cu caracter personal și colectează informații cu caracter personal în mod legal și echitabil, în măsura minimă necesară în acest scop.

(2) Operatorul de informații cu caracter personal prelucrează informațiile cu caracter personal într-un mod adecvat, necesar scopurilor în care sunt prelucrate informațiile cu caracter personal și nu le utilizează în afara acestor scopuri.

(3) Operatorul de informații cu caracter personal se asigură că informațiile cu caracter personal sunt exacte, complete și actualizate în măsura în care este necesar în legătură cu scopurile în care sunt prelucrate informațiile cu caracter personal.

(4) Operatorul de informații cu caracter personal gestionează informațiile cu caracter personal în condiții de siguranță, în conformitate cu metodele, tipurile etc. de prelucrare a informațiilor cu caracter personal, ținând seama de posibilitatea încălcării drepturilor persoanei vizate și de gravitatea riscurilor relevante.

(5) Operatorul de informații cu caracter personal face publică politica sa de confidențialitate și alte aspecte legate de prelucrarea informațiilor cu caracter personal; și garantează drepturile persoanei vizate, cum ar fi dreptul de acces la informațiile sale cu caracter personal.

(6) Operatorul de informații cu caracter personal prelucrează informațiile cu caracter personal astfel încât să reducă la minimum posibilitatea de a aduce atingere vieții private a unei persoane vizate.

(7) Dacă este încă posibil să se îndeplinească scopurile colectării informațiilor cu caracter personal prin prelucrarea informațiilor cu caracter personal anonimizate sau pseudonimizate, operatorul de informații cu caracter personal depune eforturi pentru a prelucra informațiile cu caracter personal prin anonimizare, în cazul în care anonimizarea este posibilă, sau prin pseudonimizare, în cazul în care scopul colectării informațiilor cu caracter personal este imposibil de îndeplinit prin anonimizare.

(8) Operatorul de informații cu caracter personal depune eforturi pentru a obține încrederea persoanelor vizate prin respectarea și îndeplinirea sarcinilor și a responsabilităților prevăzute în prezenta lege și în alte legi conexe.

Capitolul IX Dispoziții suplimentare

Articolul 58-2 (Exceptare de la aplicare) Prezenta lege nu se aplică informațiilor care nu mai identifică o anumită persoană atunci când sunt combinate cu alte informații, luând în considerare în mod rezonabil timpul, costul, tehnologia etc. <Articol nou introdus de Legea nr. 16930, 4 februarie 2020>

(i) Capitolul III secțiunea 3 Cazuri speciale privind datele pseudonimizate (articolele 28-2 – 28-7), permite prelucrarea informațiilor pseudonimizate fără consimțământul persoanei vizate în scopul elaborării de statistici, al cercetării științifice, al păstrării evidențelor publice etc. (articolul 28-2), dar, în astfel de cazuri, garanțiile și interdicțiile adecvate necesare pentru protejarea drepturilor persoanelor vizate sunt obligatorii (articolele 28-4 și 28-5), pot fi impuse suprataxe de penalizare pentru contravenienți (articolul 28-6), iar anumite garanții disponibile sub altă formă în temeiul PIPA nu se aplică (articolul 28-7).

(ii) Aceste dispoziții nu se aplică în cazurile în care informațiile pseudonimizate sunt prelucrate în alte scopuri decât elaborarea statisticilor, cercetarea științifică, păstrarea evidențelor publice etc. De exemplu, dacă informațiile cu caracter personal ale unei persoane din UE, care au fost transferate către Coreea în conformitate cu decizia Comisiei Europene privind caracterul adecvat al nivelului de protecție, sunt pseudonimizate în alte scopuri decât compilarea statisticilor, cercetarea științifică, păstrarea evidențelor publice etc., dispozițiile speciale din capitolul III secțiunea 3 nu se aplică ([7]).

(iii) În cazul în care un operator de informații cu caracter personal prelucrează informații pseudonimizate în scopul elaborării de statistici, al cercetării științifice, al păstrării registrelor publice etc. și în cazul în care informațiile pseudonimizate nu au fost distruse odată ce scopul specific al prelucrării a fost îndeplinit în concordanță cu articolul 37 din Constituție și cu articolul 3 (Principii privind protecția informațiilor cu caracter personal) din lege, acesta anonimizează informațiile pentru a se asigura că nu mai este posibilă identificarea unei anumite persoane, pe cont propriu sau în combinație cu alte informații, luând în considerare în mod rezonabil timpul, costul, tehnologia etc. în conformitate cu articolul 58-2 din PIPA.

5. **Măsuri de remediere etc. [articolul 64 alineatele (1), (2) și (4) din lege]**

<Legea privind protecția informațiilor cu caracter personal

(Legea nr. 16930, modificată parțial la 4 februarie 2020)>

Articolul 64 (Măsuri de remediere) (1) În cazul în care Comisia pentru protecție consideră că există motive temeinice pentru a considera că a avut loc o încălcare în ceea ce privește informațiile cu caracter personal, iar neluarea de măsuri poate cauza prejudicii dificil de remediat, aceasta poate dispune ca persoana care a încălcat prezenta lege (cu excepția agențiilor administrative centrale, a administrațiilor locale, a Adunării Naționale, a Curții, a Curții Constituționale și a Comisiei Electorale Naționale) să ia oricare dintre următoarele măsuri:

1. să suspende încălcarea în ceea ce privește informațiile cu caracter personal;

2. să suspende temporar prelucrarea informațiilor cu caracter personal;

([7]) În mod similar, excepția de la articolul 40-3 din Legea privind informațiile referitoare la credite se aplică numai prelucrării informațiilor pseudonimizate privind creditele în scopul elaborării de statistici, al cercetării științifice și al păstrării evidențelor publice.

3. alte măsuri necesare pentru protecția informațiilor cu caracter personal și prevenirea încălcării securității informațiilor cu caracter personal.

(2) În cazul în care directorul unei agenții administrative centrale asociate consideră că există motive temeinice pentru a considera că a avut loc o încălcare a informațiilor cu caracter personal și că neluarea de măsuri este de natură să cauzeze prejudicii dificil de remediat, acesta poate dispune ca un operator de informații cu caracter personal să ia oricare dintre măsurile prevăzute la alineatul (1) în temeiul legilor asociate sferei de competență a agenției administrative centrale respective.

(4) În cazul în care o agenție administrativă centrală, o administrație locală, Adunarea Națională, Curtea, Curtea Constituțională sau Comisia Electorală Națională încalcă prezenta lege, Comisia pentru protecție poate recomanda directorului agenției relevante să ia oricare dintre măsurile prevăzute la alineatul (1). În astfel de cazuri, la primirea recomandării, agenția se va conforma, cu excepția cazului în care există circumstanțe extraordinare.

(i) În primul rând, precedentele jurisprudențiale ([8]) ([9]) interpretează noțiunea de „prejudiciu dificil de remediat" ca fiind un caz care ar putea aduce atingere drepturilor personale sau vieții private a unei persoane.

(ii) În consecință, „un motiv întemeiat pentru a considera că a avut loc o încălcare în legătură cu informațiile cu caracter personal și că lipsa unei acțiuni este de natură să cauzeze un prejudiciu dificil de remediat", prevăzut la articolul 64 alineatele (1) și (2), se referă la cazurile în care se consideră că o încălcare a legii poate aduce atingere drepturilor și libertății persoanelor în ceea ce privește informațiile cu caracter personal. Acest lucru se va aplica ori de câte ori sunt încălcate oricare dintre principiile, drepturile și obligațiile prevăzute de legea privind protecția informațiilor cu caracter personal ([10]).

(iii) În conformitate cu articolul 64 alineatul (4) din Legea privind protecția informațiilor cu caracter personal este o măsură referitoare la „o încălcare a prezentei legi", și anume o acțiune împotriva unei încălcări a PIPA.

O agenție administrativă centrală etc., în calitate de autoritate publică supusă statului de drept, nu poate încălca nicio lege și este obligată să ia o măsură de remediere, inclusiv să oprească imediat acțiunea, și să compenseze daunele în cazul excepțional în care a fost totuși săvârșită o faptă ilegală.

În consecință, chiar și fără nicio intervenție din partea Comisiei pentru protecție în conformitate cu articolul 64 alineatul (4) din PIPA, o agenție administrativă centrală etc. trebuie să ia o măsură de remediere împotriva încălcărilor în cazul în care ia cunoștință de o încălcare a legii.

În special, în cazul în care Comisia pentru protecție a recomandat o măsură de remediere, în mod normal va fi clar în mod obiectiv pentru agenția administrativă centrală etc. că a încălcat legea. Astfel, pentru a justifica motivele pentru care consideră că nu ar trebui urmată o recomandare a Comisiei pentru protecție, o agenție administrativă centrală etc. trebuie să prezinte dovezi clare care să arate că nu a încălcat legea. Recomandarea trebuie urmată, cu excepția cazului în care Comisia pentru protecție stabilește că, într-adevăr, nu este cazul.

Având în vedere acest lucru, „circumstanțele extraordinare" de la articolul 64 alineatul (4) din Legea privind protecția informațiilor cu caracter personal trebuie să se limiteze strict la circumstanțele extraordinare în care există motive clare pentru ca agențiile administrative centrale etc. să demonstreze că „această lege nu a fost, de fapt, încălcată", cum ar fi „cazurile în care există circumstanțe extraordinare (de fapt sau de drept)" pe care Comisia pentru protecție nu le-a cunoscut atunci când a formulat inițial recomandarea, iar Comisia pentru protecție stabilește că, într-adevăr, nu a avut loc nicio încălcare.

6. **Aplicarea PIPA pentru prelucrarea datelor cu caracter personal în scopuri legate de securitatea națională, inclusiv investigarea încălcărilor și punerea în aplicare în conformitate cu PIPA (articolul 7-8, articolul 7-9, articolul 58, articolul 3, articolul 4 și articolul 62 din PIPA)**

<Legea privind protecția informațiilor cu caracter personal

(Legea nr. 16930, modificată parțial la 4 februarie 2020)>

Articolul 7-8 (Activitatea Comisiei pentru protecție) (1) Comisia pentru protecție desfășoară următoarele activități: […]

3. aspecte privind investigarea încălcării dreptului persoanelor vizate și dispozițiile care decurg din acestea;

4. tratarea plângerilor sau proceduri de remediere legate de prelucrarea informațiilor cu caracter personal și medierea litigiilor privind informațiile cu caracter personal;

[…]

([8]) (Hotărârea Curții Supreme 97Da10215,10222 din 26 ianuarie 1999) Dacă faptele penale ale acuzatului sunt dezvăluite prin intermediul presei, este probabil ca acest lucru să cauzeze prejudicii psihice și fizice ireparabile nu numai victimei, și anume reclamantului, ci și persoanelor din jurul acesteia, inclusiv familiilor.

([9]) (Hotărârea Înaltei Curți din Seul 2006Na92006 din 16 ianuarie 2008) Dacă se publică un articol defăimător, acesta ar putea aduce prejudicii grave ireparabile persoanei în cauză.

([10]) Aceleași principii precum cele prevăzute la punctul (ii) se aplică articolului 45-4 din Legea privind informațiile referitoare la credite.

Articolul 7-9 (Aspecte care fac obiectul unei decizii și al unei rezoluții a Comisiei pentru protecție) (1) Comisia pentru protecție deliberează și soluționează următoarele aspecte: […]

5. aspecte privind interpretarea și funcționarea legii referitoare la protecția informațiilor cu caracter personal;

[…]

Articolul 58 (Excluderea parțială a aplicării) (1) Capitolele III-VII nu se aplică următoarelor informații cu caracter personal:

1. informații cu caracter personal colectate în conformitate cu Legea privind statisticile pentru prelucrarea de către instituțiile publice;
2. informații cu caracter personal colectate sau a căror furnizare este solicitată pentru analiza informațiilor legate de securitatea națională;
3. informații cu caracter personal prelucrate temporar, atunci când sunt necesare urgent pentru siguranța și securitatea publică, sănătatea publică etc.;
4. informații cu caracter personal colectate sau utilizate în scopuri proprii de raportare de către presă, activitățile misionare ale organizațiilor religioase și, respectiv, nominalizarea candidaților de către partidele politice.

[alineatele (2) și (3) au fost omise]

(4) În cazul prelucrării informațiilor cu caracter personal în temeiul alineatului (1), operatorul de informații cu caracter personal prelucrează informațiile cu caracter personal în măsura minimă necesară pentru a atinge scopul preconizat în perioada minimă; de asemenea, ia măsurile necesare, cum ar fi garanții tehnice, de gestionare și fizice, gestionarea plângerilor individuale și alte măsuri necesare pentru gestionarea în siguranță și prelucrarea adecvată a acestor informații cu caracter personal.

Articolul 3 (Principii privind protecția informațiilor cu caracter personal) (1) Operatorul de informații cu caracter personal specifică în mod explicit scopurile în care sunt prelucrate informațiile cu caracter personal și colectează informații cu caracter personal în mod legal și echitabil, în măsura minimă necesară în acest scop.

(2) Operatorul de informații cu caracter personal prelucrează informațiile cu caracter personal într-un mod adecvat, necesar scopurilor în care sunt prelucrate informațiile cu caracter personal și nu le utilizează în afara acestor scopuri.

(3) Operatorul de informații cu caracter personal se asigură că informațiile cu caracter personal sunt exacte, complete și actualizate în măsura în care este necesar în legătură cu scopurile în care sunt prelucrate informațiile cu caracter personal.

(4) Operatorul de informații cu caracter personal gestionează informațiile cu caracter personal în condiții de siguranță, în conformitate cu metodele, tipurile etc. de prelucrare a informațiilor cu caracter personal, ținând seama de posibilitatea încălcării drepturilor persoanei vizate și de gravitatea riscurilor relevante.

(5) Operatorul de informații cu caracter personal face publică politica sa de confidențialitate și alte aspecte legate de prelucrarea informațiilor cu caracter personal; și garantează drepturile persoanei vizate, cum ar fi dreptul de acces la informațiile sale cu caracter personal.

(6) Operatorul de informații cu caracter personal prelucrează informațiile cu caracter personal astfel încât să reducă la minimum posibilitatea de a aduce atingere vieții private a unei persoane vizate.

(7) Dacă este încă posibil să se îndeplinească scopurile colectării de informații cu caracter personal prin prelucrarea informațiilor cu caracter personal anonimizate sau pseudonimizate, operatorul de informații cu caracter personal depune eforturi pentru a prelucra informațiile cu caracter personal prin anonimizare, în cazul în care anonimizarea este posibilă, sau prin pseudonimizare, în cazul în care scopul colectării informațiilor cu caracter personal este imposibil de îndeplinit prin anonimizare.

(8) Operatorul de informații cu caracter personal depune eforturi pentru a obține încrederea persoanelor vizate prin respectarea și îndeplinirea sarcinilor și a responsabilităților prevăzute în prezenta lege și în alte legi conexe.

Articolul 4 (Drepturile persoanelor vizate) O persoană vizată are următoarele drepturi în ceea ce privește prelucrarea propriilor informații cu caracter personal:

1. dreptul de a fi informată cu privire la prelucrarea unor astfel de informații cu caracter personal;
2. dreptul de a stabili dacă dorește sau nu să își dea consimțământul și domeniul de aplicare al consimțământului în ceea ce privește prelucrarea unor astfel de informații cu caracter personal;
3. dreptul de a confirma dacă informațiile cu caracter personal sunt prelucrate sau nu și de a solicita accesul (inclusiv furnizarea de copii; în continuare, se aplică aceleași dispoziții) pentru astfel de informații cu caracter personal;
4. dreptul de a suspenda prelucrarea acestor informații cu caracter personal și de a solicita rectificarea, ștergerea și distrugerea acestora;
5. dreptul la despăgubiri adecvate pentru orice prejudiciu care rezultă din prelucrarea unor astfel de informații cu caracter personal printr-o procedură promptă și echitabilă.

Articolul 62 (Raportare cu privire la încălcări) (1) Orice persoană care suferă o încălcare a drepturilor sau a intereselor legate de informațiile sale cu caracter personal în cursul prelucrării informațiilor cu caracter personal de către un operator de informații cu caracter personal poate raporta această încălcare Comisiei pentru protecție.

(2) Comisia pentru protecție poate desemna o instituție specializată care să primească și să gestioneze în mod eficient rapoartele privind cererile de despăgubire în temeiul alineatului (1), astfel cum se prevede în decretul prezidențial. În astfel de cazuri, o astfel de instituție specializată înființează și gestionează un centru de intermediere telefonică privind încălcarea securității informațiilor cu caracter personal (denumit în continuare „Centrul de intermediere telefonică privind protecția vieții private").

(3) Centrul de intermediere telefonică privind protecția vieții private are următoarele atribuții:

1. să primească rapoarte privind cererile de despăgubire și să organizeze consultări în legătură cu prelucrarea informațiilor cu caracter personal;
2. să investigheze și să confirme incidentele și să audieze opiniile părților afiliate;
3. atribuții conexe paragrafelor 1 și 2.

(4) Comisia pentru protecție poate, dacă este necesar, să detașeze un funcționar public din cadrul său la instituția specializată desemnată în temeiul articolului 32-4 alineatul (2) din Legea funcționarilor publici de stat, pentru a investiga și a confirma în mod eficient incidentele prevăzute la alineatul (3) punctul 2.

(i) Colectarea de informații cu caracter personal în scopuri de securitate națională este reglementată de legi specifice care împuternicesc autoritățile competente (de exemplu, Serviciul Național de Informații) să intercepteze comunicațiile sau să solicite divulgarea în anumite condiții și garanții (denumite în continuare: „legi privind securitatea națională"). Aceste legi privind securitatea națională includ, de exemplu, Legea privind protecția confidențialității comunicațiilor, Legea privind combaterea terorismului pentru protecția cetățenilor și a securității publice sau Legea privind sectorul telecomunicațiilor. În plus, colectarea și prelucrarea ulterioară a informațiilor cu caracter personal trebuie să respecte cerințele PIPA. În această privință, potrivit articolului 58 alineatul (1) punctul 2 din PIPA, capitolele III-VII nu se aplică informațiilor cu caracter personal colectate sau a căror furnizare este solicitată pentru analiza informațiilor legate de securitatea națională. Prin urmare, această excepție parțială se aplică prelucrării informațiilor cu caracter personal în scopuri legate de securitatea națională.

În același timp, capitolul I (Dispoziții generale), capitolul II (Stabilirea politicilor de protecție a informațiilor cu caracter personal etc.), capitolul VIII (Acțiuni colective în justiție pentru încălcarea securității datelor), capitolul IX (Dispoziții suplimentare) și capitolul X (Dispoziții privind sancțiunile) din PIPA se aplică prelucrării unor astfel de informații cu caracter personal. Aceasta include principiile generale de protecție a datelor prevăzute la articolul 3 (Principii privind protecția informațiilor cu caracter personal) și drepturile individuale garantate de articolul 4 din PIPA (Drepturile persoanelor vizate).

În plus, articolul 58 alineatul (4) din PIPA prevede că aceste informații trebuie prelucrate în măsura minimă necesară pentru atingerea scopului preconizat și pentru perioada minimă; în plus, acesta prevede obligația operatorului de informații cu caracter personal să instituie măsurile necesare pentru a asigura gestionarea în condiții de siguranță a datelor și prelucrarea corespunzătoare, cum ar fi garanții tehnice, de gestionare și fizice, precum și măsuri pentru tratarea corespunzătoare a plângerilor individuale.

În cele din urmă, se aplică dispozițiile care reglementează sarcinile și competențele PIPC (inclusiv articolul 60-65 din PIPA privind tratarea plângerilor și adoptarea de recomandări și măsuri de remediere), precum și dispozițiile privind sancțiunile administrative și penale (articolul 70 și următoarele din PIPA). În conformitate cu articolul 7-8 alineatul (1) punctele 3 și 4 și cu articolul 7-9 alineatul (1) punctul 5 din PIPA, aceste competențe de investigare și de remediere, inclusiv atunci când sunt exercitate în contextul tratării plângerilor, vizează, de asemenea, posibilele încălcări ale normelor cuprinse în legi specifice care stabilesc limitările și garanțiile în ceea ce privește colectarea de informații cu caracter personal, cum ar fi legile privind securitatea națională. Având în vedere cerințele de la articolul 3 alineatul (1) din PIPA privind colectarea legală și echitabilă a informațiilor cu caracter personal, o astfel de încălcare constituie o încălcare a „prezentei legi" în sensul articolelor 63 și 64, permițând PIPC să desfășoare o investigație și să ia măsuri de remediere ([11]). Exercitarea acestor competențe de către PIPC completează, dar nu înlocuiește, competențele Comisiei naționale pentru drepturile omului în temeiul Legii privind Comisia pentru drepturile omului.

Aplicarea principiilor, a drepturilor și obligațiilor fundamentale prevăzute de PIPA în ceea ce privește prelucrarea informațiilor cu caracter personal în scopuri legate de securitatea națională reflectă garanțiile consacrate în Constituție pentru protecția dreptului persoanei de a avea control asupra propriilor informații cu caracter personal. Astfel cum a fost recunoscut de către Curtea Constituțională, acesta include dreptul unei persoane ([12]) „de a decide personal când, cui sau de către cine și în ce măsură vor fi divulgate sau utilizate informațiile sale. Acesta este un drept fundamental ([13]), [...] menit să protejeze libertatea personală de decizie împotriva riscurilor cauzate de extinderea funcțiilor statului și de tehnologia informației și comunicațiilor". Orice limitare a acestui drept, de exemplu atunci când este necesar pentru protejarea securității naționale, necesită o echilibrare a drepturilor și a intereselor individuale cu interesul public relevant și nu poate afecta substanța dreptului [articolul 37 alineatul (2) din Constituție].

([11]) În ceea ce privește măsurile de remediere întreprinse în temeiul articolului 64, a se vedea, de asemenea, secțiunea 5 de mai sus.
([12]) Hotărârea Curții Constituționale, 99HunMa513, 2004HunMa190, 26 mai 2005.
([13]) Hotărârea Curții Constituționale, 2003HunMa282, 21 iulie 2005.

Prin urmare, atunci când prelucrează informații cu caracter personal în scopuri legate de securitatea națională, operatorul (de exemplu, NIS), printre altele:

(1) specifică în mod explicit scopurile în care sunt prelucrate informațiile cu caracter personal și colectează informații cu caracter personal în mod legal și echitabil, în măsura minimă necesară în acest scop [articolul 3 alineatul (1) din PIPA]; mai precis, aceasta colectează și prelucrează suplimentar informațiile cu caracter personal numai în scopul îndeplinirii sarcinilor care îi revin în temeiul legilor relevante, cum ar fi Legea privind Serviciul Național de Informații;

(2) prelucrează informațiile cu caracter personal în măsura minimă și pentru perioada minimă necesară pentru atingerea scopului preconizat [articolul 58 alineatul (4) din PIPA]; la atingerea scopului prelucrării, operatorul distruge în mod ireversibil informațiile cu caracter personal, cu excepția cazului în care păstrarea ulterioară este prevăzută în mod expres prin lege, caz în care informațiile cu caracter personal relevante sunt stocate și gestionate separat de alte informații cu caracter personal, nu sunt utilizate în alte scopuri decât cele specificate în lege și sunt distruse la sfârșitul perioadei de păstrare;

(3) prelucrează informațiile cu caracter personal în modul adecvat, necesar scopurilor în care sunt prelucrate informațiile cu caracter personal și nu le utilizează în afara acestor scopuri [articolul 3 alineatul (2) din PIPA];

(4) se asigură că informațiile cu caracter personal sunt exacte, complete și actualizate în măsura necesară în legătură cu scopurile în care sunt prelucrate informațiile cu caracter personal [articolul 3 alineatul (3) din PIPA];

(5) gestionează informațiile cu caracter personal în condiții de siguranță, în conformitate cu metodele, tipurile etc. de prelucrare a informațiilor cu caracter personal, ținând seama de posibilitatea încălcării drepturilor persoanei vizate și de gravitatea riscurilor relevante [articolul 3 alineatul (4) din PIPA];

(6) face publică politica sa de confidențialitate și alte aspecte legate de prelucrarea informațiilor cu caracter personal [articolul 3 alineatul (5) din PIPA];

(7) prelucrează informațiile cu caracter personal într-un mod care să reducă la minimum posibilitatea de încălcare a vieții private a unei persoane vizate [articolul 3 alineatul (6) din PIPA].

(ii) În conformitate cu articolul 58 alineatul (4) din PIPA, operatorul (de exemplu, autoritățile competente pentru securitatea națională, cum ar fi NIS) ia măsurile necesare, precum instituirea unor garanții tehnice, de gestionare și fizice, pentru a asigura respectarea acestor principii și prelucrarea adecvată a informațiilor cu caracter personal. Aceasta poate include, de exemplu, măsuri specifice pentru a asigura siguranța informațiilor cu caracter personal, cum ar fi restricții privind accesul la informațiile cu caracter personal, controale ale accesului, jurnale, punerea la dispoziția angajaților a unor cursuri de formare specifice privind gestionarea informațiilor cu caracter personal etc.

În plus, în conformitate cu articolul 3 alineatul (5) și cu articolul 4 din PIPA, persoanele vizate au, printre altele, următoarele drepturi în ceea ce privește informațiile cu caracter personal prelucrate în scopuri legate de securitatea națională:

(1) dreptul de a obține confirmarea faptului că datele sale cu caracter personal sunt sau nu sunt prelucrate, precum și informații cu privire la prelucrare, precum și de acces la informațiile respective, inclusiv furnizarea de copii [articolul 4 alineatele (1) și (3) din PIPA];

(2) dreptul de a suspenda prelucrarea și rectificarea, ștergerea și distrugerea informațiilor cu caracter personal [articolul 4 alineatul (4) din PIPA].

(iii) O persoană vizată poate depune o cerere în exercitarea acestor drepturi direct la operator sau indirect prin intermediul Comisiei pentru protecție și își poate autoriza reprezentantul să facă acest lucru. În cazul în care persoana vizată depune o cerere, operatorul acordă dreptul fără întârziere; totuși, cu condiția să poată amâna, limita sau refuza dreptul dacă este prevăzut în mod expres sau inevitabil să respecte alte legi în măsura în care și atât timp cât este necesar și proporțional pentru a proteja un obiectiv important de interes public (de exemplu, în măsura în care și atât timp cât acordarea dreptului ar pune în pericol o anchetă în curs sau ar amenința securitatea națională) sau în cazul în care acordarea dreptului poate aduce atingere vieții sau integrității fizice a unui terț sau poate încălca în mod nejustificat dreptul de proprietate și alte interese ale unui terț. În cazul în care cererea este respinsă sau restricționată, acesta notifică fără întârziere persoanei vizate motivele. Operatorul pregătește metoda și procedura pentru a permite persoanelor vizate să depună cereri și le anunță public, astfel încât persoanele vizate să poată lua cunoștință de acestea.

În plus, în conformitate cu articolul 58 alineatul (4) din PIPA (cerința de a asigura tratarea adecvată a plângerilor individuale) și cu articolul 4 alineatul (5) din PIPA (dreptul la despăgubiri adecvate pentru orice prejudiciu care rezultă din prelucrarea informațiilor cu caracter personal, printr-o procedură promptă și echitabilă), persoanele vizate au dreptul de a obține reparații. Aceasta include dreptul de a raporta o presupusă încălcare Centrului de raportare privind încălcarea securității informațiilor cu caracter personal [în conformitate cu articolul 62 alineatul (3) din PIPA], de a depune o plângere la PIPC în temeiul articolului 62 din PIPA cu privire la orice încălcare a drepturilor sau intereselor legate de informațiile cu caracter personal ale unei persoane și de a obține reparații judiciare împotriva deciziilor sau a lipsei de acțiune a PIPC în temeiul Legii privind contenciosul administrativ. În plus, persoanele vizate pot obține reparații judiciare în temeiul Legii privind contenciosul administrativ în cazul în care a avut loc o încălcare a drepturilor sau a intereselor lor ca urmare a unei dispoziții sau omisiuni a operatorului (de exemplu, colectarea ilegală a datelor cu caracter personal) sau pot obține despăgubiri pentru daune în conformitate cu Legea privind despăgubirile acordate de stat. Aceste căi de atac sunt disponibile atât în cazul unor posibile încălcări ale normelor cuprinse în legi specifice care stabilesc limitările și garanțiile în ceea ce privește colectarea de informații cu caracter personal, cum ar fi legile în materie de securitate națională, cât și în PIPA.

O persoană din UE poate depune o plângere la PIPC prin intermediul autorității sale naționale pentru protecția datelor, iar PIPC va înștiința persoana respectivă prin intermediul autorității naționale pentru protecția datelor, după încheierea investigației și încetarea măsurii de remediere (dacă este cazul).

ANEXA II

18 mai 2021

Excelenței Sale dl Didier Reynders, comisar pentru justiție al Comisiei Europene

Excelență,

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

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

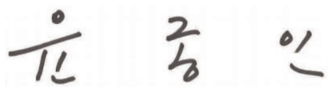
Acest document se referă la numeroase ministere și agenții ale Guvernului Coreei, iar în ceea ce privește conținutul documentului, ministerele și agențiile relevante (Comisia pentru protecția informațiilor cu caracter personal, Ministerul Justiției, Serviciul Național de Informații, Comisia națională pentru drepturile omului din Coreea, Centrul național de combatere a terorismului, Unitatea de informații financiare din Coreea) sunt responsabile de pasajele care intră în sfera lor 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,



Yoon Jong In
Președintele Comisiei pentru protecția informațiilor cu caracter personal

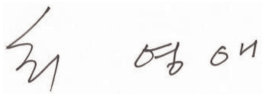
Acest document a fost elaborat de Comisia pentru protecția informațiilor cu caracter personal și de următoarele ministere și agenții:



Park Jie Won
Președinte (Director), Serviciul Național de Informații



Lee Jung Soo
Director general, Ministerul Justiției



Choi Young Ae
Președinte, Comisia națională pentru drepturile omului din Coreea



Kim Hyuck Soo
Director, Centrul național de combatere a terorismului



Kim, Jeong Kag
Comisar, Unitatea de informații financiare din Coreea

Cadrul juridic pentru colectarea și utilizarea datelor cu caracter personal de către autoritățile publice coreene în scopul aplicării legii și al securității naționale

Următorul document oferă o imagine de ansamblu asupra cadrului juridic privind colectarea și utilizarea informațiilor cu caracter personal de către autoritățile publice coreene de asigurare a respectării dreptului penal și în scopuri legate de securitatea națională (denumit în continuare „accesul administrației publice"), în special în ceea ce privește temeiurile juridice disponibile, condițiile (limitările) și garanțiile aplicabile, precum și supravegherea independentă și posibilitățile de a recurge la căi de atac individuale.

1. PRINCIPIILE JURIDICE GENERALE RELEVANTE PENTRU ACCESUL ADMINISTRAȚIEI PUBLICE

1.1. Cadrul constituțional

Constituția Republicii Coreea stabilește dreptul la viață privată, în general (articolul 17) și dreptul la confidențialitate a corespondenței, în special (articolul 18). Statul are datoria să garanteze aceste drepturi fundamentale ([1]). Constituția prevede, de asemenea, că drepturile și libertățile cetățenilor pot fi restricționate numai prin lege și atunci când acest lucru este necesar pentru securitatea națională sau pentru menținerea legii și ordinii pentru bunăstarea publică ([2]). Chiar și atunci când sunt impuse astfel de restricții, ele nu pot afecta substanța libertății sau a dreptului ([3]). Instanțele coreene au aplicat aceste dispoziții în cauzele privind ingerința administrației publice în viața privată. De exemplu, Curtea Supremă a constatat că monitorizarea civililor încălca dreptul fundamental la viață privată, subliniind că cetățenii au „dreptul de a decide singuri în privința informațiilor cu caracter personal" ([4]). În altă cauză, Curtea Constituțională a statuat că viața privată este un drept fundamental care oferă protecție împotriva intervenției și observării statului în viața privată a cetățenilor ([5]).

Constituția coreeană garantează, de asemenea, că nicio persoană nu va fi arestată, reținută, percheziționată, interogată și că nu vor avea loc puneri sub sechestru, cu excepția cazurilor prevăzute de lege ([6]). În plus, perchezițiile și punerile sub sechestru pot fi efectuate numai în baza unui mandat emis de un judecător, la cererea unui procuror și cu respectarea garanțiilor procedurale ([7]). În circumstanțe excepționale, și anume atunci când o persoană suspectată de săvârșirea de infracțiuni este reținută în timpul săvârșirii unei infracțiuni (*flagrante delicto*) sau atunci când există riscul ca o persoană suspectată de săvârșirea unei infracțiuni pasibile de pedeapsa cu închisoarea de cel puțin trei ani să fugă sau să distrugă probe, autoritățile de investigare pot efectua o percheziție sau o punere sub sechestru fără mandat, caz în care trebuie să solicite un mandat *ex post* ([8]). Aceste principii generale sunt dezvoltate suplimentar în legi specifice privind procedura penală și protecția comunicațiilor (a se vedea mai jos o prezentare detaliată).

În ceea ce privește cetățenii străini, Constituția prevede că statutul lor este garantat în conformitate cu legislația și tratatele internaționale ([9]). Mai multe acorduri internaționale la care Coreea este parte garantează drepturile la viață privată, cum ar fi Pactul internațional cu privire la drepturile civile și politice (articolul 17), Convenția privind drepturile persoanelor cu handicap (articolul 22) și Convenția cu privire la drepturile copilului (articolul 16). În plus, deși Constituția se referă, în principiu, la drepturile „cetățenilor", Curtea Constituțională a hotărât că și cetățenii străini au drepturi fundamentale ([10]). În special, Curtea a statuat că protecția demnității și a valorii unei persoane ca ființă umană,

([1]) Articolul 10 din Constituția Republicii Coreea, promulgată la 17 iulie 1948 („Constituția").
([2]) Articolul 37 alineatul (2) din Constituție.
([3]) Articolul 37 alineatul (2) din Constituție.
([4]) Hotărârea Curții Supreme a Coreei nr. 96DA42789 din 24 iulie 1998.
([5]) Hotărârea Curții Constituționale nr. 2002Hun-Ma51 din 30 octombrie 2003. În mod similar, în hotărârile 99Hun-Ma513 și 2004Hun-Ma190 (consolidate) din 26 mai 2005, Curtea Constituțională a clarificat faptul că „dreptul de a avea control asupra propriilor informații cu caracter personal este dreptul subiectului informațiilor de a decide personal când, cui sau de către cine și în ce măsură vor fi divulgate sau utilizate informațiile sale. Acesta este un drept fundamental, deși nu este specificat în Constituție, menit să protejeze libertatea personală de decizie împotriva riscurilor cauzate de extinderea funcțiilor statului și de tehnologia informației și comunicațiilor."
([6]) Articolul 12 alineatul (1) prima teză din Constituție.
([7]) Articolul 16 și articolul 12 alineatul (3) din Constituție.
([8]) Articolul 12 alineatul (3) din Constituție.
([9]) Articolul 6 alineatul (2) din Constituție.
([10]) Hotărârea Curții Constituționale nr. 93Hun-MA120 din 29 decembrie 1994. A se vedea, de exemplu, Hotărârea Curții Constituționale nr. 2014Hun-Ma346 (31 mai 2018), în care Curtea a constatat că a fost încălcat dreptul constituțional al unui cetățean sudanez reținut pe aeroport de a primi asistență din partea unui avocat. Într-o altă cauză, Curtea Constituțională a constatat că libertatea de alegere a locului de muncă legal este strâns legată de dreptul de a căuta fericirea, precum și la demnitate și valoare umană și, prin urmare, nu este rezervat doar cetățenilor, ci poate fi garantat și străinilor angajați legal în Republica Coreea (Hotărârea Curții Constituționale nr. 2007Hun-Ma1083 din 29 septembrie 2011).

precum și dreptul de a căuta fericirea sunt drepturi ale oricărei ființe umane, și nu doar ale cetățenilor ([11]). Curtea a clarificat, de asemenea, că dreptul de a avea control asupra informațiilor proprii este considerat a fi un drept fundamental, întemeiat pe dreptul la demnitate și la căutarea fericirii și pe dreptul la viață privată ([12]). Deși jurisprudența nu a abordat până în prezent în mod specific dreptul la viață privată al persoanelor de altă cetățenie decât cea coreeană, este, prin urmare, acceptat pe scară largă în rândul specialiștilor că articolele 12-22 din Constituție (care includ dreptul la viață privată, precum și libertatea personală) stabilesc „drepturile omului".

În cele din urmă, Constituția prevede, de asemenea, dreptul de a solicita despăgubiri de la autoritățile publice ([13]). În plus, în temeiul Legii privind Curtea Constituțională, orice persoană ale cărei drepturi fundamentale garantate de Constituție sunt încălcate prin exercitarea puterii guvernamentale (cu excepția hotărârilor instanțelor) poate depune o plângere constituțională la Curtea Constituțională ([14]).

1.2. **Norme generale privind protecția datelor**

Legea generală privind protecția datelor din Republica Coreea, Legea privind protecția informațiilor cu caracter personal („PIPA"), se aplică atât sectorului privat, cât și sectorului public. În ceea ce privește autoritățile publice, PIPA se referă în mod specific la obligația de a formula politici pentru a preveni „abuzul și utilizarea necorespunzătoare a informațiilor cu caracter personal, supravegherea și urmărirea indiscretă etc., precum și pentru a îmbunătăți gradul de respectare a demnității ființelor umane și a vieții private" ([15]).

Prelucrarea datelor cu caracter personal în scopul asigurării respectării legii este supusă tuturor cerințelor PIPA. Aceasta înseamnă, de exemplu, că autoritățile de asigurare a respectării dreptului penal trebuie să respecte obligațiile de prelucrare legală, și anume să se bazeze pe unul dintre temeiurile juridice enumerate în PIPA pentru colectarea, utilizarea sau furnizarea de informații cu caracter personal (articolele 15-18 din PIPA), precum și principiile limitării scopului [articolul 3 alineatele (1) și (2) din PIPA], proporționalității/reducerii la minimum a datelor [articolul 3 alineatele (1) și (6) din PIPA], păstrării limitate a datelor (articolul 21 din PIPA), securității datelor, inclusiv notificarea încălcării securității datelor [articolul 3 alineatul (4), articolul 29 și articolul 34 din PIPA], și transparenței [articolul 3 alineatele (1) și (5), articolul 20, articolul 30 și articolul 32 din PIPA]. În ceea ce privește informațiile sensibile, se aplică garanții specifice (articolul 23 din PIPA). În plus, în conformitate cu articolul 3 alineatul (5) și cu articolul 4 din PIPA, precum și cu articolele 35 - 39-2 din PIPA, persoanele fizice își pot exercita dreptul de acces, rectificare, ștergere și suspendare în fața autorităților de aplicare a legii.

Prin urmare, deși PIPA se aplică integral prelucrării datelor cu caracter personal în scopul asigurării respectării dreptului penal, conține o excepție atunci când datele cu caracter personal sunt prelucrate în scopuri legate de securitatea națională. În conformitate cu articolul 58 alineatul (1) punctul 2 din PIPA, articolele 15-50 din PIPA nu se aplică informațiilor cu caracter personal colectate sau solicitate pentru analiza informațiilor legate de securitatea națională ([16]). În schimb, rămân aplicabile dispozițiile de la capitolul I (Dispoziții generale), capitolul II (Stabilirea politicilor de protecție a informațiilor cu caracter personal etc.), capitolul VIII (Acțiuni colective în justiție pentru încălcarea securității datelor), capitolul IX (Dispoziții suplimentare) și capitolul X (Dispoziții privind sancțiunile) din PIPA. Aceasta include principiile generale de protecție a datelor prevăzute la articolul 3 (Principii privind protecția informațiilor cu caracter personal) și drepturile individuale garantate de articolul 4 din PIPA (Drepturile persoanelor vizate). Aceasta înseamnă că principiile și drepturile fundamentale sunt garantate și în acest domeniu. În plus, articolul 58 alineatul (4) din PIPA prevede că aceste informații trebuie prelucrate în măsura minimă necesară pentru atingerea scopului preconizat și pentru perioada minimă; de asemenea, acesta prevede obligația operatorului de informații cu caracter personal să instituie măsurile necesare pentru a asigura gestionarea în condiții de siguranță a datelor și prelucrarea corespunzătoare, cum ar fi garanții tehnice, de gestionare și fizice, precum și măsuri pentru tratarea corespunzătoare a plângerilor individuale.

În Notificarea nr. 2021-1 privind normele suplimentare pentru interpretarea și aplicarea Legii privind protecția informațiilor cu caracter personal, Comisia pentru protecția informațiilor cu caracter personal („PIPC") a clarificat modul în care se aplică PIPA în cazul prelucrării datelor cu caracter personal în scopuri legate de securitatea națională, având în vedere această exceptare parțială ([17]). Aceasta include, în special, drepturile persoanelor fizice (de acces, rectificare, suspendare și ștergere) și motivele, precum și posibilele limitări ale acestora. Conform notificării, aplicarea principiilor, a drepturilor și a obligațiilor de bază prevăzute în PIPA în ceea ce privește prelucrarea datelor cu caracter personal în

([11]) Hotărârea Curții Constituționale nr. 99HeonMa494 din 29 noiembrie 2001.
([12]) A se vedea, de exemplu, Hotărârea Curții Constituționale nr. 99HunMa513.
([13]) Articolul 29 alineatul (1) din Constituție.
([14]) Articolul 68 alineatul (1) din Legea privind Curtea Constituțională.
([15]) Articolul 5 alineatul (1) din PIPA.
([16]) Articolul 58 alineatul (1) punctul 2 din PIPA.
([17]) Notificarea nr. 2021-1 a PIPC privind normele suplimentare pentru interpretarea și aplicarea Legii privind protecția informațiilor cu caracter personal, secțiunea III punctul 6.

scopuri legate de securitatea națională reflectă garanțiile prevăzute în Constituție pentru protecția dreptului persoanei de a avea control asupra propriilor informații cu caracter personal. Orice limitare a acestui drept, de exemplu atunci când este necesar pentru protejarea securității naționale, necesită o echilibrare a drepturilor și a intereselor individuale cu interesul public relevant și nu poate afecta substanța dreptului [articolul 37 alineatul (2) din Constituție].

2. ACCESUL ADMINISTRAȚIEI PUBLICE ÎN SCOPUL ASIGURĂRII APLICĂRII LEGII

2.1. Autoritățile publice competente în domeniul asigurării respectării legii

În baza Codului de procedură penală („CPA"), a Legii privind protecția confidențialității comunicațiilor („CPPA") și a Legii privind activitățile de telecomunicații („TBA"), poliția, procurorii și instanțele pot colecta date cu caracter personal în scopul asigurării respectării dreptului penal. În măsura în care Legea privind Serviciul Național de Informații conferă această competență și Serviciului Național de Informații („NIS"), aceasta trebuie să respecte legile menționate anterior ([18]). În cele din urmă, Legea privind raportarea și utilizarea informațiilor specifice privind tranzacțiile financiare („ARUSFTI") oferă un temei juridic pentru ca instituțiile financiare să poată divulga informații Unității de informații financiare din Coreea („KOFIU") în scopul prevenirii spălării banilor și a finanțării terorismului. La rândul său, această agenție specializată poate furniza astfel de informații autorităților de aplicare a legii. Totuși, aceste obligații de divulgare se aplică numai operatorilor de date care prelucrează informații cu caracter personal privind creditele în conformitate cu Legea privind informațiile referitoare la credite și care fac obiectul supravegherii Comisiei pentru servicii financiare. Întrucât prelucrarea informațiilor cu caracter personal privind creditele de către acești operatori este exclusă din domeniul de aplicare al deciziei privind caracterul adecvat al nivelului de protecție, limitările și garanțiile care se aplică în temeiul ARUSFTI nu sunt descrise mai detaliat în documentul de față.

2.2. Temeiuri juridice și limitări

CPA (a se vedea 2.2.1), CPPA (a se vedea 2.2.2) și Legea privind activitățile de telecomunicații (a se vedea 2.2.3) oferă temeiuri juridice pentru colectarea de informații cu caracter personal în scopul aplicării legii și stabilesc limitările și garanțiile aplicabile.

2.2.1. *Perchezițiile și punerile sub sechestru*

2.2.1.1. Temei juridic

Procurorii și agenții poliției judiciare cu grad superior pot inspecta articole, pot percheziționa persoane sau pune sub sechestru articole numai (1) dacă o persoană este suspectată de săvârșirea unei infracțiuni (persoană suspectată de săvârșirea unei infracțiuni), (2) este necesar pentru investigație și (3) articolele care trebuie inspectate, persoanele care trebuie percheziționate și toate articolele puse sub sechestru sunt considerate a avea legătură cu cauza ([19]). De asemenea, instanțele pot efectua percheziții și pot pune sub sechestru orice articole care urmează să fie utilizate ca probe sau care sunt susceptibile de confiscare, atât timp cât se consideră că aceste articole sau persoane au legătură cu un caz specific ([20]).

2.2.1.2. Limitări și garanții

Ca o obligație generală, procurorii și agenții poliției judiciare trebuie să respecte drepturile omului în cazul persoanei suspectate de săvârșirea de infracțiuni, precum și ale oricărei alte persoane vizate ([21]). În plus, măsurile obligatorii pentru atingerea scopului investigației pot fi luate numai dacă acest lucru este prevăzut în mod explicit în CPA și în cea mai mică măsură necesară ([22]).

Perchezițiile, inspecțiile sau punerile sub sechestru efectuate de ofițerii de poliție sau de procurori în cadrul unei anchete penale pot avea loc numai în baza unui mandat emis de instanță ([23]). Autoritatea care solicită un mandat trebuie să prezinte materiale care să demonstreze motivele pentru a suspecta că o persoană a săvârșit o infracțiune, că percheziția, inspecția sau sechestrul este necesar(ă) și că există articole relevante care trebuie să fie puse sub sechestru ([24]). În ceea ce privește mandatul, acesta trebuie să conțină, printre alte elemente, numele persoanei suspectate de săvârșirea unei infracțiuni și infracțiunea; locul, persoana sau articolele care urmează să fie percheziționate sau articolele care urmează să fie puse sub sechestru; data emiterii și perioada efectivă de aplicare ([25]). În mod similar, în cazul în care, în cadrul unei proceduri judiciare în curs, perchezițiile și punerile sub sechestru sunt efectuate altfel decât în ședință publică, trebuie să se obțină în prealabil un mandat emis de instanță ([26]). Persoana în cauză și consiliul său de apărare sunt informate în prealabil cu privire la percheziție sau punere sub sechestru și pot fi prezente în momentul executării mandatului ([27]).

([18]) A se vedea articolul 3 din Legea NIS (Legea nr. 12948), care se referă la cercetarea penală a anumitor infracțiuni, cum ar fi insurecția, rebeliunea și infracțiunile legate de securitatea națională (de exemplu, spionajul). Procedurile prevăzute de CPA privind perchezițiile și punerile sub sechestru s-ar aplica într-un astfel de context, în timp ce CPPA ar reglementa colectarea datelor privind comunicațiile (a se vedea partea 3 privind dispozițiile referitoare la accesul la comunicații în scopuri legate de securitatea națională).
([19]) Articolul 215 alineatele (1) și (2) din CPA.
([20]) Articolul 106 alineatul (1), articolele 107 și 109 din CPA.
([21]) Articolul 198 alineatul (2) din CPA.
([22]) Articolul 199 alineatul (1) din CPA.
([23]) Articolul 215 alineatele (1) și (2) din CPA.
([24]) Articolul 108 alineatul (1) din Regulamentul de procedură penală.
([25]) Articolul 114 alineatul (1) din CPA coroborat cu articolul 219 din CPA.
([26]) Articolul 113 din CPA.
([27]) Articolele 121 și 122 din CPA.

Atunci când se efectuează percheziții sau puneri sub sechestru și în cazul în care articolul care trebuie percheziționat este un CD sau alt suport de stocare a datelor, în principiu, vor fi confiscate numai datele în sine (prin copiere sau imprimare), și nu întregul suport ([28]). Suportul de stocare a datelor poate fi pus sub sechestru numai atunci când se consideră că este aproape imposibil să se imprime sau să se copieze datele solicitate separat sau atunci când se consideră că este practic imposibil să se îndeplinească scopul percheziției ([29]). Persoana în cauză trebuie informată fără întârziere cu privire la punerea sub sechestru ([30]). Nu există excepții de la această cerință de notificare în temeiul CPA.

Perchezițiile, inspecțiile și punerile sub sechestru fără mandat pot avea loc numai într-un număr limitat de situații. În primul rând, aceasta este situația atunci când este imposibil să se obțină un mandat din cauza urgenței de la locul unei infracțiuni ([31]). Cu toate acestea, mandatul trebuie obținut ulterior fără întârziere ([32]). În al doilea rând, perchezițiile și inspecțiile fără mandat pot avea loc in loco atunci când o persoană suspectată de săvârșirea unei infracțiuni este arestată sau reținută ([33]). În cele din urmă, un procuror sau un agent al poliției judiciare cu grad superior poate confisca un articol fără mandat atunci când articolul a fost înlăturat de o persoană suspectată de săvârșirea unei infracțiuni sau de un terț ori a fost prezentat în mod voluntar ([34]).

Probele care au fost obținute cu încălcarea CPA vor fi considerate inadmisibile ([35]). În plus, Codul penal prevede că percheziția ilegală a persoanelor sau a reședinței persoanelor, a clădirilor păzite, a structurilor, a automobilelor, a navelor, a aeronavelor sau a încăperilor ocupate se pedepsește cu închisoare de până la trei ani ([36]). Prin urmare, această dispoziție se aplică și în cazul în care, în timpul unei percheziții ilegale, sunt puse sub sechestru obiecte precum dispozitivele de stocare a datelor.

2.2.2. *Colectarea informațiilor privind comunicațiile*

2.2.2.1. Temei juridic

Colectarea informațiilor privind comunicațiile este reglementată de o lege specifică, CPPA. În special, CPPA prevede o interdicție pentru orice persoană de a cenzura orice obiect de corespondență, de a intercepta orice tip de telecomunicații, de a furniza date de confirmare a comunicațiilor, de a înregistra sau asculta orice conversație între alte persoane care nu sunt făcute publice, cu excepția cazului în care CPA, CPPA sau Legea privind instanțele militare conțin dispoziții în acest sens ([37]). Termenul „comunicații" în sensul CPPA vizează atât corespondența obișnuită, cât și telecomunicațiile ([38]). În acest sens, CPPA face distincție între „măsurile de restricționare a comunicațiilor" ([39]) și colectarea de „date de confirmare a comunicațiilor".

Noțiunea de măsuri de restricționare a comunicațiilor acoperă „cenzura", și anume colectarea conținutului corespondenței tradiționale, precum și „interceptarea comunicațiilor", și anume interceptarea directă (obținerea sau înregistrarea) a conținutului telecomunicațiilor ([40]). Noțiunea de date de confirmare a comunicațiilor acoperă „datele privind înregistrările telecomunicațiilor", care includ data telecomunicațiilor, ora de începere și de încheiere a acestora, numărul de apeluri inițiate și primite, precum și numărul de abonat al celeilalte părți, frecvența utilizării, fișierele-jurnal privind utilizarea serviciilor de telecomunicații și informațiile de localizare (de exemplu, de la turnurile de transmisie unde se primesc semnalele) ([41]).

([28]) Articolul 106 alineatul (3) din CPA.
([29]) Articolul 106 alineatul (3) din CPA.
([30]) Articolul 219 din CPA coroborat cu articolul 106 alineatul (4) din CPA.
([31]) Articolul 216 alineatul (3) din CPA.
([32]) Articolul 216 alineatul (3) din CPA.
([33]) Articolul 216 alineatele (1) și (2) din CPA.
([34]) Articolul 218 din CPA. În ceea ce privește informațiile cu caracter personal, este vizată doar prezentarea voluntară chiar de către persoana în cauză, nu de către un operator de informații cu caracter personal care deține astfel de informații (ceea ce ar necesita un temei juridic specific astfel cum prevede Legea privind protecția informațiilor cu caracter personal). Articolele prezentate în mod voluntar sunt admise ca probe în cadrul procedurilor judiciare numai dacă nu există nicio îndoială rezonabilă cu privire la caracterul voluntar al divulgării, aspect care trebuie demonstrat de procuror. A se vedea Hotărârea Curții Supreme 2013Do11233 din 10 martie 2016.
([35]) Articolul 308-2 din CPA.
([36]) Articolul 321 din Codul penal.
([37]) Articolul 3 din CPPA. Legea privind instanțele militare reglementează, în principiu, colectarea de informații privind personalul militar și se poate aplica civililor numai într-un număr limitat de cazuri (de exemplu, în cazul comiterii de infracțiuni de către personalul militar împreună cu civili sau în cazul unei infracțiuni îndreptate împotriva armatei comise de o persoană, pot fi inițiate proceduri în fața unei instanțe militare; a se vedea articolul 2 din Legea privind instanțele militare). Dispozițiile generale care reglementează percheziții și punerile sub sechestru sunt similare cu cele prevăzute în CPA; a se vedea, de exemplu, articolele 146-149 și 153-156 din Legea privind instanțele militare. De exemplu, datele poștale pot fi colectate numai atunci când sunt necesare pentru o investigație și în baza unui mandat emis de instanța militară. În măsura în care comunicațiile electronice ar fi colectate, se aplică limitările și garanțiile prevăzute în CPPA.
([38]) Articolul 2 alineatul (1) din CPPA, și anume „transmiterea sau recepționarea tuturor tipurilor de sunete, cuvinte, simboluri sau imagini prin cablu, pe suport radio, prin cablu cu fibră optică sau alt sistem electromagnetic, inclusiv telefon, e-mail, serviciu de informare pentru membri, fax și radio paging".
([39]) Articolul 2 alineatul (7) și articolul 3 alineatul (2) din CPPA.
([40]) „Cenzura" este definită ca „deschidere a corespondenței fără consimțământul părții în cauză sau aflarea, înregistrarea sau ascunderea conținutului său prin alte mijloace" [articolul 2 alineatul (6) din CPPA]. „Interceptarea comunicațiilor" înseamnă „aflarea sau înregistrarea conținutului telecomunicațiilor prin ascultarea sau citirea în comun a sunetelor, cuvintelor, simbolurilor sau imaginilor comunicațiilor prin intermediul dispozitivelor electronice și mecanice fără consimțământul părții în cauză sau ingerința în transmiterea și recepția acestora" [articolul 2 alineatul (7) din CPPA].
([41]) Articolul 2 alineatul (11) din CPPA.

CPPA stabilește limitările și garanțiile pentru colectarea ambelor tipuri de date, iar nerespectarea mai multora dintre aceste cerințe face obiectul unor sancțiuni penale ([42]).

2.2.2.2. Limitări și garanții aplicabile în cazul colectării conținutului comunicațiilor (comunicații care restricționează măsurile)

Colectarea conținutului comunicațiilor poate avea loc doar ca mijloc suplimentar de facilitare a unei anchete penale (de exemplu, ca măsură de ultimă instanță) și trebuie depuse eforturi pentru a reduce la minimum interferența cu secretele comunicațiilor persoanelor ([43]). În concordanță cu acest principiu general, măsurile de restricționare a comunicațiilor pot fi aplicate numai în cazul în care este dificil să se prevină în alt mod săvârșirea unei infracțiuni, să se aresteze un infractor sau să se colecteze probe ([44]). Agențiile de aplicare a legii care colectează conținutul comunicațiilor trebuie să înceteze imediat să facă acest lucru odată ce continuarea accesului nu mai este considerată necesară, asigurându-se astfel că încălcarea confidențialității comunicațiilor este cât mai limitată posibil ([45]).

În plus, măsurile de restricționare a comunicațiilor pot fi utilizate numai atunci când există motive întemeiate de a suspecta că anumite infracțiuni grave enumerate în mod specific în CPPA sunt în curs de planificare, de săvârșire sau au fost săvârșite. Printre acestea se numără infracțiuni precum insurecția, infracțiuni legate de droguri sau infracțiuni care implică explozivi, precum și infracțiuni legate de securitatea națională, relațiile diplomatice sau baze și instalații militare ([46]). Ținta unei măsuri de restricționare a comunicațiilor trebuie să fie obiectele de corespondență sau telecomunicațiile specifice expediate sau primite de suspect sau obiectele de corespondență sau telecomunicațiile expediate sau primite de suspect pe o perioadă determinată ([47]).

Chiar și atunci când aceste cerințe sunt îndeplinite, colectarea datelor referitoare la conținut poate avea loc numai în baza unui mandat emis de instanță. În special, un procuror poate solicita instanței să permită colectarea de date referitoare la conținut cu privire la suspect sau la persoana cercetată ([48]). În mod similar, un agent al poliției judiciare poate solicita autorizarea unui procuror, care, la rândul său, poate solicita un mandat din partea instanței ([49]). O cerere de emitere a unui mandat trebuie formulată în scris și trebuie să conțină elemente specifice. În special, aceasta trebuie să stabilească (1) motivele întemeiate pentru a suspecta că una dintre infracțiunile enumerate este planificată, este în curs de săvârșire sau a fost săvârșită, precum și orice materiale care stabilesc prezumția de suspiciune; (2) măsurile de restricționare a comunicațiilor, precum și ținta, domeniul de aplicare, obiectivul și perioada lor efectivă; și (3) locul în care vor fi executate măsurile și modul în care acestea vor fi puse în aplicare ([50]).

În cazul în care sunt îndeplinite cerințele legale, instanța poate acorda autorizare scrisă de a lua măsuri de restricționare a comunicațiilor în ceea ce privește suspectul sau persoana cercetată ([51]). Acest mandat precizează tipurile de măsuri, precum și ținta, domeniul de aplicare, perioada efectivă, locul de executare și modul de punere în aplicare a acestora ([52]).

Măsurile de restricționare a comunicațiilor pot fi puse în aplicare numai pentru o perioadă de două luni ([53]). În cazul în care obiectivul măsurilor este atins mai devreme în perioada respectivă, măsurile trebuie să înceteze imediat. În schimb, în cazul în care condițiile necesare sunt în continuare îndeplinite, se poate depune o cerere de prelungire a perioadei efective de aplicare a măsurilor de restricționare a comunicațiilor în termenul de două luni. O astfel de cerere trebuie să includă elemente care să stabilească o prezumție pentru extinderea măsurilor ([54]). Perioada prelungită nu poate depăși în total un an sau trei ani pentru anumite infracțiuni deosebit de grave (de exemplu, infracțiuni legate de insurecție, agresiune externă, securitate națională etc.) ([55]).

Autoritățile de aplicare a legii pot impune asistența operatorilor de comunicații, oferindu-le autorizarea scrisă a instanței ([56]). Operatorii de comunicații au obligația de a coopera și de a păstra autorizarea primită în dosarele lor ([57]). Ei pot refuza cooperarea atunci când informațiile privind persoana vizată, astfel cum se indică în autorizarea scrisă a instanței (de exemplu, numărul de telefon al persoanei vizate) sunt incorecte. În plus, acestora le este interzis, în orice caz, să divulge parolele utilizate pentru telecomunicații ([58]).

([42]) Articolele 16 și 17 din CPPA. Acest lucru este valabil, de exemplu, în caz de colectare fără mandat, de nepăstrare a evidențelor, de neîntrerupere a colectării atunci când nu mai există o situație de urgență sau de nerespectare a obligației de notificare a persoanei în cauză.
([43]) Articolul 3 alineatul (2) din CPPA.
([44]) Articolul 5 alineatul (1) din CPPA.
([45]) Articolul 2 din Decretul de punere în aplicare a CPPA.
([46]) Articolul 5 alineatul (1) din CPPA.
([47]) Articolul 5 alineatul (2) din CPPA.
([48]) Articolul 6 alineatul (1) din CPPA.
([49]) Articolul 6 alineatul (2) din CPPA.
([50]) Articolul 6 alineatul (4) din CPPA și articolul 4 alineatul (1) din Decretul de punere în aplicare a CPPA.
([51]) Articolul 6 alineatul (5) și articolul 6 alineatul (8) din CPPA.
([52]) Articolul 6 alineatul (6) din CPPA.
([53]) Articolul 6 alineatul (7) din CPPA.
([54]) Articolul 6 alineatul (7) din CPPA.
([55]) Articolul 6 alineatul (8) din CPPA.
([56]) Articolul 9 alineatul (2) din CPPA.
([57]) Articolul 15-2 din CPPA și articolul 12 din Decretul de punere în aplicare a CPPA.
([58]) Articolul 9 alineatul (4) din CPPA.

Orice persoană care execută măsuri de restricționare a comunicațiilor sau căreia i s-a solicitat să coopereze trebuie să țină evidențe în care să se precizeze obiectivele măsurilor, executarea acestora, data la care a avut loc cooperarea și ținta acesteia ([59]). De asemenea, autoritățile de aplicare a legii care pun în aplicare măsuri de restricționare a comunicațiilor trebuie să țină evidențe care să stabilească detaliile și rezultatele obținute ([60]). Agenții poliției judiciare trebuie să furnizeze procurorului aceste informații prin intermediul unui raport atunci când închid o investigație ([61]).

Atunci când un procuror emite o decizie de punere sub acuzare cu privire la o cauză în care au fost utilizate măsuri de restricționare a comunicațiilor sau emite o dispoziție de a nu pune sub acuzare sau de a nu aresta persoana relevantă (și anume, nu doar suspendarea urmăririi penale), procurorul trebuie să îi comunice persoanei care face obiectul măsurilor de restricționare a comunicațiilor faptul că au fost executate măsuri de restricționare a comunicațiilor, agenția de executare și perioada de executare. O astfel de notificare trebuie transmisă în scris în termen de 30 de zile de la data dispoziției ([62]). Notificarea poate fi amânată atunci când este de natură să pună în pericol grav securitatea națională sau să perturbe siguranța și ordinea publică sau atunci când este probabil să prejudicieze grav viața și integritatea fizică a altora ([63]). Atunci când intenționează să amâne notificarea, procurorul sau agentul de poliție judiciară trebuie să obțină aprobarea șefului parchetului districtual ([64]). Odată ce motivele sesizării încetează să existe, notificarea trebuie transmisă în termen de 30 de zile de la momentul respectiv ([65]).

De asemenea, CPPA stabilește o procedură specifică pentru colectarea conținutului comunicațiilor în situații de urgență. În special, agențiile de aplicare a legii pot colecta conținutul comunicațiilor în cazul în care planificarea sau executarea de infracțiuni din sfera criminalității organizate sau a altor infracțiuni grave care pot cauza în mod direct decesul sau vătămarea gravă este iminentă și există o situație de urgență care face imposibilă parcurgerea procedurii obișnuite (astfel cum se prevede mai sus) ([66]). Într-o astfel de situație de urgență, un agent de poliție sau un procuror poate lua măsuri de restricționare a comunicațiilor fără autorizarea prealabilă a instanței, dar trebuie să solicite autorizarea instanței imediat după executare. În cazul în care agenția de aplicare a legii nu obține autorizarea instanței în termen de 36 de ore de la momentul în care au fost luate măsurile de urgență, colectarea trebuie întreruptă imediat, urmată, de regulă, de distrugerea informațiilor colectate ([67]). Agenții de poliție care efectuează operațiuni de supraveghere de urgență fac acest lucru sub controlul unui procuror sau, în cazul în care primirea în prealabil a instrucțiunilor procurorului este imposibilă din cauza necesității de a acționa urgent, poliția trebuie să obțină aprobarea unui procuror imediat după începerea executării ([68]). Normele privind notificarea persoanei, astfel cum sunt descrise mai sus, se aplică, de asemenea, în cazul colectării conținutului comunicațiilor în situații de urgență.

Colectarea de informații în situații de urgență trebuie să aibă loc întotdeauna în conformitate cu o „declarație privind cenzura/interceptarea comunicațiilor de urgență”, iar autoritatea care efectuează colectarea trebuie să țină un registru al tuturor măsurilor de urgență ([69]). Cererea adresată unei instanțe de a acorda autorizarea pentru luarea de măsuri de urgență trebuie să fie însoțită de un document scris care să indice măsurile necesare de restricționare a comunicațiilor, ținta, obiectul, domeniul de aplicare, perioada, locul de executare, metoda și o explicație cu privire la modul în care măsurile relevante de restricționare a comunicațiilor respectă articolul 5 alineatul (1) din CPPA ([70]), împreună cu documente justificative.

În cazurile în care măsurile de urgență sunt finalizate într-un termen scurt, eliminând astfel necesitatea obținerii unei autorizări din partea instanței (de exemplu, dacă suspectul este arestat imediat după inițierea interceptării, care, prin urmare, se oprește), șeful parchetului competent notifică instanței competente o măsură de urgență ([71]). Notificarea trebuie să stabilească obiectivul, ținta, domeniul de aplicare, perioada, locul de executare și metoda de colectare, precum și motivele pentru care nu a depus o cerere de autorizare din partea instanței ([72]). Această notificare permite instanței destinatare să examineze legalitatea colectării și trebuie înregistrată într-un registru al notificărilor privind măsurile de urgență.

([59]) Articolul 9 alineatul (3) din CPPA.
([60]) Articolul 18 alineatul (1) din Decretul de punere în aplicare a CPPA.
([61]) Articolul 18 alineatul (2) din Decretul de punere în aplicare a CPPA.
([62]) Articolul 9-2 alineatul (1) din CPPA.
([63]) Articolul 9-2 alineatul (4) din CPPA.
([64]) Articolul 9-2 alineatul (5) din CPPA.
([65]) Articolul 9-2 alineatul (6) din CPPA.
([66]) Articolul 8 alineatul (1) din CPPA.
([67]) Articolul 8 alineatul (2) din CPPA.
([68]) Articolul 8 alineatul (3) din CPPA și articolul 16 alineatul (3) din Decretul de punere în aplicare a CPPA.
([69]) Articolul 8 alineatul (4) din CPPA.
([70]) Și anume, că există un motiv serios de a suspecta că anumite infracțiuni grave sunt în curs de planificare sau săvârșire ori au fost săvârșite și că altfel este imposibil să se prevină săvârșirea unei infracțiuni, să se aresteze infractorul sau să se colecteze probe.
([71]) Articolul 8 alineatul (5) din CPPA.
([72]) Articolul 8 alineatele (6) și (7) din CPPA.

Ca o cerință generală, conținutul comunicațiilor obținute prin aplicarea măsurilor de restricționare a comunicațiilor în temeiul CPPA poate fi utilizat numai pentru cercetarea, urmărirea penală sau prevenirea infracțiunilor specifice enumerate mai sus, în cadrul procedurilor disciplinare pentru aceleași infracțiuni, al unei cereri de despăgubiri formulate de o parte la comunicații sau în cazul în care acest lucru este permis de alte legi ([73]).

În cazul în care sunt colectate telecomunicații transmise prin internet, se aplică garanții specifice ([74]). Aceste informații pot fi utilizate numai pentru investigarea infracțiunilor grave enumerate la articolul 5 alineatul (1) din CPPA. Pentru păstrarea informațiilor, trebuie să se obțină aprobarea instanței care a autorizat măsurile de restricționare a comunicațiilor ([75]). Cererea de păstrare trebuie să conțină informații privind măsurile de restricționare a comunicațiilor, un rezumat al rezultatelor măsurilor, motivele reținerii (împreună cu materiale justificative) și telecomunicațiile care trebuie păstrate ([76]). În absența unei astfel de cereri, telecomunicațiile obținute trebuie șterse în termen de 14 zile de la încetarea măsurilor de restricționare a comunicațiilor ([77]). În cazul respingerii unei cereri, telecomunicațiile trebuie distruse în termen de șapte zile ([78]). În cazul în care telecomunicațiile sunt șterse, trebuie depus un raport în termen de șapte zile la instanța care a autorizat măsurile de restricționare a comunicațiilor, în care să se precizeze motivele ștergerii, precum și detaliile și data acesteia.

La un nivel mai general, dacă informațiile au fost obținute în mod ilegal prin intermediul unor măsuri de restricționare a comunicațiilor, acestea nu vor fi admise ca probe în cadrul procedurilor judiciare sau disciplinare ([79]). De asemenea, CPPA interzice oricărei persoane care ia măsuri de restricționare a comunicațiilor să divulge informațiile confidențiale obținute în cursul punerii în aplicare a unor astfel de măsuri și să utilizeze informațiile obținute pentru a aduce atingere reputației celor care fac obiectul măsurilor ([80]).

2.2.2.3. Limitări și garanții aplicabile în cazul colectării informațiilor de confirmare a comunicațiilor

În temeiul CPPA, autoritățile de aplicare a legii pot solicita operatorilor de servicii de telecomunicații să furnizeze date de confirmare a comunicațiilor atunci când acest lucru este necesar pentru a efectua o investigație sau pentru a executa o pedeapsă ([81]). Spre deosebire de colectarea datelor referitoare la conținut, posibilitatea de a colecta date de confirmare a comunicațiilor nu se limitează la anumite infracțiuni specifice. Cu toate acestea, la fel ca în cazul datelor referitoare la conținut, colectarea datelor de confirmare a comunicațiilor necesită autorizarea scrisă prealabilă a unei instanțe, în aceleași condiții ca cele descrise anterior ([82]). Atunci când, din motive de urgență, nu se poate obține autorizarea instanței, datele de confirmare a comunicațiilor pot fi colectate fără mandat, caz în care autorizarea trebuie obținută imediat după solicitarea datelor și trebuie comunicată furnizorului de servicii de telecomunicații ([83]). În cazul în care nu se obține o autorizare ulterioară, informațiile colectate trebuie distruse ([84]).

Procurorii, agenții de poliție judiciară și instanțele trebuie să țină evidența solicitărilor de date de confirmare a comunicațiilor ([85]). În plus, furnizorii de servicii de telecomunicații trebuie să raporteze de două ori pe an ministrului științei și al TIC cu privire la divulgarea datelor de confirmare a comunicațiilor și trebuie să păstreze evidențe ale acestora timp de șapte ani de la data divulgării datelor ([86]).

În principiu, persoanele sunt informate cu privire la faptul că au fost colectate date de confirmare a comunicațiilor ([87]). Momentul unei astfel de notificări depinde de circumstanțele investigației ([88]). Odată ce se ia o decizie de (ne)începere a urmăririi penale, notificarea trebuie transmisă în termen de 30 de zile. În schimb, în cazul în care punerea sub acuzare este suspendată, notificarea trebuie transmisă în termen de 30 de zile de la adoptarea unei astfel de decizii. În orice caz, notificarea trebuie transmisă în termen de 30 de zile după o perioadă de un an de la colectarea informațiilor.

Notificarea poate fi amânată dacă este de natură (1) să pună în pericol securitatea națională, siguranța și ordinea publică, (2) să provoace decesul sau vătămarea corporală, (3) să împiedice procedurile judiciare echitabile (de exemplu, ducând la

([73]) Articolul 12 din CPPA.
([74]) Articolul 12-2 din CPPA.
([75]) Procurorul sau agentul de poliție care execută măsurile de restricționare a comunicațiilor trebuie să selecteze telecomunicațiile care urmează să fie păstrate în termen de 14 zile de la încetarea măsurilor și să solicite aprobarea instanței (în cazul agentului de poliție, cererea trebuie înaintată unui procuror, care, la rândul său, transmite cererea instanței), a se vedea articolul 12-2 alineatele (1) și (2) din CPPA.
([76]) Articolul 12-2 alineatul (3) din CPPA.
([77]) Articolul 12-2 alineatul (5) din CPPA.
([78]) Articolul 12-2 alineatul (5) din CPPA.
([79]) Articolul 4 din CPPA.
([80]) Articolul 11 alineatul (2) din Decretul de punere în aplicare a CPPA.
([81]) Articolul 13 alineatul (1) din CPPA.
([82]) Articolele 13 și 6 din CPPA.
([83]) Articolul 13 alineatul (2) din CPPA. La fel ca în cazul măsurilor urgente de restricționare a comunicațiilor, trebuie întocmit un document care să stabilească detaliile cazului (suspectul, măsurile care trebuie luate, infracțiunea suspectată, precum și urgența). A se vedea articolul 37 alineatul (5) din Decretul de punere în aplicare a CPPA.
([84]) Articolul 13 alineatul (3) din CPPA.
([85]) Articolul 13 alineatele (5) și (6) din CPPA.
([86]) Articolul 13 alineatul (7) din CPPA.
([87]) A se vedea articolul 13-3 alineatul (7) coroborat cu articolul 9-2 din CPPA.
([88]) Articolul 13-3 alineatul (1) din CPPA.

distrugerea probelor sau amenințarea martorilor) sau (4) să defăimeze suspectul, victimele sau alte persoane care au legătură cu cazul sau să le invadeze viața privată ([89]). Notificarea cu privire la unul dintre motivele menționate mai sus necesită autorizarea din partea șefului unui parchet districtual competent ([90]). Odată ce motivele amânării încetează să existe, notificarea trebuie transmisă în termen de 30 de zile de la momentul respectiv ([91]).

Persoanele notificate pot depune o cerere scrisă la procuror sau la agentul de poliție judiciară cu privire la motivele colectării datelor de confirmare a comunicațiilor ([92]). În acest caz, procurorul sau agentul de poliție judiciară trebuie să prezinte motivele în scris în termen de 30 de zile de la primirea cererii, cu excepția cazului în care se aplică unul dintre motivele menționate mai sus (excepții pentru amânarea notificării) ([93]).

2.2.3. *Divulgarea voluntară de către operatorii din sectorul telecomunicațiilor*

Articolul 83 alineatul (3) din TBA permite operatorilor din sectorul telecomunicațiilor să se conformeze în mod voluntar unei cereri (formulate în sprijinul unui proces penal, al unei anchete sau al executării unei pedepse) din partea unei instanțe, a unui procuror sau a șefului unei agenții de investigare care are ca obiect divulgarea „datelor privind comunicațiile". În contextul TBA, „datele privind comunicațiile" includ numele, numărul de înregistrare pentru rezidenți, adresa și numărul de telefon al utilizatorilor, datele la care utilizatorii se abonează sau își reziliază abonamentul, precum și codurile de identificare a utilizatorului (și anume codurile utilizate pentru a identifica utilizatorul de drept al sistemelor informatice sau al rețelelor de comunicații) ([94]). În sensul TBA, numai persoanele care contractează în mod direct servicii de la un furnizor coreean de telecomunicații sunt considerate utilizatori ([95]). În consecință, situațiile în care persoanele din UE ale căror date au fost transferate către Republica Coreea ar fi considerate utilizatori în temeiul TBA vor fi probabil foarte limitate, deoarece persoanele respective nu ar încheia, în mod normal, un contract direct cu un operator coreean de telecomunicații.

Cererile de obținere a datelor privind comunicațiile în temeiul TBA trebuie să fie formulate în scris și să indice motivele cererii, legătura cu utilizatorul relevant și domeniul de aplicare al datelor solicitate ([96]). În cazul în care este imposibil să se prezinte o cerere scrisă din motive de urgență, cererea scrisă trebuie transmisă imediat ce motivul urgenței dispare ([97]). Operatorii din sectorul telecomunicațiilor care se conformează cererilor de divulgare a datelor transmise în cadrul comunicațiilor trebuie să păstreze registre cu înregistrări care indică faptul că au fost furnizate date privind comunicațiile, precum și materialele aferente, cum ar fi cererea scrisă ([98]). În plus, operatorii din sectorul telecomunicațiilor trebuie să raporteze ministrului științei și TIC de două ori pe an cu privire la furnizarea de date privind comunicațiile ([99]).

Operatorii din sectorul telecomunicațiilor nu sunt obligați să dea curs cererilor de divulgare a datelor privind comunicațiile pe baza TBA. Prin urmare, fiecare cerere trebuie să fie evaluată de operator în lumina cerințelor aplicabile în materie de protecție a datelor în temeiul PIPA. În special, un operator din sectorul telecomunicațiilor trebuie să țină seama de interesele persoanei vizate și nu poate divulga informațiile în cazul în care acestea ar putea aduce atingere în mod abuziv intereselor persoanei respective sau ale unui terț ([100]). În plus, în conformitate cu Notificarea nr. 2021-1 privind normele suplimentare pentru interpretarea și aplicarea Legii privind protecția informațiilor cu caracter personal, persoana în cauză trebuie să fie informată în legătură cu divulgarea. În situații excepționale, o astfel de notificare poate fi amânată, în special dacă și atât timp cât aceasta ar pune în pericol o anchetă penală în curs sau ar putea dăuna vieții sau integrității fizice a unei alte persoane, în cazul în care aceste drepturi sau interese sunt în mod evident superioare drepturilor persoanei vizate ([101]).

În 2016, Curtea Supremă a confirmat că furnizarea voluntară de date privind comunicațiile de către operatorii din sectorul telecomunicațiilor fără mandat în baza TBA nu încalcă, ca atare, dreptul la confidențialitatea informațiilor al utilizatorului serviciului de telecomunicații. În același timp, Curtea a clarificat faptul că ar exista o astfel de încălcare dacă este evident că agenția solicitantă a abuzat de autoritatea sa pentru a solicita divulgarea datelor privind comunicațiile, încălcând astfel interesele persoanei în cauză sau ale unui terț ([102]). La un nivel mai general, orice cerere de divulgare voluntară din partea unei autorități de aplicare a legii trebuie să respecte principiile legalității, necesității și proporționalității care decurg din Constituția coreeană [articolul 12 alineatul (1) și articolul 37 alineatul (2)].

([89]) Articolul 13-3 alineatul (2) din CPPA.
([90]) Articolul 13-3 alineatul (3) din CPPA.
([91]) Articolul 13-3 alineatul (4) din CPPA.
([92]) Articolul 13-3 alineatul (5) din CPPA.
([93]) Articolul 13-3 alineatul (6) din CPPA.
([94]) Articolul 83 alineatul (3) din TBA.
([95]) Articolul 2 alineatul (9) din TBA.
([96]) Articolul 83 alineatul (4) din TBA.
([97]) Articolul 83 alineatul (4) din TBA.
([98]) Articolul 83 alineatul (5) din TBA.
([99]) Articolul 83 alineatul (6) din TBA.
([100]) Articolul 18 alineatul (2) din PIPA.
([101]) Notificarea nr. 2021-1 a PIPC privind normele suplimentare pentru interpretarea și aplicarea Legii privind protecția informațiilor cu caracter personal, secțiunea III punctul 2 subpunctul (iii).
([102]) Hotărârea Curții Supreme nr. 2012Da105482 din 10 martie 2016.

2.3. **Supravegherea**

Supravegherea autorităților de asigurare a respectării dreptului penal se realizează prin diferite mecanisme, atât la nivel intern, cât și de către organisme externe.

2.3.1. *Auditul intern*

În conformitate cu Legea privind auditurile din sectorul public, autoritățile publice sunt încurajate să înființeze un organism intern de audit intern, cu sarcina, printre altele, de a efectua controlul legalității ([103]). Șefilor acestor organisme de audit trebuie să li se garanteze independența în cea mai mare măsură posibilă ([104]). Mai precis, aceștia sunt numiți din afara autorității competente (de exemplu, foști judecători, profesori) pentru o perioadă cuprinsă între doi și cinci ani și pot fi demiși numai din motive justificate (de exemplu, atunci când nu își pot exercita atribuțiile din cauza unei tulburări psihice sau fizice, atunci când fac obiectul unor măsuri disciplinare) ([105]). De asemenea, auditorii sunt numiți pe baza condițiilor specifice prevăzute în lege ([106]). Rapoartele de audit pot include recomandări sau cereri de despăgubiri sau de rectificare, precum și mustrări și recomandări sau cereri de măsuri disciplinare ([107]). Acestea sunt notificate șefului autorității publice care face obiectul auditului, precum și Comisiei de audit și inspecție (a se vedea secțiunea 2.3.2) în termen de 60 de zile de la finalizarea auditului ([108]). Autoritatea în cauză trebuie să pună în aplicare măsurile necesare și să raporteze rezultatele Comisiei de audit și inspecție ([109]). În plus, rezultatele auditului sunt, în general, puse la dispoziția publicului ([110]). Refuzul sau obstrucționarea unui audit intern face obiectul unor amenzi administrative ([111]). În domeniul asigurării respectării dreptului penal, pentru a se conforma legislației menționate anterior, Agenția Națională de Poliție operează un sistem de inspectori generali pentru gestionarea auditurilor interne, inclusiv în ceea ce privește posibilele încălcări ale drepturilor omului ([112]).

2.3.2. *Comisia de audit și inspecție*

Comisia de audit și inspecție (*Board of Audit and Inspection* – „BAI") poate să inspecteze activitățile autorităților publice și, pe baza acestor inspecții, să emită recomandări, să solicite măsuri disciplinare sau să depună o plângere penală ([113]). BAI este instituită în mod oficial sub conducerea președintelui Republicii Coreea, dar își menține un statut independent în ceea ce privește atribuțiile care îi revin ([114]). În plus, Legea de instituire a BAI prevede că BAI trebuie să beneficieze de independență maximă în ceea ce privește numirea, concedierea și organizarea personalului său, precum și în ceea ce privește întocmirea bugetului său ([115]). Președintele BAI este numit de președintele statului, cu acordul Adunării Naționale ([116]). Ceilalți șase comisari sunt numiți de președintele statului, la recomandarea președintelui comisiei, pentru un mandat de patru ani ([117]). Comisarii (inclusiv președintele comisiei) trebuie să îndeplinească anumite calificări prevăzute de lege ([118]) și pot fi revocați numai în caz de punere sub acuzare, condamnare la închisoare sau incapacitate de a-și îndeplini atribuțiile din cauza unor deficiențe psihice sau fizice pe termen lung ([119]). În plus, comisarilor li se interzice să participe la activități politice și să dețină în același timp funcții în cadrul Adunării Naționale, al agențiilor administrative, al organizațiilor supuse auditului și inspecției de către BAI sau orice alt post sau funcție remunerat(ă) ([120]).

BAI efectuează anual un audit general, dar poate efectua, de asemenea, audituri specifice cu privire la chestiuni de interes special. BAI poate solicita prezentarea de documente în cursul unei inspecții și prezența unor persoane ([121]). În cadrul unui audit, BAI examinează veniturile și cheltuielile statului, dar supraveghează, de asemenea, respectarea generală a

([103]) Articolele 3 și 5 din Legea privind auditurile din sectorul public.
([104]) Articolul 7 din Legea privind auditurile din sectorul public.
([105]) Articolele 8-11 din Legea privind auditurile din sectorul public.
([106]) Articolul 16 și următoarele din Legea privind auditurile din sectorul public.
([107]) Articolul 23 alineatul (2) din Legea privind auditurile din sectorul public.
([108]) Articolul 23 alineatul (1) din Legea privind auditurile din sectorul public.
([109]) Articolul 23 alineatul (3) din Legea privind auditurile din sectorul public.
([110]) Articolul 26 din Legea privind auditurile din sectorul public.
([111]) Articolul 41 din Legea privind auditurile din sectorul public.
([112]) A se vedea, în special, diviziunile din subordinea directorului general pentru audit și inspecție: https://www.police.go.kr/eng/knpa/org/org01.jsp.
([113]) Articolele 24 și 31-35 din Legea privind Comisia de audit și inspecție („Legea BAI").
([114]) Articolul 2 alineatul (1) din Legea BAI.
([115]) Articolul 2 alineatul (2) din Legea BAI.
([116]) Articolul 4 alineatul (1) din Legea BAI.
([117]) Articolul 5 alineatul (1) și articolul 6 din Legea BAI.
([118]) De exemplu, să fi ocupat funcția de judecător, procuror sau avocat timp de cel puțin zece ani, să fi lucrat ca funcționar public, profesor sau să fi ocupat un post specific învățământului superior la o universitate timp de cel puțin opt ani sau să fi lucrat timp de cel puțin zece ani în cadrul unei societăți cotate la bursă sau al unei instituții cu capital de stat (din care cel puțin cinci ani ca funcționar executiv); a se vedea articolul 7 din Legea BAI.
([119]) Articolul 8 din Legea BAI.
([120]) Articolul 9 din Legea BAI.
([121]) A se vedea, de exemplu, articolul 27 din Legea BAI.

obligațiilor autorităților publice și ale funcționarilor publici în vederea îmbunătățirii funcționării administrației publice ([122]). Prin urmare, supravegherea sa depășește aspectele bugetare și include, de asemenea, un control al legalității.

2.3.3. *Adunarea Națională*

Adunarea Națională poate investiga și inspecta autoritățile publice ([123]). În cursul unei investigații sau inspecții, Adunarea Națională poate solicita prezentarea de documente și poate obliga la înfățișarea martorilor ([124]). Persoanele care depun mărturii mincinoase în timpul unei investigații a Adunării Naționale fac obiectul unor sancțiuni penale (închisoare de până la zece ani) ([125]). Procesul și rezultatele inspecțiilor pot fi făcute publice ([126]). Dacă Adunarea Națională constată o activitate ilegală sau necorespunzătoare, aceasta poate solicita autorității publice relevante să ia măsuri de remediere, inclusiv acordarea de despăgubiri, luarea de măsuri disciplinare și îmbunătățirea procedurilor sale interne ([127]). În urma unei astfel de solicitări, autoritatea trebuie să acționeze fără întârziere și să raporteze rezultatul Adunării Naționale ([128]).

2.3.4. *Comisia pentru protecția informațiilor cu caracter personal*

Comisia pentru protecția informațiilor cu caracter personal (*Personal Information Protection Commission* – „PIPC") supraveghează prelucrarea informațiilor cu caracter personal de către autoritățile de asigurare a respectării dreptului penal în concordanță cu PIPA. În plus, în conformitate cu articolul 7-8 alineatele (3) și (4) și cu articolul 7-9 alineatul (5) din PIPA, supravegherea PIPC vizează, de asemenea, posibilele încălcări ale normelor care stabilesc limitările și garanțiile în ceea ce privește colectarea de informații cu caracter personal, inclusiv cele cuprinse în legile specifice care reglementează colectarea de probe (electronice) în scopul asigurării respectării dreptului penal (a se vedea secțiunea 2.2). Având în vedere cerințele de la articolul 3 alineatul (1) din PIPA privind colectarea legală și echitabilă a informațiilor cu caracter personal, o astfel de încălcare constituie și o încălcare a PIPA, permițând PIPC să desfășoare o investigație și să ia măsuri de remediere ([129]).

În exercitarea funcției sale de supraveghere, PIPC are acces la toate informațiile relevante ([130]). PIPC poate oferi consiliere autorităților de aplicare a legii pentru a îmbunătăți nivelul de protecție a informațiilor cu caracter personal în cadrul activităților lor de prelucrare, poate impune măsuri de remediere (de exemplu, suspendarea prelucrării datelor sau luarea măsurilor necesare pentru protejarea informațiilor cu caracter personal) sau poate oferi consiliere autorității în vederea luării de măsuri disciplinare ([131]). În cele din urmă, sunt prevăzute sancțiuni penale pentru anumite încălcări ale PIPA, cum ar fi utilizarea sau divulgarea ilegală de informații cu caracter personal către terți sau prelucrarea ilegală a informațiilor sensibile ([132]). În acest sens, PIPC poate înainta chestiunea agenției de anchetă competente (inclusiv unui procuror) ([133]).

2.3.5. *Comisia națională pentru drepturile omului*

Comisia națională pentru drepturile omului (*National Human Rights Commission* – „NHRC") – un organism independent însărcinat cu protejarea și promovarea drepturilor fundamentale ([134]) – are competența de a investiga și de a remedia încălcările articolelor 10-22 din Constituție, printre care se numără dreptul la viață privată și la confidențialitate a corespondenței. NHRC este alcătuită din 11 comisari, desemnați de Adunarea Națională (patru), de președintele statului (patru) și de președintele Curții Supreme (trei) ([135]). Pentru a fi numit, un comisar trebuie (1) să fi lucrat timp de cel puțin zece ani în cadrul unei universități sau al unui institut de cercetare autorizat, cel puțin în calitate de conferențiar; (2) să fi ocupat funcția de judecător, procuror sau avocat cel puțin zece ani; (3) să fi fost implicat în activități privind drepturile omului timp de cel puțin zece ani (de exemplu, pentru o organizație non-profit, neguvernamentală sau internațională); ori (4) să fi fost recomandat de grupuri ale societății civile ([136]). Președintele Comisiei este

([122]) Articolele 20 și 24 din Legea BAI.
([123]) Articolul 128 din Legea privind Adunarea Națională și articolele 2, 3 și 15 din Legea privind inspecția și investigarea administrației de stat. Aceasta include inspecții anuale ale afacerilor guvernamentale în ansamblu și investigații cu privire la chestiuni specifice.
([124]) Articolul 10 alineatul (1) din Legea privind inspecția și investigarea administrației de stat. A se vedea, de asemenea, articolele 128 și 129 din Legea privind Adunarea Națională.
([125]) Articolul 14 din Legea privind mărturia, evaluarea etc. în fața Adunării Naționale.
([126]) Articolul 12-2 din Legea privind inspecția și investigarea administrației de stat.
([127]) Articolul 16 alineatul (2) din Legea privind inspecția și investigarea administrației de stat.
([128]) Articolul 16 alineatul (3) din Legea privind inspecția și investigarea administrației de stat.
([129]) A se vedea Notificarea PIPC nr. 2021-1 privind normele suplimentare pentru interpretarea și aplicarea Legii privind protecția informațiilor cu caracter personal.
([130]) Articolul 63 din PIPA.
([131]) Articolul 61 alineatul (2), articolul 65 alineatul (1), articolul 65 alineatul (2) și articolul 64 alineatul (4) din PIPA.
([132]) Articolele 70-74 din PIPA.
([133]) Articolul 65 alineatul (1) din PIPA.
([134]) Articolul 1 din Legea privind Comisia pentru drepturile omului („Legea NHRC").
([135]) Articolul 5 alineatele (1) și (2) din Legea NHRC.
([136]) Articolul 5 alineatul (3) din Legea NHRC.

numit de președintele statului din rândul comisarilor și trebuie să fie confirmat de Adunarea Națională ([137]). Comisarii (inclusiv președintele Comisiei) sunt numiți pentru un mandat de trei ani, cu posibilitate de reînnoire, și pot fi demiși numai dacă sunt condamnați la închisoare sau când nu mai sunt capabili să își exercite atribuțiile din cauza unor deficiențe fizice sau psihice prelungite (caz în care două treimi dintre comisari trebuie să fie de acord cu demiterea) ([138]). Comisarilor NHRC li se interzice să dețină în același timp o funcție în cadrul Adunării Naționale, al consiliilor locale sau al oricărei administrații naționale ori locale (în calitate de funcționar public) ([139]).

NHRC poate iniția o anchetă din proprie inițiativă sau în baza unei cereri din partea unei persoane. În cadrul unei anchete, NHRC poate solicita prezentarea de materiale relevante, poate efectua inspecții și poate convoca persoane să depună mărturie ([140]). În urma unei anchete, NHRC poate emite recomandări pentru îmbunătățirea sau corectarea politicilor și a practicilor specifice și le poate face publice ([141]). Autoritățile publice trebuie să notifice NHRC cu privire la un plan de punere în aplicare a acestor recomandări în termen de 90 de zile de la primirea lor ([142]). În plus, în cazul nepunerii în aplicare a recomandărilor, autoritatea în cauză trebuie să informeze Comisia în acest sens ([143]). La rândul său, NHRC poate să dezvăluie această neîndeplinire Adunării Naționale și/sau să o facă publică. Autoritățile publice respectă, în general, recomandările NHRC și sunt puternic încurajate să facă acest lucru, întrucât punerea lor în aplicare a fost evaluată în cadrul evaluării generale efectuate de Biroul pentru coordonarea politicilor guvernamentale, sub autoritatea cabinetului prim-ministrului.

2.4. **Căi de atac individuale**

2.4.1. *Mecanisme de reparație disponibile în temeiul PIPA*

Persoanele fizice își pot exercita drepturile de acces, rectificare, ștergere și suspendare în temeiul PIPA în ceea ce privește informațiile cu caracter personal prelucrate de autoritățile de asigurare a respectării dreptului penal. Accesul poate fi solicitat direct de la autoritatea relevantă sau indirect prin intermediul PIPC ([144]). Autoritatea competentă poate limita sau refuza accesul numai în cazul în care acest lucru este prevăzut de lege, în cazul în care acest lucru ar putea aduce prejudicii vieții sau integrității fizice a unui terț sau ar putea conduce la o încălcare nejustificată a drepturilor de proprietate și a altor interese ale unei alte persoane (și anume, în cazul în care interesele celeilalte persoane ar prevala asupra intereselor persoanei care formulează cererea) ([145]). Dacă o cerere de acces este refuzată, persoana trebuie să fie informată cu privire la motivele refuzului și la căile de atac disponibile ([146]). În mod similar, o cerere de rectificare sau de ștergere poate fi refuzată dacă acest lucru este prevăzut în alte legi, caz în care persoana trebuie să fie informată cu privire la motivele care stau la baza acesteia și la posibilitatea de a introduce o cale de atac ([147]).

În ceea ce privește căile de atac, persoanele pot depune o plângere la PIPC, inclusiv prin intermediul Centrului de intermediere telefonică privind protecția vieții private gestionat de Agenția coreeană pentru internet și securitate ([148]). În plus, o persoană poate apela la procedura de mediere prin intermediul Comitetului de mediere a litigiilor privind informațiile cu caracter personal ([149]). Aceste căi de atac sunt disponibile atât în cazul unor posibile încălcări ale normelor cuprinse în legi specifice care stabilesc limitările și garanțiile în ceea ce privește colectarea de informații cu caracter personal (secțiunea 2.2), cât și ale PIPA. În plus, persoanele fizice pot contesta deciziile sau inacțiunea PIPC în temeiul Legii privind contenciosul administrativ (a se vedea secțiunea 2.4.3).

([137]) Articolul 5 alineatul (5) din Legea NHRC.
([138]) Articolul 7 alineatul (1) și articolul 8 din Legea NHRC.
([139]) Articolul 10 din Legea NHRC.
([140]) Articolul 36 din Legea NHRC. În conformitate cu articolul 36 alineatul (7) din lege, prezentarea de materiale sau obiecte poate fi respinsă în cazul în care ar aduce atingere confidențialității statului care ar putea avea un efect major asupra securității statului sau a relațiilor diplomatice sau ar constitui un obstacol serios în calea unei anchete penale sau a unui proces în curs. În astfel de cazuri, Comisia poate solicita informații suplimentare din partea șefului agenției relevante (care trebuie să se conformeze cu bună-credință), dacă acest lucru este necesar pentru verifica dacă refuzul de a furniza informațiile este justificat.
([141]) Articolul 25 alineatul (1) din Legea NHRC.
([142]) Articolul 25 alineatul (3) din Legea NHRC.
([143]) Articolul 25 alineatul (4) din Legea NHRC.
([144]) Articolul 35 alineatul (2) din PIPA.
([145]) Articolul 35 alineatul (4) din PIPA.
([146]) Articolul 42 alineatul (2) din Decretul de punere în aplicare a PIPA.
([147]) Articolul 36 alineatele (1)-(2) din PIPA și articolul 43 alineatul (3) din Decretul de punere în aplicare a PIPA.
([148]) Articolul 62 din PIPA.
([149]) Articolele 40-50 din PIPA și articolele 48-2 - 57 din Decretul de punere în aplicare a PIPA.

2.4.2. *Căi de atac în fața Comisiei naționale pentru drepturile omului*

NHRC tratează plângerile formulate de persoane fizice (atât cetățeni coreeni, cât și străini) cu privire la încălcările drepturilor omului comise de autoritățile publice ([150]). Nu există nicio cerință privind calitatea procesuală activă pentru ca persoanele fizice să depună o plângere la NHRC ([151]). În consecință, o plângere va fi tratată de NHRC chiar dacă persoana în cauză nu poate demonstra un prejudiciu în fapt în etapa de admisibilitate. În contextul colectării de date cu caracter personal în scopul asigurării respectării dreptului penal, o persoană fizică nu ar fi, prin urmare, obligată să demonstreze că informațiile sale cu caracter personal au fost efectiv accesate de autoritățile publice coreene pentru ca plângerea să fie admisibilă în fața NHRC. De asemenea, o persoană fizică poate solicita soluționarea plângerii prin mediere ([152]).

Pentru a investiga o plângere, NHRC poate face uz de competențele sale de investigare, inclusiv solicitând prezentarea de materiale relevante, efectuând inspecții și citând persoane fizice pentru a depune mărturie ([153]). Dacă investigația arată că a avut loc o încălcare a legilor relevante, NHRC poate recomanda punerea în aplicare a unor căi de atac sau rectificarea sau îmbunătățirea oricărei legi, instituții, politici sau practici relevante ([154]). Căile de atac propuse pot include medierea, încetarea încălcării drepturilor omului, despăgubiri pentru daune și măsuri de prevenire a repetării acelorași încălcări sau a unor încălcări similare ([155]). În cazul colectării ilegale de informații cu caracter personal în temeiul normelor aplicabile, măsurile de remediere pot include ștergerea informațiilor cu caracter personal colectate. În cazul în care se consideră că este foarte probabil ca încălcarea să fie în desfășurare și că, dacă nu este tratată, s-ar produce un prejudiciu dificil de remediat, NHRC poate adopta măsuri urgente de remediere ([156]).

Deși NHRC nu are competența de a impune obligații, deciziile (de exemplu, o decizie de a nu continua investigarea unei plângeri) ([157]) și recomandările sale pot fi contestate în fața instanțelor coreene în temeiul Legii privind contenciosul administrativ (a se vedea secțiunea 2.4.3 de mai jos) ([158]). În plus, în cazul în care constatările NHRC arată că datele cu caracter personal au fost colectate în mod ilegal de o autoritate publică, o persoană fizică ar putea introduce căi de atac suplimentare în fața instanțelor coreene împotriva autorității publice respective, de exemplu prin contestarea colectării în temeiul Legii privind contenciosul administrativ, prin depunerea unei plângeri constituționale în temeiul Legii privind Curtea Constituțională sau prin solicitarea de despăgubiri pentru daune în temeiul Legii privind despăgubirile acordate de stat (a se vedea secțiunea 2.4.3 de mai jos).

2.4.3. *Căi de atac judiciare*

Persoanele fizice pot invoca limitările și garanțiile descrise în secțiunile anterioare pentru a obține despăgubiri în fața instanțelor coreene prin diferite căi.

În primul rând, în conformitate cu CPA, persoana în cauză și avocatul acesteia pot fi prezenți în momentul executării unui mandat de percheziție sau de punere sub sechestru și, prin urmare, pot ridica o obiecție în momentul executării mandatului ([159]). În plus, CPA prevede un așa-numit mecanism de „cvasi-plângere", care permite persoanelor fizice să sesizeze instanța competentă cu o cerere de anulare sau de modificare a unei dispoziții emise de un procuror sau de un agent de poliție cu privire la o punere sub sechestru ([160]). Acest lucru le permite persoanelor fizice să conteste măsurile luate pentru executarea unui mandat de punere sub sechestru.

([150]) Deși articolul 4 din Legea NHRC se referă la cetățenii și străinii care își au reședința în Republica Coreea, termenul „reședință" reflectă mai degrabă conceptul de jurisdicție decât teritoriul. Prin urmare, dacă drepturile fundamentale ale unui străin din afara Coreei sunt încălcate de instituțiile naționale din Coreea, persoana respectivă poate depune o plângere la NHRC. A se vedea, de exemplu, întrebarea corespunzătoare pe pagina NHRC destinată întrebărilor frecvente, disponibilă la adresa https://www.humanrights.go.kr/site/program/board/basicboard/list?boardtypeid=7025&menuid=002004005001&pagesize=10&currentpage=2. Acesta ar fi cazul când autoritățile publice coreene accesează în mod ilegal datele cu caracter personal ale unui străin transferate în Coreea.

([151]) În principiu, o plângere trebuie depusă în termen de un an de la încălcare, dar NHRC poate decide în continuare să investigheze o plângere care este depusă și după această perioadă, atât timp cât termenul de prescripție prevăzut de dreptul penal sau civil nu a expirat [articolul 32 alineatul (1) punctul (4) din Legea NHRC].

([152]) Articolul 42 și următoarele din Legea NHCR.

([153]) Articolele 36 și 37 din Legea NHRC.

([154]) Articolul 44 din Legea NHRC.

([155]) Articolul 42 alineatul (4) din Legea NHRC.

([156]) Articolul 48 din Legea NHRC.

([157]) De exemplu, dacă, în mod excepțional, NHRC nu este în măsură să inspecteze anumite materiale sau echipamente deoarece acestea se referă la secrete de stat care ar putea avea un efect semnificativ asupra securității statului sau a relațiilor diplomatice ori dacă inspecția ar reprezenta un obstacol major în calea unei anchete penale sau a unui proces în curs (a se vedea nota de subsol 166) și dacă acest lucru împiedică NHRC să efectueze ancheta necesară pentru a evalua temeinicia cererii primite, va informa persoana în cauză cu privire la motivele pentru care plângerea a fost respinsă, în conformitate cu articolul 39 din Legea NHRC. În acest caz, persoana în cauză ar putea contesta decizia NHRC în temeiul Legii privind contenciosul administrativ.

([158]) A se vedea, de exemplu, Hotărârea Înaltei Curți de la Seul 2007Nu27259 din 18 aprilie 2008, confirmată prin Hotărârea Curții Supreme 2008Du7854 din 9 octombrie 2008; Hotărârea Înaltei Curți de la Seul 2017Nu69382 din 2 februarie 2018.

([159]) Articolele 121 și 219 din CPA.

([160]) Articolul 417 din CPA coroborat cu articolul 414 alineatul (2) din CPA. A se vedea, de asemenea, Hotărârea Curții Supreme nr. 97Mo66 din 29 septembrie 1997.

În plus, persoanele fizice pot obține despăgubiri pentru daune în fața instanțelor coreene. În baza Legii privind despăgubirile acordate de stat, persoanele fizice pot solicita despăgubiri pentru prejudiciile cauzate de funcționarii publici în exercitarea atribuțiilor lor oficiale cu încălcarea legii ([161]). O cerere în temeiul Legii privind despăgubirile acordate de stat poate fi depusă la un „Consiliu pentru despăgubiri" specializat sau direct la instanțele coreene ([162]). În cazul în care victima este cetățean străin, Legea privind despăgubirile acordate de stat se aplică atât timp cât și țara de origine a cetățeanului respectiv asigură despăgubiri din partea statului pentru cetățenii coreeni ([163]). Conform jurisprudenței, această condiție este îndeplinită dacă cerințele pentru solicitarea de despăgubiri în cealaltă țară „nu sunt semnificativ disproporționate între Coreea și cealaltă țară" și „nu sunt, în general, mai stricte decât cele stabilite de Coreea, fără nicio diferență materială și de fond." ([164]) Codul civil reglementează răspunderea statului pentru despăgubiri și, în consecință, răspunderea statului acoperă, de asemenea, prejudiciile morale (de exemplu, suferința psihică) ([165]).

În cazul încălcării normelor privind protecția datelor, în cadrul PIPA este prevăzută o cale de atac suplimentară. În conformitate cu articolul 39 din PIPA, orice persoană care suferă prejudicii ca urmare a unei încălcări a PIPA sau a unei pierderi, a unui furt, a unei dezvăluiri, a unei falsificări, a unei modificări sau prejudicii aduse informațiilor sale cu caracter personal poate obține despăgubiri pentru daune în fața instanțelor. Nu există o cerință de reciprocitate similară celei prevăzute în Legea privind compensațiile acordate de stat.

În plus față de despăgubirile pentru daune, se pot obține reparații administrative în cazul acțiunilor sau omisiunilor agențiilor administrative în temeiul Legii privind contenciosul administrativ. Orice persoană fizică poate contesta o dispoziție (și anume, exercitarea sau refuzul de a exercita prerogative de autoritate publică într-un anumit caz) sau o omisiune (incapacitatea prelungită a unei agenții administrative de a adopta o anumită dispoziție contrară unei obligații legale de a face acest lucru), ceea ce poate duce la revocarea/modificarea unei dispoziții ilegale, la constatarea nulității (și anume, constatarea faptului că dispoziția nu are efect juridic sau inexistența sa în ordinea juridică) sau la constatarea că omisiunea este ilegală ([166]). Pentru a putea contesta o dispoziție administrativă, aceasta trebuie să aibă un impact direct asupra drepturilor și obligațiilor civile ([167]). Aceasta include măsuri de colectare a datelor cu caracter personal, fie direct (de exemplu, prin interceptarea comunicațiilor), fie prin intermediul unei cereri de divulgare (de exemplu, către un furnizor de servicii).

Cererile menționate anterior pot fi introduse mai întâi în fața comisiilor administrative de apel instituite în cadrul anumitor autorități publice (de exemplu, NIS, NHRC) sau în fața Comisiei administrative centrale de apel instituite în cadrul Comisiei pentru combaterea corupției și drepturile civile ([168]). O astfel de cale de atac administrativă oferă o cale alternativă, mai informală, de contestare a unei dispoziții sau a unei omisiuni a unei autorități publice. Cu toate acestea, o plângere poate fi introdusă direct în fața instanțelor coreene, în temeiul Legii privind contenciosul administrativ.

O cerere de revocare/modificare a unei dispoziții în temeiul Legii privind contenciosul administrativ poate fi depusă de orice persoană care are un interes juridic de a solicita revocarea/modificarea sau restabilirea drepturilor sale prin revocare/modificare în cazul în care dispoziția nu mai produce efecte ([169]). În mod similar, acțiunea în constatarea nulității poate fi introdusă de o persoană care are un interes juridic în această declarație, în timp ce un litigiu prin care se declară nelegalitatea unei omisiuni poate fi inițiat de orice persoană care a formulat o cerere de dispoziție și care are un interes juridic de a solicita declararea nelegalității omisiunii ([170]). În conformitate cu jurisprudența Curții Supreme, „interesul juridic" este interpretat ca un „interes protejat din punct de vedere juridic", și anume un interes direct și specific protejat prin acte cu putere de lege și norme administrative pe care se bazează dispozițiile administrative (nu interese generale, indirecte și abstracte ale publicului) ([171]). Prin urmare, persoanele fizice au un interes juridic în cazul oricărei încălcări a limitărilor și garanțiilor în legătură cu colectarea datelor lor cu caracter personal în scopul asigurării respectării dreptului penal (în temeiul unor legi specifice sau al PIPA). O hotărâre definitivă în temeiul Legii privind contenciosul administrativ este obligatorie pentru părți ([172]).

O cerere de revocare/modificare a unei dispoziții și o cerere de declarare a nelegalității unei omisiuni trebuie depuse în termen de 90 de zile de la data la care persoana respectivă a luat cunoștință de dispoziție/omisiune și, în principiu, nu

([161]) Articolul 2 alineatul (1) din Legea privind despăgubirile acordate de stat.
([162]) Articolele 9 și 12 din Legea privind despăgubirile acordate de stat. Legea instituie consilii districtuale (prezidate de procurorul adjunct al parchetului corespunzător), un consiliu central (prezidat de ministrul adjunct al justiției) și un consiliu special (prezidat de ministrul adjunct al apărării naționale și însărcinat cu cererile de despăgubire pentru prejudiciile cauzate de personalul militar sau de angajații civili ai armatei). Cererile de despăgubire sunt tratate, în principiu, de consiliile districtuale, care, în anumite circumstanțe, trebuie să înainteze cazurile consiliului central/special, de exemplu, atunci când despăgubirea depășește o anumită sumă sau când o persoană solicită o nouă deliberare. Toate consiliile sunt formate din membri numiți de ministrul justiției (de exemplu, din rândul funcționarilor publici din cadrul Ministerului Justiției, al executorilor judecătorești, al avocaților și al persoanelor cu expertiză în materie de despăgubiri acordate de stat) și fac obiectul unor norme specifice privind conflictul de interese (a se vedea articolul 7 din Decretul de punere în aplicare a Legii privind despăgubirile acordate de stat).
([163]) Articolul 7 din Legea privind despăgubirile acordate de stat.
([164]) Hotărârea Curții Supreme nr. 2013Da208388 din 11 iunie 2015.
([165]) A se vedea articolul 8 din Legea privind despăgubirile acordate de stat, precum și articolul 751 din Codul civil.
([166]) Articolele 2 și 4 din Legea privind contenciosul administrativ.
([167]) Hotărârea Curții Supreme 98Du18435 din 22 octombrie 1999, Hotărârea Curții Supreme 99Du1113 din 8 septembrie 2000 și Hotărârea Curții Supreme 2010Du3541 din 27 septembrie 2012.
([168]) Articolul 6 din Legea privind căile de atac administrative și articolul 18 alineatul (1) din Legea privind contenciosul administrativ.
([169]) Articolul 12 din Legea privind contenciosul administrativ.
([170]) Articolele 35 și 36 din Legea privind contenciosul administrativ.
([171]) Hotărârea Curții Supreme nr. 2006Du330 din 26 martie 2006.
([172]) Articolul 30 alineatul (1) din Legea privind contenciosul administrativ.

mai târziu de un an de la data emiterii dispoziției/apariției omisiunii, cu excepția cazului în care există motive justificabile ([173]). În conformitate cu jurisprudența Curții Supreme, noțiunea de „motive justificabile" trebuie interpretată în sens larg și necesită să se evalueze dacă este acceptabil din punct de vedere social să se permită o plângere tardivă, având în vedere toate circumstanțele cauzei ([174]). De exemplu, aceasta include (dar nu se limitează la) motivele pentru care partea în cauză nu poate fi considerată răspunzătoare (și anume, situații care se află în afara controlului reclamantului, de exemplu în cazul în care nu i-a fost notificată colectarea informațiilor sale cu caracter personal) sau cazurile de forță majoră (de exemplu, dezastru natural, război).

În cele din urmă, persoanele fizice pot, de asemenea, să depună o plângere constituțională la Curtea Constituțională ([175]). În temeiul Legii privind Curtea Constituțională, orice persoană ale cărei drepturi fundamentale garantate de Constituție sunt încălcate ca urmare a exercitării sau neexercitării puterii guvernamentale (cu excepția hotărârilor judecătorești) poate solicita soluționarea unei plângeri constituționale. Dacă sunt disponibile alte căi de atac, acestea trebuie mai întâi epuizate. În conformitate cu jurisprudența Curții Constituționale, cetățenii străini pot depune o plângere constituțională în măsura în care drepturile lor fundamentale sunt recunoscute în temeiul Constituției coreene (a se vedea explicațiile de la secțiunea 1.1) ([176]). Plângerile constituționale trebuie depuse în termen de 90 de zile de la data la care persoana respectivă a luat cunoștință de încălcare și în termen de un an de la producerea acesteia. Având în vedere că procedura din Legea privind contenciosul administrativ se aplică litigiilor în temeiul Legii privind Curtea Constituțională ([177]), o plângere va fi în continuare admisibilă dacă există „motive justificabile", astfel cum a fost interpretat în conformitate cu jurisprudența Curții Supreme descrisă mai sus.

Dacă trebuie epuizate mai întâi alte căi de atac, o plângere constituțională trebuie depusă în termen de 30 de zile de la hotărârea definitivă în legătură cu o astfel de cale de atac ([178]). Curtea Constituțională poate invalida exercitarea competenței guvernamentale care a cauzat încălcarea sau poate confirma că o anumită omisiune de a acționa este neconstituțională ([179]). În acest caz, autoritatea competentă este obligată să ia măsuri pentru a se conforma hotărârii Curții.

3. ACCESUL ADMINISTRAȚIEI PUBLICE ÎN SCOPURI LEGATE DE SECURITATEA NAȚIONALĂ

3.1. Autoritățile publice competente în domeniul securității naționale

Republica Coreea are două servicii de informații specializate: NIS și Comandamentul de sprijin pentru securitate în domeniul apărării. În plus, poliția și organele de urmărire penală pot, de asemenea, să colecteze informații cu caracter personal în scopuri legate de securitatea națională.

NIS este instituit prin Legea privind Serviciul Național de Informații („Legea NIS") și funcționează direct sub jurisdicția și supravegherea președintelui statului ([180]). În special, NIS colectează, compilează și distribuie informații privind țări străine (și Coreea de Nord) ([181]), informații referitoare la sarcina de combatere a spionajului (inclusiv spionaj militar și industrial), a terorismului și a activităților organizațiilor infracționale internaționale, informații privind anumite tipuri de infracțiuni îndreptate împotriva securității publice și naționale (de exemplu, insurecție internă, agresiune externă) și informații referitoare la sarcina de asigurare a securității cibernetice și de prevenire sau combatere a atacurilor și amenințărilor cibernetice ([182]). Legea NIS, care instituie NIS și stabilește sarcinile acestuia, prevede, de asemenea, principii generale pentru toate activitățile sale. Ca principiu general, NIS trebuie să mențină neutralitatea politică și să protejeze libertatea și drepturile persoanelor ([183]). Președintele NIS are sarcina de a elabora orientări generale care să stabilească principiile, domeniul de aplicare și procedurile pentru îndeplinirea atribuțiilor NIS în ceea ce privește colectarea și utilizarea informațiilor și trebuie să le raporteze Adunării Naționale ([184]). Adunarea Națională (prin intermediul Comisiei sale pentru informații) poate solicita corectarea sau completarea orientărilor în cazul în care consideră că acestea sunt ilegale sau injuste. La un nivel mai general, la îndeplinirea atribuțiilor lor, directorul și personalul NIS nu pot obliga nicio instituție, organizație sau persoană fizică să facă ceva ce nu este obligată să facă și nici să obstrucționeze exercitarea drepturilor de către nicio persoană abuzând de autoritatea lor oficială ([185]). În plus, orice cenzurare a corespondenței, interceptare a telecomunicațiilor, colectare a informațiilor de localizare, colectare a datelor de confirmare

([173]) Articolul 20 din Legea privind contenciosul administrativ. Acest termen se aplică, de asemenea, unei cereri de declarare a nelegalității unei omisiuni; a se vedea articolul 38 alineatul (2) din Legea privind contenciosul administrativ.
([174]) Hotărârea Curții Supreme 90Nu6521 din 28 iunie 1991.
([175]) Articolul 68 alineatul (1) din Legea privind Curtea Constituțională.
([176]) Hotărârea Curții Constituționale nr. 99HeonMa194 din 29 noiembrie 2001.
([177]) Articolul 40 din Legea privind Curtea Constituțională.
([178]) Articolul 69 din Legea privind Curtea Constituțională.
([179]) Articolul 75 alineatul (3) din Legea privind Curtea Constituțională.
([180]) Articolul 2 și articolul 4 alineatul (2) din Legea NIS.
([181]) Această noțiune nu se referă la informațiile privind persoanele fizice, ci la informații generale privind țările străine (tendințe, evoluții) și activitățile actorilor statali din țări terțe.
([182]) Articolul 3 alineatul (1) din Legea NIS.
([183]) Articolul 3 alineatul (1), articolul 6 alineatul (2), articolele 11 și 21. A se vedea, de asemenea, normele privind conflictele de interese, în special articolele 10 și 12.
([184]) Articolul 4 alineatul (2) din Legea NIS.
([185]) Articolul 13 din Legea NIS.

a comunicațiilor sau înregistrare ori ascultare a comunicațiilor private de către NIS trebuie să respecte CPPA, Legea privind informațiile de localizare sau CPA ([186]). Orice abuz de putere sau colectarea de informații care încalcă aceste legi face obiectul unor sancțiuni penale ([187]).

Comandamentul de sprijin pentru securitate în domeniul apărării este un serviciu militar de informații, înființat în cadrul Ministerului Apărării. Acesta este responsabil cu chestiunile legate de securitate din cadrul armatei, cu anchetele militare penale (sub rezerva Legii privind instanțele militare) și cu serviciile de informații militare. În general, Comandamentul de sprijin pentru securitate în domeniul apărării nu efectuează supravegherea civililor, cu excepția cazului în care acest lucru este necesar pentru îndeplinirea funcțiilor sale militare. Persoanele care pot fi anchetate sunt personalul militar, angajații civili ai armatei, persoanele care urmează programe de instruire militară, cadrele militare trecute în rezervă sau persoanele din serviciul de recrutare a cadrelor militare și prizonierii de război ([188]). Atunci când colectează informații privind comunicațiile în scopuri legate de securitatea națională, Comandamentul de sprijin pentru securitate în domeniul apărării face obiectul limitărilor și garanțiilor prevăzute în CPPA și în decretul de punere în aplicare a acesteia.

3.2. **Temeiuri juridice și limitări**

CPPA, Legea privind combaterea terorismului pentru protecția cetățenilor și securitatea publică („Legea privind combaterea terorismului") și TBA oferă temeiuri juridice pentru colectarea de informații cu caracter personal în scopuri legate de securitatea națională și stabilesc limitările și garanțiile aplicabile ([189]). Aceste limitări și garanții, astfel cum sunt descrise în secțiunile următoare, asigură limitarea colectării și a prelucrării informațiilor la ceea ce este strict necesar pentru atingerea unui obiectiv legitim. Aceasta exclude orice colectare în masă și arbitrară de informații cu caracter personal în scopuri legate de securitatea națională.

3.2.1. *Colectarea informațiilor privind comunicațiile*

3.2.1.1. Colectarea informațiilor privind comunicațiile de către serviciile de informații

3.2.1.1.1. Temei juridic

CPPA împuternicește serviciile de informații să colecteze date privind comunicațiile și impune furnizorilor de servicii de comunicații să coopereze la solicitările acestor agenții ([190]). Astfel cum se descrie în secțiunea 2.2.2.1, CPPA face distincție între colectarea conținutului comunicațiilor (și anume, „măsuri de restricționare a comunicațiilor", cum ar fi măsurile de „interceptare a comunicațiilor" sau de „cenzură" ([191])) și colectarea de „date de confirmare a comunicațiilor" ([192]).

Pragul pentru colectarea acestor două tipuri de informații diferă, dar procedurile și garanțiile aplicabile sunt în mare măsură identice ([193]). Colectarea datelor de confirmare a comunicațiilor (sau a metadatelor) poate avea loc în scopul prevenirii amenințărilor la adresa securității naționale ([194]). Se aplică un prag mai ridicat pentru executarea măsurilor de restricționare a comunicațiilor (și anume, pentru colectarea conținutului comunicațiilor), care pot fi luate numai atunci când se preconizează că securitatea națională va fi pusă în pericol grav, iar colectarea de informații este necesară pentru a preveni un astfel de pericol (și anume, când există un risc major pentru securitatea națională, iar colectarea este necesară pentru a preveni acest risc) ([195]). În plus, accesul la conținutul comunicațiilor poate fi obținut numai ca măsură de ultimă instanță pentru a asigura securitatea națională și trebuie depuse eforturi pentru a reduce la minimum încălcarea confidențialității comunicațiilor ([196]). Chiar și atunci când a fost obținută aprobarea/autorizarea corespunzătoare, astfel de măsuri trebuie să înceteze imediat după ce nu mai sunt necesare, asigurându-se astfel că orice încălcare a secretelor comunicațiilor unei persoane este limitată la minimum ([197]).

3.2.1.1.2. Limitări și garanții aplicabile colectării de informații privind comunicațiile care implică cel puțin un cetățean coreean

Colectarea de informații privind comunicațiile (atât în ceea ce privește conținutul, cât și metadatele) în cazul în care fie una, fie ambele persoane implicate în comunicații sunt cetățeni coreeni poate avea loc numai cu autorizarea

([186]) Articolul 14 din Legea NIS.
([187]) Articolele 22 și 23 din Legea NIS.
([188]) Articolul 1 din Legea privind instanțele militare.
([189]) Atunci când anchetează infracțiuni legate de securitatea națională, poliția și NIS vor acționa pe baza CPA, în timp ce Comandamentul de sprijin pentru securitate în domeniul apărării face obiectul Legii privind instanțele militare.
([190]) Articolul 15-2 din CPPA.
([191]) Articolul 2 alineatele (6) și (7) din CPPA.
([192]) Articolul 2 alineatul (11) din CPPA.
([193]) A se vedea, de asemenea, articolul 13-4 alineatul (2) din CPPA și articolul 37 alineatul (4) din Decretul de punere în aplicare a CPPA, care prevăd că procedurile aplicabile colectării conținutului comunicațiilor se aplică *mutatis mutandis* colectării datelor de confirmare a comunicațiilor.
([194]) Articolul 13-4 din CPPA.
([195]) Articolul 7 alineatul (1) din CPPA.
([196]) Articolul 3 alineatul (2) din CPPA.
([197]) Articolul 2 din Decretul de punere în aplicare a CPPA.

președintelui Înaltei Curți ([198]). Cererea din partea serviciilor de informații trebuie adresată în scris unui procuror sau biroului procurorului general ([199]). Aceasta trebuie să indice motivele colectării (și anume, faptul că se preconizează că securitatea națională va fi pusă în pericol grav sau că o colectare este necesară pentru prevenirea amenințărilor la adresa securității naționale), împreună cu materiale care sprijină aceste motive și care stabilesc o prezumție, precum și detaliile cererii [și anume, obiectivele, persoana (persoanele) vizată (vizate), domeniul de aplicare, perioada efectivă de colectare, precum și modul și locul în care va avea loc colectarea] ([200]). La rândul său, procurorul/biroul procurorului general solicită autorizarea președintelui Înaltei Curți ([201]). Președintele Înaltei Curți poate acorda autorizarea scrisă numai în cazul în care consideră că cererea este justificată și va respinge cererea atunci când o consideră nefondată ([202]). Mandatul specifică tipul, obiectivul, ținta, domeniul de aplicare și perioada efectivă de colectare, precum și locul și modul în care aceasta poate avea loc ([203]).

În cazul în care măsura vizează investigarea unui act de asociere infracțională care amenință securitatea națională și există o situație de urgență care face imposibilă parcurgerea procedurilor menționate anterior, se aplică norme specifice ([204]). Atunci când aceste condiții sunt îndeplinite, serviciile de informații pot aplica măsuri de supraveghere fără aprobarea prealabilă a instanței ([205]). Cu toate acestea, imediat după executarea măsurilor de urgență, serviciul de informații trebuie să solicite autorizarea instanței. În cazul în care nu se obține autorizarea în termen de 36 de ore de la momentul în care sunt luate măsurile, acestea trebuie să înceteze imediat ([206]). Colectarea de informații în situații de urgență trebuie să aibă loc întotdeauna în conformitate cu o „declarație privind cenzura/interceptarea comunicațiilor de urgență”, iar serviciul de informații care efectuează colectarea trebuie să țină un registru al tuturor măsurilor de urgență ([207]).

În cazurile în care supravegherea este finalizată într-un termen scurt, eliminând astfel necesitatea obținerii unei autorizări din partea instanței, șeful biroului procurorului general competent trebuie să trimită o notificare privind măsura de urgență pregătită de serviciul de informații președintelui instanței competente, care păstrează registrul măsurilor de urgență ([208]). Acest lucru permite instanței să examineze legalitatea colectării.

3.2.1.1.3. Limitări și garanții aplicabile în cazul colectării de informații privind comunicațiile care implică doar persoane de altă cetățenie decât cea coreeană

Pentru a colecta informații privind comunicațiile care au loc exclusiv între persoane de altă cetățenie decât cea coreeană, serviciile de informații trebuie să obțină în prealabil aprobarea scrisă a președintelui statului ([209]). Astfel de comunicații vor fi colectate în scopuri legate de securitatea națională numai dacă se încadrează în una dintre categoriile enumerate, și anume comunicații între funcționari guvernamentali sau alte persoane din țări ostile Republicii Coreea, agenții străine, grupuri sau cetățeni suspectați de implicare în activități anticoreene ([210]) sau membri ai grupurilor care operează în Peninsula Coreeană, dar care depășesc efectiv suveranitatea Republicii Coreea și grupurile lor umbrelă cu sediul în țări străine ([211]). În schimb, în cazul în care o parte la comunicații este cetățean coreean, iar cealaltă parte are altă cetățenie decât cea coreeană, va fi necesară aprobarea instanței în conformitate cu procedura descrisă în secțiunea 3.2.1.1.2.

Șeful unui serviciu de informații trebuie să prezinte directorului NIS un plan privind măsurile care urmează să fie luate ([212]). Directorul NIS analizează dacă planul este adecvat și, în caz afirmativ, îl transmite președintelui statului spre aprobare ([213]). Informațiile care trebuie incluse în plan sunt identice cu informațiile necesare pentru o cerere de autorizare din partea instanței de a colecta informații privind cetățenii coreeni (astfel cum se descrie mai sus) ([214]). În special, aceasta trebuie să indice motivele colectării (și anume, faptul că se preconizează că securitatea națională va fi pusă în pericol grav sau că o colectare este necesară pentru prevenirea amenințărilor la adresa securității naționale),

([198]) Articolul 7 alineatul (1) punctul 1 din CPPA. Instanța competentă este instanța superioară care are competență în ceea ce privește locul de domiciliu sau sediul uneia sau al ambelor părți care face/fac obiectul supravegherii.
([199]) Articolul 7 alineatul (3) din Decretul de punere în aplicare a CPPA.
([200]) Articolul 7 alineatul (3) și articolul 6 alineatul (4) din CPPA.
([201]) Articolul 7 alineatul (4) din Decretul de punere în aplicare a CPPA. Cererea procurorului adresată instanței trebuie să prezinte principalele motive de suspiciune și, în măsura în care sunt solicitate în același timp mai multe autorizări, justificarea acestora (a se vedea articolul 4 din Decretul de punere în aplicare a CPPA).
([202]) Articolul 7 alineatul (3), articolul 6 alineatul (5) și articolul 6 alineatul (9) din CPPA.
([203]) Articolul 7 alineatul (3) și articolul 6 alineatul (6) din CPPA.
([204]) Articolul 8 din CPPA.
([205]) Articolul 8 alineatul (1) din CPPA.
([206]) Articolul 8 alineatul (2) din CPPA.
([207]) Articolul 8 alineatul (4) din CPPA. A se vedea secțiunea 2.2.2.2 de mai sus pentru măsurile de urgență în contextul aplicării legii.
([208]) Articolul 8 alineatele (5) și (7) din CPPA. Această notificare trebuie să indice obiectivul, ținta, domeniul de aplicare, perioada, locul de executare și metoda de supraveghere, precum și motivele pentru care nu s-a depus o cerere înainte de luarea măsurii [articolul 8 alineatul (6) din CPPA].
([209]) Articolul 7 alineatul (1) punctul 2 din CPPA.
([210]) Aceasta se referă la activități care amenință existența și siguranța națiunii, ordinea democratică sau supraviețuirea și libertatea poporului.
([211]) În plus, în cazul în care una dintre părți este o persoană descrisă la articolul 7 alineatul (1) punctul 2 din CPPA, iar cealaltă parte este necunoscută sau nu poate fi specificată, se aplică procedura prevăzută la articolul 7 alineatul (1) punctul 2.
([212]) Articolul 8 alineatul (1) din Decretul de punere în aplicare a CPPA. Directorul NIS este numit de președintele statului în urma confirmării de către Parlament (articolul 7 din Legea NIS).
([213]) Articolul 8 alineatul (2) din Decretul de punere în aplicare a CPPA.
([214]) Articolul 8 alineatul (3) din Decretul de punere în aplicare a CPPA coroborat cu articolul 6 alineatul (4) din CPPA.

principalele motive de suspiciune, împreună cu materialele care sprijină aceste motive și care stabilesc o prezumție, precum și detaliile cererii [și anume, obiectivele, persoana (persoanele) vizată (vizate), domeniul de aplicare, perioada efectivă de colectare, precum și modul și locul în care va avea loc colectarea]. În cazul în care se solicită mai multe autorizări în același timp, scopul și motivele care stau la baza acestora ([215]).

În situații de urgență ([216]), trebuie obținută aprobarea prealabilă din partea ministrului în subordinea căruia se află serviciul de informații relevant. Totuși, în acest caz, serviciul de informații trebuie să solicite aprobarea președintelui statului imediat după luarea măsurilor de urgență. În cazul în care un serviciu de informații nu obține aprobarea în termen de 36 de ore de la depunerea cererii, colectarea trebuie întreruptă imediat ([217]). În astfel de cazuri, informațiile colectate vor fi întotdeauna distruse.

3.2.1.1.4. Limitări și garanții generale

Atunci când solicită cooperarea entităților private, serviciile de informații trebuie să le prezinte mandatul judecătoresc/autorizarea prezidențială sau o copie a copertei unei declarații privind cenzura de urgență, pe care entitatea obligată trebuie să o păstreze în dosarele sale ([218]). Entitățile cărora li se solicită să divulge informații serviciilor de informații în baza CPPA pot refuza acest lucru atunci când autorizația sau declarația privind cenzura de urgență se referă la un identificator eronat (de exemplu, un număr de telefon aparținând altei persoane decât cea identificată). În plus, parolele utilizate pentru comunicații nu pot fi divulgate în niciun caz ([219]).

Serviciile de informații pot încredința punerea în aplicare a măsurilor de restricționare a comunicațiilor sau colectarea de informații de confirmare a comunicațiilor unui oficiu poștal sau unui furnizor de servicii de telecomunicații (astfel cum sunt definite în Legea privind activitățile de telecomunicații) ([220]). Atât serviciul de informații relevant, cât și furnizorul care primește o cerere de cooperare trebuie să păstreze timp de trei ani registre care să indice scopul solicitării măsurilor, data executării sau a cooperării și obiectul măsurilor (de exemplu, poștă, telefon, e-mail) ([221]). Furnizorii de servicii de telecomunicații care furnizează date de confirmare a comunicațiilor trebuie să păstreze informațiile privind frecvența colectării în dosarele lor timp de șapte ani și să prezinte un raport de două ori pe an ministrului științei și TIC ([222]).

Serviciile de informații trebuie să prezinte directorului NIS un raport cu privire la informațiile pe care le-au colectat și la rezultatul activității de supraveghere ([223]). În ceea ce privește colectarea datelor de confirmare a comunicațiilor, trebuie să se țină evidența faptului că a fost depusă o cerere pentru astfel de date, precum și a cererii scrise în sine și a instituției care s-a bazat pe aceasta ([224]).

Colectarea atât a conținutului comunicațiilor, cât și a datelor de confirmare a comunicațiilor se poate desfășura numai pe o perioadă maximă de patru luni și, dacă obiectivul urmărit este atins între timp, trebuie întreruptă imediat ([225]). În cazul în care condițiile de autorizare persistă, termenul poate fi prelungit cu până la patru luni, cu autorizarea din partea instanței sau cu aprobarea președintelui statului. Cererea de obținere a aprobării pentru extinderea măsurilor de supraveghere trebuie făcută în scris, precizând motivele pentru care se solicită prelungirea și furnizând materiale justificative ([226]).

În funcție de temeiul juridic pentru colectare, persoanele fizice sunt, în general, informate atunci când comunicațiile lor sunt colectate. În special, indiferent dacă informațiile colectate se referă la conținutul comunicațiilor sau la datele de confirmare a comunicațiilor și indiferent dacă informațiile au fost obținute prin procedura ordinară sau într-o situație de urgență, șeful serviciului de informații trebuie să notifice în scris persoanei în cauză măsura de supraveghere în termen de 30 de zile de la data încetării supravegherii ([227]). Notificarea trebuie să menționeze (1) faptul că informațiile au fost

([215]) Articolul 8 alineatul (3) și articolul 4 din Decretul de punere în aplicare a CPPA.
([216]) Și anume, atunci când, în cazurile în care măsura vizează un act de asociere infracțională care amenință securitatea națională, nu există suficient timp pentru a obține aprobarea președintelui statului, iar neadoptarea unor măsuri de urgență poate afecta securitatea națională [articolul 8 alineatul (8) din CPPA].
([217]) Articolul 8 alineatul (9) din CPPA.
([218]) Articolul 9 alineatul (2) din CPPA și articolul 12 din Decretul de punere în aplicare a CPPA.
([219]) Articolul 9 alineatul (4) din CPPA.
([220]) Articolul 13 din Decretul de punere în aplicare a CPPA.
([221]) Articolul 9 alineatul (3) din CPPA și articolul 17 alineatul (2) din Decretul de punere în aplicare a CPPA. Această perioadă de timp nu se aplică datelor de confirmare a comunicațiilor (a se vedea articolul 39 din Decretul de punere în aplicare a CPPA).
([222]) Articolul 13 alineatul (7) din CPPA și articolul 39 din Decretul de punere în aplicare a CPPA.
([223]) Articolul 18 alineatul (3) din Decretul de punere în aplicare a CPPA.
([224]) Articolul 13 alineatul (5) și articolul 13-4 alineatul (3) din CPPA.
([225]) Articolul 7 alineatul (2) din CPPA.
([226]) Articolul 7 alineatul (2) din CPPA și articolul 5 din Decretul de punere în aplicare a CPPA.
([227]) Articolul 9-2 alineatul (3) din CPPA. În conformitate cu articolul 13-4 din CPPA, acest lucru se aplică atât colectării conținutului comunicațiilor, cât și datelor de confirmare a comunicațiilor.

colectate, (2) agenția executantă și (3) perioada de executare. Cu toate acestea, dacă este probabil ca notificarea să pună în pericol securitatea națională sau să dăuneze vieții și siguranței fizice a persoanelor, notificarea poate fi amânată ([228]). Notificarea trebuie transmisă în termen de 30 de zile de la încetarea motivelor de amânare ([229]).

Această cerință de notificare se aplică însă numai colectării de informații în cazul în care cel puțin una dintre părți este cetățean coreean. În consecință, persoanele de altă cetățenie decât cea coreeană vor fi notificate numai atunci când sunt colectate comunicațiile lor cu cetățeni coreeni. Prin urmare, nu există nicio cerință de notificare atunci când sunt colectate comunicații care au loc exclusiv între persoane de altă cetățenie decât cea coreeană.

Conținutul comunicațiilor, precum și datele de confirmare a comunicațiilor obținute prin supraveghere în temeiul CPPA pot fi utilizate numai (1) pentru investigarea, urmărirea penală sau prevenirea anumitor infracțiuni, (2) pentru procedurile disciplinare, (3) pentru procedurile judiciare în care o parte a comunicațiilor se bazează pe acestea într-o cerere de despăgubiri sau (4) în temeiul altor legi ([230]).

3.2.1.2. Colectarea informațiilor privind comunicațiile de către poliție/procurori în scopuri legate de securitatea națională

Poliția/procurorul poate colecta informații privind comunicațiile (atât conținutul comunicațiilor, cât și datele de confirmare a comunicațiilor) în scopuri legate de securitatea națională în aceleași condiții precum cele descrise în secțiunea 3.2.1.1. Atunci când se acționează în situații de urgență ([231]), procedura aplicabilă este cea descrisă anterior în ceea ce privește colectarea conținutului comunicațiilor în scopul aplicării legii în situații de urgență (și anume articolul 8 din CPPA).

3.2.2. *Colectarea de informații privind persoanele suspectate de terorism*

3.2.2.1. Temei juridic

Legea privind combaterea terorismului conferă directorului NIS competența de a colecta informații privind persoanele suspectate de terorism ([232]). O „persoană suspectată de terorism" este definită ca fiind un membru al unei grupări teroriste ([233]), o persoană care a contribuit la propagarea unei grupări teroriste (prin promovarea și diseminarea ideilor sau tacticilor unei grupări teroriste), a colectat sau a contribuit cu fonduri destinate terorismului ([234]) sau a fost implicată în alte activități de pregătire, asociere infracțională, propagandă sau instigare la terorism ori o persoană în legătură cu care există motive întemeiate pentru a fi suspectată că ar fi desfășurat astfel de activități ([235]). Ca regulă generală, orice funcționar public care aplică Legea privind combaterea terorismului trebuie să respecte drepturile fundamentale consacrate în Constituția coreeană ([236]).

Legea privind combaterea terorismului nu stabilește în sine competențe, limitări și garanții specifice pentru colectarea de informații privind persoanele suspectate de terorism, ci se referă mai degrabă la procedurile prevăzute de alte legi. În primul rând, în temeiul Legii privind combaterea terorismului, directorul NIS poate colecta (1) informații privind intrarea în și ieșirea din Republica Coreea, (2) informații privind tranzacțiile financiare și (3) informații privind comunicațiile. În funcție de tipul de informații solicitate, cerințele procedurale relevante sunt prevăzute în Legea privind imigrația și în Legea vamală, în ARUSFTI sau, respectiv, în CPPA ([237]). Pentru colectarea de informații privind intrarea în și ieșirea din Coreea, Legea privind combaterea terorismului se referă la procedurile prevăzute în Legea privind imigrația și în Legea

([228]) Articolul 9-2 alineatul (4) din CPPA.
([229]) Articolul 13-4 alineatul (2) și articolul 9-2 alineatul (6) din CPPA.
([230]) Articolul 5 alineatele (1)-(2), articolul 12 și articolul 13-5 din CPPA.
([231]) Și anume, atunci când măsura vizează un act de asociere infracțională care amenință securitatea națională și există o situație de urgență care face imposibilă parcurgerea procedurii de aprobare ordinare [articolul 8 alineatul (1) din CPPA].
([232]) Articolul 9 din Legea privind combaterea terorismului.
([233]) O „grupare teroristă" este definită ca un grup de teroriști desemnat de Organizația Națiunilor Unite [articolul 2 alineatul (2) din Legea privind combaterea terorismului].
([234]) „Terorismul" este definit la articolul 2 alineatul (1) din Legea privind combaterea terorismului ca fiind un comportament menit să împiedice exercitarea autorității statului, a unei administrații locale sau a unui guvern străin (inclusiv a administrațiilor locale și a organizațiilor internaționale) sau menit să îl/o oblige să acționeze fără a avea o obligație în acest sens ori să amenințe publicul. Aceasta include (a) uciderea unei persoane sau punerea în pericol a vieții unei persoane prin vătămare corporală sau arestarea, izolarea, răpirea unei persoane sau luarea de ostatici; (b) anumite tipuri de comportament care vizează o aeronavă (de exemplu, prăbușirea, deturnarea sau deteriorarea unei aeronave aflate în zbor); (c) anumite tipuri de comportament în legătură cu o navă (de exemplu, sechestrarea unei nave sau a unei structuri marine aflate în funcțiune, distrugerea unei nave sau a unei structuri marine aflate în funcțiune sau provocarea de daune asupra acesteia într-o măsură care să pună în pericol siguranța acesteia, inclusiv deteriorarea încărcăturii de pe o navă sau o structură marină aflată în funcțiune); (d) plasarea, detonarea sau utilizarea în orice alt mod a unei arme sau a unui dispozitiv biochimic, exploziv sau incendiar cu intenția de a cauza moartea, vătămarea gravă sau daune materiale grave ori care are un astfel de efect asupra anumitor tipuri de vehicule sau instalații (de exemplu, trenuri, tramvaie, autovehicule, parcuri și stații publice, instalații de furnizare de energie electrică, gaze și telecomunicații etc.); (e) anumite tipuri de comportament legate de materiale nucleare, materiale radioactive sau instalații nucleare (de exemplu, punerea în pericol a vieții oamenilor, a integrității fizice sau a bunurilor sau perturbarea siguranței publice prin distrugerea unui reactor nuclear sau manipularea incorectă a materialelor radioactive etc.).
([235]) Articolul 2 alineatul (3) din Legea privind combaterea terorismului.
([236]) Articolul 3 alineatul (3) din Legea privind combaterea terorismului.
([237]) Articolul 9 alineatul (1) din Legea privind combaterea terorismului.

vamală. Totuși, în prezent, aceste legi nu prevăd astfel de competențe. Pentru colectarea informațiilor privind comunicațiile și a informațiilor privind tranzacțiile financiare, Legea privind combaterea terorismului face trimitere la limitările și garanțiile prevăzute în CPPA (detaliate mai jos) și în ARUSFTI (care, după cum se explică în secțiunea 2.1, nu este relevantă în scopul evaluării pentru decizia privind caracterul adecvat al nivelului de protecție).

În plus, articolul 9 alineatul (3) din Legea privind combaterea terorismului prevede că directorul NIS poate solicita informații cu caracter personal sau informații privind localizarea unei persoane suspectate de terorism de la un operator de informații cu caracter personal ([238]) sau de la un furnizor de informații de localizare ([239]). Această posibilitate este limitată la cererile de divulgare voluntară, la care operatorii de informații cu caracter personal și furnizorii de informații de localizare nu sunt obligați să răspundă și, în orice caz, pot face acest lucru numai în conformitate cu PIPA și cu Legea privind informațiile de localizare (a se vedea secțiunea 3.2.2.2 de mai jos).

3.2.2.2. Limitări și garanții aplicabile în cazul divulgării voluntare în temeiul PIPA și al Legii privind informațiile de localizare

Cererile de cooperare voluntară în temeiul Legii privind combaterea terorismului trebuie să se limiteze la informațiile privind persoanele suspectate de terorism (a se vedea secțiunea 3.2.2.1 de mai sus). Orice astfel de solicitare din partea NIS trebuie să respecte principiile legalității, necesității și proporționalității care decurg din Constituția Coreei [articolul 12 alineatul (1) și articolul 37 alineatul (2)] ([240]), precum și cerințele PIPA pentru colectarea de informații cu caracter personal [articolul 3 alineatul (1) din PIPA; a se vedea secțiunea 1.2 de mai sus]. Legea NIS prevede, de asemenea, că NIS nu poate obliga nicio instituție, organizație sau persoană fizică să facă nimic din ceea ce nu este obligată să facă, nici să obstrucționeze exercitarea drepturilor de către nicio persoană abuzând de autoritatea sa oficială ([241]). O încălcare a acestei interdicții poate face obiectul unor sancțiuni penale ([242]).

Operatorii de informații cu caracter personal și furnizorii de informații de localizare care primesc cereri din partea NIS în temeiul Legii privind combaterea terorismului nu sunt obligați să se conformeze. Aceștia se pot conforma în mod voluntar, dar li se permite să facă acest lucru numai în conformitate cu PIPA și cu Legea privind informațiile de localizare.. În ceea ce privește conformitatea cu PIPA, operatorul trebuie să țină seama în special de interesele persoanei vizate și nu poate divulga informațiile în cazul în care acestea ar putea aduce atingere în mod abuziv intereselor persoanei sau ale unui terț ([243]). În plus, în conformitate cu Notificarea nr. 2021-1 privind normele suplimentare pentru interpretarea și aplicarea Legii privind protecția informațiilor cu caracter personal, persoana în cauză trebuie să fie informată în legătură cu divulgarea. În situații excepționale, o astfel de notificare poate fi amânată, în special dacă și atât timp cât aceasta ar pune în pericol o anchetă penală în curs sau ar putea dăuna vieții sau integrității fizice a unei alte persoane, în cazul în care aceste drepturi sau interese sunt în mod evident superioare drepturilor persoanei vizate ([244]).

3.2.2.3. Limitări și garanții în temeiul CPPA

În temeiul Legii privind combaterea terorismului, serviciile de informații pot colecta informații privind comunicațiile (atât conținutul comunicațiilor, cât și datele de confirmare a comunicațiilor) numai atunci când sunt necesare pentru activități de combatere a terorismului, și anume activități legate de prevenirea terorismului și de contramăsuri împotriva acestuia. Procedurile din CPPA descrise în secțiunea 3.2.1 se aplică în cazul colectării de informații privind comunicațiile în scopuri antiteroriste.

3.2.3. *Divulgarea voluntară de către operatorii din sectorul telecomunicațiilor*

În temeiul TBA, operatorii din sectorul telecomunicațiilor pot da curs unei cereri de divulgare a „datelor privind comunicațiile" din partea unui serviciu de informații care intenționează să colecteze informațiile pentru a preveni o amenințare la adresa securității naționale ([245]). Orice astfel de solicitare trebuie să respecte principiile legalității, necesității și proporționalității care decurg din Constituția Coreei [articolul 12 alineatul (1) și articolul 37 alineatul (2)] ([246]), precum și cerințele PIPA pentru colectarea de informații cu caracter personal [articolul 3 alineatul (1) din PIPA; a se vedea secțiunea 1.2 de mai sus]. În plus, se aplică aceleași limitări și garanții ca și în cazul divulgărilor voluntare în scopul aplicării legii (a se vedea secțiunea 2.2.3) ([247]).

([238]) Astfel cum este definit la articolul 2 din PIPA, și anume o instituție publică, o persoană juridică, o organizație, o persoană fizică etc. care prelucrează informații cu caracter personal în mod direct sau indirect pentru a gestiona dosarele cu informații cu caracter personal în scopuri oficiale sau comerciale.

([239]) Astfel cum este definit la articolul 5 din Legea privind protecția, utilizarea etc. a informațiilor de localizare (denumită în continuare „Legea privind informațiile de localizare"), și anume orice persoană care a obținut autorizarea Comisiei coreene pentru comunicații de a desfășura o activitate care implică informații de localizare.

([240]) A se vedea, de asemenea, articolul 3 alineatele (2) și (3) din Legea privind combaterea terorismului.

([241]) Articolul 11 alineatul (1) din Legea NIS.

([242]) Articolul 19 din Legea NIS.

([243]) Articolul 18 alineatul (2) din PIPA.

([244]) Notificarea nr. 2021-1 a PIPC privind normele suplimentare pentru interpretarea și aplicarea Legii privind protecția informațiilor cu caracter personal, secțiunea III punctul 2 subpunctul (iii).

([245]) Articolul 83 alineatul (3) din TBA.

([246]) A se vedea, de asemenea, articolul 3 alineatele (2) și (3) din Legea privind combaterea terorismului.

([247]) În special, cererea trebuie să fie formulată în scris și să precizeze motivele sale, precum și legătura cu utilizatorul relevant și domeniul de aplicare al informațiilor solicitate, iar furnizorul de servicii de telecomunicații trebuie să țină evidențe și să prezinte, de două ori pe an, ministrului științei și TIC un raport în acest sens.

Operatorii din sectorul telecomunicațiilor nu sunt obligați să se conformeze, dar pot face acest lucru în mod voluntar și numai în conformitate cu PIPA. În acest sens, aceleași obligații, inclusiv în ceea ce privește notificarea persoanei, se aplică operatorilor din sectorul telecomunicațiilor ca și atunci când primesc solicitări din partea autorităților de asigurare a respectării dreptului penal, astfel cum se explică mai detaliat în secțiunea 2.2.3.

3.3. **Supravegherea**

Diferite organisme supraveghează activitățile serviciilor coreene de informații. Supravegherea Comandamentului de sprijin pentru securitate în domeniul apărării este efectuată de Ministerul Apărării Naționale, în conformitate cu Directiva ministerului privind punerea în aplicare a auditului intern. NIS face obiectul supravegherii de către executiv, Adunarea Națională și alte organisme independente, astfel cum se explică în detaliu mai jos.

3.3.1. *Responsabilul cu protecția drepturilor omului*

Atunci când serviciile de informații colectează informații privind persoanele suspectate de terorism, Legea privind combaterea terorismului prevede supravegherea de către Comisia pentru combaterea terorismului și de către responsabilul cu protecția drepturilor omului (*Human Rights Protection Officer* – „HRPO") ([248]).

Comisia pentru combaterea terorismului elaborează, printre altele, politici privind activitățile de combatere a terorismului și supraveghează punerea în aplicare a măsurilor de combatere a terorismului, precum și activitățile diferitelor autorități competente în domeniul combaterii terorismului ([249]). Comisia este prezidată de prim-ministru și este alcătuită din mai mulți miniștri și șefi ai agențiilor guvernamentale, inclusiv ministrul afacerilor externe, ministrul justiției, ministrul apărării naționale, ministrul internelor și siguranței, directorul NIS, comisarul general al Agenției Naționale de Poliție și președintele Comisiei pentru servicii financiare ([250]). Atunci când desfășoară investigații privind combaterea terorismului și identifică persoanele suspectate de terorism pentru a colecta informații sau materiale necesare pentru activități de combatere a terorismului, directorul NIS trebuie să prezinte un raport președintelui Comisiei pentru combaterea terorismului (și anume, prim-ministrului) ([251]).

În plus, Legea privind combaterea terorismului instituie HRPO pentru a proteja drepturile fundamentale ale persoanelor fizice împotriva încălcărilor cauzate de activitățile de combatere a terorismului ([252]). HRPO este numit de președintele Comisiei pentru combaterea terorismului din rândul persoanelor care îndeplinesc calificările enumerate în Decretul de punere în aplicare a Legii privind combaterea terorismului [și anume, orice persoană calificată drept avocat, cu experiență profesională de cel puțin zece ani sau cu cunoștințe de specialitate în domeniul drepturilor omului și care ocupă sau a ocupat (cel puțin) funcția de conferențiar timp de cel puțin zece ani sau care a ocupat funcția de înalt funcționar public în cadrul agențiilor de stat sau al administrațiilor locale ori care are cel puțin zece ani de experiență profesională în domeniul drepturilor omului, de exemplu într-o organizație neguvernamentală] ([253]). HRPO este numit pentru o perioadă de doi ani (cu posibilitate de reînnoire a mandatului) și poate fi demis din funcție doar din motive specifice, limitate și întemeiate, de exemplu atunci când este pus sub acuzare într-un dosar penal legat de îndatoririle sale, atunci când a divulgat informații confidențiale sau din cauza unei incapacități psihice sau fizice pe termen lung ([254]).

În ceea ce privește competențele, HRPO poate emite recomandări pentru îmbunătățirea protecției drepturilor omului de către agențiile implicate în activități de combatere a terorismului și pentru prelucrarea petițiilor civile (a se vedea secțiunea 3.4.3) ([255]). În cazul în care existența unei încălcări a drepturilor omului în exercitarea atribuțiilor oficiale poate fi stabilită în mod rezonabil, HRPO poate recomanda șefului agenției responsabile să corecteze o astfel de încălcare ([256]). La rândul său, agenția responsabilă trebuie să notifice HRPO acțiunile întreprinse pentru punerea în aplicare a unei astfel de recomandări ([257]). În cazul în care o agenție nu ar pune în aplicare o recomandare a HRPO, chestiunea ar fi înaintată Comisiei, inclusiv președintelui acesteia, prim-ministrului. Până în prezent, nu au existat cazuri în care recomandările HRPO să nu fie puse în aplicare.

3.3.2. *Adunarea Națională*

Astfel cum se descrie în secțiunea 2.3.2, Adunarea Națională poate investiga și inspecta autoritățile publice și, în acest context, poate solicita prezentarea de documente și poate obliga la înfățișarea martorilor. În ceea ce privește chestiunile care intră în competența NIS, acest control parlamentar este efectuat de Comisia pentru informații a Adunării Naționale ([258]). Directorul NIS, care supraveghează îndeplinirea sarcinilor de către agenție, raportează Comisiei pentru

([248]) Articolul 7 din Legea privind combaterea terorismului.
([249]) Articolul 5 alineatul (3) din Legea privind combaterea terorismului.
([250]) Articolul 3 alineatul (1) din Decretul de punere în aplicare a Legii privind combaterea terorismului.
([251]) Articolul 9 alineatul (4) din Legea privind combaterea terorismului.
([252]) Articolul 7 din Legea privind combaterea terorismului.
([253]) Articolul 7 alineatul (1) din Decretul de punere în aplicare a Legii privind combaterea terorismului.
([254]) Articolul 7 alineatul (3) din Decretul de punere în aplicare a Legii privind combaterea terorismului.
([255]) Articolul 8 alineatul (1) din Decretul de punere în aplicare a Legii privind combaterea terorismului.
([256]) Articolul 9 alineatul (1) din Decretul de punere în aplicare a Legii privind combaterea terorismului. HRPO decide în mod autonom cu privire la adoptarea recomandărilor, dar trebuie să prezinte un raport cu aceste recomandări președintelui Comisiei pentru combaterea terorismului.
([257]) Articolul 9 alineatul (2) din Decretul de punere în aplicare a Legii privind combaterea terorismului.
([258]) Articolul 36 și articolul 37 alineatul (1) punctul 16 din Legea privind Adunarea Națională.

informații (precum și președintelui) ([259]). Comisia pentru informații poate solicita, de asemenea, un raport cu privire la o anumită chestiune, la care directorul NIS trebuie să răspundă fără întârziere ([260]). Acesta poate refuza să răspundă sau să depună mărturie în fața Comisiei pentru informații numai cu privire la secretele de stat referitoare la chestiuni militare, diplomatice sau legate de Coreea de Nord, în cazul cărora publicarea ar putea avea un impact grav asupra destinului național ([261]). În acest caz, Comisia pentru informații poate solicita o explicație din partea prim-ministrului. Dacă o astfel de explicație nu este prezentată în termen de șapte zile de la depunerea cererii, răspunsul sau mărturia nu mai pot fi refuzate.

Dacă Adunarea Națională constată că a avut loc o activitate ilegală sau necorespunzătoare, aceasta poate solicita autorității publice relevante să ia măsuri de remediere, inclusiv acordarea de despăgubiri, luarea de măsuri disciplinare și îmbunătățirea procedurilor sale interne ([262]). În urma unei astfel de solicitări, autoritatea trebuie să acționeze fără întârziere și să raporteze rezultatul Adunării Naționale. Există norme specifice privind controlul parlamentar în ceea ce privește utilizarea măsurilor de restricționare a comunicațiilor (și anume colectarea conținutului comunicațiilor) în temeiul CCPA ([263]). În legătură cu aceasta din urmă, Adunarea Națională poate solicita șefilor serviciilor de informații un raport privind orice măsură specifică de restricționare a comunicațiilor. În plus, aceasta poate efectua inspecții la fața locului ale echipamentelor de interceptare a comunicațiilor. În cele din urmă, serviciile de informații care au colectat și operatorii care au divulgat informații referitoare la conținut în scopuri legate de securitatea națională trebuie să raporteze cu privire la o astfel de divulgare la cererea Adunării Naționale.

3.3.3. *Comisia de audit și inspecție*

BAI îndeplinește aceleași funcții de supraveghere în ceea ce privește serviciile de informații ca și în domeniul asigurării respectării dreptului penal (a se vedea secțiunea 2.3.2) ([264]).

3.3.4. *Comisia pentru protecția informațiilor cu caracter personal*

În ceea ce privește prelucrarea datelor în scopuri legate de securitatea națională, inclusiv în etapa de colectare, PIPC efectuează o supraveghere suplimentară. Astfel cum s-a explicat mai detaliat în secțiunea 1.2, aceasta include principiile și obligațiile generale prevăzute la articolul 3 și la articolul 58 alineatul (4) din PIPA, precum și exercitarea drepturilor individuale garantate de articolul 4 din PIPA. În plus, în conformitate cu articolul 7-8 alineatele (3) și (4) și cu articolul 7-9 alineatul (5) din PIPA, supravegherea PIPC vizează, de asemenea, posibilele încălcări ale normelor din anumite legi specifice care stabilesc limitările și garanțiile în ceea ce privește colectarea de informații cu caracter personal, cum ar fi CPPA, Legea privind combaterea terorismului și TBA. Având în vedere cerințele de la articolul 3 alineatul (1) din PIPA privind colectarea legală și echitabilă a informațiilor cu caracter personal, orice încălcare a acestor legi constituie o încălcare a PIPA. Prin urmare, PIPC are competența de a investiga ([265]) încălcările legilor care reglementează accesul la date în scopuri legate de securitatea națională, precum și ale normelor de prelucrare prevăzute în PIPA și de a emite recomandări în vederea îmbunătățirii, de a impune măsuri de remediere, de a recomanda măsuri disciplinare și de a sesiza autoritățile de investigare relevante cu privire la eventualele infracțiuni ([266]).

3.3.5. *Comisia națională pentru drepturile omului*

Supravegherea de către NHRC se aplică în același mod serviciilor de informații ca și altor autorități guvernamentale (a se vedea secțiunea 2.3.2).

3.4. **Căi de atac individuale**

3.4.1. *Căi de atac în fața responsabilului cu protecția drepturilor omului*

În ceea ce privește colectarea de informații cu caracter personal în contextul activităților de combatere a terorismului, HRPO, instituit în cadrul Comisiei de combatere a terorismului, oferă o cale de atac specifică. HRPO tratează petițiile civile referitoare la încălcarea drepturilor omului ca urmare a activităților de combatere a terorismului ([267]). Acesta poate recomanda măsuri de remediere, iar agenția relevantă trebuie să informeze responsabilul cu privire la orice măsuri luate pentru punerea în aplicare a unei astfel de recomandări. Nu există nicio cerință privind calitatea procesuală activă pentru ca persoanele fizice să depună o plângere la HRPO. În consecință, o plângere va fi prelucrată de HRPO chiar dacă persoana în cauză nu poate demonstra un prejudiciu în fapt în etapa de admisibilitate.

([259]) Articolul 18 din Legea NIS.
([260]) Articolul 15 alineatul (2) din Legea NIS.
([261]) Articolul 17 alineatul (2) din Legea NIS. „Secretele de stat" sunt definite ca „fapte, bunuri sau cunoștințe clasificate drept secrete de stat, la care accesul este permis unor categorii limitate de persoane și care nu sunt divulgate niciunei alte țări sau organizații, pentru a se evita orice dezavantaj grav pentru siguranța națională"; a se vedea articolul 13 alineatul (4) din Legea NIS.
([262]) Articolul 16 alineatul (2) din Legea privind inspecția și investigarea administrației de stat.
([263]) Articolul 15 din CPPA.
([264]) Ca și în cazul Comisiei pentru informații a Adunării Naționale, directorul NIS poate refuza să răspundă BAI numai în ceea ce privește aspectele care constituie secrete de stat și în cazul în care publicarea ar avea un impact grav asupra securității naționale [articolul 13 alineatul (1) din Legea NIS].
([265]) Articolul 63 din PIPA.
([266]) Articolul 61 alineatul (2), articolul 65 alineatul (1), articolul 65 alineatul (2) și articolul 64 alineatul (4) din PIPA.
([267]) Articolul 8 alineatul (1) punctul 2 din Decretul de punere în aplicare a Legii privind combaterea terorismului.

3.4.2. *Mecanisme de reparație disponibile în temeiul PIPA*

Persoanele își pot exercita drepturile de acces, rectificare, ștergere și suspendare în temeiul PIPA în ceea ce privește informațiile cu caracter personal prelucrate în scopuri legate de securitatea națională ([268]). Cererile de exercitare a acestor drepturi pot fi depuse direct la serviciul de informații sau indirect prin intermediul PIPC. În special, serviciul de informații poate întârzia, limita sau refuza exercitarea dreptului în măsura în care și atât timp cât este necesar și proporțional pentru a proteja un obiectiv important de interes public (de exemplu, în măsura în care și atât timp cât acordarea dreptului ar pune în pericol o investigație în curs sau ar amenința securitatea națională) sau în cazul în care acordarea dreptului poate aduce atingere vieții sau integrității fizice a unui terț. În cazul în care cererea este respinsă sau restricționată, persoanei în cauză trebuie să i se comunice motivele fără întârziere.

În plus, în conformitate cu articolul 58 alineatul (4) din PIPA (cerința de a asigura tratarea adecvată a plângerilor individuale) și cu articolul 4 alineatul (5) din PIPA (dreptul la despăgubiri adecvate pentru orice prejudiciu care rezultă din prelucrarea informațiilor cu caracter personal, printr-o procedură promptă și echitabilă), persoanele fizice au dreptul de a obține reparații. Acesta include dreptul de a raporta o presupusă încălcare prin intermediul Centrului de intermediere telefonică privind protecția vieții private gestionat de Agenția coreeană pentru internet și securitate și de a depune o plângere la PIPC ([269]). Aceste căi de atac sunt disponibile atât în cazul unor posibile încălcări ale normelor cuprinse în legi specifice care stabilesc limitările și garanțiile în ceea ce privește colectarea de informații cu caracter personal în scopuri legate de securitatea națională, cât și ale PIPA. Astfel cum s-a explicat în Notificarea nr. 2021-1, o persoană din UE poate depune o plângere la PIPC prin intermediul autorității sale naționale pentru protecția datelor. În acest caz, PIPC va informa persoana în cauză prin intermediul autorității naționale pentru protecția datelor după încheierea investigației (inclusiv, dacă este cazul, cu informații cu privire la măsurile de remediere impuse). Deciziile sau lipsa de acțiune a PIPC pot fi atacate în continuare în fața instanțelor coreene în temeiul Legii privind contenciosul administrativ.

3.4.3. *Căi de atac în fața Comisiei naționale pentru drepturile omului*

Posibilitatea de a obține reparații individuale în fața NHRC se aplică în același mod serviciilor de informații ca și altor autorități guvernamentale (a se vedea secțiunea 2.4.2).

3.4.4. *Căi de atac judiciare*

La fel ca în cazul activităților autorităților de asigurare a respectării dreptului penal, persoanele fizice pot avea acces la căi de atac judiciare împotriva serviciilor de informații cu privire la încălcările limitărilor și garanțiilor menționate mai sus prin diferite căi.

În primul rând, persoanele fizice pot obține despăgubiri pentru daune în temeiul Legii privind despăgubirile acordate de stat. De exemplu, într-un caz, au fost acordate despăgubiri în legătură cu supravegherea ilegală de către Comandamentul de sprijin pentru apărare (predecesorul Comandamentului de sprijin pentru securitate în domeniul apărării) ([270]).

În al doilea rând, Legea privind contenciosul administrativ le permite persoanelor fizice să conteste dispozițiile și omisiunile agențiilor administrative, inclusiv ale serviciilor de informații ([271]).

În cele din urmă, persoanele fizice pot depune o plângere constituțională la Curtea Constituțională împotriva măsurilor luate de serviciile de informații în temeiul Legii privind Curtea Constituțională.

([268]) Articolul 3 alineatul (5) și articolul 4 alineatele (1), (3) și (4) din PIPA.
([269]) Articolul 62 și articolul 63 alineatul (2) din PIPA.
([270]) Hotărârea Curții Supreme nr. 96Da42789 din 24 iulie 1998.
([271]) Articolele 3 și 4 din Legea privind contenciosul administrativ.