Jornal Oficial da União Europeia

L 76

Edição em língua portuguesa

Legislação

62.º ano

19 de março de 2019

Índice

[1] Texto relevante para efeitos do EEE.

PT

Os atos cujos títulos são impressos em tipo fino são atos de gestão corrente adotados no âmbito da política agrícola e que têm, em geral, um período de validade limitado.

Os atos cujos títulos são impressos em tipo negro e precedidos de um asterisco são todos os restantes.

II

(Atos não legislativos)

DECISÕES

DECISÃO DE EXECUÇÃO (UE) 2019/419 DA COMISSÃO

de 23 de janeiro de 2019

nos termos do Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho sobre a adequação do nível de proteção dos dados pessoais assegurado pelo Japão no âmbito da Lei relativa à proteção de informações pessoais

[notificada com o número C(2019) 304]

(Texto relevante para efeitos do EEE)

A COMISSÃO EUROPEIA,

Tendo em conta o Tratado sobre o Funcionamento da União Europeia,

Tendo em conta o Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados) («RGPD») ([1]), nomeadamente o artigo 45.º, n.º 3.

Após consulta da Autoridade Europeia para a Proteção de Dados,

1. INTRODUÇÃO

(1) O Regulamento (UE) 2016/679 estabelece as regras relativas à transferência de dados pessoais para países terceiros e organizações internacionais pelos responsáveis pelo tratamento e subcontratantes na União Europeia, na medida em que essa transferência seja abrangida pelo respetivo âmbito de aplicação. As regras relativas às transferências internacionais de dados pessoais são definidas no capítulo V do referido Regulamento, mais concretamente nos artigos 44.º a 50.º. O fluxo de dados pessoais com origem em países não pertencentes à União Europeia ou a eles destinado é necessário para se poder aprofundar a cooperação e o comércio internacionais, garantindo, simultaneamente, que o nível de proteção dos dados pessoais conferido na União Europeia não é comprometido.

(2) Nos termos do artigo 45.º, n.º 3, do Regulamento (UE) 2016/679, a Comissão pode decidir, por meio de um ato de execução, que um país terceiro, um território, um ou mais setores específicos desse país terceiro, ou uma organização internacional, garantem um nível de proteção adequado. Nessa condição, as transferências de dados pessoais para esse país terceiro, território, setor ou organização internacional podem ser efetuadas sem que seja necessária mais nenhuma autorização, como previsto no artigo 45.º, n.º 1, e no considerando 103 do Regulamento.

(3) Como especificado no artigo 45.º, n.º 2, do Regulamento (UE) 2016/679, a adoção de uma decisão de adequação deve basear-se numa análise exaustiva da ordem jurídica do país terceiro no que se refere tanto às regras aplicáveis aos importadores de dados como às limitações e garantias relativas ao acesso aos dados pessoais pelas autoridades públicas. Essa análise deve permitir apurar se o país terceiro em causa garante um nível de proteção «essencialmente equivalente» ao assegurado na União Europeia [considerando 104 do Regulamento (UE) 2016/679]. Como foi esclarecido pelo Tribunal de Justiça da União Europeia, não é exigido um nível de proteção idêntico ([2]). Mais concretamente, os meios a que o país terceiro recorre podem ser diferentes dos aplicados na União Europeia, desde que se revelem, na prática, eficazes para assegurar um nível adequado de proteção ([3]). Por conseguinte, o padrão de

([1]) JO L 119 de 4.5.2016, p. 1.
([2]) Processo C-362/14, *Maximillian Schrems* v. *Data Protection Commissioner* («*Schrems*»), ECLI:EU:C:2015:650, n.º 73.
([3]) *Schrems*, n.º 74.

adequação não exige que as regras da União sejam replicadas ponto por ponto. Em vez disso, importa aferir sobretudo se, através do teor dos direitos de privacidade e da sua aplicação, controlo e execução efetivos, o sistema estrangeiro consegue, no seu conjunto, garantir o nível de proteção exigido ([4]).

(4) A Comissão procedeu a uma análise cuidadosa da legislação e das práticas do Japão. Com base nas constatações formuladas nos considerandos 6 a 175, a Comissão conclui que o Japão assegura um nível de proteção adequado dos dados pessoais transferidos para as organizações abrangidas pelo âmbito de aplicação da Lei relativa à proteção de informações pessoais ([5]) e sujeitos às condições adicionais previstas na presente decisão. Essas condições são definidas nas normas complementares (anexo I) adotadas pela Comissão de Proteção de Informações Pessoais (PPC) ([6]) e nas declarações, garantias e compromissos oficiais transmitidos pelo Governo japonês à Comissão Europeia (anexo II).

(5) Em resultado da presente decisão, as transferências de um responsável pelo tratamento de dados ou de um subcontratante no Espaço Económico Europeu (EEE) ([7]) para as referidas organizações no Japão podem ser efetuadas sem que seja necessária mais nenhuma autorização. A presente decisão não afeta a aplicação direta do Regulamento (UE) 2016/679 a essas organizações, desde que estejam preenchidas as condições fixadas no artigo 3.º.

2. NORMAS APLICÁVEIS AO TRATAMENTO DE DADOS PELOS OPERADORES COMERCIAIS

2.1. Quadro normativo do Japão em matéria de proteção de dados

(6) O sistema jurídico que rege a privacidade e a proteção dos dados no Japão tem origem na Constituição promulgada em 1946.

(7) O artigo 13.º da Constituição enuncia:

«Todas as pessoas devem ser respeitadas enquanto indivíduos. O seu direito à vida, à liberdade e à prossecução da felicidade, na medida em que não atente contra o bem-estar público, deve constituir a consideração suprema na legislação e noutros assuntos governamentais.»

(8) Com base neste artigo, o Supremo Tribunal japonês clarificou os direitos individuais no que se refere à proteção das informações pessoais. Numa decisão de 1969, reconheceu o direito à privacidade e à proteção de dados como um direito constitucional ([8]). O Tribunal considerou, nomeadamente, que «todas os indivíduos têm a liberdade de proteger as suas informações pessoais contra a transmissão a terceiros ou a divulgação pública sem motivo justificado.» Além disso, numa decisão de 6 de março de 2008 («Juki-Net») ([9]), o Supremo Tribunal considerou que «a liberdade dos cidadãos na vida privada deve ser protegida contra o exercício da autoridade pública e que pode entender-se, como uma das liberdades individuais na vida privada, que cada indivíduo tem a liberdade de proteger as suas informações pessoais contra a transmissão a terceiros ou a divulgação pública sem motivo justificado.» ([10])

(9) Em 30 de maio de 2003, o Japão promulgou um conjunto de leis no domínio da proteção de dados:

— a Lei relativa à proteção de informações pessoais (APPI);

— a Lei relativa à proteção de informações pessoais na posse de órgãos administrativos (APPIHAO);

— a Lei relativa à proteção de informações pessoais na posse de serviços administrativos legalmente constituídos (APPI-IAA).

([4]) Ver Comunicação da Comissão ao Parlamento Europeu e ao Conselho, Intercâmbio e proteção de dados pessoais num mundo globalizado, COM(2017)7 de 10.1.2017, secção 3.1., pp. 6-7.
([5]) Lei relativa à proteção de informações pessoais (Lei n.º 57, 2003).
([6]) Estão disponíveis mais informações sobre a PPC na seguinte ligação: https://www.ppc.go.jp/en (incluindo os dados de contacto para pedidos de esclarecimento e reclamações: https://www.ppc.go.jp/en/contactus/access/).
([7]) A presente decisão é relevante para efeitos do EEE. O Acordo sobre o Espaço Económico Europeu («Acordo EEE») prevê a extensão do mercado interno da União Europeia aos três Estados do EEE: Islândia, Liechtenstein e Noruega. A Decisão do Comité Misto que incorpora o Regulamento (UE) 2016/679 no anexo XI do Acordo EEE foi adotada pelo Comité Misto do EEE em 6 de julho de 2018 e entrou em vigor em 20 de julho de 2018. Deste modo, o regulamento é abrangido pelo referido acordo.
([8]) Supremo Tribunal, acórdão do Tribunal Pleno de 24 de dezembro de 1969, Keishu Vol. 23, n.º 12, p. 1625.
([9]) Supremo Tribunal, acórdão de 6 de março de 2008, Minshu Vol. 62 n.º 3, p. 665.
([10]) Supremo Tribunal, acórdão de 6 de março de 2008, Minshu Vol. 62 n.º 3, p. 665.

(10) As duas últimas leis (alteradas em 2016) contêm disposições aplicáveis à proteção de informações pessoais pelas entidades do setor público. O tratamento dos dados abrangido pelo âmbito de aplicação destes diplomas não é objeto da verificação de adequação a que a presente decisão se refere, a qual se limita à proteção das informações pessoais pelos «operadores comerciais responsáveis pela gestão de informações pessoais» (PIHBO), na aceção da APPI.

(11) A APPI foi recentemente reformulada. A APPI alterada foi promulgada em 9 de setembro de 2015 e entrou em vigor em 30 de maio de 2017. Essa alteração introduziu um conjunto de novas garantias, tendo reforçado igualmente as garantias já existentes, tornando assim o sistema de proteção de dados japonês mais semelhante ao europeu. Essas garantias incluem, designadamente, um conjunto de direitos individuais oponíveis ou a criação de uma autoridade de controlo independente (PPC) responsável pela supervisão e aplicação coerciva da APPI.

(12) Além da APPI, o tratamento das informações pessoais abrangido pelo âmbito de aplicação da presente decisão está sujeito a normas de execução adotadas com base na referida lei. Tal inclui uma alteração ao decreto ministerial de execução da Lei relativa à proteção de informações pessoais de 5 de outubro de 2016, assim como as chamadas normas de execução da Lei relativa à proteção de informações pessoais adotadas pela PPC ([11]). Os dois conjuntos normativos são juridicamente vinculativas e oponíveis, tendo entrado em vigor ao mesmo tempo que a alteração da APPI.

(13) Por outro lado, em 28 de outubro de 2016, o Conselho de Ministros do Japão (composto pelo primeiro-ministro e pelos ministros que constituem o Governo) definiu uma «Política de base» a fim de «promover de forma abrangente e integral medidas relativas à proteção das informações pessoais». Nos termos do artigo 7.º da APPI, a «Política de base» foi promulgada sob a forma de decisão do Conselho de Ministros e inclui orientações políticas relativas à aplicação coerciva da APPI, destinadas à administração central e aos órgãos de poder local.

(14) Recentemente, através de uma decisão do Conselho de Ministros de 12 de junho de 2018, o Governo japonês alterou a «Política de base». Com vista a facilitar as transferências internacionais de dados, a referida decisão do Conselho de Ministros delega na PPC, enquanto autoridade competente para administrar e aplicar a APPI, «poderes para tomar as medidas necessárias no sentido de ultrapassar as divergências dos sistemas e das operações entre o Japão e o país estrangeiro em causa, com base no artigo 6.º da Lei, por forma a assegurar o tratamento adequado das informações pessoais provenientes desse país». A decisão do Conselho de Ministros estipula que os referidos poderes incluem a competência para proporcionar uma proteção reforçada mediante a adoção pela PPC de regras mais rígidas que complementem e excedam as definidas na APPI e no decreto ministerial. Nos termos dessa decisão, essas regras mais rígidas são vinculativas e oponíveis em relação aos operadores comerciais japoneses.

(15) Com base no artigo 6.º da APPI e na referida decisão do Conselho de Ministros, em 15 de junho de 2018, a PPC adotou «Normas complementares ao abrigo da lei relativa à proteção de informações pessoais para o tratamento de dados pessoais transferidos da UE com base numa decisão de adequação» (as «normas complementares»), com vista a reforçar a proteção das informações pessoais transferidas da União Europeia para o Japão com base na presente decisão de adequação. Tais normas complementares são juridicamente vinculativas para os operadores comerciais japoneses e passíveis de execução tanto pela PPC como pelos tribunais, da mesma forma que as disposições da APPI que estas normas complementam, com regras mais rígidas e/ou mais exaustivas ([12]). Uma vez que os operadores comerciais japoneses que recebem e/ou tratam dados pessoais originários da União Europeia são legalmente obrigados a cumprir as normas complementares, deverão assegurar [nomeadamente por meios técnicos («marcação») ou organizacionais (armazenamento numa base de dados específica)] que podem identificar esses dados pessoais ao longo do seu «ciclo de vida» ([13]). Nas secções seguintes, analisa-se o teor de cada norma complementar no âmbito da avaliação dos artigos da APPI que complementa.

(16) Contrariamente à situação anterior à alteração de 2015, em que esta competência cabia a vários ministérios japoneses em setores específicos, a APPI confere poderes à PPC para adotar «orientações que assegurem a aplicação apropriada e eficaz das medidas a adotar pelos operadores comerciais» ao abrigo das normas em matéria de proteção de dados. Através das suas orientações, a PPC fornece uma interpretação vinculativa dessas normas,

([11]) Disponíveis em: https://www.ppc.go.jp/files/pdf/PPC_rules.pdf

([12]) Ver normas complementares (introdução).

([13]) Isto não é invalidado pela obrigação geral de manter registos (apenas) durante um certo período de tempo. Embora a origem dos dados esteja entre as informações de que o PIHBO que obtém os dados deva confirmar, em conformidade com o artigo 26.º, n.º 1, da APPI, o requisito previsto no artigo 26.º, n.º 4, da APPI, em conjugação com o artigo 18.º das normas da PPC, diz respeito apenas a uma forma específica de registo (ver o artigo 16.º das normas), não impedindo um PIHBO de assegurar a identificação dos dados por períodos mais longos. Este facto foi confirmado pela PPC quando confirmou que «[a] informação relativa ao facto de os dados serem originários da UE deve ser mantida pelo PIHBO enquanto tal for necessário para dar cumprimento às normas complementares».

nomeadamente da APPI. Segundo as informações prestadas pela PPC, as referidas orientações fazem parte integrante do quadro jurídico e devem ser lidas conjuntamente com o texto da APPI, o decreto ministerial, as normas da PPC e um conjunto de P&R ([14]) preparadas pela PPC, sendo, por conseguinte, «vinculativas para os operadores comerciais». Sempre que as orientações especifiquem que um operador comercial «não pode» ou «não deve» agir de determinada forma, a PPC considera que o incumprimento das disposições em causa representa uma violação da lei ([15]).

2.2. **Âmbito de aplicação material e pessoal**

(17) O âmbito de aplicação da APPI é determinado pelos conceitos definidos de informações pessoais, dados pessoais e operador comercial responsável pela gestão de informações pessoais. Ao mesmo tempo, a APPI prevê algumas derrogações importantes ao respetivo âmbito de aplicação, sendo as mais importantes as que se referem aos dados pessoais tratados anonimamente e aos tipos de tratamento específicos por determinados operadores. Embora não utilize a expressão «tratamento», a APPI recorre ao conceito equivalente de «gestão» (*handling*) que, segundo as informações recebidas do PPC, abrange «qualquer ato relativo a dados pessoais», nomeadamente a obtenção, contribuição, acumulação, organização, armazenamento, edição/tratamento, renovação, supressão, produção, utilização ou fornecimento de informações pessoais.

2.2.1. *Definição de informações pessoais*

(18) Em primeiro lugar, no que se refere ao respetivo âmbito de aplicação material, a APPI faz a distinção entre informações pessoais e dados pessoais, sendo que somente algumas das disposições da lei se aplicam à primeira categoria. Nos termos do artigo 2.º, n.º 1, da APPI, o conceito de «informações pessoais» inclui toda e qualquer informação respeitante a uma pessoa viva que permita a sua identificação. A definição distingue duas categorias de informações pessoais: i) códigos de identificação individuais e ii) outras informações pessoais pelas quais uma determinada pessoa singular pode ser identificada. A última categoria inclui igualmente informações que, por si só, não permitem a identificação, mas que, quando «cotejadas» com outras informações, permitem identificar determinada pessoa singular. De acordo com as orientações da PPC ([16]), a avaliação sobre se as informações podem ser consideradas «cotejáveis» será realizada caso a caso, tendo em conta a situação real («condição») do operador comercial. Parte-se deste princípio se a referida recolha for (ou puder ser) realizada por um operador comercial médio («normal») recorrendo aos meios ao seu dispor. Por exemplo, as informações não são consideradas «cotejáveis» com outras informações quando o operador comercial tenha de envidar esforços inusitados ou de cometer atos ilegais para as obter junto de outro ou de outros operadores comerciais.

2.2.2. *Definição de dados pessoais*

(19) Só alguns tipos de informações pessoais são abrangidos pelo conceito de «dados pessoais» ao abrigo da APPI. Com efeito, os «dados pessoais» são definidos como «informações pessoais que constituem uma base de dados de informações pessoais», isto é, um «conjunto global de informações» que compreende informações pessoais «sistematicamente organizadas para que seja possível pesquisar informações pessoais específicas através de um computador» ([17]) ou «determinadas por decreto ministerial como tendo sido sistematicamente organizadas para que seja possível pesquisar informações pessoais específicas» mas «excluindo as determinadas por decreto ministerial como sendo pouco suscetíveis de prejudicar os direitos e interesses de uma pessoa singular tendo em conta o respetivo método de utilização» ([18]).

(20) Esta derrogação é mais pormenorizada no artigo 3.º, n.º 1, do decreto ministerial, segundo o qual devem ser satisfeitas três condições cumulativas: i) o conjunto global de informações ter sido «emitido com o objetivo de ser vendido a um grande número de pessoas não especificadas e essa emissão não tenha sido efetuada em violação das disposições da lei ou do decreto em que se baseia»; ii) este ser suscetível de ser «adquirido em qualquer altura por

([14]) PPC, Perguntas e Respostas, 16 de fevereiro de 2017 (alteradas em 30 de maio de 2017), disponíveis na ligação seguinte: https://www.ppc.go.jp/files/pdf/kojouhouQA.pdf. As P&R versam sobre uma série de questões abordadas nas orientações, apresentando exemplos práticos, designadamente o que constitui dados pessoais sensíveis, a interpretação do consentimento individual, as transferências para terceiros no âmbito da computação em nuvem ou a obrigação de conservar registos aplicada às transferências transfronteiriças. As P&R apenas estão disponíveis em japonês.

([15]) Na sequência de uma pergunta específica, a PPC informou o CEPD de que «os tribunais japoneses assentam a sua [re]interpretação nas orientações sempre que devem aplicar as normas APPI/PPC nos casos concretos submetidos à sua apreciação e, por conseguinte, os respetivos acórdãos remetem diretamente para o texto das orientações da PPC. Por conseguinte, também nesta perspetiva, as orientações da PPC são vinculativas para os operadores comerciais. A PPC não tem conhecimento de que o Tribunal alguma vez tenha optado por divergir das orientações.» A este respeito, a PPC notificou a Comissão quanto a uma decisão no domínio da proteção de dados em que o tribunal recorreu explicitamente, para as suas conclusões, às orientações (ver Tribunal Distrital de Osaca, decisão de 19 de maio de 2006, Hanrei Jiho, Vol. 1948, p. 122, em que o tribunal, com base nessas orientações, determinou que o operador comercial tinha a obrigação de tomar uma medida de controlo de segurança).

([16]) Orientações da PPC (edição sobre as normas gerais), p. 6.

([17]) Abrange os sistemas de arquivo eletrónico. As orientações da PPC (edição sobre as normas gerais, p. 17) fornecem alguns exemplos específicos a este respeito, nomeadamente uma lista de endereços de correio eletrónico guardada no *software* de correio eletrónico do cliente.

([18]) Artigo 2.º, n.ºs 4 e 6, da APPI.

um grande número de pessoas não especificadas» e iii) os dados pessoais nele contidos serem fornecidos «para a sua finalidade original, sem acrescentar quaisquer outras informações relativas a pessoas vivas». Segundo as explicações fornecidas pela PPC, esta derrogação, muito circunscrita, foi introduzida para excluir as listas telefónicas ou outros tipos de listas semelhantes.

(21) No caso dos dados recolhidos no Japão, esta distinção entre «informações pessoais» e «dados pessoais» é pertinente, uma vez que é possível que essas informações nem sempre façam parte de uma «base de dados de informações pessoais» (por exemplo, um único conjunto de dados recolhido e tratado manualmente) e, portanto, essas disposições da APPI, apenas respeitantes a dados pessoais, não são aplicáveis ([19]).

(22) Em contrapartida, esta distinção não é relevante no caso de dados pessoais importados da União Europeia para o Japão com base numa decisão de adequação. Dado que esses dados são normalmente transferidos por meios eletrónicos (pois, na presente era digital, é esse é o modo habitual de intercâmbio de dados, especialmente nas grandes distâncias, como sucede entre a UE e o Japão), passando, por conseguinte, a fazer parte do sistema de arquivo eletrónico do importador dos dados, nos termos da APPI, esses dados da UE enquadram-se na categoria de «dados pessoais». No caso excecional de os dados pessoais serem transferidos da UE por outros meios (por exemplo, em suporte de papel), continuarão a ser abrangidos pela APPI se, após a transferência, passarem a fazer parte de um «conjunto global de informações» sistematicamente organizadas de modo a permitir uma pesquisa fácil de informações específicas [artigo 2.º, n.º 4, alínea ii) da APPI]. Nos termos do artigo 3.º, n.º 2, do decreto ministerial, será esse o caso quando a informação estiver estruturada «de acordo com uma regra específica» e a base de dados contemplar instrumentos como um índice ou um índice remissivo para facilitar a pesquisa. Isto corresponde à definição de «ficheiro» na aceção do artigo 2.º, n.º 1, do RGPD.

2.2.3. *Definição de dados pessoais conservados*

(23) Algumas disposições da APPI relativas aos direitos individuais, nomeadamente os artigos 27.º a 30.º, apenas se aplicam a uma categoria específica de dados pessoais, nomeadamente aos «dados pessoais conservados». Estes encontram-se definidos no artigo 2.º, n.º 7, da APPI como dados pessoais, exceto aqueles que são i) «determinados por decreto ministerial como sendo suscetíveis de prejudicar o interesse público ou outros interesses, se a sua presença ou ausência for divulgada» ou que estão ii) «destinados a ser apagados num prazo não superior a um ano, determinado por decreto ministerial».

(24) No que se refere à primeira destas duas categorias, é a mesma explicada no artigo 4.º do decreto ministerial e abrange quatro tipos de isenções ([20]). Estas isenções prosseguem objetivos semelhantes aos descritos no artigo 23.º, n.º 1, do Regulamento (UE) 2016/679, designadamente a defesa do titular dos dados («titular» segundo a terminologia da APPI) e a liberdade de outrem, a segurança nacional, a segurança pública, aplicação do direito penal ou outros objetivos importantes do interesse público geral. Além disso, a redação do artigo 4.º, n.º 1, alíneas i) a iv), do decreto ministerial implica que a aplicação dessas isenções pressuponha sempre um risco específico para um dos interesses importantes que são protegidos ([21]).

(25) A segunda categoria foi objeto de maior particularização no artigo 5.º do decreto ministerial. Considerado em conjugação com o artigo 2.º, n.º 7, da APPI, isenta os dados pessoais, que estão «destinados a ser apagados» num prazo de seis meses, do âmbito de aplicação do conceito de dados pessoais conservados. A PPC explicou que esta isenção visa incentivar os operadores comerciais a conservar e a tratar os dados durante o período de tempo mais curto possível. No entanto, tal implicaria que os titulares de dados da UE não poderiam beneficiar de direitos importantes por nenhum outro motivo exceto o prazo de conservação dos seus dados pelo operador comercial em causa.

(26) Por forma a resolver esta situação, a norma complementar 2 exige que os dados pessoais transferidos da União Europeia «sejam tratados como dados pessoais conservados na aceção do artigo 2.º, n.º 7, da lei, independentemente do prazo em que devam ser apagados». Deste modo, o prazo de conservação não terá qualquer influência sobre os direitos conferidos aos titulares de dados da UE.

([19]) Por exemplo, o artigo 23.º da APPI sobre as condições de comunicação de dados pessoais a terceiros.

([20]) Designadamente, os dados pessoais i) «em relação aos quais haja a possibilidade, se a presença ou ausência dos mesmos for divulgada, de a vida, a integridade física ou o bem-estar do titular ou de um terceiro serem lesados»; ii) dados «em relação aos quais haja a possibilidade, se a presença ou ausência dos mesmos for divulgada, de induzir ou incitar à prática de um ato ilícito ou injusto»; iii) dados «em relação aos quais haja a possibilidade, se a presença ou ausência dos mesmos for divulgada, de comprometer a segurança nacional, destruir uma relação de confiança com um país estrangeiro ou organização internacional ou incorrer em desvantagem em negociações com um país estrangeiro ou organização internacional»; e iv) dados «em relação aos quais haja a possibilidade, se a presença ou ausência dos mesmos for divulgada, de prejudicar a manutenção da segurança e da ordem públicas, designadamente a prevenção, repressão ou investigação de um crime».

([21]) Nestas condições, não é necessário notificar a pessoa em causa. Isto está em conformidade com o disposto no artigo 23.º, n.º 2, alínea h), do RGPD, que estipula que os titulares dos dados não devem ser informados da limitação se tal puder «prejudicar o objetivo da limitação».

2.2.4. *Definição de informações pessoais tratadas anonimamente*

(27) As exigências aplicáveis às informações pessoais tratadas anonimamente, tal como definidas no artigo 2.º, n.º 9, da APPI, encontram-se estipuladas na secção 2 do capítulo 4 da lei («Obrigações de um operador comercial responsável pela gestão de informações tratadas anonimamente»). Em contrapartida, estas informações não se regem pelas disposições da secção 1 do capítulo IV da APPI, a qual inclui os artigos que estipulam as garantias e os direitos em matéria de proteção de dados aplicáveis ao tratamento de dados pessoais no âmbito da referida lei. Em consequência, embora não estejam sujeitas às normas de proteção «básicas» (as especificadas na secção 1 do capítulo IV e no artigo 42.º da APPI), as «informações pessoais tratadas anonimamente» são abrangidas pelo âmbito de aplicação da APPI, nomeadamente pelos artigos 36.º a 39.º.

(28) Nos termos do artigo 2.º, n.º 9, da APPI, as «informações pessoais tratadas anonimamente» são informações relativas a uma pessoa singular que «foram geradas com base no tratamento de informações pessoais», através de medidas previstas na APPI (artigo 36.º, n.º 1) e especificadas nas normas da PPC (artigo 19.º), tendo como resultado a impossibilidade de identificar uma determinada pessoa singular ou reconstituir as informações pessoais.

(29) Decorre das referidas disposições, o que a PPC também confirma, que o processo de tornar as informações pessoais «anónimas» não tem de ser tecnicamente irreversível. Nos termos do artigo 36.º, n.º 2, da APPI, os operadores comerciais responsáveis pela gestão de «informações pessoais tratadas anonimamente» são unicamente obrigados a evitar a reidentificação através da tomada de medidas que garantam a segurança das «descrições, etc. e dos códigos de identificação individuais apagados das informações pessoais utilizadas para gerar as informações tratadas anonimamente, bem como das informações relativas ao método de tratamento efetuado».

(30) Dado que as «informações pessoais tratadas anonimamente», de acordo com a definição da APPI, incluem dados pelos quais continua a ser possível reidentificar a pessoa singular, a implicação poderá ser a de que os dados pessoais transferidos da União Europeia poderão perder parte das proteções disponíveis através de um processo que, nos termos do Regulamento (UE) 2016/679, seria considerado como uma forma de «pseudonimização» e não de «anonimização» (não alterando, portanto, a sua natureza de dados pessoais).

(31) Para resolver esta situação, as normas complementares preveem exigências adicionais apenas aplicáveis aos dados pessoais transferidos da União Europeia no âmbito desta decisão. Nos termos da norma 5 das normas complementares, essas informações pessoais apenas serão consideradas como «informações pessoais tratadas anonimamente» na aceção da APPI «se o operador comercial responsável pela gestão das informações pessoais tomar medidas que tornem a desidentificação da pessoa singular irreversível para qualquer pessoa, incluindo através do apagamento das informações relativas ao método de tratamento, etc.». Estas últimas foram especificadas nas normas complementares como informações relativas às descrições de códigos de identificação individuais que foram apagados das informações pessoais utilizadas para gerar as «informações pessoais tratadas anonimamente», bem como as informações relativas ao método de tratamento aplicado no apagamento dessas descrições e códigos de identificação individuais. Por outras palavras, as normas complementares obrigam o operador comercial que gera «informações pessoais tratadas anonimamente» a destruir a «chave» que permite a reidentificação dos dados. Tal significa que os dados pessoais com origem na União Europeia são abrangidos pelas disposições da APPI no que se refere às «informações pessoais tratadas anonimamente» apenas nos casos em que sejam igualmente consideradas como informações anónimas nos termos do Regulamento (UE) 2016/679 ([22]).

2.2.5. *Definição de operador comercial responsável pela gestão de informações pessoais (PIHBO)*

(32) No que diz respeito ao seu âmbito de aplicação pessoal, a APPI é unicamente aplicável aos PIHBO. O artigo 2.º, n.º 5, da APPI define um PIHBO como «uma pessoa que disponibiliza uma base de dados de informações pessoais, etc. para utilização na atividade comercial», excluindo o Governo e as agências administrativas tanto a nível central como local.

(33) De acordo com as orientações da PPC, «atividade comercial» significa toda e qualquer «conduta destinada a exercer, com um determinado objetivo, repetida e continuamente, quer seja ou não com fins lucrativos, uma atividade empresarial socialmente reconhecida. As organizações sem personalidade jurídica (como as associações de facto) ou as pessoas singulares são consideradas como PIHBO se disponibilizarem (utilizarem) uma base de dados de informações pessoais, etc. para o exercício da sua atividade comercial ([23]). Por conseguinte, o conceito de «atividade comercial» nos termos da APPI é muito lato, uma vez que não só inclui atividades com fins lucrativos, mas também atividades sem fins lucrativos exercidas por todos os tipos de organizações e pessoas singulares. Por outro lado, a «utilização para o exercício da atividade comercial» também abrange informações pessoais que não são utilizadas nas relações comerciais (externas) do operador, mas sim internamente, como por exemplo no tratamento dos dados dos trabalhadores.

([22]) Ver Regulamento (UE) 2016/679, considerando 26.
([23]) Orientações da PPC (edição sobre as normas gerais), p. 18.

(34) No que se refere aos beneficiários das proteções definidas na APPI, a lei não faz qualquer distinção baseada na nacionalidade, no domicílio ou na localização de uma pessoa singular. O mesmo se aplica às possibilidades de as pessoas singulares obterem reparação, quer junto da PPC quer dos tribunais.

2.2.6. *Conceitos de responsável pelo tratamento e subcontratante*

(35) Nos termos da APPI, não é feita qualquer distinção específica entre as obrigações impostas aos responsáveis pelo tratamento e as impostas aos subcontratantes. A inexistência desta distinção não afeta o nível de proteção uma vez que todos os PIHBO estão sujeitos à totalidade das disposições da lei. Um PIHBO, que confia o tratamento dos dados pessoais a um mandatário (o equivalente a um subcontratante no âmbito do RGPD) continua sujeito às obrigações decorrentes da APPI e das normas complementares relativamente aos dados que lhe sejam confiados. Além disso, nos termos do artigo 22.º da APPI, deve «exercer uma supervisão necessária e adequada» do mandatário. Por sua vez, como confirmado pela PPC, o mandatário está, por seu turno, sujeito a todas as obrigações previstas na APPI e nas normas complementares.

2.2.7. *Exclusões setoriais*

(36) O artigo 76.º da APPI exclui certos tipos de tratamento de dados do âmbito de aplicação do capítulo IV da lei, que contém as disposições principais sobre proteção de dados (princípios básicos, obrigações dos operadores comerciais, direitos individuais e supervisão pela PPC). Nos termos do artigo 43.º, n.º 2, da APPI ([24]), o tratamento abrangido pela exclusão setorial prevista no artigo 76.º também está isento dos poderes de execução coerciva da PPC.

(37) As categorias pertinentes no que se refere à exclusão setorial prevista no artigo 76.º da APPI são definidas aplicando um critério duplo baseado no tipo de PIHBO que trata as informações pessoais e na finalidade do tratamento. Mais concretamente, a exclusão aplica-se a: i) organismos de radiodifusão, editores de jornais, agências de comunicação ou outros órgãos de imprensa (incluindo pessoas singulares cuja atividade comercial consista na realização de atividades junto da imprensa), na medida em que tratem informações pessoais para efeitos de divulgação na imprensa; ii) pessoas que se dediquem à atividade de escrita profissional, na medida em que a mesma envolva informações pessoais; iii) universidades e outras organizações ou grupos orientados para estudos académicos ou pessoas singulares pertencentes a organizações desse tipo, na medida em que tratem informações pessoais para efeitos de estudos académicos; iv) instituições religiosas, na medida em que tratem informações pessoais para efeitos de atividade religiosa (incluindo todas as atividades associadas); e v) organismos políticos, na medida em que tratem informações pessoais para efeitos da sua atividade política (incluindo todas as atividades associadas). O tratamento de informações pessoais com uma das finalidades indicadas no artigo 76.º por outros tipos de PIHBO, assim como o tratamento de informações pessoais por um dos PIHBO indicados com outras finalidades, designadamente no contexto do emprego, continuam abrangidos pelas disposições do capítulo IV.

(38) A fim de assegurar um nível de proteção adequado dos dados pessoais transferidos da União Europeia para operadores comerciais no Japão, somente o tratamento de informações pessoais abrangido pelo âmbito de aplicação do capítulo IV da APPI, ou seja, por um PIHBO na medida em que o tipo de tratamento não corresponda a uma das exclusões setoriais, deve ser abrangido pela presente decisão. O seu âmbito de aplicação deve, por conseguinte, ser harmonizado com o da APPI. Segundo as informações transmitidas pela PPC, se um PIHBO abrangido pela presente decisão alterar posteriormente a finalidade de utilização (na medida do permitido), passando esta a ser abrangida por uma das exclusões setoriais previstas no artigo 76.º da APPI, tal deve ser considerado uma transferência internacional (na medida em que, nesses casos, o tratamento das informações pessoais deixa de ser abrangido pelo capítulo IV da APPI, saindo do respetivo âmbito de aplicação). O mesmo sucede caso um PIHBO forneça informações pessoais a uma entidade abrangida pelo artigo 76.º da APPI, para serem utilizadas para uma das finalidades indicadas na referida disposição. No que respeita aos dados pessoais transferidos da União Europeia, tal constituiria, por conseguinte, uma transferência subsequente sujeita às garantias pertinentes (nomeadamente as especificadas no artigo 24.º da APPI e na norma complementar 4. Quando o PIHBO deva obter primeiro o consentimento do titular dos dados ([25]), deve transmitir-lhe todas as informações necessárias, incluindo o facto de as informações pessoais deixarem de estar protegidas ao abrigo da APPI.

([24]) No que se refere a outros operadores, a PPC, no exercício das suas competências de investigação e de execução coerciva, não pode impedi-los de exercerem o seu direito à liberdade de expressão, à liberdade académica, à liberdade religiosa e à liberdade de atividade política (artigo 43.º, n.º 1, da APPI).

([25]) Tal como foi explicado pela PPC, nas respetivas orientações o consentimento é interpretado como a «expressão da intenção do titular em aceitar que as informações pessoais que lhe digam respeito possam ser tratadas segundo o método indicado por um operador comercial responsável pela gestão de informações pessoais [PIHBO]». As orientações da PPC (edição sobre as normas gerais, p. 24) enumeram as diferentes formas de expressar o consentimento consideradas «práticas comerciais correntes no Japão», como manifestar o seu acordo verbalmente, devolver um formulário ou outro documento, manifestar concordância por correio eletrónico, assinalar uma casa numa página Web, clicar na página principal, pressionar um botão de consentimento, tocar num painel tátil, etc. Todos estes métodos constituem formas de consentimento explícito.

2.3. **Garantias, direitos e obrigações**

2.3.1. *Limitação da finalidade*

(39) Os dados pessoais devem ser tratados com uma finalidade específica e, subsequentemente, utilizados apenas na medida em que essa utilização não seja incompatível com a finalidade do tratamento. Este princípio da proteção dos dados encontra-se garantido nos termos dos artigos 15.º e 16.º da APPI.

(40) A APPI assenta no princípio de que um operador comercial tem de indicar a finalidade da utilização «o mais explicitamente possível» (artigo 15.º, n.º 1), ficando subsequentemente obrigado a respeitar essa finalidade quando procede ao tratamento dos dados.

(41) Nesta matéria, o artigo 15.º, n.º 2, da APPI estabelece que o PIHBO não pode alterar a finalidade inicial «para além do âmbito reconhecido como razoavelmente pertinente para a finalidade de utilização anterior à alteração», interpretada nas orientações da PPC como correspondendo ao que pode ser objetivamente previsto pelo titular dos dados com base em «convenções sociais normais» ([26]).

(42) Por outro lado, nos termos do artigo 16,º, n.º 1, da APPI, os PIHBO estão proibidos de gerir informações pessoais «para além do âmbito necessário para cumprir uma finalidade de utilização», especificada no artigo 15.º, sem obter o consentimento prévio do titular dos dados, a menos que se aplique uma das derrogações previstas no artigo 16.º, n.º 3 ([27]).

(43) Quando as informações pessoais são obtidas junto de outro operador comercial, o PIHBO tem, em princípio, a liberdade de definir uma nova finalidade de utilização ([28]). Com vista a assegurar que, na eventualidade de uma transferência da União Europeia, esse destinatário fique vinculado à mesma finalidade para a qual os dados foram transferidos, a norma complementar 3 exige que, nos casos «em que um [PIHBO] receba dados pessoais da UE, com base numa decisão de adequação» ou em que esse operador «receba dados pessoais de outro [PIHBO] previamente transferidos da UE, com base numa decisão de adequação» (transferência subsequente), o destinatário deva «especificar a finalidade de utilização dos referidos dados pessoais no âmbito da finalidade de utilização para a qual os dados foram inicialmente ou subsequentemente recebidos». Por outras palavras, a norma garante que, num contexto de transferência, a finalidade especificada, nos termos do Regulamento (UE) 2016/679, continue a determinar o tratamento e que uma alteração dessa finalidade em qualquer fase da cadeia de tratamento no Japão exija o consentimento do titular dos dados da UE. Embora a obtenção desse consentimento exija que o PIHBO contacte o titular dos dados, quando tal não for possível, a única consequência será a obrigatoriedade de manter a finalidade original.

2.3.2. *Licitude e lealdade do tratamento*

(44) A proteção adicional referida no considerando 43 é tanto mais pertinente porquanto é através do princípio da limitação da finalidade que o sistema japonês também assegura que os dados pessoais são tratados de forma lícita e leal.

(45) Nos termos da APPI, ao recolher informações pessoais, um PIHBO é obrigado a especificar de forma pormenorizada a finalidade para que utiliza essas informações pessoais ([29]) e a informar de imediato o titular dos dados sobre a finalidade da referida utilização (ou a divulgá-la publicamente) ([30]). Além disso, o artigo 17.º da APPI estabelece que um PIHBO não deve adquirir informações pessoais fraudulentamente ou por outros meios ilícitos. No que se refere a determinadas categorias de dados, como as informações pessoais que requerem atenção especial, a sua aquisição exige o consentimento do titular dos dados (artigo 17.º, n.º 2, da APPI).

([26]) As P&R publicadas pela PPC incluem vários exemplos que ilustram este conceito. Os exemplos de situações em que a alteração permanece dentro de um âmbito razoavelmente pertinente incluem, nomeadamente, a utilização de informações pessoais adquiridas junto de compradores de bens ou serviços, no contexto de uma transação comercial, com a finalidade de informar os referidos compradores a respeito de outros bens ou serviços pertinentes disponíveis (por exemplo, o operador de um ginásio que regista os endereços de correio eletrónico dos membros para os informar sobre os cursos e programas). Ao mesmo tempo, as P&R contemplam igualmente um exemplo de uma situação em que não é permitido alterar a finalidade da utilização, nomeadamente quando uma empresa envia informações sobre os seus bens e serviços para endereços de correio eletrónico que recolheu com a finalidade de alertar sobre a ocorrência de um fraude ou furto de um cartão de membro.

([27]) Estas isenções poderão resultar de outras leis e regulamentos ou referir-se a situações em que a gestão das informações pessoais seja necessária i) para a «proteção da vida humana, da integridade física ou de bens»; ii) para «melhorar a salubridade pública ou promover o crescimento de crianças saudáveis»; ou iii) para «cooperar com agências ou organismos governamentais ou com os seus representantes» na execução das suas tarefas legais. Além disso, as categorias i) e ii) apenas se aplicam, caso seja difícil obter o consentimento do titular dos dados, e a categoria iii) apenas se aplica, caso exista o risco de a obtenção do consentimento do titular dos dados interferir na execução das referidas tarefas.

([28]) No entanto, com base no artigo 23.º, n.º 1, da APPI, o consentimento do titular dos dados é, em princípio, necessário para a divulgação dos dados junto de terceiros. Deste modo, o titular dos dados pode exercer algum controlo sobre a utilização dos seus dados por outro operador comercial.

([29]) De acordo com o artigo 15.º, n.º 1, da APPI, tal especificação deve ser «o mais explícita possível».

([30]) Artigo 18.º, n.º 1, da APPI.

(46) Subsequentemente, tal como explicado nos considerandos 41 e 42, o PIHBO está proibido de tratar as informações pessoais com outras finalidades, exceto se o titular dos dados der o seu consentimento quanto a esse tratamento ou caso se aplique uma das derrogações constantes do artigo 16.º, n.º 3, da APPI.

(47) Por último, no tocante à comunicação subsequente de informações pessoais a terceiros ([31]), o artigo 23.º, n.º 1, da APPI limita essa divulgação a casos específicos, regra geral, mediante o consentimento prévio do titular dos dados ([32]). O artigo 23.º, n.ºs 2, 3 e 4, da APPI estabelece derrogações ao requisito para obter o consentimento. No entanto, tais derrogações só se aplicam aos dados não sensíveis, exigindo que o operador comercial informe previamente os titulares dos dados em causa da sua intenção de divulgar as informações pessoais a um terceiro e da possibilidade de oposição a qualquer divulgação subsequente ([33]).

(48) No que se refere às transferências da União Europeia, os dados pessoais terão sido necessariamente recolhidos e tratados na UE primeiro, em conformidade com o Regulamento (UE) 2016/679. Tal implica sempre, por um lado, a recolha e o tratamento, incluindo para efeitos de transferência da União Europeia para o Japão, com base num dos fundamentos jurídicos indicados no artigo 6.º, n.º 1, do Regulamento e, por outro lado, a recolha para uma finalidade específica, explícita e legítima, assim como a proibição de tratamento posterior, incluindo por via de uma transferência, de uma forma incompatível com essa finalidade, como previsto nos artigos 5.º, n.º 1, alínea b) e 6.º, n.º 4, do Regulamento.

(49) Na sequência da transferência, segundo o norma complementar 3, o PIHBO que recebe os dados deve «confirmar» a(s) finalidade(s) específica(s) subjacente(s) à transferência (ou seja, a finalidade determinada nos termos do Regulamento (UE) 2016/679) e tratar subsequentemente esses dados em conformidade com essa(s) finalidade(s) ([34]). Tal implica não só que a entidade que obtém inicialmente os referidos dados pessoais no Japão, mas também qualquer destinatário futuro dos mesmos (incluindo um mandatário) fica vinculado à(s) finalidade(s) determinada(s) no Regulamento.

(50) Além disso, caso pretenda alterar a finalidade, tal como previamente especificado no Regulamento (UE) 2016/679, nos termos do artigo 16.º, n.º 1, da APPI, o PIHBO teria de obter, em princípio, o consentimento do titular dos dados. Sem o referido consentimento, qualquer tratamento de dados que excedesse o âmbito necessário para cumprir essa finalidade de utilização constituiria uma violação do artigo 16.º, n.º 1, que seria passível de execução pela PPC e pelos tribunais.

(51) Assim, dado que nos termos do Regulamento (UE) 2016/679 uma transferência exige um fundamento jurídico válido e uma finalidade determinada, os quais se encontram refletidos na finalidade de utilização «confirmada» no âmbito da APPI, a combinação das disposições aplicáveis da APPI e da norma complementar 3 assegura a licitude permanente do tratamento dos dados da UE no Japão.

2.3.3. *Exatidão e minimização dos dados*

(52) Os dados devem ser exatos e, quando necessário, objeto de atualização. Devem ser adequados, pertinentes e não excessivos relativamente às finalidades para que são tratados.

(53) Estes princípios encontram-se garantidos na legislação japonesa pelo artigo 16.º, n.º 1, da APPI, que proíbe o tratamento de informações pessoais para além do «âmbito necessário para cumprir uma finalidade de utilização». Como a PPC explica, tal não só exclui a utilização não adequada e excessiva de dados (para além do necessário para cumprir a finalidade da utilização), mas também implica a proibição de tratar dados irrelevantes para o cumprimento da finalidade de utilização.

([31]) Embora, para efeitos da aplicação do artigo 23.º os mandatários sejam excluídos da noção de «terceiro» (ver ponto 5), essa exclusão só se aplica na medida em que estes devam tratar dados pessoais no âmbito do respetivo mandato («dentro do âmbito necessário para cumprir uma finalidade de utilização»), ou seja, intervenham enquanto subcontratantes.

([32]) Os outros motivos (excecionais) são: i) a transmissão de informações pessoais «com fundamento em leis e regulamentos»; ii) casos «em que haja a necessidade de proteger uma vida humana, a integridade física ou o bem-estar e seja difícil obter o consentimento do titular»; iii) casos «em que haja uma necessidade especial de melhorar a salubridade pública ou de promover o desenvolvimento de crianças saudáveis e seja difícil obter o consentimento do titular»; e iv) casos «em que haja uma necessidade de cooperar com um organismo da administração central ou um órgão de poder local ou com uma pessoa incumbida por estes de conduzir assuntos prescritos na legislação e nos regulamentos e a obtenção do consentimento do titular puder interferir na condução dos referidos assuntos».

([33]) As informações a transmitir incluem, nomeadamente, as categorias de dados pessoais a partilhar com terceiros e o método de transmissão. Por outro lado, o PIHBO deve informar o titular dos dados sobre a possibilidade de se opor à transmissão e em que moldes pode apresentar esse pedido.

([34]) Nos termos do artigo 26.º, n.º 1, subalínea ii) da APPI, um PIHBO é obrigado, quando recebe dados pessoais de um terceiro, a «confirmar» (verificar) os «pormenores da obtenção dos dados pessoais por esse terceiro», incluindo a finalidade dessa obtenção. Embora o artigo 26.º não especifique claramente que o PIHBO deva então respeitar essa finalidade, a norma complementar 3 exige-o de forma explícita.

(54) No que se refere à obrigação de manter a exatidão e a atualidade dos dados, o artigo 19.º da APPI exige que o PIHBO «se esforce por manter os dados pessoais exatos e atuais dentro do âmbito necessário para cumprir uma finalidade de utilização». Esta disposição deve ser considerada em conjugação com o artigo 16.º, n.º 1, da APPI: de acordo com as explicações recebidas da PPC, se um PIHBO não cumprir os níveis de exatidão prescritos, não se considera que o tratamento das informações pessoais cumpra a finalidade da utilização e, por conseguinte, nos termos do artigo 16.º, n.º 1, torna-se ilícito.

2.3.4. *Limitação da conservação*

(55) Em princípio, os dados não devem ser conservados mais tempo do que o necessário para as finalidades para que são tratados.

(56) Nos termos do artigo 19.º da APPI, os PIHBO são obrigados a «esforçar-se […] por apagar os dados pessoais sem demora quando a sua utilização deixar de ser necessária». Esta disposição deve ser lida em conjugação com o artigo 16.º, n.º 1, da APPI, que proíbe o tratamento de informações pessoais para além do «âmbito necessário para cumprir uma finalidade de utilização». Uma vez cumprida a finalidade da utilização, o tratamento das informações pessoais já não pode ser considerado necessário e, portanto, não pode manter-se (a menos que o PIHBO obtenha o consentimento do titular dos dados para o efeito).

2.3.5. *Segurança dos dados*

(57) Os dados pessoais devem ser tratados de uma forma que garanta a sua segurança, incluindo proteção contra tratamento não autorizado ou ilícito e contra perda, destruição ou danos acidentais. Para este fim, os operadores comerciais devem tomar as medidas técnicas e organizativas adequadas para proteger os dados pessoais contra eventuais ameaças. Estas medidas devem ser avaliadas tendo em consideração o estado atual dos conhecimentos e os custos conexos.

(58) Este princípio foi transposto para a legislação japonesa através do artigo 20.º da APPI, que estabelece que um PIHBO «deve tomar as medidas necessárias e adequadas para controlar a segurança dos dados pessoais, incluindo a prevenção de fuga, perda ou deterioração dos dados pessoais por si geridos.» As orientações da PPC explicam as medidas a tomar, incluindo os métodos para estabelecer políticas básicas, regras de gestão dos dados e várias «medidas de controlo» (relativas à segurança organizativa, bem como à segurança humana, física e tecnológica) ([35]). Além disso, as orientações da PPC e um comunicado específico (apêndice 8 relativo ao «Conteúdo das medidas de gestão da segurança que devem ser tomadas») publicados pela PPC fornecem mais pormenores sobre as medidas respeitantes a incidentes de segurança, que envolvam, nomeadamente, a fuga de informações pessoais, no âmbito das medidas de gestão de segurança a tomar pelos PIHBO ([36]).

(59) Por outro lado, sempre que o tratamento das informações pessoas seja levado a cabo por funcionários ou subcontratantes, nos termos dos artigos 20.º e 21.º da APPI, deve ser assegurada, para efeitos de controlo da segurança, uma «supervisão necessária e adequada». Por último, nos termos do artigo 83.º da APPI, as disposições de caráter penal da lei estabelecem uma pena de prisão até um ano em caso de furto ou fuga intencional de informações pessoais.

2.3.6. *Transparência*

(60) Os titulares dos dados devem ser informados sobre as principais características do tratamento dos respetivos dados pessoais.

(61) O artigo 18.º, n.º 1, da APPI exige que o PIHBO disponibilize ao titular dos dados informação sobre a finalidade de utilização das informações pessoais obtidas, exceto nos «casos em que uma finalidade de utilização tenha sido previamente divulgada ao público». A mesma obrigação existe no caso de uma alteração autorizada da finalidade (artigo 18.º, n.º 3). Isto permite igualmente garantir que o titular dos dados é informado de que os seus dados foram recolhidos. Embora, de modo geral, a APPI não exija que o PIHBO informe o titular dos dados sobre os destinatários previstos dos dados pessoais na fase de recolha dos mesmos, em caso de divulgação subsequente, essa informação é uma condição necessária para toda e qualquer transmissão de informações a um terceiro (destinatário), com base no artigo 23.º, n.º 2, e, por conseguinte, sempre que seja efetuada sem o consentimento prévio do titular dos dados.

([35]) Orientações da PPC (edição sobre as normas gerais), p. 41 e pp. 86 a 98.

([36]) Nos termos da secção 3-3-2 das orientações da PPC, caso essa fuga, deterioração ou perda ocorra, o PIHBO é obrigado a conduzir as investigações necessárias e, em particular, a avaliar a amplitude da infração dos direitos e interesses da pessoa singular, assim como a natureza e a quantidade das informações pessoais afetadas.

(62) No que se refere aos «dados pessoais conservados», o artigo 27.º da APPI estabelece que o PIHBO deve informar o titular dos dados sobre a sua identidade (dados de contacto), a finalidade da utilização e os procedimentos de resposta a um pedido respeitante aos direitos individuais do titular dos dados, nos termos dos artigos 28.º, 29.º e 30.º da APPI.

(63) À semelhança das normas complementares, os dados pessoais transferidos da União Europeia serão considerados como «dados pessoais conservados», independentemente do respetivo prazo de conservação (a menos que sejam abrangidos por isenções), e estarão sempre sujeitos às exigências de transparência instituídas em ambas as disposições citadas.

(64) Tanto as exigências do artigo 18.º como o dever de informação sobre a finalidade de utilização, nos termos do artigo 27.º da APPI, estão abrangidas pelo mesmo conjunto de exceções, baseadas principalmente em considerações de interesse público e na proteção dos direitos e interesses do titular dos dados, de terceiros e do responsável pelo tratamento ([37]). De acordo com a interpretação desenvolvida nas orientações da PPC, as referidas exceções são aplicáveis em situações muito específicas, nomeadamente no caso de a informação sobre a finalidade da utilização for suscetível de comprometer medidas legítimas tomadas pelo operador comercial para proteger determinados interesses (por exemplo o combate à fraude, à espionagem industrial e à sabotagem).

2.3.7. *Categorias especiais de dados*

(65) Devem existir garantias específicas aplicáveis ao tratamento de «categorias especiais» de dados.

(66) O conceito de «informações pessoais que requerem atenção especial» encontra-se definido no artigo 2.º, n.º 3, da APPI. Esta disposição refere-se a «informações pessoais que incluem a raça, credo, estatuto social, historial clínico e registo criminal do titular, bem como o facto de ter sofrido danos em consequência de um crime, ou outras descrições, etc. determinadas por decreto ministerial como aquelas cujo tratamento requer atenção especial por forma a não causar discriminação injusta, prejuízo ou outras desvantagens ao titular.» Essas categorias correspondem, em grande parte, à lista de dados sensíveis nos termos dos artigos 9.º e 10.º do Regulamento (UE) 2016/679. Concretamente, o «historial clínico» corresponde aos dados relativos à saúde, enquanto o «registo criminal e o facto de ter sofrido danos em consequência de um crime» são substancialmente idênticos às categorias a que se refere o artigo 10.º do Regulamento (UE) 2016/679. As categorias previstas no artigo 2.º, n.º 3, da APPI são objeto de uma interpretação mais aprofundada no decreto ministerial e nas orientações da PPC. Segundo o ponto 8 da secção 2.3 das orientações da PPC, as subcategorias de «historial clínico», especificadas no artigo 2.º, subalíneas ii) e iii), do decreto ministerial, são interpretadas como abrangendo dados genéticos e biométricos. De igual modo, embora não inclua expressamente os termos «origem étnica» e «opiniões políticas», a lista inclui referências à «raça» e ao «credo». Tal como explicam os pontos 1 e 2 da secção 2.3 das orientações da PPC, a referência à «raça» abrange «vínculos étnicos ou vínculos a uma região do mundo específica», enquanto «credo» é entendido como incluindo opiniões religiosas e políticas.

(67) Como resulta claro da redação da disposição, não se trata de uma lista definitiva, uma vez que podem ser acrescentadas mais categorias de dados na medida em que o seu tratamento suscite um risco de «discriminação injusta, prejuízo ou outras desvantagens ao titular».

(68) Embora o conceito de dados «sensíveis» seja, por inerência, um conceito social no sentido em que se fundamenta nas tradições culturais e jurídicas, nas considerações morais, nas opções políticas, etc. de uma determinada sociedade, perante a importância de assegurar garantias adequadas para os dados sensíveis, quando transferidos para operadores comerciais no Japão, a Comissão conseguiu que as proteções especiais conferidas a «informações pessoais que requerem atenção especial», no âmbito da legislação japonesa, fossem alargadas a todas as categorias reconhecidas como «dados sensíveis» no Regulamento (UE) 2016/679. Para este efeito, a norma complementar 1 dispõe que os dados transferidos da União Europeia relativos à vida sexual, à orientação sexual ou à filiação sindical de uma pessoa singular devem ser tratados pelos PIHBO «da mesma forma que as informações pessoais que requerem atenção especial, na aceção do artigo 2.º, n.º 3, da [APPI]».

([37]) Existem i) casos em que há uma possibilidade de a informação ao titular dos dados sobre a finalidade da utilização ou a sua divulgação pública «prejudicar a vida, a integridade física, o bem-estar ou outros direitos e interesses do titular ou de um terceiro» ou «os direitos ou interesses legítimos do […] PIHBO»; ii) casos em que «há uma necessidade de cooperar com um organismo da administração central ou com um órgão de poder local» na execução das suas tarefas legais e se tal informação ou divulgação interferir nesses «assuntos»; iii) casos em que a finalidade de utilização é clara tendo em conta a situação em que os dados foram obtidos.

(69) No que se refere às garantias materiais suplementares aplicáveis às informações pessoais que requerem atenção especial, nos termos do artigo 17.º, n.º 2, da APPI, os PIHBO não estão autorizados a obter esse tipo de dados sem o consentimento prévio da pessoa singular em causa, apenas sob reserva de derrogações limitadas ([38]). Por outro lado, esta categoria de informações pessoais encontra-se excluída da possibilidade de divulgação a terceiros, com base no procedimento definido no artigo 23.º, n.º 2, da APPI (que permite a transmissão de dados a terceiros sem o consentimento prévio da pessoa singular em causa).

2.3.8. *Responsabilização*

(70) De acordo com o princípio da responsabilização, as entidades responsáveis pelo tratamento de dados são obrigadas a aplicar medidas técnicas e organizativas adequadas para cumprir as suas obrigações de proteção dos dados de forma eficaz e poder demonstrar esse cumprimento, em particular junto da autoridade de controlo competente.

(71) Como referido na nota de rodapé 34 (considerando 49), nos termos do artigo 26.º, n.º 1, da APPI, os PIHBO são obrigados a verificar a identidade de um terceiro que lhes transmita dados pessoais, bem como as «circunstâncias» em que esses dados foram obtidos por esse terceiro (no caso dos dados pessoais abrangidos pela presente decisão, de acordo com a APPI e com a norma complementar 3, tais circunstâncias devem incluir o facto de os dados serem originários da União Europeia e a finalidade da transmissão dos dados original). Esta medida tem por objetivo, entre outros, assegurar a licitude do tratamento dos dados ao longo da cadeia de tratamento dos dados pessoais pelos PIHBO. Além disso, nos termos do artigo 26.º, n.º 3, da APPI, os PIHBO são obrigados a manter um registo da data de receção e das informações (obrigatórias) recebidas do terceiro, nos termos do n.º 1, assim como do nome da pessoa singular em causa (titular dos dados), das categorias de dados tratados e, na medida em que seja pertinente, do facto de o titular dos dados ter dado o seu consentimento à partilha dos seus dados pessoais. Tal como especificado no artigo 18.º das normas da PPC, os referidos registos devem ser conservados por um período mínimo de um a três anos, consoante as circunstâncias. No exercício das suas competências, a PPC pode exigir a apresentação de tais registos ([39]).

(72) Os PIHBO devem tratar, de forma célere e adequada, eventuais reclamações apresentadas por pessoas singulares afetadas quanto ao tratamento das suas informações pessoais. A fim de facilitar o tratamento das reclamações, devem criar o «sistema necessário para cumprir [esta] finalidade», o que implica que devem aplicar procedimentos apropriados na respetiva organização (designadamente, atribuir responsabilidades ou indicar um ponto de contacto).

(73) Por último, a APPI cria um enquadramento para a participação das organizações industriais setoriais na garantia de um nível de conformidade elevado (ver capítulo IV, secção 4). A função das referidas associações acreditadas de proteção de informações pessoais ([40]) é promover a proteção das informações pessoais prestando apoio às empresas com os seus conhecimentos especializados, mas também contribuir para a aplicação de garantias, nomeadamente, através do tratamento de reclamações individuais e da ajuda na resolução de conflitos conexos. Para o efeito, podem exigir, se for caso disso, que os PIHBO participantes adotem as medidas necessárias ([41]). Além disso, no caso de violação de dados ou de outros incidentes de segurança, os PIHBO devem, em princípio, informar a PPC, assim como o titular dos dados (ou o público) e tomar as medidas necessárias, incluindo medidas para minimizar os danos e evitar a repetição de incidentes semelhantes ([42]). Embora estes esquemas sejam voluntários, em 10 de agosto de 2017, a PPC havia elaborado uma lista de 44 organizações, em que só a maior destas, o

([38]) As isenções são as seguintes: i) «casos com fundamento em leis e regulamentos»; ii) «casos em que haja a necessidade de proteger uma vida humana, a integridade física ou ao bem-estar e seja difícil obter o consentimento do titular»; iii) «casos em que haja uma necessidade especial de melhorar a salubridade pública ou de promover o desenvolvimento de crianças saudáveis e seja difícil obter o consentimento do titular»; iv) «casos em que haja uma necessidade de cooperar com um organismo da administração central ou um órgão de poder local ou com uma pessoa incumbida por estes de conduzir assuntos prescritos na legislação e nos regulamentos e a obtenção do consentimento do titular puder interferir na condução dos referidos assuntos»; e v) casos em que as referidas informações pessoais que requerem atenção especial sejam publicamente divulgadas por um titular de dados, uma organização governamental, um órgão de poder local, uma pessoa abrangida por uma das categorias do artigo 76.º, n.º 1, ou por outras pessoas previstas nas normas da PPC. Uma categoria adicional refere-se a «outros casos determinados por decreto ministerial como equivalentes aos casos definidos em cada ponto precedente» e, nos termos do decreto ministerial, abrange, nomeadamente, características pessoais notórias (por exemplo, um problema de saúde visível), quando os dados sensíveis sejam obtidos (de forma não intencional) através da observação visual ou da captação de imagens de vídeo ou fotográficas do titular dos dados, por exemplo por câmaras de videovigilância.

([39]) Nos termos do artigo 40.º, n.º 1, da APPI, a PPC pode, na medida do necessário à aplicação das disposições pertinentes da APPI, exigir que um PIHBO apresente informações ou materiais necessários, relacionados com o tratamento de informações pessoais.

([40]) A APPI estabelece, nomeadamente, as regras de acreditação das referidas organizações; ver artigos 47.º a 50.º da APPI.

([41]) Artigo 52.° da APPI.

([42]) Notificação da PPC n.º 1/2017 «Relativa às medidas a tomar nos casos em que ocorram violações de dados pessoais ou outros incidentes».

Centro de Desenvolvimento e Tratamento do Japão (JIPDEC), contava com 15 436 operadores comerciais participantes ([43]). Os esquemas acreditados abrangem associações setoriais, como por exemplo a Associação de Corretores de Valores Mobiliários do Japão, a Associação de Escolas de Condução do Japão ou a Associação de Agentes Matrimoniais ([44]).

(74) As organizações acreditadas de proteção de informações pessoais apresentam relatórios anuais sobre as respetivas operações. De acordo com a «Descrição geral da situação em matéria de aplicação [da] APPI no exercício financeiro de 2015», publicada pela PPC, as organizações acreditadas de proteção de informações pessoais receberam um total de 442 reclamações, dirigiram 123 pedidos de explicação a operadores comerciais sob a sua jurisdição, solicitaram documentos aos referidos operadores em 41 casos, emitiram 181 instruções e formularam duas recomendações ([45]).

2.3.9. *Restrições relativas a transferências subsequentes*

(75) O nível de proteção assegurado aos dados pessoais transferidos da União Europeia para operadores comerciais no Japão não pode ser prejudicado pela transferência subsequente desses dados para destinatários num país terceiro fora do Japão. As referidas «transferências subsequentes», que constituem, da perspetiva do operador comercial japonês, transferências internacionais do Japão, apenas devem ser permitidas nos casos em que o destinatário fora do Japão esteja, pelo seu lado, sujeito a normas que assegurem um nível de proteção semelhante ao garantido no âmbito da ordem jurídica japonesa.

(76) Encontra-se consagrado um primeiro nível de proteção no artigo 24.º da APPI, que proíbe, em geral, a transferência de dados pessoais para terceiros fora do território do Japão sem o consentimento prévio da pessoa singular em causa. A norma complementar 4 assegura que, no caso de transferências de dados da União Europeia, tal consentimento seja particularmente bem fundamentado, porquanto exige que «sejam fornecidas informações sobre as circunstâncias inerentes à transferência, necessárias para que o titular tome uma decisão relativamente ao seu consentimento» à pessoa singular em causa. Nessa base, o titular dos dados deve ser informado de que os dados serão transferidos para o estrangeiro (fora do âmbito de aplicação da APPI) e do país de destino concreto, permitindo-lhe assim avaliar o risco para a privacidade resultante dessa transferência. Além disso, como resulta do artigo 23.º da APPI (ver considerando 47), as informações fornecidas ao titular devem abranger os elementos obrigatórios por força do n.º 2 desse artigo, nomeadamente as categorias de dados pessoais fornecidos a terceiros e o método de divulgação.

(77) O artigo 24.º da APPI, aplicado em conjugação com o artigo 11.º, n.º 2, das normas da PPC, estabelece várias derrogações a esta regra baseada no consentimento. Por outro lado, nos termos do artigo 24.º, também se aplicam às transferências de dados internacionais as mesmas derrogações aplicáveis de acordo com o artigo 23.º, n.º 1, da APPI ([46]).

(78) A fim de assegurar a continuidade da proteção, no caso de dados pessoais transferidos da União Europeia para o Japão, no âmbito da presente decisão, a norma complementar 4 reforça o nível de proteção das transferências subsequentes desses dados pelo PIHBO para um destinatário num país terceiro. Para tal, limita e enquadra os fundamentos para as transferências internacionais a que o PIHBO pode recorrer como alternativa ao consentimento. Mais concretamente, e sob reserva das derrogações estabelecidas no artigo 23.º, n.º 1, da APPI, os dados pessoais transferidos no âmbito da presente decisão poderão ser objeto de transferências (subsequentes) sem consentimento em apenas dois casos: i) quando os dados são enviados para um país terceiro que, nos termos do artigo 24.º da APPI, a PPC reconheceu como assegurando um nível de proteção equivalente ao do Japão ([47]); ou ii) quando o PIHBO e o destinatário no país terceiro adotaram conjuntamente medidas que conferem um nível de proteção equivalente ao da APPI, considerado em conjugação com as normas complementares, através de um contrato, de outras formas de acordos vinculativos ou de convenções vinculativas no âmbito de um grupo de empresas. A segunda categoria corresponde aos instrumentos utilizados nos termos do Regulamento (UE) 2016/679 para assegurar garantias adequadas (em particular, cláusulas contratuais e normas empresariais vinculativas). Além disso, como confirmado pela PPC, mesmo nesses casos, a transferência permanece sujeita às regras gerais aplicáveis à transmissão de dados pessoais para terceiros no âmbito da APPI (nomeadamente, a exigência de obter o consentimento nos termos do artigo 23.º, n.º 1, ou, alternativamente, a obrigação de informar junto com a

([43]) De acordo com os números publicados no sítio Web PrivacyMark do JIPDEC, com data de 2 de outubro de 2017.

([44]) PPC, lista de organizações acreditadas de proteção de informações pessoais, disponível na Internet em: https://www.ppc.go.jp/personal/nintei/list/ ou https://www.ppc.go.jp/files/pdf/nintei_list.pdf

([45]) PPC, Descrição geral da situação em matéria de aplicação da APPI no exercício financeiro de 2015 (outubro de 2016), disponível na Internet (apenas em japonês) em: https://www.ppc.go.jp/files/pdf/personal_sekougaiyou_27ppc.pdf

([46]) Ver nota de rodapé 32.

([47]) Para o efeito, em conformidade com o artigo 11.º das normas da PPC, não só são necessárias normas materiais equivalentes à APPI, controladas efetivamente por uma autoridade de execução independente, mas também a garantia de que as normas relevantes são aplicadas no país terceiro.

possibilidade de retirar o consentimento, nos termos do artigo 23.º, n.º 2, da APPI). Caso não seja possível fazer chegar o pedido de consentimento ao titular dos dados ou transmitir-lhe previamente a informação exigida pelo artigo 23.º, n.º 2, da APPI, a transferência não pode ter lugar.

(79) Por conseguinte, excetuando os casos em que a PPC tenha determinado que o país terceiro em causa assegura um nível de proteção equivalente ao garantido pela APPI ([48]), as exigências definidas na norma complementar 4 excluem a utilização de instrumentos de transferência que não originem uma relação vinculativa entre o exportador de dados japonês e o importador de dados do país terceiro e que não garantam o nível de proteção necessário. Será o caso, por exemplo, do sistema de regras de privacidade transfronteiriças (CBPR) da APEC, do qual o Japão é uma economia participante ([49]), uma vez que, neste sistema, as proteções não resultam de uma convenção vinculativa entre o exportador e o importador, no contexto da sua relação bilateral, e são claramente de um nível inferior ao garantido pela conjugação da APPI e das normas complementares ([50]).

(80) Por último, no caso das transferências (subsequentes), decorre uma outra garantia dos artigos 20.º e 22.º da APPI. Nos termos destas disposições, sempre que um operador de um país terceiro (importador de dados) atua em nome do PIHBO (exportador de dados), ou seja, na qualidade de subcontratante (ulterior), o segundo é obrigado a assegurar o controlo do primeiro em matéria de segurança do tratamento dos dados.

2.3.10. *Direitos individuais*

(81) À semelhança da legislação sobre proteção de dados da UE, a APPI confere às pessoas singulares uma série de direitos oponíveis. Estes incluem o direito de acesso («divulgação»), de retificação e de apagamento, assim como o direito de oposição («cessação da utilização»).

(82) Em primeiro lugar, nos termos do artigo 28.º, n.ºs 1 e 2, da APPI, o titular dos dados tem o direito de solicitar a um PIHBO que «divulgu[e] dados pessoais conservados que o possam identificar» e, após receção de tal pedido, o PIHBO «deve […] divulgar os dados pessoais conservados» ao titular dos dados. Os artigos 29.º (direito a correção) e 30.º (direito à cessação da utilização) têm a mesma estrutura do artigo 28.º.

(83) O artigo 9.º do decreto ministerial especifica que a divulgação de dados pessoais, a que se refere o artigo 28.º, n.º 2, da APPI, deve ser efetuada por escrito, salvo acordo em contrário entre o PIHBO e o titular dos dados.

(84) Estes direitos são objeto de três tipos de restrições: as relativas aos direitos e interesses da pessoa singular ou de terceiros ([51]), ingerência grave nas operações comerciais do PIHBO ([52]) e casos em que a divulgação viole outras leis e regulamentos ([53]). As situações em que estas restrições seriam aplicáveis são semelhantes a algumas das derrogações aplicáveis nos termos do artigo 23.º, n.º 1, do Regulamento (UE) 2016/679, que permite limitações aos

([48]) Até à data, a PPC ainda não adotou qualquer decisão nos termos do artigo 24.º da APPI em que seja reconhecido que um país terceiro assegura um nível de proteção equivalente ao do Japão. A única decisão que está a ponderar adotar diz respeito ao Espaço Económico Europeu (EEE). No que se refere às decisões que possam vir a ser adotadas no futuro, a Comissão acompanhará atentamente a situação e, se for caso disso, tomará as medidas adequadas para fazer face a eventuais efeitos adversos para a continuidade da proteção (ver considerandos 176, 177 e 184, assim como o artigo 3.º, n.º 1).

([49]) Embora só duas empresas japonesas tenham sido certificadas no âmbito do sistema CBPR da APEC (ver https://english.jipdec.or.jp/sp/protection_org/cbpr/list.html). Fora do Japão, os únicos outros operadores comerciais certificados no âmbito deste sistema foram um pequeno número (23) de empresas norte-americanas (ver https://www.trustarc.com/consumer-resources/trusted-directory/#apec-list).

([50]) Designadamente, não existe qualquer definição de dados sensíveis nem proteções específicas dos mesmos, assim como não existe qualquer limitação obrigatória à conservação dos dados. Ver também Grupo de Trabalho do artigo 29.º, «Opinion 02/2014 on a referential for requirements for Binding Corporate Rules submitted to national Data Protection Authorities in the EU and Cross-Border Privacy Rules submitted to APEC CBPR Accountability Agents», 6 de março de 2014.

([51]) Segundo a PPC, as restrições só podem ser justificadas por interesses «que mereçam proteção legal». Essa avaliação deve ser efetuada caso a caso «tendo em conta o nível de interferência no direito fundamental à privacidade, incluindo à proteção dos dados, tal como reconhecido pela Constituição e pela jurisprudência.» Os interesses protegidos podem incluir, nomeadamente, os segredos comerciais.

([52]) O conceito de «ingerência grave na correta condução da atividade comercial do operador» é ilustrado nas orientações da PPC com diversos exemplos, designadamente pedidos complexos, repetidos e idênticos, apresentadas pela mesma pessoa, quando os mesmos acarretem um ónus pesado para o operador comercial, suscetível de comprometer a sua capacidade para responder a outros pedidos [orientações da PPC (edição sobre as normas gerais), p. 62]. De um modo geral, a PPC confirmou que esta categoria é limitada a casos excecionais que não se limitem a um mero inconveniente. Um PIHBO não pode, nomeadamente, recusar a divulgação pelo simples facto de ter sido solicitada uma grande quantidade de dados.

([53]) Tal como foi confirmado pela PPC, tais leis devem respeitar o direito à privacidade, consagrado na Constituição, e, por conseguinte, «refletir uma restrição necessária e razoável».

direitos das pessoas singulares por motivos relacionados com a «defesa do titular dos dados ou dos direitos e liberdades de outrem» ou «outros objetivos importantes do interesse público geral». Embora a categoria de casos em que a divulgação violaria «outras leis ou regulamentos» possa parecer lata, as leis e os regulamentos, que estabelecem limitações nesta matéria, devem respeitar o direito constitucional à privacidade e só podem impor restrições na medida em que o exercício deste direito «atente contra o bem-estar público» ([54]). Tal requer um equilíbrio entre os interesses em jogo.

(85) Nos termos do artigo 28.º, n.º 3, da APPI, caso os dados solicitados não existam ou o PIHBO em causa decida não conceder acesso aos dados conservados, este é obrigado a informar sem demora a pessoa singular.

(86) Em segundo lugar, nos termos do artigo 29.º, n.ºs 1 e 2, da APPI, um titular de dados pode solicitar a correção, o aditamento ou o apagamento dos seus dados pessoais conservados, caso estes sejam inexatos. Após receção de um pedido nesse sentido, o PIHBO «deve […] conduzir uma investigação necessária» e, com base nos resultados dessa investigação, «efetuar a correção, etc. do conteúdo dos dados conservados».

(87) Em terceiro lugar, nos termos do artigo 30.º, n.ºs 1 e 2, da APPI, um titular de dados pode solicitar a um PIHBO que deixe de utilizar informações pessoais ou que apague essas informações, sempre que sejam tratadas em violação do artigo 16.º (relativo à limitação da finalidade) ou obtidas ilicitamente em violação do artigo 17.º da APPI (relativo à obtenção fraudulenta, por outros meios ilícitos ou, no caso de dados sensíveis, sem consentimento). De igual modo, nos termos do artigo 30.º, n.ºs 3 e 4, da APPI, a pessoa singular pode solicitar ao PIHBO que deixe de transmitir as informações a terceiros, sempre que essa transmissão viole o disposto no artigo 23.º, n.º 1, ou no artigo 24.º da APPI (respeitante à transmissão a terceiros, incluindo transferências internacionais).

(88) Se o pedido tiver fundamento, o PIHBO deve deixar de utilizar os dados ou de transmiti-los a um terceiro sem demora, na medida do necessário para pôr termo à violação ou, se um determinado caso for abrangido por uma derrogação (designadamente, se a cessação da utilização for suscetível de causar custos especialmente elevados) ([55]), deve adotar medidas alternativas necessárias para proteger os direitos e os interesses da pessoa em causa.

(89) Ao contrário do direito da UE, a APPI e as normas legais acessórias pertinentes não contêm disposições jurídicas que abordem especificamente a possibilidade de oposição para efeitos de comercialização direta. Esse tratamento deve, contudo, por força da presente decisão, ter lugar no quadro de uma transferência de dados pessoais previamente recolhidos na União Europeia. Nos termos do artigo 21.º, n.º 2, do Regulamento (UE) 2016/679, o titular dos dados deve ter sempre o direito de se opor a uma transferência de dados destinados a tratamento para efeitos de comercialização direta. Além disso, como referido no considerando 43, no âmbito da norma complementar 3 um PIHBO é obrigado a tratar os dados recebidos nos termos da decisão para a mesma finalidade para a qual foram transferidos da União Europeia, a menos que o titular dos dados dê o seu consentimento quanto à alteração da finalidade da utilização. Por conseguinte, se a transferência tiver sido efetuada para uma finalidade diferente da comercialização direta, um PIHBO no Japão está proibido de tratar os dados para efeitos de comercialização direta sem o consentimento do titular dos dados da UE.

(90) Em todos os casos descritos nos artigos 28.º e 29.º da APPI, o PIHBO é obrigado a notificar sem demora a pessoa singular do resultado do pedido, tendo, além disso, de apresentar uma justificação para a eventual recusa (parcial) com base nas derrogações legais previstas nos artigos 27.º a 30.º (artigo 31.º da APPI).

([54]) O Supremo Tribunal tem interpretado o artigo 13.º da Constituição como assegurando o direito à privacidade (ver os considerandos 7 e 8 anteriores). Embora este direito possa ser restringido nos casos em que «atente contra o bem-estar público», no seu acórdão de 6 de março de 2008 (ver considerando 8), o Supremo Tribunal deixou claro que qualquer restrição (que permita, no caso em apreço, que uma autoridade pública recolha e trate dados pessoais), deve ser ponderada em função do direito à privacidade, tendo em conta fatores como a natureza dos dados em causa, os riscos que o tratamento desses dados cria para as pessoas singulares, as garantias aplicáveis e os benefícios de interesse público resultantes do tratamento. Isto é muito semelhante ao tipo de ponderação exigida pela legislação da UE, com base nos princípios da necessidade e da proporcionalidade, para autorizar qualquer restrição aos direitos e salvaguardas em matéria de proteção de dados.

([55]) Para mais explicações sobre estas derrogações, consultar o comentário pormenorizado por artigo, do Professor Katsuya Uga, sobre a Lei revista relativa à proteção de informações pessoais, 2015, p. 217. Um exemplo de pedido suscetível de causar um «montante elevado de despesas» é o caso em que apenas alguns nomes de uma longa lista (por exemplo, um diretório) são tratados em violação do princípio da limitação da finalidade e o diretório já se encontra à venda, tendo como consequência que a retirada desses exemplares e a sua substituição por novos exemplares seriam extremamente dispendiosas. No mesmo exemplo, no caso de já terem sido vendidos exemplares do diretório a um grande número de pessoas e se tornar impossível recolhê-los na totalidade, seria igualmente «difícil proceder a uma cessação da utilização». Perante tais cenários, as «medidas alternativas necessárias» poderiam incluir, por exemplo, a publicação ou distribuição de uma errata. As referidas medidas não excluem outras formas de recurso (judicial), seja por violação dos direitos de privacidade, por danos à reputação (difamação) causados pela publicação ou por violação de outros interesses.

(91) No que se refere às condições para apresentar um pedido, o artigo 32.º da APPI (em conjugação com o decreto ministerial) permite que os PIHBO estabeleçam procedimentos razoáveis, incluindo em termos das informações necessárias para identificar os dados pessoais conservados. Nos termos do n.º 4 desse artigo, não podem, contudo, impor «encargos excessivos ao titular». Em certos casos, os PIHBO poderão impor taxas, desde que o seu valor se situe «dentro do âmbito considerado razoável tendo em vista os custos reais» (artigo 33.º da APPI).

(92) Por último, a pessoa singular pode opor-se à transmissão das suas informações pessoais a terceiros, nos termos do artigo 23.º, n.º 2, da APPI, ou recusar o seu consentimento, nos termos do artigo 23.º, n.º 1 (evitando, assim, a divulgação no caso de não existir mais nenhum fundamento jurídico). De igual modo, a pessoa singular pode suspender o tratamento dos dados para uma finalidade diferente recusando o seu consentimento nos termos do artigo 16.º, n.º 1, da APPI.

(93) Ao contrário do direito da UE, a APPI e as normas legais acessórias pertinentes não contêm disposições gerais que contemplem a questão das decisões respeitantes ao titular dos dados e se baseiem exclusivamente no tratamento automatizado dos dados pessoais. No entanto, a questão é abordada em algumas normas setoriais aplicáveis no Japão, que são particularmente relevantes para este tipo de tratamento. Incluem-se aqui setores nos quais é mais provável que as empresas recorram ao tratamento automatizado de dados pessoais para tomar decisões que afetam as pessoas singulares (nomeadamente o setor financeiro). Por exemplo, as «Orientações abrangentes relativas à supervisão dos principais bancos», revistas em junho de 2017, exigem que sejam dadas à pessoa em causa explicações concretas sobre as razões do indeferimento de um pedido para celebrar um acordo de empréstimo. Deste modo, estas normas oferecem proteções, nos casos, em número provavelmente muito limitado, em que as decisões automatizadas seriam tomadas pelo próprio operador comercial japonês «importador» (e não pelo responsável pelo tratamento dos dados da UE «exportador»).

(94) Em qualquer caso, no que se refere aos dados pessoais recolhidos na União Europeia, qualquer decisão baseada num tratamento automatizado será, normalmente, tomada pelo responsável pelo tratamento dos dados na União (que tem uma relação direta com o titular dos dados em causa), estando, por conseguinte, sujeita ao Regulamento (UE) 2016/679 ([56]). Tal inclui cenários de transferência em que o tratamento seja realizado por um operador comercial estrangeiro (por exemplo, japonês), que atua como agente (subcontratante) do responsável pelo tratamento da UE (ou como subcontratante ulterior do subcontratante da UE, o qual por sua vez recebeu os dados de um responsável pelo tratamento da UE que os recolheu) que, nesta base, toma então a decisão. Deste modo, não é provável que a inexistência na APPI de regras específicas sobre a tomada de decisões automatizadas afete o nível de proteção dos dados pessoais transferidos ao abrigo da presente decisão.

2.4. **Supervisão e execução coerciva**

2.4.1. *Supervisão independente*

(95) Por forma a assegurar que também seja garantido na prática um nível adequado de proteção dos dados, deve ser criada uma autoridade de controlo independente incumbida de supervisionar e aplicar coercivamente as normas em matéria de proteção de dados. Essa autoridade deve atuar com total independência e imparcialidade no cumprimento das suas obrigações e no exercício das respetivas competências.

(96) No Japão, a autoridade incumbida de supervisionar e aplicar a APPI é a PPC. A PPC é constituída por um presidente e oito comissários, designados pelo primeiro-ministro mediante a aprovação de ambas as câmaras da Dieta. O mandato do presidente e de cada comissário é de cinco anos, com possibilidade de recondução (artigo 64.º da APPI). Os comissários só podem ser destituídos com justa causa, num conjunto limitado de circunstâncias excecionais ([57]), não podendo envolver-se ativamente em atividades políticas. Além disso, nos termos da APPI, os comissários a tempo inteiro devem abster-se de exercer outras atividades remuneradas ou de caráter comercial. Todos os comissários estão igualmente sujeitos a normas internas que os impedem de participar nas deliberações em caso de conflito de interesses. A PPC é assistida por um secretariado, chefiado por um secretário-geral, que foi criado para fins de execução das tarefas que lhe incumbem (artigo 70.º da APPI). Tanto os comissários como os demais funcionários do secretariado estão vinculados por regras estritas de confidencialidade (artigos 72.º e 82.º da APPI).

([56]) Em contrapartida, no caso excecional em que o operador japonês tenha uma relação direta com titular dos dados da UE, aquela resulta normalmente do facto de o operador ter visado essa pessoa singular na União Europeia através da oferta de bens ou serviços ou do controlo do seu comportamento. Neste cenário, o operador japonês será, ele próprio, abrangido pelo âmbito de aplicação do Regulamento (UE) 2016/679 (artigo 3.º, n.º 2), tendo, portanto, de cumprir diretamente a legislação europeia relativa à proteção de dados.

([57]) Nos termos do artigo 65.º da APPI, a destituição contra a vontade do comissário respetivo só é possível com um dos seguintes fundamentos: i) abertura de um processo de falência; ii) condenação por violação da APPI ou da Lei relativa à utilização de números de identificação; iii) condenação a uma pena de prisão sem possibilidade de prestação de trabalho ou a uma pena ainda mais severa; iv) incapacidade para executar os seus deveres por motivos de distúrbio mental ou físico, ou de conduta reprovável.

(97) Os poderes da PPC são exercidos com total independência ([58]) e são definidos principalmente nos artigos 40.º, 41.º e 42.º da APPI. Nos termos do artigo 40.º, a PPC pode solicitar aos PIHBO que comuniquem informações ou apresentem documentos sobre as operações de tratamento, podendo igualmente proceder a inspeções tanto no local como dos livros e outros documentos. Na medida do necessário à aplicação da APPI, a PPC pode ainda formular orientações ou conselhos aos PIHBO relativamente à gestão das informações pessoais. A PPC já exerceu os poderes que lhe são conferidos pelo artigo 41.º da APPI, quando formulou orientações dirigidas ao Facebook, na sequência das revelações efetuadas no âmbito do caso Facebook/Cambridge Analytica.

(98) Mais importante ainda, a PPC tem competência, quer dando seguimento a uma queixa ou atuando por sua própria iniciativa, para emitir recomendações e ordens destinadas a fazer aplicar a APPI e outras normas vinculativas (incluindo as normas complementares) em casos concretos. Tais competências são definidas no artigo 42.º da APPI. Enquanto os n.ºs 1 e 2 deste artigo preveem um mecanismo em duas etapas, pelo qual a PPC pode emitir uma ordem (apenas) na sequência de uma recomendação prévia, o n.º 3 permite que, em casos urgentes, seja diretamente adotada uma ordem.

(99) Embora nem todas as disposições do capítulo IV, secção 1, da APPI se encontrem enumeradas no artigo 42.º, n.º 1, o qual também determina o âmbito de aplicação do artigo 42.º, n.º 2, a explicação para tal poderá residir no facto de algumas destas disposições não dizerem respeito a obrigações do PIHBO ([59]) e de todas as proteções essenciais já serem asseguradas por outras disposições constantes dessa lista. Por exemplo, embora não sendo mencionado o artigo 15.º (que exige que o PIHBO defina a finalidade da utilização e trate as informações pessoais relevantes exclusivamente dentro do seu âmbito de aplicação), a não observação desta exigência pode constituir fundamento para uma recomendação, baseada numa violação do artigo 16.º, n.º 1 (que proíbe o PIHBO de tratar informações pessoais que excedam o âmbito necessário ao cumprimento da finalidade da utilização, a menos que obtenha o consentimento do titular dos dados) ([60]). Uma outra disposição, omissa no artigo 42.º, n.º 1, é o artigo 19.º da APPI relativo à exatidão e à conservação dos dados. Em caso de incumprimento desta disposição, o seu cumprimento pode ser passível de execução coerciva, quer por violação do artigo 16.º, n.º 1, ou com base numa violação do artigo 29.º, n.º 2, se a pessoa em causa solicitar a correção ou o apagamento de dados erróneos ou excessivos e o PIHBO se recusar a satisfazer o pedido. No que se refere aos *direitos* do titular dos dados, nos termos dos artigos 28.º, n.º 1, 29.º, n.º 1, e 30.º, n.º 1, a supervisão da PPC é garantida através da atribuição de poderes de execução coerciva no tocante às *obrigações* correspondentes do PIHBO definidas nos referidos artigos.

(100) Nos termos do artigo 42.º, n.º 1, da APPI, se entender que se verifica uma «necessidade de proteger os direitos e interesses de uma pessoa singular nos casos em que um [PIHBO] tenha violado» disposições específicas da APPI, a PPC pode emitir uma recomendação de «suspensão do ato de violação ou de tomada de outras medidas necessárias para retificar a violação». Tal recomendação não é vinculativa, mas abre caminho a uma ordem vinculativa em conformidade com o artigo 42.º, n.º 2, da APPI. Com base nesta disposição, se a recomendação não for acatada «sem que existam motivos legítimos» e a PPC «entender que está iminente uma violação grave dos direitos e interesses de uma pessoa singular», pode ordenar ao PIHBO que tome medidas consonantes com a recomendação.

(101) As normas complementares clarificam melhor e reforçam os poderes de execução coerciva da PPC. Mais concretamente, nos casos que envolvam dados importados da União Europeia, a PPC considera sempre a ausência da tomada de medidas por um PIHBO, em conformidade com uma recomendação emitida pela APPI, nos termos do artigo 42.º, n.º 1, sem motivos legítimos, como uma violação grave iminente dos direitos e interesses de uma pessoa singular, na aceção do artigo 42.º, n.º 2, e consequentemente como uma infração que justifica a emissão de uma ordem vinculativa. Por outro lado, a PPC apenas aceita como «motivo legítimo» para não cumprir uma recomendação uma «ocorrência de natureza extraordinária [que impeça o cumprimento] fora do controlo [do PIHBO], a qual não pode ser razoavelmente prevista (nomeadamente catástrofes naturais)» ou casos em que a necessidade de tomar medidas na sequência de uma recomendação «tenha deixado de existir porque [o PIHBO] tomou medidas alternativas para pôr termos à violação».

([58]) Ver artigo 62.º da APPI.

([59]) Determinadas disposições, por exemplo, dizem respeito a ações do PIHBO que são facultativas (artigos 32.º e 33.º da APPI), ou obrigações de «envidar os melhores esforços» que, como tal, não são passíveis de execução coerciva (artigos 31.º, 35.º, 36.º, n.º 6, e 39.º da APPI). Certas disposições não se aplicam ao PIHBO, mas sim a outros atores. É o caso, por exemplo, dos artigos 23.º, n.º 4, 26.º, n.º 2, e 34.º da APPI (todavia, a execução coerciva do artigo 26.º, n.º 2, da APPI é assegurada através da possibilidade de imposição de sanções penais nos termos do artigo 88.º, subalínea i) da APPI).

([60]) Além disso, como explicado no considerando 48, num contexto de transferência, a «finalidade da utilização» será especificada pelo exportador de dados da UE, o qual está sujeito, nesta matéria, à obrigação prevista no artigo 5.º, n.º 1, alínea b), do Regulamento (UE) 2016/679. Esta obrigação é passível de execução coerciva pela autoridade responsável pela proteção de dados na União Europeia.

(102) Nos termos do artigo 84.º da APPI, o incumprimento de uma ordem da PPC é considerado uma infração penal e um PIHBO que seja condenado pode ser punido com uma pena de prisão com possibilidade de prestação de trabalho até seis meses ou com multa até 300 000 ienes. Além disso, nos termos do artigo 85.º, subalínea i), da APPI, a falta de cooperação com a PPC ou a obstrução à sua investigação é punível com multa até 300 000 ienes. Estas sanções penais acrescem às que possam ser impostas pela violação material da APPI (ver considerando 108).

2.4.2. *Recurso judicial*

(103) A fim de assegurar uma proteção adequada e, nomeadamente, o exercício dos direitos individuais, o titular dos dados deve dispor de vias de recurso administrativas e judiciais eficazes, incluindo a possibilidade de obter uma indemnização por danos.

(104) Antes ou mesmo em vez de recorrer a vias de recurso administrativas e judiciais, a pessoa singular pode decidir apresentar uma reclamação sobre o tratamento dos seus dados pessoais junto do próprio responsável pelo tratamento. Com base no artigo 35.º da APPI, os PIHBO devem esforçar-se por tratar tais reclamações «de modo adequado e rápido» e estabelecer sistemas internos de tratamento de reclamações para atingir esse objetivo. Além disso, nos termos do artigo 61.º, alínea ii), da APPI, a PPC é responsável pela «mediação necessária quanto às reclamações apresentadas e pela cooperação prestada ao operador comercial que se ocupa da reclamação», abrangendo, em ambos os casos, as reclamações apresentadas por estrangeiros. Neste contexto, o legislador japonês confiou igualmente à administração central a tarefa de tomar as «medidas necessárias» para viabilizar e facilitar a resolução de reclamações pelos PIHBO (artigo 9.º), competindo aos órgãos de poder local assegurar a mediação nesses casos (artigo 13.º). A este respeito, as pessoas singulares podem apresentar uma reclamação junto de um dos mais de 1 700 centros do consumidor criados pelos órgãos de poder local, com base na Lei relativa à segurança do consumidor ([61]), além de poderem apresentar uma reclamação junto do Centro Nacional para os Assuntos do Consumidor do Japão. Tais reclamações podem igualmente ser apresentadas em relação a uma violação da APPI. Nos termos do artigo 19.º da Lei de Bases do Consumidor ([62]), os órgãos de poder local devem esforçar-se por participar no processo de mediação, no caso de reclamações, colocando à disposição das partes os necessários conhecimentos especializados. Estes mecanismos de resolução de litígios afiguram-se bastante eficazes, com uma taxa de resolução de 91,2 % em mais de 75 000 casos de reclamação em 2015.

(105) As violações das disposições da APPI por parte de um PIHBO podem dar origem a ações cíveis, bem como a processos penais e sanções. Em primeiro lugar, se uma pessoa singular considerar que os seus direitos foram violados, ao abrigo dos artigos 28.º, 29.º e 30.º da APPI, pode requerer uma medida inibitória, solicitando ao tribunal que condene um PIHBO a satisfazer o seu pedido, nos termos de uma destas disposições, ou seja, a divulgar os dados pessoais conservados (artigo 28.º), a retificar os dados pessoais conservados que estejam incorretos (artigo 29.º) ou a cessar o tratamento ilícito ou a transmissão não autorizada a terceiros (artigo 30.º). Esta ação pode ser instaurada sem necessidade de invocar o artigo 709.º do Código Civil ([63]) ou de recorrer ao direito penal ([64]). Tal significa, especificamente, que a pessoa singular não é obrigada a provar a existência de danos.

(106) Em segundo lugar, caso uma alegada violação não diga respeito a direitos individuais, nos termos dos artigos 28.º, 29.º e 30.º, mas sim a princípios gerais em matéria de proteção de dados ou a obrigações do PIHBO, a pessoa singular em causa pode instaurar uma ação cível contra o operador comercial, com base nas disposições relativas à responsabilidade civil do Código Civil do Japão, nomeadamente o artigo 709.º. Conquanto uma ação judicial ao abrigo do artigo 709.º exija, além da prova da culpa (dolo ou negligência), prova da existência de danos, nos termos do artigo 710.º do Código Civil, tais danos podem ser materiais ou morais. O montante da indemnização não está sujeito a qualquer limitação.

(107) No que respeita às vias de recurso disponíveis, o artigo 709.º do Código Civil japonês faz referência a uma indemnização pecuniária. No entanto, a jurisprudência japonesa tem interpretado este artigo como abrindo igualmente a possibilidade de obter uma medida inibitória ([65]). Deste modo, se um titular de dados intentar uma ação ao abrigo do artigo 709.º do Código Civil alegando que os seus direitos ou interesses foram lesados pela violação de uma disposição da APPI por parte do demandado, a ação intentada pode incluir, para além da indemnização por danos, o requerimento de uma medida inibitória destinada a pôr fim ao tratamento ilícito.

([61]) Lei n.º 50 de 5 de junho de 2009.
([62]) Lei n.º 60 de 22 de agosto de 2012.
([63]) O artigo 709.º do Código Civil constitui o principal fundamento para a instauração de processos civis de indemnização. Em conformidade com esta disposição, «uma pessoa que tenha violado, de forma intencional ou negligente, qualquer direito de outrem ou qualquer interesse juridicamente protegido de outrem, é responsável pela indemnização pelos danos daí resultantes.»
([64]) Tribunal Superior de Tóquio, acórdão de 20 de maio de 2015 (não publicado); Tribunal Distrital de Tóquio, acórdão de 8 de setembro de 2014, Westlaw Japan 2014WLJPCA09088002. Ver também o artigo 34.º, n.ºs 1 e 3, da APPI.
([65]) Ver Supremo Tribunal, acórdão de 24 de setembro de 2002 (Hanrei Times vol. 1106, p. 72).

(108) Em terceiro lugar, além das vias de recurso previstas no âmbito do direito civil (penal), o titular dos dados pode apresentar uma reclamação junto de um procurador ou de um agente da polícia judiciária quanto às violações da APPI que possam originar sanções de caráter penal. O capítulo VII da APPI contém várias disposições de ordem penal. A mais importante (artigo 84.º) refere-se ao incumprimento pelo PIHBO das ordens da PPC, nos termos do artigo 42.º, n.ºs 2 e 3. Se um operador comercial não cumprir uma ordem emitida pela PPC, o presidente desta comissão (assim como qualquer outro responsável governamental) ([66]) pode remeter o caso para um procurador ou agente da polícia judiciária e, desse modo, desencadear a abertura de um processo penal. A violação de uma ordem da PPC é punível com pena de prisão com possibilidade de prestação de trabalho até seis meses ou uma multa até 300 000 ienes. Outras disposições da APPI, que impõem sanções em caso de violações da APPI com impacto nos direitos e interesses de titulares de dados, incluem o artigo 83.º (relativo à «transmissão ou utilização dissimuladas» de uma base de dados de informações pessoais «com a finalidade de obter […] lucros ilícitos») e o artigo 88.º, subalínea i) (relativo à não prestação por parte de um terceiro de informações corretas ao PIHBO quando este recebe dados pessoais, em conformidade com o artigo 26.º, n.º 1, da APPI, em particular, sobre os pormenores da obtenção prévia dos referidos dados por esse terceiro). As referidas violações da APPI são puníveis, respetivamente, com pena de prisão com possibilidade de prestação de trabalho até um ano ou com multa até 500 000 ienes (no caso do artigo 83.º) ou com uma coima até 100 000 ienes [no caso do artigo 88.º, subalínea i)]. Embora a ameaça de uma sanção penal já tenha um forte efeito dissuasor sobre os administradores das empresas que dirigem as operações de tratamento dos PIHBO, assim como sobre as pessoas singulares que tratam os dados, o artigo 87.º da APPI clarifica que se um representante, trabalhador ou outro funcionário de uma pessoa coletiva violar o disposto nos artigos 83.º a 85.º da APPI, «o autor da infração deve ser punido, aplicando-se à pessoa coletiva em causa a multa prevista nos artigos correspondentes». Neste caso, podem ser impostas tanto ao trabalhador como à empresa multas até ao montante máximo previsto na lei.

(109) Por último, as pessoas singulares podem igualmente obter reparação contra as ações ou omissões da PPC. A este respeito, a legislação japonesa providencia várias vias de recurso administrativo e judicial.

(110) Caso uma pessoa singular não esteja satisfeita com uma linha de ação tomada pela PPC, pode interpor recurso administrativo no âmbito da Lei relativa à apreciação de reclamações administrativas ([67]). Por outro lado, se a pessoa singular entender que a PPC deveria ter atuado, mas não o fez, pode, nos termos do artigo 36.º, n.º 3, da referida lei, solicitar que a PPC emita um ato ou uma orientação administrativa, se considerar que «não foi emitido ou imposto qualquer ato ou orientação administrativa para retificar a violação».

(111) No que se refere ao recursos judiciais, ao abrigo da Lei do contencioso administrativo, uma pessoa singular, que não esteja satisfeita com um ato administrativo emitido pela PPC, pode intentar uma ação de condenação à prática de ato devido ([68]), em que requer ao tribunal que condene a PPC a tomar medidas adicionais ([69]). Em alguns casos, o tribunal pode também proferir uma decisão provisória de condenação à prática de ato devido, por forma a evitar danos irreversíveis ([70]). Além disso, nos termos da mesma lei, uma pessoa singular pode requerer a revogação de uma decisão da PPC ([71]).

(112) Por último, uma pessoa singular pode igualmente intentar uma ação de indemnização estatal contra a PPC, nos termos do artigo 1.º, n.º 1, da Lei relativa a recurso contra o Estado, no caso de ter sofrido danos causados pelo facto de uma ordem emitida pela PPC a um operador comercial ter sido ilícita ou de a PPC não ter exercido a sua autoridade.

3. ACESSO E UTILIZAÇÃO DE DADOS PESSOAIS TRANSFERIDOS DA UNIÃO EUROPEIA POR AUTORIDADES PÚBLICAS NO JAPÃO

(113) A Comissão avaliou igualmente as limitações e garantias, incluindo a supervisão e os mecanismos individuais de recurso disponíveis na legislação japonesa, no tocante à recolha e utilização subsequente de dados pessoais transferidos por autoridades públicas para operadores comerciais no Japão, para fins de interesse público, designadamente para efeitos de aplicação do direito penal e de segurança nacional («acesso governamental»). Nesta matéria, o Governo japonês apresentou à Comissão declarações, garantias e compromissos oficiais, assinados ao mais alto nível ministerial e das agências, os quais constam do anexo II da presente decisão.

([66]) Artigo 239.°, n.º 2, do Código de Processo Civil.
([67]) Lei n.º 160 de 2014.
([68]) Artigo 37.º, n.º 2, da Lei do contencioso administrativo.
([69]) Nos termos do artigo 3.º, n.º 6, da Lei do contencioso administrativo, o termo «ação de condenação à prática de ato devido» refere-se a uma ação judicial para obter a condenação por parte do tribunal de um órgão administrativo para que pratique um ato administrativo que «devia» ter inicialmente praticado, mas não praticou.
([70]) Artigo 37.º, n.º 5, da Lei do contencioso administrativo.
([71]) Capítulo II, secção 1, da Lei do contencioso administrativo.

3.1. **Quadro jurídico geral**

(114) Enquanto exercício da autoridade pública, o acesso governamental no Japão deve ter lugar no pleno respeito pela lei (princípio da legalidade). A Constituição japonesa contém disposições nesta matéria que limitam e enquadram a recolha de dados pessoais pelas autoridades públicas. Como já foi mencionado em relação ao tratamento pelos operadores comerciais, o Supremo Tribunal do Japão, com base no artigo 13.º da Constituição, que protege o direito à liberdade, tem reconhecido o direito à privacidade e à proteção dos dados ([72]). Um aspeto importante desse direito é a liberdade de não permitir que as informações pessoais sejam divulgadas a terceiros ([73]). Tal implica o direito à proteção efetiva dos dados pessoais contra abusos e (em particular) contra o acesso ilícito. É assegurada proteção adicional no artigo 35.º da Constituição, relativo ao direito de todas as pessoas à inviolabilidade do seu domicílio, documentos e haveres, o que exige que as autoridades públicas obtenham um mandado judicial emitido com «justificação suficiente» ([74]) em todos os casos de «buscas e apreensões». No seu acórdão de 15 de março de 2017 (processo GPS), o Supremo Tribunal esclareceu que a exigência de mandado judicial se aplica sempre que haja uma ingerência do Governo na esfera privada sem ter em conta a vontade da pessoa singular, nomeadamente através de um «inquérito coercivo». Um juiz só pode emitir um mandado se existirem suspeitas concretas da prática de um crime, ou seja, quando disponha de provas documentais que o levem a considerar que a pessoa objeto do inquérito cometeu uma infração penal ([75]). Consequentemente, as autoridades japonesas não estão autorizadas a recolher informações pessoais por meios coercivos em situações em que ainda não tenha ocorrido qualquer violação da lei ([76]), designadamente a fim de evitar um crime ou qualquer outra ameaça à segurança (como no caso de inquéritos por razão de segurança nacional).

(115) Ao abrigo do princípio da reserva da lei, a recolha de dados no âmbito de um inquérito coercivo deve ser especificamente autorizada por lei (como dispõe, por exemplo, o artigo 197.º, n.º 1, do Código de Processo Penal (CPP), em relação à recolha coerciva de informações para efeitos de uma investigação criminal). Esta exigência aplica-se igualmente ao acesso a informações eletrónicas.

(116) Mais importante ainda, o artigo 21.º, n.º 2, da Constituição garante o sigilo de todos os meios de comunicação, sendo que a legislação apenas permite limitações por razões de interesse público. O artigo 4.º da Lei relativa às atividades de telecomunicações, que proíbe a violação do sigilo das comunicações geridas pelas empresas de telecomunicações, aplica esta exigência de confidencialidade ao nível do direito comum. Esta exigência tem sido interpretada como proibindo a divulgação de informações contidas nas comunicações, exceto com o consentimento dos utilizadores ou quando baseada numa das isenções explícitas de responsabilidade penal nos termos do Código Penal ([77]).

(117) A Constituição garante ainda o direito de acesso aos tribunais (artigo 32.º) e o direito de processar o Estado para obter reparação, no caso de uma pessoa singular ter sofrido danos na sequência de um ato ilegal praticado por um funcionário público (artigo 17.º).

(118) No que se refere, em especial, ao direito à proteção dos dados, o capítulo III, secções 1, 2 e 3, da APPI estabelece os princípios gerais que abrangem todos os setores, incluindo o setor público. Em concreto, o artigo 3.º da APPI prevê que todas as informações pessoais devem ser geridas em conformidade com o princípio do respeito pela personalidade das pessoas singulares. Uma vez recolhidas («obtidas») as informações pessoais pelas autoridades públicas ([78]), incluindo as integradas em registos eletrónicos, a sua gestão rege-se pela Lei relativa à proteção de

([72]) Ver, por exemplo, o acórdão do Supremo Tribunal de 12 de setembro de 2003, processo n.º 1656 [2002 (Ju)]. O Supremo Tribunal considerou, nomeadamente, que «todos os indivíduos têm a liberdade de proteger as suas informações pessoais contra a transmissão a terceiros ou a divulgação pública sem motivo justificado.»

([73]) Supremo Tribunal, acórdão de 6 de março de 2008 (Juki-net).

([74]) Só se verifica «justificação suficiente» quando se considera que a pessoa singular em causa (suspeito, arguido) cometeu uma infração e a busca e apreensão são necessárias para efeitos da investigação criminal. Ver acórdão do Supremo Tribunal de 18 de março de 1969, processo n.º 100 [1968 (Shi)].

([75]) Ver artigo 156.°, n.º 1, das Regras de Processo Penal.

([76]) Deve notar-se, no entanto, que a Lei relativa à repressão do crime organizado e ao controlo dos produtos do crime, de 15 de junho de 2017, estabelece uma nova infração que criminaliza a preparação de atos de terrorismo e algumas outras formas de crime organizado. Só é possível abrir um inquérito no caso de uma suspeita concreta, baseada em provas, de que estão reunidas as três condições necessárias à configuração de uma infração (envolvimento num grupo de crime organizado, «ato de planear» e «ato de preparar a comissão» do crime). Ver também, por exemplo, os artigos 38.º a 40.º da Lei relativa à prevenção de atividades subversivas (Lei n.º 240 de 21 de julho de 1952).

([77]) Artigo 15.º, n.º 8, das Orientações relativas à proteção de informações pessoais no setor de telecomunicações.

([78]) Órgão administrativos na aceção do artigo 2.º, n.º 1, da APPIHAO. De acordo com a informação recebida do Governo japonês, todas as autoridades públicas, com exceção da polícia distrital, são abrangidas pela definição de «órgãos administrativos». Ao mesmo tempo, a polícia distrital funciona no âmbito do enquadramento jurídico estabelecido pelas Portarias distritais relativas à proteção de informações pessoais (ver artigo 11.º da APPI e a «Política de base»), as quais prescrevem disposições para a proteção de informações pessoais equivalentes às da APPIHAO. Ver anexo II, ponto I.B. Tal como explicado pela PPC, em conformidade com a «Política de base», estas portarias devem ser adotadas com base no teor da APPIHAO, devendo o Ministério dos Assuntos Internos e das Comunicações formular comunicações que forneçam as orientações necessárias aos órgãos de poder local. Tal como sublinhado pela PPC, «dentro deste[s] limite[s], devem ser adotadas portarias relativas à proteção de informações pessoais em cada distrito […], assentes na "Política de base" e no teor das comunicações».

informações pessoais na posse de órgãos administrativos («APPIHAO») ([79]). Esta inclui também, em princípio ([80]), o tratamento de informações pessoais para efeitos de aplicação do direito penal ou de segurança nacional. A APPIHAO prevê, entre outras disposições, que as autoridades públicas: i) só podem conservar informações pessoais na medida do necessário à execução das suas funções; ii) não devem utilizar essas informações para uma finalidade «injusta» ou divulgá-las a terceiros sem justificação; (iii) devem especificar a finalidade e não a alterar para além do que pode razoavelmente considerar-se como relevante para a finalidade original (limitação da finalidade); iv) não devem, em princípio, utilizar ou transmitir a terceiros as informações pessoais conservadas e, caso considerem necessário fazê-lo, devem impor limitações à finalidade ou ao método de utilização das informações por terceiros; v) devem esforçar-se por garantir a correção das informações (qualidade dos dados); vi) devem tomar as medidas necessárias à gestão adequada das informações e à prevenção de fuga, perda ou deterioração das mesmas (segurança dos dados); e vii) devem esforçar-se por tratar, de forma correta e expedita, quaisquer reclamações relativas ao tratamento das informações ([81]).

3.2. **Acesso e utilização pelas autoridades públicas japonesas para efeitos de aplicação do direito penal**

(119) A legislação japonesa contém várias limitações ao acesso e utilização de dados pessoais para efeitos de aplicação do direito penal, bem como mecanismos de supervisão e vias de recurso que estabelecem garantias suficientes para a proteção eficaz dos dados contra ingerência ilícita e o risco de abusos.

3.2.1. *Base jurídica e limitações/garantias aplicáveis*

(120) O quadro jurídico japonês autoriza a recolha de informações eletrónicas para efeitos de aplicação do direito penal, com base num mandado (recolha coerciva) ou num pedido de divulgação voluntária.

3.2.1.1. Inquérito coercivo baseado num mandado judicial

(121) Conforme indicado no considerando 115, a recolha de dados no âmbito de um inquérito coercivo deve ser especificamente autorizada por lei e só pode ser efetuada com base num mandado judicial «emitido com justificação suficiente» (artigo 35.º da Constituição). No que se refere à investigação de infrações penais, esta exigência encontra-se consignada nas disposições do Código de Processo Penal («CPP»). Nos termos do artigo 197.º, n.º 1, do CPP, «não serão aplicadas» medidas coercivas «a menos que tenham sido definidas disposições especiais neste código». Relativamente à recolha de informações eletrónicas, as únicas bases jurídicas pertinentes ([82]) nesta matéria são o artigo 218.º (busca e apreensão) e o artigo 222.º, n.º 2, ambos do CPP, segundo os quais as medidas coercivas para a interceção de comunicações eletrónicas sem o consentimento de qualquer uma das partes serão executadas com base noutras leis, nomeadamente, a Lei das Escutas para efeitos de investigação criminal («Lei das Escutas»). Em ambos os casos, aplica-se a exigência de um mandado.

(122) Mais concretamente, nos termos do artigo 218.º, n.º 1, do CPP, o procurador, procurador adjunto ou agente da polícia judiciária pode, se necessário para a investigar a infração, efetuar uma busca ou apreensão (incluindo uma ordem de entrega de registos) mediante mandado previamente emitido por um juiz ([83]). Um tal mandado deve conter, entre outros elementos, o nome do suspeito ou do arguido, a infração que lhe é imputada ([84]), os registos eletromagnéticos a apreender e o «local ou materiais» a inspecionar (artigo 219.º, n.º 1, do CPP).

([79]) As informações pessoais obtidas pelos funcionários de um órgão administrativo, no decurso do exercício das suas competências, e na posse desse órgão administrativo para efeitos de utilização organizativa, são abrangidas pela definição de «informações pessoais conservadas» na aceção do artigo 2.º, n.º 3, da APPIHAO, desde que se encontrem registadas em «documentos administrativos». Estas incluem as informações eletrónicas recolhidas e tratadas posteriormente pelos referidos órgãos, uma vez que a definição de «documentos administrativos» no artigo 2.º, n.º 2, da Lei relativa ao acesso a informações na posse de órgãos administrativos (Lei n.º 42 de 1999) abrange os registos eletromagnéticos.

([80]) No entanto, nos termos do artigo 53.º, n.º 2, do Código de Processo Penal, o capítulo IV da APPIHAO encontra-se excluído, no caso de «documentos relacionados com processos jurídicos», os quais, segundo a informação recebida, incluem informações eletrónicas baseadas em mandados ou pedidos de cooperação voluntária no âmbito de uma investigação criminal. De igual modo, no que se refere às informações recolhidas no domínio da segurança nacional, as pessoas singulares não podem fazer valer os seus direitos de forma eficaz, ao abrigo da APPIHAO, se o dirigente da autoridade pública tiver «motivos razoáveis» para considerar que essa divulgação «é suscetível de prejudicar a segurança nacional» [ver artigo 14,º. subalínea iv)]. No entanto, as autoridades públicas são obrigadas a permitir a divulgação, pelo menos parcial, sempre que possível (artigo 15.º).

([81]) Ver as referências específicas à APPIHAO no anexo II, ponto II.A.1, (b)(2).

([82]) Embora o artigo 220.º do CPP autorize uma busca e apreensão «de imediato», sem um mandado, caso um procurador, um procurador adjunto ou um agente da polícia judiciária detenha um suspeito/infrator em flagrante, tal não se aplica num contexto de transferência e, portanto, para efeitos da presente decisão.

([83]) Em conformidade com o artigo 222.º, n.º 1, em conjugação com o artigo 110.º, do CPP, o mandado de busca/apreensão de registos deve ser apresentado à pessoa a quem é imposta a medida.

([84]) Ver igualmente o artigo 189.º, n.º 2, do CPP, nos termos do qual um agente da polícia judiciária deve investigar o infrator e as provas da infração «quando considere que foi cometida uma infração.» De igual modo, o artigo 155.º, n.º 1, das Regras de Processo Penal exige que um pedido escrito de mandado contenha, entre outros elementos, a «infração imputada» e um «resumo dos factos do crime».

(123) No que se refere à interceção de comunicações, o artigo 3.º da Lei das Escutas apenas autoriza tais medidas em condições muito específicas. Em particular, as autoridades públicas devem obter previamente um mandado judicial que só pode ser emitido para a investigação de crimes graves específicos (enumerados no anexo da lei) ([85]) e no caso de ser «extremamente difícil identificar o criminoso ou esclarecer, por outros meios, as circunstâncias/pormenores do crime» ([86]). Nos termos do artigo 5.º da Lei das Escutas, o mandado é emitido por um período de tempo limitado e o juiz pode impor condições adicionais. A Lei das Escutas prevê, além disso, uma série de outras garantias, nomeadamente a presença obrigatória de testemunhas (artigos 12.º e 20.º), a proibição de realizar escutas aos membros de certos grupos que têm acesso a informações confidenciais (por exemplo, médicos e advogados) (artigo 15.º), a obrigação de pôr termo a escutas que já não se justifiquem embora o mandato ainda seja válido (artigo 18.º) ou a obrigação geral de informar a pessoa escutada e de lhe facultar acesso às gravações no prazo de trinta dias a contar da data de termo da escuta (artigos 23.º e 24.º).

(124) No que se refere a quaisquer medidas coercivas baseadas num mandado, este tipo de averiguação só pode ser conduzida «na medida do necessário para atingir o seu objetivo», ou seja, se os objetivos da investigação não puderem ser atingidos de outro modo (artigo 197.º, n.º 1, do CPP). Se bem que os critérios para determinar a necessidade não sejam especificados em mais pormenor no direito comum, o Supremo Tribunal do Japão decidiu que o juiz que emite um mandado deve proceder a uma avaliação geral tendo particularmente em conta i) a gravidade da infração e a forma como foi cometida; ii) o valor e a importância dos materiais a apreender como elementos de prova; iii) a probabilidade (risco) de esses elementos de prova serem ocultados ou destruídos; e iv) a medida em que a apreensão pode prejudicar a pessoa afetada ([87]).

3.2.1.2. Pedido de divulgação voluntária com base numa «ficha de inquérito»

(125) Nos limites da sua competência, as autoridades públicas podem também recolher informações eletrónicas com base em pedidos de divulgação voluntária. Trata-se de uma forma não coerciva de cooperação em que a satisfação do pedido não pode ser imposta ([88]), dispensando assim as autoridades públicas do dever de obter um mandado judicial.

(126) Se o pedido se dirigir a um operador comercial e se referir a informações pessoais, o operador comercial é obrigado a cumprir as exigências da APPI. Nos termos do artigo 23.º, n.º 1, da APPI, os operadores comerciais só podem divulgar informações pessoais a terceiros sem o consentimento da pessoa singular em causa em casos determinados, incluindo quando a divulgação «se fundamente em leis e regulamentos» ([89]). No domínio da aplicação do direito penal, a base jurídica para tais pedidos está prevista no artigo 197.º, n.º 2, do CPP, nos termos do qual «pode ser solicitado às organizações privadas que transmitam informações necessárias relacionadas com a investigação.» Uma vez que só é permitida no âmbito de uma investigação criminal, uma «ficha de inquérito» pressupõe uma suspeita concreta de um crime já cometido ([90]). Além disso, dado que tais investigações são geralmente conduzidas pela polícia distrital, aplicam-se as limitações definidas no artigo 2.º, n.º 2, da Lei da Polícia ([91]). Nos termos desta disposição, as atividades da polícia estão «estritamente limitadas» ao cumprimento das suas responsabilidades e deveres (ou seja, a prevenção, a repressão e a investigação de crimes). Por outro lado, no exercício das suas funções, a polícia deve atuar de modo imparcial, justo e sem preconceito, não podendo, em circunstância alguma, abusar dos seus poderes «de uma forma que interfira nos direitos e liberdades de uma pessoa singular garantidos na Constituição do Japão» (que incluem, como indicado, o direito à privacidade e à proteção dos dados) ([92]).

(127) No que se refere especificamente ao artigo 197.º, n.º 2, do CPP, a Agência Nacional de Polícia («NPA»), enquanto autoridade federal responsável, entre outros, por todos os assuntos relativos à polícia judiciária, emitiu instruções à

([85]) O anexo refere-se a 9 tipos de crime, designadamente, crimes relacionados com estupefacientes e armas, tráfico de seres humanos e homicídio organizado. Deve notar-se que a infração recentemente introduzida da «preparação de atos de terrorismo e outros crimes organizados» (ver a nota de rodapé 76) não faz parte desta lista restritiva.

([86]) Por outro lado, nos termos do artigo 23.º da Lei das Escutas, a autoridade de investigação deve notificar por escrito deste facto a pessoa cujas comunicações tenham sido intercetadas (e, por conseguinte, incluídas no registo da intercetação).

([87]) Ver anexo II, ponto II.A.1 (b)(1).

([88]) De acordo com a informação recebida, não há nenhuma lei que determine consequências negativas (incluindo sanções) para os operadores comerciais que não cooperem. Ver anexo II, ponto II.A.2 (a).

([89]) De acordo com as orientações da PPC (edição sobre as normas gerais), o artigo 23,º, n.º 1, subalínea i) estabelece a base para a divulgação de informações pessoais em resposta a um mandado (artigo 218.º do CPP) e a uma «ficha de inquérito» (artigo 197.º, n.º 2, do CPP).

([90]) Isto significa que a «ficha de inquérito» só pode ser utilizada para recolher informações sobre casos concretos e não para proceder à recolha de dados pessoais em grande escala. Ver igualmente anexo II, ponto I.A.2 (b)(1).

([91]) Bem como os regulamentos da Comissão Distrital para a Segurança Pública, ver artigo 189.º, n.º 1, do CPP.

([92]) Ver também o artigo 3.º da Lei da Polícia, nos termos do qual o juramento profissional prestado por todos os agentes da polícia deve «ser fiel à obrigação de fazer valer e defender a Constituição e as leis do Japão, assim como de executar as suas funções com imparcialidade, equidade, justiça e sem preconceito.»

polícia distrital ([93]) sobre a «utilização correta de inquéritos escritos em processos de investigação». Nos termos desta notificação, os pedidos devem ser apresentados através do formulário pré-estabelecido («formulário n.º 49» ou a denominada «ficha de inquérito») ([94]), bem como dizer respeito a registos «relativos a uma investigação específica», e as informações solicitadas devem ser «necessárias para [essa] investigação». Em cada caso, o investigador-chefe deve «examinar exaustivamente a necessidade, conteúdo, etc. [do] inquérito concreto» e obter a aprovação interna de um funcionário superior.

(128) Além disso, em dois acórdãos de 1969 e 2008 ([95]), o Supremo Tribunal do Japão estipulou limitações quanto a medidas não coercivas que interferem no direito à privacidade ([96]). Em particular, o tribunal considerou que tais medidas deviam ser «razoáveis» e cingir-se aos «limites geralmente admissíveis», ou seja, deviam ser necessárias para a investigação de um suspeito (recolha de elementos de prova) e aplicadas «por métodos adequados ao cumprimento da finalidade [da] investigação.» ([97]) Os acórdãos revelam que tal pressupõe um teste de proporcionalidade que considera todas as circunstâncias do caso (designadamente, o grau de ingerência no direito à privacidade, incluindo a expectativa de privacidade, a gravidade do crime, a probabilidade de obter elementos de prova úteis, a importância desses elementos, eventuais meios alternativos de investigação, etc.) ([98]).

(129) Além destas limitações ao exercício da autoridade pública, espera-se que os próprios operadores comerciais verifiquem («confirmem») a necessidade e a «racionalidade» da transmissão a terceiros ([99]). Coloca-se também aqui a questão de saber se estão legalmente impedidos de cooperar. Estas obrigações legais contraditórias podem resultar, nomeadamente, de deveres de confidencialidade, decorrentes por exemplo do artigo 134.º do Código Penal (respeitante à relação entre um médico, um advogado, um sacerdote, etc. e um cliente). De igual modo, «qualquer pessoa que exerça atividade no setor das telecomunicações deve, enquanto em funções, preservar as informações confidenciais de terceiros de que tenha tomado conhecimento no âmbito de comunicações geridas pela empresa de telecomunicações» (artigo 4.º, n.º 2, da Lei relativa às atividades de telecomunicações). Esta obrigação é acompanhada pela sanção estabelecida no artigo 179.º da Lei relativa às atividades de telecomunicações, nos termos do qual qualquer pessoa que viole o sigilo das comunicações geridas por uma empresa de telecomunicações será dada como culpada de uma infração penal e punida com uma pena de prisão com possibilidade de prestação de trabalho até dois anos ou com multa até um milhão de ienes ([100]). Embora esta exigência não seja absoluta e permita que sejam adotadas medidas em violação do sigilo das comunicações, que constituam «atos justificáveis» na aceção do artigo 35.º do Código Penal ([101]), esta derrogação não abrange a resposta a pedidos não coercivos por parte das autoridades públicas quanto à divulgação de informações eletrónicas nos termos do artigo 197.º, n.º 2, do CPP.

3.2.1.3. Utilização adicional das informações recolhidas

(130) Após a respetiva recolha pelas autoridades públicas japonesas, as informações pessoais são abrangidas pelo âmbito de aplicação da APPIHAO. Esta lei regulamenta a gestão (tratamento) das «informações pessoais conservadas» e,

([93]) Nos termos do artigo 30.º, n.º 1, e do artigo 31.º, n.º 2, da Lei da Polícia, o diretor-geral dos serviços da polícia regional (delegações da Agência Nacional de Polícia) deve «supervisionar e instruir» a polícia distrital.

([94]) A ficha de inquérito deve também especificar os dados de contacto do «responsável» («nome da secção [cargo], nome do responsável, número de telefone profissional, número da extensão, etc.»).

([95]) Supremo Tribunal, acórdão de 24 de dezembro de 1969 (1965(A) 1187); acórdão de 15 de abril de 2008 (2007(A) 839).

([96]) Embora estes acórdãos não digam respeito à recolha de informações em formato eletrónico, o Governo japonês esclareceu que a aplicação dos critérios definidos pelo Supremo Tribunal são extensíveis a qualquer ingerência das autoridades públicas no direito à privacidade, nomeadamente a «todas as investigações voluntárias». Os referidos critérios, por conseguinte, vinculam as autoridades japonesas quando solicitam a divulgação voluntária de informações. Ver anexo II, ponto II.A.2 (b)(1).

([97]) De acordo com a informação recebida, estes fatores devem ser considerados «razoáveis em conformidade com as convenções socialmente aceites.» Ver anexo II, ponto II.A.2 (b)(1).

([98]) Para considerações semelhantes no quadro das investigações coercivas (escutas telefónicas), ver igualmente o acórdão do Supremo Tribunal de 16 de dezembro de 1999, 1997 (A) 636.

([99]) Nesta matéria, as autoridades japonesas salientaram as orientações da PPC (edição sobre as normas gerais) e o ponto 5/14 das «P&R» preparadas pela PPC para a aplicação da APPI. De acordo com as autoridades japonesas, «perante a consciencialização crescente entre as pessoas singulares a respeito dos seus direitos de privacidade, juntamente com a carga de trabalho decorrente destes pedidos, os operadores comerciais são cada vez mais cautelosos nas suas respostas aos mesmos». Ver o anexo II, ponto II.A.2), também com referência à notificação de 1999 da Agência Nacional de Polícia. De acordo com a informação recebida, houve efetivamente casos em que os operadores comerciais se recusaram a cooperar. Por exemplo, no seu relatório de 2017 sobre transparência, a LINE (a aplicação de mensagens mais popular do Japão) refere o seguinte: «Após recebermos um pedido de organismos de investigação, etc., […] verificamos a respetiva adequação dos pontos de vista da legalidade, da proteção dos utilizadores, etc. Se a nossa verificação apurar qualquer lacuna jurídica, o pedido é indeferido. Se o âmbito da reclamação for demasiado lato para efeitos de investigação, solicitamos ao organismo de investigação que preste esclarecimentos. Se esses esclarecimentos se revelarem injustificados, não respondemos ao pedido.» Disponível na internet em: https://linecorp.com/en/security/transparency/top

([100]) As sanções consistem em três anos de prisão com possibilidade de prestação de trabalho ou em multa até 2 milhões de ienes no caso de pessoas que «exercem atividade no setor das telecomunicações».

([101]) «Atos justificáveis», na aceção do Código Penal, são, nomeadamente, os atos de uma empresa de telecomunicações pelos quais esta cumpre medidas impostas pelo Estado com força de lei (medidas coercivas), designadamente quando as autoridades de investigação tomam medidas com base num mandado emitido por um juiz. Ver o anexo II, ponto II.A.2 (b)(2), com referência às orientações sobre proteção das informações pessoais na atividade de telecomunicações.

nesta medida, impõe um conjunto de limitações e garantias (ver o considerando 118) ([102]). Por outro lado, o facto de um órgão administrativo poder conservar informações pessoais «apenas quando a conservação é necessária para a condução dos assuntos sob a sua jurisdição previstos nas leis e nos regulamentos» (artigo 3.º, n.º 1, da APPIHAO) também impõe restrições, pelo menos indiretamente, à recolha inicial.

3.2.2. *Supervisão independente*

(131) No Japão, a recolha de informações eletrónicas no domínio da aplicação do direito penal incumbe sobretudo ([103]) à polícia distrital ([104]), que está sujeita, nesta matéria, a vários níveis de supervisão.

(132) Em primeiro lugar, em todos os casos em que são recolhidas informações eletrónicas por meios coercivos (busca e apreensão), a polícia tem de obter previamente um mandado judicial (ver o considerando 121). Em tais casos, a recolha será, por conseguinte, verificada previamente por um juiz, com base numa norma rigorosa de «justificação suficiente».

(133) Embora não exista qualquer verificação prévia por um juiz no caso de pedidos de divulgação voluntária, os operadores comerciais a quem se dirigem podem opor-se aos mesmos sem arriscar sofrer consequências negativas (devendo tomar em consideração o impacto na privacidade de tal divulgação). Além disso, nos termos do artigo 192.º, n.º 1, do CPP, os agentes da polícia devem sempre cooperar e coordenar as suas ações com a procuradoria (e a Comissão Distrital para a Segurança Pública) ([105]). Por seu lado, a procuradoria pode emitir as instruções gerais necessárias, em que estabelece normas para uma investigação justa, e/ou emitir ordens específicas relativas a uma investigação concreta (artigo 193.º do CPP). Caso essas instruções e/ou ordens não sejam acatadas, pode abrir um processo tendo em vista uma ação disciplinar (artigo 194.º do CPP). Como tal, a polícia distrital funciona sob a supervisão da procuradoria.

(134) Em segundo lugar, nos termos do artigo 62.º da Constituição, ambas as câmaras do Parlamento japonês (a Dieta) podem conduzir investigações relativas ao Governo, incluindo sobre a licitude da recolha de informações pela polícia. Para o efeito, podem exigir a presença e o depoimento de testemunhas e/ou a entrega de registos. Tais poderes de investigação encontram-se especificados em mais pormenor na Lei da Dieta, em particular, no capítulo XII. Mais concretamente, o artigo 104.º da Lei da Dieta estabelece que o Conselho de Ministros, os organismos públicos e outras instâncias governamentais «devem satisfazer os pedidos de uma Câmara ou de qualquer uma das suas comissões para que apresentem relatórios e registos necessários para apreciação no âmbito da investigação.» A recusa em satisfazer tais pedidos só é permitida se o Governo apresentar um motivo plausível, que a Dieta considere aceitável, ou mediante a emissão de uma declaração formal de que a divulgação dos relatórios ou registos seria «gravemente prejudicial para o interesse nacional» ([106]). Além disso, os membros da Dieta podem formular perguntas por escrito ao Conselho de Ministros (artigos 74.º e 75.º da Lei da Dieta), sendo que, no passado, estas «perguntas escritas» também abordaram a gestão de informações pessoais pela administração ([107]). O papel de supervisão do executivo por parte da Dieta é acompanhado de obrigações de comunicação de informações, nomeadamente nos termos do artigo 29.º da Lei das Escutas.

(135) Em terceiro lugar, ainda no âmbito do poder executivo, a polícia distrital está sujeita a supervisão independente. Esta refere-se, em particular, às Comissões Distritais para a Segurança Pública, criadas a nível distrital, a fim de assegurar a administração democrática e a neutralidade política da polícia ([108]). Estas comissões são constituídas por membros designados pelo Governador Distrital, mediante a aprovação da Assembleia Distrital (de entre cidadãos sem atividade, nos cinco anos anteriores, como funcionários públicos na polícia), os quais só podem ser destituídos com justa causa ([109]). Segundo a informação recebida, não estão sujeitas a instruções, podendo assim ser consideradas plenamente independentes ([110]). No que se refere às competências e poderes das Comissões Distritais para a

([102]) Ver a secção 3.1. relativamente aos direitos das pessoas singulares em causa.
([103]) Em princípio, um procurador ou um procurador adjunto sob a tutela do mesmo pode, se assim o entender, investigar uma infração (artigo 191.º, n.º 1, do CPP).
([104]) Segundo a informação recebida, a Agência Nacional de Polícia não conduz investigações criminais individualizadas. Ver anexo II, ponto II.A.1 (a).
([105]) Ver igualmente o artigo 246.º do CPP, nos termos do qual a polícia judiciária tem a obrigação de transmitir o processo à procuradoria, uma vez conduzida a investigação de uma infração penal («Princípio de transmissão em todos os casos»).
([106]) Alternativamente, a Dieta pode solicitar que o Conselho de Supervisão e Análise de Segredos Especialmente Designados conduza um inquérito sobre a recusa em responder. Ver o artigo 104.º-II da Lei da Dieta.
([107]) Ver anexo II, ponto II.B.4.
([108]) Além disso, nos termos do artigo 100.º da Lei da Autonomia Local, as assembleias locais podem investigar as atividades das autoridades com poderes coercivos a nível distrital, incluindo a polícia distrital.
([109]) Ver artigos 39.º a 41.º da Lei da Polícia. No que se refere à neutralidade política, ver também o artigo 42.º da Lei da Polícia.
([110]) Ver anexo II, ponto II.B.3 («sistema de independência do conselho»).

Segurança Pública, nos termos do artigo 38.º, n.º 3, conjugado com os artigos 2.º e 36.º, n.º 2, da Lei da Polícia, estas são responsáveis pela «proteção dos direitos e liberdades das pessoas singulares». Para o efeito, têm competência para «supervisionar» ([111]) todas as atividades de investigação da polícia distrital, incluindo a recolha de dados pessoais. Compete-lhes, nomeadamente, «instruir, se for caso disso, a polícia distrital, em pormenor ou em relação a casos concretos sob investigação quanto a faltas graves cometidas por agentes da polícia.» ([112]) Se o chefe da polícia distrital ([113]) receber uma instrução desse tipo ou tomar conhecimento da suspeita de uma falta grave por parte do pessoal (incluindo a violação de leis ou a negligência no cumprimento do dever), é obrigado a investigar imediatamente a ocorrência e a comunicar o resultado dessa investigação à Comissão Distrital para a Segurança Pública (artigo 56.º, n.º 3, da Lei da Polícia). Se a comissão considerar necessário, pode igualmente incumbir um dos seus membros de apreciar a evolução da implementação. O processo continua até que a Comissão Distrital para a Segurança Pública considere que o incidente foi devidamente resolvido.

(136) Além disso, no que se refere à aplicação correta da APPIHAO, o ministro ou o diretor de serviços competente (por exemplo, o comissário-geral da Agência Nacional de Polícia) dispõe de poderes de execução coerciva, subordinados à supervisão do Ministério dos Assuntos Internos e das Comunicações. Nos termos do artigo 49.º da APPIHAO, o Ministério dos Assuntos Internos e das Comunicações «pode recolher relatórios sobre a evolução da aplicação desta lei» junto dos responsáveis pelos órgãos administrativos (ministro). Esta função de supervisão é apoiada por contributos dos 51 «centros de informações globais» do Ministério dos Assuntos Internos e das Comunicações (um em cada distrito do Japão), os quais procedem anualmente o tratamento de milhares de consultas de pessoas singulares ([114]) (as quais podem, por sua vez, revelar eventuais violações da lei). Sempre que o entenda necessário para garantir o cumprimento da lei, o referido ministério pode solicitar a apresentação de explicações e materiais, bem como emitir pareceres, relativamente à gestão de informações pessoais pelo órgão administrativo em causa (artigos 50.º e 51.º da APPIHAO).

3.2.3. *Recurso individual*

(137) Além da supervisão *ex officio*, as pessoas singulares dispõem igualmente de várias possibilidades de obter reparação individual, tanto através de autoridades independentes (como as Comissões Distritais para a Segurança Pública ou a PPC) como dos tribunais japoneses.

(138) Em primeiro lugar, relativamente a informações pessoais recolhidas pelos órgãos administrativos, estes são obrigados a «esforçar-se por tratar, de forma correta e expedita, quaisquer reclamações» relativas ao seu tratamento subsequente (artigo 48.º da APPIHAO). Embora o capítulo IV da APPIHAO sobre direitos individuais não se aplique no caso de informações pessoais registadas em «documentos relacionados com processos jurídicos e com materiais apreendidos» (artigo 53.º-2, n.º 2, do CPP), que abranjam informações pessoais recolhidas no âmbito de investigações criminais, as pessoas singulares podem apresentar uma reclamação com base nos princípios gerais de proteção de dados, como por exemplo a obrigação de apenas conservar informações pessoais «quando a conservação seja necessária para [aplicar coercivamente a lei]» (artigo 3.º, n.º 1, da APPIHAO).

(139) Além disso, o artigo 79.º da Lei da Polícia garante às pessoas singulares, que tenham preocupações quanto ao respeito pela «execução do dever» pelo pessoal da polícia, o direito de apresentar uma reclamação junto da (competente) Comissão Distrital para a Segurança Pública independente. A Comissão procede «fidedignamente» ao tratamento destas reclamações em conformidade com as leis e as portarias locais e notifica o reclamante por escrito dos resultados. Com base na sua competência para supervisionar e «instruir» a polícia distrital relativamente a uma «falta grave por parte do pessoal» (artigos 38.º, n.º 3, e 43.º-2, n.º 1) da Lei da Polícia), pode solicitar à polícia distrital que investigue os factos, tome medidas adequadas, com base no resultado da investigação, e comunique os resultados. Se entender que a investigação conduzida pela polícia não foi adequada, a Comissão pode também emitir instruções sobre o tratamento a dar à reclamação.

(140) A fim de facilitar o tratamento das reclamações, a Agência Nacional de Polícia emitiu uma «comunicação» à polícia e às Comissões Distritais para a Segurança Pública sobre o tratamento correto das reclamações relativas à execução

([111]) Ver artigos 5.º, n.º 3, e 38.º, n.º 3, da Lei da Polícia.

([112]) Ver artigos 38.º, n.º 3, e 43.º-2, n.º 1, da Lei da Polícia. Caso «emita uma instrução, na aceção do artigo 43.º-2, n.º 1), a Comissão Distrital para a Segurança Pública pode instruir uma comissão por si designada para acompanhar a sua implementação (n.º 2). Por outro lado, a Comissão pode recomendar ação disciplinar ou a destituição do chefe da polícia distrital (artigo 50.º, n.º 2), assim como de outros agentes da polícia (artigo 55.º, n.º 4, da Lei da Polícia).

([113]) O mesmo se aplica ao superintendente geral no caso da polícia metropolitana de Tóquio (ver artigo 48.º, n.º 1, da Lei da Polícia).

([114]) Segundo a informação recebida, no exercício financeiro de 2017 (abril de 2017 a março de 2018), foi tratado um total de 5 186 consultas de pessoas singulares pelos «centros de informações globais».

do dever pelos agentes da polícia. Neste documento, a Agência Nacional de Polícia define normas para a interpretação e aplicação do artigo 79.º da Lei da Polícia. Entre outras exigências, requer que a polícia distrital estabeleça um «sistema de tratamento de reclamações» e que trate e comunique «imediatamente» todas as reclamações à Comissão Distrital para a Segurança Pública competente. A referida comunicação define reclamação como o pedido de correção «de uma desvantagem concreta sofrida como resultado de um comportamento ilegal ou inadequado» ([115]) ou «a falta de adoção das medidas necessárias por um agente da polícia no exercício de funções» ([116]), bem como «a insatisfação/descontentamento com a forma inadequada como um agente da polícia exerceu as respetivas funções». Deste modo, o âmbito material da reclamação é definido de uma forma lata, abrangendo todos os pedidos ilegais de recolha de dados, e dispensando o autor da mesma de demonstrar a existência de danos sofridos em resultado da intervenção do agente da polícia. Mais importante ainda, essa comunicação estipula que os estrangeiros (entre outros) deverão receber assistência na formulação das reclamações. Na sequência de uma reclamação, as Comissões Distritais para a Segurança Pública devem assegurar que a polícia distrital analisa os factos, adota medidas «em conformidade com o resultado da análise» e comunica os resultados. Sempre que considere que a análise foi insuficiente, a Comissão emite uma instrução sobre o tratamento da reclamação, que a polícia distrital é obrigada a seguir. Tendo em conta os relatórios recebidos e as medidas adotadas, a Comissão notifica a pessoa singular indicando, nomeadamente, as medidas tomadas para atender a reclamação. A comunicação da Agência Nacional de Polícia salienta que as reclamações devem ser tratadas «com a devida atenção» e que o resultado deve ser comunicado «dentro do prazo […] considerado adequado à luz das normas sociais e do senso comum.»

(141) Em segundo lugar, uma vez que qualquer recurso terá lugar, naturalmente, num sistema e numa língua estrangeiros, a fim de facilitar a obtenção de reparação por pessoas singulares da UE, cujos dados tenham sido transferidos para operadores comerciais no Japão e subsequentemente utilizados por autoridades públicas, o Governo japonês criou, no âmbito das suas competências, um mecanismo específico, administrado e supervisionado pela PPC, para tratar e resolver as reclamações neste domínio. Este mecanismo assenta no dever de cooperação, que a APPI impõe às autoridades públicas japonesas, e no papel especial da PPC relativamente às transferências internacionais de dados de países terceiros, nos termos do artigo 6.º da APPI e da «Política de Base» (tal como definida pelo Governo japonês por decreto ministerial). Os pormenores deste mecanismo figuram nas declarações, garantias e compromissos oficiais recebidos do Governo japonês e que constam do anexo II da presente decisão. O mecanismo não está sujeito a quaisquer requisitos em matéria de legitimidade, podendo ser utilizado por qualquer pessoa singular, independentemente de ser ou não suspeita ou acusada da prática de um crime.

(142) Nos termos do mecanismo, uma pessoa que suspeite que os seus dados transferidos da União Europeia foram recolhidos ou utilizados pelas autoridades públicas no Japão (incluindo as responsáveis pela aplicação do direito penal), em violação das normas aplicáveis, pode apresentar uma reclamação à PPC (individualmente ou através da respetiva autoridade responsável pela proteção de dados, na aceção do artigo 51.º do RGPD). A PPC tem a obrigação de tratar a reclamação e de, numa primeira fase, informar as autoridades públicas competentes sobre a mesma, incluindo os organismos de controlo pertinentes. Estas autoridades são obrigadas a cooperar com a PPC, «incluindo através da disponibilização das informações necessárias e do material relevante, para que esta possa avaliar se a recolha ou a utilização subsequente das informações pessoais respeitou as normas em vigor» ([117]). Esta obrigação, resultante do artigo 80.º da APPI (que exige às autoridades públicas japonesas que cooperem com a PPC), é de aplicação geral, abrangendo assim a análise de todas as medidas de investigação adotadas pelas referidas autoridades. Estas encontram-se, aliás, obrigadas a prestar essa cooperação por força das garantias prestadas por escrito pelos ministérios e pelos diretores de serviços competentes, como consta do anexo II.

(143) Se a avaliação indicar que ocorreu uma violação das normas em vigor, a «cooperação das autoridades públicas em causa com a PPC inclui a obrigação de pôr termo à violação», o que, no caso da recolha ilícita de informações pessoais, implica o apagamento dos dados. Mais importante ainda, esta obrigação é cumprida sob a supervisão da PPC, que «confirmará, antes de concluir a avaliação, que foi posto termo à violação.»

(144) Uma vez concluída a avaliação, a PPC deve notificar a pessoa singular do resultado da mesma, dentro de um prazo razoável, incluindo, das eventuais medidas corretivas adotadas. Ao mesmo tempo, a PPC deve informar igualmente a pessoa singular sobre a possibilidade de obter confirmação do resultado junto da autoridade pública competente e sobre a identidade da autoridade a quem esse pedido de confirmação deve ser dirigido. A possibilidade de receber

([115]) A condição de que exista uma «desvantagem concreta» exige apenas que o reclamante tenha sido individualmente afetado pela conduta (ou inação) da polícia, não tendo de demonstrar que ocorreu algum dano.

([116]) A observância da lei, nomeadamente dos requisitos legais para a recolha e utilização de dados pessoais, faz parte dessas incumbências. Ver o artigo 2.º, n.º 2, e o artigo 3.º da Lei da Polícia.

([117]) Ao proceder a essa avaliação, a PPC coopera com o Ministério dos Assuntos Internos e das Comunicações, que, como se refere no considerando 136, pode solicitar a apresentação de explicações e materiais, bem como emitir pareceres, relativamente à gestão de informações pessoais pelo órgão administrativo relevante (artigos 50.º e 51.º da APPIHAO).

esta confirmação, incluindo as razões subjacentes à decisão da autoridade competente, podem ser úteis para a tomada de medidas adicionais pela pessoa em causa, inclusive para efeitos da interposição de um recurso judicial. As informações pormenorizadas sobre o resultado da avaliação podem ser limitadas, desde que existam motivos razoáveis para considerar que a comunicação das mesmas é suscetível de comportar um risco para a investigação em curso.

(145) Em terceiro lugar, uma pessoa que discorde de uma decisão judicial de apreensão (mandado) ([118]) dos respetivos dados pessoais ou das medidas tomadas pela polícia ou pela procuradoria para executar essa decisão, pode apresentar um pedido para que a decisão ou as medidas em causa sejam revogadas ou alteradas (artigos 429.º, n.º 1, e 430.º, n.os 1 e 2, do CPP e artigo 26.º da Lei das Escutas) ([119]). Caso o tribunal de recurso considere o mandado ou a respetiva execução («procedimento de apreensão») como sendo ilegal, considera o pedido procedente e ordena a devolução dos materiais apreendidos ([120]).

(146) Em quarto lugar, como uma forma mais indireta de controlo judicial, qualquer pessoa singular que considere ilícita a recolha das suas informações pessoais no âmbito de uma investigação criminal, pode invocar essa ilicitude em sede de julgamento penal. Se o tribunal concordar, as provas serão consideradas inadmissíveis e serão excluídas.

(147) Por último, nos termos do artigo 1.º, n.º 1, da Lei relativa a recurso contra o Estado, um tribunal pode determinar o pagamento de indemnização, no caso de um funcionário público, que exerça a autoridade pública do Estado, ter causado, no exercício das suas funções, danos à pessoa singular em causa, ilegalmente e com culpa (de forma intencional ou negligente). Nos termos do artigo 4.º da Lei relativa a recurso contra o Estado, a responsabilidade do Estado por danos baseia-se nas disposições do Código Civil. Nesta matéria, o artigo 710.º do Código Civil determina que a responsabilidade não abrange unicamente os danos materiais, cobrindo igualmente os danos morais (designadamente, sob a forma de «angústia mental»). Tal inclui casos em que a privacidade de uma pessoa tenha sido violada através de vigilância ilícita e/ou da recolha das suas informações pessoais (por exemplo, a execução ilegal de um mandado) ([121]).

(148) Além de compensação monetária, as pessoas singulares podem também, sob certas condições, obter uma medida inibitória (designadamente, o apagamento dos dados pessoais recolhidos pelas autoridades públicas), com base nos seus direitos de privacidade consagrados no artigo 13.º da Constituição ([122]).

(149) No que se refere a todas estas vias de recurso, o mecanismo de resolução de litígios criado pelo Governo japonês prevê que uma pessoa singular, que esteja insatisfeita com o resultado do processo, possa interpelar a PPC, «a qual informará a pessoa sobre as diversas possibilidades e os procedimentos circunstanciados para obter reparação proporcionados pelas leis e regulamentos japoneses.» Por outro lado, a PPC «prestará apoio à pessoa singular, incluindo aconselhamento e assistência na tomada de outras medidas junto do órgão administrativo ou judicial relevante.»

(150) Estas incluem o exercício dos direitos processuais ao abrigo do Código de Processo Penal. Por exemplo, «[c]aso a avaliação revele que determinada pessoa singular é suspeita num processo penal, a PPC informa essa pessoa do facto» ([123]), bem como da possibilidade conferida pelo artigo 259.º do CPP de solicitar à procuradoria que a notifique se decidir não instaurar uma ação penal. De igual modo, se a avaliação revelar que foi iniciado um processo relacionado com as informações pessoais da pessoa singular e que o mesmo foi arquivado, a PPC informa a pessoa de que pode, nos termos do artigo 53.º do CPP (e do artigo 4.º da Lei relativa aos autos finais dos processos penais), consultar os autos do processo. A obtenção de acesso pela pessoa singular aos autos do seu

([118]) Tal inclui um mandado de autorização da escuta, caso em que a Lei das Escutas determina um requisito específico de notificação (artigo 23.º). Nos termos desta disposição, a autoridade de investigação deve notificar por escrito deste facto as pessoas cujas comunicações tenham sido intercetadas (e, por conseguinte, incluídas no registo da intercetação). Um outro exemplo é o artigo 100.º, n.º 3, do CPP, nos termos do qual o tribunal, depois de apreender objetos postais ou telegramas enviados ao arguido ou por este, deve notificar o remetente ou o destinatário, a menos que haja o risco que essa notificação possa obstruir um processo judicial. O artigo 222.º, n.º 1, do CPP faz referência a esta disposição sobre buscas e apreensões levadas a cabo por uma autoridade de investigação.

([119]) Se bem que tal pedido não tenha o efeito automático de suspender a execução da decisão de apreensão, o tribunal de recurso pode ordenar a suspensão até proferir uma decisão quanto ao mérito. Ver artigos 429.º, n.º 2, e 432.º, em conjugação com o artigo 424.º do CPP.

([120]) Ver anexo II, ponto II.C(1).

([121]) Ver anexo II, ponto II.C.2.

([122]) Ver, nomeadamente, o acórdão do Tribunal Distrital de Tóquio de 24 de março de 1988 (n.º 2925); Tribunal Distrital de Osaca, acórdão de 26 de abril de 2007 (n.º 2925). De acordo com o Tribunal Distrital de Osaca, deve ser encontrado um equilíbrio entre vários fatores, como por exemplo: i) a natureza e conteúdo das informações pessoais em causa; ii) a forma como foram recolhidas; iii) as desvantagens para a pessoa singular, caso as informações não sejam apagadas; e iv) o interesse público, incluindo as desvantagens para a autoridade pública, caso as informações sejam apagadas.

([123]) Em qualquer caso, após o início do processo penal, o arguido deve ter a possibilidade de inspecionar esses elementos de prova (ver artigos 298.º a 299.º do CCP). No que se refere às vítimas de um crime, ver artigos 316.º a 333.º do CPP.

processo é importante, na medida em que a ajuda a melhor compreender a investigação conduzida contra si e a preparar, deste modo, uma eventual ação judicial (nomeadamente o pedido de indemnização), caso considere que os seus dados foram ilicitamente recolhidos ou utilizados.

3.3. **Acesso e utilização pelas autoridades públicas japonesas para efeitos de segurança nacional**

(151) Segundo as autoridades japonesas, nenhuma lei nacional permite formular um pedido coercivo de informações ou «escutas administrativas» fora do âmbito das investigações criminais. Por conseguinte, por razões de segurança nacional, as informações só podem ser obtidas junto de uma fonte de informação a que qualquer pessoa tenha livre acesso ou através de divulgação voluntária. Os operadores comerciais que recebam um pedido de cooperação voluntária (sob a forma de divulgação de informações eletrónicas) não têm qualquer obrigação jurídica de prestar essas informações ([124]).

(152) Por outro lado, segundo as informações recebidas, só quatro entidades governamentais têm competência para recolher informações eletrónicas na posse de operadores comerciais japoneses, por razões de segurança nacional, nomeadamente: i) o Serviço de Informações e Investigação do Governo (CIRO); ii) o Ministério da Defesa; iii) a polícia (tanto a Agência Nacional de Polícia ([125]) como a polícia distrital); e iv) a Agência de Informações de Segurança Pública («PSIA»). No entanto, o CIRO nunca recolhe informações diretamente junto dos operadores comerciais, incluindo através da intercetação de comunicações. Quando recebam informações de outras autoridades públicas, a fim de fornecer análises ao Governo, estas outras autoridades são obrigadas, por seu turno, a cumprir a lei, nomeadamente as limitações e garantias analisadas na presente decisão. Por esse motivo, as suas atividades não são pertinentes num contexto de transferência.

3.3.1. *Base jurídica e limitações/garantias aplicáveis*

(153) De acordo com a informação recebida, o Ministério da Defesa recolhe informações (eletrónicas) com base na lei que criou este ministério. Nos termos do respetivo artigo 3.º, a função do Ministério da Defesa é assegurar a gestão e o funcionamento das forças militares e «conduzir os assuntos com elas relacionados a fim de garantir a paz e a independência nacionais, bem como a segurança da nação.» O artigo 4.º, n.º 4, da referida lei estabelece que jurisdição do Ministério da Defesa abrange a «defesa e proteção», as ações a empreender pelas Forças de Autodefesa e a mobilização das forças militares, incluindo a recolha das informações necessárias à condução desses assuntos. A sua competência para recolher informações (eletrónicas) junto dos operadores comerciais limita-se à recolha através de cooperação voluntária.

(154) Quanto à polícia distrital, as suas responsabilidades e deveres incluem a «manutenção da segurança e da ordem públicas» (artigo 35.º, n.º 2, em conjugação com o artigo 2.º, n.º 1, da Lei da Polícia). No quadro destas competências, a polícia pode recolher informações, mas unicamente a título voluntário, sem qualquer força jurídica. Além disso, as atividades da polícia devem ser «limitadas ao estritamente necessário» para desempenhar as suas funções. Além disso, deve atuar de forma «imparcial, não partidária, justa e sem preconceitos», sem nunca abusar dos seus poderes «de forma alguma que interfira nos direitos e liberdades de uma pessoa singular consagrados na Constituição do Japão» (artigo 2.º da Lei da Polícia).

(155) Por último, a PSIA pode conduzir inquéritos ao abrigo da Lei relativa à prevenção de atividades subversivas («SAPA») e da Lei relativa ao controlo de organizações que cometeram assassínios em massa («ACO»), quando tais inquéritos se tornem necessários para preparar a adoção de medidas de controlo contra certas organizações ([126]). No âmbito de ambas as leis, a pedido do diretor-geral da PSIA, a Comissão de Análise da Segurança Pública pode emitir determinados «atos» (vigilância/proibições no caso da ACO ([127]), dissolução/proibições no caso da SAPA ([128])) e, no contexto da PSIA, pode conduzir inquéritos ([129]). Segundo a informação recebida, os referidos

([124]) Deste modo, os operadores comerciais têm a liberdade de decidir não cooperar, sem correrem o risco de sanções ou de outras consequências negativas. Ver anexo II, ponto III.A.1.

([125]) Contudo, de acordo com a informação recebida, a principal função da Agência Nacional de Polícia é coordenar as investigações conduzidas pelos vários departamentos da polícia distrital e proceder ao intercâmbio das informações com autoridades estrangeiras. Mesmo no exercício destas funções, a Agência está sujeita à fiscalização da Comissão Nacional para a Segurança Pública, que é responsável, nomeadamente, pela proteção dos direitos e liberdades das pessoas singulares (artigo 5.º, n.º 1, da Lei da Polícia).

([126]) Ver anexo II, ponto III.A.1 (3). O âmbito de aplicação de cada uma destas leis é limitado, sendo que a SAPA se refere a «atividades terroristas subversivas» e a ACO ao «ato de assassínio em massa» (na aceção de «atividade terrorista subversiva» que lhe é dada pela SAPA, «pela qual um grande número de pessoas é indiscriminadamente assassinado»).

([127]) Ver os artigos 5.º e 8.º da ACO. Um ato de vigilância implica igualmente uma obrigação de comunicação de informações para a organização visada pela medida. Ver os artigos 12.º, 13.º e 15.º a 27.º da ACO quanto às garantias processuais, nomeadamente, as exigências de transparência e a autorização prévia da Comissão de Análise da Segurança Pública.

([128]) Ver os artigos 5.º e 7.º da SAPA. Ver os artigos 11.º a 25.º da SAPA quanto às garantias processuais, nomeadamente, as exigências de transparência e a autorização prévia da Comissão de Análise da Segurança Pública.

([129]) Ver o artigo 27.° da SAPA e os artigos 29.º e 30.º da ACO.

inquéritos são sempre conduzidos a título voluntário, o que significa que a PSIA não pode obrigar um detentor de informações pessoais a fornecer essas informações ([130]). Em todos os casos, os controlos e inquéritos devem ser conduzidos apenas na medida mínima necessária para alcançar a finalidade do controlo, não devendo, em circunstância alguma, ser realizados para restringir «de forma injustificada» os direitos e liberdades consagrados na Constituição do Japão (artigo 3.º, n.º 1, da SAPA/ACO). Por outro lado, nos termos do artigo 3.º, n.º 2, da SAPA/ACO, a PSIA não pode, em caso algum, abusar dos referidos controlos ou dos inquéritos conduzidos para preparar esses controlos. Um oficial de informações de segurança pública que tenha abusado da autoridade que lhe confere a respetiva lei, obrigando uma pessoa a fazer algo que não é obrigada a fazer ou interferindo no exercício dos seus direitos, pode, nos termos do artigo 45.º da SAPA ou do artigo 42.º da ACO, incorrer em sanções penais. Por último, as duas leis prescrevem explicitamente que as respetivas disposições, incluindo os poderes nelas conferidos, não devem «em circunstância alguma ser objeto de interpretação alargada» (artigo 2.º da SAPA/ACO).

(156) Aplicam-se a todos os casos de acesso governamental, por razões de segurança nacional, descritos nesta secção, as limitações estipuladas pelo Supremo Tribunal japonês aos inquéritos voluntários, o que significa que a recolha de informações (eletrónicas) deve respeitar os princípios da necessidade e da proporcionalidade («método adequado») ([131]). Como confirmaram explicitamente as autoridades japonesas, «a recolha e o tratamento da informação só podem ter lugar na medida do necessário ao desempenho das atribuições específicas da autoridade pública competente, assim como com base em ameaças concretas». Por conseguinte, encontra-se excluída «a recolha maciça e indiscriminada de informações pessoais, ou o acesso aos mesmos, por razões de segurança nacional» ([132]).

(157) Do mesmo modo, uma vez recolhidas, quaisquer informações pessoais conservadas pelas autoridades públicas para efeitos de segurança nacional são abrangidas pela APPIHAO e beneficiam, por conseguinte, das proteções que esta lei confere, quando se trata da sua conservação, utilização e divulgação subsequentes (ver considerando 118).

3.3.2. *Supervisão independente*

(158) A recolha de informações pessoais por razões de segurança nacional está sujeita a vários níveis de supervisão dos três ramos do poder.

(159) Em primeiro lugar, a Dieta, através das suas comissões especializadas, pode examinar a licitude dos inquéritos com base nos respetivos poderes de escrutínio parlamentar (artigo 62.º da Constituição e artigo 104.º da Lei da Dieta; ver considerando 134). Esta função de supervisão é facilitada por obrigações específicas de comunicação de informações sobre as atividades levadas a cabo no âmbito de algumas das bases jurídicas supramencionadas ([133]).

(160) Em segundo lugar, existem vários mecanismos de supervisão a nível do poder executivo.

(161) No que se refere ao Ministério da Defesa, a supervisão é exercida pela Inspeção-Geral da Conformidade Jurídica (IGO) ([134]), criada com base no artigo 29.º da lei que cria o Ministério da Defesa como um serviço dentro deste ministério, sob a tutela do ministro da Defesa (ao qual presta contas), mas independente dos departamentos operacionais do ministério. Incumbe à IGO assegurar o cumprimento das leis e regulamentos, assim como o correto exercício das funções pelos funcionários do Ministério da Defesa. Os seus poderes incluem a autoridade para realizar as denominadas «inspeções de defesa», tanto a intervalos regulares («inspeções de defesa regulares») como em casos individuais («inspeções de defesa especiais»), as quais também já abrangeram a gestão correta das informações pessoais ([135]). No contexto destas inspeções, a IGO pode entrar em instalações (escritórios) e requerer

([130]) Ver anexo II, ponto III.A.1 (3).

([131]) Ver anexo II, ponto III.A.2 (b): «Resulta da jurisprudência do Supremo Tribunal que os pedidos de cooperação voluntária dirigidos a operadores económicos devem ser necessários à investigação das suspeitas de um crime e ser razoáveis para atingir os objetivos dessa investigação. Embora os inquéritos conduzidos pelas autoridades de investigação no domínio da segurança nacional sejam diferentes dos conduzidos pelas autoridades com poderes coercivos, no que se refere à respetiva base jurídica e finalidade, os princípios centrais da "necessidade da investigação" e da "adequação do método" aplicam-se de igual modo no domínio da segurança nacional, devendo ser cumpridos tendo devidamente em conta as circunstâncias específicas de cada caso.»

([132]) Ver anexo II, ponto III.A.2 (b).

([133]) Ver, nomeadamente, o artigo 36.º da SAPA e o artigo 31.º da ACO (em relação à PSIA).

([134]) O diretor da IGO é um ex-procurador. Ver anexo II, ponto III.B.3.

([135]) Ver anexo II, ponto III.B.3. De acordo com o exemplo descrito, a inspeção de defesa regular de 2016, respeitante à «consciência/preparação para a conformidade jurídica» incluiu, entre outros aspetos, a «situação da proteção das informações pessoais» (gestão, conservação, etc.). O relatório resultante identificou alguns casos de gestão inadequada de dados e tendo requerido a introdução de melhorias nesta matéria. O Ministério da Defesa publicou o relatório no seu sítio Web.

a apresentação de documentos e informações, incluindo explicações da parte do vice-ministro adjunto do Ministério da Defesa. A inspeção termina com a elaboração de um relatório a apresentar ao ministro da Defesa, descrevendo as constatações e as medidas adotadas para introduzir melhorias (cuja aplicação pode, mais uma vez, ser verificada através de inspeções subsequentes). Por sua vez, o relatório constitui a base das instruções do ministro da Defesa com vista à adoção das medidas necessárias para resolver a situação; compete ao vice-ministro adjunto proceder à aplicação dessas medidas, tendo de apresentar um relatório sobre o seguimento que lhes é dado.

(162) No que se refere à polícia distrital, a supervisão é assegurada pelas Comissões Distritais para a Segurança Pública independentes, como referido no considerando 135 a respeito da aplicação do direito penal.

(163) Por último, conforme indicado, a PSIA só pode conduzir inquéritos na medida necessária à adoção de um ato de proibição, dissolução ou vigilância, nos termos da SAPA/ACO, sendo que a Comissão Distrital para a Segurança Pública independente ([136]) exerce supervisão ex ante sobre estes atos. Além disso, são conduzidas inspeções regulares/periódicas (que examinam, de forma exaustiva, as operações da PSIA) ([137]) e inspeções internas especiais ([138]) das atividades de departamentos/gabinetes específicos, etc. por inspetores designados para o efeito, as quais podem resultar em instruções aos chefes dos departamentos relevantes, etc. para que adotem medidas corretivas ou de melhoria.

(164) Estes mecanismos de supervisão, que são ainda mais reforçados pela possibilidade de as pessoas singulares desencadearem a intervenção da PPC, na qualidade de autoridade de controlo independente (ver secção 168 infra), proporcionam garantias adequadas contra o risco de abusos pelas autoridades japonesas dos seus poderes no domínio da segurança nacional e contra eventual recolha ilícita de informações eletrónicas.

3.3.3. *Recurso individual*

(165) No que respeita ao recurso individual no caso de informações pessoais recolhidas e «conservadas» pelos órgãos administrativos, estes são obrigados a «esforçar-se por tratar, de forma correta e expedita, quaisquer reclamações» quanto ao respetivo tratamento (artigo 48.º da APPIHAO).

(166) Por outro lado, ao contrário das investigações criminais, a APPIHAO confere, em princípio, às pessoas singulares (incluindo estrangeiros residentes fora do seu país) o direito à divulgação ([139]), correção (incluindo o apagamento) e suspensão da utilização/transmissão. No entanto, o dirigente do órgão administrativo pode recusar a divulgação, no caso de informações «em relação às quais existam motivos razoáveis […] para considerar que essa divulgação é suscetível de prejudicar a segurança nacional» (ver artigo 14,º. subalínea iv) da APPIHAO) e pode, inclusivamente, fazê-lo sem revelar a existência de tais informações (artigo 17.º da APPIHAO). De igual modo, embora uma pessoa singular possa requerer a suspensão da utilização ou o apagamento, nos termos do artigo 36.º, n.º 1, subalínea i) da APPIHAO, caso o órgão administrativo tenha obtido as informações de forma ilícita ou as conserve/utilize para além do necessário para alcançar a finalidade especificada, a autoridade pode rejeitar o pedido, se entender que a suspensão da utilização «é suscetível de entravar a correta condução dos assuntos relativos à finalidade da utilização das informações pessoais conservadas, devido à natureza dos assuntos referidos» (artigo 38.º da APPIHAO). De qualquer modo, sempre que seja possível separar e excluir facilmente partes que sejam objeto de uma derrogação, os órgãos administrativos são obrigados a permitir a sua divulgação, pelo menos, parcial (ver, por exemplo, o artigo 15.º, n.º 1, da APPIHAO) ([140]).

([136]) Nos termos da Lei que cria a Comissão de Análise da Segurança Pública, o presidente e os membros desta Comissão devem «exercer os seus poderes de uma forma independente» (artigo 3.º). São nomeados pelo primeiro-ministro mediante a aprovação de ambas as câmaras da Dieta e só podem ser destituídos com justa causa (por exemplo, prisão, conduta reprovável, distúrbio mental ou físico, abertura de um processo de falência).

([137]) Regulamento relativo à inspeção periódica da Agência de Informações de Segurança Pública (diretor-geral da PSIA, instrução n.º 4, 1986).

([138]) Regulamento relativo à inspeção especial da Agência de Informações de Segurança Pública (diretor-geral da PSIA, instrução n.º 11, 2008). São realizadas inspeções especiais quando o diretor-geral da PSIA as entende necessárias.

([139]) Tal refere-se ao direito de receber uma cópia das «informações pessoais conservadas».

([140]) Ver igualmente a possibilidade de «divulgação discricionária», mesmo no caso de estarem incluídas «informações confidenciais» nas «informações pessoais conservadas» cuja divulgação seja solicitada (artigo 16.º da APPIHAO).

(167) Seja como for, o órgão administrativo deve tomar uma decisão por escrito dentro de um prazo determinado (30 dias, que em certas condições pode ser prorrogado por mais 30 dias). Se o pedido for rejeitado, atendido apenas parcialmente ou a pessoa em causa, por outro motivo, considerar que a conduta do órgão administrativo é «ilegal ou injusta» pode requerer a sua reapreciação administrativa com base na Lei relativa à apreciação de reclamações administrativas ([141]). Nesse caso, o presidente do órgão administrativo decide sobre o recurso deve consultar o Comité de Avaliação da Divulgação de Informações e da Proteção de Informações Pessoais (artigos 42.º e 43.º da APPIHAO), um comité especializado e independente cujos membros são designados pelo primeiro-ministro mediante a aprovação de ambas as câmaras da Dieta. Segundo a informação recebida, o Comité de Avaliação pode realizar uma apreciação ([142]) e solicitar, neste contexto, ao órgão administrativo que disponibilize as informações pessoais conservadas, incluindo todo e qualquer conteúdo classificado, assim como outras informações e documentos. Embora não seja juridicamente vinculativo, o relatório final enviado ao reclamante, bem como ao órgão administrativo, e tornado público é, em quase todos os casos, respeitado ([143]). Além disso, a pessoa singular tem a possibilidade de contestar judicialmente a decisão sobre o recurso com base na Lei do contencioso administrativo. Tal abre caminho ao controlo judicial da utilização da(s) derrogação(ões) relacionada(s) com a segurança nacional, incluindo se tal derrogação foi utilizada abusivamente ou continua a justificar-se.

(168) A fim de facilitar o exercício dos direitos supramencionados, ao abrigo da APPIHAO, o Ministério dos Assuntos Internos e das Comunicações criou 51 «centros de informações globais», que prestam informações consolidadas sobre esses direitos, sobre os procedimentos aplicáveis para apresentar um pedido e sobre as possíveis vias de recurso ([144]). Quanto aos órgãos administrativos, estes são obrigados a prestar «informações que contribuam para especificar as informações pessoais conservadas detidas» ([145]) e a tomar «outras medidas adequadas tendo em vista a conveniência da pessoa que pretende apresentar o pedido» (artigo 47.º, n.º 1, da APPIHAO).

(169) Como sucede no caso dos inquéritos no domínio da aplicação do direito penal, também no domínio da segurança nacional as pessoas singulares podem obter reparação individual contactando diretamente a PPC. É, assim, desencadeado o procedimento específico de resolução de litígios, criado pelo Governo japonês para as pessoas singulares da UE cujos dados pessoais sejam transferidos no âmbito da presente decisão (ver as explicações pormenorizadas nos considerandos 141 a 144 e 149).

(170) Além disso, as pessoas singulares podem recorrer judicialmente intentando uma ação por danos, ao abrigo da Lei relativa a recurso contra o Estado, que também abrange danos morais e, sob certas condições, requerer o apagamento dos dados recolhidos (ver considerando 147).

4. CONCLUSÃO: NÍVEL ADEQUADO DE PROTEÇÃO DOS DADOS PESSOAIS TRANSFERIDOS DA UNIÃO EUROPEIA PARA OPERADORES COMERCIAIS NO JAPÃO

(171) A Comissão entende que a APPI, completada pelas normas complementares constantes do anexo I, juntamente com as declarações, garantias e compromissos oficiais constantes do anexo II, asseguram um nível de proteção dos dados pessoais transferidos da União Europeia essencialmente equivalente ao garantido pelo Regulamento (UE) 2016/679.

(172) Por outro lado, a Comissão considera que os mecanismos de controlo e as vias de recurso previstos na legislação japonesa permitem, no seu conjunto, identificar e sancionar na prática as violações pelos PIHBO destinatários, proporcionando vias judiciais aos titulares dos dados para ter acesso aos respetivos dados pessoais e, em última instância, requerer a retificação ou apagamento dos mesmos.

([141]) Lei relativa à apreciação de reclamações administrativas (Lei n.º 160 de 2014), nomeadamente o artigo 1.º, n.º 1.

([142]) Ver artigo 9.º da Lei que cria o Comité de Avaliação da Divulgação de Informações e da Proteção de Informações Pessoais (Lei n.º 60 de 2003).

([143]) Segundo a informação recebida, nos 13 anos que decorreram desde 2005 (quando a APPIHAO entrou em vigor), apenas por duas vezes, em mais de 2000 casos, o órgão administrativo não deu seguimento às conclusões do relatório, apesar de as decisões administrativas terem sido contestadas pelo Comité de Avaliação em várias ocasiões. Por outro lado, se o órgão administrativo tomar uma decisão que diverge das constatações do relatório, deve indicar claramente os motivos dessa divergência. Ver o anexo II, ponto III.C, com referência ao artigo 50.º, n.º 1, subalínea iv), da Lei relativa à apreciação de reclamações administrativas.

([144]) Os centros de informações globais (um em cada distrito do Japão) fornecem aos cidadãos explicações sobre as informações pessoais recolhidas pelas autoridades públicas (por exemplo, as bases de dados existentes) e as normas em vigor em matéria de proteção de dados (APPIHAO), incluindo sobre o exercício dos direitos à divulgação, correção ou suspensão da utilização. Simultaneamente, funcionam como ponto de contacto para os pedidos de esclarecimento/reclamações por parte dos cidadãos. Ver anexo II, ponto II.C.4, a).

([145]) Ver também os artigos 10.º e 11.º da APPIHAO sobre o «registo de ficheiros de informações pessoais», os quais contêm, todavia, amplas derrogações no tocante a «ficheiros de informações pessoais» preparados ou obtidos para efeitos de investigação criminal ou que incluem matérias relativas à segurança e a outros interesses importantes do Estado (ver artigo 10.º, n.º 2, subalíneas i) e ii) da APPIHAO).

(173) Por último, com base nas informações disponíveis sobre o quadro jurídico japonês, incluindo as declarações, garantias e compromissos do Governo japonês, que constam do anexo II, a Comissão entende que qualquer ingerência das autoridades públicas japonesas nos direitos fundamentais das pessoais singulares, cujos dados pessoais sejam transferidos da União Europeia para o Japão, para fins de interesse público, designadamente, para efeitos de aplicação do direito penal e de segurança nacional, será limitada ao estritamente necessário para alcançar o objetivo legítimo em causa, existindo uma proteção jurídica eficaz contra tal ingerência.

(174) Assim, atendendo as constatações efetuadas na presente decisão, a Comissão considera que o Japão garante um nível adequado de proteção dos dados pessoais transferidos da União Europeia para PIHBO no Japão sujeitos à APPI, exceto quando o destinatário seja abrangido por uma das categorias enumeradas no artigo 76.º, n.º 1, da APPI e em que a totalidade ou parte das finalidades do tratamento corresponda a uma das finalidades prescritas nessa disposição.

(175) Consequentemente, a Comissão conclui que se encontra satisfeito o padrão de adequação descrito no artigo 45.º do Regulamento (UE) 2016/679, interpretado em função da Carta dos Direitos Fundamentais da União Europeia, nomeadamente no acórdão *Schrems* ([146]).

5. AÇÃO DAS AUTORIDADES RESPONSÁVEIS PELA PROTEÇÃO DOS DADOS E INFORMAÇÃO À COMISSÃO

(176) Em conformidade com a jurisprudência do Tribunal de Justiça ([147]) e tal como reconhecido no artigo 45.º, n.º 4, do Regulamento (UE) 2016/679, a Comissão deve controlar, de forma continuada, os desenvolvimentos relevantes no país terceiro após a adoção de uma decisão de adequação, por forma a avaliar se o Japão continua a assegurar um nível de proteção essencialmente equivalente. De qualquer modo, tal verificação é necessária sempre que a Comissão obtenha informações que suscitem dúvidas justificadas a esse respeito.

(177) Por conseguinte, a Comissão deve controlar, de forma continuada, a situação relativamente ao quadro jurídico e à prática real em matéria de tratamento de dados pessoais, conforme a avaliação da presente decisão, incluindo o cumprimento pelas autoridades japonesas das declarações, garantias e compromissos que constam do anexo II. Para facilitar este processo, espera-se que as autoridades japonesas informem a Comissão sobre desenvolvimentos materiais que afetem a presente decisão, tanto no tocante ao tratamento de dados pessoais pelos operadores comerciais como às limitações e garantias aplicáveis ao acesso aos dados pessoais pelas autoridades públicas. Tal deverá incluir as eventuais decisões adotadas pela PPC nos termos do artigo 24.º da APPI reconhecendo que um país terceiro assegura um nível de proteção equivalente ao garantido no Japão.

(178) Além disso, a fim de permitir à Comissão o exercício eficaz da sua função de controlo, os Estados-Membros devem informar a Comissão sobre qualquer medida pertinente adotada pelas autoridades nacionais responsáveis pela proteção dos dados, em particular no que se refere a consultas ou reclamações de titulares de dados da UE relativas à transferência de dados pessoais da União Europeia para operadores comerciais no Japão. A Comissão deve igualmente ser informada sobre quaisquer indícios de que as ações das autoridades públicas japonesas responsáveis pela prevenção, investigação, deteção ou repressão de infrações penais ou pela segurança nacional, incluindo os organismos de controlo, não asseguram o nível de proteção exigido.

(179) Os Estados-Membros e os respetivos órgãos são obrigados a tomar as medidas necessárias para cumprir os atos das instituições da União, uma vez que se presume que os mesmos são lícitos e logo produzem efeitos jurídicos até serem revogados, anulados no âmbito de um recurso de anulação ou declarados inválidos na sequência de um reenvio prejudicial ou de uma exceção de ilegalidade. Consequentemente, uma decisão de adequação da Comissão adotada nos termos do artigo 45.º, n.º 3, do Regulamento (UE) 2016/679 é vinculativa para todos os organismos dos Estados-Membros aos quais se destina, nomeadamente para as suas autoridades de controlo independentes. Simultaneamente, tal como explicado no acórdão *Schrems* ([148]) do Tribunal de Justiça e reconhecido no artigo 58.º, n.º 5, do Regulamento, se uma autoridade responsável pela proteção de dados colocar em causa, nomeadamente na sequência de uma reclamação, a conformidade de uma decisão de adequação da Comissão com a proteção dos direitos fundamentais à privacidade e à proteção dos dados da pessoa singular, a legislação nacional deve proporcionar-lhe uma via de recurso que lhe permita apresentar tais objeções perante um tribunal nacional que, em caso de dúvida, deve suspender a instância e proceder a um reenvio prejudicial para o Tribunal de Justiça ([149]).

([146]) Ver nota 3, acima.
([147]) *Schrems*, n.º 76.
([148]) *Schrems*, n.º 65.
([149]) *Schrems*, n.º 65: «Incumbe ao legislador nacional prever vias de recurso que permitam à autoridade nacional de controlo em causa invocar as críticas que considera fundadas perante os órgãos jurisdicionais nacionais, para que estes últimos, caso partilhem das dúvidas dessa autoridade quanto à validade da decisão da Comissão, procedam a um reenvio prejudicial para efeitos da apreciação da validade da decisão.»

6. REAPRECIAÇÃO PERIÓDICA DA VERIFICAÇÃO DE ADEQUAÇÃO

(180) Por força do artigo 45.º, n.º 3, do Regulamento (UE) 2016/679 ([150]) e atendendo a que o nível de proteção conferido pelo quadro jurídico japonês pode vir a alterar-se, a Comissão deve, na sequência da adoção da presente decisão, avaliar periodicamente se as verificações de adequação do nível de proteção assegurado pelo Japão continuam a justificar-se de facto e de direito.

(181) Para tal, a presente decisão deverá ser sujeita a uma primeira avaliação no prazo de dois anos após a sua entrada em vigor. Na sequência dessa primeira avaliação e em função dos seus resultados, a Comissão decidirá, em estreita consulta com o comité criado nos termos do artigo 93.º, n.º 1, do RGPD, se se deve ou não manter o ciclo de dois anos. Em qualquer caso, as revisões subsequentes devem ter lugar, pelo menos, de quatro em quatro anos ([151]). A avaliação deverá abranger todos os aspetos do funcionamento da presente decisão, nomeadamente a aplicação das normas complementares (com especial atenção às proteções conferidas no caso de transferências subsequentes), a aplicação das normas relativas ao consentimento, incluindo em caso de retirada do mesmo, a eficácia do exercício dos direitos individuais, assim como as limitações e garantias respeitantes ao acesso governamental, incluindo o mecanismo de recurso previsto no anexo II da presente decisão. Deve igualmente abranger a eficácia da supervisão e da aplicação coerciva da legislação, no que diz respeito às regras aplicáveis a ambas as organizações e no domínio da aplicação do direito penal e da segurança nacional.

(182) A fim de realizar a avaliação, a Comissão deverá reunir-se com a PPC, acompanhada, se for caso disso, por outras autoridades japonesas responsáveis pelo acesso governamental, incluindo os organismos de controlo pertinentes. Essa reunião será aberta à participação de representantes dos membros do Comité Europeu para a Proteção de Dados (CEPD). No quadro da avaliação conjunta, a Comissão deverá solicitar à PPC que preste informações exaustivas sobre todos os aspetos pertinentes para a verificação de adequação, incluindo quanto às limitações e garantias respeitantes ao acesso governamental ([152]). A Comissão deve também procurar obter explicações sobre quaisquer informações que tenha recebido com relevância para a presente decisão, incluindo relatórios públicos das autoridades japonesas ou de outras partes interessadas no Japão, do CEPD, de autoridades responsáveis pela proteção de dados individuais, de grupos da sociedade civil, notícias na comunicação social ou qualquer outra fonte de informação disponível.

(183) Com base na avaliação conjunta, a Comissão deverá preparar um relatório público a apresentar ao Parlamento Europeu e ao Conselho.

7. SUSPENSÃO DA DECISÃO DE ADEQUAÇÃO

(184) Se a Comissão concluir, com base em verificações regulares e pontuais ou em quaisquer outras informações disponíveis, que o nível de proteção conferido pelo quadro jurídico japonês deixou de poder ser considerado como essencialmente equivalente ao da União Europeia, deverá informar as autoridades japonesas competentes do facto e solicitar que sejam adotadas medidas apropriadas dentro de um prazo razoável que especificará. Tal inclui as normas aplicáveis tanto aos operadores comerciais como às autoridades públicas japonesas responsáveis pela aplicação do direito penal ou pela segurança nacional. A título de exemplo, esse procedimento deve ser acionado sempre que transferências subsequentes, incluindo as efetuadas com base nas decisões adotadas pela PPC nos termos do artigo 24.º da APPI, que reconheçam que um país terceiro assegura um nível de proteção equivalente ao garantido no Japão, deixem de ser levadas a cabo ao abrigo de garantias que assegurem a continuidade da proteção, na aceção do artigo 44.º do RGPD.

(185) Se, uma vez decorrido o prazo especificado, as autoridades japonesas competentes não demonstrarem, de forma satisfatória, que a presente decisão continua a basear-se num nível de proteção adequado, a Comissão deve, por força do artigo 45.º, n.º 5, do Regulamento (UE) 2016/679, iniciar o procedimento conducente à suspensão total ou parcial ou à revogação da presente decisão. Em alternativa, a Comissão pode dar início ao procedimento de alteração da presente decisão, nomeadamente sujeitando as transferências de dados a condições adicionais ou limitando o âmbito de aplicação da verificação de adequação às transferências de dados em relação às quais a continuidade da proteção na aceção do artigo 44.º do RGPD possa ser assegurada.

([150]) Nos termos do artigo 45.º, n.º 3, do Regulamento (UE) 2016/679, «[o] ato de execução prevê um procedimento de avaliação periódica, no mínimo de quatro em quatro anos, que deverá ter em conta todos os desenvolvimentos pertinentes no país terceiro ou na organização internacional.»

([151]) O artigo 45.º, n.º 3, do Regulamento (UE) 2016/679 prevê a realização de uma avaliação periódica, no mínimo de quatro em quatro anos. Ver igualmente o referencial de adequação do CEPD, WP 254 rev. 01.

([152]) Ver igualmente anexo II, ponto IV: «No quadro da avaliação periódica da decisão de adequação, a PPC e a Comissão Europeia trocarão informações sobre o tratamento de dados, nas condições da verificação de adequação, incluindo as previstas na presente declaração.»

(186) Mais concretamente, a Comissão deverá iniciar o procedimento de suspensão ou de revogação quando existam indícios de que os operadores comerciais, que recebem dados pessoais ao abrigo da presente decisão, não cumprem as normas complementares constantes do anexo I e/ou que estas normas não são eficazmente aplicadas, ou ainda se as autoridades japonesas não cumprirem as declarações, garantias e compromissos constantes do anexo II da presente decisão.

(187) A Comissão deverá igualmente ponderar a possibilidade de iniciar o procedimento conducente à alteração, suspensão ou revogação da presente decisão, se apurar, no contexto da avaliação conjunta ou por outra forma, que as autoridades japonesas competentes não prestam as informações ou esclarecimentos necessários à avaliação do nível de proteção conferido aos dados pessoais transferidos da União Europeia para o Japão ou do cumprimento da presente decisão. Nesta matéria, a Comissão deverá ter em conta em que medida a informação pertinente pode ser obtida junto de outras fontes.

(188) Por motivos de urgência devidamente justificados, como o risco de violação grave dos direitos dos titulares dos dados, a Comissão pode ponderar a adoção de uma decisão de suspensão ou revogação da presente decisão, com efeitos imediatos, nos termos do artigo 93.º, n.º 3, do Regulamento (UE) 2016/679, em conjugação com o artigo 8.º do Regulamento 182/2011 do Parlamento Europeu e do Conselho ([153]).

8. **CONSIDERAÇÕES FINAIS**

(189) O Comité Europeu para a Proteção de Dados publicou o seu parecer ([154]), que foi tido em conta na preparação da presente decisão.

(190) O Parlamento Europeu adotou uma resolução relativa a uma estratégia comercial digital, que insta a Comissão a atribuir prioridade à adoção de decisões de adequação com parceiros comerciais importantes e a acelerar o respetivo processo, nas condições definidas no Regulamento (UE) 2016/679, enquanto mecanismo fundamental para proteger a transferência de dados pessoais da União Europeia ([155]). O Parlamento Europeu adotou igualmente uma resolução sobre a adequação da proteção dos dados pessoais concedida pelo Japão ([156]).

(191) As medidas previstas na presente decisão são conformes com o disposto no parecer emitido pelo comité criado nos termos do artigo 93.º, n.º 1, do RGPD,

ADOTOU A PRESENTE DECISÃO:

Artigo 1.º

1. Para efeitos do artigo 45.º do Regulamento (UE) 2016/679, o Japão assegura um nível adequado de proteção dos dados pessoais transferidos da União Europeia para operadores comerciais neste país, responsáveis pela gestão de informações pessoais e sujeitos à Lei relativa à proteção de informações pessoais, completadas pelas normas complementares definidas no anexo I, em conjunto com as declarações, garantias e compromissos oficiais constantes do anexo II.

([153]) Regulamento (UE) n.º 182/2011 do Parlamento Europeu e do Conselho, de 16 de fevereiro de 2011, que estabelece as regras e os princípios gerais relativos aos mecanismos de controlo pelos Estados-Membros do exercício das competências de execução pela Comissão (JO L 55 de 28.2.2011, p. 13)

([154]) Parecer 28/2018 sobre o projeto de decisão de execução da Comissão Europeia sobre a adequação do nível de proteção dos dados pessoais assegurado pelo Japão, de 5 de dezembro de 2018.

([155]) Resolução do Parlamento Europeu de 12 de dezembro de 2017 «Rumo a uma estratégia comercial digital» [2017/2065(INI)]. Ver, nomeadamente, o ponto 8 («…recorda que os dados pessoais podem ser transferidos para países terceiros sem recorrer às disciplinas gerais dos acordos comerciais se forem cumpridos, tanto atualmente como no futuro, os requisitos consagrados no […] capítulo V do Regulamento (UE) 2016/679 relativo à proteção de dados; reconhece que as decisões de adequação, nomeadamente parciais e setoriais, são um mecanismo fundamental para proteger a transferência de dados pessoais da UE para um país terceiro; observa que a UE só adotou decisões de adequação relativamente a quatro dos seus 20 maiores parceiros comerciais…») e o ponto 9 («Solicita à Comissão que dê prioridade à adoção de decisões de adequação mútua e acelere o respetivo processo, desde que os países terceiros assegurem, por força da sua legislação nacional ou dos seus compromissos internacionais, um nível de proteção "essencialmente equivalente" ao garantido na UE…»).

([156]) Resolução do Parlamento Europeu, de 13 de dezembro de 2018, sobre a adequação da proteção dos dados pessoais concedida pelo Japão [2018/2979 (RSP)].

2. A presente decisão não se aplica aos dados pessoais transferidos para destinatários abrangidos por uma das categorias seguintes, quando a totalidade ou parte das finalidades do tratamento de dados pessoais corresponda a uma das finalidades enumeradas, respetivamente:

a) organismos de radiodifusão, editores de jornais, agências de comunicação ou outros órgãos de imprensa (incluindo pessoas singulares cuja atividade comercial consista na realização de atividades junto da imprensa), na medida em que tratem dados pessoais para efeitos de divulgação na imprensa;

b) pessoas que se dediquem à atividade de escrita profissional, na medida em que a mesma envolva dados pessoais;

c) universidades e outras organizações ou grupos orientados para estudos académicos ou pessoas singulares pertencentes a organizações desse tipo, na medida em que tratem dados pessoais para efeitos de estudos académicos;

d) instituições religiosas, na medida em que tratem dados pessoais para efeitos de atividade religiosa (incluindo todas as atividades associadas); bem como

e) organismos políticos, na medida em que tratem dados pessoais para efeitos da sua atividade política (incluindo todas as atividades associadas).

Artigo 2.º

Sempre que, para efeitos de proteção das pessoas singulares no que se refere ao tratamento dos seus dados pessoais, as autoridades competentes dos Estados-Membros exercerem as suas competências, nos termos do artigo 58.º do Regulamento (UE) 2016/679, tendo como resultado a suspensão ou a proibição definitiva dos fluxos de dados para um determinado operador comercial no Japão, dentro do âmbito de aplicação previsto no artigo 1.º, o Estado-Membro em causa deve informar de imediato a Comissão.

Artigo 3.º

1. A Comissão deve garantir o acompanhamento contínuo da aplicação do enquadramento normativo em que assenta a presente decisão, nomeadamente as condições em que se procede a transferências subsequentes, por forma a avaliar se o Japão continua a assegurar um nível de proteção adequado na aceção do artigo 1.º.

2. Os Estados-Membros e a Comissão devem comunicar-se reciprocamente os casos em que a Comissão de Proteção de Informações Pessoais, ou qualquer outra autoridade japonesa competente, deixe de cumprir o enquadramento normativo em que a presente decisão assenta.

3. Os Estados-Membros e a Comissão devem comunicar-se reciprocamente quaisquer informações relativas a indícios de que a ingerência das autoridades japonesas no direito das pessoas singulares à proteção dos dados pessoais excede o estritamente necessário ou de que não existe uma proteção jurídica eficaz contra tal ingerência.

4. No prazo de dois anos a contar da data de notificação da presente decisão aos Estados-Membros e, subsequentemente, de quatro em quatro anos, a Comissão deve avaliar a verificação prevista no artigo 1.º, n.º 1, com base em todas as informações disponíveis, incluindo as recebidas no âmbito da avaliação conjunta realizada com as autoridades japonesas competentes.

5. Se a Comissão tomar conhecimento de quaisquer indícios de que deixou de ser assegurado um nível de proteção adequado, deve informar desse facto as autoridades japonesas competentes. Se necessário, poderá decidir suspender, alterar ou revogar a presente decisão ou limitar o respetivo âmbito de aplicação, sobretudo se houver indícios de que:

a) os operadores comerciais no Japão que receberam dados pessoais da União Europeia nos termos da presente decisão não respeitam as garantias adicionais definidas nas normas complementares constantes do anexo I da presente decisão ou de que a supervisão e a aplicação coerciva nesta matéria são insuficientes;

b) as autoridades públicas japonesas não cumprem as declarações, garantias e compromissos constantes do anexo II da presente decisão, incluindo no que se refere às condições e limitações em matéria de recolha de dados pessoais transferidos no âmbito da presente decisão, e de acesso aos mesmos pelas autoridades públicas japonesas para efeitos de aplicação do direito penal e de segurança nacional.

A Comissão pode igualmente apresentar os referidos projetos de medidas se a falta de cooperação do Governo japonês a impedir de determinar se a verificação prevista no artigo 1.º, n.º 1, da presente decisão foi afetada.

Artigo 4.º

Os Estados-Membros são os destinatários da presente decisão.

Feito em Bruxelas, em 23 de janeiro de 2019.

Pela Comissão
Věra JOUROVÁ
Membro da Comissão

ANEXO 1

NORMAS COMPLEMENTARES AO ABRIGO DA LEI RELATIVA À PROTEÇÃO DE INFORMAÇÕES PESSOAIS PARA O TRATAMENTO DE DADOS PESSOAIS TRANSFERIDOS DA UE COM BASE NUMA DECISÃO DE ADEQUAÇÃO

Índice

Terminologia:

«Lei»	Lei relativa à proteção de informações pessoais (Lei n.º 57 de 2003)
«Decreto ministerial»	Decreto ministerial de execução da Lei relativa à proteção de informações pessoais (decreto ministerial n.º 507 de 2003)
«Normas»	Normas de execução da Lei relativa à proteção de informações pessoais (Norma n.º 3 de 2016 da Comissão de Proteção de Informações Pessoais)
«Orientações sobre as normas gerais»	Orientações quanto à Lei relativa à proteção de informações pessoais (volume sobre as normas gerais) (comunicação n.º 65 de 2015 da Comissão de Proteção de Informações Pessoais)
«UE»	União Europeia, incluindo os seus Estados-Membros e, por força do Acordo EEE, a Islândia, o Liechtenstein e a Noruega
«RGPD»	Regulamento do Parlamento Europeu e do Conselho relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados)
«Decisão de adequação»	Decisão em que a Comissão Europeia constata que um país terceiro ou um território do mesmo assegura um nível adequado de proteção dos dados pessoais nos termos do artigo 45.º do RGPD.

A fim de assegurar a transferência mútua e sem sobressaltos de dados pessoais entre o Japão e a UE, a Comissão de Proteção de Informações Pessoais decidiu considerar a UE como um país estrangeiro que possui um sistema de proteção das informações pessoais reconhecido como equivalente ao do Japão quanto à proteção dos direitos e interesses das pessoas singulares, nos termos do artigo 24.º da Lei. Simultaneamente, a Comissão Europeia decidiu, por seu turno, que o Japão assegura um nível adequado de proteção dos dados pessoais nos termos do artigo 45.º do RGPD.

Isto possibilita a fluidez da transferência de dados pessoais entre o Japão e a UE, garantindo um elevado nível de proteção dos direitos e interesses das pessoas singulares. A fim de assegurar um elevado nível de proteção das informações pessoais recebidas da UE com base numa decisão de adequação e tendo em conta o facto de que, embora exista um elevado grau de convergência, subsistem diferenças relevantes entre os dois sistemas, a Comissão de Proteção de Informações Pessoais adotou as presentes normas complementares, com base na Lei relativa à execução da cooperação com os governos de outros países, tendo em vista assegurar um tratamento adequado dos dados pessoais recebidos da UE, com base numa decisão de adequação, pelos operadores comerciais responsáveis pela gestão de informações pessoais, bem como o cumprimento adequado e eficaz das obrigações previstas nas referidas normas ([1]).

([1]) Artigo 4.º, artigo 6.º, artigo 8.º, artigo 24.º, artigo 60.º artigo 78.º da Lei, e artigo 11.º das normas.

Mais concretamente, o artigo 6.º da Lei prevê a possibilidade de se adotarem medidas legislativas ou de outro tipo para reforçar a proteção das informações pessoais e criar um sistema de informações pessoais compatível com as normas internacionais, mediante a definição de regras mais rigorosas que complementem e vão mais longe do que as estipuladas na Lei e no decreto ministerial. A Comissão de Proteção de Informações Pessoais, enquanto autoridade responsável por administrar a aplicação geral da Lei, pode portanto definir, nos termos do artigo 6.º da Lei, regras mais rigorosas através da formulação das presentes normas complementares, que preveem um nível mais elevado de proteção dos direitos e interesses das pessoas singulares quanto ao tratamento dos dados pessoais recebidos da UE com base numa decisão de adequação, nomeadamente no que se refere à definição de «informações pessoais que requerem atenção especial», nos termos do artigo 2.º, n.º 3, e de «dados pessoais conservados», nos termos do artigo 2.º, n.º 7, da Lei (incluindo quanto ao prazo de conservação aplicável).

Deste modo, as normas complementares são vinculativas para os operadores comerciais responsáveis pela gestão de informações pessoais que recebam dados pessoais transferidos da UE com base numa decisão de adequação, estando, por conseguinte, obrigados a cumpri-las. Enquanto normas juridicamente vinculativas, todos os direitos e obrigações são passíveis de execução pela Comissão de Proteção de Informações Pessoais, tal como as disposições da Lei que visam complementar com regras mais rigorosas e/ou pormenorizadas. Em caso de violação dos direitos e obrigações decorrentes das normas complementares, as pessoas singulares podem obter reparação junto dos tribunais, assim como no que se refere às disposições da Lei que visam complementar com regras mais rigorosas e/ou pormenorizadas.

No que se refere à execução coerciva pela Comissão de Proteção de Informações Pessoais, quando um operador comercial responsável pela gestão de informações pessoais não cumpra alguma das obrigações que lhe incubem por força das normas complementares, a Comissão de Proteção de Informações Pessoais pode adotar medidas nos termos do artigo 42.º da Lei. No que respeita em geral às informações pessoais recebidas da UE com base numa decisão de adequação, o facto de um operador comercial responsável pela gestão de informações pessoais não adotar medidas conformes com uma recomendação formulada nos termos do artigo 42.º, n.º 1, da Lei, sem que para tal apresente um motivo legítimo ([2]), é considerado uma violação grave iminente dos direitos e interesses de uma pessoa singular, na aceção do artigo 42.º, n.º 2, da Lei.

1. Informações pessoais que requerem atenção especial (artigo 2.º, n.º 3, da Lei).

Artigo 2.º, n.º 3, da Lei

3. Para efeitos da Lei, entende-se por «informações pessoais que requerem atenção especial» a raça, credo, estatuto social, historial clínico e registo criminal do titular, bem como o facto de ter sofrido danos em consequência de um crime, assim como outras descrições determinadas pelo decreto ministerial como descrições cujo tratamento requer uma atenção especial para não causar discriminação injusta, prejuízo ou outras desvantagens ao titular.

Artigo 2.º do decreto ministerial

As referidas descrições, determinadas por decreto ministerial nos termos do artigo 2.º, n.º 3, da Lei, são aquelas que contenham qualquer das características seguintes (com exceção das que se inserem no âmbito do historial clínico ou do registo criminal do titular):

i) a existência de alguma deficiência física, intelectual ou mental (incluindo em termos de desenvolvimento) ou qualquer outra deficiência física ou mental funcional elencada nas normas da Comissão de Proteção de Informações Pessoais;

ii) os resultados de um exame médico ou de outro tipo (a seguir designados «exames médicos») para prevenir ou diagnosticar precocemente uma doença realizado pelo titular junto de um médico ou de outra pessoa que exerça funções no âmbito da medicina (a seguir designada «médico»);

iii) o facto de um médico ter prescrito ao titular indicações, terapias ou receitas médicas para melhorar a sua condição física e mental, em função dos resultados de exames médicos, ou por motivo de doença, ferimento ou de qualquer alteração física ou mental;

iv) o facto de ter sido efetuada uma detenção, revista ou apreensão, ou de ter sido instaurada uma ação ou processo penal contra o titular na qualidade de suspeito ou de réu;

([2]) Entende-se por motivo legítimo um acontecimento de caráter extraordinário, fora do controlo do operador comercial responsável pela gestão de informações pessoais, que não pudesse ter sido razoavelmente previsto (por exemplo, uma catástrofe natural) ou quando a necessidade de tomar medidas quanto a uma recomendação formulada pela Comissão de Proteção de Dados Pessoais nos termos do artigo 42.º, n.º 1, da Lei tenha cessado em virtude de o referido operador ter adotado medidas alternativas que remedeiem plenamente a violação.

v) o facto de ter sido efetuada em relação ao titular uma investigação, uma medida de observação/proteção, a realização de uma audiência ou a adoção de uma decisão, medida cautelar ou qualquer outro processo relacionado com a proteção de menores, enquanto menor ou pessoa suspeita nos termos do artigo 3.º, n.º 1, da Lei relativa aos menores.

Artigo 5.º das normas

As deficiências físicas ou mentais funcionais a que se referem as normas da Comissão de Proteção de Informações Pessoais ao abrigo do artigo 2.º, alínea i), do decreto, são as seguintes:

i) deficiências físicas elencadas no quadro anexo à Lei sobre o bem-estar das pessoas com deficiência física (Lei n.º 283 de 1949);

ii) deficiências intelectuais previstas na Lei relativa ao bem-estar das pessoas com deficiência intelectual (Lei n.º 37 de 1960);

iii) deficiências mentais previstas na Lei sobre a saúde mental e o bem-estar das pessoas com deficiência mental (Lei n.º 123 de 1950) (incluindo as deficiências em matéria de desenvolvimento previstas no artigo 2.º, n.º (1), da Lei sobre o apoio às pessoas com deficiência de desenvolvimento, exceto as deficiências intelectuais ao abrigo da Lei relativa ao bem-estar das pessoas com deficiência intelectual);

iv) doenças incuráveis ou outras doenças específicas graves previstas no decreto ministerial, nos termos do artigo 4.º, n.º 1, da Lei sobre o apoio à vida quotidiana e social das pessoas com deficiência (Lei n.º 123 de 2005), equivalentes às prescritas pelo ministro da Saúde, do Trabalho e Segurança Social ao abrigo do referido parágrafo.

Se os dados pessoais recebidos da UE com base numa decisão de adequação contiverem dados relativos à vida sexual ou à orientação sexual de uma pessoa singular, ou à sua filiação sindical, definidos como categorias especiais de dados pessoais no âmbito do RGPD, os operadores comerciais responsáveis pela gestão de informações pessoais são obrigados a tratar esses dados como «informações pessoais que requerem atenção especial», na aceção do artigo 2.º, n.º 3, da Lei.

2. «Dados pessoais conservados» (artigo 2.º, n.º 7, da Lei)

Artigo 2.º, n.º 7, da Lei

7. Entende-se por «dados pessoais conservados» os dados pessoais cujo teor o operador comercial responsável pela gestão de informações pessoais pode divulgar, corrigir, acrescentar ou suprimir, pôr termo à respetiva utilização, eliminar ou deixar de transmitir a terceiros, e que não sejam considerados pelo decreto ministerial como suscetíveis de prejudicar o interesse público ou outros interesses se a sua presença ou ausência for divulgada, ou aqueles que se destinem a ser suprimidos no prazo máximo de um ano previsto pelo decreto ministerial.

Artigo 4.º do decreto ministerial

Em conformidade com o decreto ministerial, constituem «dados pessoais conservados» nos termos do artigo 2.º, n.º 7, os dados pessoais:

i) em relação aos quais haja a possibilidade, quando a presença ou ausência dos mesmos seja divulgada, de a vida, a integridade física ou o bem-estar do titular ou de um terceiro serem lesados;

ii) em relação aos quais haja a possibilidade, se a presença ou ausência dos mesmos for divulgada, de induzir ou incitar à prática de um ato ilícito ou injusto;

iii) em relação aos quais haja a possibilidade, se a presença ou ausência dos mesmos for divulgada, de comprometer a segurança nacional, destruir uma relação de confiança com um país estrangeiro ou organização internacional ou causar uma desvantagem em negociações com um país estrangeiro ou organização internacional;

iv) em relação aos quais haja a possibilidade, se a presença ou ausência dos mesmos for divulgada, de prejudicar a manutenção da segurança e da ordem públicas, designadamente a prevenção, a repressão ou a investigação de um crime.

Artigo 5.º do decreto ministerial

O prazo fixado pelo decreto ministerial nos termos do artigo 2.º, n.º 7, da Lei é de seis meses.

Os dados pessoais recebidos da UE com base numa decisão de adequação devem ser tratados como dados pessoais conservados, na aceção do artigo 2.º, n.º 7, da Lei, independentemente do prazo em que devam ser apagados.

Se os dados pessoais recebidos da UE com base numa decisão de adequação forem qualificados como dados pessoais considerados pelo decreto ministerial como «suscetíveis de prejudicar o interesse público ou outros interesses se a sua presença ou ausência for divulgada», não devem ser tratados como dados pessoais conservados (ver artigo 4.º do decreto ministerial; Orientações sobre as normas gerais, «2-7. Dados pessoais conservados»).

3. Definição de uma finalidade de utilização específica, restrições à finalidade de utilização (artigo 15.º, n.º 1, artigo 16.º, n.º 1, e artigo 26.º, n.os 1 e 3, da Lei)

Artigo 15.º, n.º 1, da Lei

1. No tratamento das informações pessoais, o operador comercial responsável pela gestão de informações pessoais deverá especificar o mais claramente possível a finalidade para que as mesmas são utilizadas («finalidade de utilização»).

Artigo 16.º, n.º 1, da Lei

1. O operador comercial responsável pela gestão de informações pessoais não pode tratar as informações sem antes ter obtido o consentimento do titular para além do necessário para atingir uma das finalidades de utilização especificadas nos termos do artigo anterior.

Artigo 26.º (n.os 1 e 3) da Lei

1. Quando receba dados pessoais de um terceiro, o operador comercial responsável pela gestão de informações pessoais deve confirmar os seguintes elementos, em conformidade com as normas estabelecidas pela Comissão de Proteção de Informações Pessoais. (omissão)

   i) (omissão)

   ii) as circunstâncias em que os referidos dados pessoais foram obtidos pelo terceiro

3. Após confirmar o disposto no n.º 1, o operador comercial responsável pela gestão de informações pessoais deve registar, em conformidade com as normas da Comissão de Proteção de Informações Pessoais, a data em que recebeu os dados pessoais, os elementos confirmados e os outros elementos prescritos pelas referidas normas.

Caso um operador comercial responsável pela gestão de informações pessoais trate informações pessoais para além do necessário para atingir uma das finalidades de utilização especificadas no artigo 15.º, n.º 1, da Lei, deve obter previamente o consentimento do titular (artigo 16.º, n.º 1). Quando receba dados pessoais de um terceiro, o operador comercial responsável pela gestão de informações pessoais deve, nos termos das normas, confirmar certos elementos, como as circunstâncias em que os referidos dados pessoais foram obtidos pelo terceiro, registando esses elementos (artigo 26.º, n.os 1 e 3, da Lei).

Quando um operador comercial responsável pela gestão de informações pessoais receba dados pessoais da UE com base numa decisão de adequação, as circunstâncias relativas à obtenção dos referidos dados devem ser confirmadas e registadas, como previsto no artigo 26.º, n.os 1 e 3, incluindo a finalidade de utilização para que os mesmos foram transferidos da UE.

Do mesmo modo, quando um operador comercial responsável pela gestão de informações pessoais receber, de outro operador comercial, dados pessoais previamente transferidos da UE com base numa decisão de adequação, as circunstâncias relativas à obtenção desses dados devem ser confirmadas e registadas, como previsto no artigo 26.º, n.os 1 e 3, incluindo a finalidade de utilização para que foram transferidos da UE.

Nos casos acima referidos, o operador comercial responsável pela gestão de informações pessoais deve indicar a finalidade da utilização dos referidos dados no âmbito da utilização para a qual foram inicialmente ou posteriormente transferidos, tal como confirmados e registados nos termos do artigo 26.º, n.os 1 e 3, utilizando os referidos dados unicamente para essa finalidade (artigo 15.º, n.º 1, e no artigo 16.º, n.º 1, da Lei).

4. Restrições à transferência para terceiros num país estrangeiro (artigo 24.º da Lei; artigo 11.º, n.º 2, das normas.

Artigo 24.º da Lei

Salvo nos casos previstos no n.º 1 do artigo anterior, o operador comercial responsável pela gestão de informações pessoais que transfira dados pessoais para um terceiro (com exceção da pessoa que cria o sistema em conformidade com as normas da Comissão de Proteção de Informações Pessoais, tal como necessário para, de forma contínua, adotar medidas equivalentes às que esses operadores devem tomar quanto ao tratamento de dados pessoais nos termos do presente artigo) situado num país estrangeiro (ou seja, num país ou região que se situe fora do território do Japão (com exceção das normas da Comissão de Proteção de Informações Pessoais que determinam que um determinado país estrangeiro possui um sistema de proteção da informações pessoais que reconhecidamente impõe normas equivalentes às do Japão no que se refere à proteção dos direitos e interesses de uma pessoa singular) deve obter previamente o consentimento do titular quanto à transferência desses dados para um terceiro que se encontre num país estrangeiro. Nesse caso, não é aplicável o disposto no artigo anterior.

Artigo 11.º, n.º 2, das normas

Os critérios fixados nas normas estabelecidas pela Comissão de Proteção de Informações Pessoais nos termos do artigo 24.º da Lei consideram-se satisfeitos quando:

i) o operador comercial responsável pela gestão de informações pessoais e a pessoa que recebe os dados pessoais asseguraram que o tratamento dos dados pessoais pela pessoa que os recebe implica a aplicação das medidas nos termos do Capítulo IV, secção 1, da Lei através de um método adequado e razoável;

ii) a pessoa que recebe os dados pessoais obteve um reconhecimento no âmbito do quadro internacional relativo ao tratamento de dados pessoais.

Caso decida fornecer a um terceiro que se encontre num país estrangeiro dados pessoais recebidos da UE com base numa decisão de adequação, o operador comercial responsável pela gestão de informações pessoais deve obter previamente o consentimento do titular quanto a essa transferência nos termos do artigo 24.º da Lei, após ter recebido informações sobre as circunstâncias em que essa transferência se processa necessárias para o titular poder tomar uma decisão quanto a esse consentimento, salvo nos casos previstos nas alíneas seguintes.

i) quando o terceiro em causa se encontre num país que as normas considerem como um país estrangeiro e que possui um sistema de proteção da informações pessoais que reconhecidamente impõe normas equivalentes às do Japão no que se refere à proteção dos direitos e interesses de uma pessoa singular);

ii) quando o operador comercial responsável pela gestão de informações pessoais e o terceiro que recebe os dados pessoais tiverem, no que se refere ao tratamento de dados pessoais por esse terceiro, adotado conjuntamente medidas que proporcionam um nível de proteção equivalente ao previsto na Lei, em articulação com as presentes normas, através de um método adequado e razoável (nomeadamente um contrato, outro tipo de acordo vinculativo ou qualquer acordo vinculativo no âmbito de um agrupamento de empresas);

iii) nos casos abrangidos por cada um dos elementos enumerados no artigo 23.º, n.º 1, da Lei.

5. Informações tratadas anonimamente (artigo 2.º, n.º 9, e artigo 36.º, n.ºs 1 e 2, da Lei)

Artigo 2.º, n.º 9, da Lei

9. Para efeitos da Lei, entende-se por «informações tratadas anonimamente» relativas a uma pessoa singular as informações obtidas a partir do tratamento de informações pessoais de uma forma que impeça a identificação de uma determinada pessoa mediante a adoção das medidas prescritas em cada uma das subalíneas seguintes, em conformidade com as diferentes categorias de informações pessoais estabelecidas em cada uma delas, e não permita a reconstituição das informações pessoais.

i) informações pessoais abrangidas pelo n.º 1, alínea i);

Supressão de uma parte das descrições constantes das referidas informações pessoais (incluindo a substituição das mesmas por outras descrições, utilizando um método sem regularidade que permita reconstituir essa parte das descrições)

ii) informações pessoais abrangidas pelo n.º 1, alínea ii);

Supressão de todos os códigos de identificação individuais constantes das referidas informações pessoais (incluindo a substituição dos mesmos por outras descrições, utilizando um método sem regularidade que permita reconstituir os referidos códigos de identificação individuais)

Artigo 36.º, n.º 1, da Lei

1. Quando produza informações tratadas anonimamente (apenas as que constituem uma base de dados de informações tratadas de forma anónima, etc.), o operador comercial responsável pela gestão de informações pessoais deve tratar as informações pessoais em conformidade com as normas que a Comissão de Proteção de Informações Pessoais considera necessárias para impedir a identificação de uma determinada pessoa singular e a reconstituição das informações pessoais utilizadas na sua produção.

Artigo 19.º das normas

As normas estabelecidas pela Comissão de Proteção de Informações Pessoais nos termos do artigo 36.º, n.º 1, da Lei preveem:

i) a supressão de parte ou da totalidade das descrições que permitem identificar determinada pessoa e que constam das informações pessoais (incluindo a sua substituição por outras, utilizando um método sem regularidade que permita reconstituir essas descrições na totalidade ou em parte);

ii) a supressão de todos os códigos de identificação individuais contidos nas informações pessoais (incluindo a sua substituição por outras descrições, utilizando um método sem regularidade que permita reconstituir os referidos códigos de identificação individuais);

iii) a supressão dos referidos códigos (unicamente os que estabelecem ligações entre informações e que sejam efetivamente tratados por um operador comercial responsável pela gestão de informações pessoais) que permitam estabelecer uma ligação entre as informações pessoais e as resultantes de intervenções operadas sobre estas (nomeadamente substituindo os referidos códigos por outros que não permitam associar essas informações pessoais às resultantes de intervenções operadas sobre estas, utilizando um método sem regularidade que permita reconstituir esses códigos);

iv) a supressão das descrições idiossincráticas (incluindo a sua substituição por outras descrições, mediante a utilização de um método sem regularidade que permita reconstituir as descrições idiossincráticas);

v) para além das medidas previstas nas alíneas anteriores, a adoção das medidas adequadas com base na análise das características, das bases de dados de informações pessoais, como a diferença entre descrições, etc., contidas em informações pessoais e descrições, contidas noutras informações pessoais que constituem bases de dados pessoais que incluam as referidas informações pessoais.

Artigo 36.º, n.º 2, da Lei

1. Quando produza informações tratadas anonimamente, o operador comercial responsável pela gestão de informações pessoais deve, nos termos das normas prescritas pela Comissão de Proteção de Dados Pessoais, adotar as medidas necessárias para prevenir a fuga de informações relativas a essas descrições ou aos códigos de identificação individuais eliminados das informações pessoais utilizados para produzir as informações tratadas anonimamente, assim como as informações relativas ao método de tratamento, em conformidade com o disposto no número anterior, adotando medidas para garantir a segurança dessas informações.

Artigo 20.º das normas

As normas estabelecidas pela Comissão de Proteção de Informações Pessoais nos termos do artigo 36.º, n.º 2, da Lei preveem:

i) a definição inequívoca dos poderes e responsabilidades da pessoa que trata as informações relativas às descrições e aos códigos de identificação individuais suprimidos das informações pessoais utilizadas para produzir as informações tratadas anonimamente, bem como informação relativa ao método de tratamento utilizado, nos termos do disposto no artigo 36.º, n.º 1 (unicamente as informações que permitem reconstituir as informações pessoais através dessas informações conexas).

ii) o estabelecimento de regras e procedimentos quanto às «informações relativas ao método de tratamento», o método de tratamento adequado, as informações conexas nos termos das regras e procedimentos, a avaliação do tratamento realizado e com base nos resultados dessa avaliação, a adoção das medidas necessárias para introduzir melhorias.

iii) adoção das medidas necessárias e adequadas para impedir que uma pessoa não autorizada possa tratar informações relativas ao método de tratamento.

As informações pessoais recebidas da UE com base numa decisão de adequação só podem ser consideradas «informações tratadas anonimamente», na aceção do artigo 2.º, n.º 9, da Lei, se o operador comercial responsável pela gestão de informações pessoais adotar medidas que tornem a desidentificação da pessoa singular irreversível para qualquer pessoa, incluindo através do apagamento das informações relativas ao método de tratamento [ou seja, as informações relativas a essas descrições e códigos de identificação individuais que foram suprimidas das informações pessoais utilizadas para produzir as informações tratadas anonimamente e as informações relativas ao método de tratamento, nos termos do artigo 36.º, n.º 1, da Lei (unicamente as que permitam reconstituir as informações pessoais através da utilização dessas informações relacionadas)].

ANEXO 2

Sua Excelência, Věra Jourová, Comissária da Justiça, Consumidores e Igualdade de Género da Comissão Europeia

Excelência,

Congratulo-me com os debates construtivos entre o Japão e a Comissão Europeia com vista ao estabelecimento de um quadro para a transferência mútua de dados pessoais entre o Japão e a UE.

Na sequência do pedido formulado pela Comissão Europeia ao Governo do Japão, tenho a honra de enviar em anexo um documento que apresenta uma panorâmica do quadro jurídico relativo ao acesso à informação por parte do Governo do Japão.

O referido documento diz respeito a diversos ministérios e agências do Governo do Japão: Quanto ao seu teor, os ministérios e agências competentes (Secretariado do Gabinete, Agência Nacional de Polícia, Comissão de Proteção da Informação Pessoal, Ministério dos Assuntos Internos e das Comunicações, Ministério da Justiça, Agência de Informações em matéria de Segurança Pública, Ministério da Defesa) são responsáveis pelas passagens no âmbito das respetivas competências. São seguidamente indicados os ministérios e agências competentes, assim como as respetivas assinaturas.

A Comissão de Proteção da Informação Pessoal aceita quaisquer perguntas quanto a este documento e coordenará as respostas necessárias entre os ministérios e agências competentes.

Espero que este documento seja útil para a tomada de decisões no âmbito da Comissão Europeia.

Muito agradeço o seu grande contributo até à data nesta matéria.

Queira aceitar, Senhora Comissária, os protestos da minha mais elevada consideração,

Yoko Kamikawa

Ministra da Justiça

O presente documento foi elaborado pelo Ministério da Justiça e pelos ministérios e agências competentes.

Koichi Hamano

Conselheiro, Secretariado do Gabinete

Schunichi Kuryu

Comissário-geral da Agência Nacional de Polícia

Mari Sonoda

Secretária-geral da Comissão de Proteção da Informação Pessoal

Mitsuru Yasuda

Vice-ministro, Ministério dos Assuntos Internos e das Comunicações

Seimei Nakagawa

Agência de Informações em matéria de Segurança Pública

Kenichi Takahashi

Vice-ministro administrativo da Defesa

14 de setembro de 2018

Recolha e utilização de informações pessoais pelas autoridades públicas japonesas para efeitos de aplicação da lei penal e de segurança nacional

O documento que se segue apresenta uma panorâmica do quadro jurídico para a recolha e utilização de informações (eletrónicas) pessoais pelas autoridades públicas japonesas para efeitos de aplicação da lei penal e de segurança nacional (a seguir designado «acesso governamental»), em especial no que diz respeito às bases jurídicas disponíveis, às condições (limitações) aplicáveis e às salvaguardas, incluindo o controlo independente e as possibilidades de reparação individual. A presente declaração é dirigida à Comissão Europeia com vista a expressar o compromisso e a garantia de que o acesso governamental às informações pessoais transferidas da UE para o Japão será limitado ao necessário, proporcionado e sujeito a um controlo independente, e que as pessoas em causa poderão obter reparação em caso de violação do seu direito fundamental à privacidade e à proteção de dados. A presente declaração ilustra igualmente a criação de um novo mecanismo de reparação, gerido pela Comissão de Proteção de Informações Pessoais (PPC), para tratar as reclamações de cidadãos da UE relativas ao acesso governamental aos seus dados pessoais transferidos da UE para o Japão.

I. **Princípios gerais do direito aplicáveis ao acesso governamental**

Enquanto exercício da autoridade pública, o acesso governamental só pode ter lugar no pleno respeito pela lei (princípio da legalidade). No Japão, as informações pessoais são protegidas tanto no setor privado como no setor público através de um mecanismo com vários níveis.

A. Enquadramento constitucional e princípio da reserva da lei

O artigo 13.º da Constituição e a jurisprudência reconhecem o direito à privacidade como um direito constitucional. A este respeito, o Supremo Tribunal declarou que é natural que as pessoas não queiram que terceiros conheçam as suas informações pessoais sem uma razão válida, e que esta expectativa deve ser protegida [1]. Outras proteções estão consagradas no artigo 21.º, n.º 2, da Constituição, que garante o respeito pelo sigilo das comunicações, e no artigo 35.º da Constituição, que garante o direito de não ser objeto de busca e apreensão sem mandado, o que significa que a recolha de informações pessoais, incluindo o acesso por meios coercivos, deve sempre basear-se num mandado judicial. Tal mandado só pode ser emitido para a investigação de um crime já cometido. Por conseguinte, no quadro jurídico do Japão, não é permitida a recolha de informações por meios coercivos para efeitos de segurança nacional (e não de uma investigação criminal).

Além disso, em conformidade com o princípio da reserva da lei, a recolha coerciva de informações deve ser especificamente autorizada por lei. No caso da recolha não coerciva/voluntária, as informações são obtidas a partir de uma fonte que pode ser livremente consultada ou recebida com base num pedido de divulgação voluntária, ou seja, um pedido que não pode executado contra a pessoa singular ou coletiva detentora da informação. No entanto, tal só é admissível na medida em que a autoridade pública for competente para realizar a investigação, dado que cada autoridade pública só pode atuar no âmbito das suas competências administrativas previstas na lei (independentemente do facto de as suas atividades interferirem ou não com os direitos e liberdades das pessoas singulares). Este princípio aplica-se à capacidade da autoridade de recolher informações pessoais.

B. Regras específicas em matéria de proteção de informações pessoais

A Lei relativa à proteção de informações pessoais («APPI») e a Lei relativa à proteção de informações pessoais na posse de órgãos administrativos («APPIHAO»), que se baseiam e dão execução a disposições constitucionais, garantem o direito à informação pessoal, tanto no setor privado como no público.

O artigo 7.º da APPI estabelece que a PPC formulará a «Política de base em matéria de proteção das informações pessoais» («Política de base»). A referida política, adotada através de uma decisão do Conselho de Ministros do Japão enquanto órgão central do Governo japonês (Primeiro-Ministro e Ministros de Estado), define as orientações para a proteção das informações pessoais no Japão. Deste modo, a PPC, enquanto autoridade de controlo independente, serve de «centro de comando» do sistema de proteção de informações pessoais do Japão.

Sempre que os órgãos administrativos recolhem informações pessoais, independentemente de o fazerem por meios coercivos ou não coercivos, têm, em princípio [2], de cumprir os requisitos estipulados na APPIHAO. A APPIHAO é uma lei geral aplicável ao tratamento de «informações pessoais conservadas» [3] por «órgãos administrativos» (tal como definido no artigo 2.º, n.º 1, da APPIHAO). Por conseguinte, abrange igualmente o tratamento de dados no domínio da

[1] Supremo Tribunal, Acórdão de 12 de setembro de 2003 [2002 (Ju) n.º 1656].

[2] Quanto às exceções relativas ao capítulo 4 da APPIHAO, ver ponto 16.

[3] Por «informações pessoais conservadas» no artigo 2.º, n.º 5, da APPIHAO, entendem-se as informações pessoais preparadas ou obtidas por um funcionário de um órgão administrativo no âmbito das suas funções e detidas por esse órgão administrativo para utilização organizacional pelos seus funcionários.

aplicação do direito penal e da segurança nacional. Entre as autoridades públicas autorizadas a dar execução ao acesso governamental, todas as autoridades, com exceção da polícia distrital, são autoridades governamentais nacionais que se enquadram na definição de «órgãos administrativos». O tratamento de informações pessoais pela polícia distrital é regido por portarias distritais ([4]) que estabelecem os princípios para a proteção de informações pessoais, direitos e obrigações equivalentes aos da APPIHAO.

II. **Acesso governamental para fins de aplicação do direito penal**

A) Bases jurídicas e limitações

1) Recolha de informações pessoais por meios coercivos

a) Bases jurídicas

Em conformidade com o artigo 35.º da Constituição, o direito de todas as pessoas à inviolabilidade do seu domicílio, documentos e haveres contra entradas, buscas e apreensões não pode ser comprometido, salvo mediante um mandado emitido por uma «justificação suficiente» e, em especial descrevendo o lugar a pesquisar e as coisas a apreender. Por conseguinte, a recolha coerciva de informações eletrónicas pelas autoridades públicas no contexto de uma investigação criminal só pode ter lugar com base num mandado. Tal aplica-se tanto à recolha de registos eletrónicos que contenham informações (pessoais) como à interceção de comunicações em tempo real (as chamadas escutas telefónicas). A única exceção a esta regra (que, no entanto, não é relevante no contexto da transferência eletrónica de dados pessoais do estrangeiro) é o artigo 220.º, n.º 1, do Código de Processo Penal ([5]), segundo o qual um procurador, um procurador adjunto ou um agente da polícia judiciária podem, ao deter um suspeito ou um «infrator em flagrante», proceder, se necessário, à busca e à apreensão «no local no momento da detenção».

O artigo 197.º, n.º 1, do Código de Processo Penal, estabelece que «não serão aplicadas medidas coercivas a menos que tenham sido definidas disposições especiais neste código». No que diz respeito à recolha coerciva de informações eletrónicas, as bases jurídicas pertinentes neste domínio são o artigo 218.º, n.º 1, do Código de Processo Penal (segundo o qual, o procurador, procurador adjunto ou agente da polícia judiciária pode, se necessário para a investigação de uma infração, efetuar uma busca, apreensão ou inspeção mediante mandado emitido por um juiz) e o artigo 222.º, n.º 2, do Código de Processo Penal (segundo o qual, as medidas coercivas para a interceção de comunicações eletrónicas sem o consentimento de uma das partes devem ser executadas com base noutros atos). Esta última disposição remete para a Lei das Escutas para efeitos de investigação criminal («Lei das Escutas»), que, no artigo 3.º, n.º 1, estabelece as condições em que as comunicações relativas a determinados crimes graves podem ser escutadas com base num mandado emitido por um juiz. ([6])

No que diz respeito à polícia, o poder de investigação compete em todos os casos à polícia distrital, dado que a Agência Nacional de Polícia (NPA) não efetua investigações criminais com base no Código de Processo Penal.

b) Limitações

A recolha coerciva de informações eletrónicas é limitada pela Constituição e pelos atos de atribuição de competências, tal como interpretados pela jurisprudência, que estabelece, nomeadamente, os critérios a aplicar pelos tribunais na emissão de um mandado. Além disso, a APPIHAO impõe uma série de limitações aplicáveis à recolha e ao tratamento da informação (embora as portarias locais reproduzam essencialmente os mesmos critérios aplicáveis à polícia distrital).

1. Limitações decorrentes da Constituição e do ato de atribuição de competências

Nos termos do artigo 197.º, n.º 1, do Código de Processo Penal, não serão aplicadas medidas coercivas a menos que tenham sido definidas disposições especiais neste código. O artigo 218.º, n.º 1, do Código de Processo Penal estabelece que a apreensão, etc., só pode ser efetuada com base num mandado emitido por um juiz «se tal for necessário para a

([4]) Cada distrito tem a sua própria «portaria distrital» aplicável à proteção das informações pessoais pela polícia distrital. Não existem traduções destas portarias distritais.

([5]) O artigo 220.º, n.º 1, do Código de Processo Penal prevê que, quando um procurador, um procurador adjunto ou um agente da polícia judiciária detêm um suspeito, podem, se necessário, tomar as seguintes medidas: a) Entrada na residência de outra pessoa, etc., para procurar o suspeito; b) Busca, apreensão ou inspeção no local no momento da detenção.

([6]) Mais especificamente, esta disposição prevê que «o procurador ou a polícia judiciária podem, nos casos abrangidos por qualquer dos seguintes travessões, quando existam indícios suficientes para suspeitar que se realizarão comunicações sobre compromissos, preparativos, conspirações relativas a ações posteriores como a eliminação de provas, etc., instruções e outras intercomunicações relativas ao crime contemplado em cada um dos referidos travessões (a seguir denominados "séries de crimes" no segundo e terceiro travessões), bem como comunicações que contenham elementos relacionados com o referido crime (a seguir denominadas "comunicações relacionadas com o crime" neste número) e nos casos em que é extremamente difícil identificar o autor do crime ou clarificar as situações ou os elementos da prática de um crime por qualquer outro meio, escutar comunicações relacionadas com o crime, com base num mandado de um juiz relativo a um meio de comunicação especificado por número de telefone e outros números ou códigos para identificar a fonte ou o destinatário do telefone que seja utilizado pelo suspeito de acordo com o contrato com empresas prestadoras de serviços de telecomunicações, etc. (exceto as que podem considerar-se não suspeitas de ser utilizadas como "comunicações relacionadas com o crime"), ou as em que existam motivos para suspeitar que estão a ser utilizadas como "comunicações relacionadas com o crime", poderão realizar-se escutas telefónicas das comunicações relacionadas com o crime».

investigação de um crime». Embora os critérios de apreciação da necessidade não estejam especificados em mais pormenor no direito, o Supremo Tribunal ([7]) decidiu que, ao avaliar a necessidade das medidas, o juiz deve efetuar uma avaliação global, tendo em conta, nomeadamente, os seguintes elementos:

a) Gravidade do crime e forma como foi cometido;

b) Valor e importância do material apreendido como elementos de prova;

c) Probabilidade de ocultação ou destruição do material apreendido;

d) Extensão das desvantagens causadas por uma apreensão;

e) Outras circunstâncias conexas.

As limitações decorrem também do requisito constante do artigo 35.º da Constituição relativo a uma «justificação suficiente». Ao abrigo da cláusula «justificação suficiente», podem ser emitidos mandados, quando: [1] existe a necessidade de uma investigação criminal (ver acórdão do Supremo Tribunal de 18 de março de 1969 (1968 (Shi) n.º 100), acima mencionado), [2] existe uma situação em que se considera que o suspeito (o arguido) cometeu um crime (artigo 156.º, n.º 1, das Regras de Processo Penal) ([8])[3] o mandado de investigação relativo a buscas corporais, haveres, à residência ou a qualquer outro local de uma pessoa que não seja o arguido só pode ser emitido se for razoável presumir que existam elementos que devem ser apreendidos (artigo 102.º, n.º 2, do Código de Processo Penal). Quando um juiz considerar que as provas documentais apresentadas pelas autoridades de investigação revelam fundamentos insuficientes para suspeitar de um crime, indefere o pedido de mandado. Deve observar-se, a este respeito, que, nos termos da Lei relativa à repressão do crime organizado e ao controlo dos produtos do crime, os «atos preparatórios para cometer» um crime planeado (por exemplo, preparação de dinheiro para cometer um crime de terrorismo) constituem, por si só, um crime, podendo, por conseguinte, ser objeto de investigação coerciva com base num mandado.

Por último, se o mandado disser respeito a buscas corporais, haveres, à residência ou a qualquer outro local de uma pessoa que não seja o suspeito ou o arguido, este só pode ser emitido se for razoável presumir que existem elementos que devem ser apreendidos (artigo 102.º, n.º 2, e artigo 222.º, n.º 1, do Código de Processo Penal).

No que diz respeito especificamente à interceção de comunicações para efeitos de investigações criminais com base na Lei das Escutas, tal só pode ser efetuada quando estiverem preenchidos os requisitos estritos previstos no artigo 3.º, n.º 1. De acordo com esta disposição, a interceção exige sempre um mandado judicial prévio, que só pode ser emitido em situações restritas ([9]).

2. Limitações decorrentes da APPIHAO

No que diz respeito à recolha ([10]) e ao tratamento posterior (incluindo, nomeadamente, a conservação, gestão e utilização) de informações pessoais pelos órgãos administrativos, a APPIHAO prevê as seguintes limitações:

a) De acordo com o artigo 3.º, n.º 1, da APPIHAO, os órgãos administrativos só podem conservar informações pessoais quando tal for necessário ao exercício das funções que lhe competem, em conformidade com as disposições legislativas e regulamentares. Em caso de conservação, devem também especificar (tanto quanto possível) finalidade da utilização das informações pessoais. Nos termos do artigo 3.º, n.ºs 2 e 3, da APPIHAO, os órgãos administrativos não devem conservar informações pessoais para além do âmbito necessário para a consecução da finalidade da utilização especificada, não devendo alterar essa finalidade para além do que possa ser razoavelmente considerado adequado para a finalidade inicial.

b) O artigo 5.º da APPIHAO estabelece que o responsável por um órgão administrativo deve esforçar-se por manter as informações pessoais conservadas de forma a que estas se mantenham exatas e atualizadas e dentro do âmbito necessário para atingir a finalidade da utilização.

c) O artigo 6.º, n.º 1, da APPIHAO prevê que o responsável por um órgão administrativo tome as medidas necessárias para evitar fugas, perdas ou danos dos dados, bem como para a gestão adequada das informações pessoais conservadas.

d) De acordo com o artigo 7.º da APPIHAO, nenhum funcionário (incluindo os antigos funcionários) deve divulgar as informações pessoais obtidas a qualquer outra pessoa sem um motivo fundamentado ou utilizá-las para uma finalidade injusta.

([7]) Acórdão de 18 de março de 1969 (1968 (Shi) n.º 100).
([8]) O artigo 156.°, n.º 1, das Regras de Processo Penal, estabelece: «No preenchimento do pedido previsto no n.º 1 do artigo anterior, o requerente deve fornecer elementos com base nos quais se considere que o suspeito ou arguido cometeu o crime.»
([9]) Ver nota 6.
([10]) O artigo 3.º, n.ºs 1 e 2, da APPIHAO limita o âmbito da conservação e, por conseguinte, também da recolha de informações pessoais.

e) Além disso, o artigo 8.º, n.º 1, da APPIHAO estabelece que o responsável por um órgão administrativo não deve, salvo disposição legislativa ou regulamentar em contrário, utilizar ou prestar a outra pessoa informações pessoais conservadas para uma finalidade diferente da especificada. Embora o artigo 8.º, n.º 2, contenha exceções a esta regra em situações específicas, tais exceções aplicam-se apenas se essa divulgação excecional não for suscetível de causar «prejuízos injustos» aos direitos e interesses do titular dos dados em causa ou de um terceiro.

f) De acordo com o artigo 9.º da APPIHAO, sempre que forem prestadas informações pessoais a outra pessoa, o responsável pelo órgão administrativo em causa deve, se necessário, impor restrições quanto à finalidade ou ao método de utilização, ou quaisquer outras restrições que se mostrem necessárias; pode também solicitar à pessoa que recebe as informações que tome as medidas necessárias para evitar fugas e para a correta gestão da informação.

g) O artigo 48.º da APPIHAO estabelece que o responsável de um órgão administrativo deve esforçar-se por tratar de forma adequada e expedita todas as reclamações relativas ao tratamento de informações pessoais.

2) Recolha de informações pessoais através de pedidos de cooperação voluntária (investigação voluntária)

a) Base jurídica

Para além da utilização de meios coercivos, as informações pessoais podem ser obtidas a partir de uma fonte livremente consultada ou ser divulgadas voluntariamente, nomeadamente por parte dos operadores comerciais que as detêm.

No que diz respeito a este último caso, o artigo 197.º, n.º 2, do Código de Processo Penal confere poderes ao Ministério Público e à polícia judiciária para realizar «inquéritos por escrito sobre questões relativas à investigação» (as chamadas «fichas de inquérito»). Ao abrigo do Código de Processo Penal, as pessoas investigadas são convidadas a informar as autoridades de investigação. No entanto, não existe qualquer forma de as obrigar a informar as autoridades, se os serviços públicos e/ou as organizações privadas objeto dos inquéritos se recusarem a responder. Se não responderem aos inquéritos, não podem ser aplicadas quaisquer sanções penais ou de outro tipo. Se as autoridades de investigação considerarem as informações solicitadas indispensáveis, terão de as obter através de busca e apreensão com base num mandado judicial.

Perante a consciencialização crescente entre as pessoas singulares quanto aos seus direitos de privacidade, juntamente com a carga de trabalho decorrente destes pedidos, os operadores comerciais são cada vez mais cautelosos nas suas respostas aos mesmos ([11]). Ao decidirem cooperar, os operadores comerciais, em especial, têm em conta a natureza das informações solicitadas, a sua relação com a pessoa cuja informação está em jogo, os riscos para a sua reputação, os riscos de litígio, etc.

b) Limitações

No que diz respeito à recolha coerciva de informações eletrónicas, a investigação voluntária é limitada pela Constituição, tal como interpretada pela jurisprudência, e pelo ato de atribuição de competências. Além disso, os operadores comerciais não estão legalmente autorizados a divulgar informações em determinadas situações. Por último, a APPIHAO estabelece uma série de limitações aplicáveis à recolha e ao tratamento das informações (embora as portarias locais reproduzam essencialmente os mesmos critérios aplicáveis à polícia distrital).

1. Limitações decorrentes da Constituição e do ato de atribuição de competências

Ao ter em conta o objetivo do artigo 13.º da Constituição, o Supremo Tribunal em duas decisões de 24 de dezembro de 1969 (1965 (A) n.º 1187) e de 15 de abril de 2008 (2007 (A) n.º 839) impôs limites aos inquéritos voluntários efetuados pelas autoridades de investigação. Embora estas decisões se refiram a casos em que as informações pessoais (sob a forma de imagens) foram recolhidas através de fotografias/filmagens, as conclusões são relevantes para os inquéritos voluntários (não coercivos) que interferem na vida privada de uma pessoa em geral. Por conseguinte, são aplicáveis e têm de ser cumpridas no que diz respeito à recolha de informações pessoais através de um inquérito voluntário, tendo em conta as circunstâncias específicas de cada caso.

De acordo com essas decisões, a legalidade do inquérito voluntário depende do cumprimento de três critérios, a saber:

— «suspeita de um crime» (ou seja, deve apreciar-se se foi cometido um crime);

— «necessidade de investigação» (ou seja, deve apreciar-se se o pedido permanece dentro do âmbito necessário para efeitos da investigação); e

([11]) Ver também a notificação emitida pela Agência Nacional de Polícia em 7 de dezembro de 1999 (infra p. 9) que indica a mesma situação.

— «adequação dos métodos» (ou seja, deve apreciar-se se o inquérito voluntário é «adequado» ou razoável para atingir o objetivo da investigação) ([12]).

Em geral, tendo em conta os três critérios acima referidos, a legalidade do inquérito voluntário é apreciada no sentido de poder ou não ser considerada razoável em conformidade com as convenções socialmente aceites.

O requisito de o inquérito ser «necessário» também decorre diretamente do artigo 197.º do Código de Processo Penal e foi confirmado nas instruções emitidas pela Agência Nacional de Polícia para a polícia distrital no que se refere à utilização de «fichas de inquérito». A notificação da Agência Nacional de Polícia de 7 de dezembro de 1999 estabelece uma série de limitações processuais, incluindo a obrigação de utilizar «fichas de inquérito» apenas se tal se revelar necessário para efeitos da investigação. Além disso, o artigo 197.º, n.º 1, do Código de Processo Penal está limitado às investigações penais, pelo que só pode ser aplicado em caso de suspeita concreta de um crime já cometido. Em contrapartida, esta base jurídica não é aplicável à recolha e utilização de informações pessoais nos casos em que ainda não tenha ocorrido qualquer violação da lei.

2. Limitações relativas a certos operadores comerciais

São aplicáveis limitações adicionais em certos domínios, com base na proteção prevista noutras leis.

Em primeiro lugar, as autoridades de investigação, bem como os operadores de telecomunicações que detêm informações pessoais têm o dever de respeitar o sigilo das comunicações, tal como garantido pelo artigo 21.º, n.º 2, da Constituição ([13]). Além disso, os operadores de telecomunicações têm o mesmo dever ao abrigo do artigo 4.º da Lei relativa às atividades de telecomunicações ([14]). De acordo com as «Orientações sobre proteção das informações pessoais na atividade de telecomunicações», que foram emitidas pelo Ministério dos Assuntos Internos e das Comunicações com base na Constituição e na Lei relativa às atividades de telecomunicações, nos casos em que está em causa o sigilo das comunicações, os operadores de telecomunicações não devem divulgar a terceiros informações pessoais sobre o sigilo da comunicação, exceto se tiverem obtido o consentimento da pessoa em causa ou se puderem invocar uma das «causas justificáveis» para não dar cumprimento ao Código Penal. Tais causas referem-se a «atos justificáveis» (artigo 35.º do Código Penal), «autodefesa» (artigo 36.º do Código Penal) e «neutralização de perigo imediato» (artigo 37.º do Código Penal). Os «atos justificáveis» ao abrigo do Código Penal são unicamente os atos do operador de telecomunicações que dão cumprimento a medidas obrigatórias do Estado, com exceção do inquérito voluntário. Por conseguinte, se as autoridades de investigação solicitarem informações pessoais com base numa «ficha de inquérito» (artigo 197.º, n.º 2, do Código de Processo Penal), os operadores de telecomunicações estão proibidos de divulgar os dados.

Em segundo lugar, os operadores comerciais são obrigados a recusar pedidos de cooperação voluntária nos casos em que a lei os proíbe de divulgar informações pessoais. A título de exemplo, tal inclui os casos em que o operador tem o dever de respeitar a confidencialidade das informações, por exemplo, nos termos do artigo 134.º do Código Penal ([15]).

3. Limitações com base na APPIHAO

No que diz respeito à recolha e ao tratamento posterior das informações pessoais pelos órgãos administrativos, a APPIHAO prevê limitações, tal como acima explicado na secção II.A.1), alínea b), (2). As limitações equivalentes decorrem das portarias distritais aplicáveis à polícia distrital.

B) Controlo

1) Controlo judicial

No que diz respeito à recolha de informações pessoais através de meios coercivos, esta deve basear-se num mandado ([16]), estando, por conseguinte, sujeita ao exame prévio de um juiz. No caso de a investigação ser ilegal, um juiz pode excluir essas provas no processo penal subsequente. Uma pessoa pode solicitar essa exclusão no seu processo penal, alegando que a investigação era ilegal.

([12]) A gravidade do crime e a urgência são fatores relevantes para avaliar a «adequação dos métodos».

([13]) O artigo 21.º, n.º 2, da Constituição estabelece: «Não pode ser exercida qualquer censura nem violado o sigilo das comunicações.»

([14]) O artigo 4.º da Lei relativa às atividades de telecomunicações estabelece o seguinte: «(1) O sigilo das comunicações geridas por uma empresa de telecomunicações não pode ser violado. (2) As pessoas que exerçam uma atividade de telecomunicações não podem divulgar os segredos obtidos durante o exercício das suas funções no que diz respeito às comunicações geridas pelas empresas de telecomunicações. O mesmo se aplica mesmo após essas pessoas terem cessado funções.»

([15]) O artigo 134.º do Código Penal estabelece: «(1) Quando um médico, farmacêutico, distribuidor farmacêutico, parteira, procurador, advogado, notário ou qualquer outra pessoa que anteriormente exerça uma das profissões acima referidas divulga, sem um motivo fundamentado, as informações confidenciais de outra pessoa obtidas no decurso do exercício da profissão, está sujeito a pena de prisão com possibilidade de prestação de trabalho por um período não superior a 6 meses ou a uma multa até 100 000 ienes. (2) O mesmo se aplica se uma pessoa que exerça ou tenha exercido uma atividade religiosa divulgar, sem motivo fundamentado, as informações confidenciais de outra pessoa obtidas no decurso dessas atividades religiosas.»

([16]) Relativamente à exceção a esta regra, ver nota 5.

2) Controlo com base na APPIHAO

No Japão, o ministro ou responsável por cada ministério ou agência tem autoridade de controlo e de execução coerciva com base na APPIHAO, enquanto o ministro dos Assuntos Internos e das Comunicações pode investigar a execução coerciva da APPIHAO por todos os outros ministérios.

Se o ministro dos Assuntos Internos e das Comunicações – com base, por exemplo, na investigação relativa ao estado da execução coerciva da APPIHAO ([17]), no tratamento de reclamações ou de investigações dirigidas a um dos seus centros de informações globais – o considerar necessário para atingir o objetivo da APPIHAO, pode solicitar ao responsável por um órgão administrativo que apresente materiais e explicações relativamente ao tratamento dado às informações pessoais em causa, com base no artigo 50.º da APPIHAO. O ministro pode formular pareceres dirigidos ao responsável pelo órgão administrativo sobre o tratamento de informações pessoais sempre que o considere necessário para a realização dos objetivos dessa lei. Pode, além disso, solicitar, por exemplo, uma revisão das medidas através das ações que possa empreender nos termos dos artigos 50.º e 51.º da lei, quando suspeite que ocorreu uma infração ou uma aplicação incorreta do referido ato, o que contribui para assegurar a aplicação uniforme e o cumprimento da APPIHAO.

3) Controlo pelas comissões de segurança pública no que respeita à polícia

No que diz respeito à administração da polícia, a Agência Nacional de Polícia está sujeita ao controlo da Comissão Nacional de Segurança Pública, enquanto a polícia distrital está sujeita ao controlo de uma das comissões distritais de segurança pública estabelecidas em cada distrito. Cada um destes organismos de controlo assegura a gestão democrática e a neutralidade política da administração da polícia.

A Comissão Nacional de Segurança Pública é responsável pelos assuntos sob a sua jurisdição nos termos da lei da polícia e de outras leis. Tal inclui a nomeação do comissário geral da Agência Nacional de Polícia e dos quadros superiores da polícia local, bem como a definição de políticas globais que estabelecem orientações de base ou medidas relativas à administração da Agência Nacional de Polícia.

As comissões distritais de segurança pública são compostas por membros que representam a população do respetivo distrito com base na Lei da Polícia e gerem a polícia distrital como um conselho independente. Os membros são nomeados pelo governador distrital com o consentimento da assembleia distrital, com base no artigo 39.º da Lei da Polícia. O seu mandato é de três anos e só podem ser demitidos contra a sua vontade por motivos específicos enumerados na lei (por exemplo, incapacidade para o exercício das suas funções, incumprimento do dever, má conduta, etc.), o que garante a sua independência (ver artigos 40.º e 41.º da Lei da Polícia). Além disso, a fim de garantir a sua neutralidade política, o artigo 42.º da Lei da Polícia proíbe que um membro da comissão se torne membro de um órgão legislativo, dirigente executivo de um partido político ou de qualquer outro organismo político, ou que participe ativamente em movimentos políticos. Embora cada comissão esteja sob a jurisdição do respetivo governador distrital, tal não implica nenhuma autoridade do governador para emitir instruções sobre o exercício das suas funções.

Nos termos do artigo 38.º, n.º 3, conjugado com os artigos 2.º e 36.º, n.º 2, da Lei da Polícia, incumbe às comissões distritais de segurança pública a «proteção dos direitos e liberdades das pessoas singulares». Para o efeito, recebem relatórios dos comandantes da polícia distrital relativamente às atividades sob a sua jurisdição, incluindo em reuniões regulares, realizadas três ou quatro vezes por mês. As comissões fornecem orientações sobre estas questões através do estabelecimento de políticas globais.

Além disso, no âmbito das suas funções de controlo, as comissões distritais de segurança pública podem emitir orientações para a polícia distrital relativamente a casos concretos quando o considerem necessário no contexto de uma inspeção das atividades da polícia distrital ou de uma conduta indevida do seu pessoal. As referidas comissões podem ainda, se o considerarem necessário, ter um membro designado da comissão que reveja o estado de execução da orientação emitida (artigo 43.º-2, da Lei da Polícia).

([17]) A fim de garantir a transparência e facilitar o controlo pelo Ministério dos Assuntos Internos e das Comunicações, os responsáveis por órgãos administrativos são obrigados, nos termos do artigo 11.º da APPIHAO, a registar todos os dados previstos no artigo 10.º, n.º 1, da APPIHAO, tais como o nome do órgão administrativo que conserva o ficheiro, a finalidade da utilização do mesmo, o método de recolha das informações pessoais, etc. (o denominado «Registo de informações pessoais»). No entanto, os ficheiros de informações pessoais abrangidos pelo artigo 10.º, n.º 2, da APPIHAO, como os preparados ou obtidos no âmbito de uma investigação criminal ou sobre matérias relevantes para a segurança nacional, estão isentos da obrigação de notificar o Ministério dos Assuntos Internos e das Comunicações e de inclusão no registo público. No entanto, nos termos do artigo 7.º da Lei sobre a gestão dos registos públicos e dos arquivos, os responsáveis pelos órgãos administrativos são sempre obrigados a registar a classificação, o título, o período de conservação e o local de armazenamento, etc., dos documentos administrativos («ficheiro de gestão dos documentos administrativos»). A catalogação das informações de ambos os registos é publicada na Internet e permite às pessoas verificar que tipo de informações pessoais está contido no ficheiro e que órgão administrativo conserva a informação.

4) Controlo parlamentar

As câmaras do Parlamento japonês (a Dieta) podem conduzir investigações relativas às atividades das autoridades públicas e, para o efeito, solicitar a apresentação de documentos e o depoimento de testemunhas (artigo 62.º da Constituição). Neste contexto, a comissão competente da Dieta pode examinar a adequação das atividades de recolha de informações conduzidas pela polícia.

Estas competências são especificadas de forma mais pormenorizada na Lei que rege o Parlamento. Nos termos do seu artigo 104.º, o Parlamento pode exigir que o Governo e os organismos públicos elaborem relatórios e registos necessários à investigação. Além disso, os membros da Dieta podem apresentar «inquéritos por escrito» nos termos do artigo 74.º da Lei que rege o Parlamento. Tais inquéritos têm de ser aprovados pelo Presidente da Câmara e, em princípio, devem receber uma resposta por escrito por parte do Governo no prazo de sete dias (quando for impossível responder dentro desse prazo, tal deve ser justificado, devendo ser fixado um novo prazo, segundo o artigo 75.º da Lei que rege o Parlamento). No passado, os inquéritos por escrito levados a cabo pela Dieta já abrangeram igualmente o tratamento de informações pessoais pela administração ([18]).

C) Vias de recurso individuais

Nos termos do artigo 32.º da Constituição do Japão, a ninguém pode ser negado o direito de acesso aos tribunais. Além disso, o artigo 17.º da Constituição garante a qualquer pessoa o direito de processar o Estado ou uma entidade pública para obter reparação (como previsto na lei) quando essa pessoa tenha sofrido danos provocados por uma ação ilegal de um funcionário público.

1) Vias de recurso judicial contra a recolha coerciva de informações com base num mandado (artigo 430.º do Código de Processo Penal)

Nos termos do artigo 430.º, n.º 2, do Código de Processo Penal, uma pessoa que não esteja satisfeita com as medidas tomadas por um agente da polícia relativamente a uma apreensão de bens (nomeadamente se tais bens contiverem informações pessoais) com base num mandado, pode apresentar um pedido ao tribunal competente para que essas medidas sejam «revogadas ou alteradas».

Esse recurso pode ser apresentado sem que a pessoa tenha de esperar pela conclusão do processo. Se o tribunal considerar que a apreensão dos bens era desnecessária, ou que existem outras razões para a considerar ilegal, pode ordenar a sua revogação ou alteração.

2) Vias de recurso judicial ao abrigo do Código de Processo Civil e da Lei relativa ao recurso contra o Estado

Se considerar que o seu direito à privacidade nos termos do artigo 13.º da Constituição foi violado, uma pessoa pode intentar uma ação civil solicitando a supressão das informações pessoais recolhidas para uma investigação criminal.

Além disso, uma pessoa pode intentar uma ação de indemnização por perdas e danos com base na Lei relativa ao recurso contra o Estado, em conjugação com os artigos pertinentes do Código Civil, caso considere que o seu direito à privacidade foi violado e que sofreu danos em resultado da recolha dos seus dados pessoais ou do controlo ([19]). Os «danos» que podem ser objeto de um pedido de indemnização não se limitam aos danos materiais (artigo 710.º do Código Civil), sendo igualmente abrangidos os danos morais sob forma de «angústia mental». O montante da indemnização por danos morais será avaliado pelo juiz com base numa «avaliação livre, tendo em conta os vários fatores de cada caso» ([20]).

O artigo 1.º, n.º 1, da Lei relativa ao recurso contra o Estado atribui um direito de indemnização, no caso de (i) um funcionário público, que exerça a autoridade pública do Estado, (ou de uma entidade pública) ter (ii) no exercício das suas funções, (iii) intencional ou negligentemente, ou (iv) ilegalmente causado danos a outra pessoa.

A pessoa deve intentar a ação judicial de acordo com o Código de Processo Civil. Segundo as regras aplicáveis, deve fazê-lo no tribunal competente do local em que a responsabilidade civil foi incorrida.

([18]) Ver, por exemplo, o inquérito por escrito da Câmara dos Conselheiros n.º 92, de 27 de março de 2009, relativo ao tratamento das informações recolhidas no âmbito de investigações criminais, incluindo violações de obrigações de confidencialidade pelas autoridades policiais e judiciárias.

([19]) Um exemplo dessa ação é o «Processo da lista da Agência de Defesa» [Tribunal de Niigata, decisão de 11 de maio de 2006 (2002 (Wa) n.º 514)]. Neste caso, um funcionário da Agência de Defesa elaborou, conservou e distribuiu uma lista das pessoas que apresentaram pedidos de divulgação de documentos administrativos detidos pela Agência de Defesa. Dessa lista constavam informações pessoais do requerente. Insistindo que a sua vida privada, o direito de conhecer, etc., tinham sido violados, o requerente solicitou o pagamento de uma indemnização por perdas e danos ao abrigo do artigo 1.º, n.º 1, da Lei relativa ao recurso contra o Estado. O pedido foi parcialmente deferido pelo tribunal que concedeu uma indemnização parcial ao requerente.

([20]) Supremo Tribunal, decisão de 5 de abril de 1910 (1910 (O) n.º 71).

3) Vias de recurso individual contra investigações ilegais/inadequadas efetuadas pela polícia: reclamação à Comissão Distrital da Segurança Pública (artigo 79.º Lei da Polícia)

Em conformidade com o artigo 79.º da Lei da Polícia ([21]), tal como precisado numa instrução dada pelo responsável da Agência Nacional de Polícia à polícia distrital e às comissões distritais de segurança pública ([22]), as pessoas podem apresentar uma reclamação por escrito ([23]) junto das comissões distritais de segurança pública contra qualquer conduta ilegal ou abusiva por parte de um agente da polícia no exercício das suas funções; tal inclui as obrigações no que diz respeito à recolha e utilização de informações pessoais. A Comissão deve proceder «fidedignamente» ao tratamento destas reclamações em conformidade com as leis e as portarias locais e notificar o reclamante por escrito dos seus resultados.

Com base na sua competência de controlo, em conformidade com o artigo 38.º, n.º 3, da Lei da Polícia, a comissão distrital de segurança pública emitirá instruções à polícia distrital para investigar os factos, aplicar as medidas necessárias em função dos resultados do exame e comunicar os resultados à comissão. Sempre que o considerar necessário, a comissão pode igualmente dar instruções sobre o tratamento da reclamação, por exemplo, se considerar que a investigação levada a cabo pela polícia é insuficiente. Este procedimento é descrito na comunicação da Agência Nacional de Polícia dirigida aos comandantes da polícia distrital.

A notificação dos resultados da investigação ao reclamante é feita igualmente em função dos relatórios da polícia sobre a investigação e das medidas tomadas a pedido da comissão.

4) Vias de recurso individuais ao abrigo da APPIHAO e do Código de Processo Penal

a) APPIHAO

Nos termos do artigo 48.º da APPIHAO, os órgãos administrativos devem esforçar-se por tratar, de forma correta e expedita, quaisquer reclamações quanto ao tratamento de informações pessoais. Como forma de prestar informações consolidadas às pessoas (por exemplo, sobre os direitos de divulgação, correção e suspensão da utilização dessas informações no âmbito da APPIHAO) e como ponto de contacto para os inquéritos, o Ministério dos Assuntos Internos e das Comunicações criou centros de informações globais sobre a divulgação de informações / proteção de informações pessoais em cada um dos distritos, com base no artigo 47.º, n.º 2, da APPIHAO. É igualmente possível realizar inquéritos junto de não residentes. A título de exemplo, no exercício financeiro de 2017 (abril de 2017 a março de 2018), o número total de casos em que os centros de informações globais responderam a inquéritos, etc., foi de 5186.

Os artigos 12.º e 27.º da APPIHAO reconhecem às pessoas singulares o direito de solicitar a comunicação e a correção das informações pessoais conservadas. Além disso, nos termos do artigo 36.º da APPIHAO, podem solicitar a suspensão da utilização ou a supressão dos dados pessoais conservados, caso o órgão administrativo não tenha obtido licitamente as informações pessoais conservadas, ou conserve ou utilize essas informações em violação da lei.

No entanto, no que diz respeito às informações pessoais recolhidas (com base num mandado ou através de uma «ficha de inquérito») e conservadas para investigações penais ([24]), essas informações são geralmente abrangidas pela categoria de «informações pessoais registadas nos documentos relativos a processos judiciais e materiais apreendidos». Por conseguinte, são excluídas do âmbito de aplicação dos direitos individuais no capítulo 4 do Código de Processo Penal, nos termos do artigo 53.º-2, do Código de Processo Penal ([25]). O tratamento desses dados pessoais e os direitos individuais de acesso e correção estão, em vez disso, sujeitos a regras especiais ao abrigo do Código de Processo Penal e da Lei relativa aos autos

([21]) Artigo 79.º da Lei da Polícia (excerto):
1. Qualquer pessoa que esteja insatisfeita com a forma como os agentes da polícia distrital exercem as suas funções pode apresentar uma reclamação por escrito à comissão distrital de segurança pública através do procedimento previsto na Portaria da Comissão Nacional de Segurança Pública.
2. A comissão distrital de segurança pública que receba uma reclamação nos termos do número anterior deve proceder fidedignamente à sua apreciação de acordo com a legislação e as portarias locais, informando por escrito o reclamante do resultado, exceto quando:
   1) a reclamação possa ser considerada como tendo sido apresentada com o intuito de impedir o exercício das funções da polícia distrital;
   2) a residência do reclamante seja desconhecida;
   3) A reclamação possa ser considerada como tendo sido apresentada juntamente com outros reclamantes tendo estes já sido notificados do resultado da reclamação conjunta.

([22]) Agência Nacional de Polícia, Comunicação sobre o tratamento adequado de reclamações relativas ao exercício das funções dos agentes de polícia, 13 de abril de 2001, com o anexo 1 «Normas de interpretação/execução do artigo 79.º da Lei da Polícia».

([23]) De acordo com a Comunicação da Agência Nacional de Polícia (ver nota anterior), as pessoas com dificuldades na formulação de uma reclamação por escrito poderão beneficiar de assistência. Tal inclui expressamente o caso dos estrangeiros.

([24]) Por outro lado, existem documentos que não são classificados como «documentos relacionados com processos», uma vez que não constituem informações obtidas através de um mandado ou de inquéritos por escrito sobre questões relacionadas com a investigação, mas criados com base nesses documentos. Tal sucede quando a informação privada não é abrangida pelo artigo 45.º, n.º 1, da APPIHAO e, por conseguinte, essa informação não é excluída da aplicação do capítulo 4 da APPIHAO.

([25]) O artigo 53.º-2, n.º 2, do Código de Processo Penal prevê que as disposições do capítulo IV da APPIHAO não se aplicam às informações pessoais registadas em documentos relacionados com processos judiciais e materiais apreendidos.

finais dos processos penais (ver infra) ([26]). Esta exclusão é justificada por vários fatores, tais como a proteção da vida privada das pessoas, o sigilo das investigações e a correta condução do processo penal. Dito isto, permanecem aplicáveis as disposições do capítulo 2 da APPIHAO que regula os princípios do tratamento de tais informações.

b) Código de Processo Penal

Nos termos do Código de Processo Penal, as possibilidades de acesso a informações pessoais recolhidas para efeitos de uma investigação criminal dependem tanto da fase do processo como do papel da pessoa na investigação (suspeito, arguido, vítima, etc.).

Em derrogação à regra prevista no artigo 47.º do Código de Processo Penal, segundo a qual os documentos relativos ao processo não devem ser tornados públicos antes do início do processo (uma vez que tal poderia violar a honra e/ou a privacidade das pessoas singulares em causa e prejudicar a investigação/processo), a inspeção dessas informações pela vítima de um crime é, em princípio, autorizada na medida em que seja considerada razoável tendo em conta o objetivo da disposição do artigo 47.º do Código de Processo Penal ([27]).

No que se refere aos suspeitos, serão normalmente informados do facto de serem objeto de uma investigação criminal após interrogatório pela polícia judiciária ou pelo Ministério Público. Se, posteriormente, o Ministério Público decidir não intentar uma ação penal, deve notificar imediatamente o suspeito desse facto, a seu pedido (artigo 259.º do Código de Processo Penal).

Além disso, na sequência de uma ação penal, o Ministério Público deve dar ao arguido ou ao seu advogado a possibilidade de consultar previamente os elementos de prova antes de solicitar o seu exame pelo tribunal (artigo 299.º do Código de Processo Penal), o que permite ao arguido verificar as suas informações pessoais recolhidas no quadro da investigação criminal.

Por último, a proteção das informações pessoais recolhidas no âmbito de uma investigação criminal, quer se trate de um suspeito, de um arguido ou de qualquer outra pessoa singular (por exemplo, uma vítima de um crime), é garantida pela obrigação de confidencialidade (artigo 100.º da Lei relativa ao Serviço Público Nacional) e pela imposição de sanções em caso de fuga de informações confidenciais tratadas no quadro do exercício dos deveres de serviço público (artigo 109.º, alínea xii), da Lei relativa ao Serviço Público Nacional).

5) Vias de recurso individuais face a investigações ilegais/inadequadas realizadas pelas autoridades públicas: reclamação junto da PPC

Em conformidade com o artigo 6.º da APPI, o Governo deve tomar as medidas necessárias, em colaboração com os governos de países terceiros, para criar um sistema de informações pessoais compatível com as normas internacionais, através da promoção da cooperação com organizações internacionais e outros quadros internacionais. Com base nesta disposição, a política de base em matéria de proteção das informações pessoais (adotada por decisão do Conselho de Ministros) delega na PPC, enquanto autoridade competente para a administração geral da APPI, poderes para tomar as medidas necessárias no sentido de ultrapassar as divergências dos sistemas e das operações entre o Japão e o país estrangeiro em causa, por forma a assegurar o tratamento adequado das informações pessoais provenientes desse país.

Além disso, tal como previsto no artigo 61.º, alíneas i) e ii), da APPI, a PPC é encarregada da formulação e promoção de uma política de base, bem como da mediação de reclamações apresentadas contra operadores comerciais. Por último, os órgãos administrativos devem comunicar e cooperar estreitamente entre si (artigo 80.º da APPI).

Com base nestas disposições, a PPC tratará das reclamações apresentadas por indivíduos, do seguinte modo:

a) Uma pessoa singular que suspeite que os seus dados transferidos da UE tenham sido recolhidos ou utilizados pelas autoridades públicas do Japão, incluindo as autoridades responsáveis pelas atividades referidas nos capítulos II e III da presente «declaração», em violação das regras aplicáveis, incluindo os que estão sujeitos a esta «declaração», pode apresentar uma reclamação junto da PPC (individualmente ou através da sua autoridade responsável pela proteção de dados).

b) A PPC trata a reclamação, exercendo nomeadamente os seus poderes ao abrigo do artigo 6.º, n.º 61, alínea ii), e do artigo 80.º da APPI, e informa da reclamação as autoridades públicas competentes, incluindo os organismos de controlo pertinentes.

([26]) Nos termos do Código de Processo Penal e da Lei relativa aos autos finais dos processos penais, o acesso e a correção de materiais apreendidos, bem como os documentos/informações pessoais relativos a processos penais, estão sujeitos a um sistema único e distinto de regras que visa proteger a privacidade das pessoas em causa, o sigilo das investigações e a correta condução do processo penal, etc.

([27]) Mais especificamente, a inspeção de informações relacionadas com elementos de prova objetivos é, em princípio, autorizada para as vítimas da criminalidade no que diz respeito aos registos não relacionados com ações penais no âmbito dos processos objeto da participação das vítimas prevista no artigo 316.º, n.º 33, do Código de Processo Penal, a fim de tornar a proteção das vítimas da criminalidade mais satisfatória.

Estas autoridades são obrigadas a cooperar com a PPC, ao abrigo do artigo 80.º da APPI, incluindo através da disponibilização das informações necessárias e do material relevante, para que a PPC possa avaliar se a recolha ou a utilização subsequente das informações pessoais ocorreu em conformidade com as regras aplicáveis. Na realização da sua avaliação, a PPC cooperará com o Ministério dos Assuntos Internos e das Comunicações.

c) Se a avaliação indicar que ocorreu uma violação das regras aplicáveis, a cooperação das autoridades públicas em causa com a PPC inclui a obrigação de pôr termo à violação.

Em caso de recolha ilegal de informações pessoais no quadro das regras aplicáveis, isso deve incluir a supressão das informações pessoais recolhidas.

Em caso de violação das regras aplicáveis, a PPC irá igualmente confirmar, antes de concluir a avaliação, que foi posto totalmente termo à violação.

d) Uma vez concluída a avaliação, a PPC deve notificar a pessoa singular do resultado da avaliação, dentro de um prazo razoável, incluindo, sendo caso disso, as eventuais medidas corretivas tomadas. Com base nesta notificação, a PPC deve igualmente informar a pessoa singular sobre a possibilidade de obter confirmação do resultado junto da autoridade pública competente e sobre a autoridade a quem esse pedido de confirmação deve ser dirigido.

As informações pormenorizadas sobre o resultado da avaliação podem ser limitadas, desde que existam motivos razoáveis para considerar que a comunicação das mesmas é suscetível de comportar um risco para a investigação em curso.

Se a reclamação disser respeito à recolha ou utilização de dados pessoais no âmbito da aplicação do direito penal, e se a avaliação revelar que foi iniciado um processo relacionado com as informações pessoais da pessoa singular e que o mesmo foi encerrado, a PPC informará a pessoa singular de que pode, nos termos do artigo 53.º do Código de Processo Penal e do artigo 4.º da Lei relativa aos autos finais dos processos penais, consultar os autos do processo.

Se a avaliação revelar que uma pessoa singular é suspeita num processo penal, a PPC informará o indivíduo sobre esse facto e sobre a possibilidade de apresentar um pedido nos termos do artigo 259.º do Código de Processo Penal.

e) Se uma pessoa ainda não estiver satisfeita com o resultado deste processo, pode dirigir-se à CPP, que informará o indivíduo das várias possibilidades e procedimentos pormenorizados para obter reparação ao abrigo da legislação e regulamentação japonesas. A PPC prestará apoio à pessoa singular, incluindo aconselhamento e assistência na tomada de outras medidas junto do órgão administrativo ou judicial relevante.

III. **Acesso do Governo por motivos de segurança nacional**

A. Bases e limitações jurídicas para a recolha de informações pessoais

1) Bases jurídicas para a recolha de informações pelo ministério/agência em causa

Tal como acima referido, a recolha de informações pessoais por motivos de segurança nacional por parte dos órgãos administrativos deve ser abrangida pelo âmbito da sua jurisdição administrativa.

No Japão, não existe legislação que permita a recolha de informações por meios coercivos apenas por motivos de segurança nacional. Nos termos do artigo 35.º da Constituição, é possível recolher informações pessoais por meios coercivos apenas com base num mandado emitido por um tribunal para a investigação de uma infração. Por conseguinte, esse mandado só pode ser emitido para efeitos de uma investigação criminal. Tal significa que, no sistema jurídico japonês, não é permitida a recolha/acesso a informações, por meios coercivos, por motivos de segurança nacional. Em vez disso, no domínio da segurança nacional, os ministérios ou agências em causa só podem obter informações junto de fontes de acesso livre, ou receber informações de operadores comerciais ou de pessoas singulares numa base de divulgação voluntária de informações. Os operadores comerciais que recebem um pedido de cooperação voluntária não têm qualquer obrigação legal de prestar essas informações e, por conseguinte, não sofrem quaisquer consequências negativas se se recusarem a cooperar.

Vários serviços e agências ministeriais têm responsabilidades no domínio da segurança nacional.

1) Secretariado do Conselho de Ministros

O Secretariado do Conselho de Ministros procede à recolha de informações e à investigação sobre importantes políticas do Conselho de Ministros ([28]), tal como previsto no artigo 12.º, n.º 2, da Lei relativa ao Conselho de Ministros ([29]). No entanto, o Secretariado do Conselho de Ministros não tem poderes para recolher informações pessoais diretamente junto dos operadores comerciais. Recolhe, integra, analisa e avalia as informações obtidas a partir de documentação de fonte aberta, de outras autoridades públicas, etc.

2) Polícia municipal/Agência Nacional de Polícia (NPA)

Em cada município, a polícia municipal está habilitada a recolher informações no âmbito da sua jurisdição, nos termos do artigo 2.º da Lei relativa às forças policiais. Pode acontecer que a NPA recolha diretamente informações no âmbito da sua jurisdição, ao abrigo da referida lei. Trata-se, nomeadamente, das atividades do Gabinete de Segurança da NPA e do Departamento de Negócios Estrangeiros e Informações. Nos termos do artigo 24.º da Lei relativa às forças policiais, o Gabinete de Segurança está incumbido das questões relativas à polícia de segurança das informações ([30]) e o Departamento de Negócios Estrangeiros e Informações está encarregado dos assuntos relativos a nacionais estrangeiros, bem como aos nacionais japoneses cujas bases de atividade estejam localizadas em países estrangeiros.

3) Agência de Informações em matéria de Segurança Pública (PSIA)

A aplicação da Lei relativa à prevenção de atividades subversivas (SAPA) e da Lei relativa ao controlo das organizações que cometeram atos indiscriminados de assassinato em massa (ACO) é principalmente da responsabilidade da Agência de Informações em matéria de Segurança Pública (PSIA). Trata-se de uma agência do Ministério da Justiça.

A SAPA e a ACO estipulam que podem ser adotadas disposições administrativas (ou seja, medidas que ordenem a limitação das atividades dessas organizações, a sua dissolução, etc.), sob condições estritas, contra as organizações que cometam determinados atos graves («atividade terrorista subversiva» ou «atos indiscriminados de assassinato em massa»), em violação da «segurança pública» ou da «organização fundamental da sociedade», de acordo com a Constituição. As «atividades terroristas subversivas» são abrangidas pelo âmbito de aplicação da SAPA (ver artigo 4.º, que abrange atividades como insurreição, instigação de agressão estrangeira, homicídio com intenções políticas, etc.), ao passo que a ACO cobre «atos indiscriminados de assassinato em massa» (ver artigo 4.º da ACO). Apenas podem estar sujeitas às disposições da SAPA ou da ACO as organizações identificadas com precisão que representem ameaças internas ou externas específicas para a segurança pública.

Para o efeito, a SAPA e a ACO cobrem juridicamente as atividades de investigação. Os poderes de investigação fundamentais dos agentes da PSIA estão definidos no artigo 27.º da SAPA e no artigo 29.º da ACO. As investigações da PSIA ao abrigo destas disposições são realizadas na medida em que sejam necessárias para a aplicação das disposições acima referidas em matéria de controlo de organizações (por exemplo, os grupos extremistas de esquerda, a seita *Aum Shinrikyo* e um certo grupo japonês estreitamente associado à Coreia do Norte foram objeto de investigação no passado). No entanto, estas investigações não podem basear-se em meios obrigatórios, pelo que uma organização titular de informações pessoais não pode ser obrigada a prestar essas informações.

A recolha e a utilização, a título voluntário, de informações divulgadas à PSIA estão sujeitas às garantias e limitações aplicáveis previstas na lei, como, por exemplo, a confidencialidade das comunicações garantida pela Constituição e as regras relativas ao tratamento das informações pessoais no âmbito da APPIHAO.

4) Ministério da Defesa

Quanto à recolha de informações pelo Ministério da Defesa, este recolhe informações com base nos artigos 3.º e 4.º da Lei relativa à criação do Ministério da Defesa, na medida necessária ao exercício da sua competência administrativa, incluindo, no que diz respeito à defesa e proteção, as medidas a tomar pelas Forças de Autodefesa, bem como o destacamento das Forças de Autodefesa em Terra, no Mar e no Ar. O Ministério da Defesa só pode recolher informações para estes fins através da cooperação voluntária e de fontes de acesso gratuito. Não recolhe informações sobre o público em geral.

2) Limitações e garantias

a) Limitações jurídicas

1. Limitações gerais com base na APPIHAO

A APPIHAO é uma lei geral aplicável à recolha e ao tratamento de informações pessoais pelos órgãos administrativos em qualquer domínio de atividade desses órgãos. Por conseguinte, as limitações e garantias descritas na secção II.A.1) b)(2) aplicam-se igualmente à conservação, armazenamento, utilização, etc. de informações pessoais no domínio da segurança nacional.

([28]) Essas funções são da responsabilidade do gabinete de informação e investigação do Conselho de Ministros, com base no artigo 4.º da Lei orgânica relativa ao secretariado do Conselho de Ministros,

([29]) Inclui «a recolha e a investigação de informações sobre políticas importantes do Conselho de Ministros».

([30]) A polícia de segurança das informações é responsável pelas atividades de repressão da criminalidade relacionadas com a segurança pública e o interesse nacional, o que inclui a repressão da criminalidade e a recolha de informações sobre atos ilegais relacionados com grupos extremistas de esquerda e de direita e atividades prejudiciais para os interesses do Japão.

2. Limitações específicas aplicáveis às forças policiais (NPA e polícia municipal)

Tal como especificado na secção relativa à recolha de informações para efeitos de aplicação da lei, as forças policiais só podem recolher informações no âmbito das suas competências e, ao fazê-lo, podem, nos termos do artigo 2.º, n.º 2, da Lei relativa às forças policiais, agir apenas numa medida «estritamente limitada» ao desempenho das suas funções e de um modo «imparcial, independente, sem preconceitos e justo». Além disso, os seus poderes «nunca podem ser utilizados de forma abusiva para interferir nos direitos e liberdades de uma pessoa singular garantidos pela Constituição do Japão».

3. Limitações específicas aplicáveis à PSIA

Tanto o artigo 3.º da SAPA como o artigo 3.º da ACO estabelecem que as investigações realizadas ao abrigo desses atos devem ser realizadas apenas na medida do mínimo necessário para atingir o objetivo prosseguido e não devem ser realizadas de forma a restringir injustificadamente os direitos humanos fundamentais. Além disso, nos termos do artigo 45.º da SAPA e do artigo 42.º da ACO, se um agente da PSIA abusar da sua autoridade, tal constitui uma infração penal passível de sanções penais mais pesadas do que os abusos «gerais» de autoridade noutros domínios do setor público.

4. Limitações específicas aplicáveis ao Ministério da Defesa

No que diz respeito à recolha/organização de informações pelo Ministério da Defesa, tal como referido no artigo 4.º da Lei relativa à criação do Ministério da Defesa, a atividade deste ministério no âmbito da recolha de informações limita-se ao «necessário» para exercer as suas funções no que respeita 1) à defesa e proteção, 2) às medidas a tomar pelas Forças de Autodefesa, e 3) às organizações, ao número de pessoal, à estrutura, ao equipamento e ao destacamento das Forças de Autodefesa em Terra, no Mar e no Ar.

b) Outras limitações

Como explicado na secção II.A.2) b) 1) relativamente às investigações criminais, resulta da jurisprudência do Supremo Tribunal que os pedidos de cooperação voluntária dirigidos a operadores económicos devem ser necessários à investigação das suspeitas de um crime e ser razoáveis para atingir os objetivos dessa investigação.

Embora as investigações realizadas pelas autoridades de investigação no domínio da segurança nacional sejam diferentes das realizadas pelas autoridades com poderes coercivos, no que se refere à respetiva base jurídica e finalidade, os princípios centrais da «necessidade da investigação» e da «adequação do método» aplicam-se de igual modo no domínio da segurança nacional, devendo ser cumpridos tendo devidamente em conta as circunstâncias específicas de cada processo.

A combinação das referidas limitações assegura que a recolha e o tratamento das informações só podem ter lugar na medida do necessário para o desempenho das atribuições específicas da autoridade pública competente, assim como com base em ameaças concretas. Por conseguinte, encontra-se excluída a recolha maciça e indiscriminada de informações pessoais, ou o acesso às mesmas, por razões de segurança nacional.

B) Controlo

1) Controlo com base na APPIHAO

Como explicado na secção II.B.2), no setor público japonês, o ministro ou o responsável por cada ministério ou agência dispõe de poderes para controlar e fazer cumprir a APPIHAO no respetivo ministério ou agência. Além disso, o Ministro dos Assuntos Internos e das Comunicações pode verificar a aplicação da Lei, solicitar a cada ministro que apresente documentação e explicações com base nos artigos 49.º e 50.º, e endereçar pareceres a cada ministro com base no artigo 51.º. Pode, por exemplo, solicitar uma revisão das medidas através de ações tomadas nos termos dos artigos 50.º e 51.º da Lei.

2) Controlo das forças policiais pelas comissões de segurança pública

Tal como explicado na secção «II. Recolha de informações para fins de aplicação da legislação penal», as comissões municipais independentes de segurança pública supervisionam as atividades da polícia municipal.

No que diz respeito à Agência Nacional de Polícia (NPA), as funções de supervisão são exercidas pela Comissão Nacional de Segurança Pública. Nos termos do artigo 5.º da Lei relativa às forças policiais, esta comissão é responsável, em especial, pela «proteção dos direitos e liberdades das pessoas singulares». Para o efeito, deve definir, nomeadamente, políticas globais que estabeleçam a regulamentação relativa à administração das atividades previstas em cada alínea do artigo 5.º, n.º 4, da Lei relativa às forças policiais, bem como outras orientações e medidas de base necessárias para a execução das referidas atividades. A Comissão Nacional de Segurança Pública (NPSC) tem o mesmo grau de independência que as comissões municipais de segurança pública (PPSC).

3) Controlo do Ministério da Defesa pelo gabinete do inspetor-geral em matéria de conformidade legal

O gabinete do inspetor-geral em matéria de conformidade legal (IGO) é um gabinete independente do Ministério da Defesa, sob a supervisão direta do ministro da defesa, nos termos do artigo 29.º da Lei relativa à criação do Ministério da Defesa. O IGO pode efetuar inspeções em matéria de conformidade legal e regulamentar por parte dos funcionários do Ministério da Defesa. Estas inspeções são designadas por «inspeções no domínio da defesa».

O IGO realiza inspeções do ponto de vista de um gabinete independente, de modo a garantir a conformidade legal a nível de todo o ministério, incluindo as Forças de Autodefesa (SDF). Exerce as suas funções de forma independente dos serviços operacionais do Ministério da Defesa. Na sequência de uma inspeção, o IGO apresenta as suas conclusões, juntamente com as necessárias melhorias qualitativas, direta e imediatamente ao ministro da defesa. Com base no relatório do IGO, o ministro da defesa pode emitir ordens de execução das medidas necessárias para corrigir uma determinada situação. O vice-ministro adjunto é responsável pela aplicação destas medidas e deve informar o ministro da defesa sobre a situação a nível da sua aplicação.

Como medida de transparência voluntária, os resultados das inspeções no domínio da defesa são publicados no sítio Web do Ministério da Defesa (embora tal não seja exigido por lei).

Existem três categorias de inspeções no domínio da defesa:

i) Inspeções periódicas no domínio da defesa, que são realizadas periodicamente ([31]);

ii) Inspeções no domínio da defesa para controlos realizados para verificar se foram efetivamente tomadas medidas de melhoria qualitativa; e

iii) Inspeções especiais no domínio da defesa realizadas para matérias específicas ordenadas pelo ministro da defesa.

No contexto dessas inspeções, o inspetor-geral pode solicitar a apresentação de relatórios ao serviço em causa e de documentos, a introdução em locais para a realização de inspeções, a exigência de explicações ao vice-ministro adjunto, etc. Tendo em conta a natureza das tarefas de inspeção do OIG, este serviço é dirigido por peritos jurídicos muito experientes (ex-procurador-geral).

4) Controlo da PSIA

A PSIA realiza inspeções periódicas e especiais sobre as operações dos seus serviços e gabinetes (Gabinete de Informações de Segurança Pública, Serviços de Informações de Segurança Pública e subserviços, etc.). Para efeitos da inspeção periódica, é designado como inspetor(es) um diretor-geral adjunto e/ou um diretor. Essas inspeções dizem igualmente respeito à gestão das informações pessoais.

5) Controlo parlamentar

No que diz respeito à recolha de informações para fins de aplicação da lei, o Parlamento, através da sua comissão competente, pode examinar a legalidade das atividades de recolha de informações no domínio da segurança nacional. Os poderes de investigação do Parlamento baseiam-se no artigo 62.º da Constituição e nos artigos 74.º e 104.º da Lei que rege o Parlamento.

C. Vias de recurso individuais

As vias de recurso individuais podem ser acionadas através das mesmas vias que no domínio da aplicação do direito penal, o que inclui igualmente o novo mecanismo de vias de recurso, administrado e supervisionado pela PPC, para o tratamento e a resolução de reclamações apresentadas por pessoas singulares da UE. Ver, a este respeito, as disposições relevantes da secção II.C.

Além disso, existem vias de recurso individuais específicas disponíveis no domínio da segurança nacional.

As informações pessoais recolhidas por um órgão de administração para efeitos de segurança nacional estão sujeitas ao disposto no capítulo 4 da APPIHAO. Tal inclui o direito de solicitar a divulgação (artigo 12.º), a retificação (incluindo a adição ou a supressão) (artigo 27.º) das informações pessoais conservadas de pessoas singulares, bem como o direito de solicitar a suspensão da utilização das informações pessoais no caso de o órgão de administração ter obtido ilegalmente as

([31]) Como exemplo de uma inspeção pertinente para as questões abrangidas por esta declaração, pode ser feita referência à inspeção periódica no domínio da defesa de 2016, no que diz respeito à «sensibilização/preparação para a conformidade legal», uma vez que a proteção de informações pessoais foi um dos pontos centrais da inspeção. Mais especificamente, a inspeção incidiu sobre a situação a nível da gestão, armazenamento, etc. das informações pessoais. No seu relatório, o IGO identificou vários aspetos inadequados na gestão das informações pessoais, que devem ser melhorados, como a incapacidade de proteger os dados através de uma palavra-passe. O relatório está disponível no sítio Web do Ministério da Defesa.

informações em causa (artigo 36.º). Deste modo, no domínio da segurança nacional, o exercício desses direitos está sujeito a determinadas restrições: os pedidos de divulgação, correção ou suspensão não serão deferidos quando digam respeito a «informações em relação às quais existam motivos razoáveis para que o responsável por um órgão administrativo considere que a divulgação é suscetível de prejudicar a segurança nacional, a relação de confiança mútua com um outro país ou uma organização internacional, ou provocar uma situação de desvantagem nas negociações com um outro país ou uma organização internacional» (artigo 14.º, alínea iv)). Por conseguinte, nem toda a recolha voluntária de informações relacionadas com a segurança nacional é abrangida por esta isenção, uma vez que esta última exige sempre uma avaliação concreta dos riscos envolvidos na sua divulgação.

Além disso, se o pedido da pessoa singular for rejeitado com base no facto de as informações em causa serem consideradas não suscetíveis de divulgação, na aceção do artigo 14.º, alínea iv), a pessoa singular em causa pode interpor um recurso administrativo para a revisão dessa decisão, alegando, por exemplo, que as condições enunciadas no artigo 14.º, alínea iv), não estão preenchidas no processo em apreço. Nesse caso, antes de tomar uma decisão, o responsável pelo órgão de administração em causa deve consultar o Comité de Avaliação da Divulgação de Informações e da Proteção de Informações Pessoais. Este comité irá rever o recurso de um ponto de vista independente. Trata-se de um organismo altamente especializado e independente, cujos membros são nomeados pelo primeiro-ministro, com a aprovação das duas Câmaras do Parlamento, entre pessoas com competências especializadas relevantes ([32]). O comité goza de poderes de investigação sólidos, incluindo a possibilidade de solicitar documentos e a divulgação das informações pessoais em causa, de deliberar à porta fechada e de aplicar o procedimento do índice de Vanghn ([33]). Em seguida, o comité elabora um relatório escrito, comunicado à pessoa singular em causa ([34]). As conclusões contidas no relatório são tornadas públicas. Embora o relatório não seja formalmente vinculativo do ponto de vista jurídico, quase todos os relatórios são cumpridos pelo órgão de administração em causa ([35]).

Por último, nos termos do artigo 3.º, n.º 3, da Lei do contencioso administrativo, a pessoa singular em causa pode intentar uma ação judicial destinada a revogar a decisão tomada pelo órgão administrativo de não divulgar as informações pessoais.

IV. **Reexame periódico**

No quadro do reexame periódico da decisão de adequação, a PPC e a Comissão Europeia trocarão informações sobre o tratamento de dados, à luz das condições da verificação da adequação, incluindo as previstas na presente declaração.

([32]) Ver artigo 4.º da Lei que cria o Comité de Avaliação da Divulgação de Informações e da Proteção de Informações Pessoais.
([33]) Ver artigo 9.º da Lei que cria o Comité de Avaliação da Divulgação de Informações e da Proteção de Informações Pessoais.
([34]) Ver artigo 16.º da Lei que cria o Comité de Avaliação da Divulgação de Informações e da Proteção de Informações Pessoais.
([35]) Nos últimos três anos, não ocorreu qualquer caso em que o órgão administrativo em causa tenha tomado uma decisão que divirja das conclusões do comité. Retrocedendo, são muito poucos os casos em que tal aconteceu: apenas duas situações, num total de 2 000 processos desde 2005 (ano de entrada em vigor da APPIHAO). Quando o órgão de administração toma uma decisão que difere das conclusões do comité, nos termos do artigo 50.º, n.º 1, ponto 4, da Lei relativa à apreciação de reclamações administrativas, tal como aplicado com a substituição do artigo 42.º, n.º 2, da APPIHAO, deve indicar claramente as razões para tal.

ISSN 1977-0774 (edição eletrónica)
ISSN 1725-2601 (edição em papel)

Serviço das Publicações da União Europeia
2985 Luxemburgo
LUXEMBURGO

PT