II

(Atos não legislativos)

DECISÕES

DECISÃO DE EXECUÇÃO (UE) 2022/254 DA COMISSÃO

de 17 de dezembro de 2021

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

[notificada com o número C(2021) 9316]

(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) ([1]), nomeadamente o artigo 45.º, n.º 3,

Considerando o seguinte:

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, na medida em que essa transferência seja abrangida pelo respetivo âmbito de aplicação. As regras relativas às transferências internacionais de dados são definidas no capítulo V (artigos 44.º a 50.º) do referido regulamento. Embora a circulação de dados pessoais com origem e destino a países não pertencentes à União Europeia seja essencial para o desenvolvimento do comércio transfronteiriço e da cooperação internacional, é indispensável garantir que o nível de proteção conferido aos dados pessoais na União não é comprometido por transferências para países terceiros ([2]).

(2) Nos termos do artigo 45.º, n.º 3, do Regulamento (UE) 2016/679, a Comissão pode decidir, através de um ato de execução, que um país terceiro, um território ou um ou mais setores específicos de um país terceiro, ou uma organização internacional, garante um nível de proteção adequado. Nessa condição, as transferências de dados pessoais para um país terceiro podem realizar-se sem que para tal seja necessária mais nenhuma autorização, conforme previsto no artigo 45.º, n.º 1, e no considerando 103 do Regulamento (UE) 2016/679.

(3) Conforme estabelecido 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, que abranja tanto as regras aplicáveis a importadores de dados como as limitações e garantias relativas ao acesso aos dados pessoais pelas autoridades públicas. Na sua avaliação, a Comissão tem de 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]. A questão de saber se é esse o caso deve ser apreciada à luz da legislação da União Europeia, nomeadamente pelo Regulamento (UE) 2016/679, bem como pela jurisprudência do Tribunal de Justiça da União Europeia ([3]).

([1]) JO L 119 de 4.5.2016, p. 1.
([2]) Ver considerando 101 do Regulamento (UE) 2016/679.
([3]) Ver, mais recentemente, o acórdão do Tribunal de Justiça de 16 de julho de 2020, Facebook Ireland e Schrems («Schrems II»), C-311/18, ECLI:EU:C:2020:559.

(4) Conforme esclareceu o Tribunal de Justiça da União Europeia, não é exigido um nível de proteção idêntico ([4]). Mais concretamente, os meios a que o país terceiro em causa recorre para proteger os dados pessoais podem ser diferentes dos aplicados na União, desde que se revelem, na prática, eficazes para assegurar um nível adequado de proteção ([5]). Por conseguinte, o padrão de adequação não exige que as regras da União sejam replicadas ponto por ponto. Em vez disso, importa aferir sobretudo se, por meio 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 ([6]). O documento de referência relativo à adequação do Comité Europeu para a Proteção de Dados, que procura clarificar esta norma, também fornece orientações a este respeito ([7]).

(5) A Comissão procedeu a uma análise cuidadosa da legislação e das práticas da Coreia. Com base nas conclusões apresentadas nos considerandos (8) a (208), a Comissão conclui que a República da Coreia garante um nível adequado de proteção dos dados pessoais transferidos de um responsável pelo tratamento ou subcontratante na União ([8]) para entidades (por exemplo, pessoas singulares ou coletivas, organizações, instituições públicas) na Coreia abrangidas pelo âmbito de aplicação da Lei relativa à proteção de informações pessoais (Lei n.º 10465, de 29 de março de 2011, com a última redação que lhe foi dada pela Lei n.º 16930, de 4 de fevereiro de 2020), que inclui tanto os responsáveis pelo tratamento como os subcontratantes ([9]) na aceção do Regulamento (UE) 2016/679. A verificação da adequação não abrange o tratamento de dados pessoais para atividades missionárias por organizações religiosas e para a nomeação de candidatos por partidos políticos, ou o tratamento de informações pessoais de crédito nos termos da Lei de informações de crédito por parte dos responsáveis pelo tratamento que sejam sujeitos à supervisão da Comissão de Serviços Financeiros.

(6) Esta conclusão tem em conta as garantias adicionais estabelecidas na Notificação n.º 2021-5 (anexo I) e as declarações, garantias e compromissos oficiais do Governo coreano perante a Comissão (anexo II).

(7) A presente decisão tem por efeito possibilitar as transferências para os responsáveis pelo tratamento e para os subcontratantes na República da Coreia sem necessidade de obter qualquer outra autorização. A mesma não afeta a aplicação direta do Regulamento (UE) 2016/679 às referidas entidades que preencham as condições relativas ao âmbito de aplicação territorial do referido regulamento, previstas no seu artigo 3.º.

2. NORMAS APLICÁVEIS AO TRATAMENTO DE DADOS PESSOAIS

2.1 Quadro de proteção de dados da República da Coreia

(8) O sistema jurídico que rege a privacidade e a proteção dos dados na Coreia tem origem na Constituição coreana promulgada em 17 de julho de 1948. Embora o direito à proteção de dados pessoais não esteja expressamente consagrado na Constituição, é, no entanto, reconhecido como um direito fundamental, decorrente dos direitos constitucionais à dignidade humana e à prossecução da felicidade (artigo 10.º), da vida privada (artigo 17.º) e da privacidade das comunicações (artigo 18.º). Esta aceção foi confirmada tanto pelo Supremo Tribunal ([10]) como pelo Tribunal Constitucional ([11]). As restrições aos direitos e liberdades fundamentais (incluindo o direito à privacidade) só podem ser impostas por lei quando tal for necessário para efeitos de segurança nacional ou para a manutenção da ordem pública e não podem afetar o conteúdo essencial do direito ou liberdade em causa (artigo 37.º, n.º 2,).

([4]) Acórdão do Tribunal de Justiça de 6 de outubro de 2015, Maximillian Schrems/Data Protection Commissioner («Schrems»), C-362/14, ECLI:EU:C:2015:650, n.º 73.

([5]) Acórdão do Tribunal de Justiça de 6 de outubro de 2015, Maximillian Schrems/Data Protection Commissioner («Schrems»), C-362/14, ECLI:EU:C:2015:650, n.º 74.

([6]) Ver Comunicação da Comissão ao Parlamento Europeu e ao Conselho intitulada «Intercâmbio e proteção de dados pessoais num mundo globalizado», COM(2017) 7, de 10 de janeiro de 2017, secção 3.1, p. 6-7.

([7]) Comité Europeu para a Proteção de Dados, documento de referência relativo à adequação, WP 254 rev. 01, disponível na seguinte ligação: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=614108.

([8]) 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, Listenstaine 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. Para efeitos da decisão, as referências à UE e aos Estados-Membros da UE devem, por conseguinte, ser entendidas como abrangendo também os Estados do EEE.

([9]) Ver secção 2.2.3 da presente decisão.

([10]) Ver, por exemplo, a Decisão n.º 2014Da77970 do Supremo Tribunal, de 15 de outubro de 2015 [resumo em inglês disponível na hiperligação do documento «Lawmaker's disclosure of teachers' trade union members case» (não traduzido para português) em https://www.privacy.go.kr/eng/enforcement_01.do] e a jurisprudência aí citada, incluindo a Decisão n.º 2012Da49933, de 24 de julho de 2014.

([11]) Ver, em especial, a Decisão n.º 99Hun-ma513 do Tribunal Constitucional, de 26 de maio de 2005 (resumo em inglês disponível em http://www.koreanlii.or.kr/w/index.php/99Hun-Ma513?ckattempt=2) e a Decisão n.º 2014JHun-ma449 2013 Hun-Ba68 (consolidada), de 23 de dezembro de 2015 [resumo em inglês disponível na hiperligação do documento «Change of resident registration number case» (não traduzido para português) em https://www.privacy.go.kr/eng/enforcement_01.do].

(9) Embora a Constituição se refira, em vários locais, aos direitos dos cidadãos coreanos, o Tribunal Constitucional afirmou que também os nacionais estrangeiros são objeto de direitos fundamentais ([12]). Em especial, o Tribunal declarou que a proteção da dignidade e do valor do ser humano, bem como o direito à felicidade, são direitos de qualquer ser humano e não apenas dos cidadãos ([13]). Além disso, de acordo com as declarações oficiais do Governo coreano ([14]), é geralmente reconhecido que os artigos 12.º a 22.º da Constituição (que incluem os direitos de privacidade) preveem direitos humanos fundamentais ([15]). Embora, até à data, não exista jurisprudência específica respeitante ao direito à privacidade dos nacionais estrangeiros, o seu fundamento na proteção da dignidade humana e na prossecução da felicidade apoia esta conclusão ([16]).

(10) Além disso, a Coreia promulgou um conjunto de leis no domínio da proteção de dados que preveem garantias para todas as pessoas singulares, independentemente da sua nacionalidade ([17]). Para efeitos da presente decisão, as leis aplicáveis são:

— Lei relativa à proteção de informações pessoais;

— Lei relativa à utilização e proteção de informações de crédito ([18]);

— Lei relativa à proteção da privacidade das comunicações.

(11) A Lei relativa à proteção de informações pessoais estabelece o quadro jurídico geral para a proteção de dados na República da Coreia. É complementada por um decreto de execução (Decreto Presidencial n.º 23169, de 29 de setembro de 2011, com a última redação que lhe foi dada pelo Decreto Presidencial n.º 30892, de 4 de agosto de 2020) (Decreto de Execução da Lei relativa à proteção de informações pessoais), que, tal como a Lei relativa à proteção de informações pessoais, é juridicamente vinculativo e tem força executiva.

(12) Além disso, as «notificações» regulamentares adotadas pela Comissão de Proteção de Informações Pessoais preveem regras adicionais sobre a interpretação e a aplicação da Lei relativa à proteção de informações pessoais. Com base no disposto no artigo 5.º (Obrigações do Estado) e no artigo 14.º da Lei relativa à proteção de informações pessoais (Cooperação internacional), a Comissão de Proteção de Informações Pessoais adotou a Notificação n.º 2021-5, de 1 de setembro de 2020 (com a redação que lhe foi dada pela Notificação n.º 2021-1, de 21 de janeiro de 2021, e pela Notificação n.º 2021-5 de 16 de novembro de 2021, Notificação n.º 2021-5), sobre a interpretação, aplicação e execução de determinadas disposições da Lei relativa à proteção de informações pessoais. A referida notificação fornece esclarecimentos aplicáveis a qualquer tratamento de dados pessoais ao abrigo da Lei relativa à proteção de informações pessoais, bem como garantias adicionais para os dados pessoais transferidos para a Coreia com base na presente decisão. A notificação é juridicamente vinculativa para os responsáveis pelo tratamento de dados pessoais e pode ser executada tanto pela Comissão de Proteção de Informações Pessoais como pelos tribunais ([19]). Uma violação das regras estabelecidas na notificação implica uma violação das disposições pertinentes da Lei relativa à proteção de informações pessoais que as mesmas complementam. Por conseguinte, o teor das garantias adicionais é analisado no âmbito da avaliação dos artigos pertinentes da Lei relativa à proteção de informações pessoais. Por fim, o Manual da Lei relativa à proteção de informações pessoais e as orientações adotadas pela Comissão de Proteção de Informações Pessoais ([20]) contêm orientações adicionais sobre a Lei relativa à proteção de informações pessoais e o respetivo decreto de execução, que informam a aplicação e o cumprimento das regras em matéria de proteção de dados por parte da Comissão de Proteção de Informações Pessoais.

([12]) Decisão n.º 93 Hun-MA120 do Tribunal Constitucional, de 29 de dezembro de 1994.

([13]) Decisão n.º 99HeonMa494 do Tribunal Constitucional, de 29 de novembro de 2001.

([14]) Ver anexo II, ponto 1.1.

([15]) Ver também o artigo 1.º da Lei relativa à proteção de informações pessoais, que refere expressamente as liberdades e direitos das pessoas singulares. Mais especificamente, prevê que a lei tem por objetivo «abranger o tratamento e a proteção de dados pessoais com vista à proteção da liberdade e dos direitos das pessoas singulares e concretizar a dignidade e o valor das pessoas singulares». De igual modo, o artigo 5.º, n.º 1, da Lei relativa à proteção de informações pessoais estabelece a responsabilidade do Estado para «formular políticas que visem evitar consequências nocivas da recolha para finalidades não previstas, o abuso e a utilização indevida de informações pessoais, a vigilância e a perseguição indiscriminada, etc. e para reforçar a dignidade do ser humano e a privacidade individual».

([16]) Além disso, o artigo 6.º, n.º 2, da Constituição prevê que o estatuto dos nacionais estrangeiros é garantido nos termos do direito e dos tratados internacionais. A Coreia é Parte em vários acordos internacionais que garantem o direito à privacidade, tais como o Pacto Internacional sobre os Direitos Civis e Políticos (artigo 17.º), a Convenção sobre os Direitos das Pessoas com Deficiência (artigo 22.º) e a Convenção sobre os Direitos da Criança (artigo 16.º).

([17]) Tal inclui regras pertinentes para a proteção de dados pessoais, mas que não se aplicam a uma situação em que os dados pessoais são recolhidos na União e transferidos para a Coreia ao abrigo do Regulamento (UE) 2016/679, por exemplo, na Lei relativa à proteção e à utilização das informações de localização.

([18]) O objetivo desta lei é promover um negócio de informação de crédito sólido, promovendo a utilização eficiente e a gestão sistemática de informações de crédito e protegendo a privacidade contra a utilização indevida e abusiva de informações de crédito (artigo 1.º da lei).

([19]) Por exemplo, os tribunais coreanos pronunciaram-se sobre o cumprimento das notificações regulamentares em vários casos, nomeadamente responsabilizando os responsáveis pelo tratamento coreanos por violações de uma notificação (ver, por exemplo, a Decisão 2018Da219406 do Supremo Tribunal, de 25 de outubro de 2018, em que o tribunal ordenou a um responsável pelo tratamento que pagasse uma indemnização às pessoas singulares por danos sofridos devido a uma violação da notificação relativa à norma para as medidas destinadas a garantir a segurança das informações pessoais. Ver também a Decisão n.º 2018Da219352 do Supremo Tribunal, de 25 de outubro de 2018, a Decisão n.º 2011Da24555 do Supremo Tribunal, de 16 de maio de 2016, a Decisão n.º 2014Gahap511956 do Tribunal Central da Comarca de Seul, de 13 de outubro de 2016, a Decisão n.º 2009Gahap43176 do Tribunal Central da Comarca de Seul, de 26 de janeiro de 2010).

([20]) Artigo 12.º, n.º 1, da Lei relativa à proteção de informações pessoais.

(13) Além disso, a Lei relativa à utilização e proteção de informações de crédito estabelece regras específicas aplicáveis tanto a operadores comerciais «normais» como a entidades especializadas no setor financeiro quando tratam informações pessoais sobre o crédito, ou seja, as informações necessárias para determinar a solvabilidade das partes em transações financeiras ou comerciais. Nas referidas informações incluem-se, nomeadamente, o nome, os dados de contacto, as transações financeiras, a notação de crédito, a situação em matéria de seguros ou o saldo do empréstimo, quando tais informações são utilizadas para determinar a solvabilidade de uma pessoa singular ([21]). Em contrapartida, quando essas informações são utilizadas para outros fins (como os recursos humanos), a Lei relativa à proteção de informações pessoais aplica-se em todos os seus elementos. No que respeita às disposições específicas da Lei relativa à utilização e proteção de informações de crédito em matéria de proteção de dados, o cumprimento é supervisionado, em parte, pela Comissão de Proteção de Informações Pessoais (relativamente às organizações comerciais, ver o artigo 45.º-3 da Lei relativa à utilização e proteção de informações de crédito) e, em parte, pela Comissão de Serviços Financeiros ([22]) (relativamente ao setor financeiro, incluindo agências de notação de crédito, bancos, companhias de seguros, caixas económicas mutualistas, sociedades financeiras de crédito especializadas, sociedades de serviços de investimento financeiro, sociedades de financiamento de valores mobiliários, cooperativas de crédito, etc., ver o artigo 45.º, n.º 1, da Lei relativa à utilização e proteção de informações de crédito, conjugado com o artigo 36.º-2 do Decreto de Execução da Lei relativa à utilização e proteção de informações de crédito e o artigo 38.º da Lei relativa à Comissão de Serviços Financeiros). A este respeito, o âmbito de aplicação da presente decisão limita-se a operadores comerciais sujeitos à fiscalização da Comissão de Proteção de Informações Pessoais ([23]). As regras específicas da Lei relativa à utilização e proteção de informações de crédito aplicáveis neste contexto (aplicam-se as regras gerais da Lei relativa à proteção de informações pessoais quando não existem regras específicas) encontram-se descritas no ponto 2.3.11.

2.2 **Âmbito de aplicação material e pessoal da Lei relativa à proteção de informações pessoais**

(14) Salvo disposição específica em contrário noutras leis, a proteção dos dados pessoais é regida pela Lei relativa à proteção de informações pessoais (artigo 6.º). O âmbito de aplicação material e pessoal da mesma é determinado pelos conceitos definidos de «informações pessoais», «tratamento» e «responsável pelo tratamento de informações pessoais».

2.2.1 *Definição de dados pessoais*

(15) O artigo 2.º, n.º 1, da Lei relativa à proteção de informações pessoais define as informações pessoais como as informações relativas a uma pessoa singular viva que a identifique diretamente, por exemplo, através do seu nome, número de registo ou imagem residente, ou indiretamente, nomeadamente quando as informações que não podem, por si só, identificar uma determinada pessoa singular podem ser facilmente combinadas com outras informações. Determinar se as informações podem ser «facilmente» combinadas depende da probabilidade razoável dessa combinação, tendo em conta a possibilidade de obter outras informações, bem como o tempo, o custo e a tecnologia necessários para identificar uma pessoa.

(16) Além disso, as informações com recurso a pseudónimos – ou seja, informações que não podem identificar uma pessoa singular específica sem as utilizar ou combinar com informações adicionais para as repor na sua situação original – são consideradas dados pessoais ao abrigo da Lei relativa à proteção de informações pessoais (artigo 2.º, n.º 1, alínea c), da Lei relativa à proteção de informações pessoais). Em contrapartida, as informações totalmente «anónimas» estão excluídas do âmbito de aplicação da Lei relativa à proteção de informações pessoais (artigo 58.º, n.º 2, da Lei relativa à proteção de informações pessoais). É o caso das informações através das quais não é possível identificar uma pessoa singular específica, mesmo que combinadas com outras informações, tendo em conta o tempo, o custo e a tecnologia razoavelmente necessários para a identificação.

(17) Tal corresponde ao âmbito de aplicação material do Regulamento (UE) 2016/679 e aos respetivos conceitos de «dados pessoais», «pseudonimização» ([24]) e «informações anónimas» ([25]).

([21]) Artigo 2.º, n.º 1, da Lei relativa à utilização e proteção de informações de crédito.

([22]) A Comissão dos Serviços Financeiros é a autoridade de supervisão da Coreia para o setor financeiro e, nessa qualidade, também aplica a Lei relativa à utilização e proteção de informações de crédito.

([23]) Caso esta situação se altere no futuro, por exemplo, alargando a jurisdição da Comissão de Proteção de Informações Pessoais a todo o tratamento de informações pessoais de crédito no âmbito da Lei relativa à utilização e proteção de informações de crédito, poderá considerar-se a possibilidade de alterar a decisão de adequação de modo a abranger também as entidades atualmente sujeitas à supervisão da Comissão dos Serviços Financeiros.

([24]) Em conformidade com a Lei relativa à proteção de informações pessoais, por «tratamento com recurso a pseudónimos» entende-se o tratamento com o uso de métodos tais como a supressão parcial de dados pessoais ou a substituição parcial ou total de dados pessoais, de modo que não seja possível reconhecer nenhuma pessoa singular específica sem informações adicionais (artigo 2.º, n.ºs 1 e 2, da Lei relativa à proteção de informações pessoais). Este conceito corresponde à definição de «pseudonimização» constante do artigo 4.º, ponto 5, do Regulamento (UE) 2016/679, que se refere ao «tratamento de dados pessoais de forma que deixem de poder ser atribuídos a um titular de dados específico sem recorrer a informações suplementares, desde que essas informações suplementares sejam mantidas separadamente e sujeitas a medidas técnicas e organizativas para assegurar que os dados pessoais não possam ser atribuídos a uma pessoa singular identificada ou identificável».

([25]) Em especial, o considerando 26 do Regulamento (UE) 2016/679 esclarece que o regulamento não se aplica a informações anónimas, ou seja, às informações que não digam respeito a uma pessoa singular identificada ou identificável. Por sua vez, tal depende de todos os meios suscetíveis de ser razoavelmente utilizados, tais como a seleção, quer pelo responsável pelo tratamento quer por outra pessoa, para identificar direta ou indiretamente a pessoa singular. Para determinar se há uma probabilidade razoável de os meios serem utilizados para identificar a pessoa singular, importa considerar todos os fatores objetivos, como os custos e o tempo necessário para a identificação, tendo em conta a tecnologia disponível à data do tratamento dos dados e a evolução tecnológica.

2.2.2 *Definição de tratamento*

(18) O conceito de «tratamento» é definido em termos gerais na Lei relativa à proteção de informações pessoais como abrangendo a recolha, a produção, a ligação, a interligação, o registo, o armazenamento, a retenção, o tratamento de valor acrescentado, a edição, a obtenção, a produção, a correção, a recuperação, a utilização, o fornecimento e a divulgação, a destruição de informações pessoais e outras atividades semelhantes ([26]). Embora certas disposições da Lei relativa à proteção de informações pessoais se refiram apenas a tipos específicos de tratamento, tais como «utilização», «prestação» ou «recolha» ([27]), a noção de «utilização» é interpretada como incluindo qualquer tipo de tratamento que não seja «recolha» ou «prestação» (por terceiros). Esta interpretação lata da noção de «utilização» garante, assim, a inexistência de lacunas na proteção no que respeita a atividades de tratamento específicas. Por conseguinte, o conceito de «tratamento» é igual ao constante do Regulamento (UE) 2016/679.

2.2.3 *Responsável pelo tratamento de informações pessoais e subcontratante*

(19) A Lei relativa à proteção de informações pessoais aplica-se aos «responsáveis pelo tratamento de informações pessoais» (responsável pelo tratamento). À semelhança do Regulamento (UE) 2016/679, o conceito inclui qualquer instituição pública, pessoa coletiva, organização ou pessoa singular que proceda ao tratamento de dados pessoais, de forma direta ou indireta, para a gestão de ficheiros de dados pessoais, como parte das respetivas atividades ([28]). Neste contexto, por «ficheiro de informações pessoais» entende-se qualquer conjunto ou conjuntos de informações pessoais estruturadas ou organizadas de forma sistemática, com base numa determinada regra, para facilitar o acesso às informações pessoais (artigo 2.º, n.º 4, da Lei relativa à proteção de informações pessoais) ([29]). A nível interno, o responsável pelo tratamento está obrigado a formar as pessoas singulares envolvidas no tratamento que se encontrem sob a sua direção, tais como dirigentes ou funcionários da empresa, e a exercer um controlo e supervisão adequados (artigo 28.º, n.º 1, da Lei relativa à proteção de informações pessoais).

(20) Aplicam-se obrigações específicas quando um responsável pelo tratamento subcontrata o tratamento de dados pessoais a um terceiro («subcontratante»). Em especial, a subcontratação deve ser regida por um acordo juridicamente vinculativo (normalmente um contrato) ([30]) que defina o âmbito do trabalho subcontratado, a finalidade do tratamento, as garantias técnicas e de gestão a aplicar, a supervisão pelo responsável pelo tratamento, a responsabilidade (como a indemnização por danos causados por uma violação das obrigações contratuais), bem como as limitações a qualquer outra subcontratação ulterior ([31]) (artigo 26.º, n.ºs 1 e 2, da Lei relativa à proteção de informações pessoais conjugado com o artigo 28.º, n.º 1, do decreto de execução) ([32]).

(21) Além disso, o responsável pelo tratamento tem de publicar e atualizar continuamente informações detalhadas sobre o trabalho subcontratado e a identidade do subcontratante ou, na medida em que o tratamento subcontratado diga respeito a atividades de comercialização direta, notificar diretamente as pessoas singulares sobre as informações pertinentes (artigo 26.º, n.ºs 2 e 3, da Lei relativa à proteção de informações pessoais, conjugado com o artigo 28.º, n.ºs 2 a 5, do decreto de execução) ([33]).

(22) Além disso, nos termos do artigo 26.º, n.º 4, da Lei relativa à proteção de informações pessoais, conjugado com o artigo 28.º, n.º 6, do decreto de execução, o responsável pelo tratamento tem a obrigação de «educar» o subcontratante acerca das medidas de segurança necessárias, bem como de supervisionar, nomeadamente através de inspeções, se o subcontratante cumpre todas as obrigações do responsável pelo tratamento ao abrigo da Lei relativa à proteção de informações pessoais ([34]), bem como ao abrigo do contrato de subcontratação. Em caso de danos decorrentes de uma violação da Lei relativa à proteção de informações pessoais pelo subcontratante, as ações ou omissões por este cometidas serão imputadas ao responsável pelo tratamento para efeitos de responsabilidade, tal como acontece no caso de um trabalhador (artigo 26.º, n.º 6, da Lei relativa à proteção de informações pessoais).

([26]) Artigo 2.º, n.º 2, da Lei relativa à proteção de informações pessoais.

([27]) Por exemplo, os artigos 15.º a 19.º da Lei relativa à proteção de informações pessoais referem-se apenas à recolha, à utilização e à prestação de informações pessoais.

([28]) Artigo 2.º, n.º 5, da Lei relativa à proteção de informações pessoais. Na aceção da Lei relativa à proteção de informações pessoais, as instituições públicas incluem todos os departamentos ou serviços administrativos centrais e respetivos organismos associados, os órgãos de administração local, as escolas e as empresas públicas investidas por órgão da administração local, os órgãos administrativos da Assembleia Nacional e o poder judicial (incluindo o Tribunal Constitucional) (artigo 2.º, n.º 6, da Lei relativa à proteção de informações pessoais, conjugado com o artigo 2.º do Decreto de Execução da Lei relativa à proteção de informações pessoais).

([29]) Corresponde ao âmbito de aplicação material do Regulamento (UE) 2016/679. De acordo com o disposto no artigo 2.º, n.º 1, do Regulamento (UE) 2016/679, o «regulamento aplica-se ao tratamento de dados pessoais por meios total ou parcialmente automatizados, bem como ao tratamento por meios não automatizados de dados pessoais contidos em ficheiros ou a eles destinados». Nos termos do artigo 4.º, ponto 6, do Regulamento (UE) 2016/679, por «ficheiro» entende-se «qualquer conjunto estruturado de dados pessoais, acessível segundo critérios específicos». Em consonância com esta definição, no considerando 15 explica-se que a proteção das pessoas singulares deve aplicar-se «ao tratamento de dados pessoais por meios automatizados, bem como ao tratamento manual, se os dados pessoais estiverem contidos ou se forem destinados a um sistema de ficheiros. Os ficheiros ou os conjuntos de ficheiros bem como as suas capas, que não estejam estruturados de acordo com critérios específicos, não deverão ser abrangidos pelo âmbito de aplicação do presente regulamento».

([30]) Ver o Manual da Lei relativa à proteção de informações pessoais, capítulo III, secção 2, sobre o artigo 26.º (p. 203-212), que explica que o artigo 26.º, n.º 1, da Lei relativa à proteção de informações pessoais se refere a disposições vinculativas, tais como contratos ou disposições semelhantes.

([31]) Nos termos do artigo 26.º, n.º 5, da Lei relativa à proteção de informações pessoais, o subcontratante está proibido de utilizar quaisquer informações pessoais fora do âmbito do trabalho subcontratado ou de fornecer informações pessoais a terceiros. O incumprimento deste requisito pode dar origem a uma sanção penal nos termos do artigo 71.º, ponto 2, da Lei relativa à proteção de informações pessoais.

([32]) O incumprimento deste requisito pode dar origem à aplicação de uma coima, ver artigo 75.º, n.º 4, ponto 4, da Lei relativa à proteção de informações pessoais.

([33]) O incumprimento deste requisito pode dar origem à aplicação de uma coima, ver artigo 75.º, n.º 2, ponto 1, e n.º 4, ponto 5, da Lei relativa à proteção de informações pessoais.

([34]) Ver também o artigo 26.º, n.º 7, da Lei relativa à proteção de informações pessoais, segundo o qual os artigos 15.º a 25.º, 27.º a 31.º, 33.º a 38.º e 50.º se aplicam ao subcontratante, com as devidas adaptações.

(23) Embora a Lei relativa à proteção de informações pessoais não utilize, por conseguinte, conceitos diferentes para «responsáveis pelo tratamento» e «subcontratantes», as regras em matéria de subcontratação preveem essencialmente obrigações e garantias equivalentes às que regulam a relação entre os responsáveis pelo tratamento e os subcontratantes ao abrigo do Regulamento (UE) 2016/679.

2.2.4 *Disposições especiais aplicáveis aos prestadores de serviços de informação e comunicação*

(24) Embora a Lei relativa à proteção de informações pessoais se aplique ao tratamento de dados pessoais por qualquer responsável pelo tratamento, certas disposições contêm regras específicas (como *lex specialis*) aplicáveis ao tratamento de dados pessoais de «utilizadores» levado a cabo por «prestadores de serviços de informação e comunicação» ([35]). O conceito de «utilizadores» abrange pessoas singulares que utilizam serviços de informação e comunicação (artigo 2.º, n.º 1, ponto 4, da Lei relativa à promoção da utilização das redes de informação e comunicação e da proteção de dados, a seguir designada por Lei relativa às redes). Tal exige que a pessoa singular utilize diretamente serviços de telecomunicações prestados por um operador de telecomunicações coreano ou utilize serviços de informação ([36]) fornecidos comercialmente (ou seja, com fins lucrativos) por uma entidade que, por sua vez, depende dos serviços de um operador de telecomunicações licenciado/registado na Coreia ([37]). Em ambos os casos, a entidade vinculada pelas disposições específicas da Lei relativa à proteção de informações pessoais é uma entidade que disponibiliza um serviço em linha diretamente a uma pessoa singular (ou seja, um utilizador).

(25) Em contrapartida, uma verificação de adequação diz exclusivamente respeito ao nível de proteção conferido aos dados pessoais transferidos de um responsável pelo tratamento/subcontratante na União para uma entidade num país terceiro (neste caso: a República da Coreia). Neste último cenário, as pessoas singulares na União terão normalmente uma relação direta apenas com o «exportador de dados» na União e não com qualquer prestador de serviços de informação e comunicação coreano ([38]). Por conseguinte, as disposições específicas da Lei relativa à proteção de informações pessoais relativas a dados pessoais dos utilizadores de serviços de informação e comunicação só se aplicarão, quando muito, em situações limitadas aos dados pessoais transferidos ao abrigo da presente decisão.

2.2.5 *Isenção de determinadas disposições da Lei relativa à proteção de informações pessoais*

(26) O artigo 58.º, n.º 1, da Lei relativa à proteção de informações pessoais exclui a aplicação de parte da Lei relativa à proteção de informações pessoais (ou seja, os artigos 15.º a 57.º) relativamente a quatro categorias de tratamento de dados ([39]). Em especial, não são aplicáveis as partes da Lei relativa à proteção de informações pessoais respeitantes aos motivos específicos para o tratamento, a certas obrigações em matéria de proteção de dados, às regras pormenorizadas para o exercício dos direitos individuais, bem como às regras que regem a resolução de litígios pelo Comité de Mediação de Litígios de Informações Pessoais. Continuam a aplicar-se outras disposições básicas da Lei relativa à proteção de informações pessoais, em especial as disposições gerais relativas aos princípios de proteção de dados (artigo 3.º da Lei relativa à proteção de informações pessoais) – incluindo, por exemplo, os princípios da legalidade, especificação da finalidade e limitação da finalidade, minimização dos dados, exatidão e segurança dos dados – e aos direitos individuais (de acesso, retificação, apagamento e suspensão, ver artigo 4.º da Lei relativa à proteção de informações pessoais). Além disso, o artigo 58.º, n.º 4, da Lei relativa à proteção de informações pessoais impõe obrigações específicas a essas atividades de tratamento, nomeadamente no que diz respeito à minimização dos dados, à conservação limitada de dados, às medidas de segurança e ao tratamento das reclamações ([40]). Consequentemente, as pessoas singulares podem ainda apresentar uma reclamação junto da Comissão de Proteção de Informações Pessoais se os referidos princípios e obrigações não forem respeitados e a Comissão de Proteção de Informações Pessoais estiver habilitada a tomar medidas coercivas em caso de incumprimento.

([35]) Ver, em especial, o artigo 18.º, n.º 2, e o capítulo VI da Lei relativa à proteção de informações pessoais.

([36]) Os serviços de informação incluem a prestação de informações e serviços de intermediação para a prestação de informações.

([37]) Ver o artigo 2.º, n.º 1, ponto 3, (conjugado com o artigo 2.º, n.º 1, pontos 2 e 4) da Lei relativa às redes e o artigo 2.º, n.os 6 e 8, da Lei relativa às atividades de telecomunicações.

([38]) Na medida em que os prestadores coreanos de serviços de informação e comunicação tenham uma relação direta com as pessoas singulares na UE (através da oferta de serviços em linha), tal poderá conduzir à aplicação direta do Regulamento (UE) 2016/679, nos termos do seu artigo 3.º, n.º 2, alínea a).

([39]) O artigo 58.º, n.º 2, da Lei relativa à proteção de informações pessoais prevê ainda que os artigos 15.º e 22.º, o artigo 27.º, n.os 1 e 2, e os artigos 34.º e 37.º não se aplicam às informações pessoais tratadas através de dispositivos de tratamento de dados visuais instalados e operados em locais abertos. Uma vez que esta disposição diz respeito à utilização da videovigilância na Coreia, ou seja, a recolha direta de informações pessoais de pessoas singulares na Coreia, a mesma não é relevante para efeitos da presente decisão, que abrange as transferências de dados pessoais dos responsáveis pelo tratamento/subcontratantes na UE para entidades na Coreia. Além disso, nos termos do artigo 58.º, n.º 3, da Lei relativa à proteção de informações pessoais, o artigo 15.º (recolha e utilização de informações pessoais), o artigo 30.º (obrigação de implementar uma política de privacidade pública) e o artigo 31.º (obrigação de nomear um responsável pela privacidade) não se aplicam às informações pessoais tratadas para gerir grupos ou associações de amizade (por exemplo, clubes de ocupação de tempos livres). Uma vez que esses grupos são considerados de natureza pessoal, sem qualquer relação com uma atividade profissional ou comercial, não é necessária qualquer base jurídica específica (como o consentimento das pessoas singulares em causa) para recolher e utilizar as respetivas informações neste âmbito. No entanto, continuam a aplicar-se todas as restantes disposições da Lei relativa à proteção de informações pessoais (por exemplo, minimização dos dados, limitação da finalidade, legalidade do tratamento, segurança e direitos individuais). Além disso, qualquer tratamento das informações pessoais que ultrapasse a finalidade de criar um grupo social não beneficiaria da exceção.

([40]) Mais especificamente, o artigo 58.º, n.º 4, da Lei relativa à proteção de informações pessoais prevê a obrigação de tratar as informações pessoais na medida do mínimo necessário para atingir o objetivo pretendido, de as tratar durante um período mínimo e de tomar as medidas necessárias para a gestão segura e o tratamento adequado dessas informações pessoais. Tais medidas incluem garantias técnicas, de gestão e físicas, bem como medidas destinadas a assegurar o tratamento adequado das reclamações individuais.

(27) Em primeiro lugar, a isenção parcial abrange os dados pessoais recolhidos nos termos da Lei relativa a estatísticas para tratamento por parte de instituições públicas. De acordo com os esclarecimentos prestados pelo Governo coreano, os dados pessoais tratados neste contexto dizem normalmente respeito a nacionais coreanos e só excecionalmente podem incluir informações sobre estrangeiros, nomeadamente no caso de estatísticas sobre entradas e saídas do território ou sobre investimentos estrangeiros. No entanto, mesmo nestas situações, esses dados não são normalmente transferidos dos responsáveis pelo tratamento/subcontratantes na União, mas sim recolhidos diretamente pelas autoridades públicas da Coreia ([41]). Além disso, à semelhança do previsto no considerando 162 do Regulamento (UE) 2016/679, o tratamento de dados ao abrigo da Lei relativa a estatísticas está sujeito a várias condições e garantias. Em especial, a esta lei impõe obrigações específicas, tais como garantir a exatidão, a coerência e a imparcialidade, assegurar a confidencialidade das pessoas singulares, proteger as informações dos inquiridos no âmbito de inquéritos estatísticos, nomeadamente a fim de impedir que tais informações sejam utilizadas para outras finalidades que não a compilação de estatísticas e sujeitar os membros do pessoal a requisitos de confidencialidade ([42]). As autoridades públicas que tratam estatísticas devem também respeitar, nomeadamente, os princípios da minimização de dados, da limitação da finalidade e da segurança (artigos 3.º e 58.º, n.º 4, da Lei relativa à proteção de informações pessoais) e permitir que as pessoas singulares exerçam os respetivos direitos (de acesso, retificação, apagamento e suspensão, ver artigo 4.º da Lei relativa à proteção de informações pessoais). Por último, é necessário que os dados sejam tratados de forma anónima ou pseudonimizada, caso tal permita cumprir a finalidade do tratamento (artigo 3.º, n.º 7, da Lei relativa à proteção de informações pessoais).

(28) Em segundo lugar, o artigo 58.º, n.º 1, da Lei relativa à proteção de informações pessoais refere-se aos dados pessoais recolhidos ou solicitados para a análise de informações relacionadas com a segurança nacional. O âmbito e as consequências desta isenção parcial encontram-se descritas pormenorizadamente no considerando (149).

(29) Em terceiro lugar, a isenção parcial aplica-se ao tratamento temporário de dados pessoais quando tal seja urgentemente necessário por razões de proteção e segurança públicas, incluindo a saúde pública. Esta categoria é interpretada de forma estrita pela Comissão de Proteção de Informações Pessoais e, de acordo com as informações recebidas, nunca foi utilizada. Aplica-se apenas em situações de emergência que exijam uma ação urgente, por exemplo, para detetar agentes infecciosos ou para salvar e ajudar as vítimas de catástrofes naturais ([43]). Mesmo nestas situações, a isenção parcial só abrange o tratamento de dados pessoais durante um período limitado para a realização dessa ação. São ainda mais limitadas as situações em que tal se poderia aplicar às transferências de dados abrangidas pela presente decisão, tendo em conta a reduzida probabilidade de os dados pessoais transferidos da União para operadores coreanos serem do tipo suscetível de tornar o seu posterior tratamento «urgentemente necessário» para essas emergências.

(30) Por último, a isenção parcial aplica-se aos dados pessoais recolhidos ou utilizados pela imprensa, para atividades missionárias por organizações religiosas ou para a nomeação de candidatos por partidos políticos. A isenção só se aplica quando os dados pessoais são tratados pela imprensa, organizações religiosas ou partidos políticos para essas finalidades específicas (ou seja, atividades jornalísticas, trabalho missionário e nomeação de candidatos políticos). Quando essas entidades tratam dados pessoais para outras finalidades, como a gestão de recursos humanos ou a administração interna, a Lei relativa à proteção de informações pessoais aplica-se na íntegra.

(31) No que respeita ao tratamento de dados pessoais pela imprensa para atividades jornalísticas, o equilíbrio entre a liberdade de expressão e outros direitos (incluindo o direito à privacidade) é proporcionado pela Lei relativa a arbitragem e vias de recurso por danos causados por notícias da imprensa («Lei da imprensa») ([44]). Em especial, o artigo 5.º da Lei relativa à imprensa prevê que a imprensa (ou seja, qualquer organismo de radiodifusão, jornal,

([41]) Nesta matéria, o artigo 33.º da Lei relativa a estatísticas exige que as instituições públicas protejam as informações dos inquiridos em inquéritos estatísticos, inclusive para impedir que tais informações sejam utilizadas para outras finalidades que não a compilação de estatísticas.

([42]) Artigo 2.º, n.ºs 2 e 3, artigo 30.º, n.º 2, e artigos 33.º e 34.º da Lei relativa às estatísticas.

([43]) Manual da Lei relativa à proteção de informações pessoais, secção relativa ao artigo 58.º.

([44]) Por exemplo, o artigo 4.º da Lei relativa à imprensa estabelece que as notícias de imprensa devem ser imparciais e objetivas, no interesse público, respeitar a dignidade e o valor do ser humano e não podem difamar outras pessoas singulares nem violar os seus direitos, a moral pública ou a ética social.

periódico ou em linha), qualquer serviço noticioso na Internet ou organismo de radiodifusão multimédia na Internet não pode violar a privacidade das pessoas singulares. Se, ainda assim, ocorrer uma violação da privacidade, esta deve ser rapidamente sanada, em conformidade com os procedimentos específicos previstos na referida lei. A este respeito, a Lei relativa à imprensa concede um conjunto de direitos às pessoas singulares que sofrem danos devido a uma notícia de imprensa, tais como a publicação de uma correção de uma falsa declaração, uma retificação através de uma declaração contraditória ou de uma nova notícia (quando a notícia de imprensa disser respeito a alegações de crimes de que a pessoa singular é posteriormente absolvida) ([45]). As reclamações apresentadas podem ser resolvidas diretamente pelos órgãos de comunicação social (através de um provedor de justiça) ([46]), por conciliação ou arbitragem (perante uma Comissão de Arbitragem de Imprensa especializada) ([47]) ou perante os tribunais. As pessoas singulares podem igualmente ser indemnizadas quando sofrem danos patrimoniais, pela violação de um direito de personalidade ou qualquer outro sofrimento emocional devido a um ato ilegal da imprensa (por dolo ou negligência) ([48]). Nos termos da Lei relativa à imprensa, a imprensa será responsável na medida em que uma notícia de imprensa que interfira com os direitos de uma pessoa singular não seja contrária aos valores sociais e seja publicada com o consentimento da pessoa singular em causa ou no interesse público (e existam motivos suficientes para considerar que a notícia corresponde à verdade) ([49]).

(32) Embora o tratamento de dados pessoais pela imprensa para atividades jornalísticas esteja, por conseguinte, sujeito a garantias específicas decorrentes da Lei relativa à imprensa, não existem garantias adicionais que enquadrem a utilização das exceções para as atividades de tratamento por parte de organizações religiosas e partidos políticos de uma forma comparável aos artigos 85.º, 89.º e 91.º do Regulamento (UE) 2016/679. Por conseguinte, a Comissão considera adequado excluir do âmbito de aplicação da presente decisão as organizações religiosas, na medida em que tratem dados pessoais para as suas atividades missionárias, e os partidos políticos, na medida em que tratem dados pessoais no contexto da nomeação de candidatos.

2.3 **Garantias, direitos e obrigações**

2.3.1 *Licitude e lealdade do tratamento*

(33) Os dados pessoais devem ser objeto de um tratamento lícito e leal.

(34) Este princípio está consagrado no artigo 3.º, n.os 1 e 2, da Lei relativa à proteção de informações pessoais e é reforçado pelo disposto no artigo 59.º da Lei relativa à proteção de informações pessoais, que proíbe o tratamento de dados pessoais «por meio fraudulento, inadequado ou injusto», «sem autoridade legal» ou «sem ser a autoridade competente» ([50]). Estes princípios gerais do tratamento lícito são estabelecidos nos artigos 15.º a 19.º da Lei relativa à proteção de informações pessoais, que estabelecem as diferentes bases jurídicas para o tratamento (recolha, utilização e fornecimento a terceiros), incluindo as circunstâncias em que tal pode implicar uma alteração da finalidade (artigo 18.º da Lei relativa à proteção de informações pessoais).

([45]) Artigos 15.º a 17.º da Lei relativa à imprensa.

([46]) Cada órgão de imprensa ou meio de comunicação social deve ter o seu próprio provedor para prevenir e sanar eventuais danos causados pela imprensa (por exemplo, recomendando a correção de notícias falsas ou que prejudiquem a reputação de terceiros), artigo 6.º da Lei relativa à imprensa.

([47]) A Comissão é composta por entre 40 e 90 comissários responsáveis pela arbitragem, nomeados pelo Ministro da Cultura, do Desporto e do Turismo entre pessoas qualificadas como juízes, advogados, pessoas envolvidas no jornalismo durante, pelo menos, dez anos, ou outras pessoas com conhecimentos especializados relacionados com a imprensa. Ao mesmo tempo, os comissários responsáveis pela arbitragem não podem ser funcionários públicos, membros de partidos políticos ou jornalistas. Nos termos do artigo 8.º da Lei relativa à imprensa, os comissários responsáveis pela arbitragem devem desempenhar as suas funções de forma independente e não podem estar sujeitos a quaisquer ordens ou instruções relacionadas com essas funções. Além disso, estão em vigor regras específicas para prevenir conflitos de interesses, por exemplo, regras que excluem comissários específicos do tratamento de casos individuais em que o cônjuge ou familiares sejam parte (artigo 10.º da Lei relativa à imprensa). A Comissão pode tratar os litígios através de conciliação ou arbitragem, mas pode igualmente formular recomendações para sanar infrações (artigo 5.º da Lei relativa à imprensa).

([48]) Artigo 30.º da Lei relativa à imprensa.

([49]) Artigo 5.º da Lei relativa à imprensa.

([50]) O artigo 59.º da Lei relativa à proteção de informações pessoais proíbe qualquer pessoa que trate ou tenha tratado informações pessoais para obter informações pessoais ou obter o consentimento para o tratamento de informações pessoais por meio fraudulento, inadequado ou injusto, divulgue informações pessoais obtidas no exercício da sua atividade comercial ou as forneça para utilização por terceiros sem autorização ou danifique, destrua, altere, forje ou divulgue informações pessoais de outrem sem autoridade legal ou sem ser a autoridade competente. Uma violação desta proibição pode conduzir a sanções penais, ver artigo 71.º, n.os 5 e 6 e artigo 72.º, n.º 2, da Lei relativa à proteção de informações pessoais. Além disso, o artigo 70.º, n.º 2, da Lei relativa à proteção de informações pessoais permite a aplicação de uma sanção penal pela obtenção de informações pessoais tratadas por terceiros de modo fraudulento ou com recurso a outros meios ou métodos injustos, ou pelo seu fornecimento a terceiros para fins lucrativos ou injustos, bem como por cumplicidade ou organização desse comportamento.

(35) Nos termos do artigo 15.º, n.º 1, da Lei relativa à proteção de informações pessoais, um responsável pelo tratamento só pode recolher dados pessoais (no âmbito da finalidade da recolha) com base num número limitado de fundamentos jurídicos. Trata-se de: 1) consentimento do titular dos dados ([51]) (ponto 1); 2) necessidade de celebrar e executar um contrato com o titular dos dados (ponto 4); 3) uma autorização especial nos termos da lei ou a necessidade de cumprimento de uma obrigação legal (ponto 2); a necessidade ([52]) de uma instituição pública desempenhar as funções no âmbito da sua jurisdição, conforme previsto na lei; 4) a necessidade manifesta de proteção da vida, do corpo ou dos interesses patrimoniais do titular dos dados ou de um terceiro perante um perigo iminente (apenas se o titular dos dados não estiver em condições de manifestar a sua intenção ou se não for possível obter o consentimento prévio) (ponto 5); 5) a necessidade de alcançar o «interesse justificável» do responsável pelo tratamento se este for «manifestamente superior» aos interesses do titular dos dados (e apenas quando o tratamento apresentar uma «relação significativa» com o interesse legítimo e não exceder o que é razoável) (ponto 6) ([53]). Estes fundamentos para o tratamento são essencialmente equivalentes aos previstos no artigo 6.º do Regulamento (UE) 2016/679, incluindo o fundamento de «interesse justificável» que é igual ao fundamento de «interesse legítimo» previsto no artigo 6.º, n.º 1, alínea f), do Regulamento (UE) 2016/679.

(36) Uma vez recolhidos, os dados pessoais podem ser utilizados para a finalidade de recolha (artigo 15.º, n.º 1, da Lei relativa à proteção de informações pessoais), ou «no âmbito razoavelmente relacionado» com a finalidade da recolha, tendo em conta eventuais desvantagens causadas ao titular dos dados e desde que tenham sido adotadas as medidas de segurança necessárias (por exemplo, cifragem) (artigo 15.º, n.º 3, da Lei relativa à proteção de informações pessoais). Para determinar se a finalidade de utilização está «razoavelmente relacionada» com a finalidade de recolha inicial, o decreto de execução estabelece critérios específicos semelhantes aos do artigo 6.º, n.º 4, do Regulamento (UE) 2016/679. Em especial, deve existir uma relevância considerável para a finalidade inicial, uma previsibilidade da utilização adicional (por exemplo, à luz das circunstâncias em que as informações foram recolhidas e, sempre que possível, os dados devem ser pseudonimizados ([54]). Os critérios específicos utilizados por um responsável pelo tratamento nesta avaliação devem ser previamente divulgados na política de privacidade ([55]). Além disso, o responsável pela privacidade (ver considerando (94)) é especificamente obrigado a verificar se a utilização posterior ocorre dentro desses parâmetros.

([51]) O consentimento deve ser dado livremente, informado, específico e expresso de uma das várias formas previstas por lei. Em qualquer caso, o consentimento não pode ser obtido por meios fraudulentos, inadequados ou injustos por qualquer outra forma (artigo 59.º, n.º 1, da Lei relativa à proteção de informações pessoais). Em primeiro lugar, nos termos do artigo 4.º, ponto 2, da Lei relativa à proteção de informações pessoais, os titulares dos dados têm o direito de «consentir ou não» e de «decidir o âmbito do consentimento» e devem ser informados desse facto (artigo 15.º, n.º 2, artigo 16.º, n.ºs 2 e 3, artigo 17.º, n.º 2, e artigo 18.º, n.º 3, da Lei relativa à proteção de informações pessoais). O artigo 22.º, n.º 5, da Lei relativa à proteção de informações pessoais contém uma garantia adicional ao proibir um responsável pelo tratamento de recusar o fornecimento de bens ou serviços quando tal possa comprometer a liberdade de escolha da pessoa singular na concessão do consentimento. Incluem-se aqui as situações em que apenas certos tipos de tratamento exigem o consentimento (enquanto outros têm por base um contrato), abrangendo também o tratamento posterior de dados pessoais recolhidos no contexto do fornecimento de bens ou serviços. Em segundo lugar, nos termos do artigo 15.º, n.º 2, do artigo 17.º, n.os 2 e 3, e do artigo 18.º, n.º 3, da Lei relativa à proteção de informações pessoais, ao solicitar o consentimento, o responsável pelo tratamento deve informar o titular dos dados dos «elementos» dos dados pessoais em causa (por exemplo, que diz respeito a dados sensíveis, ver artigo 17.º, n.º 2, ponto 2, alínea a), do Decreto de Execução da Lei relativa à proteção de informações pessoais), a finalidade do tratamento, o período de conservação e qualquer destinatário dos dados. Qualquer pedido deste tipo deve ser apresentado «de forma explicitamente reconhecível», distinguindo as matérias que exigem o consentimento de outras matérias (artigo 22.º, n.os 1 a 4 da Lei relativa à proteção de informações pessoais). O artigo 17.º, n.º 1, pontos 1 a 6, do Decreto de Execução da Lei relativa à proteção de informações pessoais estabelece os métodos específicos através dos quais o responsável pelo tratamento deve obter o consentimento, como o consentimento escrito com a assinatura do titular dos dados ou o consentimento (na resposta) por correio eletrónico. Embora a Lei relativa à proteção de informações pessoais não confira especificamente às pessoas singulares o direito geral de retirar o consentimento, estas, em vez disso, dispõem do direito de obter a suspensão do tratamento dos dados que lhes digam respeito, o qual, quando exercido, conduzirá à cessação do tratamento e ao apagamento dos dados (ver considerando 78 relativo ao direito de suspensão).

([52]) De acordo com as informações recebidas da Comissão de Proteção de Informações Pessoais, as instituições públicas só podem invocar este fundamento se o tratamento de informações pessoais for inevitável, ou seja, deve ser impossível ou excessivamente difícil para a instituição desempenhar as suas funções sem proceder ao tratamento dos dados.

([53]) O artigo 39.º-3 da Lei relativa à proteção de informações pessoais impõe obrigações específicas (mais rigorosas) aos prestadores de serviços de informação e comunicação no que respeita à recolha e utilização de informações pessoais dos seus utilizadores. Em especial, exige que o prestador obtenha o consentimento do utilizador, após ter fornecido informações sobre a finalidade da recolha/utilização, as categorias de informações pessoais a recolher e o período durante o qual as informações serão tratadas (artigo 39.º-3, n.º 1, da Lei relativa à proteção de informações pessoais). O mesmo se aplica perante a alteração de algum dos seguintes aspetos. A falta de consentimento para a recolha de informações está sujeita a sanções penais (artigo 71.º, n.ºs 4 e 5, da Lei relativa à proteção de informações pessoais). Excecionalmente, as informações pessoais dos utilizadores podem ser recolhidas ou utilizadas pelos fornecedores de informação e comunicação sem obter o consentimento prévio. Este é o caso: 1) quando é claramente difícil obter o consentimento normal para as informações pessoais necessárias para executar o contrato que rege a prestação de serviços de comunicação de informações por razões económicas e tecnológicas (por exemplo, quando são inevitavelmente criados dados pessoais no processo de execução de um contrato, tais como informações sobre faturação, registos de acesso e registos de pagamento); 2) quando for necessário para o pagamento de encargos na sequência da prestação de serviços de informação e comunicação; ou 3) quando permitido por outra legislação (por exemplo, o artigo 21.º, n.º 1, ponto 6, da Lei relativa à proteção dos consumidores no comércio eletrónico prevê que os operadores comerciais podem recolher informações pessoais sobre os tutores legais de um menor, a fim de confirmar se foi obtido um consentimento válido em nome do menor) (artigo 39.º-3, n.º 2, da Lei relativa à proteção de informações pessoais). Em todos os casos, os fornecedores de informação e comunicação não podem recusar-se a prestar serviços pelo simples facto de o utilizador não fornecer mais informações pessoais do que o mínimo exigido (ou seja, as informações necessárias para executar os elementos essenciais do serviço em causa), ver o artigo 39.º-3, n.º 3, da Lei relativa à proteção de informações pessoais.

([54]) Ver o artigo 14.º-2 do Decreto de Execução da Lei relativa à proteção de informações pessoais.

([55]) Artigo 14.º-2, n.º 2, do Decreto de Execução da Lei relativa à proteção de informações pessoais.

(37) Aplicam-se regras semelhantes (mas algo mais rigorosas) ao fornecimento de dados a terceiros. Nos termos do artigo 17.º, n.º 1, da Lei relativa à proteção de informações pessoais, o fornecimento de dados pessoais a terceiros é permitido com base no consentimento ([56]) ou, no âmbito da finalidade da recolha, se a informação tiver sido recolhida com base num dos fundamentos jurídicos previstos no artigo 15.º, n.º 1, pontos 2, 3 e 5, da Lei relativa à proteção de informações pessoais. Tal exclui, em especial, qualquer divulgação baseada no «interesse justificável» do responsável pelo tratamento. Além do mencionado, o artigo 17.º, n.º 4, da Lei relativa à proteção de informações pessoais permite a disponibilização a um terceiro «no âmbito razoavelmente relacionado» com a finalidade da recolha, também tendo em conta eventuais desvantagens causadas ao titular dos dados e desde que tenham sido adotadas as medidas de segurança necessárias (por exemplo, cifragem). Devem ser tidos em conta os mesmos fatores que os descritos no considerando (36) para avaliar se a disposição está no âmbito razoavelmente relacionado com a finalidade de recolha e se são aplicáveis as mesmas garantias (ou seja, no que respeita à transparência através da política de privacidade e à participação do responsável pela privacidade).

(38) A receção de dados pessoais pela União por um responsável pelo tratamento coreano é considerada uma «recolha» na aceção do artigo 15.º da Lei relativa à proteção de informações pessoais. A Notificação n.º 2021--5 (anexo I, ponto I, da presente decisão) esclarece que a finalidade para a qual os dados foram transferidos pela entidade da UE em causa constitui a finalidade da recolha para o responsável pelo tratamento de dados coreano. Consequentemente, os responsáveis coreanos pelo tratamento de dados que recebem dados pessoais da União são, em princípio, obrigados a tratar essas informações no âmbito da finalidade da transferência, em conformidade com o disposto no artigo 17.º da Lei relativa à proteção de informações pessoais.

(39) Aplicam-se limitações especiais no caso de o responsável pelo tratamento procurar utilizar os dados pessoais ou fornecê-los a terceiros para uma finalidade diferente da finalidade de recolha ([57]). Nos termos do artigo 18.º, n.º 2, da Lei relativa à proteção de informações pessoais, um responsável pelo tratamento privado pode excecionalmente ([58]) utilizar dados pessoais ou fornecê-los a terceiros para uma finalidade diferente: 1) tendo por base o consentimento adicional (no sentido de «autónomo») do titular dos dados; 2) quando tal esteja previsto em disposições legais especiais; ou 3) quando seja manifestamente necessário para a proteção da vida, do corpo ou dos interesses patrimoniais do titular dos dados ou de um terceiro perante um perigo iminente (apenas se o titular dos dados não estiver em condições de manifestar a sua intenção e se não for possível obter o consentimento prévio) ([59]).

(40) As instituições públicas podem também utilizar dados pessoais ou fornecê-los a terceiros para uma finalidade diferente em certas situações. Tal inclui os casos em que, de outro modo, as instituições públicas não poderiam exercer as suas funções estatutárias, conforme previsto na lei, sob reserva de autorização da Comissão de Proteção de Informações Pessoais. Além disso, as instituições públicas podem fornecer dados pessoais a outra autoridade ou tribunal, sempre que tal seja necessário para a investigação e a ação penal por crimes ou para um despacho de acusação, para que um tribunal exerça as suas funções relacionadas com processos judiciais em curso, ou para a execução de uma sanção penal ou de um despacho de guarda ou de detenção ([60]). Podem também fornecer dados pessoais a um governo estrangeiro ou a uma organização internacional para cumprir uma obrigação legal decorrente de um tratado ou de uma convenção internacional, caso em que têm também de cumprir os requisitos aplicáveis às transferências transfronteiriças de dados (ver considerando (90)).

(41) Os princípios da licitude e da lealdade do tratamento são, por conseguinte, aplicados no quadro jurídico coreano de uma forma essencialmente equivalente à do Regulamento (UE) 2016/679, autorizando o tratamento apenas com base em fundamentos legítimos e claramente definidos. Além disso, em todos os casos mencionados, o tratamento só é permitido se não for suscetível de «violar injustamente» os interesses do titular dos dados ou de um terceiro, o que exige uma ponderação de interesses. Além disso, o artigo 18.º, n.º 5, da Lei relativa à proteção de informações pessoais prevê garantias adicionais quando o responsável pelo tratamento fornece os dados pessoais a terceiros, o que pode incluir um pedido para restringir a finalidade e o método de utilização ou a implementação de medidas de segurança específicas. Por sua vez, os terceiros ficam obrigados a executar as medidas solicitadas.

([56]) As violações do disposto no artigo 17.º, n.º 1, ponto 1, da Lei relativa à proteção de informações pessoais podem conduzir à aplicação de sanções penais (artigo 71.º, n.º 1, da Lei relativa à proteção de informações pessoais).

([57]) Por «finalidade prevista» entende-se a finalidade para a qual as informações foram recolhidas. Por exemplo, quando as informações são recolhidas com base no consentimento da pessoa singular em causa, a finalidade prevista é a que é comunicada à pessoa singular nos termos do artigo 15.º, n.º 2, da Lei relativa à proteção de informações pessoais.

([58]) Ver artigo 18.º, n.º 1, da Lei relativa à proteção de informações pessoais. As violações do disposto no artigo 18.º, n.ºs 1 e 2, podem conduzir à aplicação de sanções penais (artigo 71.º, n.º 2, da Lei relativa à proteção de informações pessoais).

([59]) A utilização de informações pessoais ou o seu fornecimento a terceiros por prestadores de serviços de informação e comunicação para finalidade diferente da inicial só pode ocorrer com base nos motivos enunciados no artigo 18.º, n.º 2, pontos 1 e 2, da Lei relativa à proteção de informações pessoais (ou seja, quando é obtido consentimento adicional ou quando a lei prevê disposições especiais). Ver artigo 18.º, n.º 2, da Lei relativa à proteção de informações pessoais.

([60]) Exceto quando o tratamento for necessário para a investigação de crimes, para um despacho de acusação e para ações penais, as instituições públicas que utilizem informações pessoais ou as forneçam a terceiros para finalidades diferentes da finalidade de recolha (por exemplo, quando tal seja especificamente permitido por lei ou necessário para executar um tratado) são obrigadas a publicar os fundamentos jurídicos para o tratamento, a sua finalidade e âmbito de aplicação no seu sítio Web ou no Jornal Oficial e a conservar registos (artigo 18.º, n.º 4, da Lei relativa à proteção de informações pessoais com o artigo 15.º do Decreto de Execução da Lei relativa à proteção de informações pessoais).

(42) Por último, o artigo 28.º-2 da Lei relativa à proteção de informações pessoais permite o tratamento (posterior) de informações pseudonimizadas sem o consentimento da pessoa singular em causa para efeitos de estatísticas, de investigação científica ([61]) e de arquivo no interesse público, sob reserva de garantias específicas. À semelhança do Regulamento (UE) 2016/679 ([62]), a Lei relativa à proteção de informações pessoais facilita, por conseguinte, o tratamento (posterior) de dados pessoais para essas finalidades, num quadro que preveja garantias adequadas para proteger os direitos das pessoas singulares. Em vez de recorrer à pseudonimização como possível garantia, a Lei relativa à proteção de informações pessoais impõe-na como condição prévia para a realização de determinadas atividades de tratamento para efeitos de estatísticas, de investigação científica e de arquivo no interesse público (por exemplo, para poder tratar os dados sem consentimento ou combinar diferentes conjuntos de dados).

(43) Além disso, a Lei relativa à proteção de informações pessoais impõe um conjunto de garantias específicas, em especial em termos de medidas técnicas e organizativas necessárias, conservação de registos, limitações à partilha de dados e resolução de eventuais riscos de reidentificação. A combinação das várias garantias descritas nos considerandos (44) a (48) garante que o tratamento de dados pessoais neste contexto está sujeito a proteções essencialmente equivalentes às que seriam exigidas em conformidade com o Regulamento (UE) 2016/679.

(44) Em primeiro lugar, e mais importante ainda, o artigo 28.º-5, n.º 1, da Lei relativa à proteção de informações pessoais proíbe o tratamento de informações pseudonimizadas com a finalidade de identificar uma determinada pessoa. Se, ainda assim, forem geradas informações suscetíveis de identificar uma pessoa singular durante o tratamento de informações pseudonimizadas, o responsável pelo tratamento deve suspender imediatamente o tratamento e destruir essas informações (artigo 28.º-5, n.º 2, da Lei relativa à proteção de informações pessoais). O incumprimento destas disposições está sujeito a coimas e constitui uma infração penal ([63]). Tal significa que, mesmo nas situações em que seria possível, *na prática*, reidentificar a pessoa, essa reidentificação é proibida *por lei*.

(45) Em segundo lugar, quando se tratar (posteriormente) informações pseudonimizadas para essas finalidades, o responsável pelo tratamento deve adotar medidas tecnológicas, de gestão e físicas específicas para garantir a segurança das informações (incluindo o armazenamento e a gestão separados das informações necessárias para repor a informação pseudonimizadas no seu estado original) ([64]). Além disso, devem ser conservados registos das informações pseudonimizadas tratadas, da finalidade do tratamento, do histórico de utilização e de quaisquer terceiros destinatários (artigo 29.º-5, n.º 2, do Decreto de Execução da Lei relativa à proteção de informações pessoais).

(46) Em terceiro e último lugar, a Lei relativa à proteção de informações pessoais prevê garantias específicas para impedir a identificação de pessoas singulares por terceiros em caso de partilha de informações. Em especial, ao fornecerem informações pseudonimizadas a terceiros para efeitos de estatísticas, de investigação científica ou de arquivo de interesse público, os responsáveis pelo tratamento não podem incluir informações que possam ser utilizadas para identificar uma pessoa singular específica (artigo 28.º-2, n.º 2, da Lei relativa à proteção de informações pessoais) ([65]).

(47) Mais especificamente, embora a Lei relativa à proteção de informações pessoais permita a combinação de informações pseudonimizadas (tratadas por diferentes responsáveis pelo tratamento) para efeitos de estatísticas, de investigação científica ou de arquivo no interesse público, a Lei relativa à proteção de informações pessoais reserva esse poder a instituições especializadas dotadas de instalações de segurança específicas (artigo 28.º-3, n.º 1, da Lei relativa à proteção de informações pessoais) ([66]). Ao solicitar uma combinação de dados pseudonimizados, o responsável pelo tratamento deve apresentar documentação sobre, entre outros elementos, os dados a

([61]) O artigo 2.º, n.º 8, da Lei relativa à proteção de informações pessoais define «investigação científica» como a investigação que aplica métodos científicos, como o desenvolvimento tecnológico e a demonstração, a investigação fundamental, a investigação aplicada e a investigação financiada pelo setor privado. Estas categorias correspondem às estabelecidas no considerando 159 do Regulamento (UE) 2016/679.

([62]) Ver o artigo 5.º, n.º 1, alínea b), e artigo 89.º, n.ºs 1 e 2, e os considerandos 50 e 157 do Regulamento (UE) 2016/679.

([63]) Ver artigo 28.º-6.º, n.º 1, artigo 71.º, n.ºs 4-3, e artigo 75.º, n.º 2, ponto 4-4, da Lei relativa à proteção de informações pessoais.

([64]) Artigo 28.º-4 da Lei relativa à proteção de informações pessoais e 29.º-5 do Decreto de Execução da Lei relativa à proteção de informações pessoais. O incumprimento desta obrigação está sujeito a sanções administrativas e penais, ver o artigo 73.º, n.º 1, e artigo 75.º, n.º 2, ponto 6, da Lei relativa à proteção de informações pessoais.

([65]) As violações destes requisitos podem conduzir à aplicação de sanções penais (artigo 71.º, n.º 2, da Lei relativa à proteção de informações pessoais). A Comissão de Proteção de Informações Pessoais começou imediatamente a aplicar estas novas regras, por exemplo, na sua decisão de 28 de abril de 2021, em que impôs uma coima e medidas corretivas a uma empresa que, entre outras violações da Lei relativa à proteção de informações pessoais, não cumpriu o requisito previsto no artigo 28.º-2, n.º 2, da Lei relativa à proteção de informações pessoais, ver https://www.pipc.go.kr/np/cop/bbs/selectBoardArticle.do?bbsId=BS074&mCode=C020010000&nttId=7298&fbclid=IwAR3SKcMQi6G5pR9k4I7j6GNXtc8aBVDOwcURevvvzQtYI7AS40UKYXoOXo8.

([66]) Para a designação da instituição especializada («Agência Especializada em Combinação de Dados»), é necessário apresentar um pedido à Comissão de Proteção de Informações Pessoais juntamente com documentos comprovativos que especifiquem, nomeadamente, as instalações e o equipamento criados para combinar de forma segura dados pseudonimizados e que confirmem que o requerente emprega, pelo menos, três membros do pessoal a tempo inteiro com qualificações ou experiência em matéria de proteção de dados pessoais (artigo 29.º-2, n.ºs 1 e 2, do Decreto de Execução da Lei relativa à proteção de informações pessoais). Os requisitos pormenorizados, por exemplo no que respeita às qualificações do pessoal, às instalações disponíveis, às medidas de segurança, às políticas e procedimentos internos, bem como os requisitos financeiros constam da Notificação n.º 2020-9 da Comissão de Proteção de Informações Pessoais relativa à combinação e a divulgação de informações anónimas (anexo I). A designação de uma agência especializada em combinação de dados pode ser revogada pela Comissão de Proteção de Informações Pessoais (após a realização de uma audição) por determinados motivos, por exemplo, se a agência deixar de cumprir as normas de segurança exigidas para a designação ou se ocorrer uma violação de dados no contexto da combinação de dados (artigo 29.º-2, n.ºs 5 a 6, do Decreto de Execução da Lei relativa à proteção de informações pessoais). A Comissão de Proteção de Informações Pessoais deve publicar a designação (ou revogação da designação) de uma agência especializada em combinação de dados (artigo 29.º-2, n.º 7, do Decreto de Execução da Lei relativa à proteção de informações pessoais).

combinar, a finalidade da combinação, bem como as medidas de segurança propostas para o tratamento dos dados combinados ([67]). Para permitir a combinação, o responsável pelo tratamento tem de enviar os dados para serem combinados à instituição especializada e fornecer uma «chave de combinação» (ou seja, as informações que foram utilizadas na pseudonimização) à Agência de Internet e Segurança da Coreia ([68]). Esta última gera «dados de ligação da chave de combinação» (que permite associar as chaves de combinação de diferentes requerentes a fim de obter a combinação dos conjuntos de dados) e fornece-os à instituição especializada ([69]).

(48) O responsável pelo tratamento que solicita a combinação pode analisar as informações combinadas nas instalações da instituição especializada, num espaço em que são aplicadas medidas de segurança técnica, física e administrativa específicas (artigo 29.º-3 do Decreto de Execução da Lei relativa à proteção de informações pessoais). Os responsáveis pelo tratamento que contribuem com um conjunto de dados para essa combinação só podem recolher os dados combinados fora da instituição especializada na sequência de uma maior pseudonimização ou anonimização dos dados combinados e com a aprovação dessa instituição (artigo 28.º-3, n.º 2, da Lei relativa à proteção de informações pessoais) ([70]). Ao ponderar se deve ou não conceder essa aprovação, a instituição avaliará a ligação entre os dados combinados e a finalidade do tratamento e se foi elaborado um plano de segurança específico para a utilização desses dados ([71]). A exportação de informações combinadas para fora da instituição não será permitida se as informações contiverem dados que permitam a identificação de uma pessoa ([72]). Por último, a combinação e a divulgação de dados pseudonimizados pela instituição especializada são supervisionadas pela Comissão de Proteção de Informações Pessoais (artigo 29.º-4, n.º 3, do Decreto de Execução da Lei relativa à proteção de informações pessoais).

2.3.2 *Tratamento de categorias especiais de dados pessoais*

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

(50) A Lei relativa à proteção de informações pessoais contém regras específicas relativas ao tratamento de dados sensíveis ([73]), que são definidos como dados pessoais que revelem informações sobre ideologia, crença, admissão ou saída de um sindicato ou partido político, opiniões políticas, saúde e vida sexual de uma pessoa, bem como outras informações pessoais suscetíveis de ameaçar «notoriamente» a privacidade do titular dos dados e que tenham sido prescritas como informações sensíveis por decreto presidencial ([74]). De acordo com os esclarecimentos prestados pela Comissão de Proteção de Informações Pessoais, a vida sexual é interpretada como abrangendo também a orientação ou preferências sexuais da pessoa ([75]). Além disso, o artigo 18.º do decreto de execução acrescenta outras categorias ao âmbito de dados sensíveis, em especial as informações de ADN obtidas a partir de testes genéticos e os dados que constituem o registo criminal. A recente alteração do Decreto de Execução da Lei relativa à proteção de informações pessoais alargou ainda mais o conceito de dados sensíveis, incluindo também dados pessoais que revelem a origem racial ou étnica e informações biométricas ([76]). 'Na sequência dessa alteração, o conceito de dados sensíveis ao abrigo da Lei relativa à proteção de informações pessoais é essencialmente equivalente à constante do artigo 9.º do Regulamento (UE) 2016/679.

(51) Nos termos do artigo 23.º, n.º 1, da Lei relativa à proteção de informações pessoais e à semelhança do disposto no artigo 9.º, n.º 1, do Regulamento (UE) 2016/679, o tratamento de dados sensíveis é, em geral, proibido, salvo se se aplicar uma das exceções elencadas ([77]). Estas limitam o tratamento aos casos em que o responsável pelo

([67]) Artigo 8.º, n.ºs 1 a 2, da Notificação n.º 2020-9 relativa à combinação e a divulgação de informações pseudonimizadas.
([68]) Artigo 2.º, n.ºs 3 e 6, e artigo 9.º, n.º 1, da Notificação n.º 2020-9 relativa à combinação e a divulgação de informações pseudonimizadas.
([69]) Artigo 2.º, n.º 4, e artigo 9.º, n.ºs 2 a 3, da Notificação n.º 2020-9 relativa à combinação e a divulgação de informações pseudonimizadas. A instituição especializada deve destruir imediatamente os dados de ligação da chave de combinação após a combinação (artigo 9.º, n.º 4, da notificação).
([70]) As violações dos requisitos para a combinação de conjuntos de dados podem conduzir à aplicação de sanções penais (artigo 71.º, n.º 4-2, da Lei relativa à proteção de informações pessoais). Ver também o artigo 29.º-2, n.º 4, do Decreto de Execução da Lei relativa à proteção de informações pessoais.
([71]) O procedimento para aprovar uma divulgação de dados combinados encontra-se descrito no artigo 11.º da Notificação n.º 2020-9 relativa à combinação e a divulgação de informações pseudonimizadas. Em especial, a instituição especializada deve criar um «comité de avaliação de divulgação», composto por membros com conhecimentos e experiência substanciais em matéria de proteção de dados.
([72]) Artigo 29.º-2, n.º 4, do Decreto de Execução da Lei relativa à proteção de informações pessoais e Notificação n.º 2020-9, artigo 11.º.
([73]) A necessidade de prever proteções específicas para o tratamento de dados sensíveis, tais como dados relativos à saúde ou ao comportamento sexual, foi igualmente reconhecida pelo Tribunal Constitucional coreano, ver Decisão n.º HunMa 1139 do Tribunal Constitucional, de 31 de maio de 2007.
([74]) Artigo 23.º, n.º 1, da Lei relativa à proteção de informações pessoais.
([75]) Ver também o Manual da Lei relativa à proteção de informações pessoais, capítulo III, secção 2 relativa ao artigo 23.º (p. 157-164).
([76]) Ou seja, informações pessoais resultantes de um tratamento técnico específico de dados relativo às características físicas, fisiológicas ou comportamentais de uma pessoa singular para efeitos de identificação única dessa pessoa.
([77]) O incumprimento destes requisitos pode dar origem a sanções nos termos do artigo 71.º, ponto 3, da Lei relativa à proteção de informações pessoais.

tratamento informa o titular dos dados em conformidade com os artigos 15.º e 17.º da Lei relativa à proteção de informações pessoais e obtém consentimento separado (ou seja, separado do consentimento para o tratamento de outros dados pessoais) ou em que o tratamento é exigido ou permitido por lei. As autoridades públicas podem também tratar informações biométricas, informações de ADN obtidas a partir de testes genéticos, informações pessoais que revelem a origem racial ou étnica e dados que constituam um registo criminal por motivos exclusivamente disponíveis (por exemplo, quando necessário para a investigação de crimes ou, se necessário, para que um tribunal prossiga um processo) ([78]). Como tal, as bases jurídicas disponíveis para o tratamento de dados sensíveis são mais limitadas do que para outros tipos de dados pessoais e ainda mais restritivas no direito coreano do que as previstas no artigo 9.º, n.º 2, do Regulamento (UE) 2016/679.

(52) Além disso, o artigo 23.º, n.º 2, da Lei relativa à proteção de informações pessoais – incumprimento que pode conduzir a sanções ([79]) – sublinha a importância, em particular, de assegurar segurança adequada no tratamento de dados sensíveis, de modo que estes não possam ser extraviados, furtados, divulgados, forjados, alterados ou danificados. Embora este seja um requisito geral ao abrigo do artigo 29.º da Lei relativa à proteção de informações pessoais, o artigo 3.º, n.º 4, esclarece que o nível de segurança tem de se adaptar ao tipo de dados pessoais que são tratados, o que significa ser necessário ter em conta os riscos em particular envolvidos no tratamento de dados sensíveis. Além disso, o tratamento de dados deve ser sempre efetuado de forma a minimizar a possibilidade de violar a privacidade do titular dos dados e, se possível, de forma anónima (artigo 3.º, n.ºs 6 e 7, da Lei relativa à proteção de informações pessoais). Estes requisitos são particularmente pertinentes quando o tratamento diz respeito a dados sensíveis.

2.3.3 *Limitação das finalidades*

(53) Os dados pessoais devem ser recolhidos para uma finalidade específica e de um modo que não seja incompatível com a finalidade do tratamento.

(54) Este princípio é assegurado pelo artigo 3.º, n.ºs 1 e 2, da Lei relativa à proteção de informações pessoais, segundo o qual o responsável pelo tratamento deve «especificar e explicitar» a finalidade do tratamento, tratar os dados pessoais de forma adequada e não os utilizar para além dessa finalidade. O princípio geral da limitação da finalidade é igualmente confirmado no artigo 15.º, n.º 1, no artigo 18.º, n.º 1, no artigo 19.º e – para os subcontratantes – no artigo 26.º, n.º 1, ponto 1, n.ºs 5 e 7, da Lei relativa à proteção de informações pessoais. Em especial, os dados pessoais só podem, em princípio, ser utilizados e fornecidos a terceiros no âmbito da finalidade para a qual foram recolhidos (artigo 15.º, n.º 1, e artigo 17.º, n.º 1, ponto 2). O tratamento para uma finalidade compatível, ou seja, «dentro do âmbito razoavelmente relacionado com a finalidade inicial da recolha», só pode ocorrer se não afetar negativamente os titulares dos dados em causa e se forem adotadas medidas de segurança (como a cifragem) necessárias (artigo 15.º, n.º 3, e artigo 17.º, n.º 4, da Lei relativa à proteção de informações pessoais). Para determinar se o tratamento posterior se destina a uma finalidade compatível, o Decreto de Execução da Lei relativa à proteção de informações pessoais enumera critérios específicos semelhantes aos previstos no artigo 6.º, n.º 4, do Regulamento (UE) 2016/679, ver o considerando (36).

(55) Conforme explicado no considerando (38), a finalidade da recolha no caso de os responsáveis pelo tratamento coreanos receberem dados pessoais da União é a finalidade para a qual os dados são transferidos. Uma alteração de finalidade pelo responsável pelo tratamento só é autorizada a título excecional, em casos específicos (enumerados) (artigo 18.º, n.º 2, pontos 1 a 3, da Lei relativa à proteção de informações pessoais, ver também o considerando (39)). Na medida em que uma alteração da finalidade é autorizada por lei, esta legislação deve, por sua vez, respeitar o direito fundamental à privacidade e à proteção de dados, bem como os princípios da necessidade e da proporcionalidade estabelecidos na Constituição coreana. Além disso, o artigo 18.º, n.ºs 2 e 5, da Lei relativa à proteção de informações pessoais prevê garantias adicionais, em especial o requisito de que essa alteração de finalidade não pode violar injustamente os interesses do titular dos dados, o que implica sempre uma ponderação de interesses. Esta disposição prevê um nível de proteção essencialmente equivalente ao previsto no artigo 5.º, n.º 1, alínea b), e no artigo 6.º, conjugado com o considerando 50 do Regulamento (UE) 2016/679.

2.3.4 *Exatidão e minimização dos dados*

(56) Os dados pessoais devem ser exatos e, se necessário, atualizados. Devem ser adequados, pertinentes e limitar-se ao que é necessário relativamente às finalidades para que são tratados.

([78]) O artigo 18.º do Decreto de Execução da Lei relativa à proteção de informações pessoais prevê que as categorias de dados aí enumeradas fiquem excluídas do disposto no artigo 23.º, n.º 1, da lei, quando tratadas por uma instituição pública nos termos do artigo 18.º, n.º 2, pontos 5 a 9, da Lei relativa à proteção de informações pessoais.

([79]) Ver artigo 73.º, ponto 1, e artigo 75.º, n.º 2, ponto 6, da Lei relativa à proteção de informações pessoais.

(57) O princípio da exatidão é igualmente reconhecido no artigo 3.º, n.º 3, da Lei relativa à proteção de informações pessoais, que exige que os dados pessoais sejam exatos e completos, e que estejam atualizados na medida do necessário em relação às finalidades para que os dados são tratados. A minimização dos dados é exigida nos termos do artigo 3.º, n.ºs 1 e 6, e do artigo 16.º, n.º 1, da Lei relativa à proteção de informações pessoais, que estipulam que o responsável pelo tratamento deve recolher dados pessoais (apenas) «na medida do necessário» para a finalidade a que se destinam, recaindo nele o ónus da prova a este respeito. Se for possível cumprir o objetivo da recolha através do tratamento de forma anónima de informações, os responsáveis pelo tratamento devem esforçar-se por o fazer (artigo 3.º, n.º 7, da Lei relativa à proteção de informações pessoais).

2.3.5 *Limitação da conservação*

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

(59) O princípio da limitação da conservação está igualmente previsto no artigo 21.º, n.º 1, da Lei relativa à proteção de informações pessoais ([80]), que exige que o responsável pelo tratamento «destrua» ([81]) os dados pessoais imediatamente após a consecução da finalidade do tratamento ou após o termo do período de conservação dos dados (consoante o que ocorrer primeiro), salvo se a lei exigir conservação posterior ([82]). Neste caso, os dados pessoais pertinentes devem ser armazenados e geridos separadamente de outras informações pessoais (artigo 21.º, n.º 3, da Lei relativa à proteção de informações pessoais).

(60) O artigo 21.º, n.º 1, da Lei relativa à proteção de informações pessoais não se aplica quando os dados pseudonimizados são tratados para efeitos de estatísticas, de investigação científica ou de arquivo no interesse público ([83]). Para garantir o princípio da conservação limitada de dados também neste caso, a Notificação n.º 2021-5 exige que os responsáveis pelo tratamento anonimizem as informações, em conformidade com o artigo 58.º-2 da Lei relativa à proteção de informações pessoais, se os dados não tiverem sido destruídos após o cumprimento da finalidade específica do tratamento ([84]).

2.3.6 *Segurança dos dados*

(61) 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 conta o estado da técnica, os custos conexos e a natureza, o âmbito, o contexto e as finalidades do tratamento, bem como os riscos para os direitos das pessoas singulares.

(62) O artigo 3.º, n.º 4, da Lei relativa à proteção de informações pessoais estabelece um princípio semelhante de segurança, que exige a gestão das informações pessoais pelos responsáveis pelo tratamento de forma segura, de acordo com os métodos de tratamento, os tipos, entre outros aspetos, das informações pessoais, tendo em conta a possibilidade de violação dos direitos dos titulares dos dados e a gravidade dos riscos relevantes. Além disso, o responsável pelo tratamento deve tratar as informações pessoais de forma a minimizar a possibilidade de violar a privacidade do titular dos dados e esforçar-se por tratar os dados pessoais de forma anónima ou pseudonimizada, se possível (artigo 3.º, n.ºs 6 e 7, da Lei relativa à proteção de informações pessoais).

(63) Estes requisitos gerais são aprofundados no artigo 29.º da Lei relativa à proteção de informações pessoais, nos termos do qual qualquer responsável pelo tratamento deve tomar as medidas técnicas, de gestão e físicas, como a elaboração de um plano de gestão interno e a preservação de registos de acesso, entre outros, que sejam necessárias, conforme estipulado em decreto presidencial, de modo que as informações pessoais não possam ser extraviadas, furtadas, divulgadas, forjadas, alteradas ou danificadas. O artigo 30.º, n.º 1, do Decreto de Execução da Lei relativa à proteção de informações pessoais especifica essas medidas por referência 1) à formulação e execução de um plano de gestão

([80]) Artigo 8.º (conjugado com o artigo 8.º-2 do decreto de execução), artigo 11.º (conjugado com o artigo 12.º, n.º 2, do decreto de execução).

([81]) Sobre os métodos de destruição das informações pessoais, ver artigo 16.º do Decreto de Execução da Lei relativa à proteção de informações pessoais. O artigo 21.º, n.º 2, da Lei relativa à proteção de informações pessoais esclarece que tal inclui as medidas necessárias para bloquear a recuperação e o relançamento.

([82]) O incumprimento destes requisitos pode dar origem a sanções penais (artigo 73.º, n.ºs 1 e 2, da Lei relativa à proteção de informações pessoais). O artigo 39.º-6 da Lei relativa à proteção de informações pessoais impõe aos prestadores de serviços de informação e comunicação um requisito adicional de eliminação de informações pessoais de utilizadores que não tenham utilizado os serviços de informação e comunicação oferecidos durante, pelo menos, um ano (a menos que a conservação posterior de dados seja exigida por lei ou ocorra a pedido do indivíduo). As pessoas singulares devem ser informadas da intenção de eliminar as informações 30 dias antes do termo do prazo de um ano (artigo 39.º-6, n.º 2, da Lei relativa à proteção de informações pessoais e artigo 48.º-5, n.º 3, da Lei relativa à proteção de informações pessoais). Se a lei exigir conservação posterior, os dados conservados devem ser armazenados separadamente de outras informações dos utilizadores e só podem ser utilizados ou divulgados em conformidade com essa lei (artigo 48.º-5, n.ºs 1 e 2, do Decreto de Execução da Lei relativa à proteção de informações pessoais).

([83]) Artigo 28.º-7 da Lei relativa à proteção de informações pessoais.

([84]) Notificação n.º 2021-5 (anexo I), ponto 4.

interna para o tratamento seguro de dados pessoais, 2) aos controlos e restrições de acesso, 3) à adoção de tecnologia de cifragem para o armazenamento e a transmissão seguros de dados pessoais, 4) aos registos de acesso, 5) aos programas de segurança e 6) às medidas físicas, tais como um sistema seguro de armazenamento ou bloqueio ([85]).

(64) Além disso, aplicam-se obrigações específicas em caso de violação de dados (artigo 34.º da Lei relativa à proteção de informações pessoais, conjugado com os artigos 39.º e 40.º do Decreto de Execução da Lei relativa à proteção de informações pessoais) ([86]). Em especial, o responsável pelo tratamento é obrigado a notificar sem demora aos titulares dos dados lesados os pormenores da violação ([87]), incluindo informações sobre as contramedidas (obrigatórias) tomadas pelo responsável pelo tratamento e o que os titulares dos dados podem fazer para minimizar o risco de danos (artigo 34.º, n.os 1 e 2, da Lei relativa à proteção de informações pessoais) ([88]). Se a violação de dados disser respeito a, pelo menos, mil titulares de dados, o responsável pelo tratamento deve também comunicar sem demora a violação de dados e as contramedidas tomadas à Comissão de Proteção de Informações Pessoais e à Agência de Internet e Segurança da Coreia, que pode prestar assistência técnica (artigo 34.º, n.º 3, da Lei relativa à proteção de informações pessoais, conjugado com o artigo 39.º do Decreto de Execução da Lei relativa à proteção de informações pessoais). Os responsáveis pelo tratamento são responsáveis pelos danos resultantes de violações de dados, em conformidade com as disposições da Lei Civil sobre responsabilidade civil (ver também o ponto 2.5 sobre reparação) ([89]).

(65) No cumprimento das suas obrigações em matéria de segurança, o responsável pelo tratamento deve ser coadjuvado por um responsável pela privacidade, cujas funções incluem, nomeadamente, a criação de um sistema de controlo interno para prevenir a divulgação, o abuso e a utilização indevida de informações pessoais (artigo 31.º, n.º 2, ponto 4, da Lei relativa à proteção de informações pessoais). Além disso, o responsável pelo tratamento tem o dever de efetuar o controlo e a supervisão adequados dos membros do seu pessoal que tratam dados pessoais, nomeadamente no que respeita à gestão segura dos mesmos. Tal inclui a formação necessária («ensino») dos trabalhadores (artigo 28.º, n.os 1 e 2, da Lei relativa à proteção de informações pessoais). Por último, no caso de subcontratação ulterior, o responsável pelo tratamento deve impor requisitos ao «subcontratante», nomeadamente no que respeita à gestão segura dos dados pessoais («garantias técnicas e de gestão»), bem como supervisionar a forma como os requisitos são aplicados através de inspeções (artigo 26.º, n.os 1 e 4, da Lei relativa à proteção de informações pessoais, conjugado com o artigo 28.º, n.º 1, pontos 3 e 4, e n.º 6, do Decreto de Execução da Lei relativa à proteção de informações pessoais).

2.3.7 *Transparência*

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

([85]) No que respeita ao tratamento de dados pessoais por prestadores de serviços de informação e comunicação, o artigo 39.º-5 da Lei relativa à proteção de informações pessoais prevê explicitamente que o número de pessoas que tratam informações pessoais dos utilizadores deve ser limitado ao mínimo. Além disso, os prestadores de serviços de informação e comunicação devem assegurar que as informações pessoais dos utilizadores não são expostas ao público através da rede de comunicação e informação (artigo 39.º-10, n.º 1, da Lei relativa à proteção de informações pessoais). As informações expostas devem ser eliminadas ou bloqueadas a pedido da Comissão de Proteção de Informações Pessoais (artigo 39.º-10, n.º 2, da Lei relativa à proteção de informações pessoais). De um modo mais geral, os prestadores de serviços de informação e comunicação (e terceiros que recebem dados pessoais dos utilizadores) estão sujeitos a obrigações de segurança adicionais, especificadas no artigo 48.º, n.º 2, do Decreto de Execução da Lei relativa à proteção de informações pessoais, por exemplo, o desenvolvimento e a aplicação de um plano de gestão interna no que respeita a medidas de segurança, medidas para assegurar o controlo do acesso, a cifragem, a utilização de *software* para detetar programas maliciosos, etc.

([86]) Além disso, há uma proibição geral de danificar, destruir, alterar, forjar ou divulgar informações pessoais sem autoridade legal (ver artigo 59.º, ponto 3, da Lei relativa à proteção de informações pessoais).

([87]) O requisito de notificação da pessoa singular não se aplica na medida em que ocorra uma violação de dados no que respeita a informações pseudonimizadas tratadas para efeitos de estatísticas, de investigação científica ou de arquivo no interesse público (artigo 28.º-7 da Lei relativa à proteção de informações pessoais, que prevê uma isenção do artigo 34.º, n.º 1, e do artigo 39.º-4 da Lei relativa à proteção de informações pessoais). Assegurar a notificação individual exigiria que o responsável pelo tratamento em causa identificasse pessoas singulares do conjunto de dados pseudonimizado, o que é expressamente proibido ao abrigo do artigo 28.º-5 da Lei relativa à proteção de informações pessoais. No entanto, continua a aplicar-se o requisito geral de notificação (da Comissão de Proteção de Informações Pessoais) da violação de dados.

([88]) Os requisitos de notificação, incluindo o seu calendário e a possibilidade de notificação «por fases», são especificados em maior detalhe no artigo 40.º do Decreto de Execução da Lei relativa à proteção de informações pessoais. Aplicam-se regras mais rigorosas aos prestadores de serviços de informação e comunicação que são obrigados a notificar o titular dos dados e a Comissão de Proteção de Informações Pessoais no prazo de 24 horas após terem tomado conhecimento de que as informações pessoais foram extraviadas, furtadas ou vazadas (artigo 39.º-4, n.º 1, da Lei relativa à proteção de informações pessoais). Esta notificação tem de incluir pormenores sobre as informações pessoais que foram vazadas, o momento em que tal ocorreu, as medidas que o utilizador pode tomar, as medidas de resposta adotadas pelo prestador de serviços e os dados de contacto do serviço ao qual o utilizador pode dirigir perguntas (artigo 39.º-4, n.º 1, pontos 1 a 5, da Lei relativa à proteção de informações pessoais). Se existir uma razão justificável, por exemplo, não dispor dos dados de contacto do utilizador, podem utilizar-se outros meios de notificação, por exemplo, disponibilizando as informações ao público num sítio Web (artigo 39.º-4, n.º 1, da Lei relativa à proteção de informações pessoais, conjugado com o artigo 48.º-4, n.º 4 e seguintes, do Decreto de Execução da Lei relativa à proteção de informações pessoais). Nesse caso, a Comissão de Proteção de Informações Pessoais deve ser informada dos motivos (artigo 34.º-4, n.º 3, da Lei relativa à proteção de informações pessoais).

([89]) Ver, por exemplo, Decisões n.os 2011Da59834, 2011Da59858 e 2011Da59841 do Supremo Tribunal, de 26 de dezembro de 2012. Está disponível um resumo em inglês no seguinte endereço: http://library.scourt.go.kr/SCLIB_data/decision/9-69%202012.12.26.2011Da59834.htm.

(67) Tal é assegurado de diferentes formas no sistema coreano. Além do direito à informação previsto no artigo 4.º, ponto 1, (em geral) e no artigo 20.º, n.º 1, da Lei relativa à proteção de informações pessoais (para os dados pessoais recolhidos junto de terceiros), bem como o direito de acesso nos termos do artigo 35.º da Lei relativa à proteção de informações pessoais, esta lei inclui um requisito geral de transparência no que respeita à finalidade do tratamento (artigo 3.º, n.º 1, da Lei relativa à proteção de informações pessoais) e requisitos específicos de transparência no caso de o tratamento se basear no consentimento (artigo 15.º, n.º 2, artigo 17.º, n.º 2, e artigo 18.º, n.º 3, da Lei relativa à proteção de informações pessoais) ([90]). Além disso, o artigo 20.º, n.º 2, da Lei relativa à proteção de informações pessoais exige que certos responsáveis pelo tratamento – aqueles cujo tratamento excede determinados limiares ([91]) – notifiquem o titular dos dados, cujos dados pessoais tenham sido recebidos de um terceiro, da fonte de informação, da finalidade do tratamento e do direito do titular de exigir a suspensão do tratamento, a menos que tal notificação se revele impossível devido à inexistência de informações de contacto. São aplicáveis exceções a determinados ficheiros de dados pessoais na posse de autoridades públicas, em especial ficheiros que contenham dados tratados para efeitos de segurança nacional, outros interesses nacionais («graves») especialmente importantes, ou para fins de aplicação do direito penal, ou quando a notificação seja suscetível de causar danos não patrimoniais a outra pessoa ou causar injustificadamente danos ao direito de propriedade e a outros interesses materiais de outra pessoa, mas apenas quando os interesses públicos ou privados em causa forem «manifestamente superiores» aos direitos dos titulares dos dados em causa (artigo 20.º, n.º 4, da Lei relativa à proteção de informações pessoais). Tal requer uma ponderação de interesses.

(68) Além disso, o artigo 3.º, n.º 5, da Lei relativa à proteção de informações pessoais estabelece que os responsáveis pelo tratamento devem tornar pública a sua política de privacidade (e outras questões relacionadas com o tratamento de dados pessoais). Este requisito é especificado em maior pormenor no artigo 30.º da Lei relativa à proteção de informações pessoais, conjugado com o artigo 31.º do Decreto de Execução da Lei relativa à proteção de informações pessoais. Em conformidade com essas disposições, a política de privacidade pública deve incluir, entre outros elementos, 1) os tipos de dados pessoais tratados, 2) a finalidade do tratamento, 3) o período de conservação, 4) se os dados pessoais são fornecidos a terceiros ([92]), 5) qualquer subcontratação ulterior, 6) informações sobre os direitos do titular dos dados e a forma de os exercer e 7) informações de contacto (incluindo o nome do responsável pela privacidade ou do serviço interno responsável por assegurar o cumprimento das regras em matéria de proteção de dados e tratamento de reclamações). A política de proteção da vida privada deve ser disponibilizada ao público, de modo que as pessoas em causa possam reconhecê-la com facilidade (artigo 30.º, n.º 2, da Lei relativa à proteção de informações pessoais) ([93]) e ser permanentemente atualizada (artigo 31.º, n.º 2, do Decreto de Execução da Lei relativa à proteção de informações pessoais).

(69) As instituições públicas estão sujeitas a uma obrigação adicional de registo, nomeadamente, das seguintes informações junto da Comissão de Proteção de Informações Pessoais: 1) o nome da instituição pública, 2) os motivos e finalidades para o tratamento dos ficheiros de dados pessoais, 3) os elementos dos dados pessoais registados, 4) o método de tratamento, 5) o período de conservação, 6) o número de titulares de dados cujos dados pessoais são conservados, 7) o serviço que trata os pedidos dos titulares dos dados e 8) os destinatários dos dados pessoais quando os dados são fornecidos de forma rotineira ou reiterada (artigo 32.º, n.º 1, da Lei relativa à proteção de informações pessoais) ([94]). Os ficheiros de dados pessoais registados são tornados públicos pela Comissão de Proteção de Informações Pessoais e devem também ser mencionados pelas instituições públicas na sua política de proteção da vida privada (artigo 30.º, n.º 1, e artigo 32.º, n.º 4, da Lei relativa à proteção de informações pessoais).

(70) A fim de aumentar a transparência para os titulares de dados na União cujos dados pessoais são transferidos para a Coreia com base na presente decisão, o ponto 3, alíneas i) e ii), da Notificação n.º 2021-5 (anexo I) impõe requisitos adicionais de transparência. Em primeiro lugar, ao receber dados pessoais da União com base na presente decisão,

([90]) Em especial, quando as informações pessoais são tratadas com o consentimento de uma pessoa singular, o responsável pelo tratamento deve informá-la da finalidade do tratamento, dos pormenores sobre as informações a tratar, do destinatário das informações, do período durante o qual as informações pessoais são conservadas e utilizadas, bem como do facto de que a pessoa tem o direito de recusar o consentimento (e qualquer desvantagem que daí possa resultar).

([91]) Nos termos do artigo 15.º-2, n.º 1, do Decreto de Execução da Lei relativa à proteção de informações pessoais, trata-se de responsáveis pelo tratamento de informações sensíveis respeitantes a, pelo menos, 50 000 titulares de dados, ou de informações pessoais «normais» respeitantes a, pelo menos, um milhão de titulares de dados. O artigo 15.º-2, n.º 2, do Decreto de Execução da Lei relativa à proteção de informações pessoais estabelece os métodos e os prazos de notificação, o artigo 15.º-2, n.º 3, a obrigação de conservar determinados registos dessa notificação. Além disso, aplicam-se regras específicas a determinadas categorias de prestadores de serviços de informação e comunicação (aqueles que geraram, pelo menos, dez mil milhões de receitas de vendas no ano anterior, ou os que armazenam/gerem dados pessoais de, pelo menos, um milhão de utilizadores por dia, em média, nos três meses anteriores ao final do ano anterior), que são obrigados a notificar regularmente os utilizadores do histórico de utilização das suas informações pessoais, a menos que tal se revele impossível devido à falta de informações de contacto (artigo 39.º-8 da Lei relativa à proteção de informações pessoais e artigo 48.º-6 do Decreto de Execução da Lei relativa à proteção de informações pessoais).

([92]) De acordo com as informações recebidas do Governo coreano, tal implica uma obrigação de enumerar individualmente os destinatários na política de privacidade pública.

([93]) O artigo 31.º, n.º 3, do Decreto de Execução da Lei relativa à proteção de informações pessoais especifica outras modalidades.

([94]) A obrigação de registo não se aplica a determinados tipos de ficheiros de informações pessoais, por exemplo os que registam questões relacionadas com segurança nacional, segredos diplomáticos, investigações criminais, ação penal, sanções, investigações de crimes relacionados com a fiscalidade, ou processos exclusivamente relacionados com o desempenho de funções internas (artigo 32.º, n.º 2, da Lei relativa à proteção de informações pessoais).

os responsáveis pelo tratamento coreanos devem notificar os titulares dos dados em causa sem demora injustificada (e, em qualquer caso, o mais tardar um mês após a transferência) do nome e dos dados de contacto das entidades que transferem e recebem as informações, dos dados pessoais (ou categorias de dados pessoais) transferidos, da finalidade da recolha pelo responsável pelo tratamento coreano, do período de conservação e dos direitos disponíveis ao abrigo da Lei relativa à proteção de informações pessoais. Em segundo lugar, ao fornecer a terceiros dados pessoais recebidos da União com base na presente decisão, os titulares dos dados devem ser informados, nomeadamente, do destinatário, dos dados pessoais ou das categorias de dados pessoais a fornecer, do país para o qual os dados são fornecidos (se for caso disso), bem como dos direitos disponíveis ao abrigo da Lei relativa à proteção de informações pessoais ([95]). Desta forma, a notificação assegura que as pessoas singulares da UE continuam a ser informadas dos responsáveis pelo tratamento específicos que tratam as informações que lhe dizem respeito e estão em condições de exercer os seus direitos perante as entidades competentes.

(71) O ponto 3, alínea iii), da notificação (anexo I) permite certas exceções limitadas e qualificadas a estas obrigações adicionais de transparência, que são essencialmente equivalentes às previstas no Regulamento (UE) 2016/679. Em especial, a notificação dos titulares de dados na União não é exigida 1) quando e enquanto for necessário limitar a notificação por razões de interesse público (por exemplo, quando as informações são tratadas para efeitos de segurança nacional ou investigações criminais em curso), na medida em que os objetivos de interesse público sejam manifestamente superiores aos direitos do titular dos dados; 2) quando o titular dos dados já tenha conhecimento das informações; 3) quando e enquanto a notificação for suscetível de causar danos não patrimoniais da pessoa singular ou de outra pessoa ou de constituir a violação injustificada de interesses patrimoniais de outra pessoa, quando esses direitos ou interesses forem manifestamente superiores aos direitos do titular dos dados; ou 4) quando não existirem dados de contacto para as pessoas singulares em causa ou se for necessário envidar um esforço desproporcionado para as notificar. Para determinar se é ou não possível contactar o titular dos dados ou se tal implica esforços excessivos, é necessário ter em conta a possibilidade de cooperação com o exportador de dados na União.

(72) Por conseguinte, no que respeita a transparência, as regras enunciadas nos considerandos (67) a (71) asseguram um nível de proteção essencialmente equivalente ao previsto no Regulamento (UE) 2016/679.

2.3.8 *Direitos individuais*

(73) Os titulares dos dados devem ter determinados direitos que podem ser exercidos contra o responsável pelo tratamento ou subcontratante, nomeadamente o direito de acesso aos dados, o direito de retificação, o direito de oposição ao tratamento e o direito de apagamento dos dados. Ao mesmo tempo, tais direitos podem estar sujeitos a limitações, na medida em que estas sejam necessárias e proporcionadas para assegurar objetivos importantes do interesse público geral.

(74) Nos termos do artigo 3.º, n.º 5, da Lei relativa à proteção de informações pessoais, o responsável pelo tratamento garante aos titulares dos dados os direitos enumerados no artigo 4.º da Lei relativa à proteção de informações pessoais e especificados nos artigos 35.º a 37.º, 39.º e 39.º-2 da Lei relativa à proteção de informações pessoais.

(75) Em primeiro lugar, as pessoas singulares têm direito à informação e direito de acesso. Quando o responsável pelo tratamento tiver recolhido dados pessoais de um terceiro – como será sempre o caso quando os dados são transferidos da União – os titulares dos dados têm geralmente o direito de receber informações sobre 1) a «fonte» dos dados pessoais recolhidos (ou seja, o transmitente), 2) a finalidade do tratamento e 3) o facto de o titular dos dados ter o direito de exigir a suspensão do tratamento (artigo 20.º, n.º 1, da Lei relativa à proteção de informações pessoais). Aplicam-se exceções limitadas, nomeadamente quando a notificação for suscetível de causar danos não patrimoniais a outra pessoa ou causar injustificadamente danos ao direito de propriedade e a outros interesses materiais de outra pessoa, mas apenas quando os interesse de terceiros sejam explicitamente superiores aos direitos do titular dos dados (artigo 20.º, n.º 4, ponto 2, da Lei relativa à proteção de informações pessoais).

(76) Além disso, o artigo 35.º, n.ºs 1 e 3, da Lei relativa à proteção de informações pessoais, conjugado com o artigo 41.º, n.º 4, do Decreto de Execução da Lei relativa à proteção de informações pessoais, confere aos titulares dos dados o direito de acesso às informações pessoais que lhe digam respeito ([96]). O direito de acesso abrange a confirmação do tratamento, informações sobre o tipo de dados tratados, a finalidade do tratamento, o período de conservação, bem como qualquer divulgação a terceiros e o fornecimento de uma cópia das informações pessoais tratadas (artigo 4.º, ponto 3, da Lei relativa à proteção de informações pessoais, conjugado com o artigo 41.º, n.º 1, do Decreto de Execução da Lei relativa à proteção de informações

([95]) Notificação n.º 2021-5, ponto 3, alínea i), (anexo I).

([96]) Em conformidade com o artigo 35.º, n.º 3, da Lei relativa à proteção de informações pessoais, conjugado com o artigo 42.º, n.º 2, do Decreto de Execução da Lei relativa à proteção de informações pessoais, o responsável pelo tratamento pode adiar o acesso por «justa causa» (ou seja, por motivos justificados, por exemplo, se for necessário mais tempo para avaliar se o acesso pode ser concedido), mas deve notificar o titular dos dados dessa justificação no prazo de dez dias e fornecer informações sobre as vias ao seu dispor para recorrer desta decisão. Assim que o motivo do adiamento deixe de existir, o acesso deve ser concedido.

pessoais) ([97]). O acesso só pode ser limitado (acesso parcial) ([98]) ou recusado quando a lei preveja essa possibilidade ([99]), quando o mesmo for suscetível de causar danos não patrimoniais a um terceiro ou constituir a violação injustificada do direito de propriedade e de outros interesses materiais de outra pessoa (artigo 35.º, n.º 4, da Lei relativa à proteção de informações pessoais) ([100]). Neste caso, é necessário proceder a uma ponderação entre os direitos e liberdades constitucionalmente protegidos da pessoa singular, por um lado, e de outras pessoas, por outro. Nos casos em que o acesso é limitado ou recusado, o responsável pelo tratamento deve notificar o titular dos dados dos motivos e das vias ao seu dispor para recorrer da decisão (artigo 41.º, n.º 5, e artigo 42.º, n.º 2, do Decreto de Execução da Lei relativa à proteção de informações pessoais).

(77) Em segundo lugar, os titulares dos dados têm direito à retificação ou apagamento ([101]) dos dados pessoais que lhe digam respeito, salvo disposição específica em contrário prevista noutra legislação (artigo 36.º, n.ºs 1 e 2, da Lei relativa à proteção de informações pessoais) ([102]). Após a receção de um pedido, o responsável pelo tratamento deve investigar sem demora o assunto, tomar as medidas necessárias ([103]) e notificar o titular dos dados desse facto no prazo de dez dias. Se o pedido não puder ser deferido, esta obrigação de notificação abrange os motivos da recusa e as vias de recurso (ver artigo 36.º, n.º 4, conjugado com o artigo 43.º, n.º 3, do Decreto de Execução da Lei relativa à proteção de informações pessoais) ([104]).

(78) Por último, os titulares dos dados têm direito à suspensão imediata do tratamento dos dados pessoais que lhes digam respeito ([105]), a não ser que seja aplicável uma das exceções enumeradas (artigo 37.º, n.ºs 1 e 2, da Lei relativa à proteção de informações pessoais) ([106]). O responsável pelo tratamento pode recusar o pedido 1) quando tal for especificamente autorizado por lei ou se for necessário («inevitável») para o cumprimento de obrigações legais, 2) quando a suspensão for suscetível de causar danos não patrimoniais a um terceiro ou constituir a violação injustificada do direito de propriedade e de outros interesses materiais, 3) quando for impossível para uma instituição pública o exercício das respetivas funções previstas na lei sem proceder ao tratamento das informações, ou 4) quando o titular dos dados não denuncie expressamente o contrato subjacente com o responsável pelo tratamento, mesmo que seja impossível executar o contrato sem esse tratamento. Neste caso, o responsável pelo tratamento deve, sem demora, notificar o titular dos dados dos motivos da recusa e das vias de recurso (artigo 37.º, n.º 2, da Lei relativa à proteção de informações pessoais, conjugado com o artigo 44.º, n.º 2, do Decreto de Execução da Lei relativa à proteção de informações pessoais). Nos termos do artigo 37.º, n.º 4, da Lei relativa à proteção de informações pessoais, no cumprimento do pedido de suspensão, o responsável pelo tratamento deve tomar imediatamente as medidas necessárias, incluindo a destruição das informações pessoais pertinentes ([107]).

(79) O direito de suspensão aplica-se igualmente quando os dados pessoais são utilizados para fins de comercialização direta, ou seja, para promover bens ou serviços ou para solicitar a aquisição de bens ou serviços. Além disso, esse tratamento posterior exige geralmente o consentimento (adicional) específico do titular dos dados (ver artigo 15.º, n.º 1, ponto 1, artigo 17.º, n.º 2, ponto 1, da Lei relativa à proteção de informações pessoais) ([108]). Ao solicitar este consentimento, o responsável pelo

([97]) O acesso a informações pessoais tratadas por uma instituição pública pode ser obtido diretamente junto da instituição ou indiretamente mediante a apresentação de um pedido à Comissão de Proteção de Informações Pessoais, que o transmite sem demora (artigo 35.º, n.º 2, da Lei relativa à proteção de informações pessoais e artigo 41.º, n.º 3, do Decreto de Execução da Lei relativa à proteção de informações pessoais).

([98]) Nos termos do artigo 42.º, n.º 1, do Decreto de Execução da Lei relativa à proteção de informações pessoais, o responsável pelo tratamento tem a obrigação de conceder acesso parcial quando, pelo menos, uma parte da informação não estiver abrangida pelos motivos da recusa.

([99]) Essa lei deve, por sua vez, respeitar o direito fundamental à privacidade e à proteção de dados, bem como os princípios da necessidade e da proporcionalidade estabelecidos na Constituição coreana.

([100]) Além disso, as instituições públicas podem recusar o acesso se este causar graves dificuldades na execução de determinadas funções, incluindo auditorias em curso ou a aplicação, cobrança ou reembolso de impostos (artigo 35.º, n.º 4, da Lei relativa à proteção de informações pessoais).

([101]) Neste caso, o responsável pelo tratamento deve tomar medidas que impeçam a recuperação das informações pessoais, ver artigo 36.º, n.º 3, da Lei relativa à proteção de informações pessoais.

([102]) Tal legislação deve cumprir os requisitos da Constituição, segundo os quais um direito fundamental só pode ser limitado quando tal for necessário para efeitos de segurança nacional ou para a manutenção da ordem pública, e não pode afetar o conteúdo essencial da liberdade ou do direito (artigo 37.º, n.º 2, da Constituição).

([103]) O artigo 43.º, n.º 2, do Decreto de Execução da Lei relativa à proteção de informações pessoais prevê um procedimento especial no caso de o responsável pelo tratamento tratar ficheiros de informações pessoais fornecidos por outro responsável pelo tratamento.

([104]) A não adoção das medidas necessárias para corrigir ou apagar as informações pessoais e a utilização ou prestação contínuas dessas informações a terceiros podem dar origem a sanções penais (artigo 73.º, n.º 2, da Lei relativa à proteção de informações pessoais).

([105]) Em conformidade com o artigo 44.º, n.º 2, do Decreto de Execução da Lei relativa à proteção de informações pessoais, o responsável pelo tratamento deve informar o titular dos dados de que suspendeu devidamente o tratamento no prazo de dez dias a contar da receção do pedido.

([106]) No que respeita às instituições públicas, o direito à suspensão do tratamento pode ser exercido no que respeita às informações contidas nos ficheiros de informação pessoal registados (artigo 37.º conjugado com o artigo 32.º da Lei relativa à proteção de informações pessoais). Esse registo não é necessário num número limitado de situações, por exemplo, quando os ficheiros de informações pessoais dizem respeito a segurança nacional, investigações criminais, relações diplomáticas, etc. (artigo 32.º, n.º 2, da Lei relativa à proteção de informações pessoais).

([107]) A não suspensão do tratamento pode dar origem a sanções penais (artigo 73.º, n.º 3, da Lei relativa à proteção de informações pessoais).

([108]) O Comité de Mediação de Litígios (ver considerando 133) tratou vários processos em que as pessoas singulares reclamaram da utilização dos dados que lhe diziam respeito para fins de comercialização direta sem consentimento, que culminaram, por exemplo, no pagamento de uma indemnização e no apagamento de dados pessoais por parte do responsável pelo tratamento pertinente [ver, por exemplo, Comité de Mediação de Litígios 20R10-024(2020.11.18), 20R08-015(2020.8.28), 20R07-031 (2020.9.1)].

tratamento deve informar o titular dos dados, em especial, no que respeita à utilização prevista dos dados para fins de comercialização direta – ou seja, o facto de poder ser contactado no âmbito da promoção de bens ou serviços ou de um pedido da sua aquisição – «de forma explicitamente reconhecível» (artigo 22.º, n.ºs 2 e 4, da Lei relativa à proteção de informações pessoais, conjugado com o artigo 17.º, n.º 2, ponto 1, do Decreto de Execução da Lei relativa à proteção de informações pessoais).

(80) A fim de facilitar o exercício dos direitos individuais, o responsável pelo tratamento deve estabelecer procedimentos específicos e anunciá-los publicamente (artigo 38.º, n.º 4, da Lei relativa à proteção de informações pessoais) ([109]). Tal inclui procedimentos para a formulação de objeções perante a recusa de um pedido (artigo 38.º, n.º 5, da Lei relativa à proteção de informações pessoais). O responsável pelo tratamento deve assegurar que o procedimento para o exercício de direitos é de fácil utilização pelo titular dos dados e não mais difícil do que o procedimento para a recolha dos dados pessoais. Inclui-se aqui também a obrigação de prestar informações sobre o procedimento no respetivo sítio Web (artigo 41.º, n.º 2, artigo 43.º, n.º 1, e artigo 44.º, n.º 1, do Decreto de Execução da Lei relativa à proteção de informações pessoais) ([110]). As pessoas singulares podem autorizar um representante para apresentar esse pedido (artigo 38.º, n.º 1, da Lei relativa à proteção de informações pessoais, conjugado com o artigo 45.º do Decreto de Execução da Lei relativa à proteção de informações pessoais). Embora o responsável pelo tratamento tenha o direito de cobrar uma taxa (e, no caso de um pedido de envio de cópias de dados pessoais, portes de correio), o montante tem de ser determinado dentro dos limites das despesas efetivamente necessárias para o tratamento do pedido. Não podem ser cobradas taxas (nem portes de correio) quando o responsável pelo tratamento tiver sido a causa do pedido (artigo 38.º, n.º 3, da Lei relativa à proteção de informações pessoais, conjugado com o artigo 47.º do Decreto de Execução da Lei relativa à proteção de informações pessoais).

(81) A Lei relativa à proteção de informações pessoais e o respetivo decreto de execução 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, no que se refere aos dados pessoais recolhidos na União, qualquer decisão baseada num tratamento automatizado será, normalmente, tomada pelo responsável pelo tratamento na União (que tem uma relação direta com o titular dos dados em causa), estando, por conseguinte, sujeita ao Regulamento (UE) 2016/679 ([111]). Tal inclui cenários de transferência em que o tratamento seja realizado por um operador comercial estrangeiro (por exemplo, coreano), que atua como agente (subcontratante) do responsável pelo tratamento na União (ou como subcontratante ulterior do subcontratante da União, o qual por sua vez recebeu os dados de um responsável pelo tratamento da União que os recolheu) que, nesta base, toma então a decisão. Deste modo, não é provável que a inexistência na Lei relativa à proteção de informações pessoais de regras específicas sobre a tomada de decisões automatizadas afete o nível de proteção dos dados pessoais transferidos ao abrigo da presente decisão.

(82) A título de exceção, as disposições relativas à transparência mediante pedido (artigo 20.º) e aos direitos individuais (artigos 35.º a 37.º), bem como à obrigação de notificação individual para os prestadores de serviços de informação e comunicação (artigo 39.º-8.º da Lei relativa à proteção de informações pessoais), não se aplicam às informações pseudonimizadas quando estas são tratadas para efeitos de estatísticas, de investigação científica ou de arquivo no interesse público (artigo 28.º-7 da Lei relativa à proteção de informações pessoais) ([112]). Em conformidade com a abordagem do artigo 11.º, n.º 2 (conjugado com o considerando 57) do Regulamento (UE) 2016/679, tal justifica-se pelo facto de, para garantir a transparência ou conceder direitos individuais, o responsável pelo tratamento teria de identificar se os dados (e, em caso afirmativo, quais) estão relacionados com a pessoa singular que apresenta o pedido, o que é expressamente proibido ao abrigo da Lei relativa à proteção da privacidade das comunicações (artigo 28.º-5, n.º 1, da Lei relativa à proteção da privacidade das comunicações). Além disso, se essa reidentificação implicar a anulação da pseudonimização para todo o conjunto de dados (pseudonimizados), tal exporia a riscos acrescidos as informações pessoais das restantes pessoas singulares em causa. Enquanto o Regulamento (UE) 2016/679 se refere a situações em que a reidentificação é praticamente impossível, a Lei relativa à proteção de informações pessoais adota uma abordagem mais rigorosa ao proibir expressamente a reidentificação em todas as situações em que são tratadas informações pseudonimizadas.

(83) O sistema coreano, conforme descrito nos considerandos (74) a (82), contém, por conseguinte, regras sobre os direitos dos titulares de dados que proporcionam um nível de proteção essencialmente equivalente ao previsto no Regulamento (UE) 2016/679.

([109]) Ver também o artigo 30.º, n.º 1, ponto 5, da Lei relativa à proteção de informações pessoais no que respeita à política de privacidade, a qual, entre outros aspetos, deve conter informações sobre os direitos que as pessoas singulares têm ao seu dispor e a forma de os exercer.

([110]) Ver também o artigo 39.º-7, n.º 2, da Lei relativa à proteção de informações pessoais no que respeita aos prestadores de serviços de informação e comunicação.

([111]) Em contrapartida, no caso excecional em que o operador de uma empresa coreana 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 de uma empresa coreana 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.

([112]) Ver também a Notificação n.º 2021-5, que confirma que a secção III da Lei relativa à proteção de informações pessoais (incluindo o artigo 28.º-7) só se aplica quando as informações pseudonimizadas são tratadas para efeitos de investigação científica, de estatísticas ou de arquivo no interesse público, ver o anexo I, ponto 4, da presente decisão.

2.3.9 *Transferências ulteriores*

(84) O nível de proteção conferido aos dados pessoais transferidos da União para responsáveis pelo tratamento na República da Coreia não pode ser prejudicado pela transferência subsequente desses dados para destinatários num país terceiro.

(85) Essas «transferências ulteriores» constituem transferências internacionais da República da Coreia na perspetiva do responsável pelo tratamento coreano. A este respeito, a Lei relativa à proteção de informações pessoais distingue entre a subcontratação do tratamento a um subcontratante e o fornecimento de dados pessoais a terceiros ([113]).

(86) Em primeiro lugar, quando o tratamento de dados pessoais é objeto de subcontratação a uma entidade localizada num país terceiro, o responsável pelo tratamento coreano tem de assegurar o cumprimento das disposições da Lei relativa à proteção de informações pessoais em matéria de subcontratação (artigo 26.º da Lei relativa à proteção de informações pessoais). Tal inclui a implementação de um instrumento juridicamente vinculativo que, entre outros aspetos, limite o tratamento pelo subcontratante ao objetivo do trabalho objeto de subcontratação, imponha garantias técnicas e de gestão e limite a subcontratação ulterior (ver artigo 26.º, n.º 1, da Lei relativa à proteção de informações pessoais), e a publicação de informações sobre o trabalho objeto de subcontratação. Além disso, o responsável pelo tratamento tem a obrigação de «ensinar» o subcontratante acerca das medidas de segurança necessárias e supervisionar, nomeadamente através de inspeções, o cumprimento de todas as obrigações do responsável pelo tratamento ao abrigo da Lei relativa à proteção de informações pessoais ([114]), bem como do contrato de subcontratação.

(87) Se o subcontratante causar danos ao tratar dados pessoais em violação da Lei relativa à proteção de informações pessoais, tal será imputado ao responsável pelo tratamento para efeitos de responsabilidade, tal como aconteceria com os trabalhadores do responsável pelo tratamento (artigo 26.º, n.º 6, da Lei relativa à proteção de informações pessoais). Por conseguinte, o responsável pelo tratamento coreano continua a ser responsável pelos dados pessoais que foram objeto de subcontratação e deve assegurar que o subcontratante no estrangeiro trata as informações em conformidade com a Lei relativa à proteção de informações pessoais. Se o subcontratante tratar as informações em violação do disposto na Lei relativa à proteção de informações pessoais, o responsável pelo tratamento coreano pode ser considerado responsável pelo incumprimento da sua obrigação de assegurar o cumprimento da Lei relativa à proteção de informações pessoais, nomeadamente através da sua supervisão do subcontratante. As garantias incluídas no contrato de subcontratação e a responsabilidade do responsável pelo tratamento coreano pelas ações do subcontratante asseguram a continuidade da proteção quando o tratamento de dados pessoais é objeto de subcontratação a uma entidade fora da Coreia.

(88) Em segundo lugar, os responsáveis pelo tratamento coreanos podem fornecer dados pessoais a terceiros localizados fora da Coreia. Embora a Lei relativa à proteção de informações pessoais inclua uma série de fundamentos jurídicos que permitem a prestação a terceiros em geral, se o terceiro estiver localizado fora da Coreia, o responsável pelo tratamento tem, em princípio ([115]), de obter o consentimento do titular dos dados ([116]) depois de ter fornecido informações sobre 1) o tipo de dados pessoais, 2) o destinatário dos dados pessoais, 3) a finalidade da transferência na aceção da finalidade do tratamento prosseguido pelo destinatário, 4) o período de conservação dos dados para o tratamento pelo destinatário, bem como 5) o facto de o titular dos dados poder recusar o consentimento (artigo 17.º, n.ºs 2 e 3, da Lei relativa à proteção de informações pessoais). A Notificação n.º 2021-5, no ponto relativo à transparência (ver considerando (70)), exige que as pessoas singulares sejam informadas sobre o país terceiro ao qual os seus dados serão fornecidos. Tal garante que os titulares de dados na União possam tomar uma decisão plenamente informada sobre consentir ou não um fornecimento ao estrangeiro. Além disso, o responsável pelo tratamento não pode celebrar um contrato com o destinatário terceiro em violação da Lei relativa à proteção de informações pessoais, o que significa que o contrato não pode conter obrigações que contrariem os requisitos impostos pela Lei relativa à proteção de informações pessoais ao responsável pelo tratamento ([117]).

([113]) As regras específicas aplicam-se aos prestadores de serviços de informação e comunicação. Em conformidade com o artigo 39.º-12 da Lei relativa à proteção de informações pessoais, os prestadores de serviços de informação e comunicação devem, em princípio, obter o consentimento do utilizador para qualquer transferência de informações pessoais no estrangeiro. Caso sejam transferidas informações pessoais no âmbito da subcontratação de operações de tratamento, incluindo relativamente a armazenamento, o consentimento não é necessário se as pessoas singulares em causa tiverem sido informadas antecipadamente, de forma direta ou através de aviso público, de forma a permitir um acesso fácil, 1) dos elementos das informações a transferir, 2) do país para o qual as informações serão transferidas (bem como da data e do método da transferência), 3) do nome do destinatário e 4) da finalidade da utilização e da conservação pelo destinatário (artigo 39.º-12, n.º 3, da Lei relativa à proteção de informações pessoais). Além disso, aplicam-se nesse caso os requisitos gerais relativos à subcontratação. Relativamente a cada transferência, é necessário implementar garantias específicas em matéria de segurança, tratamento de reclamações e litígios, bem como outras medidas necessárias para proteger a informação dos utilizadores (artigo 48.º-10 do Decreto de Execução da Lei relativa à proteção de informações pessoais).

([114]) Ver também o artigo 26.º, n.º 7, da Lei relativa à proteção de informações pessoais, nos termos do qual os artigos 15.º a 25.º, 27.º a 31.º, 33.º a 38.º e 50.º se aplicam ao subcontratante, com as devidas adaptações.

([115]) O fornecimento a terceiros de informações pessoais de utilizadores por prestadores de serviços de informação e comunicação exige sempre o consentimento do utilizador (artigo 39.º-12, n.º 2, da Lei relativa à proteção de informações pessoais).

([116]) Tal como explicado em maior pormenor no considerando 51, para que esse consentimento seja válido, é necessário que o mesmo seja dado livremente, informado e específico.

([117]) Ver também o artigo 39.º-12, n.º 1, da Lei relativa à proteção de informações pessoais no que respeita aos prestadores de serviços de informação e comunicação.

(89) Sem o consentimento da pessoa, os dados pessoais podem ser fornecidos a terceiros (no estrangeiro) se a finalidade da divulgação se mantiver num âmbito razoavelmente relacionado com a finalidade inicial da recolha (artigo 17.º, n.º 4, da Lei relativa à proteção de informações pessoais, ver considerando (36)). No entanto, ao decidir divulgar (ou não) dados pessoais para uma finalidade relacionada, o responsável pelo tratamento deve ter em conta se a divulgação causa desvantagens à pessoa singular e se foram tomadas as medidas de segurança necessárias (tal como a cifragem). Uma vez que o país terceiro para o qual os dados pessoais são transferidos não pode oferecer proteções semelhantes às previstas na Lei relativa à proteção de informações pessoais, a Notificação n.º 2021-5, ponto 2, reconhece que tais desvantagens podem surgir e só podem ser evitadas se o responsável pelo tratamento coreano e o destinatário no estrangeiro, com recurso a um instrumento juridicamente vinculativo (como um contrato), garantirem um nível de proteção equivalente à Lei relativa à proteção de informações pessoais, incluindo no que respeita aos direitos dos titulares dos dados.

(90) Aplicam-se regras especiais à divulgação para uma finalidade não prevista, ou seja, ao fornecimento de dados a terceiros para uma nova finalidade (não relacionada), o que só pode acontecer por uma das razões previstas no artigo 18.º, n.º 2, da Lei relativa à proteção de informações pessoais, conforme descrito no considerando (39). No entanto, mesmo nessas condições, o fornecimento a terceiros é excluído se for suscetível de constituir uma violação injustificada dos interesses do titular dos dados ou de um terceiro, o que exige uma ponderação de interesses. Além disso, nos termos do artigo 18.º, n.º 5, da Lei relativa à proteção de informações pessoais, o responsável pelo tratamento deve aplicar garantias adicionais, o que pode incluir pedir ao terceiro a restrição da finalidade e do método de tratamento ou a implementação de medidas de segurança específicas. Mais uma vez, tendo em conta que o país terceiro para o qual os dados pessoais são transferidos não pode oferecer proteções semelhantes às previstas na Lei relativa à proteção de informações pessoais, a Notificação n.º 2021-5, ponto 2, reconhece que uma violação injustificada dos interesses da pessoa singular ou de um terceiro pode surgir e só pode ser evitada se o responsável pelo tratamento coreano e o destinatário no estrangeiro, com recurso a um instrumento juridicamente vinculativo (como um contrato), garantirem um nível de proteção equivalente à Lei relativa à proteção de informações pessoais, incluindo no que respeita aos direitos dos titulares dos dados.

(91) As regras enunciadas nos considerandos (86) a (90), por conseguinte, asseguram a continuidade da proteção quando os dados pessoais são transferidos ulteriormente (para um subcontratante ou para um terceiro) da República da Coreia de uma forma essencialmente equivalente à prevista no Regulamento (UE) 2016/679.

2.3.10 *Responsabilização*

(92) 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.

(93) Nos termos do artigo 3.º, n.os 6 e 8, da Lei relativa à proteção de informações pessoais, o responsável pelo tratamento deve tratar os dados pessoais de forma a minimizar a possibilidade de violar a privacidade da pessoa em causa e esforçar-se por obter a confiança do titular dos dados, observando e exercendo as obrigações e as responsabilidades previstas na Lei relativa à proteção de informações pessoais e noutra legislação conexa. Tal inclui o estabelecimento de um plano de gestão interna (artigo 29.º da Lei relativa à proteção de informações pessoais), bem como a formação e a supervisão adequadas do pessoal (artigo 28.º da Lei relativa à proteção de informações pessoais).

(94) Como forma de assegurar a responsabilização, o artigo 31.º da Lei relativa à proteção de informações pessoais, conjugado com o artigo 32.º do Decreto de Execução da Lei relativa à proteção de informações pessoais, estabelece a obrigação de os responsáveis pelo tratamento designarem um responsável pela privacidade que assuma de forma exaustiva a responsabilidade pelo tratamento de informações pessoais. Em especial, esse responsável pela privacidade fica encarregado de desempenhar as seguintes funções: 1) estabelecimento e aplicação de um plano de proteção de dados pessoais e elaboração da política de privacidade, 2) realização de inquéritos regulares sobre a situação e as práticas de tratamento de dados pessoais, com vista a melhorar eventuais deficiências, 3) tratamento de reclamações e indemnizações corretivas, 4) estabelecimento de um sistema de controlo interno para prevenir a divulgação, o abuso ou a utilização abusiva de dados pessoais, 5) elaboração e execução de um programa de ensino, 6) proteção, controlo e gestão de ficheiros de dados pessoais e 7) destruição dos dados pessoais uma vez atingida a finalidade do tratamento ou o termo do período de conservação dos dados. No exercício destas funções, o responsável pela privacidade pode inspecionar a situação do tratamento de dados pessoais e dos sistemas conexos e solicitar informações a esse respeito (artigo 31.º, n.º 3, da Lei relativa à proteção de informações pessoais). Se o responsável pela privacidade tomar conhecimento de qualquer violação da Lei relativa à proteção de informações pessoais ou de outra legislação pertinente em matéria de proteção de dados, deve tomar imediatamente medidas corretivas e comunicá-las ao órgão de gestão («chefe») do responsável pelo tratamento, se necessário (artigo 31.º, n.º 4, da Lei relativa à proteção de informações pessoais). Nos termos do artigo 31.º, n.º 5, da Lei relativa à proteção de informações pessoais, o responsável pela privacidade não pode sofrer desvantagens injustificadas em consequência do exercício destas funções.

(95) Além disso, os responsáveis pelo tratamento devem ser pró-ativos no esforço para realizar uma avaliação do impacto na privacidade nos casos em que o funcionamento dos ficheiros de dados pessoais implique um risco para a privacidade (artigo 33.º, n.º 8, da Lei relativa à proteção de informações pessoais). Com base no artigo 33.º, n.ºs 1 e 2, da Lei relativa à proteção de informações pessoais, conjugado com os artigos 35.º, 36.º e 38.º do Decreto de Execução da Lei relativa à proteção de informações pessoais, fatores como o tipo e a natureza dos dados tratados (em especial, se constituem informações sensíveis), o seu volume, o período de conservação dos dados e a probabilidade de violações de dados serão pertinentes para avaliar o grau de risco para os direitos dos titulares dos dados. O objetivo da avaliação do impacto na privacidade é assegurar que os fatores de risco em matéria de privacidade, bem como quaisquer contramedidas de segurança ou de outra natureza, são analisados e indicar as questões que necessitam de melhorias (ver artigo 33.º, n.º 1, da Lei relativa à proteção de informações pessoais, em conjugação com o artigo 38.º do Decreto de Execução da Lei relativa à proteção de informações pessoais).

(96) As instituições públicas têm a obrigação de realizar uma avaliação de impacto aquando do tratamento de determinados ficheiros de dados pessoais que apresentam um risco mais elevado de eventuais violações da privacidade (artigo 33.º, n.º 1, da Lei relativa à proteção de informações pessoais). Em conformidade com o artigo 35.º do Decreto de Execução da Lei relativa à proteção de informações pessoais, este é o caso, nomeadamente, dos ficheiros que contêm informações sensíveis sobre pelo menos 50 mil titulares de dados, dos ficheiros que serão confrontados com outros ficheiros e consequentemente irão conter informações sobre pelo menos 500 mil titulares de dados, ou dos ficheiros que contêm informações sobre pelo menos um milhão de titulares de dados. O resultado de uma avaliação de impacto realizada por uma instituição pública deve ser comunicado à Comissão de Proteção de Informações Pessoais (artigo 33.º, n.º 1, da Lei relativa à proteção de informações pessoais), que pode emitir o seu parecer (artigo 33.º, n.º 3, da Lei relativa à proteção de informações pessoais).

(97) Por último, o artigo 13.º da Lei relativa à proteção de informações pessoais prevê que a Comissão de Proteção de Informações Pessoais estabeleça as políticas necessárias para promover e apoiar atividades de autorregulação em matéria de proteção de dados por parte dos responsáveis pelo tratamento, nomeadamente através de ensino em matéria de proteção de dados, da promoção e do apoio às organizações envolvidas na proteção de dados, e prestando assistência aos responsáveis pelo tratamento na definição e aplicação de regras de autorregulação. Além disso, deve introduzir e facilitar o sistema de marcação de privacidade eletrónica. A este respeito, o artigo 32.º-2 da Lei relativa à proteção de informações pessoais, conjugado com os artigos 34.º-2 a 34.º-8 do Decreto de Execução da Lei relativa à proteção de informações pessoais, prevê a possibilidade de certificar que os sistemas de tratamento e proteção de dados pessoais do responsável pelo tratamento cumprem os requisitos da Lei relativa à proteção de informações pessoais. De acordo com estas regras, pode ser concedida uma certificação ([118]) (por um período de 3 anos) se o responsável pelo tratamento cumprir os critérios de certificação determinados pela Comissão de Proteção de Informações Pessoais, incluindo o estabelecimento de garantias de gestão, técnicas e físicas para proteger os dados pessoais ([119]). A Comissão de Proteção de Informações Pessoais deve examinar os sistemas do responsável pelo tratamento pertinente para efeitos de certificação, pelo menos, uma vez por ano, a fim de manter a sua eficácia, o que pode conduzir à revogação da certificação (artigo 32.º, n.º 4, da Lei relativa à proteção de informações pessoais, conjugado com o artigo 34.º-5 do Decreto de Execução da Lei relativa à proteção de informações pessoais, a chamada «gestão de acompanhamento»).

(98) Por conseguinte, o quadro coreano aplica o princípio da responsabilização de forma a assegurar um nível de proteção essencialmente equivalente ao previsto no Regulamento (UE) 2016/679, nomeadamente com a previsão de diferentes mecanismos para assegurar e demonstrar a conformidade com a Lei relativa à proteção de informações pessoais.

2.3.11 *Regras especiais para o tratamento de informações de crédito pessoal*

(99) Conforme descrito no considerando (13), a Lei relativa à utilização e proteção de informações de crédito estabelece regras específicas para o tratamento de informações pessoais de crédito por parte de operadores comerciais. Ao processar informações pessoais de crédito, os operadores comerciais devem, por conseguinte, cumprir os requisitos gerais da Lei relativa à proteção de informações pessoais, a menos que a Lei relativa à utilização e proteção de informações de crédito contenha regras mais específicas. Este será, por exemplo, o caso quando tratam informações relativas a um cartão de crédito ou a uma conta bancária no âmbito de uma transação comercial com uma pessoa singular. Enquanto legislação setorial para o tratamento de informações (tanto pessoais como não pessoais) de crédito, a Lei relativa à utilização e proteção de informações de crédito não só impõe garantias específicas em matéria de proteção de dados (por exemplo, em termos de transparência e segurança), mas também, de um modo mais geral, regula as circunstâncias específicas em que é possível tratar as informações pessoais sobre crédito. Tal reflete-se, em especial, nos requisitos pormenorizados para a utilização, o fornecimento de dados a terceiros e a conservação desses dados.

(100) Tal como a Lei relativa à proteção de informações pessoais, a Lei relativa à utilização e proteção de informações de crédito reflete o princípio da licitude e da proporcionalidade. Em primeiro lugar, como requisito geral, o artigo 15.º, n.º 1, da Lei relativa à utilização e proteção de informações de crédito apenas permite a recolha de informações pessoais de crédito por meios razoáveis e equitativos e na medida do necessário para cumprir uma finalidade específica, em conformidade com o artigo 3.º, n.ºs 1 e 2, da Lei relativa à proteção de informações pessoais. Em segundo lugar, a Lei relativa à utilização e proteção de informações de crédito regula especificamente a licitude do tratamento das informações pessoais de crédito, restringindo a sua recolha, utilização e fornecimento a terceiros e associando, de um modo geral, essas atividades de tratamento ao requisito do consentimento da pessoa em causa.

([118]) Além disso, se o responsável pelo tratamento pretender fazer referência ou promover a certificação nas suas atividades empresariais pode utilizar a marca de proteção da informação pessoal estabelecida pela Comissão de Proteção de Informações Pessoais. Ver o artigo 34.º-7 do Decreto de Execução da Lei relativa à proteção de informações pessoais.

([119]) O «*Personal Information & Information Security Management System*» (sistema de informações pessoais e de gestão da segurança da informação, ISMS-P), que certifica que os responsáveis pelo tratamento estão a operar um sistema de gestão abrangente, tem sido desenvolvido desde novembro de 2018.

(101) As informações pessoais de crédito podem ser recolhidas com base num dos motivos previstos pela Lei relativa à proteção de informações pessoais ou em motivos específicos estabelecidos na Lei relativa à utilização e proteção de informações de crédito. Uma vez que o artigo 45.º do Regulamento (UE) 2016/679 pressupõe uma transferência de dados pessoais por um responsável pelo tratamento ou subcontratante na União, mas não abrange a recolha direta (por exemplo, a partir da pessoa singular ou de um sítio Web) por um responsável pelo tratamento na Coreia, apenas o consentimento e os motivos previstos ao abrigo da Lei relativa à proteção de informações pessoais são relevantes para a presente decisão. Esses motivos incluem, em especial, as situações em que a transferência é necessária para a execução de um contrato com a pessoa singular ou para os interesses legítimos do responsável pelo tratamento coreano (artigo 15.º, n.º 1, pontos 4 e 6, da Lei relativa à proteção de informações pessoais) ([120]).

(102) Uma vez recolhidas, as informações pessoais de crédito podem ser utilizadas 1) para a finalidade inicial para a qual foram (diretamente) fornecidas pela pessoa singular ([121]), 2) para uma finalidade compatível com a finalidade inicial da recolha ([122]), 3) para determinar se se deve estabelecer ou manter uma relação comercial a pedido da pessoa singular ([123]) 4) para efeitos de estatísticas, de investigação e de arquivo no interesse público ([124]), se as informações forem pseudonimizadas ([125]), 5) se for obtido um novo consentimento ou 6) nos termos da lei.

(103) Se um operador comercial pretender divulgar informações pessoais de crédito a um terceiro, deve obter o consentimento da pessoa singular ([126]) depois de a ter informado sobre o destinatário dos dados, a finalidade do tratamento pelo destinatário, os pormenores dos dados a fornecer, o período de conservação pelo destinatário e o direito de recusar o consentimento (artigo 32.º, n.º 1, da Lei relativa à utilização e proteção de informações de crédito e artigo 28.º, n.º 2, do Decreto de Execução da Lei relativa à utilização e proteção de informações de crédito) ([127]). Este requisito de consentimento não se aplica em situações específicas, nomeadamente quando são divulgadas informações pessoais de crédito ([128]): 1) a um subcontratante para efeitos de subcontratação ([129]); 2) a terceiros em caso de transmissão, cisão ou fusão de empresas; 3) para efeitos de estatísticas, de investigação e de arquivo no interesse público, se as informações forem pseudonimizadas; 4) para uma finalidade compatível com a finalidade inicial da recolha; 5) a terceiros que utilizem as informações para cobrar uma dívida da pessoa singular ([130]); 6) dar cumprimento a uma decisão judicial; 7) a um procurador/agente da polícia judiciária numa situação de emergência em que a vida da pessoa singular esteja em perigo ou se preveja ofensas à sua integridade física e não haja tempo

([120]) A Lei relativa à utilização e proteção de informações de crédito também contém outras bases jurídicas para a recolha, ou seja, quando a lei o exija, quando a informação seja tornada pública por uma instituição pública nos termos da legislação em matéria de liberdade de informação, ou quando a informação esteja disponível numa rede social. Para que o operador comercial possa invocar este último motivo, tem de conseguir demonstrar que a recolha continua a fazer parte do âmbito do consentimento do titular dos dados, com base numa interpretação razoável («objetiva») e tendo em conta a natureza dos dados, a intenção e a finalidade da sua disponibilização na rede social, se a finalidade da recolha é «altamente pertinente» para esse fim, etc. (artigo 13.º do Decreto de Execução da Lei relativa à utilização e proteção de informações de crédito). No entanto, conforme explicado no considerando (101), estes motivos não serão, em princípio, pertinentes num cenário de transferência.

([121]) Por exemplo, quando as informações de crédito forem geradas/fornecidas no contexto de uma transação comercial com a pessoa singular. No entanto, este motivo não pode ser invocado para utilizar as informações pessoais de crédito para fins de comercialização direta (ver artigo 33.º, n.º 1, ponto 3, da Lei relativa à utilização e proteção de informações de crédito).

([122]) Para determinar se a finalidade da utilização é compatível com a finalidade inicial da recolha, é necessário ter em conta os seguintes fatores: 1) a relação («pertinência») entre os dois objetivos; 2) o modo como as informações foram recolhidas; 3) o impacto da utilização no indivíduo; e 4) se foram aplicadas medidas de segurança adequadas, tais como a pseudonimização (artigo 32.º, n.º 6, ponto 9-4, da Lei relativa à utilização e proteção de informações de crédito).

([123]) Por exemplo, um responsável pelo tratamento pode ter de ter em conta as informações pessoais de crédito que recebeu de uma pessoa para decidir se deve ou não alargar o prazo de um empréstimo a essa pessoa.

([124]) Artigo 33.º da Lei relativa à utilização e proteção de informações de crédito, conjugado com o artigo 32.º, n.º 6, pontos 9-2, 9-4 e 10 da Lei relativa à utilização e proteção de informações de crédito.

([125]) O conceito de «pseudonimização» está definido no artigo 2.º, n.º 15, da Lei relativa à utilização e proteção de informações de crédito como o tratamento de informações pessoais de crédito, de forma que as pessoas singulares só possam ser identificadas a partir de informações em combinação com informações adicionais. Embora a Lei relativa à utilização e proteção de informações de crédito contenha garantias específicas para o tratamento de informações pseudonimizadas para efeitos de estatísticas, de investigação e de arquivo no interesse público (artigo 40.º-2 da Lei relativa à utilização e proteção de informações de crédito), estas regras não se aplicam às organizações comerciais. Em vez disso, estas últimas continuam a estar sujeitas aos requisitos específicos da secção III da Lei relativa à proteção de informações pessoais, conforme descrito nos considerandos (42) a (48). Além disso, o artigo 40.º-3 da Lei relativa à utilização e proteção de informações de crédito isenta o tratamento de informações pseudonimizadas de crédito – sempre que tal seja efetuado para efeitos de estatísticas, de investigação científica ou de arquivo no interesse público – dos requisitos em matéria de transparência e direitos individuais, à semelhança da exceção prevista no artigo 28.º-7 da Lei relativa à proteção de informações pessoais e sob reserva das garantias previstas na secção III da Lei relativa à proteção de informações pessoais, conforme descrito em maior pormenor nos considerandos (42) a (48).

([126]) Tal não se aplica quando as informações são fornecidas a terceiros a fim de manter as informações pessoais de crédito exatas e atualizadas, desde que a disposição se mantenha dentro do objetivo inicial do tratamento (artigo 32.º, n.º 1, da Lei relativa à utilização e proteção de informações de crédito). Tal pode ocorrer, por exemplo, quando são fornecidas informações atualizadas a uma agência de notação de risco de crédito para garantir a exatidão dos seus registos.

([127]) Caso não seja exequível fornecer as informações acima referidas, pode ser suficiente reencaminhar a pessoa singular para o destinatário terceiro para obter as informações solicitadas.

([128]) Uma vez que a Lei relativa à utilização e proteção de informações de crédito não regulamenta especificamente a divulgação de informações pessoais de crédito no estrangeiro, esta divulgação tem de respeitar as garantias em matéria de transferências ulteriores impostas pelo ponto 2 da Notificação n.º 2021-5.

([129]) A subcontratação do tratamento de informações pessoais relativas ao crédito só pode ocorrer tendo por base um contrato escrito e em conformidade com os requisitos do artigo 26.º, n.ºs 1 a 3 e 5, da Lei relativa à proteção de informações pessoais, conforme descrito no considerando (20) (artigo 17.º da Lei relativa à utilização e proteção de informações de crédito e artigo 14.º do Decreto de Execução da Lei relativa à utilização e proteção de informações de crédito). O subcontratante não pode utilizar as informações fora do âmbito das tarefas objeto da subcontratação e a empresa que subcontrata deve estabelecer requisitos de segurança específicos (por exemplo, cifragem) e ensinar ao subcontratante a forma de evitar que as informações de crédito sejam extraviadas, furtadas, divulgadas, alteradas ou comprometidas.

([130]) Ver também o artigo 28.º, n.º 10, pontos 1, 2 e 6, do Decreto de Execução da Lei relativa à utilização e proteção de informações de crédito.

disponível para emitir um mandado judicial ([131]); 8) às autoridades tributárias competentes para cumprimento da legislação fiscal; ou 9) em conformidade com outra legislação. Em caso de divulgação baseada num destes motivos, o titular dos dados deve ser previamente notificado desse facto (artigo 32.º, n.º 7, da Lei relativa à utilização e proteção de informações de crédito).

(104) A Lei relativa à utilização e proteção de informações de crédito também regula especificamente a duração do tratamento das informações pessoais de crédito com base num desses motivos para a utilização ou o fornecimento a terceiros após o termo da relação comercial com a pessoa singular ([132]). Só podem ser conservadas as informações necessárias para estabelecer ou manter essa relação, sob reserva de garantias adicionais (devem ser conservadas separadamente das informações de crédito relativas a pessoas singulares com as quais esteja em curso uma relação comercial, protegidas por medidas de segurança específicas e acessíveis apenas a pessoas autorizadas) ([133]). Todos os outros dados devem ser suprimidos (artigo 17.º-2, n.º 1, ponto 2, do Decreto de Execução da Lei relativa à utilização e proteção de informações de crédito). Para determinar quais os dados necessários para a relação comercial, importa ter em conta diferentes fatores, nomeadamente se teria sido possível estabelecer a relação sem os dados e os mesmos estão diretamente relacionados com os bens ou serviços fornecidos à pessoa singular (artigo 17.º-2, n.º 2, do Decreto de Execução da Lei relativa à utilização e proteção de informações de crédito).

(105) Mesmo nos casos em que as informações pessoais de crédito possam, em princípio, ser conservadas após o fim da relação comercial, as mesmas devem ser eliminadas no prazo de três meses após a consecução da finalidade do tratamento ([134]) ou, em qualquer caso, decorridos cinco anos (artigo 20.º-2 da Lei relativa à utilização e proteção de informações de crédito). Num número limitado de circunstâncias, as informações pessoais de crédito podem ser conservadas por um período superior a cinco anos, em especial se tal for necessário para cumprir uma obrigação legal, se tal for necessário para os interesses vitais da vida, do corpo ou do património de um indivíduo, para o arquivo de informações pseudonimizadas (que foram utilizadas para efeitos de estatísticas, de investigação científica e de arquivo no interesse público) ou para efeitos de seguros (em especial para pagamentos de seguros ou para prevenir a fraude em matéria de seguros) ([135]). Nestes casos excecionais, aplicam-se garantias específicas (tais como notificar a pessoa singular da utilização posterior, separar as informações conservadas das informações relativas às pessoas singulares com as quais ainda existe uma relação comercial, limitar os direitos de acesso, ver o artigo 17.º-2, n.ºs 1 e 2, do Decreto de Execução da Lei relativa à utilização e proteção de informações de crédito).

(106) A Lei relativa à utilização e proteção de informações de crédito especifica ainda os princípios da exatidão e da qualidade dos dados, exigindo que as informações pessoais de crédito sejam registadas, modificadas e geridas, a fim de as manter exatas e atualizadas (artigo 18.º, n.º 1, da Lei relativa à utilização e proteção de informações de crédito e artigo 15.º, n.º 3, do Decreto de Execução da Lei relativa à utilização e proteção de informações de crédito) ([136]). Ao fornecerem informações de crédito a outras entidades (como as agências de notação do risco de crédito), os operadores comerciais são também especificamente obrigados a verificar a exatidão das informações, a fim de garantir que apenas as informações exatas são registadas e geridas pelo destinatário (artigo 15.º, n.º 1, do Decreto de Execução da Lei relativa à utilização e proteção de informações de crédito, conjugado com o artigo 18.º, n.º 1, da Lei relativa à utilização e proteção de informações de crédito). De um modo mais geral, a Lei relativa à utilização e proteção de informações de crédito exige a conservação de registos sobre a recolha, a utilização, a divulgação a terceiros e a destruição de informações pessoais de crédito (artigo 20.º, n.º 2, da Lei relativa à utilização e proteção de informações de crédito) ([137]).

(107) Além disso, o tratamento de informações pessoais de crédito está sujeito a requisitos específicos em matéria de segurança dos dados. Em especial, a Lei relativa à utilização e proteção de informações de crédito exige a aplicação de medidas tecnológicas, físicas e organizativas para impedir o acesso ilícito a sistemas informáticos, bem como a alteração, destruição ou qualquer outro risco para os dados tratados (por exemplo, através de controlos de acesso, ver artigo 19.º da Lei relativa à utilização e proteção de informações de crédito e artigo 16.º do Decreto de Execução da Lei relativa à utilização e proteção de informações de crédito). Além disso, aquando da troca de informações pessoais de créditos com terceiros, é necessário celebrar um acordo que estabeleça medidas de segurança específicas (artigo 19.º, n.º 2, da Lei relativa à utilização e proteção de informações de crédito). Em caso de violação das informações pessoais de crédito, é necessário tomar medidas para minimizar eventuais danos e as pessoas singulares em causa devem ser imediatamente notificadas (artigo 39.º-4, n.ºs 1 e 2, da Lei relativa à utilização e proteção de informações de crédito). Além disso, a Comissão de Proteção de Informações Pessoais deve ser informada da notificação feita às pessoas singulares e das medidas aplicadas (artigo 39.º-4, n.º 4, da Lei relativa à utilização e proteção de informações de crédito).

([131]) Neste caso, é necessário solicitar imediatamente um mandado. Se o mandado não for emitido no prazo de 36 horas, os dados recebidos devem ser apagados sem demora (artigo 32.º, n.º 6, ponto 6, da Lei relativa à utilização e proteção de informações de crédito).

([132]) Por exemplo, porque as obrigações contratuais foram cumpridas, uma das partes exerceu o seu direito de denúncia, ver o artigo 17.º-2, n.º 5, do Decreto de Execução da Lei relativa à utilização e proteção de informações de crédito.

([133]) Artigo 20.º-2, n.º 1, da Lei relativa à utilização e proteção de informações de crédito e artigo 17.º-2, n.º 1, ponto 1, do Decreto de Execução da Lei relativa à utilização e proteção de informações de crédito.

([134]) Este período tem em conta que, muitas vezes, a eliminação não será possível de imediato, mas exige normalmente determinadas medidas (por exemplo, separar os dados de outros dados e efetuar a eliminação sem afetar a estabilidade dos sistemas de informação), cuja aplicação demora algum tempo.

([135]) Artigo 20.º-2, n.º 2, da Lei relativa à utilização e proteção de informações de crédito.

([136]) O artigo 18.º, n.º 2, da Lei relativa à utilização e proteção de informações de crédito e o artigo 15.º, n.º 4, do Decreto de Execução da Lei relativa à utilização e proteção de informações de crédito estabelecem regras mais específicas no que respeita a este requisito de conservação de registos, por exemplo, para registos relativos a informações suscetíveis de prejudicar uma pessoa singular, tais como informações sobre incumprimentos e falência.

([137]) No que respeita a outros mecanismos de responsabilização, a Lei relativa à utilização e proteção de informações de crédito exige que determinadas organizações (por exemplo, cooperativas e empresas públicas, ver artigo 21.º, n.º 2, do Decreto de Execução da Lei relativa à utilização e proteção de informações de crédito) nomeiem um «administrador/tutor de informações de crédito» encarregado de controlar o cumprimento da Lei relativa à utilização e proteção de informações de crédito e desempenhar as funções de responsável pela privacidade ao abrigo da Lei relativa à proteção de informações pessoais (artigo 20.º, n.ºs 3 e 4, da Lei relativa à utilização e proteção de informações de crédito).

(108) A Lei relativa à utilização e proteção de informações de crédito também impõe obrigações específicas de transparência na obtenção do consentimento para a utilização ou o fornecimento de informações pessoais de crédito (artigo 32.º, n.º 4, e artigo 34.º-2 da Lei relativa à utilização e proteção de informações de crédito e artigo 30.º-3 do Decreto de Execução da Lei relativa à utilização e proteção de informações de crédito) e, de um modo mais geral, antes de fornecer informações a terceiros (artigo 32.º, n.º 7, da Lei relativa à utilização e proteção de informações de crédito) ([138]). Além disso, as pessoas singulares têm o direito de obter, mediante pedido, informações sobre a utilização e o fornecimento das informações que lhes digam respeito em matéria de crédito a terceiros nos três anos anteriores ao pedido (incluindo o objetivo e as datas dessa utilização/fornecimento) ([139]).

(109) Nos termos da Lei relativa à utilização e proteção de informações de crédito, as pessoas singulares têm igualmente o direito de aceder às informações pessoais de crédito que lhes digam respeito (artigo 38.º, n.º 1, da Lei relativa à utilização e proteção de informações de crédito) e de obter a retificação de dados inexatos (artigo 38.º, n.ºs 2 e 3, da Lei relativa à utilização e proteção de informações de crédito) ([140]). Além disso, além do direito geral ao apagamento ao abrigo da Lei relativa à proteção de informações pessoais (ver considerando (77)), a Lei relativa à utilização e proteção de informações de crédito prevê um direito específico ao apagamento das informações pessoais de crédito que tenham sido conservadas para lá dos períodos de conservação mencionados no considerando (104), ou seja, cinco anos (para as informações pessoais de crédito necessárias para estabelecer ou manter uma relação comercial) ou três meses (para outros tipos de informações pessoais de crédito) ([141]). Um pedido de apagamento pode, a título excecional, ser recusado nos casos em que seja necessária uma conservação posterior nas circunstâncias descritas no considerando (105). Se uma pessoa solicitar o apagamento, mas for aplicável uma das exceções, é necessário aplicar garantias específicas às informações de crédito em causa (artigo 38.º-3, n.º 3, da Lei relativa à utilização e proteção de informações de crédito e artigo 33.º-3 do Decreto de Execução da Lei relativa à utilização e proteção de informações de crédito). Por exemplo, as informações devem ser conservadas separadamente de outras informações, só podem ser consultadas por uma pessoa autorizada e devem estar sujeitas a medidas de segurança específicas.

(110) Para além dos direitos mencionados no considerando (109), a Lei relativa à utilização e proteção de informações de crédito garante às pessoas singulares o direito de solicitar a um responsável pelo tratamento que deixe de as contactar para efeitos de comercialização direta (artigo 37.º, n.º 2, da lei) e o direito de portabilidade dos dados. No que diz respeito a este último, a Lei relativa à utilização e proteção de informações de crédito permite que as pessoas singulares solicitem a transmissão das informações pessoais de crédito que lhes digam respeito a elas próprias ou a determinados terceiros (tais como instituições financeiras e sociedades de notação de risco). As informações pessoais de crédito devem ser tratadas e transmitidas ao terceiro num formato que possa ser processado por um dispositivo de tratamento de informações (por exemplo, um computador).

(111) Na medida em que a Lei relativa à utilização e proteção de informações de crédito contém regras específicas em comparação com a Lei relativa à proteção de informações pessoais, a Comissão considera, por conseguinte, que também estas regras asseguram um nível de proteção essencialmente equivalente ao proporcionado pelo Regulamento (UE) 2016/679.

2.4 **Supervisão e execução coerciva**

(112) Por forma a assegurar que 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.

2.4.1 *Supervisão independente*

(113) Na República da Coreia, a autoridade independente incumbida de supervisionar e aplicar a Lei relativa à proteção de informações pessoais é a Comissão de Proteção de Informações Pessoais. A Comissão de Proteção de Informações Pessoais é constituída por um presidente, um vice-presidente e sete comissários. O presidente e o vice-presidente são nomeados pelo presidente da República, mediante recomendação do primeiro-ministro. Dois dos comissários são nomeados pelo presidente da República por recomendação do presidente e cinco são nomeados por recomendação da Assembleia Nacional (dos quais, dois por recomendação do partido político a que pertence o presidente da República e três por recomendação de outros partidos políticos (artigo 7.º-2, n.º 2, da Lei relativa à proteção de informações pessoais), o que contribui para o combate ao

([138]) Tal inclui um requisito geral de notificação (artigo 32.º, n.º 7, da Lei relativa à utilização e proteção de informações de crédito) e uma obrigação específica de transparência no caso de as informações que permitem determinar a solvabilidade de uma pessoa singular serem fornecidas a determinadas entidades, como as agências de notação do risco de crédito e as agências de recolha de informações de crédito (artigo 35.º-3 da Lei relativa à utilização e proteção de informações de crédito e artigo 30.º-3 do Decreto de Execução da Lei relativa à utilização e proteção de informações de crédito), ou quando uma relação de transação comercial for recusada ou terminada com base em informações pessoais de crédito recebidas de terceiros (artigo 36.º da Lei relativa à utilização e proteção de informações de crédito e artigo 31.º do Decreto de Execução da Lei relativa à utilização e proteção de informações de crédito).

([139]) Artigo 35.º da Lei relativa à utilização e proteção de informações de crédito. Certas organizações comerciais, como as cooperativas e as empresas públicas (artigo 21.º, n.º 2, do Decreto de Execução da Lei relativa à utilização e proteção de informações de crédito), estão sujeitas a requisitos de transparência adicionais, por exemplo, para tornar públicas determinadas informações (artigo 31.º da Lei relativa à utilização e proteção de informações de crédito) e informar as pessoas singulares de eventuais desvantagens para a sua notação de crédito quando realizam transações financeiras que apresentam riscos de crédito (artigo 35.º-2 da Lei relativa à utilização e proteção de informações de crédito).

([140]) No que respeita às condições e exceções aos direitos de acesso e de retificação, aplicam-se as regras da Lei relativa à proteção de informações pessoais (descritas nos considerandos (76) a (77)). Além disso, o artigo 38.º, n.os 4 a 8, da Lei relativa à utilização e proteção de informações de crédito e o artigo 33.º do Decreto de Execução da Lei relativa à utilização e proteção de informações de crédito especificam outras modalidades. Em especial, um operador comercial que tenha corrigido ou eliminado informações inexatas em matéria de crédito deve notificar a pessoa singular desse facto. Além disso, qualquer terceiro a quem essas informações tenham sido comunicadas nos seis meses anteriores deve ser notificado e a pessoa singular em causa deve ser informada desse facto. Se uma pessoa singular não estiver satisfeita com a forma como um pedido de retificação foi tratado, pode apresentar um pedido à Comissão de Proteção de Informações Pessoais, que verifica a atuação do responsável pelo tratamento e pode impor medidas corretivas.

([141]) Artigo 38.º-3 da Lei relativa à utilização e proteção de informações de crédito.

partidarismo no processo de nomeação ([142]). Este procedimento está em conformidade com os requisitos aplicáveis à nomeação de membros das autoridades competentes em matéria de proteção de dados na União (artigo 53.º, n.º 1, do Regulamento (UE) 2016/679). Além disso, todos os comissários devem abster-se de exercer qualquer atividade em empresas que visam o lucro, atividades políticas e cargos na administração pública ou na Assembleia Nacional (artigo 7.º-6 e artigo 7.º-7, n.º 1, ponto 3, da Lei relativa à proteção de informações pessoais) ([143]). Todos os comissários estão sujeitos a regras específicas que os impedem de participar nas deliberações em caso de conflito de interesses (artigo 7.º-11 da Lei relativa à proteção de informações pessoais). A Comissão de Proteção de Informações Pessoais é assistida por um secretariado (artigo 7.º-13) e pode criar subcomissões (compostas por três comissários) para tratar das infrações menores e das questões recorrentes (artigo 7.º-12 da Lei relativa à proteção de informações pessoais).

(114) Cada membro da Comissão de Proteção de Informações Pessoais é nomeado por três anos e pode ser reconduzido uma vez (artigo 7.º-4, n.º 1, da Lei relativa à proteção de informações pessoais). Os comissários só podem ser destituídos em circunstâncias específicas, nomeadamente se deixarem de poder exercer as suas funções devido a uma deficiência mental ou física prolongada, violarem a lei ou preencherem um dos motivos para a inibição de funções ([144]) (artigo 7.º-5 da Lei relativa à proteção de informações pessoais). Este preceito confere-lhes proteção institucional no exercício das respetivas funções.

(115) De um modo mais geral, o artigo 7.º, n.º 1, da Lei relativa à proteção de informações pessoais garante explicitamente a independência da Comissão de Proteção de Informações Pessoais e o artigo 7.º-5, n.º 2, da Lei relativa à proteção de informações pessoais exige que os comissários desempenhem as suas funções de forma independente, em conformidade com a lei e a sua consciência ([145]). As garantias institucionais e processuais descritas, incluindo no que respeita à nomeação e destituição dos seus membros, garantem que a Comissão de Proteção de Informações Pessoais atua com total independência, sem influências ou instruções externas. Além disso, enquanto serviço administrativo central, a Comissão de Proteção de Informações Pessoais propõe anualmente o seu próprio orçamento (que é examinado pelo Ministério das Finanças no âmbito do orçamento geral nacional antes da adoção pela Assembleia Nacional) e é responsável pela gestão do seu pessoal. A Comissão de Proteção de Informações Pessoais dispõe atualmente de um orçamento de cerca de 35 milhões de EUR e conta com 154 membros do pessoal (incluindo 40 trabalhadores especializados em tecnologias da informação e comunicação, 32 trabalhadores centrados em investigação e 40 juristas).

(116) As funções e competências da Comissão de Proteção de Informações Pessoais estão principalmente previstas nos artigos 7.º-8 e 7.º-9, bem como nos artigos 61.º a 66.º da Lei relativa à proteção de informações pessoais ([146]). Em especial, as tarefas da Comissão de Proteção de Informações Pessoais incluem o aconselhamento sobre legislação e regulamentação relacionadas com a proteção de dados, o desenvolvimento de políticas e orientações em matéria de proteção de dados, a investigação de violações dos direitos individuais, o tratamento de reclamações e a mediação de litígios, a aplicação da Lei relativa à proteção de informações pessoais, a garantia da ensino e promoção no domínio da proteção de dados e o intercâmbio e cooperação com as autoridades competentes em matéria de proteção de dados de países terceiros ([147]).

(117) Com base no artigo 68.º da Lei relativa à proteção de informações pessoais, conjugado com o artigo 62.º do Decreto de Execução da Lei relativa à proteção de informações pessoais, certas funções da Comissão de Proteção de Informações Pessoais foram delegadas na Agência de Internet e Segurança da Coreia, nomeadamente: 1) ensino e relações públicas, 2) formação de especialistas e elaboração de critérios para as avaliações do impacto na privacidade, 3) tratamento de pedidos de designação de uma chamada instituição de avaliação do impacto na privacidade, 4) tratamento de pedidos de acesso indireto a dados pessoais na posse de autoridades públicas (artigo 35.º, n.º 2, da Lei relativa à proteção de informações pessoais) e 5) a tarefa de solicitar materiais e realizar inspeções no que respeito a reclamações recebidas através do chamado centro de atendimento para a privacidade. No contexto do tratamento das queixas através do centro de atendimento para a privacidade, a Agência de Internet e Segurança da Coreia transmite o caso à Comissão de Proteção

([142]) Só podem ser nomeados comissários da Comissão de Proteção de Informações Pessoais as pessoas singulares que satisfaçam os seguintes critérios: altos funcionários públicos responsáveis pelos assuntos de informações pessoais; antigos juízes, magistrados do Ministério Público ou advogados com, pelo menos, dez anos de atividade; antigos gestores com experiência em proteção de dados que tenham exercido funções numa instituição ou organização pública durante mais de três anos ou que tenham sido recomendados por essa instituição ou organização; e antigos professores associados com conhecimentos profissionais no domínio da proteção de dados que tenham exercido funções durante, pelo menos, cinco anos numa instituição académica (artigo 7.º-2 da Lei relativa à proteção de informações pessoais).

([143]) Ver também o artigo 4.º-2 do Decreto de Execução da Lei relativa à proteção de informações pessoais.

([144]) Ver o artigo 7.º-7 da Lei relativa à proteção de informações pessoais, nos termos do qual os nacionais não coreanos e os membros de partidos políticos não podem tornar-se membros da Comissão de Proteção de Informações Pessoais. O mesmo se aplica às pessoas singulares que, nomeadamente, receberam determinados tipos de sanções penais, tenham sido demitidas de funções por sanção disciplinar nos últimos cinco anos (artigo 7.º-7 da Lei relativa à proteção de informações pessoais, conjugado com o artigo 33.º da Lei relativa aos funcionários públicos).

([145]) Embora o artigo 7.º, n.º 2, da Lei relativa à proteção de informações pessoais se refira ao poder geral do primeiro-ministro, nos termos do artigo 18.º da Lei relativa à organização governamental, de suspender ou revogar – com a aprovação do presidente da República – qualquer disposição ilegal ou injusta de um serviço administrativo central, tal poder não é concedido no que respeita aos poderes de investigação ou de execução da Comissão de Proteção de Informações Pessoais (ver artigo 7.º, n.º 2, pontos 1 e 2 da Lei relativa à proteção de informações pessoais). De acordo com as explicações recebidas do Governo coreano, o artigo 18.º da Lei relativa à organização governamental destina-se a dar ao primeiro-ministro a possibilidade de agir em circunstâncias extraordinárias, por exemplo, para mediar um desacordo entre diferentes serviços do Estado. No entanto, o primeiro-ministro nunca fez uso deste poder desde que esta disposição foi adotada em 1963.

([146]) Quando necessário para a execução das tarefas previstas no artigo 7.º-9, n.º 1, da Lei relativa à proteção de informações pessoais, a Comissão de Proteção de Informações Pessoais pode solicitar o parecer de funcionários públicos pertinentes, peritos em proteção de dados, organizações cívicas e operadores económicos pertinentes. Além disso, a Comissão de Proteção de Informações Pessoais pode solicitar materiais pertinentes, formular recomendações para melhorias e verificar se estas são aplicadas (artigo 7.º-9, n.ºs 2 a 5, da Lei relativa à proteção de informações pessoais).

([147]) Ver também o artigo 9.º da Lei relativa à proteção de informações pessoais (plano diretor trienal para a proteção de informações pessoais), artigo 12.º da Lei relativa à proteção de informações pessoais (orientações básicas para a proteção de informações pessoais), artigo 13.º da Lei relativa à proteção de informações pessoais (políticas de promoção e apoio à autorregulação).

de Informações Pessoais ou ao Ministério Público se considerar ter ocorrido uma violação da lei. A possibilidade de apresentar uma reclamação ao centro de atendimento para a privacidade não impede as pessoas singulares de apresentarem diretamente uma reclamação junto da Comissão de Proteção de Informações Pessoais ou de recorrerem à Comissão de Proteção de Informações Pessoais se considerarem que a sua reclamação não foi tratada de forma satisfatória pela Agência de Internet e Segurança da Coreia.

2.4.2 *Execução, incluindo sanções*

(118) A fim de assegurar o cumprimento da Lei relativa à proteção de informações pessoais, o legislador atribuiu à Comissão de Proteção de Informações Pessoais poderes de investigação e de execução, que vão de recomendações a coimas. Estes poderes são ainda complementados por um regime de sanções penais.

(119) No que respeita aos poderes de investigação, se houver uma suspeita ou denúncia de uma violação da Lei relativa à proteção de informações pessoais, ou se tal for necessário para proteger os direitos dos titulares dos dados contra infrações, a Comissão de Proteção de Informações Pessoais pode realizar inspeções no local e solicitar todos os materiais pertinentes (como artigos e documentos) aos responsáveis pelo tratamento de dados pessoais (artigo 63.º da Lei relativa à proteção de informações pessoais, em conjugação com o artigo 60.º do respetivo decreto de execução) ([148]).

(120) Em termos de execução, nos termos do artigo 61.º, n.º 2, da Lei relativa à proteção de informações pessoais, a Comissão de Proteção de Informações Pessoais pode prestar aconselhamento aos responsáveis pelo tratamento de dados sobre como melhorar o nível de proteção dos dados pessoais em atividades de tratamento específicas. Os responsáveis pelo tratamento de dados devem envidar esforços sinceros para seguirem esses conselhos e informar a Comissão do resultado. Além disso, quando existam motivos razoáveis para crer que ocorreu uma violação da Lei relativa à proteção de informações pessoais, e que a não adoção de medidas é suscetível de causar danos difíceis de reparar, a Comissão de Proteção de Informações Pessoais pode impor medidas corretivas (artigo 64.º, n.º 1, da Lei relativa à proteção de informações pessoais) ([149]). O ponto 5 da Notificação n.º 2021-5 (anexo I) esclarece, com efeito vinculativo, que estas condições estão preenchidas no que respeita à violação de qualquer disposição da Lei relativa à proteção de informações pessoais que proteja os direitos à privacidade das pessoas singulares relativamente às informações pessoais ([150]). As medidas que a Comissão de Proteção de Informações Pessoais está habilitada a tomar incluem ordenar a cessação da conduta causadora da violação, a suspensão temporária do tratamento dos dados ou quaisquer outras medidas necessárias. O incumprimento de uma medida corretiva pode levar a uma sanção mediante uma coima máxima de 50 milhões de won (artigo 75.º, n.º 2, ponto 13, da Lei relativa à proteção de informações pessoais).

(121) No que respeita a determinadas autoridades públicas (como a Assembleia Nacional, serviços administrativos centrais, administrações locais e os tribunais), o artigo 64.º, n.º 4, da Lei relativa à proteção de informações pessoais prevê que a Comissão de Proteção de Informações Pessoais pode «recomendar» qualquer uma das medidas corretivas mencionadas no considerando (120) e que essas autoridades são obrigadas a cumprir essa recomendação, a menos que se verifiquem circunstâncias extraordinárias. De acordo com o ponto 5 da Notificação n.º 2021-5, tal refere-se a circunstâncias extraordinárias de facto ou de direito de que a Comissão não tinha conhecimento quando formulou a sua recomendação. A autoridade pública em causa só pode invocar tais circunstâncias extraordinárias se demonstrar claramente que não ocorreu qualquer infração e a Comissão de Proteção de Informações Pessoais determinar que tal não é, efetivamente, o caso. Caso contrário, terá de seguir a recomendação e «adotar uma medida corretiva, nomeadamente, pôr imediatamente termo à ação e indemnizar os danos no caso excecional de um ato ilegal ter sido, mesmo assim, cometido».

(122) A Comissão de Proteção de Informações Pessoais também pode solicitar a outros serviços administrativos com competência específica ao abrigo da legislação setorial (por exemplo, saúde, educação) que realizem uma investigação – individual ou conjuntamente com a Comissão de Proteção de Informações Pessoais – sobre as (suspeitas de) violações da privacidade por parte dos responsáveis pelo tratamento que operam nestes setores sob a sua jurisdição, bem como que imponham medidas corretivas (artigo 63.º, n.ºs 4 e 5, da Lei relativa à proteção da privacidade das comunicações). Nesse caso, a Comissão de Proteção de Informações Pessoais determina os fundamentos, o objeto e o âmbito da investigação ([151]). Por sua vez, o serviço administrativo competente deve apresentar um plano de inspeção à Comissão e notificá-la do resultado da inspeção. A Comissão de Proteção de Informações Pessoais pode recomendar a adoção de uma medida corretiva específica, que o serviço competente deve esforçar-se por aplicar. Em qualquer caso, tal pedido não limita a sua competência para realizar a sua própria investigação ou impor sanções.

([148]) A Comissão de Proteção de Informações Pessoais pode, além disso, entrar nas instalações do responsável pelo tratamento para inspecionar a situação das operações comerciais, registos, documentos, etc. (artigo 63.º, n.º 2, da Lei relativa à proteção de informações pessoais). Ver também o artigo 45.º-3 da Lei relativa à utilização e proteção de informações de crédito e o artigo 36.º-4 do respetivo decreto de execução no que respeita aos poderes da Comissão de Proteção de Informações Pessoais nos termos da referida lei.

([149]) Ver também o artigo 45.º-4 da Lei relativa à utilização e proteção de informações de crédito no que respeita aos poderes da Comissão de Proteção de Informações Pessoais nos termos da referida lei.

([150]) O ponto 5 da notificação prevê que «um motivo válido para considerar que houve uma infração no que respeita às informações pessoais, e que a não adoção de medidas é suscetível de causar danos difíceis de reparar, na aceção do artigo 64.º, n.ºs 1 e 2, da Lei relativa à proteção de informações pessoais, refere-se a uma violação de qualquer um dos princípios, direitos e deveres constantes da lei para proteger os direitos das pessoas singulares às informações pessoais». O mesmo se aplica aos poderes da Comissão de Proteção de Informações Pessoais nos termos do artigo 45.º-4 da Lei relativa à utilização e proteção de informações de crédito.

([151]) Artigo 60.º do Decreto de Execução da Lei relativa à proteção de informações pessoais.

(123) Além dos seus poderes de correção, a Comissão de Proteção de Informações Pessoais pode impor coimas entre 10 e 50 milhões de won por infrações a vários requisitos da Lei relativa à proteção de informações pessoais (artigo 75.º da referida lei) ([152]). Tal inclui, nomeadamente, o incumprimento dos requisitos de licitude do tratamento, a não adoção das medidas de segurança necessárias, a não notificação dos titulares dos dados em caso de violação de dados, o incumprimento dos requisitos de subcontratação ulterior, a não definição e divulgação de uma política de privacidade, a não designação de um responsável pela privacidade, ou a omissão de agir a pedido do titular dos dados no exercício dos seus direitos individuais, bem como certas violações processuais (não cooperação durante uma investigação). Caso o mesmo responsável pelo tratamento viole várias disposições da Lei relativa à proteção de informações pessoais, é possível aplicar uma coima por cada violação e, na fixação do montante da coima, será tido em conta o número de pessoas singulares afetadas.

(124) Além disso, sempre que existam motivos razoáveis para suspeitar de uma violação da Lei relativa à proteção de informações pessoais ou de qualquer outra «legislação relacionada com a proteção de dados», a Comissão de Proteção de Informações Pessoais pode apresentar uma queixa-crime ao organismo de investigação competente (como um procurador, ver o artigo 65.º, n.º 1, da Lei relativa à proteção de informações pessoais). Pode ainda recomendar ao responsável pelo tratamento que tome medidas disciplinares contra a pessoa responsável (nomeadamente o gestor responsável, ver o artigo 65.º, n.º 2, da Lei relativa à proteção de informações pessoais). Ao receber essa recomendação, o responsável pelo tratamento deve segui-la ([153]) e notificar a Comissão de Proteção de Informações Pessoais, por escrito, dos resultados (artigo 65.º da Lei relativa à proteção de informações pessoais em conjugação com o artigo 58.º do respetivo decreto de execução).

(125) No que respeita às recomendações nos termos do artigo 61.º, às medidas corretivas nos termos do artigo 64.º, à acusação ou recomendação de medidas disciplinares nos termos do artigo 65.º, e à imposição de coimas nos termos do artigo 75.º da Lei relativa à proteção de informações pessoais, a Comissão de Proteção de Informações Pessoais pode divulgar os factos – ou seja, a infração, a entidade que infringiu a lei e a(s) medida(s) imposta(s) –, publicando-os no seu sítio Web ou num jornal diário nacional (artigo 66.º da Lei relativa à proteção de informações pessoais, em conjugação com o artigo 61.º, n.º 1, do respetivo decreto de execução) ([154]).

(126) Por último, o cumprimento dos requisitos em matéria de proteção de dados da Lei relativa à proteção de informações pessoais (bem como de outra «legislação relacionada com a proteção de dados») é apoiado por um regime de sanções penais. A este respeito, os artigos 70.º a 73.º da referida lei contêm disposições sancionatórias que podem levar à imposição de uma multa (entre 20 e 100 milhões de won) ou de uma pena de prisão (variando a pena máxima entre dois e dez anos). As infrações pertinentes incluem, nomeadamente, a utilização de dados pessoais ou o fornecimento desses dados a terceiros sem o consentimento necessário, o tratamento de informação sensível contrariamente à proibição estabelecida no artigo 23.º, n.º 1, da Lei relativa à proteção de informações pessoais, o incumprimento dos requisitos de segurança aplicáveis que resulte na perda, roubo, divulgação, falsificação, alteração ou deterioração de dados pessoais, a não adoção das medidas necessárias para corrigir, apagar ou suspender dados pessoais, ou a transferência ilícita de dados pessoais para um país terceiro ([155]). Nos termos do artigo 74.º da Lei relativa à proteção de informações pessoais, em cada um destes casos, o funcionário, o agente ou o representante do responsável pelo tratamento, bem como o próprio responsável pelo tratamento, são responsáveis ([156]).

(127) Além das sanções penais previstas na Lei relativa à proteção de informações pessoais, a utilização abusiva de dados pessoais também pode constituir uma infração nos termos do Código Penal. É o caso, designadamente, da violação do sigilo de cartas, documentos ou registos eletrónicos (artigo 316.º), da divulgação de informações sujeitas a sigilo profissional (artigo 317.º), da fraude através da utilização de computadores (artigo 347.º-2), bem como do peculato e abuso de confiança (artigo 355.º).

(128) Por conseguinte, o sistema coreano combina diferentes tipos de sanções, desde medidas corretivas e coimas a sanções penais, que são suscetíveis de ter um efeito dissuasor particularmente forte nos responsáveis pelo

([152]) Além disso, nos casos em que os sistemas de tratamento e proteção de dados pessoais operados por um responsável pelo tratamento tenham sido certificados como estando em conformidade com a Lei relativa à proteção de informações pessoais, mas em que os critérios de certificação nos termos do artigo 34.º-2, n.º 1, do decreto de execução da referida lei não foram efetivamente cumpridos, ou em caso de uma violação grave de qualquer «legislação relacionada com a proteção de informações [pessoais]», a Comissão de Proteção de Informações Pessoais pode revogar a certificação (artigo 32.º-2, n.ºs 3 e 5, da Lei relativa à proteção de informações pessoais). A Comissão deve notificar o responsável pelo tratamento dessa revogação e anunciá-la publicamente, ou publicá-la no seu sítio Web ou no Jornal Oficial (artigo 34.º-4 do Decreto de Execução da Lei relativa à proteção de informações pessoais). Estão ainda previstas coimas (artigo 52.º da Lei relativa à utilização e proteção de informações de crédito) e sanções penais (artigo 50.º da referida lei) para violações da Lei relativa à utilização e proteção de informações de crédito.

([153]) Nos termos do artigo 58.º, n.º 2, do Decreto de Execução da Lei relativa à proteção de informações pessoais, caso circunstâncias especiais tornem o cumprimento da recomendação «impraticável», o responsável pelo tratamento tem de apresentar uma justificação fundamentada à Comissão de Proteção de Informações Pessoais.

([154]) Ao decidir se deve ou não fazer tal divulgação pública, a Comissão de Proteção de Informações Pessoais deve ter em conta a substância e a gravidade da violação, a sua duração e frequência, bem como as suas consequências (extensão dos danos). A entidade em causa deve ser previamente notificada e ter a possibilidade de se defender. Ver o artigo 61.º, n.ºs 2 e 3, do Decreto de Execução da Lei relativa à proteção de informações pessoais.

([155]) Ver o artigo 71.º, ponto 2, em conjugação com o artigo 18.º, n.º 1, da Lei relativa à proteção de informações pessoais (incumprimento das condições do artigo 17.º, n.º 3, da referida lei, a que se refere o artigo 18.º, n.º 1). Ver também o artigo 75.º, n.º 2, ponto 1, em conjugação com o artigo 17.º, n.º 2, da Lei relativa à proteção de informações pessoais (não fornecimento das informações necessárias ao indivíduo em causa nos termos do artigo 17.º, n.º 2, da referida lei, a que se refere o artigo 17.º, n.º 3).

([156]) Além disso, o artigo 74.º-2 da Lei relativa à proteção de informações pessoais permite o confisco de quaisquer montantes, bens ou outros lucros obtidos em consequência da violação ou, se o confisco for impossível, a «cobrança» do benefício obtido ilicitamente.

tratamento e nas pessoas que tratam os dados. Imediatamente após a sua criação, em 2020, a Comissão de Proteção de Informações Pessoais começou a fazer uso dos seus poderes. Do relatório anual de 2021 da Comissão de Proteção de Informações Pessoais depreende-se que a Comissão já formulou várias recomendações, aplicou coimas e medidas corretivas, tanto a operadores do setor público (cerca de 34 autoridades públicas) como a operadores privados (cerca de 140 empresas) ([157]). Importa referir alguns processos, por exemplo, a aplicação, em dezembro de 2020, de uma coima de 6 700 de won a uma empresa pela violação de diferentes disposições da Lei relativa à proteção de informações pessoais (nomeadamente requisitos em matéria de segurança, de consentimento para a prestação de serviços por terceiros e de transparência) ([158]) e a aplicação, em abril de 2021, de uma coima de 103,3 milhões de won a uma empresa de tecnologia de IA (por violar, entre outras disposições, as regras relativas à licitude do tratamento, designadamente ao consentimento, e ao tratamento de informações pseudonimizadas) ([159]). Em agosto de 2021, a Comissão de Proteção de Informações Pessoais concluiu uma outra investigação à atividade de três empresas, que culminou em medidas corretivas e na aplicação de coimas num montante máximo de 6 470 milhões de won (nomeadamente por não terem informado as pessoas singulares sobre a divulgação de dados pessoais a terceiros, incluindo transferências para países terceiros) ([160]). Além disso, já antes da recente reforma, a Coreia do Sul tinha um sólido historial de execução, tendo as autoridades responsáveis feito uso de todo o conjunto de medidas coercivas, nomeadamente coimas, medidas corretivas e «nomeação e partilha», relativamente a vários responsáveis pelo tratamento, incluindo prestadores de serviços de comunicação (Comissão das Comunicações da Coreia), bem como operadores comerciais, instituições financeiras, autoridades públicas, universidades e hospitais (Ministério do Interior e da Segurança) ([161]). Consequentemente, a Comissão conclui que o sistema coreano assegura a execução efetiva das regras relativas à proteção de dados na prática, garantindo assim um nível de proteção essencialmente equivalente ao previsto no Regulamento (UE) 2016/679.

2.5 **Recurso**

(129) 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.

(130) O sistema coreano proporciona às pessoas singulares vários mecanismos para exercer efetivamente os seus direitos e obter reparação (judicial).

(131) Numa primeira fase, as pessoas singulares que considerem que os seus direitos ou interesses em matéria de proteção de dados foram violados podem recorrer ao responsável pelo tratamento em causa. Nos termos do artigo 30.º, n.º 1, ponto 5, da Lei relativa à proteção de informações pessoais, a política de privacidade do responsável pelo tratamento deve incluir, nomeadamente, informações sobre os direitos dos titulares de dados e a forma de os exercer. Além disso, deve fornecer informações de contacto, como o nome e o número de telefone do responsável pela privacidade ou do departamento responsável pela proteção de dados, para permitir a apresentação de reclamações («queixas»). Na organização do responsável pelo tratamento, o responsável pela privacidade está incumbido do tratamento de reclamações, da adoção de medidas corretivas em caso de violação da privacidade e das indemnizações corretivas (artigo 31.º, n.º 2, ponto 3, e n.º 4, da Lei relativa à proteção de informações pessoais). É pertinente, por exemplo, em caso de violação de dados, uma vez que o responsável pelo tratamento tem de informar o titular dos dados do(s) ponto(s) de contacto para comunicar eventuais danos, entre outros (artigo 34.º, n.º 1, ponto 5, da Lei relativa à proteção de informações pessoais).

(132) Além disso, a Lei relativa à proteção de informações pessoais oferece às pessoas singulares várias vias de recurso contra os responsáveis pelo tratamento. Em primeiro lugar, qualquer pessoa que considere que os seus direitos ou interesses em matéria de proteção de dados foram violados pelo responsável pelo tratamento pode denunciar essa infração diretamente à Comissão de Proteção de Informações Pessoais e/ou a uma das instituições especializadas por ela designadas para receber e tratar reclamações; tal inclui a Agência de Internet e Segurança da Coreia que, para o efeito, gere um centro de atendimento para as informações pessoais (o chamado «centro de atendimento para a privacidade») (artigo 62.º, n.ºs 1 e 2, da Lei relativa à proteção de informações pessoais, em conjugação com o artigo 59.º do respetivo decreto de execução). O centro de atendimento telefónico para a privacidade investiga e estabelece infrações, presta aconselhamento em matéria de tratamento de dados pessoais (artigo 62.º, n.º 3, da Lei relativa à proteção de informações pessoais) e pode comunicar infrações à Comissão de Proteção de Informações Pessoais (não podendo, no entanto, adotar, por si mesmo, medidas coercivas). O centro de atendimento telefónico

([157]) Ver o relatório anual de 2021 da Comissão de Proteção de Informações Pessoais, p. 50-55 (disponível apenas em coreano), em https://www.pipc.go.kr/np/cop/bbs/selectBoardArticle.do?bbsId=BS074&mCode=C020010000&nttId=7511#LINK.

([158]) Ver em (disponível apenas em coreano) https://www.pipc.go.kr/np/cop/bbs/selectBoardArticle.do?bbsId=BS074&mCode=C020010000&nttId=6954#LINK.

([159]) Ver em (disponível apenas em coreano) https://www.pipc.go.kr/np/cop/bbs/selectBoardArticle.do?bbsId=BS074&mCode=C020010000&nttId=7298&fbclid=IwAR3SKcMQi6G5pR9k4l7j6GNXtc8aBVDOwcURevvvzQtYI7AS40UKYXoOXo8.

([160]) Ver em (disponível apenas em coreano): https://www.pipc.go.kr/np/cop/bbs/selectBoardArticle.do?bbsId=BS074&mCode=C020010000&nttId=7497#LINK.

([161]) Ver, por exemplo, o relatório anual de 2020 em (disponível apenas em coreano) https://www.pipc.go.kr/np/cop/bbs/selectBoardList.do?bbsId=BS079&mCode=D070020000 e os exemplos fornecidos em inglês em https://www.privacy.go.kr/eng/enforcement_02.do.

para a privacidade recebe um grande número de reclamações/pedidos (por exemplo, 177 457 em 2020, 159 255 em 2019 e 164 497 em 2018) ([162]). De acordo com as informações recebidas da Comissão de Proteção de Informações Pessoais, a própria Comissão recebeu cerca de mil reclamações entre agosto de 2020 e agosto de 2021. Em resposta a uma reclamação, a Comissão de Proteção de Informações Pessoais, pode formular recomendações de melhorias, medidas corretivas, uma «acusação» ao organismo de investigação competente (incluindo um procurador) ou uma recomendação de medidas disciplinares (ver os artigos 61.º, 64.º e 65.º da Lei relativa à proteção de informações pessoais). As decisões da Comissão de Proteção de Informações Pessoais (como a recusa de tratar uma reclamação ou o indeferimento de uma reclamação quanto ao mérito) podem ser contestadas ao abrigo da Lei relativa ao contencioso administrativo ([163]).

(133) Em segundo lugar, nos termos dos artigos 40.º a 50.º da Lei relativa à proteção de informações pessoais, em conjugação com os artigos 48.º-14 a 57.º do respetivo decreto de execução, os titulares dos dados podem apresentar reclamações ao chamado «Comité de Mediação de Litígios», composto por representantes nomeados pelo presidente da Comissão de Proteção de Informações Pessoais de entre os membros do seu Serviço Executivo Superior e por pessoas nomeadas com base na sua experiência em matéria de proteção de dados entre determinados grupos elegíveis (ver artigo 40.º, n.ºs 2, 3, e 7, da Lei relativa à proteção de informações pessoais, e artigo 48.º-14 do respetivo decreto de execução) ([164]). A possibilidade de recorrer à mediação junto do Comité de Mediação de Litígios constitui uma via alternativa para obter reparação, mas não limita o direito da pessoa singular de recorrer à Comissão de Proteção de Informações Pessoais ou aos tribunais. Para analisar o caso, o Comité pode solicitar às partes no litígio que forneçam os materiais necessários e/ou convocar testemunhas pertinentes (artigo 45.º da Lei relativa à proteção de informações pessoais). Uma vez esclarecida a questão, o Comité elabora um projeto de decisão de mediação ([165]), relativamente ao qual a maioria dos seus membros deve chegar a acordo. O projeto de decisão de mediação pode incluir a suspensão da violação, as medidas corretivas necessárias (incluindo a restituição ou a indemnização), bem como quaisquer medidas necessárias para evitar a repetição da mesma violação ou de violações similares (artigo 47.º, n.º 1, da Lei relativa à proteção de informações pessoais). Se ambas as partes aceitarem a decisão de mediação, esta terá o mesmo efeito que uma transação em tribunal (artigo 47.º, n.º 5, da Lei relativa à proteção de informações pessoais). Nenhuma das partes está impedida de intentar uma ação judicial enquanto a mediação estiver em curso; nesse caso, a mediação será suspensa (ver artigo 48.º, n.º 2, da Lei relativa à proteção de informações pessoais) ([166]). Os números anuais publicados pela Comissão de Proteção de Informações Pessoais mostram que as pessoas singulares recorrem regularmente ao procedimento junto do Comité de Mediação de Litígios, o que conduz, muitas vezes, a um resultado positivo. Por exemplo, em 2020, o Comité tratou 126 processos, dos quais 89 foram resolvidos junto do Comité (com 77 processos em que as partes chegaram a acordo antes do fim do processo de mediação e 12 processos em que as partes aceitaram a proposta de mediação), o que resultou numa taxa de mediação de 70,6 % ([167]). De igual modo, em 2019, o Comité tratou 139 processos, dos quais 92 foram resolvidos, o que resultou numa taxa de mediação de 62,2 %.

(134) Além disso, nos casos em que, pelo menos, 50 pessoas singulares sofram danos, ou em que os seus direitos em matéria de proteção de dados tenham sido violados da mesma forma ou de forma similar na sequência do mesmo (tipo de) incidente ([168]), um titular de dados ou uma organização de proteção de dados pode solicitar a mediação coletiva de litígios em nome desse grupo; outros titulares de dados podem pedir para se juntar a essa mediação, que será anunciada publicamente pelo Comité de Mediação de Litígios (artigo 49.º, n.ºs 1 a 3, da Lei relativa à proteção de informações pessoais, em conjugação com os artigos 52.º a 54.º do respetivo decreto de execução) ([169]). O Comité de

([162]) Ver relatório anual da Comissão de Proteção de Informações Pessoais de 2021, p. 174. Em 2020, essas reclamações diziam respeito, por exemplo, à recolha de dados sem consentimento, ao incumprimento das obrigações de transparência, às violações da Lei relativa à proteção de informações pessoais pelos subcontratantes, a medidas de segurança insuficientes, à falta de resposta aos pedidos dos titulares dos dados, bem como a inquéritos gerais.

([163]) Mais especificamente, as pessoas singulares podem recorrer do exercício ou da recusa de exercício do poder público por parte de um serviço administrativo (artigo 2.º, n.º 1, ponto 1, e artigo 3.º, ponto 1, da Lei relativa ao contencioso administrativo). O considerando (181) contém informações mais pormenorizadas sobre os aspetos processuais, incluindo os requisitos de admissibilidade.

([164]) Todos os membros têm um mandato fixo e só podem ser destituídos com justa causa (ver artigo 40.º, n.º 5, e artigo 41.º da Lei relativa à proteção de informações pessoais). Além disso, o artigo 42.º da referida lei contém garantias de proteção contra conflitos de interesses.

([165]) Ver o artigo 44.º da Lei relativa à proteção de informações pessoais. Além disso, pode propor um projeto de acordo e recomendar um acordo sem mediação (ver artigo 46.º da Lei relativa à proteção de informações pessoais).

([166]) Além disso, o Comité pode rejeitar a mediação se considerar inadequado mediar o litígio, tendo em conta a sua natureza, ou porque o pedido de mediação foi apresentado com um propósito injusto (artigo 48.º da Lei relativa à proteção de informações pessoais).

([167]) Ver relatório anual da Comissão de Proteção de Informações Pessoais, p. 174-180. Estes processos diziam respeito, nomeadamente, a violações da obrigação de obter consentimento para a recolha de dados, do princípio da limitação da finalidade e dos direitos dos titulares dos dados.

([168]) Ver o artigo 49.º, n.º 1, da Lei relativa à proteção de informações pessoais, segundo o qual os titulares dos dados têm de sofrer danos ou uma violação dos seus direitos «de uma forma idêntica ou similar», e o artigo 52.º, ponto 2, do decreto de execução da referida lei, que estabelece que «[a]s principais questões do incidente são comuns de facto ou de direito».

([169]) Além disso, mesmo as não partes podem beneficiar de uma decisão de mediação de litígios coletiva aceite pelo responsável pelo tratamento, na medida em que o Comité de Mediação de Litígios pode aconselhar o responsável pelo tratamento a elaborar e a apresentar um plano de indemnização que (também) as abranja (artigo 49.º, n.º 5, da Lei relativa à proteção de informações pessoais).

Mediação de Litígios pode selecionar, pelo menos, uma pessoa que represente o interesse comum de forma mais adequada como parte representativa (artigo 49.º, n.º 4, da Lei relativa à proteção de informações pessoais). Se o responsável pelo tratamento rejeitar a mediação coletiva de litígios ou não aceitar a decisão de mediação, algumas organizações ([170]) podem intentar uma ação coletiva para resolver a violação (artigos 51.º a 57.º da Lei relativa à proteção de informações pessoais).

(135) Em terceiro lugar, no caso de uma violação da privacidade que cause «danos» à pessoa singular, o titular dos dados tem direito a uma reparação adequada através de um «procedimento rápido e justo» (artigo 4.º, ponto 5, com o artigo 39.º da Lei relativa à proteção de informações pessoais) ([171]). O responsável pelo tratamento pode eximir-se da responsabilidade, provando a ausência de culpa («intenção dolosa» ou negligência). Sempre que o titular dos dados sofra danos por perda, roubo, divulgação, falsificação, alteração ou deterioração dos seus dados pessoais, o tribunal pode determinar uma indemnização até ao triplo dos danos efetivos, tendo em conta um conjunto de fatores (artigo 39.º, n.os 3 e 4, da Lei relativa à proteção de informações pessoais). Em alternativa, o titular dos dados pode pedir um «montante razoável» de indemnização não superior a três milhões de won (artigo 39.º-2, n.os 1 e 2, da Lei relativa à proteção de informações pessoais). Além disso, nos termos do Código Civil, é possível pedir uma indemnização a qualquer pessoa «que cause prejuízos ou danos a outra pessoa por ato ilícito, intencional ou negligente» ([172]) ou a uma pessoa «que tenha causado danos a outra, à sua liberdade ou reputação, ou que lhe tenha infligido sofrimento psíquico» ([173]). Tal responsabilidade civil decorrente da violação das regras relativas à proteção de dados foi confirmada pelo Supremo Tribunal ([174]). Se os danos tiverem sido causados por uma ação ilícita de uma autoridade pública, é ainda possível apresentar um pedido de indemnização ao abrigo da Lei relativa às indemnizações do Estado ([175]). Um pedido de indemnização ao abrigo da referida lei pode ser apresentado a um «Conselho de Indemnizações» especializado, ou diretamente nos tribunais coreanos ([176]). A responsabilidade do Estado também cobre danos não patrimoniais (como o sofrimento mental) ([177]). Se a vítima for um nacional estrangeiro, a Lei relativa às indemnizações do Estado aplica-se desde que o seu país de origem garanta igualmente uma indemnização do Estado aos nacionais coreanos ([178]).

(136) Em quarto lugar, o Supremo Tribunal reconheceu que as pessoas singulares têm o direito de requerer uma medida inibitória por violação dos seus direitos ao abrigo da Constituição, incluindo o direito à proteção dos dados pessoais ([179]). Neste contexto, um tribunal pode, por exemplo, ordenar aos responsáveis pelo tratamento que suspendam ou cessem qualquer atividade ilícita. Além disso, os direitos à proteção de dados, nomeadamente os direitos protegidos pela Lei relativa à proteção de informações pessoais, podem ser exercidos mediante ações cíveis. Esta aplicação horizontal da proteção constitucional da privacidade às relações entre partes privadas foi reconhecida pelo Supremo Tribunal ([180]).

([170]) Nomeadamente, grupos de consumidores ou ONG sem fins lucrativos de uma determinada dimensão em termos de número de membros, cujo objetivo declarado seja a proteção de dados [embora, no caso destas últimas, com o requisito adicional de que, pelo menos, 100 titulares de dados que tenham sofrido o mesmo (tipo de) infração tenham apresentado um pedido para intentar uma ação coletiva]. Ver o artigo 51.º da Lei relativa à proteção de informações pessoais.

([171]) Os artigos 43.º a 43.º-3 da Lei relativa à utilização e proteção de informações de crédito também estabelecem a responsabilidade de indemnizar por danos resultantes de violações da referida lei.

([172]) Artigo 750.º do Código Civil.

([173]) Artigo 751.º, n.º 1, do Código Civil.

([174]) Ver, por exemplo, a Decisão n.º 2015Da251539, 251546, 251553, 251560, 251577 do Supremo Tribunal, de 30 de maio de 2018. Além disso, o Supremo Tribunal confirmou que as violações de dados podem levar a uma indemnização ao abrigo do Código Civil, ver a Decisão n.º 2011Da59834, 59858, 59841 do Supremo Tribunal, de 26 de dezembro de 2012 (resumo em inglês disponível em http://library.scourt.go.kr/SCLIB_data/decision/9-69%202012.12.26.2011Da59834.htm). Neste caso, o Supremo Tribunal esclareceu que, para avaliar se houve um sofrimento emocional que se qualifique como dano indemnizável, devem ser considerados vários fatores, como o tipo e as características das informações divulgadas, a identificabilidade da pessoa devido à violação, a possibilidade de acesso aos dados por terceiros, o grau de difusão das informações pessoais, se tal levou a quaisquer violações adicionais dos direitos individuais, a forma como as informações pessoais foram geridas e protegidas, etc.

([175]) Com base na Lei relativa às indemnizações do Estado, as pessoas singulares podem requerer uma indemnização por danos infligidos por funcionários públicos, no exercício das suas funções oficiais, em violação da lei (artigo 2.º, n.º 1, da referida lei).

([176]) Artigos 9.º e 12.º da Lei relativa às indemnizações do Estado. A lei cria Conselhos Distritais (presididos pelo procurador-adjunto da procuradoria correspondente), um Conselho Central (presidido pelo vice-ministro da Justiça) e um Conselho Especial (encarregado dos pedidos de indemnização por danos infligidos por militares ou funcionários civis das forças armadas, presidido pelo vice-ministro da Defesa Nacional). Os pedidos de indemnização são, em princípio, tratados pelos Conselhos Distritais que, em determinadas circunstâncias, têm de transmitir os casos ao Conselho Central/Especial, por exemplo, se a indemnização exceder um determinado montante ou no caso de um indivíduo se candidatar a uma nova deliberação. Todos os Conselhos são compostos por membros nomeados pelo ministro da Justiça (por exemplo, entre os funcionários públicos do Ministério da Justiça, oficiais de justiça, advogados e pessoas com conhecimentos especializados relacionados com indemnizações do Estado) e estão sujeitos a regras específicas em matéria de conflitos de interesses (ver artigo 7.º do Decreto de Execução da Lei relativa às indemnizações do Estado).

([177]) Ver o artigo 8.º da Lei relativa às indemnizações do Estado (que faz referência ao Código Civil), bem como o artigo 751.º do Código Civil.

([178]) Artigo 7.º da Lei relativa às indemnizações do Estado.

([179]) Decisão n.º 93Da40614 do Supremo Tribunal, de 12 de abril de 1996, e Decisão n.º 2008Da42430 do Supremo Tribunal, de 2 de setembro de 2011 (resumo em inglês disponível em https://www.scourt.go.kr/eng/supreme/decisions/NewDecisionsView.work?seq=696&pageIndex=1&mode=6&searchWord=).

([180]) Ver, por exemplo, a Decisão n.º 2008Da42430 do Supremo Tribunal, de 2 de setembro de 2011 (resumo em inglês disponível em https://www.scourt.go.kr/eng/supreme/decisions/NewDecisionsView.work?seq=696&pageIndex=1&mode=6&searchWord=).

(137) Por último, as pessoas singulares podem apresentar uma queixa-crime nos termos da Lei relativa ao processo penal (artigo 223.º) junto de um procurador público ou agente da polícia judiciária ([181]).

(138) Por conseguinte, o sistema coreano oferece várias vias de recurso, desde opções facilmente acessíveis e de baixo custo [por exemplo, contactando o centro de atendimento para a privacidade ou através da mediação (coletiva)] a vias administrativas (perante a Comissão de Proteção de Informações Pessoais) e judiciais, nomeadamente com a possibilidade de obter uma indemnização por danos.

3. ACESSO E UTILIZAÇÃO DE DADOS PESSOAIS TRANSFERIDOS DA UNIÃO EUROPEIA POR AUTORIDADES PÚBLICAS NA REPÚBLICA DA COREIA

(139) A Comissão avaliou igualmente as limitações e garantias, incluindo a supervisão e os mecanismos individuais de recurso disponíveis na legislação coreana, no tocante à recolha e utilização subsequente pelas autoridades públicas coreanas de dados pessoais transferidos para responsáveis pelo tratamento na Coreia, para fins de interesse público, designadamente para efeitos de aplicação do direito penal e de segurança nacional («acesso governamental»). Nesta matéria, o Governo coreano apresentou à Comissão declarações, garantias e compromissos oficiais, assinados ao mais alto nível ministerial e dos organismos, os quais constam do anexo II da presente decisão.

(140) Ao avaliar se as condições em que o governo acede aos dados transferidos para a Coreia ao abrigo da presente decisão cumprem o teste de «equivalência essencial» nos termos do artigo 45.º, n.º 1, do Regulamento (UE) 2016/679, conforme interpretado pelo Tribunal de Justiça da União Europeia, à luz da Carta dos Direitos Fundamentais, a Comissão teve em conta sobretudo os seguintes critérios.

(141) Em primeiro lugar, qualquer restrição ao direito de proteção de dados pessoais deve ser prevista por lei, o que implica que a própria base jurídica que permite a ingerência nesses direitos deve definir o alcance da restrição ao exercício do direito em causa ([182]).

(142) Em segundo lugar, para satisfazer o requisito da proporcionalidade, segundo o qual as derrogações à proteção de dados pessoais e as suas restrições devem ocorrer na estrita medida do necessário numa sociedade democrática para alcançar os objetivos específicos de interesse geral equivalentes aos reconhecidos pela União, a regulamentação do país terceiro em causa que permite a ingerência deve prever regras claras e precisas que regulem o alcance e a aplicação das medidas em causa e imponham requisitos mínimos, de modo que as pessoas cujos dados foram transferidos disponham de garantias suficientes que permitam proteger eficazmente os seus dados pessoais contra os riscos de abuso ([183]). A regulamentação deve, em especial, indicar em que circunstâncias e em que condições se pode adotar uma medida que preveja o tratamento desses dados ([184]), bem como sujeitar o cumprimento desses requisitos a uma supervisão independente ([185]).

(143) Em terceiro lugar, essa regulamentação e respetivos requisitos devem ser juridicamente vinculativos no direito interno. Tal diz respeito, em primeiro lugar, às autoridades do país terceiro em questão, mas os requisitos legais também devem ser oponíveis nos tribunais contra essas autoridades ([186]). Em particular, os titulares de dados devem dispor da possibilidade de recorrer a medidas jurídicas corretivas eficazes num tribunal independente e imparcial, para ter acesso a dados pessoais que lhes digam respeito ou para obter a retificação ou a supressão desses dados ([187]).

3.1 Quadro jurídico geral

(144) As limitações e garantias aplicáveis à recolha e utilização subsequente de dados pessoais pelas autoridades públicas coreanas decorrem do quadro constitucional geral, das leis específicas que regulam as suas atividades nos domínios da aplicação do direito penal e da segurança nacional, bem como das regras especificamente aplicáveis ao tratamento de dados pessoais.

([181]) Conforme explicado no considerando (127), a utilização indevida de dados pode constituir uma infração penal nos termos do Código Penal.

([182]) Ver acórdão do Tribunal de Justiça de 16 de julho de 2020, Facebook Ireland e Schrems («Schrems II»), C-311/18, ECLI:EU:C:2020:559, n.ºs 174 a 175, e a jurisprudência referida. Ver ainda, no que diz respeito ao acesso das autoridades públicas dos Estados-Membros, o acórdão do Tribunal de Justiça de 6 de outubro de 2020, Privacy International, C-623/17, ECLI:EU:C:2020:790, n.º 65; e o acórdão do Tribunal de Justiça de 6 de outubro de 2020, La Quadrature du Net e o., processos apensos C-511/18, C-512/18 e C-520/18, ECLI:EU:C:2020:791, n.º 175.

([183]) Ver acórdão do Tribunal de Justiça de 16 de julho de 2020, Facebook Ireland e Schrems («Schrems II»), C-311/18, ECLI:EU:C:2020:559, n.ºs 176 e 181, bem como a jurisprudência referida. Ver ainda, no que diz respeito ao acesso das autoridades públicas dos Estados-Membros, o acórdão do Tribunal de Justiça de 6 de outubro de 2020, Privacy International, C-623/17, ECLI:EU:C:2020:790, n.º 68; e o acórdão do Tribunal de Justiça de 6 de outubro de 2020, La Quadrature du Net e o., processos apensos C-511/18, C-512/18 e C-520/18, ECLI:EU:C:2020:791, n.º 132.

([184]) Ver acórdão do Tribunal de Justiça de 16 de julho de 2020, Facebook Ireland e Schrems («Schrems II»), C-311/18, ECLI:EU:C:2020:559, n.º 176. Ver ainda, no que diz respeito ao acesso das autoridades públicas dos Estados-Membros, o acórdão do Tribunal de Justiça de 6 de outubro de 2020, Privacy International, C-623/17, ECLI:EU:C:2020:790, n.º 68; e o acórdão do Tribunal de Justiça de 6 de outubro de 2020, La Quadrature du Net e o., processos apensos C-511/18, C-512/18 e C-520/18, ECLI:EU:C:2020:791, n.º 132.

([185]) Ver acórdão do Tribunal de Justiça de 16 de julho de 2020, Facebook Ireland e Schrems («Schrems II»), C-311/18, ECLI:EU:C:2020:559, n.º 179.

([186]) Ver acórdão do Tribunal de Justiça de 16 de julho de 2020, Facebook Ireland e Schrems («Schrems II»), C-311/18, ECLI:EU:C:2020:559, n.ºs 181 a 182.

([187]) Ver acórdão do Tribunal de Justiça de 6 de outubro de 2015, Maximillian Schrems/Data Protection Commissioner («Schrems»), C-362/14, ECLI:EU:C:2015:650, n.º 95; e acórdão do Tribunal de Justiça de 16 de julho de 2020, Facebook Ireland e Schrems («Schrems II»), C-311/18, ECLI:EU:C:2020:559, n.º 194. A esse respeito, o TJUE salientou que a observância do artigo 47.º da Carta dos Direitos Fundamentais, que garante o direito à ação por um tribunal independente e imparcial, «faz parte do nível de proteção exigido na União [e] deve ser constatada pela Comissão antes de adotar uma decisão de adequação ao abrigo do artigo 45.º, n.º 1, do Regulamento (UE) 2016/679» (Schrems II, n.º 186).

(145) Em primeiro lugar, o acesso aos dados pessoais pelas autoridades públicas coreanas rege-se pelos princípios gerais da legalidade, da necessidade e da proporcionalidade que decorrem da Constituição coreana ([188]). Mais especificamente, os direitos e liberdades fundamentais (nomeadamente o direito à privacidade e à privacidade da correspondência) ([189]) só podem ser restringidos por lei, quando necessário, por razões de segurança nacional, de manutenção da ordem e da segurança pública e para o bem-estar público. Tais restrições não podem afetar a essência do direito ou da liberdade em causa. No que respeita especificamente às buscas e apreensões, a Constituição prevê que estas só podem ser realizadas nas condições previstas na lei, com base num mandado emitido por um juiz e no respeito das garantias processuais ([190]). Por último, as pessoas singulares podem invocar os seus direitos e liberdades junto do Tribunal Constitucional se considerarem que estes foram violados pelas autoridades públicas no exercício dos seus poderes ([191]). Do mesmo modo, as pessoas que tenham sofrido danos devido a um ato ilícito cometido por um funcionário público no exercício das suas funções oficiais têm o direito de pedir uma indemnização justa ([192]).

(146) Em segundo lugar, conforme descrito com mais pormenor nos pontos 3.2.1 e 3.3.1, os princípios gerais referidos no considerando (145) também estão refletidos nas leis específicas que regulam os poderes das autoridades de aplicação da lei e das autoridades nacionais de segurança. Por exemplo, no que respeita às investigações criminais, a Lei relativa ao processo penal prevê que só possam ser tomadas medidas obrigatórias quando explicitamente previsto na referida lei e na medida do necessário para alcançar o objetivo da investigação ([193]). Do mesmo modo, o artigo 3.º da Lei relativa à proteção da privacidade das comunicações proíbe o acesso às comunicações privadas, exceto com base na lei e sob reserva das limitações e garantias nela previstas. No domínio da segurança nacional, a Lei relativa ao Serviço Nacional de Informações prevê que qualquer acesso a comunicações ou informações de localização deve respeitar a lei, e sujeita o abuso de poder e as violações da lei a sanções penais ([194]).

(147) Em terceiro lugar, o tratamento de dados pessoais pelas autoridades públicas, nomeadamente para efeitos de aplicação da lei e de segurança nacional, está sujeito às regras relativas à proteção de dados nos termos da Lei relativa à proteção de informações pessoais ([195]). Como princípio geral, o artigo 5.º, n.º 1, da referida lei exige que as autoridades públicas elaborem políticas para prevenir «o abuso e a utilização indevida de informações pessoais, a vigilância e a perseguição indiscriminada, etc. e para reforçar a dignidade dos seres humanos e a privacidade individual». Além disso, qualquer responsável pelo tratamento deve tratar os dados pessoais de forma a minimizar a possibilidade de violação da privacidade do titular dos dados (artigo 3.º, n.º 6, da Lei relativa à proteção de informações pessoais).

(148) Todos os requisitos da Lei relativa à proteção de informações pessoais, descritos em pormenor no ponto 2, são aplicáveis ao tratamento de dados pessoais para efeitos de aplicação da lei. Tal inclui os princípios fundamentais (como a licitude e a lealdade, a limitação das finalidades, a exatidão, a minimização dos dados, a limitação da conservação, a segurança e a transparência), as obrigações (por exemplo, no que respeita à notificação de violações de dados e aos dados sensíveis) e os direitos (de obter acesso, retificação, apagamento e suspensão).

(149) Embora o tratamento de dados pessoais para efeitos de segurança nacional esteja sujeito a um conjunto mais limitado de disposições ao abrigo da Lei relativa à proteção de informações pessoais, os princípios fundamentais, bem como as regras em matéria de supervisão, execução e recurso, são aplicáveis ([196]). Mais especificamente, os artigos 3.º e 4.º da referida lei estabelecem os princípios gerais de proteção de dados (licitude e lealdade, limitação das finalidades, exatidão, minimização dos dados, segurança e transparência) e os direitos individuais (o direito de ser informado, o direito de acesso e os direitos de retificação, apagamento e suspensão) ([197]). Além disso, o artigo 4.º, n.º 5, confere às pessoas o direito a uma reparação adequada por quaisquer danos resultantes do tratamento dos seus dados pessoais, através de um procedimento rápido e justo. Tal é complementado por obrigações mais específicas de apenas tratar dados pessoais na medida do mínimo necessário para atingir

([188]) Ver o anexo II, ponto 1.1.
([189]) Artigo 37.º, n.º 2, da Constituição.
([190]) Artigo 16.º e artigo 12.º, n.º 3, da Constituição. O artigo 12.º, n.º 3, da Constituição define ainda as circunstâncias excecionais em que podem ocorrer buscas ou apreensões sem mandado (embora continue a ser necessário um mandado *ex post*), ou seja, em flagrante delito ou, no caso de crimes puníveis com uma pena de prisão mínima de três anos, se existir o risco de destruição de provas ou de fuga do suspeito.
([191]) Artigo 68.º, n.º 1, da Lei relativa ao Tribunal Constitucional.
([192]) Artigo 29.º, n.º 1, da Constituição.
([193]) Artigo 199.º, n.º 1, da Lei relativa ao processo penal. De um modo mais geral, ao exercerem os seus poderes ao abrigo da Lei relativa ao processo penal, as autoridades públicas têm de respeitar os direitos fundamentais dos suspeitos de crimes e de qualquer outra pessoa em causa (artigo 198.º, n.º 2, da referida lei).
([194]) Artigo 14.º da Lei relativa ao Serviço Nacional de Informações.
([195]) Ver o anexo II, ponto 1.2.
([196]) Artigo 58.º, n.º 1, ponto 2, da Lei relativa à proteção de informações pessoais. Ver também o ponto 6 da Notificação n.º 2021-5 (anexo I). Esta isenção de determinadas disposições da Lei relativa à proteção de informações pessoais só se aplica quando os dados pessoais são tratados para fins de segurança nacional. Uma vez terminada a situação de segurança nacional que justifica o tratamento de dados, deixa de ser possível invocar a isenção, aplicando-se todos os requisitos da Lei relativa à proteção de informações pessoais.
([197]) Tais direitos só podem ser restringidos quando previsto por lei, na medida e durante o tempo necessário e proporcionado para proteger um objetivo de interesse público importante, ou quando a concessão do direito puder causar danos à vida ou integridade física de um terceiro, ou resultar numa infração injustificada da propriedade e de outros interesses de um terceiro. Ver o ponto 6 da Notificação n.º 2021-5.

o objetivo pretendido e durante um período mínimo, de estabelecer as medidas necessárias para garantir a segurança da gestão dos dados e um tratamento adequado (como garantias técnicas, de gestão e físicas), bem como de estabelecer medidas para o tratamento adequado de queixas individuais (reclamações) ([198]). Por último, os princípios gerais da legalidade, da necessidade e da proporcionalidade da Constituição coreana (ver considerando (145)) também se aplicam ao tratamento de dados pessoais para efeitos de segurança nacional.

(150) Estas limitações e garantias gerais podem ser invocadas pelas pessoas singulares junto de organismos de supervisão independentes (por exemplo, a Comissão de Proteção de Informações Pessoais e/ou a Comissão Nacional dos Direitos Humanos, ver os considerandos (177) e (178)) e dos tribunais (ver considerandos (179) a (183)) para obter reparação.

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

(151) O direito da República da Coreia impõe várias limitações ao acesso e à utilização de dados pessoais para efeitos de aplicação do direito penal, e prevê mecanismos de recurso e supervisão neste domínio, que estão em conformidade com os requisitos referidos nos considerandos (141) a (143) da presente decisão. Os pontos seguintes descrevem as condições nas quais esse acesso pode ser efetuado e as garantias aplicáveis à utilização desses poderes.

3.2.1 *Bases jurídicas, limitações e garantias*

(152) Os dados pessoais tratados pelos responsáveis pelo tratamento coreanos que seriam transferidos da União ao abrigo da presente decisão ([199]) podem ser recolhidos pelas autoridades coreanas para efeitos de aplicação do direito penal no contexto de uma busca ou apreensão (com base na Lei relativa ao processo penal), através do acesso a informações sobre comunicações (com base na Lei relativa à proteção da privacidade das comunicações), ou da obtenção de dados de assinantes por meio de pedidos de divulgação voluntária (com base na Lei relativa às atividades de telecomunicações) ([200]).

3.2.1.1 Buscas e apreensões

(153) A Lei relativa ao processo penal prevê que uma busca ou apreensão só pode ser realizada se uma pessoa for suspeita de um crime, se for necessária para a investigação e se se tiver estabelecido uma ligação entre a investigação e a pessoa a ser objeto da busca ou o artigo a inspecionar ou apreender ([201]). Além disso, uma busca ou apreensão (como qualquer medida obrigatória) só pode ser autorizada/executada na medida do necessário ([202]). Se uma busca disser respeito a um disco de um computador ou a outro suporte de armazenamento de dados, em princípio, só serão apreendidos os dados necessários (copiados ou impressos) e não todo o suporte ([203]). Este só poderá ser apreendido quando se considerar substancialmente impossível imprimir ou copiar separadamente os dados necessários, ou quando se considerar substancialmente impraticável alcançar a finalidade da busca de outra forma ([204]). Por conseguinte, a Lei relativa ao processo penal estabelece regras claras e precisas sobre o âmbito e a aplicação destas medidas, assegurando assim que a ingerência nos direitos das pessoas em caso de busca ou apreensão será limitada ao necessário para uma investigação criminal específica e proporcional ao objetivo prosseguido.

([198]) Artigo 58.º, n.º 4, da Lei relativa à proteção de informações pessoais.

([199]) Ver o anexo II, ponto 2.1. A declaração oficial do Governo coreano (anexo II, ponto 2.1) refere também a possibilidade de recolher informações sobre transações financeiras para efeitos de prevenção do branqueamento de capitais e do financiamento do terrorismo, com base na Lei relativa à comunicação e utilização de informações específicas sobre transações financeiras. No entanto, a referida lei apenas impõe obrigações de divulgação aos responsáveis pelo tratamento de informações pessoais de crédito nos termos da Lei relativa à utilização e proteção de informações de crédito e que estão sujeitos à supervisão da Comissão dos Serviços Financeiros (ver considerando (13)). Dado que o tratamento de informações pessoais de crédito por esses responsáveis pelo tratamento está excluído do âmbito de aplicação da presente decisão, a Lei relativa à comunicação e utilização de informações específicas sobre transações financeiras não é pertinente para a presente avaliação.

([200]) O artigo 3.º da Lei relativa à proteção da privacidade das comunicações também refere a Lei relativa ao Tribunal Militar como possível base jurídica para a recolha de dados de comunicações. No entanto, essa lei rege a recolha de informações sobre o pessoal militar e só pode ser aplicada a civis num número limitado de casos (por exemplo, se o pessoal militar e os civis cometerem um crime em conjunto, ou se uma pessoa cometer um crime contra as forças armadas, a ação pode ser intentada junto de um tribunal militar, ver o artigo 2.º da Lei relativa ao Tribunal Militar). Em qualquer caso, estabelece disposições gerais que regem as buscas e as apreensões semelhantes à Lei relativa ao processo penal (ver, por exemplo, os artigos 146.º a 149.º e 153.º a 156.º da Lei relativa ao Tribunal Militar) e que, por exemplo, preveem que o correio postal só pode ser recolhido quando necessário para uma investigação e com base num mandado do Tribunal Militar. Caso as comunicações eletrónicas fossem recolhidas com base nessa lei, aplicar-se-iam as limitações e garantias da Lei relativa à proteção da privacidade das comunicações. Ver o anexo II, ponto 2.2.2.1, e a nota de rodapé 50.

([201]) Artigo 215.º, n.ºs 1 e 2, da Lei relativa ao processo penal. Ver também o artigo 106.º, n.º 1, e os artigos 107.º e 109.º da referida lei, que preveem que os tribunais podem realizar buscas e apreensões desde que se considere que os artigos ou as pessoas em causa estão relacionados com um processo específico. Ver o anexo II, ponto 2.2.1.2.

([202]) Artigo 199.º, n.º 1, da Lei relativa ao processo penal.

([203]) Artigo 106.º, n.º 3, da Lei relativa ao processo penal.

([204]) Artigo 106.º, n.º 3, da Lei relativa ao processo penal.

(154) Em termos de garantias processuais, a Lei relativa ao processo penal exige a obtenção de um mandado de um tribunal para realizar uma busca ou apreensão ([205]). Só é permitido fazê-lo sem mandado a título excecional, nomeadamente em circunstâncias urgentes ([206]), *in loco* no momento da prisão ou da detenção de um suspeito de crime ([207]), ou quando um artigo é deitado fora ou voluntariamente produzido por um suspeito de crime ou terceiro (no que respeita aos dados pessoais, pela própria pessoa em causa) ([208]). As buscas e apreensões ilegais estão sujeitas a sanções penais ([209]) e quaisquer elementos de prova obtidos em violação da Lei relativa ao processo penal são considerados inadmissíveis ([210]). Por último, as pessoas em causa devem ser sempre notificadas de uma busca ou apreensão (nomeadamente da apreensão dos seus dados) sem demora ([211]), o que, por sua vez, facilitará o exercício dos seus direitos substantivos e do direito à reparação (ver, em especial, a possibilidade de contestar a execução de um mandado de apreensão, considerando (180)).

3.2.1.2 Acesso às informações sobre comunicações

(155) Com base na Lei relativa à proteção da privacidade das comunicações, as autoridades coreanas responsáveis pela aplicação do direito penal podem tomar dois tipos de medidas ([212]): por um lado, a recolha de «dados de confirmação das comunicações» ([213]), o que inclui a data das telecomunicações, a respetiva hora de início e de fim, o número de chamadas efetuadas e recebidas, bem como o número de assinante da outra parte, a frequência de utilização, os ficheiros de registo relativos à utilização dos serviços de telecomunicações e informações de localização (por exemplo, das torres de transmissão onde os sinais são recebidos); por outro lado, «medidas de restrição das comunicações», que abrangem a recolha do conteúdo do correio tradicional e a interceção direta do conteúdo das telecomunicações ([214]).

(156) O acesso aos dados de confirmação das comunicações só pode ser efetuado quando necessário para conduzir uma investigação criminal ou executar uma pena ([215]), com base num mandado emitido por um tribunal ([216]). A este respeito, a Lei relativa à proteção da privacidade das comunicações exige que sejam fornecidas informações pormenorizadas tanto no pedido do mandado (por exemplo, sobre as razões do pedido, a relação com o alvo/assinante e os dados necessários) como no próprio mandado (por exemplo, sobre o objetivo, o alvo e o âmbito da medida) ([217]). A recolha sem mandado só pode ser realizada quando motivos de urgência

([205]) Artigo 215.º, n.ºs 1 e 2, da Lei relativa ao processo penal, artigo 113.º da referida lei. Ao requerer um mandado, a autoridade em causa deve apresentar elementos que demonstrem os motivos para suspeitar que uma pessoa cometeu um crime, que a busca, inspeção ou apreensão são necessárias, e que os artigos pertinentes a apreender existem (artigo 108.º, n.º 1, do Regulamento de Processo Penal). O próprio mandado deve especificar, nomeadamente, os nomes do suspeito de crime e a infração, o local, a pessoa ou os artigos a sujeitar à busca, ou os artigos a apreender, a data de emissão e o período efetivo de aplicação (artigo 114.º, n.º 1, em conjugação com o artigo 219.º da Lei relativa ao processo penal). Ver o anexo II, ponto 2.2.1.2.

([206]) Ou seja, quando é impossível obter um mandado devido à urgência no local de uma infração (artigo 216.º, n.º 3, da Lei relativa ao processo penal), devendo, contudo, obter-se posteriormente um mandado o mais rápido possível (artigo 216.º, n.º 3, da referida lei).

([207]) Artigo 216.º, n.ºs 1 e 2, da Lei relativa ao processo penal.

([208]) Artigo 218.º da Lei relativa ao processo penal. Além disso, conforme explicado no anexo II, ponto 2.2.1.2, os artigos apresentados voluntariamente só são admitidos como elementos de prova em processos judiciais se não houver dúvidas razoáveis quanto à natureza voluntária da divulgação, facto que cabe ao procurador demonstrar.

([209]) Artigo 321.º do Código Penal.

([210]) Artigo 308.º-2 da Lei relativa ao processo penal. Além disso, a pessoa em causa (e o seu advogado) pode estar presente quando um mandado de busca ou apreensão é executado e, por conseguinte, pode também levantar uma objeção no momento da execução (artigos 121.º e 219.º da Lei relativa ao processo penal).

([211]) Artigos 121.º e 122.º da Lei relativa ao processo penal (no que respeita às buscas) e artigo 219.º, em conjugação com o artigo 106.º, n.º 4, da referida lei (no que respeita às apreensões).

([212]) Ver também o anexo II, ponto 2.2.2.1. Tais medidas podem ser tomadas com a assistência forçada dos operadores de telecomunicações, mediante a apresentação de uma autorização por escrito obtida de um tribunal (artigo 9.º, n.º 2, da Lei relativa à proteção da privacidade das comunicações), que deve ser conservada pelos operadores (artigo 15.º-2 da Lei relativa à proteção da privacidade das comunicações e artigo 12.º do respetivo decreto de execução). Os fornecedores de telecomunicações podem recusar cooperar quando as informações sobre a pessoa visada, conforme indicadas na autorização escrita do tribunal (por exemplo, o número de telefone da pessoa) estiverem incorretas, e estão proibidos, em qualquer circunstância, de divulgar as palavras-passe utilizadas nas telecomunicações (artigo 9.º, n.º 4, da Lei relativa à proteção da privacidade das comunicações).

([213]) Artigo 2.º, n.º 11, da Lei relativa à proteção da privacidade das comunicações.

([214]) Ver o artigo 2.º, n.º 6, da Lei relativa à proteção da privacidade das comunicações, que se refere à «censura» (abertura de correio sem o consentimento da parte interessada ou aquisição de conhecimento sobre o respetivo conteúdo, bem como o registo ou a retenção do mesmo por outros meios), e o artigo 2.º, n.º 7, da referida lei, que se refere às «escutas telefónicas» (aquisição ou gravação do conteúdo de telecomunicações através da escuta ou da leitura coletiva dos sons, das palavras, dos símbolos ou das imagens das comunicações através de dispositivos eletrónicos e mecânicos, sem o consentimento da parte interessada ou interferência na sua transmissão e receção).

([215]) Artigo 13.º, n.º 1, da Lei relativa à proteção da privacidade das comunicações. Ver também o anexo II, ponto 2.2.2.3. Além disso, os dados de localização em tempo real e os dados de confirmação das comunicações relativos a uma estação de base específica só podem ser recolhidos para a investigação de crimes graves ou se, de outra forma, for difícil impedir a prática de um crime ou recolher elementos de prova (artigo 13.º, n.º 2, da Lei relativa à proteção da privacidade das comunicações). Tal reflete a necessidade de prever garantias adicionais em caso de medidas particularmente intrusivas na privacidade, em consonância com o princípio da proporcionalidade.

([216]) Artigos 13.º e 6.º da Lei relativa à proteção da privacidade das comunicações.

([217]) Ver o artigo 13.º, n.ºs 3 e 9, em conjugação com o artigo 6.º, n.ºs 4 e 6, da Lei relativa à proteção da privacidade das comunicações.

impossibilitem a obtenção da autorização judicial, caso em que o mandado deve ser obtido e comunicado ao fornecedor de telecomunicações imediatamente após o pedido dos dados ([218]). Se o tribunal recusar a autorização posterior, as informações recolhidas devem ser destruídas ([219]).

(157) Em termos de garantias adicionais no que respeita à recolha de dados de confirmação das comunicações, a Lei relativa à proteção da privacidade das comunicações impõe requisitos específicos em matéria de conservação de registos e de transparência ([220]). Mais especificamente, tanto as autoridades responsáveis pela aplicação do direito penal ([221]) como os fornecedores de telecomunicações ([222]) têm de conservar registos dos pedidos e das divulgações efetuadas. Além disso, em princípio, as autoridades responsáveis pela aplicação do direito penal têm de notificar as pessoas de que os seus dados de confirmação das comunicações foram recolhidos ([223]). Tal notificação só pode ser diferida em circunstâncias excecionais, com base numa autorização do diretor de uma procuradoria distrital competente ([224]). Essa autorização só pode ser concedida quando a notificação for suscetível de 1) pôr em perigo a segurança nacional, a segurança e a ordem públicas, 2) causar a morte ou lesões corporais, 3) impedir um processo judicial justo (por exemplo, levando à destruição de elementos de prova ou ameaçando testemunhas), ou 4) difamar o suspeito, as vítimas ou outras pessoas relacionadas com o processo, ou invadir a sua privacidade. Nesses casos, a notificação tem de ser feita no prazo de 30 dias após a cessação do(s) motivo(s) do diferimento ([225]). Após a notificação, as pessoas singulares têm o direito de obter informações sobre os motivos da recolha dos seus dados ([226]).

(158) No que respeita às medidas de restrição das comunicações, aplicam-se regras mais rigorosas, só podendo ser utilizadas quando houver motivos substanciais para suspeitar que certos crimes graves especificamente enumerados na Lei relativa à proteção da privacidade das comunicações estão a ser planeados ou estão a ser ou foram cometidos ([227]). Além disso, as medidas de restrição das comunicações só podem ser tomadas como medida de último recurso e nos casos em que, de outro modo, seja difícil impedir a prática de um crime, prender um criminoso ou recolher provas ([228]). Devem ser imediatamente interrompidas assim que deixem de ser necessárias, a fim de garantir que a violação da privacidade das comunicações seja o mais limitada possível ([229]). As informações obtidas ilegalmente através de medidas de restrições das comunicações não são admitidas como elementos de prova em processos judiciais ou disciplinares ([230]).

(159) Em termos de garantias processuais, a Lei relativa à proteção da privacidade das comunicações exige a obtenção de um mandado judicial para a execução de medidas de restrição das comunicações ([231]). Mais uma vez, a referida lei exige que o pedido de mandado e o próprio mandado contenham informações pormenorizadas ([232]), nomeadamente sobre a justificação do pedido, bem como as comunicações a obter (que devem ser as do suspeito sob investigação) ([233]). Tais medidas só podem ser tomadas sem um mandado em caso de uma ameaça iminente de criminalidade organizada ou de iminência de outro crime grave suscetível de causar diretamente a morte ou ferimentos graves, e se existir uma situação de emergência que impossibilite o seguimento do procedimento

([218]) Artigo 13.º, n.º 2, da Lei relativa à proteção da privacidade das comunicações.
([219]) Artigo 13.º, n.º 3, da Lei relativa à proteção da privacidade das comunicações.
([220]) Ver o anexo II, ponto 2.2.2.3.
([221]) Artigo 13.º, n.ºs 5 e 6, da Lei relativa à proteção da privacidade das comunicações.
([222]) Artigo 13.º, n.º 7, da Lei relativa à proteção da privacidade das comunicações. Além disso, os fornecedores de telecomunicações têm de comunicar, duas vezes por ano, a divulgação de dados de confirmação das comunicações ao Ministério da Ciência e das TIC.
([223]) Ver o artigo 13.º-3, n.º 7, em conjugação com o artigo 9.º-2 da Lei relativa à proteção da privacidade das comunicações. Mais especificamente, as pessoas têm de ser notificadas no prazo de 30 dias a contar da decisão de (não) deduzir acusação, ou no prazo de 30 dias após um ano depois de ter sido tomada uma decisão de suspensão da acusação (embora, em qualquer caso, a notificação deva ser enviada no prazo de 30 dias após um ano depois da recolha das informações), ver o artigo 13.º-3, n.º 1, da Lei relativa à proteção da privacidade das comunicações.
([224]) Artigo 13.º-3, n.os 2 e 3, da Lei relativa à proteção da privacidade das comunicações.
([225]) Artigo 13.º-3, n.º 4, da Lei relativa à proteção da privacidade das comunicações.
([226]) Artigo 13.º-3, n.º 5, da Lei relativa à proteção da privacidade das comunicações. A pedido da pessoa, o procurador ou o agente da polícia judiciária têm de apresentar os motivos, por escrito, no prazo de 30 dias a contar da receção do pedido, a menos que se aplique uma das exceções para o diferimento da notificação (artigo 13.º-3, n.º 6, da Lei relativa à proteção da privacidade das comunicações).
([227]) Por exemplo, insurreição, crimes relacionados com a droga, crimes que envolvam explosivos, bem como crimes relacionados com a segurança nacional, relações diplomáticas ou bases e instalações militares, ver o artigo 5.º, n.º 1, da Lei relativa à proteção da privacidade das comunicações. Ver também o anexo II, ponto 2.2.2.2.
([228]) Artigo 3.º, n.º 2, e artigo 5.º, n.º 1, da Lei relativa à proteção da privacidade das comunicações.
([229]) Artigo 2.º do Decreto de Execução da Lei relativa à proteção da privacidade das comunicações.
([230]) Artigo 4.º da Lei relativa à proteção da privacidade das comunicações.
([231]) Artigo 6.º, n.ºs 1, 2, 5 e 6, da Lei relativa à proteção da privacidade das comunicações.
([232]) O pedido de mandado tem de descrever 1) as razões substanciais para suspeitar (*prima facie*) que um dos crimes enumerados está planeado, está a ser ou foi cometido, bem como qualquer material de apoio; 2) as medidas de restrição das comunicações, bem como o seu alvo, âmbito, objetivo e período efetivo; e 3) o local onde as medidas seriam executadas e a forma como seriam levadas a cabo (artigo 6.º, n.º 4, da Lei relativa à proteção da privacidade das comunicações e artigo 4.º, n.º 1, do respetivo decreto de execução). O próprio mandado tem de especificar as medidas, bem como o seu alvo, âmbito, período efetivo, local de execução e a forma como devem ser executadas (artigo 6.º, n.º 6, da Lei relativa à proteção da privacidade das comunicações).
([233]) O alvo de uma medida de restrição das comunicações deve consistir em envios postais ou telecomunicações específicos enviados ou recebidos pelo suspeito, ou envios postais ou telecomunicações enviados ou recebidos pelo suspeito durante um período de tempo determinado (artigo 5.º, n.º 2, da Lei relativa à proteção da privacidade das comunicações).

regular ([234]). No entanto, nesse caso, o pedido de mandado tem de ser apresentado imediatamente após a adoção da medida ([235]). As medidas de restrição das comunicações só podem ser executadas por um período máximo de dois meses ([236]) e só podem ser prorrogadas com a aprovação do tribunal se as condições para a sua execução se mantiverem ([237]). O período prorrogado não pode exceder um ano no total, ou três anos no caso de determinados crimes particularmente graves (como crimes relacionados com a insurreição, agressão estrangeira, segurança nacional) ([238]).

(160) Tal como no que respeita à recolha de dados de confirmação das comunicações, a Lei relativa à proteção da privacidade das comunicações exige que os fornecedores de telecomunicações ([239]) e as autoridades responsáveis pela aplicação da lei ([240]) mantenham registos da execução das medidas de restrição das comunicações, e prevê a notificação da pessoa em causa, que pode, excecionalmente, ser diferida, se necessário, por razões importantes de interesse público ([241]).

(161) Por último, o incumprimento de várias limitações e garantias da Lei relativa à proteção da privacidade das comunicações (nomeadamente das obrigações de obtenção de um mandado, de conservação de registos e de notificação da pessoa), no que respeita à recolha de dados de confirmação das comunicações e à utilização de medidas de restrição das comunicações, está sujeito a sanções penais ([242]).

(162) Por conseguinte, os poderes das autoridades responsáveis pela aplicação do direito penal para recolher dados de comunicações com base na Lei relativa à proteção da privacidade das comunicações (tanto o conteúdo das comunicações como os dados de confirmação das comunicações) estão circunscritos por regras claras e precisas e sujeitos a várias garantias. Estas garantem, designadamente, a supervisão da execução dessas medidas, *ex ante* (mediante aprovação judicial prévia) e *ex post* (através de requisitos de conservação de registos e de apresentação de relatórios), e facilitam o acesso das pessoas singulares a vias de recurso eficazes (assegurando que são informadas da recolha dos seus dados).

3.2.1.3 Pedidos de divulgação voluntária de dados de assinantes

(163) Além de recorrerem às medidas obrigatórias descritas nos considerandos (153) a (162), as autoridades coreanas responsáveis pela aplicação da lei podem solicitar aos fornecedores de telecomunicações «dados de comunicações» a título voluntário, em apoio de um processo penal, de uma investigação ou da execução de uma pena (artigo 83.º, n.º 3, da Lei relativa às atividades de telecomunicações). Esta possibilidade só existe em relação a conjuntos de dados limitados, ou seja, o nome, número de registo de residente, endereço e número de telefone dos utilizadores, as datas em que os utilizadores subscrevem ou cancelam a sua subscrição, bem como os códigos de identificação dos utilizadores (ou seja, códigos utilizados para identificar o utilizador legítimo dos sistemas informáticos ou das redes de comunicações) ([243]). Uma vez que apenas as pessoas singulares que contratam diretamente os serviços de um fornecedor de telecomunicações coreano são consideradas «utilizadores» ([244]), as pessoas singulares da UE cujos dados tenham sido transferidos para a República da Coreia não estão normalmente abrangidas por esta categoria ([245]).

(164) As divulgações voluntárias estão sujeitas a diferentes limitações, tanto no que respeita ao exercício de poderes por parte da autoridade de aplicação da lei como à resposta do operador de telecomunicações. Como requisito geral, as autoridades responsáveis pela aplicação da lei devem agir de acordo com os princípios constitucionais da necessidade e da proporcionalidade (artigo 12.º, n.º 1, e artigo 37.º, n.º 2, da Constituição), incluindo quando

([234]) Artigo 8.º, n.º 1, da Lei relativa à proteção da privacidade das comunicações. No entanto, a recolha de informações em situações de emergência deve ser sempre efetuada em conformidade com uma «declaração de censura/escutas telefónicas de emergência», e a autoridade responsável pela recolha deve manter um registo de todas as medidas de emergência (artigo 8.º, n.º 4, da Lei relativa à proteção da privacidade das comunicações).

([235]) A recolha deve ser imediatamente interrompida se o serviço responsável pela aplicação da lei não obtiver autorização judicial no prazo de 36 horas (artigo 8.º, n.º 2, da Lei relativa à proteção da privacidade das comunicações), caso em que, conforme explicado no anexo II, ponto 2.2.2.2, as informações recolhidas serão, em princípio, destruídas. O tribunal também tem de ser notificado caso as medidas de emergência tenham sido concluídas num espaço de tempo tão curto que evite a necessidade de autorização (por exemplo, se o suspeito for detido imediatamente após o início da interceção, ver o artigo 8.º, n.º 5, da Lei relativa à proteção da privacidade das comunicações). Nesse caso, é necessário fornecer ao tribunal informações sobre o objetivo, alvo, âmbito, período, local de execução e método de recolha, bem como os fundamentos para não apresentar um pedido de autorização judicial (artigo 8.º, n.ºs 6 e 7, da Lei relativa à proteção da privacidade das comunicações).

([236]) Artigo 6.º, n.º 7, da Lei relativa à proteção da privacidade das comunicações. Se o objetivo das medidas for atingido mais cedo durante esse período, as medidas devem ser imediatamente interrompidas.

([237]) Artigo 6.º, n.ºs 7 e 8, da Lei relativa à proteção da privacidade das comunicações.

([238]) Artigo 6.º, n.º 8, da Lei relativa à proteção da privacidade das comunicações.

([239]) Artigo 9.º, n.º 3, da Lei relativa à proteção da privacidade das comunicações.

([240]) Artigo 18.º, n.º 1, do Decreto de Execução da Lei relativa à proteção da privacidade das comunicações.

([241]) Mais especificamente, o procurador tem de notificar a pessoa em causa no prazo de 30 dias a contar do despacho de uma acusação ou de uma disposição de não acusação ou detenção (artigo 9.º-2, n.º 1, da Lei relativa à proteção da privacidade das comunicações). A notificação pode ser diferida com a aprovação do diretor de uma procuradoria distrital se for suscetível de pôr seriamente em perigo a segurança nacional ou de perturbar a ordem e a segurança públicas, ou quando for suscetível de causar danos materiais à vida e à integridade física de terceiros (artigo 9.º-2, n.ºs 4 a 6, da Lei relativa à proteção da privacidade das comunicações).

([242]) Artigos 16.º e 17.º da Lei relativa à proteção da privacidade das comunicações.

([243]) Artigo 83.º, n.º 3, da Lei relativa às atividades de telecomunicações. Ver também o anexo II, ponto 2.2.3.

([244]) Artigo 2.º, n.º 9, da Lei relativa às atividades de telecomunicações.

([245]) Ver também o anexo II, ponto 2.2.3.

solicitam informações a título voluntário. Além disso, têm de cumprir a Lei relativa à proteção de informações pessoais, nomeadamente recolhendo apenas os dados pessoais mínimos necessários para alcançar um objetivo legítimo, de forma a minimizar o impacto na privacidade das pessoas (como o artigo 3.º, n.os 1 e 6, da Lei relativa à proteção de informações pessoais). Mais especificamente, os pedidos de obtenção de dados de comunicações com base na Lei relativa às atividades de telecomunicações devem ser efetuados por escrito e indicar as razões do pedido, a ligação ao utilizador em causa e o âmbito dos dados solicitados ([246]).

(165) Os fornecedores de telecomunicações não são obrigados a satisfazer esses pedidos e só o podem fazer em conformidade com a Lei relativa à proteção de informações pessoais. Tal significa, nomeadamente, que devem ponderar os diferentes interesses em jogo e que não podem fornecer os dados se tal for suscetível de violar injustamente os interesses da pessoa ou de um terceiro ([247]). Seria o caso, por exemplo, se fosse evidente que a autoridade requerente abusou da sua autoridade ([248]). Os operadores de telecomunicações devem manter registos das divulgações de informações ao abrigo da Lei relativa às atividades de telecomunicações e apresentar relatórios duas vezes por ano ao Ministério da Ciência e das TIC ([249]).

(166) Além disso, em conformidade com o ponto 3 da Notificação n.º 2021-5 (anexo I), os fornecedores de telecomunicações devem, em princípio, notificar a pessoa em causa quando responderem voluntariamente a um pedido ([250]). Tal permitirá, por sua vez, que a pessoa exerça os seus direitos e, caso os seus dados sejam divulgados ilegalmente, que obtenha reparação contra o responsável pelo tratamento (por exemplo, por divulgar os dados em violação da Lei relativa à proteção de informações pessoais ou por responder a um pedido claramente desproporcionado) ou contra a autoridade responsável pela aplicação da lei (por exemplo, por atuar para além dos limites do que é necessário e proporcionado ou por não respeitar os requisitos processuais da Lei relativa às atividades de telecomunicações).

3.2.2 *Utilização adicional das informações recolhidas*

(167) O tratamento de dados pessoais recolhidos pelas autoridades coreanas responsáveis pela aplicação do direito penal está sujeito a todos os requisitos da Lei relativa à proteção de informações pessoais, incluindo no que respeita à limitação das finalidades (artigo 3.º, n.os 1 e 2), à licitude da utilização e ao fornecimento a terceiros (artigos 15.º, 17.º e 18.º), às transferências internacionais (artigos 17.º e 18.º, conjugados com o disposto na secção 2 da Notificação n.º 2021-5) ([251]), à proporcionalidade/minimização dos dados (artigo 3.º, n.os 1 e 6) e à limitação da conservação (artigo 21.º) ([252]).

(168) No que respeita ao conteúdo das comunicações obtido através da execução de medidas de restrição das comunicações, a Lei relativa à proteção da privacidade das comunicações limita especificamente a sua possível utilização à investigação, repressão ou prevenção de crimes graves ([253]); a processos disciplinares pelos mesmos crimes; pedidos de indemnização apresentados por uma parte nas comunicações ou quando tal seja expressamente permitido por outras leis ([254]). Além disso, os conteúdos recolhidos das telecomunicações transmitidas através da Internet só podem ser conservados com a aprovação do tribunal que autorizou as medidas de restrição das comunicações ([255]), tendo em vista a sua utilização na investigação, repressão ou prevenção de crimes graves ([256]). De um modo mais geral, a Lei relativa à proteção da privacidade das comunicações proíbe a divulgação de informações confidenciais obtidas através de medidas de restrição das comunicações e a utilização dessas informações para prejudicar a reputação das pessoas sujeitas às medidas ([257]).

3.2.3 *Supervisão*

(169) Na Coreia, as atividades das autoridades responsáveis pela aplicação do direito penal são supervisionadas por diferentes organismos ([258]).

([246]) Artigo 83.º, n.º 4, da Lei relativa às atividades de telecomunicações. Em caso de impossibilidade de apresentar um pedido por escrito devido a uma urgência, o pedido escrito deve ser apresentado logo que o motivo da urgência deixe de existir (artigo 83.º, n.º 4, da Lei relativa às atividades de telecomunicações).

([247]) Artigo 18.º, n.º 2, da Lei relativa à proteção de informações pessoais.

([248]) Decisão n.º 2012Da105482 do Supremo Tribunal, de 10 de março de 2016. Ver também o anexo II, ponto 2.2.3, sobre esta decisão do Supremo Tribunal.

([249]) Artigo 83.º, n.os 5 e 6, da Lei relativa às atividades de telecomunicações.

([250]) Este requisito está sujeito a exceções limitadas e qualificadas, em especial se e na medida em que a notificação possa comprometer uma investigação criminal em curso, ou seja, suscetível de prejudicar a vida ou a integridade física de outra pessoa, sempre que esses direitos ou interesses sejam manifestamente superiores aos direitos do titular dos dados. Ver o ponto 3, alínea iii), ponto 1, da notificação.

([251]) Em especial, as autoridades públicas coreanas são obrigadas a assegurar, através de um instrumento juridicamente vinculativo, um nível de proteção equivalente ao da Lei relativa à proteção de informações pessoais (ver também considerando (90)).

([252]) Ver o anexo II, ponto 1.2.

([253]) Ver o considerando (158).

([254]) Artigo 12.º da Lei relativa à proteção da privacidade das comunicações. Ver o anexo II, ponto 2.2.2.2.

([255]) O procurador ou o agente de polícia que executa as medidas de restrição das comunicações tem de selecionar as telecomunicações a conservar no prazo de 14 dias após o termo das medidas e solicitar a aprovação do tribunal (no caso de uma proposta da polícia, o pedido deve ser apresentado a um procurador que, por sua vez, o apresenta ao tribunal), ver o artigo 12.º-2, n.os 1 e 2, da Lei relativa à proteção da privacidade das comunicações.

([256]) O pedido de autorização tem de conter informações sobre as medidas de restrição das comunicações, um resumo dos resultados das medidas, os motivos para a conservação (juntamente com os materiais de apoio) e as telecomunicações a conservar (artigo 12.º-2, n.º 3, da Lei relativa à proteção da privacidade das comunicações). Se não for apresentado qualquer pedido, os dados obtidos devem ser apagados no prazo de 14 dias após o termo da medida de restrição das comunicações (artigo 12.º-2, n.º 5, da Lei relativa à proteção da privacidade das comunicações) e, se o pedido for rejeitado, no prazo de sete dias (artigo 12.º-2, n.º 5, da referida lei). Em ambos os casos, no prazo de sete dias, deve apresentar-se um relatório sobre o apagamento ao tribunal que autorizou a recolha.

([257]) Artigo 11.º, n.º 2, do Decreto de Execução da Lei relativa à proteção da privacidade das comunicações.

([258]) Ver o anexo II, ponto 2.3.

(170) Em primeiro lugar, a polícia está sujeita a uma supervisão interna efetuada por um Inspetor-Geral ([259]), que realiza o controlo da legalidade, nomeadamente no que respeita a eventuais violações dos direitos humanos. O Inspetor-Geral foi criado para aplicar a Lei relativa às auditorias do setor público, que incentiva a criação de organismos de auditoria interna e estabelece requisitos específicos para a sua composição e funções. Mais especificamente, a lei exige que o diretor de um organismo de auditoria interna seja nomeado externamente à autoridade em causa (por exemplo, antigos juízes, professores) por um período de dois a cinco anos ([260]), que só possa ser destituído por motivos justificados (por exemplo, quando incapaz de desempenhar funções por motivos de saúde ou quando sujeito a medidas disciplinares) ([261]), e que lhe seja garantida a maior independência possível ([262]). A obstrução de uma auditoria interna está sujeita a coimas ([263]). Os relatórios de auditoria (que podem incluir recomendações, pedidos de medidas disciplinares e pedidos de compensação ou correção) são comunicados ao diretor da autoridade pública em causa, à Comissão de Auditoria e Inspeção ([264]) e, de um modo geral, são tornados públicos ([265]). Os resultados da aplicação do relatório devem também ser comunicados à Comissão de Auditoria e Inspeção ([266]) (ver considerando (173) sobre os seus poderes, incluindo o de supervisão).

(171) Em segundo lugar, a Comissão de Proteção de Informações Pessoais supervisiona a conformidade do tratamento de dados por parte das autoridades responsáveis pela aplicação do direito penal com a Lei relativa à proteção de informações pessoais e com outras leis que protegem a privacidade das pessoas singulares, nomeadamente as que regulam a recolha de provas (eletrónicas) para efeitos de aplicação do direito penal, conforme descrito no ponto 3.2.1 ([267]). Mais especificamente, uma vez que esta supervisão abrange a licitude e a lealdade da recolha e do tratamento de dados (artigo 3.º, n.º 1, da Lei relativa à proteção de informações pessoais), que serão infringidas caso o acesso e a utilização dos dados pessoais violem essas leis ([268]), a Comissão de Proteção de Informações Pessoais também pode investigar e fazer cumprir as limitações e garantias descritas no ponto 3.2.1 ([269]). No exercício desta função de supervisão, a Comissão de Proteção de Informações Pessoais pode fazer uso de todos os seus poderes de investigação e reparação, conforme descrito em pormenor no ponto 2.4.2. Já antes da recente reforma da Lei relativa à proteção de informações pessoais (ou seja, no seu anterior papel de supervisão do setor público), a Comissão de Proteção de Informações Pessoais levou a cabo várias atividades de supervisão ao tratamento de dados pessoais por parte das autoridades responsáveis pela aplicação do direito penal, por exemplo, no contexto do interrogatório de suspeitos (processo n.º 2013-16, de 26 de agosto de 2013), no que respeita ao envio de notificações às pessoas singulares sobre a imposição de coimas (processo n.º 2015-02-04, de 26 de janeiro de 2015), à partilha de dados com outras autoridades (processo n.º 2018-15-146, de 9 de julho de 2018, processo n.º 2018-25-308, de 10 de dezembro de 2018, processo n.º 2019-02-015, de 29 de janeiro de 2019), à recolha de impressões digitais ou fotografias (processo n.º 2019-17-273, de 9 de setembro de 2019), e à utilização de *drones* (processo n.º 2020-01-004, de 13 de janeiro de 2020). Nesses processos, a Comissão de Proteção de Informações Pessoais investigou o cumprimento de várias disposições da Lei relativa à proteção de informações pessoais (por exemplo, a licitude do tratamento, os princípios da limitação das finalidades e da minimização dos dados), mas também de outras disposições pertinentes de outras leis, como a Lei relativa ao processo penal, e, se necessário, emitiu recomendações para tornar o tratamento conforme com os requisitos em matéria de proteção de dados.

(172) Em terceiro lugar, a supervisão independente é assegurada pela Comissão Nacional dos Direitos Humanos ([270]), que pode investigar violações dos direitos à privacidade e à privacidade da correspondência no âmbito do seu mandato geral de proteção dos direitos fundamentais dos artigos 10.º a 22.º da Constituição. A Comissão Nacional dos Direitos Humanos é composta por 11 comissários, que têm de reunir requisitos específicos ([271]), e que são designados pelo presidente da República em conformidade com os procedimentos estabelecidos por lei. Mais especificamente, quatro comissários são designados por nomeação da Assembleia Nacional, quatro por nomeação do presidente da República e três por nomeação do juiz presidente do Supremo Tribunal ([272]). O presidente da Comissão é nomeado pelo presidente da República de entre os comissários e tem de ser confirmado pela Assembleia Nacional ([273]). Os comissários (incluindo o presidente) são nomeados por um período renovável

([259]) Ver o anexo II, ponto 2.3.1. Ver também https://www.police.go.kr/eng/knpa/org/org01.jsp.
([260]) Da mesma forma, os auditores são nomeados com base em condições específicas estabelecidas na lei, ver os artigos 16.º e seguintes da Lei relativa às auditorias do setor público.
([261]) Artigos 8.º a 11.º da Lei relativa às auditorias do setor público.
([262]) Artigo 7.º da Lei relativa às auditorias do setor público.
([263]) Artigo 41.º da Lei relativa às auditorias do setor público.
([264]) Artigo 23.º, n.º 1, da Lei relativa às auditorias do setor público.
([265]) Artigo 26.º da Lei relativa às auditorias do setor público.
([266]) Artigo 23.º, n.º 3, da Lei relativa às auditorias do setor público.
([267]) Ver o artigo 7.º-8, n.ºs 3 e 4, e o artigo 7.º-9, n.º 5, da Lei relativa à proteção de informações pessoais.
([268]) Ver o ponto 6 (anexo I) da Notificação n.º 2021-5 da Comissão de Proteção de Informações Pessoais.
([269]) Ver também o anexo II, ponto 2.3.4.
([270]) Artigo 1.º da Lei relativa à Comissão Nacional dos Direitos Humanos.
([271]) Para ser nomeado, um comissário deve 1) ter exercido funções, no mínimo durante dez anos, numa universidade ou num instituto de investigação autorizado, pelo menos como professor associado; 2) ter exercido as funções de juiz, procurador ou advogado durante, pelo menos, dez anos; 3) ter estado envolvido em atividades relacionadas com os direitos humanos durante, pelo menos, dez anos (por exemplo, numa organização não governamental ou internacional sem fins lucrativos); ou 4) ter sido recomendado por grupos da sociedade civil (artigo 5.º, n.º 3, da Lei relativa à Comissão Nacional dos Direitos Humanos). Além disso, uma vez nomeados, os comissários estão proibidos de exercer um mandato simultâneo na Assembleia Nacional, nos conselhos locais ou em qualquer governo estatal ou local (na qualidade de funcionários públicos), ver o artigo 10.º da Lei relativa à Comissão Nacional dos Direitos Humanos.
([272]) Artigo 5.º, n.ºs 1 e 2, da Lei relativa à Comissão Nacional dos Direitos Humanos.
([273]) Artigo 5.º, n.º 5, da Lei relativa à Comissão Nacional dos Direitos Humanos.

de três anos e só podem ser destituídos se forem condenados a penas de prisão ou já não conseguirem desempenhar as suas funções devido a deficiências físicas ou mentais crónicas (caso em que dois terços dos comissários têm de concordar com a destituição) ([274]). No âmbito de uma investigação, a Comissão Nacional dos Direitos Humanos pode solicitar a apresentação de materiais pertinentes, realizar inspeções e convocar pessoas para testemunhar ([275]). Em termos de poderes de reparação, pode emitir recomendações (públicas) para melhorar ou corrigir políticas e práticas específicas, às quais as autoridades públicas devem responder com uma proposta de plano de execução ([276]). Se a autoridade em causa não aplicar as recomendações, deve informar a Comissão desse facto ([277]), que pode, por sua vez, comunicar essa omissão à Assembleia Nacional e/ou torná-la pública. De acordo com a declaração oficial do Governo coreano (anexo II, ponto 2.3.5), de um modo geral, as autoridades coreanas cumprem as recomendações da Comissão Nacional dos Direitos Humanos e têm um forte incentivo para o fazer, uma vez que esse cumprimento tem sido avaliado no âmbito de uma avaliação geral contínua sob a autoridade do gabinete do primeiro-ministro. Os dados anuais relativos às suas atividades mostram que a Comissão Nacional dos Direitos Humanos supervisiona ativamente as atividades das autoridades responsáveis pela aplicação do direito penal, com base em petições individuais ou através de investigações *ex officio* ([278]).

(173) Em quarto lugar, a supervisão geral da legalidade das atividades das autoridades públicas é efetuada pela Comissão de Auditoria e Inspeção, que analisa as receitas e as despesas do Estado, mas também, de um modo mais geral, supervisiona o cumprimento das obrigações das autoridades públicas com vista a melhorar o funcionamento da administração pública ([279]). A Comissão de Auditoria e Inspeção é formalmente criada sob a égide do presidente da República da Coreia, mas mantém um estatuto independente no que respeita às suas funções ([280]). Além disso, é-lhe concedida total independência no que respeita à nomeação, destituição e organização do seu pessoal, bem como à elaboração do seu orçamento ([281]). A Comissão de Auditoria e Inspeção é composta por um presidente (nomeado pelo presidente da República, com o consentimento da Assembleia Nacional) ([282]) e por seis comissários (nomeados pelo presidente da República mediante recomendação do seu próprio presidente) ([283]), que devem reunir os requisitos específicos previstos na lei ([284]) e que só podem ser destituídos em caso de impugnação, condenação a prisão ou incapacidade para desempenhar as suas funções devido a deficiências mentais ou físicas crónicas ([285]). A Comissão de Auditoria e Inspeção realiza uma auditoria geral anualmente, mas também pode realizar auditorias específicas sobre questões de especial interesse. Na realização de uma auditoria ou inspeção, pode solicitar a apresentação de documentos e solicitar a presença de pessoas ([286]). A Comissão de Auditoria e Inspeção pode emitir recomendações, solicitar medidas disciplinares ou apresentar uma queixa-crime ([287]).

(174) Por último, a Assembleia Nacional efetua o controlo parlamentar das autoridades públicas através de investigações e inspeções ([288]) das suas atividades ([289]). Pode solicitar a divulgação de documentos, obrigar à comparência de testemunhas ([290]), recomendar medidas corretivas (se concluir que ocorreram atividades ilícitas ou

([274]) Artigo 7.º, n.º 1, e artigo 8.º da Lei relativa à Comissão Nacional dos Direitos Humanos.

([275]) Artigo 36.º da Lei relativa à Comissão Nacional dos Direitos Humanos. Nos termos do artigo 6.º, n.º 7, da referida lei, a apresentação de materiais ou artigos pode ser rejeitada se prejudicar a confidencialidade do Estado suscetível de afetar substancialmente a segurança do Estado ou as relações diplomáticas ou constituir um sério obstáculo a uma investigação criminal ou a um julgamento pendente. Nesses casos, se necessário para permitir verificar se a recusa em fornecer as informações é justificada, a Comissão pode solicitar informações adicionais ao diretor do serviço em causa (que tem de cumprir esse requisito de boa-fé).

([276]) Artigo 25.º, n.ºs 1 e 3, da Lei relativa à Comissão Nacional dos Direitos Humanos.

([277]) Artigo 25.º, n.º 4, da Lei relativa à Comissão Nacional dos Direitos Humanos.

([278]) Por exemplo, entre 2015 e 2019, a Comissão Nacional dos Direitos Humanos recebeu anualmente entre 1 380 e 1 699 petições contra as autoridades responsáveis pela aplicação do direito penal e tratou um número igualmente elevado (por exemplo, tratou 1 546 reclamações contra a polícia em 2018 e 1 249 em 2019); também realizou várias investigações *ex officio*, conforme descrito mais pormenorizadamente no relatório anual de 2018 da Comissão Nacional dos Direitos Humanos (disponível em https://www.humanrights.go.kr/site/program/board/basicboard/view?menuid=002003003001&pagesize=10&boardtypeid=7017&boardid=7602641) e no relatório anual de 2019 (disponível em https://www.humanrights.go.kr/site/program/board/basicboard/view?menuid=002003003001&pagesize=10&boardtypeid=7017&boardid=7606217).

([279]) Artigos 20.º e 24.º da Lei relativa à Comissão de Auditoria e Inspeção. Ver o anexo II, ponto 2.3.2.

([280]) Artigo 2.º, n.º 1, da Lei relativa à Comissão de Auditoria e Inspeção.

([281]) Artigo 2.º, n.º 2, da Lei relativa à Comissão de Auditoria e Inspeção.

([282]) Artigo 4.º, n.º 1, da Lei relativa à Comissão de Auditoria e Inspeção.

([283]) Artigo 5.º, n.º 1, e artigo 6.º da Lei relativa à Comissão de Auditoria e Inspeção.

([284]) Por exemplo, terem exercido funções como juízes, procuradores públicos ou advogados durante, pelo menos, dez anos, terem trabalhado no funcionalismo público ou sido professores ou ocupado uma posição superior numa universidade durante, pelo menos, oito anos, ou terem trabalhado numa empresa cotada em bolsa ou numa instituição com capitais públicos durante, pelo menos, dez anos (dos quais, pelo menos, cinco anos como diretores executivos), ver o artigo 7.º da Lei relativa à Comissão de Auditoria e Inspeção. Além disso, os comissários estão proibidos de participar em atividades políticas e de exercer simultaneamente funções na Assembleia Nacional, em serviços administrativos, organizações sujeitas a auditorias e inspeções realizadas pela Comissão de Auditoria e Inspeção ou qualquer outro serviço ou cargo remunerado (artigo 9.º da Lei relativa à Comissão de Auditoria e Inspeção).

([285]) Artigo 8.º da Lei relativa à Comissão de Auditoria e Inspeção.

([286]) Ver, por exemplo, o artigo 27.º da Lei relativa à Comissão de Auditoria e Inspeção.

([287]) Artigos 24.º e 31.º a 35.º da Lei relativa à Comissão de Auditoria e Inspeção.

([288]) Artigo 128.º da Lei relativa à Assembleia Nacional e artigos 2.º, 3.º e 15.º da Lei relativa à inspeção e investigação da administração do Estado. Tal inclui inspeções anuais de assuntos governamentais, no seu conjunto, mas também investigações sobre questões específicas.

([289]) Ver o anexo, ponto 2.2.3.

([290]) Artigo 10.º, n.º 1, da Lei relativa à inspeção e investigação da administração do Estado. Ver também os artigos 128.º e 129.º da Lei relativa à Assembleia Nacional.

inadequadas) ([291]) e tornar públicos os resultados das suas conclusões ([292]). Sempre que a Assembleia Nacional solicite a adoção de medidas corretivas, que podem, por exemplo, incluir a concessão de indemnizações, a tomada de medidas disciplinares ou a melhoria dos procedimentos internos, a autoridade pública em causa é obrigada a agir sem demora e a comunicar os resultados à Assembleia Nacional ([293]).

3.2.4 *Recurso*

(175) O sistema coreano oferece diferentes vias (judiciais) para obter reparação, incluindo indemnizações por danos.

(176) Em primeiro lugar, a Lei relativa à proteção de informações pessoais confere às pessoas singulares o direito de acesso, retificação, apagamento e suspensão dos dados pessoais tratados para efeitos de aplicação do direito penal ([294]).

(177) Em segundo lugar, as pessoas singulares podem fazer uso dos diferentes mecanismos de recurso oferecidos pela Lei relativa à proteção de informações pessoais se os seus dados tiverem sido tratados por uma autoridade responsável pela aplicação do direito penal em violação da referida lei ou das limitações e garantias que regem a recolha de dados pessoais noutras leis (ou seja, a Lei relativa ao processo penal ou a Lei relativa à proteção da privacidade das comunicações, ver o considerando (171)). Mais especificamente, podem apresentar uma reclamação junto da Comissão de Proteção de Informações Pessoais (nomeadamente através do centro de atendimento para a privacidade gerido pela Agência de Internet e Segurança da Coreia ([295])) ou do Comité de Mediação de Litígios de Informações Pessoais ([296]). Estas possibilidades de vias de recurso não estão sujeitas a outros requisitos de admissibilidade. Com base na Lei relativa ao contencioso administrativo, as pessoas singulares podem ainda recorrer/contestar as decisões ou a inação da Comissão de Proteção de Informações Pessoais (ver considerando (132)).

(178) Em terceiro lugar, qualquer pessoa singular ([297]) pode apresentar uma reclamação junto da Comissão Nacional dos Direitos Humanos relativa a uma violação do direito à privacidade e à proteção de dados por parte de uma autoridade de aplicação do direito penal coreana. A Comissão pode recomendar a retificação ou a melhoria de qualquer lei, instituição, política ou prática pertinente ([298]), ou a aplicação de vias de recurso, como a mediação ([299]), a cessação da violação dos direitos humanos, a indemnização por danos e medidas para evitar a repetição de violações idênticas ou similares ([300]). De acordo com a declaração oficial do Governo coreano (anexo II, ponto 2.4.2), tal pode incluir também o apagamento de dados pessoais recolhidos ilicitamente. Embora a Comissão Nacional dos Direitos Humanos não tenha competência para emitir decisões vinculativas, oferece uma via de recurso mais informal, económica e facilmente acessível, em especial porque, conforme explicado no anexo II, ponto 2.4.2, não exige a demonstração de um prejuízo de facto para que uma reclamação seja investigada ([301]). Deste modo garante-se a possibilidade de investigar as reclamações das pessoas singulares relativas à recolha dos dados que lhes digam respeito, mesmo se a pessoa singular não estiver em condições de demonstrar que os dados que lhe dizem respeito foram efetivamente recolhidos (por exemplo, em virtude de a pessoa singular não ter sido ainda notificada). Os relatórios anuais de atividades da Comissão Nacional dos Direitos Humanos mostram que, na prática, as pessoas também utilizam esta via para contestar as atividades das autoridades responsáveis pela aplicação do direito penal, nomeadamente no que respeita ao tratamento de dados pessoais ([302]). Se uma pessoa não estiver satisfeita com o resultado de um processo junto da Comissão Nacional dos Direitos Humanos, pode

([291]) Artigo 16.º, n.º 2, da Lei relativa à inspeção e investigação da administração do Estado.

([292]) Artigo 12.º-2 da Lei relativa à inspeção e investigação da administração do Estado.

([293]) Artigo 16.º, n.º 3, da Lei relativa à inspeção e investigação da administração do Estado.

([294]) Este direito pode ser exercido diretamente junto da autoridade competente ou indiretamente através da Comissão de Proteção de Informações Pessoais (artigo 35.º, n.º 2, da Lei relativa à proteção de informações pessoais). Conforme descrito em mais pormenor nos considerandos (76) a (78), as exceções a estes direitos só serão aplicáveis quando necessário para proteger interesses (públicos) importantes.

([295]) Artigo 62.º da Lei relativa à proteção de informações pessoais.

([296]) Artigos 40.º a 50.º da Lei relativa à proteção de informações pessoais e artigos 48.º-2 a 57.º do respetivo decreto de execução. Ver também o anexo II, ponto 2.4.1.

([297]) Conforme explicado no anexo II, ponto 2.4.2, embora o artigo 4.º da Lei relativa à Comissão Nacional dos Direitos Humanos se refira a cidadãos e estrangeiros residentes na República da Coreia, o termo «residir» reflete um conceito de jurisdição e não de território. Por conseguinte, se os direitos fundamentais de um estrangeiro fora da Coreia forem violados por instituições nacionais na Coreia, essa pessoa pode apresentar uma reclamação junto da Comissão Nacional dos Direitos Humanos. Tal seria o caso se as autoridades públicas coreanas acedessem ilegalmente aos dados pessoais de um estrangeiro transferidos para a Coreia. Ver, nomeadamente, as explicações fornecidas em https://www.humanrights.go.kr/site/program/board/basicboard/list?boardtypeid=7025&menuid=002004005001&pagesize=10&currentpage=2.

([298]) Artigo 44.º da Lei relativa à Comissão Nacional dos Direitos Humanos.

([299]) Uma pessoa singular também pode solicitar a resolução da reclamação através da mediação, ver o artigo 42.º e seguintes da Lei relativa à Comissão Nacional dos Direitos Humanos.

([300]) Artigo 42.º, n.º 4, da Lei relativa à Comissão Nacional dos Direitos Humanos. Além disso, a Comissão Nacional dos Direitos Humanos pode adotar medidas de reparação urgentes no caso de uma infração em curso que seja suscetível de causar danos difíceis de reparar se deixada por tramitar (ver artigo 48.º da Lei relativa à Comissão Nacional dos Direitos Humanos).

([301]) Em princípio, uma reclamação tem de ser apresentada no prazo de um ano a contar da data da violação, mas a Comissão Nacional dos Direitos Humanos pode ainda decidir investigar uma reclamação apresentada após esse prazo, desde que o período de prescrição ao abrigo do direito penal ou civil não tenha expirado (artigo 32.º, n.º 1, ponto 4, da Lei relativa à Comissão Nacional dos Direitos Humanos).

([302]) Por exemplo, no passado, a Comissão Nacional dos Direitos Humanos tratou reclamações e emitiu recomendações relativamente a apreensões ilegais e a uma violação do requisito de informar as pessoas de uma apreensão (ver p. 80 e 91 do relatório anual de 2018 da Comissão Nacional dos Direitos Humanos, disponível em https://www.humanrights.go.kr/site/program/board/basicboard/view?menuid=002003003001&pagesize=10&boardtypeid=7017&boardid=7604746), bem como relativamente ao tratamento ilícito de informações pessoais por parte da polícia, do Ministério Público e dos tribunais (ver p. 157-158 do relatório anual de 2019 da Comissão Nacional dos Direitos Humanos, disponível em https://www.humanrights.go.kr/site/program/board/basicboard/view?menuid=002003003001&pagesize=10&boardtypeid=7017&boardid=7603308, e p. 76 do relatório anual de 2019, disponível em https://www.humanrights.go.kr/site/program/board/basicboard/view?menuid=002003003001&pagesize=10&boardtypeid=7017&boardid=7606217).

contestar as suas decisões (como uma decisão de não prosseguir a investigação de uma reclamação ([303])) e recomendações junto dos tribunais coreanos ao abrigo da Lei relativa ao contencioso administrativo (ver considerando (181)) ([304]). Além disso, um procedimento junto da Comissão Nacional dos Direitos Humanos pode ainda facilitar o acesso aos tribunais, uma vez que a pessoa pode procurar obter uma reparação adicional contra a autoridade pública que tratou ilegalmente os seus dados com base nas conclusões da Comissão, em conformidade com os procedimentos descritos nos considerandos (181) a (183).

(179) Por último, existem diferentes vias de recurso judiciais disponíveis, que permitem às pessoas invocar as limitações e garantias descritas no ponto 3.2.1 para obter reparação ([305]).

(180) No que respeita às apreensões (incluindo de dados), a Lei relativa ao processo penal prevê a possibilidade de a pessoa se opor ou contestar a execução de um mandado mediante a apresentação ao tribunal competente de um pedido de anulação ou alteração de uma disposição tomada por um procurador ou agente da polícia ([306]).

(181) De um modo mais geral, as pessoas singulares podem contestar as ações ([307]) ou omissões ([308]) das autoridades públicas (incluindo as autoridades responsáveis pela aplicação do direito penal) ao abrigo da Lei relativa ao contencioso administrativo ([309]). A ação administrativa é considerada um «ato contestável» se tiver um impacto direto nos direitos e deveres civis ([310]), o que, tal como confirmado pelo Governo coreano (anexo II, ponto 2.4.3), é o caso das medidas de recolha de dados pessoais, diretamente (por exemplo, através da interceção de comunicações), ou através de pedidos de divulgação vinculativos (por exemplo, a um prestador de serviços) ou pedidos de cooperação voluntária. Para que uma reclamação ao abrigo da Lei relativa ao contencioso administrativo seja admissível, a pessoa singular tem de ter um interesse jurídico em intentar a ação ([311]). De acordo com a jurisprudência do Supremo Tribunal, o «interesse jurídico» é interpretado como um «interesse protegido juridicamente», ou seja, um interesse direto e específico protegido pelas disposições legislativas e regulamentares em que se baseiam os atos administrativos (ou seja, não se trata de interesses gerais, indiretos e abstratos do público) ([312]). As pessoas têm um interesse jurídico no caso de qualquer violação das limitações e garantias aplicáveis à recolha dos seus dados pessoais para efeitos de aplicação do direito penal (ao abrigo de leis específicas ou da Lei relativa à proteção de informações pessoais). Com base na Lei relativa ao contencioso administrativo, um tribunal pode decidir revogar ou alterar um ato ilegal, emitir uma declaração de nulidade (ou seja, uma declaração de que o ato não produz efeitos jurídicos ou é inexistente na ordem jurídica) ou emitir uma declaração de que uma omissão é ilegal ([313]). Uma decisão transitada em julgado nos termos da Lei relativa ao contencioso administrativo é vinculativa para as partes ([314]).

([303]) Por exemplo, se a Comissão Nacional dos Direitos Humanos, excecionalmente, não puder inspecionar determinados materiais ou instalações por dizerem respeito a segredos de Estado suscetíveis de afetar substancialmente a segurança do Estado ou as relações diplomáticas, ou se a inspeção constituir um sério obstáculo a uma investigação criminal ou a um julgamento pendente e se tal impedir a Comissão de realizar a investigação necessária para avaliar o mérito da petição recebida, deve informar a pessoa em causa das razões pelas quais a reclamação foi rejeitada, em conformidade com o artigo 39.º da Lei relativa à Comissão Nacional dos Direitos Humanos. Nesse caso, a pessoa poderia contestar essa decisão ao abrigo da Lei relativa ao contencioso administrativo.

([304]) Ver, por exemplo, a Decisão n.º 2007NU27259 do Tribunal Superior de Seul, de 18 de abril de 2008, confirmada pela Decisão n.º 2008Du7854 do Supremo Tribunal, de 9 de outubro de 2008; e a Decisão n.º 2017NU69382 do Tribunal Superior de Seul, de 2 de fevereiro de 2018.

([305]) Ver o anexo II, ponto 2.4.3.

([306]) Artigo 417.º em conjugação com o artigo 414.º, n.º 2, da Lei relativa ao processo penal. Ver também a Decisão n.º 97Mo66 do Supremo Tribunal, de 29 de setembro de 1997.

([307]) A Lei relativa ao contencioso administrativo refere-se a um «ato», ou seja, o exercício do poder público, ou a recusa de o exercer, num caso específico.

([308]) Nos termos da Lei relativa ao contencioso administrativo, omissão refere-se à não emissão prolongada por parte de um serviço administrativo de um determinado ato, não obstante a sua obrigação legal de o fazer.

([309]) Um recurso administrativo pode ser interposto, em primeiro lugar, junto de comissões de recursos administrativos criadas sob a tutela de determinadas autoridades públicas (como o Serviço Nacional de Informações e a Comissão Nacional dos Direitos Humanos) ou junto da Comissão Central de Recursos Administrativos, criada sob a tutela da Comissão de Combate à Corrupção e dos Direitos Civis (artigo 6.º da Lei relativa aos recursos administrativos e artigo 18.º, n.º 1, da Lei relativa ao contencioso administrativo), como via de recurso mais informal. No entanto, também é possível intentar uma ação diretamente nos tribunais coreanos com base na Lei relativa ao contencioso administrativo.

([310]) Decisão n.º 98Du18435 do Supremo Tribunal, de 22 de outubro de 1999, Decisão n.º 99Du1113 do Supremo Tribunal, de 8 de setembro de 2000, e Decisão n.º 2010Du3541 do Supremo Tribunal, de 27 de setembro de 2012.

([311]) Artigos 12.º, 35.º e 36.º da Lei relativa ao contencioso administrativo. Além disso, os pedidos de revogação/alteração de um ato e de confirmação da ilegalidade de uma omissão devem ser apresentados no prazo de 90 dias a contar da data em que a pessoa toma conhecimento do ato ou da omissão e, em princípio, o mais tardar um ano a contar da data em que o ato é emitido ou em que a omissão ocorreu, salvo se existirem razões justificáveis (artigo 20.º e artigo 38.º, n.º 2, da Lei relativa ao contencioso administrativo). O conceito de «razões justificáveis» foi interpretado em sentido lato pelo Supremo Tribunal e exige que se avalie se é socialmente aceitável permitir a apresentação de uma reclamação tardia, à luz de todas as circunstâncias do processo (Decisão n.º 90NU6521 do Supremo Tribunal, de 28 de junho de 1991). Conforme confirmado pelo Governo coreano no anexo II, ponto 2.4.3, tal inclui, nomeadamente, razões para o atraso pelas quais a parte em causa não pode ser responsabilizada (ou seja, situações que escapam ao controlo do autor da reclamação, por exemplo, quando este não foi notificado da recolha das suas informações pessoais) ou motivos de força maior (por exemplo, uma catástrofe natural ou uma guerra).

([312]) Decisão n.º 2006Du330 do Supremo Tribunal, de 26 de março de 2006.

([313]) Artigos 2.º e 4.º da Lei relativa ao contencioso administrativo.

([314]) Artigo 30.º, n.º 1, da Lei relativa ao contencioso administrativo.

(182) Além de contestarem a ação governamental através do contencioso administrativo, as pessoas singulares também podem apresentar uma queixa constitucional ao Tribunal Constitucional relativamente a qualquer violação dos seus direitos fundamentais devido ao exercício ou não exercício do poder governamental (excluindo os acórdãos dos tribunais) ([315]). Se existirem outras vias de recurso, estas devem ser esgotadas em primeiro lugar. De acordo com a jurisprudência do Tribunal Constitucional, os estrangeiros podem apresentar uma queixa constitucional na medida em que os seus direitos fundamentais sejam reconhecidos pela Constituição coreana (ver explicações do ponto 1.1) ([316]). O Tribunal Constitucional pode invalidar o exercício do poder governamental que causou a infração ou confirmar a inconstitucionalidade de uma determinada omissão ([317]). Nesse caso, a autoridade competente é obrigada a tomar medidas para cumprir a decisão do Tribunal.

(183) Além disso, as pessoas singulares podem obter uma indemnização por danos nos tribunais coreanos. Tal inclui, em primeiro lugar, a possibilidade de pedir uma indemnização por violações da Lei relativa à proteção de informações pessoais cometidas pelas autoridades responsáveis pela aplicação do direito penal, em conformidade com o artigo 39.º (ver também o considerando (135)). De um modo mais geral, as pessoas singulares podem pedir uma indemnização por danos causados por funcionários públicos no exercício das suas funções oficiais em violação da lei, com base na Lei relativa às indemnizações do Estado (ver também o considerando (135)) ([318]).

(184) Os mecanismos descritos nos considerandos (176) a (183) oferecem vias de recurso administrativas e judiciais eficazes aos titulares dos dados, permitindo-lhes, em particular, exercer os seus direitos, nomeadamente o direito de acesso aos seus dados pessoais, ou obter a retificação ou o apagamento desses dados.

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

(185) O direito da República da Coreia contém uma série de limitações e garantias no que respeita ao acesso e à utilização de dados pessoais para efeitos de segurança nacional, e prevê mecanismos de recurso e supervisão neste domínio, que estão em conformidade com os requisitos referidos nos considerandos (141) a (143) da presente decisão. Os pontos seguintes descrevem as condições nas quais esse acesso pode ser efetuado e as garantias aplicáveis à utilização desses poderes.

3.3.1 *Bases jurídicas, limitações e garantias*

(186) Na República da Coreia, é possível aceder aos dados pessoais para efeitos de segurança nacional com base na Lei relativa à proteção da privacidade das comunicações, na Lei relativa às atividades de telecomunicações e na Lei relativa ao antiterrorismo para a proteção dos cidadãos e da segurança pública («Lei antiterrorismo») ([319]). A principal autoridade ([320]) com competências no domínio da segurança nacional é o Serviço Nacional de Informações ([321]). A recolha e utilização de dados pessoais pelo Serviço Nacional de Informações tem de cumprir os requisitos legais pertinentes (nomeadamente a Lei relativa à proteção de informações pessoais e a Lei relativa

([315]) Artigo 68.º, n.º 1, da Lei relativa ao Tribunal Constitucional. As queixas constitucionais têm de ser apresentadas no prazo de 90 dias a contar da data em que a pessoa tiver tomado conhecimento da infração e no prazo de um ano após a sua ocorrência. Conforme também explicado no anexo II, ponto 2.4.3, dado que o procedimento da Lei relativa ao contencioso administrativo é aplicado aos litígios ao abrigo da Lei relativa ao Tribunal Constitucional, nos termos do artigo 40.º da referida lei, uma queixa continuará a ser admissível se existirem «razões justificáveis», tal como interpretadas em conformidade com a jurisprudência do Supremo Tribunal descrita na nota de rodapé 312. Se for necessário esgotar outras vias de recurso primeiro, a queixa constitucional deve ser apresentada no prazo de 30 dias a contar da decisão final relativa a essas vias (artigo 69.º da Lei relativa ao Tribunal Constitucional).

([316]) Decisão n.º 99HeonMa194 do Supremo Tribunal, de 29 de novembro de 2001.

([317]) Artigo 75.º, n.º 3, da Lei relativa ao Tribunal Constitucional.

([318]) Artigo 2.º, n.º 1, da Lei relativa às indemnizações do Estado.

([319]) Ver o anexo II, ponto 3.1.

([320]) A título excecional, a polícia e o Ministério Público também podem recolher informações pessoais para efeitos de segurança nacional (ver nota de rodapé 327 e anexo II, ponto 3.2.1.2). Além disso, o serviço de informações militares coreano (o Comando de Apoio à Segurança da Defesa, criado sob a tutela do Ministério da Defesa) tem competências no domínio da segurança nacional. No entanto, conforme explicado no anexo II, ponto 3.1, só é responsável pelas informações militares e apenas efetua a vigilância de civis quando tal seja necessário para o exercício das suas funções militares. Mais especificamente, só pode investigar pessoal militar, funcionários civis das forças armadas, pessoas em formação militar, reserva militar ou recrutamento militar e prisioneiros de guerra (artigo 1.º da Lei relativa ao Tribunal Militar). Ao recolher informações sobre comunicações para efeitos de segurança nacional, o Comando de Apoio à Segurança da Defesa está sujeito às limitações e garantias estabelecidas pela Lei relativa à proteção da privacidade das comunicações e pelo seu decreto de execução.

([321]) O mandato do Serviço Nacional de Informações consiste em recolher, compilar e distribuir informações sobre países estrangeiros (ou seja, informações gerais sobre tendências e desenvolvimentos relativamente a países estrangeiros, ou sobre as atividades dos intervenientes estatais); informações relacionadas com o combate à espionagem (incluindo a espionagem militar e industrial), o terrorismo e as atividades das organizações criminosas internacionais; informações sobre determinados tipos de crimes contra a segurança pública e nacional (por exemplo, insurreição interna, agressão estrangeira) e informações relacionadas com a garantia da cibersegurança e a prevenção ou o combate a ciberataques e ameaças (artigo 4.º, n.º 2, da Lei relativa ao Serviço Nacional de Informações). Ver também o anexo II, ponto 3.1.

à proteção da privacidade das comunicações) ([322]) e as orientações gerais elaboradas pelo presidente da República e revistas pela Assembleia Nacional ([323]). Como princípio geral, o Serviço Nacional de Informações deve manter a neutralidade política e proteger a liberdade e os direitos individuais ([324]). Além disso, o seu pessoal não pode abusar da sua autoridade pública para forçar uma instituição, organização ou pessoa singular a fazer algo que não seja obrigada a fazer (nos termos da lei), nem obstruir o exercício dos direitos de qualquer pessoa ([325]).

3.3.1.1 Acesso às informações sobre comunicações

(187) Com base na Lei relativa à proteção da privacidade das comunicações, as autoridades públicas coreanas ([326]) podem recolher dados de confirmação das comunicações (ou seja, a data das telecomunicações, a respetiva hora de início e de fim, o número de chamadas efetuadas e recebidas, bem como o número de assinante da outra parte, a frequência de utilização, os ficheiros de registo relativos à utilização dos serviços de telecomunicações e informações sobre a localização, ver o considerando (155)) e o conteúdo das comunicações (através de medidas de restrição das comunicações, ver o considerando (155)) para efeitos de segurança nacional (conforme determinado pelo mandato do Serviço Nacional de Informações, ver a nota de rodapé 322). Estes poderes abrangem dois tipos de informações: 1) comunicações em que uma ou ambas as partes são nacionais coreanos ([327]); e 2) comunicações de a) países hostis à República da Coreia, b) agências, grupos ou nacionais estrangeiros suspeitos de envolvimento em atividades anticoreanas ([328]), ou c) membros de grupos que operam na Península da Coreia, mas efetivamente fora da soberania da República da Coreia, e os seus grupos de coordenação estabelecidos em países estrangeiros ([329]). Por conseguinte, as comunicações de pessoas singulares da UE transferidas da União para a República da Coreia com base na presente decisão só podem ser recolhidas ao abrigo da Lei relativa à proteção da privacidade das comunicações para efeitos de segurança nacional (sob reserva das condições estabelecidas nos considerandos (188) a (192)) se ocorrerem entre uma pessoa singular da UE e um nacional coreano, ou se disserem respeito a comunicações exclusivamente entre nacionais não coreanos abrangidas por uma das três categorias referidas no ponto 2, alíneas a), b) e c).

(188) Em ambos os casos, a recolha de dados de confirmação das comunicações só pode ser realizada para efeitos de prevenção de ameaças à segurança nacional ([330]), enquanto as medidas de restrição das comunicações só podem ser tomadas quando existir um risco grave para a segurança nacional e a recolha for necessária para o evitar ([331]). Além disso, o acesso ao conteúdo das comunicações só pode ser efetuado como medida de último recurso, devendo ser envidados esforços para minimizar a violação da privacidade das comunicações ([332]), garantindo assim que esta continua a ser proporcional ao objetivo de segurança nacional em causa. A recolha do conteúdo das comunicações e dos dados de confirmação das comunicações só pode realizar-se durante um período máximo de quatro meses e deve ser imediatamente interrompida se o objetivo visado for alcançado mais cedo ([333]). Se as condições pertinentes continuarem a estar preenchidas, o prazo pode ser prorrogado, mediante autorização prévia de um tribunal (para as medidas descritas no considerando (189)) ou do presidente da República (para as medidas descritas no considerando (190)) ([334]), por um período máximo de quatro meses.

(189) As mesmas garantias processuais aplicam-se à recolha de dados de confirmação das comunicações e do conteúdo das comunicações ([335]). Mais especificamente, se pelo menos uma das pessoas envolvidas na comunicação for um nacional coreano, o serviço de informações tem de apresentar um pedido por escrito à Procuradoria

([322]) Ver também os artigos 14.º, 22.º e 23.º da Lei relativa ao Serviço Nacional de Informações.
([323]) Artigo 4.º, n.º 2, da Lei relativa ao Serviço Nacional de Informações.
([324]) Artigo 3.º, n.º 1, artigo 6.º, n.º 2, e artigos 11.º e 21.º da Lei relativa ao Serviço Nacional de Informações. Ver também as regras em matéria de conflitos de interesses, nomeadamente os artigos 10.º e 12.º da Lei relativa ao Serviço Nacional de Informações.
([325]) Artigo 13.º da Lei relativa ao Serviço Nacional de Informações.
([326]) Tal inclui os serviços de informações (ou seja, o Serviço Nacional de Informações e o Comando de Apoio à Segurança da Defesa) e a polícia/o Ministério Público.
([327]) Artigo 7.º, n.º 1, ponto 1, da Lei relativa à proteção da privacidade das comunicações.
([328]) Conforme explicado pelo Governo coreano na nota de rodapé 244 do anexo II, tal refere-se a atividades que ameaçam a existência e a segurança da nação, a ordem democrática ou a sobrevivência e liberdade do povo.
([329]) Artigo 7.º, n.º 1, ponto 2, da Lei relativa à proteção da privacidade das comunicações.
([330]) Artigo 13.º-4, da Lei relativa à proteção da privacidade das comunicações.
([331]) Artigo 7.º, n.º 1, da Lei relativa à proteção da privacidade das comunicações.
([332]) Artigo 3.º, n.º 2, da Lei relativa à proteção da privacidade das comunicações. Além disso, as medidas de restrição das comunicações devem ser imediatamente interrompidas logo que deixem de ser necessárias, garantindo assim que qualquer violação dos segredos de comunicação da pessoa singular em causa seja limitada ao mínimo (artigo 2.º do Decreto de Execução da Lei relativa à proteção da privacidade das comunicações).
([333]) Artigo 7.º, n.º 2, da Lei relativa à proteção da privacidade das comunicações.
([334]) O pedido de autorização para a prorrogação das medidas de vigilância tem de ser apresentado por escrito, indicando as razões pelas quais a prorrogação é solicitada e fornecendo materiais de apoio (artigo 7.º, n.º 2, da Lei relativa à proteção da privacidade das comunicações e artigo 5.º do respetivo decreto de execução).
([335]) Ver o artigo 13.º-4, n.º 2, da Lei relativa à proteção da privacidade das comunicações e o artigo 37.º, n.º 4, do respetivo decreto de execução, segundo os quais os procedimentos aplicáveis à recolha do conteúdo das comunicações também se aplicam à recolha de dados de confirmação das comunicações. Ver também o anexo II, ponto 3.2.1.1.1.

Superior que, por sua vez, tem de solicitar um mandado a um juiz presidente superior do Tribunal Superior ([336]). A Lei relativa à proteção da privacidade das comunicações enumera as informações que devem ser fornecidas no pedido ao procurador, no pedido de mandado e no próprio mandado, que incluem, nomeadamente, a justificação do pedido e os principais motivos de suspeita, os materiais de apoio, bem como informações sobre o objetivo, o alvo [ou seja, a(s) pessoa(s) visada(s)], o âmbito e a duração da medida proposta ([337]). A recolha sem mandado só pode ser realizada se houver um ato de conspiração que ameace a segurança nacional e se existir uma situação de emergência que impossibilite a realização dos referidos procedimentos ([338]). No entanto, também nesse caso, o pedido de mandado tem de ser apresentado imediatamente após a adoção da medida ([339]). Por conseguinte, a Lei relativa à proteção da privacidade das comunicações define claramente o âmbito e as condições destes tipos de recolha, e submete-os a garantias (processuais) específicas (incluindo a aprovação judicial prévia), que asseguram que a utilização de tais medidas se limita ao que é necessário e proporcionado. Além disso, a obrigação de fornecer informações pormenorizadas no pedido de um mandado e no próprio mandado exclui a possibilidade de acesso indiscriminado.

(190) Para as comunicações entre nacionais não coreanos que se enquadram numa das três categorias específicas enumeradas no considerando (187), deve ser apresentado um pedido ao diretor do Serviço Nacional de Informações que, após uma análise da adequação das medidas propostas, tem de solicitar a aprovação prévia, por escrito, do Presidente da República da Coreia ([340]). O pedido elaborado pelo serviço de informações tem de incluir as mesmas informações pormenorizadas que o pedido de um mandado judicial (ver considerando (189)), nomeadamente no que se refere à justificação do pedido e aos principais motivos de suspeita, aos materiais de apoio e às informações sobre os objetivos, a(s) pessoa(s) visada(s), o âmbito e a duração das medidas propostas ([341]). Em situações de emergência ([342]), deve obter-se a aprovação prévia do ministro que tutela o serviço de informações em causa, embora o serviço de informações tenha de solicitar a aprovação do presidente da República imediatamente após a adoção das medidas de emergência ([343]). Também no que respeita à recolha de comunicações exclusivamente entre nacionais não coreanos, a Lei relativa à proteção da privacidade das comunicações limita, portanto, a utilização de tais medidas ao que é necessário e proporcionado, definindo claramente as categorias limitadas de pessoas que podem ser sujeitas a tais medidas e estabelecendo critérios pormenorizados que os serviços de informações devem demonstrar para justificar um pedido de recolha de informações. Além disso, tal exclui novamente a possibilidade de acesso indiscriminado. Embora não exista uma aprovação prévia independente dessas medidas, a supervisão independente é assegurada *ex post*, nomeadamente pela Comissão de Proteção de Informações Pessoais e pela Comissão Nacional dos Direitos Humanos (ver, por exemplo, os considerandos (199) a (200)).

(191) Além disso, a Lei relativa à proteção da privacidade das comunicações impõe várias garantias adicionais que contribuem para a supervisão *ex post* e facilitam o acesso das pessoas singulares a vias de recurso eficazes. Em primeiro lugar, no que respeita a qualquer tipo de recolha para efeitos de segurança nacional, a referida lei prevê diferentes requisitos de conservação de registos e apresentação de relatórios. Mais especificamente, quando solicitam a cooperação de operadores privados, os serviços de informações têm de apresentar o mandado judicial/a autorização presidencial ou uma cópia da capa de uma declaração de censura de emergência, que a entidade visada deve conservar nos seus arquivos ([344]). Quando os operadores privados são obrigados a cooperar, tanto a autoridade pública requerente como o operador em causa devem conservar registos sobre a finalidade

([336]) Artigo 6.º, n.ºs 5 e 8, e artigo 7.º, n.º 1, ponto 1, e n.º 3, da Lei relativa à proteção da privacidade das comunicações, em conjugação com o artigo 7.º, n.ºs 3 e 4, do respetivo decreto de execução.

([337]) Ver o artigo 7.º, n.º 3, e o artigo 6.º, n.º 4, da Lei relativa à proteção da privacidade das comunicações (para o pedido do serviço de informações), o artigo 4.º do Decreto de Execução da Lei relativa à proteção da privacidade das comunicações (para o pedido do procurador), e o artigo 7.º, n.º 3, e o artigo 6.º, n.º 6, da Lei relativa à proteção da privacidade das comunicações (para o mandado).

([338]) Artigo 8.º da Lei relativa à proteção da privacidade das comunicações.

([339]) Artigo 8.º, n.ºs 2 e 8, da Lei relativa à proteção da privacidade das comunicações. A recolha deve ser imediatamente interrompida se a autorização judicial não for obtida no prazo de 36 horas a contar do momento em que as medidas são tomadas. Nos casos em que a vigilância é concluída num curto espaço de tempo, excluindo a autorização do tribunal, o diretor da Procuradoria Superior competente tem de enviar uma notificação de medida de emergência elaborada pelo serviço de informações ao presidente do tribunal competente que, nesta base, pode analisar a legalidade da recolha (artigo 8.º, n.ºs 5 e 7, da Lei relativa à proteção da privacidade das comunicações). Esta notificação tem de indicar o objetivo, o alvo, o âmbito, o período, o local de execução e o método de vigilância, bem como os motivos para não apresentar um pedido antes de tomar a medida (artigo 8.º, n.º 6, da Lei relativa à proteção da privacidade das comunicações). De um modo mais geral, os serviços de informações só podem tomar medidas de emergência em conformidade com uma «declaração de censura/escutas telefónicas de emergência» e devem conservar registos dessas medidas (artigo 8.º, n.º 4, da Lei relativa à proteção da privacidade das comunicações).

([340]) Artigo 8.º, n.ºs 1 e 2, do Decreto de Execução da Lei relativa à proteção da privacidade das comunicações.

([341]) Artigo 8.º, n.º 3, do Decreto de Execução da Lei relativa à proteção da privacidade das comunicações, em conjugação com o artigo 6.º, n.º 4, da referida lei.

([342]) Ou seja, nos casos em que a medida visa um ato de conspiração que ameaça a segurança nacional, em que não há tempo suficiente para obter a aprovação do presidente e em que a não adoção de medidas de emergência pode prejudicar a segurança nacional (artigo 8.º, n.º 8, da Lei relativa à proteção da privacidade das comunicações).

([343]) Artigo 8.º, n.º 9, da Lei relativa à proteção da privacidade das comunicações. A recolha deve ser imediatamente interrompida se a autorização não for obtida no prazo de 36 horas a contar do momento em que o pedido é apresentado.

([344]) Artigo 9.º, n.º 2, da Lei relativa à proteção da privacidade das comunicações e artigo 12.º do respetivo decreto de execução. Ver o artigo 13.º do Decreto de Execução da Lei relativa à proteção da privacidade das comunicações sobre a possibilidade de exigir a assistência das estações de correio e dos prestadores de serviços de telecomunicações. Os operadores privados a quem é solicitada a divulgação de informações podem recusar fazê-lo quando o mandado/a autorização ou a declaração de censura de emergência se refere a um identificador errado (por exemplo, um número de telefone pertencente a um indivíduo diferente do identificado). Em qualquer caso, estão proibidos de divulgar as palavras-passe utilizadas nas comunicações (artigo 9.º, n.º 4, da Lei relativa à proteção da privacidade das comunicações).

e o objeto das medidas, bem como sobre a data de execução ([345]). Além disso, os serviços de informações têm de comunicar ao diretor do Serviço Nacional de Informações as informações recolhidas e os resultados da atividade de vigilância ([346]).

(192) Em segundo lugar, as pessoas singulares têm de ser notificadas da recolha dos seus dados (dados de confirmação das comunicações ou do conteúdo das comunicações) para efeitos de segurança nacional se esta disser respeito a comunicações em que, pelo menos, uma das partes é um nacional coreano ([347]). Esta notificação tem de ser apresentada por escrito no prazo de 30 dias a contar da data em que terminou a recolha (incluindo se os dados tiverem sido obtidos de acordo com o procedimento de emergência) e só pode ser diferida se e enquanto puser em risco a segurança nacional ou prejudicar a vida e a segurança física das pessoas ([348]). Independentemente dessa notificação, as pessoas singulares podem obter reparação através de diferentes vias, conforme explicado mais pormenorizadamente no ponto 3.3.4.

3.3.1.2 Recolha de informações sobre suspeitos de terrorismo

(193) A Lei antiterrorismo prevê que o Serviço Nacional de Informações possa recolher dados sobre suspeitos de terrorismo ([349]), em conformidade com as limitações e garantias previstas noutras leis ([350]). Mais especificamente, o Serviço Nacional de Informações pode obter dados de comunicações (com base na Lei relativa à proteção da privacidade das comunicações) e outras informações pessoais (através de um pedido de divulgação voluntária) ([351]). No que respeita à recolha de informações sobre comunicações (ou seja, o conteúdo das comunicações ou os dados de confirmação das comunicações), aplicam-se as limitações e garantias descritas no ponto 3.3.1.1, incluindo a exigência de obtenção de um mandado aprovado pelo tribunal. No que respeita aos pedidos de divulgação voluntária de outros tipos de dados pessoais de suspeitos de terrorismo, o Serviço Nacional de Informações deve cumprir os requisitos da Constituição e da Lei relativa à proteção de informações pessoais em matéria de necessidade e proporcionalidade (ver considerando (164)) ([352]). Os responsáveis pelo tratamento que recebem esses pedidos podem cumpri-lo voluntariamente nas condições estabelecidas na Lei relativa à proteção de informações pessoais (por exemplo, em conformidade com o princípio da minimização dos dados e limitando o impacto na privacidade do indivíduo) ([353]). Nesse caso, têm também de cumprir a obrigação de notificar a pessoa em causa de acordo com a Notificação n.º 2021-5 (ver considerando (166)).

([345]) No que se refere às medidas de restrição das comunicações, esses registos têm de ser conservados durante três anos, ver o artigo 9.º, n.º 3, da Lei relativa à proteção da privacidade das comunicações e o artigo 17.º, n.º 2, do respetivo decreto de execução. No que respeita aos dados de confirmação das comunicações, os serviços de informações devem conservar registos da apresentação de um pedido de tais dados, bem como do próprio pedido escrito e da instituição que o invocou (artigo 13.º, n.º 5, e artigo 13.º-4, n.º 3, da Lei relativa à proteção da privacidade das comunicações). Os prestadores de serviços de telecomunicações têm de conservar registos durante sete anos e comunicar duas vezes por ano ao Ministro da Ciência e das TIC a frequência dessas divulgações (artigo 9.º, n.º 3, da Lei relativa à proteção da privacidade das comunicações, em conjugação com o artigo 13.º, n.º 7, da referida lei e o artigo 37.º n.º 4, e artigo 39.º do respetivo decreto de execução).

([346]) Artigo 18.º, n.º 3, do Decreto de Execução da Lei relativa à proteção da privacidade das comunicações.

([347]) Artigo 9.º-2, n.º 3, e artigo 13.º-4 da Lei relativa à proteção da privacidade das comunicações. A notificação tem de incluir 1) o facto de as informações terem sido recolhidas, 2) o serviço de execução e 3) o período de execução.

([348]) Artigo 9.º-2, n.º 4, da Lei relativa à proteção da privacidade das comunicações. Nesse caso, a notificação deve ser apresentada no prazo de 30 dias a partir do momento em que os motivos para o diferimento deixarem de existir, ver o artigo 13.º-4, n.º 2, e o artigo 9.º-2, n.º 6, da Lei relativa à proteção da privacidade das comunicações.

([349]) Ou seja, membros de um grupo terrorista (conforme designado pelas Nações Unidas, ver o artigo 2.º, n.º 2, da Lei antiterrorismo); pessoas que promovam e divulguem ideias ou táticas de um grupo terrorista, mobilizem ou contribuam para fundos para o terrorismo, ou estejam envolvidas noutras atividades de preparação, conspiração, propagação ou instigação do terrorismo; ou pessoas em relação às quais existam motivos válidos para suspeitar que realizaram tais atividades (artigo 2.º, n.º 3, da Lei antiterrorismo). O conceito de «terrorismo» é definido no artigo 2.º, n.º 1, da Lei antiterrorismo como um comportamento levado a cabo com a finalidade de impedir o exercício da autoridade do Estado, de um governo local ou de um governo estrangeiro (incluindo organizações internacionais), ou com a finalidade de o obrigar a agir sem qualquer obrigação legal de o fazer, ou de ameaçar o público. Tais comportamentos podem incluir, por exemplo, matar, raptar ou fazer alguém refém; sequestrar/tomar, destruir ou danificar um navio ou aeronave; utilizar armas bioquímicas, explosivas ou incendiárias com a intenção de causar a morte, ferimentos ou danos graves; e fazer mau uso de materiais nucleares ou radioativos.

([350]) Artigo 9.º, n.ºs 1 e 3, da Lei antiterrorismo.

([351]) Embora a Lei antiterrorismo também refira a possibilidade de recolher informações sobre a entrada e a saída da República da Coreia com base na Lei relativa à imigração e no Código Aduaneiro, atualmente, essas leis não preveem esses poderes (ver anexo II, ponto 3.2.2.1). Em qualquer caso, não seriam, em princípio, aplicáveis aos dados transferidos com base na presente decisão, uma vez que normalmente diriam respeito a informações que seriam recolhidas diretamente pelas autoridades coreanas (e não ao acesso a dados anteriormente transferidos da União para responsáveis pelo tratamento coreanos). Além disso, a Lei antiterrorismo indica a Lei relativa à comunicação e utilização de informações específicas sobre transações financeiras como base jurídica para a recolha de informações sobre transações financeiras. No entanto, conforme explicado na nota de rodapé 200, os tipos de dados que podem ser obtidos com base nessa lei não estão abrangidos pelo âmbito de aplicação da presente decisão. Por último, a Lei antiterrorismo prevê igualmente que o Serviço Nacional de Informações possa recolher informações de localização através de pedidos não vinculativos, caso em que os fornecedores dessas informações as podem divulgar voluntariamente nas condições estabelecidas na Lei relativa à proteção de informações pessoais (conforme descrito no considerando (193)) e na Lei relativa às informações de localização. No entanto, conforme também explicado na nota de rodapé 17, as informações de localização não seriam transferidas da União para responsáveis pelo tratamento coreanos com base na presente decisão, mas geradas na Coreia.

([352]) Ver o anexo II, ponto 3.2.2.2.

([353]) Ver o artigo 58.º, n.º 4, da Lei relativa à proteção de informações pessoais, que exige que as informações pessoais apenas sejam tratadas na medida do mínimo necessário para atingir o objetivo pretendido, e o artigo 3.º, n.º 6, da referida lei, que prevê que as informações pessoais tenham de ser tratadas de forma a minimizar a possibilidade de violação da privacidade do indivíduo. Ver também o artigo 59.º, pontos 2 e 3, da Lei relativa à proteção de informações pessoais segundo o qual os responsáveis pelo tratamento estão proibidos de divulgar informações pessoais a terceiros sem autorização.

3.3.1.3 Pedidos de divulgação voluntária de dados de assinantes

(194) Com base na Lei relativa às atividades de telecomunicações, os fornecedores de telecomunicações podem divulgar voluntariamente dados de assinantes (ver considerando (163)) a pedido de um serviço de informações que pretenda recolher essas informações para prevenir uma ameaça para a segurança nacional ([354]). No que respeita a tais pedidos do Serviço Nacional de Informações, aplicam-se as mesmas limitações (decorrentes da Constituição, da Lei relativa à proteção de informações pessoais e da Lei relativa às atividades de telecomunicações) que no domínio da aplicação do direito penal, conforme estabelecidas no considerando (164) ([355]). Os fornecedores de telecomunicações não são obrigados a obedecer e só o podem fazer nas condições estabelecidas na Lei relativa à proteção de informações pessoais (nomeadamente, em conformidade com o princípio da minimização dos dados e limitando o impacto na privacidade do indivíduo, ver também o considerando (193)). No que respeita à conservação de registos e à notificação da pessoa em causa, aplicam-se os mesmos requisitos que no domínio da aplicação do direito penal (ver considerandos (165) e (166)).

3.3.2 *Utilização adicional das informações recolhidas*

(195) O tratamento de dados pessoais recolhidos pelas autoridades coreanas para efeitos de segurança nacional está sujeito aos seguintes princípios da Lei relativa à proteção de informações pessoais: limitação das finalidades (artigo 3.º, n.ºs 1 e 2), licitude e lealdade do tratamento (artigo 3.º, n.º 1), proporcionalidade/minimização dos dados (artigo 3.º, n.ºs 1 e 6, e artigo 58.º), exatidão (artigo 3.º, n.º 3), transparência (artigo 3.º, n.º 5), segurança (artigo 58.º, n.º 4) e limitação da conservação (artigo 58.º, n.º 4) ([356]). A eventual divulgação de dados pessoais a terceiros (incluindo países terceiros) só pode ocorrer em conformidade com estes princípios (nomeadamente, a limitação da finalidade e a minimização dos dados), após avaliar a conformidade com os princípios da necessidade e da proporcionalidade (artigo 37.º, n.º 2, da Constituição) e tendo em conta o impacto nos direitos das pessoas singulares em causa (artigo 3.º, n.º 6, da Lei relativa à proteção de informações pessoais).

(196) No que respeita ao conteúdo das comunicações e aos dados de confirmação das comunicações, a Lei relativa à proteção da privacidade das comunicações limita ainda mais a utilização desses dados aos processos judiciais, quando uma parte relacionada com a comunicação os invoca num pedido de indemnização, ou às utilizações permitidas ao abrigo de outras leis ([357]).

3.3.3 *Supervisão*

(197) As atividades das autoridades de segurança nacionais coreanas são supervisionadas por diferentes organismos ([358]).

(198) Em primeiro lugar, a Lei antiterrorismo prevê mecanismos de supervisão específicos para as atividades de luta contra o terrorismo, nomeadamente a recolha de dados sobre os suspeitos de terrorismo. Mais concretamente, a nível do executivo, as atividades de luta contra o terrorismo são supervisionadas pela Comissão de Luta contra o Terrorismo ([359]), à qual o diretor do Serviço Nacional de Informações tem de apresentar relatórios sobre as investigações e a deteção de suspeitos de terrorismo para recolher informações ou materiais necessários para essas atividades ([360]). Além disso, o responsável pela proteção dos direitos humanos supervisiona especificamente a conformidade das atividades de luta contra o terrorismo com os direitos fundamentais ([361]). Este responsável é nomeado pelo presidente da Comissão de Luta contra o Terrorismo entre as pessoas que reúnem os requisitos específicos enumerados no Decreto de Execução da Lei antiterrorismo ([362]) por um período (renovável) de dois anos, e só pode ser destituído por motivos específicos, limitados e com justa causa ([363]). No exercício da sua função de supervisão, o responsável pela proteção dos direitos humanos pode emitir recomendações gerais para

([354]) Artigo 83.º, n.º 3, da Lei relativa às atividades de telecomunicações.
([355]) Ver também o anexo II, ponto 3.2.3.
([356]) Ver o anexo II, ponto 1.2.
([357]) Artigo 5.º, n.ºs 1 e 2, e artigos 12.º e 13.º-5 da Lei relativa à proteção da privacidade das comunicações.
([358]) Ver o anexo II, ponto 3.3.
([359]) Artigo 5.º, n.º 3, da Lei antiterrorismo. A Comissão é presidida pelo primeiro-ministro e composta por vários ministros e diretores de agências governamentais, como os ministros dos Negócios Estrangeiros, da Justiça, da Defesa Nacional e do Interior e da Segurança, o diretor do Serviço Nacional de Informações e o comissário-geral da Agência Nacional de Polícia (artigo 3.º, n.º 1, do Decreto de Execução da Lei antiterrorismo).
([360]) Artigo 9.º, n.º 4, da Lei antiterrorismo.
([361]) Artigo 7.º da Lei antiterrorismo.
([362]) Ou seja, qualquer pessoa qualificada como advogado com, pelo menos, dez anos de experiência profissional, ou com conhecimentos especializados no domínio dos direitos humanos e que exerça ou tenha exercido funções (pelo menos) como professor associado durante, no mínimo, dez anos, ou como funcionário público superior em organismos estatais ou administrações locais, ou com, pelo menos, dez anos de experiência profissional no domínio dos direitos humanos, por exemplo, numa organização não governamental (artigo 7.º, n.º 1, do Decreto de Execução da Lei antiterrorismo).
([363]) Por exemplo, quando acusado num processo penal relacionado com as suas funções, por divulgação de informações confidenciais ou devido a incapacidade mental ou física crónica (artigo 7.º, n.º 3, do Decreto de Execução da Lei antiterrorismo).

melhorar a proteção dos direitos humanos ([364]) e recomendações específicas de medidas corretivas, caso tenha sido constatada uma violação dos direitos humanos ([365]). As autoridades públicas são obrigadas a informar o responsável pela proteção dos direitos humanos do seguimento dado às suas recomendações ([366]).

(199) Em segundo lugar, a Comissão de Proteção de Informações Pessoais supervisiona o cumprimento, por parte das autoridades nacionais de segurança, das regras relativas à proteção de dados, que incluem as disposições aplicáveis da Lei relativa à proteção de informações pessoais (ver considerando (149)) e as limitações e garantias aplicáveis à recolha de dados pessoais ao abrigo de outras leis (Lei relativa à proteção da privacidade das comunicações, Lei antiterrorismo e Lei relativa às atividades de telecomunicações, ver também o considerando (171)) ([367]). No exercício desta função de supervisão, a Comissão de Proteção de Informações Pessoais pode fazer uso de todos os seus poderes de investigação e reparação, conforme descrito em pormenor no ponto 2.4.2.

(200) Em terceiro lugar, as atividades das autoridades nacionais de segurança estão sujeitas à supervisão independente da Comissão Nacional dos Direitos Humanos, em conformidade com os procedimentos descritos no considerando (172) ([368]).

(201) Em quarto lugar, a função de supervisão da Comissão de Auditoria e Inspeção também se estende às autoridades nacionais de segurança, embora o Serviço Nacional de Informações possa, em circunstâncias excecionais, recusar-se a fornecer determinadas informações ou materiais, quando estes constituam segredos de Estado e o conhecimento público teria um impacto grave na segurança nacional ([369]).

(202) Por último, o controlo parlamentar das atividades do Serviço Nacional de Informações é efetuado pela Assembleia Nacional (através de um Comité de Informações especializado) ([370]). A Lei relativa à proteção da privacidade das comunicações estabelece um papel de supervisão específico para a Assembleia Nacional no que respeita à utilização de medidas de restrição das comunicações para efeitos de segurança nacional ([371]). Mais especificamente, a Assembleia Nacional pode realizar inspeções no local de equipamentos de escutas telefónicas e pode exigir que tanto o Serviço Nacional de Informações como os operadores de telecomunicações que tenham divulgado o conteúdo de comunicações apresentem relatórios sobre essa divulgação. A Assembleia Nacional pode também exercer as suas funções gerais de supervisão (em conformidade com os procedimentos descritos no considerando (174)). A Lei relativa ao Serviço Nacional de Informações exige que o diretor do Serviço Nacional de Informações responda sem demora quando o Comité de Informações solicita um relatório sobre uma questão específica ([372]), com regras específicas para determinadas informações particularmente sensíveis. Concretamente, o diretor do Serviço Nacional de Informações só pode recusar-se a responder ou a testemunhar perante o Comité em circunstâncias excecionais, ou seja, se o pedido disser respeito a segredos de Estado relativos a questões militares, diplomáticas ou relacionadas com a Coreia do Norte em que o conhecimento público possa ter um impacto grave no «destino nacional» do país ([373]). Nesse caso, o Comité de Informações pode solicitar uma explicação ao primeiro-ministro e, caso não seja prestada qualquer explicação no prazo de sete dias, a resposta ou o testemunho não podem ser recusados.

3.3.4 *Recurso*

(203) Também no domínio da segurança nacional, o sistema coreano oferece diferentes vias (judiciais) para obter reparação, incluindo indemnizações por danos. Estes mecanismos oferecem vias de recurso administrativas e judiciais eficazes aos titulares dos dados, permitindo-lhes, em particular, exercer os seus direitos, nomeadamente o direito de acesso aos seus dados pessoais ou de obter a retificação ou o apagamento desses dados.

(204) Em primeiro lugar, nos termos do artigo 3.º, n.º 5, e do artigo 4.º, n.ºs 1, 3 e 4, da Lei relativa à proteção de informações pessoais, as pessoas singulares podem exercer os seus direitos de acesso, retificação, apagamento e suspensão junto das autoridades nacionais de segurança. O ponto 6 da Notificação n.º 2021-5 (anexo I da presente decisão) esclarece melhor a forma como estes direitos se aplicam no contexto do tratamento de dados

([364]) Artigo 8.º, n.º 1, do Decreto de Execução da Lei antiterrorismo.
([365]) Artigo 9.º, n.º 1, do Decreto de Execução da Lei antiterrorismo. O responsável pela proteção dos direitos humanos tem autonomia para decidir sobre a adoção de recomendações, mas tem de as comunicar ao presidente da Comissão de Luta contra o Terrorismo.
([366]) Artigo 9.º, n.º 2, do Decreto de Execução da Lei antiterrorismo. De acordo com a declaração oficial do Governo coreano, a não aplicação de uma recomendação do responsável pela proteção dos direitos humanos seria levada à Comissão de Luta contra o Terrorismo, que inclui o primeiro-ministro, embora, até à data, não tenha havido casos em que essas recomendações não tenham sido seguidas (ver anexo II, ponto 3.3.1).
([367]) Anexo II, ponto 3.3.4.
([368]) Especificamente no que respeita ao Serviço Nacional de Informações, no passado, a Comissão Nacional dos Direitos Humanos realizou investigações *ex officio* e tratou várias reclamações individuais. Ver, por exemplo, o relatório anual de 2018 da Comissão Nacional dos Direitos Humanos, p. 128 (disponível em https://www.humanrights.go.kr/site/program/board/basicboard/view?menuid=002003003001&pagesize=10&boardtypeid=7017&boardid=7604746) e o relatório anual de 2019 da Comissão Nacional dos Direitos Humanos, p. 70 (disponível em https://www.humanrights.go.kr/site/program/board/basicboard/view?menuid=002003003001&pagesize=10&boardtypeid=7017&boardid=7606217).
([369]) Artigo 13.º, n.º 1, da Lei relativa ao Serviço Nacional de Informações.
([370]) Artigo 36.º e artigo 37.º, n.º 1, ponto 15, da Lei relativa à Assembleia Nacional.
([371]) Artigo 15.º da Lei relativa à proteção da privacidade das comunicações.
([372]) Artigo 15.º, n.º 2, da Lei relativa ao Serviço Nacional de Informações.
([373]) Artigo 17.º, n.º 2, da Lei relativa ao Serviço Nacional de Informações. Os «segredos de Estado» são definidos como factos, bens ou conhecimentos (classificados) que não devem ser divulgados a nenhum outro país ou organização, a fim de evitar qualquer desvantagem grave para a segurança nacional, e aos quais só é permitido um acesso limitado. Ver o artigo 13.º, n.º 4, da Lei relativa ao Serviço Nacional de Informações.

para efeitos de segurança nacional. Mais concretamente, uma autoridade nacional de segurança só pode limitar ou recusar o exercício do direito na medida e durante o tempo necessário e proporcionado para proteger um objetivo importante de interesse público (por exemplo, na medida e durante o tempo em que a concessão do direito possa pôr em risco uma investigação em curso ou ameaçar a segurança nacional), ou quando a concessão do direito possa causar danos à vida ou à integridade física de um terceiro. Por conseguinte, a invocação de tal restrição exige um equilíbrio entre os direitos e interesses da pessoa singular e o interesse público pertinente e não pode, em qualquer caso, afetar a essência do direito (artigo 37.º, n.º 2, da Constituição). Se o pedido for recusado ou restringido, a pessoa deve ser notificada sem demora dos motivos.

(205) Em segundo lugar, as pessoas singulares têm o direito de obter reparação ao abrigo da Lei relativa à proteção de informações pessoais se os seus dados tiverem sido tratados por uma autoridade nacional de segurança em violação da referida lei ou das limitações e garantias previstas noutras leis que regem a recolha de dados pessoais (nomeadamente, a Lei relativa à proteção da privacidade das comunicações, ver o considerando (171)) ([374]). Este direito pode ser exercido através de uma reclamação à Comissão de Proteção de Informações Pessoais (incluindo através do centro de atendimento para a privacidade, gerido pela Agência de Internet e Segurança da Coreia) ([375]). Além disso, a fim de facilitar o acesso a vias de recurso contra as autoridades nacionais de segurança coreanas, as pessoas singulares da UE podem apresentar uma reclamação à Comissão de Proteção de Informações Pessoais através da sua autoridade nacional responsável pela proteção de dados ([376]). Nesse caso, a Comissão de Proteção de Informações Pessoais notificará a pessoa através da autoridade nacional responsável pela proteção de dados uma vez concluída a investigação (incluindo, se for caso disso, informações sobre as medidas corretivas impostas). Com base na Lei relativa ao contencioso administrativo, as pessoas singulares podem ainda recorrer/contestar as decisões ou a inação da Comissão de Proteção de Informações Pessoais (ver considerando (132)).

(206) Em terceiro lugar, as pessoas singulares podem apresentar uma reclamação ao responsável pela proteção dos direitos humanos sobre a violação do seu direito à privacidade/proteção de dados no contexto de atividades de luta contra o terrorismo (ou seja, nos termos da Lei antiterrorismo) ([377]), que pode recomendar medidas corretivas. Dado que não existem requisitos de admissibilidade junto do responsável pela proteção dos direitos humanos, a reclamação será tratada mesmo que a pessoa em causa não consiga demonstrar que foi efetivamente lesada (por exemplo, devido à alegada recolha ilícita dos seus dados por uma autoridade nacional de segurança) ([378]). A autoridade competente tem de informar o responsável pela proteção dos direitos humanos de quaisquer medidas tomadas para aplicar as suas recomendações.

(207) Em quarto lugar, as pessoas singulares podem apresentar uma reclamação à Comissão Nacional dos Direitos Humanos relativa à recolha dos seus dados pelas autoridades nacionais de segurança e obter reparação em conformidade com o procedimento descrito no considerando (178) ([379]).

(208) Por último, existem diferentes vias de recurso judiciais disponíveis ([380]), que permitem às pessoas singulares invocar as limitações e garantias descritas no ponto 3.3.1 para obter reparação. Mais especificamente, as pessoas singulares podem contestar a legalidade das ações das autoridades nacionais de segurança com base na Lei relativa ao contencioso administrativo [em conformidade com o procedimento descrito no considerando (181) ou com a Lei relativa ao Tribunal Constitucional (ver considerando (182))]. Além disso, podem obter uma indemnização por danos com base na Lei relativa às indemnizações do Estado (conforme descrito com mais pormenor no considerando (183)).

4. **CONCLUSÃO**

(209) A Comissão entende que a República da Coreia, através da Lei relativa à proteção de informações pessoais, das regras especiais aplicáveis a determinados setores (conforme analisado no ponto 2) e das garantias adicionais previstas na Notificação n.º 2021-5 (anexo I), assegura um nível de proteção dos dados pessoais transferidos da União Europeia essencialmente equivalente ao garantido pelo Regulamento (UE) 2016/679.

(210) Além disso, a Comissão considera que os mecanismos de supervisão e as vias de recurso previstos na legislação coreana permitem, no seu conjunto, identificar e abordar na prática as violações às regras de proteção de dados por parte dos responsáveis pelo tratamento de dados na Coreia, 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.

([374]) Artigo 58.º, n.º 4, e artigo 4.º, n.º 5, da Lei relativa à proteção de informações pessoais. Ver o anexo II, ponto 3.4.2.
([375]) Artigo 62.º e artigo 63.º, n.º 2, da Lei relativa à proteção de informações pessoais.
([376]) Notificação n.º 2021-5 (anexo I, ponto 6).
([377]) Artigo 8.º, n.º 1, ponto 2, do Decreto de Execução da Lei antiterrorismo.
([378]) Ver o anexo II, ponto 3.4.1.
([379]) Por exemplo, a Comissão Nacional dos Direitos Humanos recebe regularmente reclamações contra o Serviço Nacional de Informações, ver os dados do relatório anual de 2019 da Comissão Nacional dos Direitos Humanos sobre o número de reclamações recebidas entre 2015 e 2019, p. 70 (disponível em https://www.humanrights.go.kr/site/program/board/basicboard/view?menuid=002003003001&pagesize=10&boardtypeid=7017&boardid=7606217).
([380]) Ver o anexo II, ponto 3.4.4.

(211) Por último, com base nas informações disponíveis sobre o quadro jurídico coreano, incluindo as declarações, garantias e compromissos do Governo coreano, que constam do anexo II, a Comissão entende que qualquer ingerência das autoridades públicas coreanas no interesse público, designadamente para efeitos de aplicação do direito penal e de segurança nacional, nos direitos fundamentais das pessoais singulares, cujos dados pessoais sejam transferidos da União Europeia para a República da Coreia, será limitada ao estritamente necessário para alcançar o objetivo legítimo em causa, existindo uma proteção jurídica eficaz contra tal ingerência.

(212) Assim, atendendo às constatações efetuadas na presente decisão, deve decidir-se que a República da Coreia garante um nível adequado de proteção, na aceção do artigo 45.º do Regulamento (UE) 2016/679, interpretado em função da Carta dos Direitos Fundamentais da União Europeia, aos dados pessoais transferidos da União Europeia para a República da Coreia para responsáveis pelo tratamento de dados pessoais na República da Coreia sujeitos à Lei relativa à proteção de informações pessoais, com exceção das organizações religiosas na medida em que tratem dados pessoais para as suas atividades missionárias, partidos políticos, na medida em que tratem dados pessoais no contexto da nomeação de candidatos, e responsáveis pelo tratamento que estejam sujeitos à supervisão da Comissão dos Serviços Financeiros para o tratamento de informações pessoais de crédito nos termos da Lei relativa às informações de crédito, na medida em que tratem essas informações.

5. EFEITOS DA PRESENTE DECISÃO E AÇÃO DAS AUTORIDADES DE PROTEÇÃO DE DADOS

(213) Os Estados-Membros e os respetivos organismos 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.

(214) 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. Mais especificamente, as transferências de um responsável pelo tratamento de dados ou de um subcontratante na União Europeia para responsáveis pelo tratamento na República da Coreia podem ser efetuadas sem que seja necessária mais nenhuma autorização.

(215) Importa recordar que, nos termos do artigo 58.º, n.º 5, do Regulamento (UE) 2016/679, e conforme explicado pelo Tribunal de Justiça no acórdão Schrems ([381]), se uma autoridade nacional 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 junto de um tribunal nacional, que poderá ter de proceder a um reenvio prejudicial para o Tribunal de Justiça ([382]).

6. CONTROLO E RENOVAÇÃO DA PRESENTE DECISÃO

(216) Em conformidade com a jurisprudência do Tribunal de Justiça ([383]), 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 país terceiro em causa 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.

(217) Por conseguinte, a Comissão deve controlar, de forma continuada, a situação na República da Coreia 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 coreanas das representações, garantias e compromissos que constam do anexo II. Para facilitar este processo, as autoridades coreanas são convidadas a informar a Comissão sobre desenvolvimentos materiais que afetem a presente decisão, no tocante ao tratamento de dados pessoais pelos operadores comerciais e pelas autoridades públicas, bem como às limitações e garantias aplicáveis ao acesso aos dados pessoais pelas autoridades públicas.

([381]) Acórdão do Tribunal de Justiça de 6 de outubro de 2015, Maximillian Schrems/Data Protection Commissioner («Schrems»), C-362/14, ECLI:EU:C:2015:650, n.º 65.

([382]) Acórdão do Tribunal de Justiça de 6 de outubro de 2015, Maximillian Schrems/Data Protection Commissioner («Schrems»), C-362/14, ECLI:EU:C:2015:650, 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 dessa decisão.»

([383]) Acórdão do Tribunal de Justiça de 6 de outubro de 2015, Maximillian Schrems/Data Protection Commissioner («Schrems»), C-362/14, ECLI:EU:C:2015:650, n.º 76.

(218) 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 responsáveis pelo tratamento de dados na República da Coreia. A Comissão deve igualmente ser informada sobre quaisquer indícios de que as ações das autoridades públicas coreanas responsáveis pela prevenção, investigação, deteção ou repressão de infrações penais ou pela segurança nacional, incluindo os organismos de supervisão, não asseguram o nível de proteção exigido.

(219) Por força do artigo 45.º, n.º 3, do Regulamento (UE) 2016/679 ([384]), e atendendo a que o nível de proteção conferido pelo quadro jurídico coreano 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 pela República da Coreia continuam a justificar-se de facto e de direito.

(220) Para tal, a presente decisão deverá ser sujeita a uma primeira avaliação no prazo de três 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 Regulamento (UE) 2016/679, se se deve ou não manter o ciclo de três anos. Em qualquer caso, as avaliações subsequentes devem ser realizadas, no mínimo, de quatro em quatro anos ([385]). A avaliação deverá abranger todos os aspetos do funcionamento da presente decisão, nomeadamente a aplicação das garantias adicionais constantes do anexo I da presente decisão, com especial atenção às proteções conferidas no caso de transferências subsequentes; evolução da jurisprudência pertinente; as regras relativas ao tratamento de informações pseudonimizadas para efeitos de estatísticas, investigação científica e arquivo no interesse público, bem como à aplicação das exceções previstas no artigo 28.º, n.º 7, da Lei relativa à proteção de informações pessoais; a eficácia do exercício dos direitos individuais, nomeadamente antes da recente reforma da Comissão de Proteção de Informações Pessoais, e a aplicação de exceções a esses direitos; a aplicação das isenções parciais ao abrigo da Lei relativa à proteção de informações pessoais, assim como as limitações e garantias respeitantes ao acesso governamental (conforme estabelecidas no anexo II da presente decisão), incluindo a cooperação da Comissão de Proteção de Informações Pessoais com as autoridades de proteção de dados da UE no que respeita a reclamações de pessoas singulares. Deve igualmente abranger a eficácia da supervisão e da execução, no que respeita à Lei relativa à proteção de informações pessoais e no domínio da aplicação do direito penal e da segurança nacional (nomeadamente da Comissão de Proteção de Informações Pessoais e da Comissão Nacional dos Direitos Humanos).

(221) A fim de realizar a avaliação, a Comissão deverá reunir-se com a Comissão de Proteção de Informações Pessoais, acompanhada, se for caso disso, por outras autoridades coreanas responsáveis pelo acesso governamental, incluindo os organismos de supervisão pertinentes. Essa reunião será aberta à participação de representantes dos membros do Comité Europeu para a Proteção de Dados. No quadro da avaliação, a Comissão deverá solicitar à Comissão de Proteção de Informações Pessoais que preste informações exaustivas sobre todos os aspetos pertinentes para a verificação de adequação, incluindo quanto às limitações e garantias respeitantes ao acesso governamental ([386]). A Comissão deve também procurar obter explicações sobre quaisquer informações que tenha recebido com relevância para a presente decisão, incluindo relatórios públicos das autoridades coreanas ou de outras partes interessadas na Coreia, do Comité Europeu para a Proteção de Dados, de autoridades responsáveis pela proteção de dados individuais, de grupos da sociedade civil, dos meios de comunicação social ou qualquer outra fonte de informação disponível.

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

7. SUSPENSÃO, REVOGAÇÃO OU ALTERAÇÃO DA PRESENTE DECISÃO

(223) Sempre que as informações disponíveis, nomeadamente as resultantes do controlo da presente decisão ou fornecidas pelas autoridades coreanas ou dos Estados-Membros, revelarem que o nível de proteção conferido pela República da Coreia pode já não ser adequado, a Comissão deve informar sem demora as autoridades coreanas competentes desse facto e solicitar que sejam adotadas medidas adequadas dentro de um prazo razoável a especificar.

(224) Se, uma vez decorrido o prazo especificado, as autoridades coreanas competentes não tomarem essas medidas ou não demonstrarem, de forma satisfatória, que a presente decisão continua a basear-se num nível de proteção adequado, a Comissão dará início ao procedimento referido no artigo 93.º, n.º 2, do Regulamento (UE) 2016/679 com vista à suspensão total ou parcial ou à revogação da presente decisão.

(225) Em alternativa, a Comissão dará início a esse procedimento com vista a alterar a 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 continua a ser assegurado um nível adequado de proteção.

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

([385]) 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 Comité Europeu para a Proteção de Dados, WP 254 rev. 01.

([386]) Ver o anexo II da presente decisão.

(226) 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 garantias adicionais constantes do anexo I e/ou que estas garantias não são eficazmente aplicadas, ou ainda se as autoridades coreanas não cumprirem as representações, garantias e compromissos constantes do anexo II da presente decisão.

(227) 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 ou por outra forma, que as autoridades coreanas competentes não prestam as informações ou esclarecimentos necessários à avaliação do nível de proteção conferido aos dados pessoais transferidos da União Europeia para a República da Coreia, ou no que respeita ao 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.

(228) Por imperativos de urgência devidamente justificados, a Comissão recorrerá à possibilidade de adotar, em conformidade com o procedimento referido no artigo 93.º, n.º 3, do Regulamento (UE) 2016/679, atos de execução imediatamente aplicáveis que suspendam, revoguem ou alterem a decisão.

8. **CONSIDERAÇÕES FINAIS**

(229) O Comité Europeu para a Proteção de Dados publicou o seu parecer ([387]), que foi tido em conta na elaboração da presente decisão.

(230) As medidas previstas na presente decisão estão em conformidade com o parecer do Comité instituído ao abrigo do artigo 93.º, n.º 1, do Regulamento (UE) 2016/679,

ADOTOU A PRESENTE DECISÃO:

Artigo 1.º

1. Para o efeito do artigo 45.º do Regulamento (UE) 2016/679, a República da Coreia assegura um nível adequado de proteção dos dados pessoais transferidos da União Europeia para entidades neste país, sujeitos à Lei relativa à proteção de informações pessoais, complementada pelas garantias adicionais definidas no anexo I, em conjunto com as declarações, garantias e compromissos oficiais constantes do anexo II.

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 nela enumeradas, respetivamente:

a) Organizações religiosas, na medida em que tratem dados pessoais para as suas atividades missionárias;

b) Partidos políticos, na medida em que tratem dados pessoais no contexto da nomeação de candidatos;

c) Entidades que estejam sujeitas à supervisão da Comissão dos Serviços Financeiros para o tratamento de informações pessoais de crédito nos termos da Lei relativa às informações de crédito, na medida em que tratem essas informações.

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 no que respeita às transferências de dados abrangidas pelo âmbito de aplicação previsto no artigo 1.º da presente decisão, o Estado-Membro em causa deve informar de imediato a Comissão.

Artigo 3.º

1. A Comissão deve garantir o controlo contínuo da aplicação do quadro jurídico em que assenta a presente decisão, nomeadamente as condições em que se procede a transferências ulteriores, o exercício dos direitos fundamentais e o acesso das autoridades públicas coreanas a dados transferidos com base na presente decisão, por forma a avaliar se a República da Coreia continua a assegurar um nível de proteção adequado na aceção do artigo 1.º.

([387]) Parecer 32/2021 sobre o projeto de decisão de execução da Comissão Europeia nos termos do Regulamento (UE) 2016/679 relativa à adequação do nível de proteção de dados pessoais na República da Coreia, disponível na seguinte ligação: https://edpb.europa.eu/our-work-tools/our-documents/opinion-art-70/opinion-322021-regarding-european-commission-draft_en.

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 coreana competente, deixe de cumprir o quadro jurídico em que assenta a presente decisão.

3. Os Estados-Membros e a Comissão devem comunicar-se reciprocamente quaisquer informações relativas a indícios de que a ingerência das autoridades públicas coreanas 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. Três anos após a data de notificação da presente decisão aos Estados-Membros e, subsequentemente, pelo menos de quatro em quatro anos, a Comissão deve avaliar a verificação referida no artigo 1.º, n.º 1, com base em todas as informações disponíveis, incluindo as recebidas no âmbito da avaliação realizada em conjunto com as autoridades coreanas 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 coreanas competentes. Se necessário, poderá decidir suspender, alterar ou revogar a presente decisão ou limitar o respetivo âmbito de aplicação, em conformidade com o disposto no artigo 45.º, n.º 5, do Regulamento (UE) 2016/679, sobretudo se tiver indícios de que:

a) Os responsáveis pelo tratamento na Coreia que receberam dados pessoais da União Europeia nos termos da presente decisão não respeitam as garantias adicionais constantes do anexo I, ou de que a supervisão e a aplicação coerciva nesta matéria são insuficientes;

b) As autoridades públicas coreanas não cumprem as declarações, garantias e compromissos constantes do anexo II, nomeadamente 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 coreanas para efeitos de aplicação do direito penal e de segurança nacional.

A Comissão pode igualmente adotar as referidas medidas se a falta de cooperação do Governo coreano a impedir de determinar se a República da Coreia continua a assegurar um nível de proteção adequado.

Artigo 4.º

Os destinatários da presente decisão são os Estados-Membros.

Feito em Bruxelas, em 17 de dezembro de 2021.

Pela Comissão
Didier REYNDERS
Membro da Comissão

ANEXO I

NORMAS COMPLEMENTARES PARA A INTERPRETAÇÃO E APLICAÇÃO DA LEI RELATIVA À PROTEÇÃO DE INFORMAÇÕES PESSOAIS RELACIONADAS COM O TRATAMENTO DE DADOS PESSOAIS TRANSFERIDOS PARA A COREIA

Índice

I. **Síntese**

A Coreia e a União Europeia (a seguir designada por «UE») têm conduzido discussões em matéria de adequação, em resultado das quais a Comissão Europeia determinou que a Coreia está a garantir um nível adequado de proteção de dados pessoais em conformidade com o artigo 45.º do RGPD.

Neste contexto, a Comissão de Proteção de Informações Pessoais adotou esta notificação com base no artigo 5.º (Obrigações de Estado, etc.) e no artigo 14.º (Cooperação internacional) ([1]) da Lei relativa à proteção de informações pessoais, a fim de clarificar a interpretação, a aplicação e a execução de determinadas disposições da lei, incluindo no que se refere ao tratamento de dados pessoais transferidos para a Coreia com base na decisão de adequação da UE.

Como a presente notificação tem o estatuto de norma administrativa que o serviço administrativo competente estabelece e anuncia para clarificar as normas de interpretação, aplicação e execução da Lei relativa à proteção de informações pessoais no sistema jurídico da Coreia, tem força jurídica vinculativa em relação ao responsável pelo tratamento de informações pessoais no sentido de que qualquer violação desta notificação pode ser considerada como uma violação das disposições relevantes da Lei relativa à proteção de informações pessoais. Além disso, se os direitos e interesses pessoais forem violados devido a uma violação da presente notificação, os indivíduos afetados têm direito a obter reparação junto da Comissão de Proteção de Informações Pessoais ou dos tribunais.

Assim, se o responsável pelo tratamento das informações pessoais, que trata as informações pessoais transferidas para a Coreia de acordo com a decisão de adequação da UE, não tomar medidas em conformidade com a presente notificação, considerar-se-á «que existe um motivo substancial para considerar que se verificou uma infração no que respeita às informações pessoais, e a não tomada de medidas é suscetível de causar danos difíceis de reparar», nos termos do artigo 64.º, n.os 1 e 2, da lei. Nesses casos, a Comissão de Proteção de Informações Pessoais ou os serviços administrativos centrais conexos podem ordenar ao responsável pelo tratamento das informações pessoais em causa que tome

([1]) O artigo 14.º da Lei relativa à proteção de informações pessoais determina que a autoridade do Governo da Coreia estabelece políticas destinadas a melhorar o nível de proteção das informações pessoais no contexto internacional e prevenir a violação dos direitos dos titulares dos dados decorrente da transferência transfronteiriça de informações pessoais.

medidas corretivas, etc., de acordo com a autoridade conferida por esta disposição, e, dependendo de violações específicas da lei, podem também ser impostas penas correspondentes (sanções, coimas, etc.).

II. **Definição dos termos**

São as seguintes as definições dos termos utilizados na presente disposição:

(i) Lei: Lei relativa à proteção de informações pessoais (Lei n.º 16930, alterada em 4 de fevereiro de 2020 e que entrou em vigor em 5 de agosto de 2020);

(ii) Decreto Presidencial: Decreto de Execução da Lei relativa à proteção de informações pessoais (Decreto Presidencial n.º 30509, de 3 de março de 2020, que altera outras leis);

(iii) Titular dos dados: uma pessoa singular identificável através da informação tratada nos presentes termos para se tornar o titular dessas informações;

(iv) Responsável pelo tratamento das informações pessoais: uma instituição pública, pessoa coletiva, organização, pessoa singular, etc. que trata informações pessoais, direta ou indiretamente, como parte das respetivas atividades;

(v) UE: a UE (a partir do final de fevereiro de 2020, os 27 Estados-Membros da UE [2], nomeadamente Bélgica, Alemanha, França, Itália, Luxemburgo, Países Baixos, Dinamarca, Irlanda, Grécia, Portugal, Espanha, Áustria, Finlândia, Suécia, Chipre, Chéquia, Estónia, Hungria, Letónia, Lituânia, Malta, Polónia, Eslováquia, Eslovénia, Roménia, Bulgária e Croácia) bem como os países associados à UE através do Acordo EEE (Islândia, Listenstaine e Noruega);

(vi) RGPD: A lei geral da UE relativa à proteção de informações pessoais, Regulamento Geral sobre a Proteção de Dados [Regulamento (UE) 2016/679];

(vii) Decisão de adequação: decisão tomada pela Comissão Europeia, em conformidade com o n.º 3 do artigo 45.º do RGPD, de que um país terceiro, o território de um país terceiro, uma ou mais áreas ou uma organização internacional garantem um nível adequado de proteção das informações pessoais.

III. **Normas complementares**

1. **Limitação da utilização indevida e do fornecimento de informações pessoais (artigos 3.º, 15.º e 18.º da lei)**

<Lei relativa à proteção de informações pessoais

(Lei n.º 16930, parcialmente alterada em 4 de fevereiro de 2020)>

Artigo 3.º (Princípios em matéria de proteção de informações pessoais) 1) O responsável pelo tratamento das informações pessoais deve especificar explicitamente as finalidades para as quais as informações pessoais são tratadas, bem como recolher as informações pessoais de forma lícita e leal, na medida mínima necessária para essas finalidades.

2. O responsável pelo tratamento das informações pessoais deve tratar as informações pessoais de forma adequada e necessária para as finalidades para as quais as informações pessoais são tratadas, e não deve utilizá-las para além dessas finalidades.

Artigo 15.º (Recolha e utilização de informações pessoais) 1) O responsável pelo tratamento das informações pessoais pode recolher informações pessoais em qualquer uma das seguintes circunstâncias, e utilizá-las no âmbito da finalidade para que foram recolhidas:

1. Sempre que seja obtido o consentimento de um titular de dados;

2. Sempre que existam disposições especiais na legislação ou seja inevitável o cumprimento de obrigações legais;

3. Sempre que seja inevitável para o exercício das funções de uma instituição pública sob a sua jurisdição, conforme estipulado por lei, etc.;

4. Sempre que seja inevitavelmente necessário celebrar e executar um contrato com um titular de dados;

[2] Até ao final do período de transição, estes também incluem o Reino Unido, conforme previsto nos artigos 126.º, 127.º e 132.º do Acordo sobre a saída do Reino Unido da Grã-Bretanha e da Irlanda do Norte da União Europeia e da Comunidade Europeia da Energia Atómica (2019/C 384 I/01).

5. Sempre que seja considerado manifestamente necessário para a proteção dos interesses vitais, corporais ou materiais do titular dos dados ou de terceiros contra perigo iminente, quando o titular dos dados ou o seu representante legal não estiver em condições de exprimir a sua intenção, ou quando não for possível obter o consentimento prévio devido a endereços desconhecidos, etc.;

6. Sempre que seja necessário satisfazer o interesse justificável de um responsável pelo tratamento de informações pessoais, interesse esse manifestamente superior aos direitos do titular dos dados. Nesses casos, o tratamento só será permitido na medida em que esteja substancialmente relacionado com o interesse justificável do responsável pelo tratamento das informações pessoais e não exceda um âmbito razoável.

Artigo 18.º (Limitação da utilização indevida e do fornecimento de informações pessoais) 1) O responsável pelo tratamento das informações pessoais não deve utilizar informações pessoais para além do âmbito previsto no artigo 15.º, n.º 1, e no artigo 39.º-3, n.ºs 1 e 2, ou fornecê-las a terceiros para além do âmbito previsto no artigo 17.º, n.ºs 1 e 3.

2) Não obstante o disposto no n.º 1, sempre que se aplique qualquer um dos parágrafos seguintes, o responsável pelo tratamento das informações pessoais poderá utilizar informações pessoais ou fornecê-las a terceiros para outras finalidades, salvo se tal for suscetível de infringir injustamente os interesses do titular dos dados ou de terceiros: desde que os prestadores de serviços de informação e comunicação [conforme estabelecido no artigo 2.º, n.º 1, ponto 3, da Lei relativa à promoção da utilização das redes de informação e comunicação e à proteção da informação, etc.; deste ponto em diante o mesmo se aplica], que tratam as informações pessoais dos utilizadores [conforme estabelecido no artigo 2.º, n.º 1, ponto 4, da Lei relativa à promoção da utilização das redes de informação e comunicação e à proteção da informação, etc.; deste ponto em diante o mesmo se aplica] estejam apenas sujeitos aos primeiro e segundo parágrafos, e o quinto ao nono parágrafos sejam apenas aplicáveis às instituições públicas:

1. Sempre que seja obtido o consentimento adicional de um titular de dados;

2. Sempre que existam outras disposições especiais na legislação;

3. Sempre que seja considerado manifestamente necessário para a proteção dos interesses vitais, corporais ou materiais do titular dos dados ou de terceiros contra perigo iminente, quando o titular dos dados ou o seu representante legal não estiver em condições de exprimir a sua intenção, ou quando não for possível obter o consentimento prévio devido a endereços desconhecidos;

4. Eliminado;<pela Lei n.º 16930, de 4 de fevereiro de 2020>

5. Sempre que seja impossível desempenhar as funções sob a sua jurisdição, conforme previsto em qualquer lei, a menos que o responsável pelo tratamento das informações pessoais utilize informações pessoais para outra finalidade distinta da prevista ou as forneça a terceiros, e estas estejam sujeitas à deliberação e resolução da Comissão;

6. Sempre que seja necessário fornecer informações pessoais a um governo estrangeiro ou organização internacional para a celebração de um tratado ou outra convenção internacional;

7. Sempre que seja necessário para a investigação de um crime, para um despacho de acusação e para ação penal;

8. Sempre que seja necessário para que um tribunal desempenhe funções relacionadas com julgamentos;

9. Sempre que seja necessário para a aplicação de penas, colocação sob controlo judiciário ou detenção.

Omitidos os n.ºs 3 e 4

5) Sempre que um responsável pelo tratamento das informações pessoais fornecer informações pessoais a terceiros para outra finalidade distinta da prevista no n.º 2, o responsável pelo tratamento das informações pessoais deve solicitar ao destinatário das informações pessoais que limite a finalidade e o método de utilização e outras questões necessárias, ou que prepare as garantias necessárias para a segurança das informações pessoais. Nesses casos, a pessoa que recebe tal pedido deve tomar as medidas necessárias para garantir a segurança das informações pessoais.

i) O artigo 3.º, n.ºs 1 e 2, da Lei prescreve o princípio de que um responsável pelo tratamento de informações pessoais deve recolher apenas as informações pessoais mínimas necessárias para o cumprimento da finalidade do tratamento das informações pessoais de forma lícita e legal, e não as deve utilizar para outra finalidade distinta da prevista ([3]).

ii) De acordo com este princípio, o n.º 1 do artigo 15.º da lei estipula que quando um responsável pelo tratamento de informações pessoais recolhe informações pessoais, as informações pessoais podem ser utilizadas no âmbito da finalidade para que foram recolhidas, e o n.º 1 do artigo 18.º estipula que as informações pessoais não devem ser utilizadas para além da finalidade para que foram recolhidas nem fornecidas a terceiros.

([3]) Como estas disposições estabelecem princípios gerais que se aplicam a qualquer tratamento de informações pessoais, incluindo quando esse tratamento é especificamente regulado por outras leis, os esclarecimentos constantes do presente ponto aplicam-se também quando os dados pessoais são tratados com base noutras leis (ver, por exemplo, artigo 15.º, n.º 1, da Lei relativa a informações de crédito, que se refere especificamente a estas disposições).

iii) Por outro lado, mesmo que as informações pessoais possam ser utilizadas para finalidades distintas das previstas ou fornecidas a terceiros nos casos excecionais ([4]) descritos nos parágrafos do artigo 18.º, n.º 2, da lei, deve ser solicitado que a finalidade ou método de utilização seja restringido para que as informações pessoais possam ser tratadas com segurança de acordo com o n.º 5, ou sejam tomadas as medidas necessárias para garantir a segurança das informações pessoais.

iv) As disposições anteriores são igualmente aplicáveis ao tratamento de todas as informações pessoais recebidas de um país terceiro na área de jurisdição da Coreia, independentemente da nacionalidade do titular dos dados.

v) Por exemplo, se um responsável pelo tratamento de informações pessoais na UE transferir informações pessoais para um responsável pelo tratamento de informações pessoais coreano de acordo com a decisão de adequação da Comissão Europeia, a finalidade da transferência das informações pessoais pelo responsável pelo tratamento da UE será considerada a finalidade de recolha das informações pessoais pelo responsável pelo tratamento de informações pessoais coreano e, nesses casos, o responsável pelo tratamento de informações pessoais coreano só poderá utilizar as informações pessoais ou fornecê-las a terceiros para fins de recolha, exceto nos casos excecionais descritos nos parágrafos do artigo 18.º, n.º 2, da lei.

2. **Limitação da transferência subsequente de dados pessoais (artigo 17.º, n.ºs 3 e 4, e artigo 18.º da lei)**

<Lei relativa à proteção de informações pessoais

(Lei n.º 16930, parcialmente alterada em 4 de fevereiro de 2020)>

Artigo 17.º (Fornecimento de informações pessoais) 1) Suprimir

2) Um responsável pelo tratamento de informações pessoais deve informar o titular dos dados das seguintes questões quando obtiver o consentimento previsto no n.º 1, ponto 1. O mesmo se aplica quando qualquer um dos seguintes elementos for modificado:

1. O destinatário das informações pessoais;
2. A finalidade para a qual o destinatário das informações pessoais utiliza tais informações;
3. Os elementos das informações pessoais a fornecer;
4. O período durante o qual o destinatário conserva e utiliza as informações pessoais;
5. O facto de o titular dos dados ter o direito de recusar o consentimento e as desvantagens, se as houver, resultantes da recusa de consentimento.

3) Um responsável pelo tratamento de informações pessoais deve informar o titular dos dados das questões previstas no n.º 2 e obter o consentimento do titular dos dados, a fim de fornecer informações pessoais a terceiros no estrangeiro; e não deve celebrar qualquer contrato para a transferência transfronteiriça de informações pessoais em violação da presente lei.

4) Um responsável pelo tratamento de informações pessoais pode fornecer informações pessoais sem o consentimento do titular dos dados no âmbito razoavelmente relacionado com as finalidades para as quais as informações pessoais foram inicialmente recolhidas, de acordo com as matérias prescritas pelo Decreto Presidencial, tendo em consideração se são causadas desvantagens ao titular dos dados, se foram tomadas as medidas necessárias para garantir a segurança, designadamente a encriptação, etc.

※ Ver as páginas 3, 4 e 5 relativas ao artigo 18.º.

< **Decreto de Execução da Lei relativa à proteção de informações pessoais**

([Data de aplicação: 5 de fevereiro de 2021.] [Decreto Presidencial n.º 30892, de 4 de agosto de 2020, que altera outras leis])>

Artigo 14.º-2 (Normas relativas à utilização/fornecimento adicional de informações pessoais, etc.)

1) Se um responsável pelo tratamento de informações pessoais utilizar ou fornecer informações pessoais (a seguir designado por «utilização ou prestação adicional de informações pessoais») sem o consentimento do titular dos dados nos termos do artigo 15.º, n.º 3, da lei ou do artigo 17.º, n.º 4, da lei, o responsável pelo tratamento das informações pessoais deve considerar as seguintes questões:

1. Se está razoavelmente relacionado com a finalidade original para a qual as informações pessoais foram recolhidas;
2. Se é previsível uma utilização ou fornecimento adicional de informações pessoais à luz das circunstâncias em que as informações pessoais foram recolhidas e das práticas de tratamento;
3. Se a utilização ou o fornecimento adicional de informações pessoais não infringe injustamente os interesses do titular dos dados; e
4. Se foram tomadas as medidas necessárias para garantir a segurança, tais como a pseudonimização ou a encriptação.

([4]) Os prestadores de serviços de comunicação de informações estão apenas sujeitos ao artigo 18.º, n.º 2, primeiro e segundo parágrafos. O quinto ao nono parágrafos apenas se aplicam às instituições públicas.

2) O responsável pelo tratamento das informações pessoais deve divulgar previamente os critérios de avaliação das questões referidas nos parágrafos do n.º 1 da Política de Privacidade, nos termos do artigo 30.º, n.º 1, da lei, e o diretor de privacidade, nos termos do artigo 31.º, n.º 1, da lei, deve verificar se o responsável pelo tratamento das informações pessoais utiliza ou fornece informações pessoais adicionais em conformidade com as normas pertinentes.

i) Se o responsável pelo tratamento das informações pessoais fornecer informações pessoais a terceiros no estrangeiro, deve informar previamente os titulares dos dados de todas as questões descritas no artigo 17.º, n.º 2, da lei e obter o seu consentimento, exceto nos casos abrangidos pelos n.ºs 1 ou 2. Não deve ser celebrado qualquer contrato relativo ao fornecimento transfronteiriço de dados pessoais em violação da desta lei.

(1) Se as informações pessoais forem fornecidas no âmbito razoavelmente relacionado com a finalidade inicial para a qual as informações foram recolhidas, nos termos do artigo 17.º, n.º 4, da lei. Contudo, os casos a que esta disposição pode ser aplicada limitam-se aos casos em que as normas relativas à utilização e ao fornecimento adicional de informações pessoais, estabelecidas no artigo 14.º-2 do decreto de execução, são cumpridas. Além disso, o responsável pelo tratamento das informações pessoais deve considerar se o fornecimento de informações pessoais pode causar desvantagens aos titulares dos dados e se tomou as medidas necessárias para garantir a segurança, designadamente, a encriptação.

(2) Se for possível fornecer informações pessoais a terceiros nos casos excecionais mencionados no artigo 18.º, n.º 2, da lei (ver p. 3 a 5). Contudo, mesmo nesses casos, se o fornecimento de tais informações pessoais for suscetível de infringir injustamente os interesses do titular dos dados ou de um terceiro, as informações pessoais não podem ser fornecidas a um terceiro. Além disso, o fornecedor de informações pessoais deve solicitar ao destinatário das informações pessoais que limite a finalidade ou o método de utilização das informações pessoais ou tome as medidas necessárias para garantir a sua segurança, de modo que as informações pessoais possam ser tratadas com segurança.

ii) Se as informações pessoais forem fornecidas a terceiros no estrangeiro, podem não receber o nível de proteção garantido pela Lei relativa à proteção de informações pessoais da Coreia devido a diferenças nos sistemas de proteção de informações pessoais de diferentes países. Consequentemente, esses casos serão considerados como «casos em que podem ser causadas desvantagens ao titular dos dados», mencionados no artigo 17.º, n.º 4, da lei, ou «casos em que o interesse de um titular de dados ou de um terceiro é injustamente violado», mencionados no artigo 18.º, n.º 2, da lei e no artigo 14.º-2 do decreto de execução da mesma lei ([5]). Para cumprir os requisitos destas disposições, o responsável pelo tratamento das informações pessoais e os terceiros devem, por conseguinte, assegurar explicitamente um nível de proteção equivalente ao da lei, incluindo a garantia do exercício dos direitos do titular dos dados em documentos juridicamente vinculativos, tais como contratos, mesmo após a transferência das informações pessoais para o estrangeiro.

3. **Notificação relativa aos dados quando não tenham sido obtidos dados pessoais do titular dos dados (artigo 20.º da lei)**

<Lei relativa à proteção de informações pessoais

(Lei n.º 16930, parcialmente alterada em 4 de fevereiro de 2020)>

Artigo 20.º (Notificação sobre fontes, etc. de informações pessoais recolhidas de terceiros) 1) Quando um responsável pelo tratamento de informações pessoais tratar informações pessoais recolhidas de terceiros, o responsável pelo tratamento das informações pessoais notificará imediatamente o titular dos dados das seguintes questões, a pedido desse titular de dados:

1. A fonte das informações pessoais recolhidas;

2. A finalidade do tratamento das informações pessoais;

3. O facto de o titular dos dados ter o direito de exigir a suspensão do tratamento das informações pessoais, conforme estipulado no artigo 37.º.

2) Não obstante o disposto no n.º 1, quando um responsável pelo tratamento de informações pessoais que cumpra os critérios estipulados no decreto presidencial, tendo em conta os tipos e quantidade de informações pessoais tratadas, o número de empregados, o volume de vendas, etc., recolhe informações pessoais de terceiros e as trata nos termos do artigo 17.º, n.º 1, ponto 1, o responsável pelo tratamento das informações pessoais notificará a pessoa em causa das questões referidas no n.º 1): desde que tal não se aplique quando as informações recolhidas pelo responsável pelo tratamento das informações pessoais não contenham quaisquer informações pessoais, como dados de contacto, através das quais possa ser feita a notificação ao titular dos dados.

([5]) Nos termos do artigo 18.º, n.º 2, ponto 2, da Lei relativa à proteção de informações pessoais, tal também se aplica quando as informações pessoais são divulgadas a terceiros no estrangeiro com base nas disposições de outras leis (por exemplo, a Lei relativa às informações de crédito).

3) As questões necessárias em relação ao prazo, método e procedimento de notificação ao titular dos dados, nos termos da frase principal do n.º 2, serão estipulados em decreto presidencial.

4) O n.º 1 e a cláusula principal do n.º 2 não são aplicáveis a nenhuma das seguintes circunstâncias: desde que seja o caso apenas quando for manifestamente superior aos direitos dos titulares de dados nos termos da presente lei:

1. Sempre que as informações pessoais, objeto de um pedido de notificação, estiverem incluídas nos ficheiros de informações pessoais a que se refere qualquer uma das alíneas do artigo 32.º, n.º 2;

2. Sempre que tal notificação seja suscetível de lesar a vida ou a integridade física de qualquer outra pessoa, ou prejudicar injustamente os bens e outros interesses de qualquer outra pessoa.

(i) Se o responsável pelo tratamento das informações pessoais receber as informações pessoais transferidas da UE com base na sua decisão de adequação ([6]), deve notificar o titular dos dados das informações seguintes, constantes dos pontos 1) a 5), sem atraso injustificado e, em qualquer caso, o mais tardar um mês após a transferência.

(1) O nome e os dados de contacto das pessoas que transferem e recebem as informações pessoais;

(2) Os elementos ou categorias das informações pessoais transferidas;

(3) A finalidade da recolha e utilização das informações pessoais (conforme estabelecido pelo exportador de dados nos termos do ponto 1 da presente notificação);

(4) O período de conservação das informações pessoais;

(5) Informações sobre os direitos do titular dos dados relativamente ao tratamento das informações pessoais, o método e o procedimento de exercício dos direitos e as eventuais desvantagens que o seu exercício possa causar.

(ii) Além disso, se o responsável pelo tratamento das informações pessoais fornecer as informações pessoais indicadas em i) a terceiros na República da Coreia ou no estrangeiro, deve notificar o titular dos dados das informações seguintes, constantes dos pontos 1) a 5), antes de as informações pessoais serem fornecidas.

(1) O nome e os dados de contacto das pessoas que fornecem e recebem as informações pessoais;

(2) Os elementos ou categorias das informações pessoais fornecidas;

(3) O país ao qual as informações pessoais serão fornecidas, a data prevista e o método de fornecimento das mesmas (limitados aos casos em que as informações pessoais sejam fornecidas a terceiros no estrangeiro);

(4) A finalidade e a base jurídica do fornecedor de informações pessoais para o fornecimento das informações pessoais;

(5) Informações sobre os direitos do titular dos dados relativamente ao tratamento das informações pessoais, o método e o procedimento de exercício dos direitos e as eventuais desvantagens que o seu exercício possa causar.

(iii) O responsável pelo tratamento das informações pessoais não pode aplicar o disposto nas alíneas i) ou ii) em qualquer dos casos enunciados de 1) a 4).

(1) Se as informações pessoais a notificar forem incluídas em qualquer um dos seguintes ficheiros de informações pessoais mencionados no artigo 32.º, n.º 2, da lei, na medida em que os interesses protegidos por esta disposição sejam manifestamente superiores aos direitos do titular dos dados, e apenas na medida em que a notificação ameace a prossecução dos interesses em causa, por exemplo, pondo em risco investigações criminais em curso ou ameaçando a segurança nacional.

(2) Se e na medida em que a notificação for suscetível de lesar a vida ou a integridade física de outra pessoa, ou de infringir injustamente os interesses materiais de outra pessoa, quando esses direitos ou interesses forem manifestamente superiores aos direitos do titular dos dados.

(3) Se o titular dos dados já possuir as informações que o responsável pelo tratamento das informações pessoais deve notificar de acordo com a alínea i) ou ii).

(4) Se o responsável pelo tratamento das informações pessoais não possuir quaisquer dados de contacto do titular dos dados ou se o contacto com o titular dos dados envolver esforços excessivos, incluindo no contexto do tratamento nas condições estabelecidas na secção 3 da Lei relativa à proteção de informações pessoais. Para determinar se é ou não possível contactar o titular dos dados, ou se tal envolve esforços excessivos, deve ser tida em conta a possibilidade de cooperação com o exportador de dados na UE.

([6]) As obrigações previstas em i), ii) e iii) aplicam-se igualmente quando o responsável pelo tratamento que recebe informações pessoais da UE com base na decisão de adequação trata essas informações com base noutras leis, como, por exemplo, a Lei relativa às informações de crédito.

4. **Âmbito de aplicação da isenção especial ao tratamento de informações pseudonimizadas (artigos 28.º-2, 28.º--3, 28.º-4, 28.º-5, 28.º-6 e 28.º-7, artigo 3.º e artigo 58.º-2 da lei)**

<Lei relativa à proteção de informações pessoais

(Lei n.º 16930, parcialmente alterada em 4 de fevereiro de 2020)>

Capítulo III Tratamento das informações pessoais

SECÇÃO 3 Casos especiais respeitantes a dados apresentados sob pseudónimo

Artigo 28.º-2 (Tratamento de dados apresentados sob pseudónimo) 1) Um responsável pelo tratamento de informações pessoais pode tratar informações pseudonimizadas sem o consentimento dos titulares dos dados para fins estatísticos, de investigação científica e de arquivo no interesse público, etc.

2) Um responsável pelo tratamento de informações pessoais não deve incluir informações que possam ser utilizadas para identificar uma determinada pessoa singular quando fornecer informações pseudonimizadas a terceiros, nos termos do n.º 1.

Artigo 28.º-3 (Restrição à combinação de dados apresentados sob pseudónimo) 1) Não obstante o artigo 28.º-2, a combinação de informações pseudonimizadas tratadas por diferentes responsáveis pelo tratamento de informações pessoais para fins estatísticos, de investigação científica e de preservação de registos de interesse público, etc. será conduzida por uma instituição especializada, designada pela Comissão de Proteção ou pelo chefe do serviço administrativo central relacionado.

2) Um responsável pelo tratamento de informações pessoais que pretenda divulgar as informações combinadas fora da organização que as combinou deve obter a aprovação do chefe da instituição especializada após o tratamento das informações, a fim de as pseudonimizar ou na forma a que se refere o artigo 58.º-2.

3) As questões necessárias, incluindo os procedimentos e métodos de combinação nos termos do n.º 1, as normas e procedimentos para designar ou cancelar a designação de uma instituição especializada de gestão e supervisão, e as normas e procedimentos de exportação e aprovação nos termos do n.º 2, serão estipulados em decreto presidencial.

Artigo 28.º-4 (Obrigação de tomar medidas de segurança no caso de dados apresentados sob pseudónimo) 1) Ao tratar as informações pseudonimizadas, um responsável pelo tratamento de informações pessoais deve tomar as medidas técnicas, organizacionais e físicas necessárias para conservar e gerir separadamente as informações adicionais necessárias à reposição do estado original, conforme necessário para garantir a segurança, tal como estipulado em decreto presidencial, de modo que as informações pessoais não possam ser extraviadas, roubadas, divulgadas, falsificadas, alteradas ou danificadas.

2) Um responsável pelo tratamento de informações pessoais que pretenda tratar as informações pseudonimizadas deve preparar e manter registos relacionados com as matérias estipuladas pelo Decreto Presidencial, incluindo a finalidade do tratamento das informações pseudonimizadas, e um terceiro destinatário quando são fornecidas informações pseudonimizadas, para gerir o tratamento das informações pseudonimizadas.

Artigo 28.º-5 (Atos proibidos no tratamento de informações pseudonimizadas) 1) Ninguém pode tratar as informações pseudonimizadas para efeitos de identificar uma determinada pessoa singular.

2) Quando as informações que identificam uma determinada pessoa singular são geradas enquanto as informações pseudonimizadas são tratadas, o responsável pelo tratamento das informações pessoais deve terminar o tratamento das informações, bem como recuperar e destruir imediatamente as informações.

Artigo 28.º-6 (Imposição de sobretaxas administrativas para o tratamento de informações pseudonimizadas) 1) A Comissão pode impor uma coima não superior a três centésimos do total das vendas ao responsável pelo tratamento de dados que tenha tratado dados para efeitos de identificar uma determinada pessoa singular, em violação do artigo 28.º-5, n.º 1: Desde que, no caso de não existirem vendas ou de existirem dificuldades no cálculo das receitas das vendas, o responsável pelo tratamento dos dados possa ser sujeito a uma multa não superior a 400 milhões ganhos ou a três centésimos do montante do capital, consoante o que for maior.

2) O artigo 34.º-2, n.os 3 a 5, é aplicável, com as devidas adaptações, às questões necessárias para impor e cobrar sobretaxas administrativas.

Artigo 28.º-7 (Âmbito de aplicação) 1) Os artigos 20.º, 21.º e 27.º, o artigo 34.º, n.º 1, os artigos 35.º a 37.º e os artigos 39.º-3, 39.º-4, 39.º-6 a 39.º-8 não se aplicam às informações pseudonimizadas.

Capítulo I Disposições gerais

Artigo 3.º (Princípios em matéria de proteção de informações pessoais) 1) O responsável pelo tratamento das informações pessoais deve especificar explicitamente as finalidades para as quais as informações pessoais são tratadas, bem como recolher as informações pessoais de forma lícita e leal, na medida mínima necessária para essas finalidades.

2. O responsável pelo tratamento das informações pessoais deve tratar as informações pessoais de forma adequada e necessária para as finalidades para as quais as informações pessoais são tratadas, e não deve utilizá-las para além dessas finalidades.

3) O responsável pelo tratamento das informações pessoais deve assegurar que estas sejam exatas, completas e atualizadas, na medida necessária para as finalidades para que são tratadas.

4) O responsável pelo tratamento das informações pessoais deve gerir com segurança as informações pessoais de acordo com os métodos de tratamento, tipos, etc. de informações pessoais, tendo em conta a possibilidade de violação dos direitos do titular dos dados e a gravidade dos riscos pertinentes.

5) O responsável pelo tratamento das informações pessoais deve tornar pública a sua política de privacidade e outras questões relacionadas com o tratamento das informações pessoais, bem como garantir os direitos do titular dos dados, nomeadamente o direito de acesso às suas informações pessoais.

6) O responsável pelo tratamento das informações pessoais deve tratar as informações pessoais de uma forma que minimize a possibilidade de violação da privacidade de um titular de dados.

7) Se continuar a ser possível cumprir as finalidades da recolha de informações pessoais através do processamento de informações pessoais anonimizadas ou pseudonimizadas, o responsável pelo tratamento das informações pessoais deve esforçar-se por tratar as informações pessoais através da anonimização, sempre que esta seja possível, ou através da pseudonimização, se for impossível cumprir as finalidades da recolha de informações pessoais através da anonimização.

8) O responsável pelo tratamento das informações pessoais deve esforçar-se por obter a confiança dos titulares de dados, observando e desempenhando as funções e responsabilidades previstas na presente lei e noutra legislação conexa.

CAPÍTULO IX Disposições complementares

Artigo 58.º (Isenção da aplicação) A presente lei não se aplica às informações que tenham deixado de identificar uma determinada pessoa singular quando combinadas com outras informações, considerando razoavelmente o prazo, o custo, a tecnologia, etc. <Este artigo foi recentemente inserido pela Lei n.º 16930, de 4 de fevereiro de 2020.>

i) O capítulo III, secção 3 – Casos especiais respeitantes a dados apresentados sob pseudónimo (artigos 28.º-2 a 28.º-7) permite o tratamento de informações pseudonimizadas sem o consentimento do titular dos dados para fins de compilação de estatísticas, investigação científica, preservação de registos públicos, etc. (artigo 28.º-2), mas nesses casos são obrigatórias garantias e proibições adequadas necessárias para proteger os direitos os titulares dos dados (artigos 28.º-4 e 28.º-5), podem ser impostas sanções aos infratores (artigo 28.º-6) e não se aplicam certas garantias de outro modo disponíveis ao abrigo da Lei relativa à proteção de informações pessoais (artigo 28.º-7).

ii) Estas disposições não se aplicam aos casos em que as informações pseudonimizadas são tratadas para finalidades distintas da compilação de estatísticas, da investigação científica, da preservação de registos públicos, etc. Por exemplo, se as informações pessoais de uma pessoa singular da UE, que tenham sido transferidas para a Coreia de acordo com a decisão de adequação da Comissão Europeia, forem pseudonimizadas para finalidades distintas da compilação de estatísticas, da investigação científica, da preservação de registos públicos, etc., as disposições especiais do capítulo III, secção 3, não se aplicam ([7]).

iii) Quando um responsável pelo tratamento de informações pessoais trata informações pseudonimizadas para fins de compilação de estatísticas, investigação científica, preservação de registos públicos, etc., e se as informações pseudonimizadas não tiverem sido destruídas uma vez cumprida a finalidade específica do tratamento, nos termos do artigo 37.º da Constituição e do artigo 3.º (Princípios em matéria de proteção de informações pessoais) da lei, deve anonimizar as informações com vista a assegurar que estas deixem de identificar uma pessoa singular específica, isoladamente ou quando combinadas com outras informações, considerando razoavelmente o prazo, o custo, a tecnologia, etc., em conformidade com o artigo 58.º-2 da Lei relativa à proteção de informações pessoais.

5. **Medidas corretivas, etc. (artigo 64.º, n.os 1, 2 e 4, da lei)**

<Lei relativa à proteção de informações pessoais

(Lei n.º 16930, parcialmente alterada em 4 de fevereiro de 2020)>

Artigo 64.º (Medidas corretivas) 1) Sempre que a Comissão de Proteção entenda que existe um motivo substancial para considerar que se verificou uma infração no que respeita às informações pessoais, e que a não adoção de medidas é suscetível de causar danos difíceis de reparar, poderá ordenar ao infrator da presente lei (excluindo os serviços administrativos centrais, os governos locais, a Assembleia Nacional, o Tribunal, o Tribunal Constitucional e a Comissão Nacional de Eleições) que tome qualquer uma das medidas seguintes:

1. A suspensão da infração respeitante às informações pessoais;

2. A suspensão temporária do tratamento das informações pessoais;

([7]) Da mesma forma, a exceção do artigo 40.º-3 da Lei relativa às informações de crédito só se aplica ao tratamento de informações de crédito pseudonimizadas para fins de compilação de estatísticas, investigação científica e preservação de registos públicos.

3. Outras medidas necessárias para proteger as informações pessoais e para prevenir a violação de informações pessoais.

2) Se o chefe de um serviço administrativo central relacionado considerar que há um motivo substancial para considerar que se verificou uma infração no que respeita às informações pessoais, e que a não tomada de medidas é suscetível de causar danos difíceis de reparar, pode ordenar a um responsável pelo tratamento de informações pessoais que tome qualquer uma das medidas previstas no n.º 1 nos termos da legislação abrangida pela jurisdição do referido serviço administrativo central relacionado.

4) Quando um serviço administrativo central, um governo local, a Assembleia Nacional, o Tribunal, o Tribunal Constitucional ou a Comissão Nacional de Eleições viola a presente lei, a Comissão de Proteção pode recomendar ao chefe do serviço em questão que tome qualquer uma das medidas previstas no n.º 1. Nesses casos, ao receber a recomendação, o serviço deve cumpri-la, a menos que se verifiquem circunstâncias extraordinárias.

i) Em primeiro lugar, há precedentes jurídicos ([8]), ([9]) que interpretam «danos difíceis de reparar» como uma situação que pode lesar os direitos pessoais ou a privacidade de uma pessoa singular.

ii) Por conseguinte, «um motivo válido para considerar que houve uma infração no que respeita às informações pessoais, e que a não adoção de medidas é suscetível de causar danos difíceis de reparar», estabelecido no artigo 64.º, n.ºs 1 e 2, refere-se a casos em que uma violação da lei é considerada como suscetível de violar os direitos e a liberdade das pessoas singulares no que diz respeito às informações pessoais. Tal aplica-se sempre que seja violado qualquer um dos princípios, direitos e deveres definidos na lei para proteger as informações pessoais ([10]).

iii) Nos termos do artigo 64.º, n.º 4, da Lei relativa à proteção de informações pessoais, existe uma medida relativa a «uma violação da presente lei», ou seja, a instauração de uma ação judicial contra uma violação da Lei relativa à proteção de informações pessoais.

Um serviço administrativo central, etc., enquanto autoridade pública vinculada ao Estado de direito, não pode violar a lei e é obrigado a adotar uma medida corretiva, nomeadamente pôr imediatamente termo à ação, e indemnizar os danos no caso excecional de um ato ilegal ter sido, mesmo assim, cometido.

Consequentemente, mesmo sem qualquer intervenção da Comissão de Proteção, nos termos do artigo 64.º, n.º 4, da Lei relativa à proteção de informações pessoais, um serviço administrativo central, etc., deve tomar uma medida corretiva contra as violações, se tiver conhecimento de qualquer violação da lei.

Em especial, sempre que a Comissão de Proteção tenha recomendado uma medida corretiva, será em regra objetivamente claro ao serviço administrativo central, etc. que violou a lei. Assim, para justificar por que razão considera que uma recomendação da Comissão de Proteção não deve ser seguida, um serviço administrativo central, etc. deve apresentar fundamentos claros que possam provar que não violou a lei. A recomendação deve ser seguida, a menos que a Comissão de Proteção determine que tal não é de facto o caso.

Tendo isto em consideração, as «circunstâncias extraordinárias» a que se refere o artigo 64.º, n.º 4, da Lei relativa à proteção de informações pessoais devem ser estritamente limitadas a circunstâncias extraordinárias em que existam motivos claros para os serviços administrativos centrais, etc. provarem que «a presente Lei não foi de facto violada», tais como «casos em que existam circunstâncias extraordinárias (factuais ou jurídicas)» que a Comissão de Proteção não conhecia quando formulou inicialmente a sua recomendação e a Comissão de Proteção determinar que, de facto, não ocorreu qualquer violação.

6. **Aplicação da Lei relativa à proteção de informações pessoais ao tratamento de dados pessoais para efeitos de segurança nacional, incluindo a investigação de infrações e a execução, em conformidade com a Lei relativa à proteção de informações pessoais (artigos 7.º-8 e 7.º-9 e artigos 58.º, 3.º, 4.º e 62.º da Lei relativa à proteção de informações pessoais)**

<Lei relativa à proteção de informações pessoais

(Lei n.º 16930, parcialmente alterada em 4 de fevereiro de 2020)>

Artigo 7.º-8 (Trabalho da Comissão de Proteção) 1) A Comissão de Proteção deve desempenhar o seguinte trabalho: […]

3. Questões relativas à investigação de violações do direito dos titulares de dados e as disposições daí decorrentes;

4. Tratamento de reclamações ou procedimentos de reparação relativos ao tratamento de informações pessoais e à mediação de litígios em matéria de informações pessoais;

[…]

([8]) (Acórdão do Supremo Tribunal de 26 de janeiro de 1999, 97Da10215,10222) Se os factos imputados ao arguido em processo penal forem revelados através dos meios de comunicação social, é provável que causem danos mentais e físicos irreparáveis não só à vítima, ou seja, ao autor, mas também às pessoas próximas deste, incluindo as famílias.

([9]) (Acórdão do Supremo Tribunal de Seul de 16 de janeiro de 2008, 2006Na92006) Se for publicado um artigo difamatório, é provável que cause danos graves e irreparáveis à pessoa envolvida.

([10]) Aplicam-se ao artigo 45.º-4 da Lei relativa às informações de crédito os mesmos princípios estabelecidos na subalínea ii).

Artigo 7.º-9 (Questões sujeitas a deliberação e resolução pela Comissão de Proteção) 1) A Comissão de Proteção delibera e decide nas matérias seguintes: […]

5. Questões relativas à interpretação e funcionamento da lei relacionada com a proteção de informações pessoais;

[…]

Artigo 58.º (Exclusão parcial de aplicação) 1) Os capítulos III a VII não se aplicam a nenhuma das seguintes informações pessoais:

1. Informações pessoais recolhidas nos termos da Lei relativa a estatísticas para tratamento por parte de instituições públicas;
2. Informações pessoais recolhidas ou solicitadas para a análise de informações relacionadas com a segurança nacional;
3. Informações pessoais tratadas temporariamente quando são urgentemente necessárias para a segurança e proteção pública, a saúde pública, etc.;
4. Informações pessoais recolhidas ou utilizadas para os seus próprios fins de divulgação pela imprensa, atividades missionárias por parte de organizações religiosas e nomeação de candidatos por partidos políticos, respetivamente.

[Omitidos os n.os 2 e 3]

4) No caso de tratamento de informações pessoais nos termos do n.º 1, um responsável pelo tratamento de informações pessoais deve tratar as informações pessoais na medida mínima necessária para atingir o objetivo pretendido durante o período de tempo mínimo, bem como tomar as medidas necessárias, tais como garantias técnicas, de gestão e físicas, tratamento de queixas individuais e outras medidas necessárias para a gestão segura e o tratamento adequado dessas informações pessoais.

Artigo 3.º (Princípios em matéria de proteção de informações pessoais) 1) O responsável pelo tratamento das informações pessoais deve especificar explicitamente as finalidades para as quais as informações pessoais são tratadas, bem como recolher as informações pessoais de forma lícita e leal, na medida mínima necessária para essas finalidades.

2. O responsável pelo tratamento das informações pessoais deve tratar as informações pessoais de forma adequada e necessária para as finalidades para as quais as informações pessoais são tratadas, e não deve utilizá-las para além dessas finalidades.

3) O responsável pelo tratamento das informações pessoais deve assegurar que estas sejam exatas, completas e atualizadas, na medida necessária para as finalidades para que são tratadas.

4) O responsável pelo tratamento das informações pessoais deve gerir com segurança as informações pessoais de acordo com os métodos de tratamento, tipos, etc. de informações pessoais, tendo em conta a possibilidade de violação dos direitos do titular dos dados e a gravidade dos riscos pertinentes.

5) O responsável pelo tratamento das informações pessoais deve tornar pública a sua política de privacidade e outras questões relacionadas com o tratamento das informações pessoais, bem como garantir os direitos do titular dos dados, nomeadamente o direito de acesso às suas informações pessoais.

6) O responsável pelo tratamento das informações pessoais deve tratar as informações pessoais de uma forma que minimize a possibilidade de violação da privacidade de um titular de dados.

7) Se continuar a ser possível cumprir as finalidades da recolha de informações pessoais através do processamento de informações pessoais anonimizadas ou pseudonimizadas, o responsável pelo tratamento das informações pessoais deve esforçar-se por tratar as informações pessoais através da anonimização, sempre que esta seja possível, ou através da pseudonimização, se for impossível cumprir as finalidades da recolha de informações pessoais através da anonimização.

8) O responsável pelo tratamento das informações pessoais deve esforçar-se por obter a confiança dos titulares de dados, observando e desempenhando as funções e responsabilidades previstas na presente lei e noutra legislação conexa.

Artigo 4.º (Direitos dos titulares de dados) Assistem a um titular de dados os seguintes direitos em relação ao tratamento das suas próprias informações pessoais:

1. O direito a ser informado sobre o tratamento dessas informações pessoais;
2. O direito de determinar se consente ou não e o âmbito do consentimento relativamente ao tratamento dessas informações pessoais;
3. O direito de confirmar se as informações pessoais estão ou não a ser tratadas e de solicitar acesso às mesmas (incluindo o fornecimento de cópias); deste ponto em diante o mesmo se aplica) a essas informações pessoais;
4. O direito de suspender o tratamento e de solicitar a retificação, apagamento e destruição dessas informações pessoais;
5. O direito à reparação adequada de quaisquer danos resultantes do tratamento dessas informações pessoais através de um procedimento rápido e justo.

Artigo 62.º (Denúncia de violações) 1) Qualquer pessoa que seja vítima de violação de direitos ou interesses relacionados com as suas informações pessoais no decurso do tratamento das informações pessoais por um responsável pelo tratamento de informações pessoais pode denunciar tal violação à Comissão de Proteção.

2) A Comissão de Proteção pode designar uma instituição especializada, a fim de receber e tratar eficazmente as denúncias, nos termos do n.º 1, conforme definido em decreto presidencial. Nesses casos, essa instituição especializada deve criar e operar um centro de atendimento para violações de informações pessoais (a seguir designado por «centro de atendimento para a privacidade»).

3) O centro de atendimento para a privacidade desempenhará as seguintes funções:

1. Receber denúncias e prestar aconselhamento em relação ao tratamento de informações pessoais;
2. Investigar e confirmar incidentes e ouvir opiniões de partes relacionadas;
3. Deveres relativos aos primeiro e segundo parágrafos.

4) A Comissão de Proteção pode, se necessário, enviar um funcionário público à instituição especializada designada nos termos do n.º 2, em conformidade com o artigo 32.º-4 da Lei relativa aos funcionários públicos do Estado, a fim de investigar e confirmar eficazmente os incidentes nos termos do n.º 3, ponto 2.

(i) a recolha de informações pessoais para fins de segurança nacional é regulada por leis específicas que habilitam as autoridades competentes (por exemplo, o Serviço Nacional de Informações) a intercetar comunicações ou a solicitar a sua divulgação mediante determinadas condições e garantias (a seguir designadas por «leis relativas à segurança nacional»). Estas leis relativas à segurança nacional incluem, por exemplo, a Lei relativa à proteção da privacidade das comunicações, a Lei antiterrorismo para a proteção dos cidadãos e da segurança pública ou a Lei relativa às atividades de telecomunicações. Além disso, a recolha e tratamento subsequente de informações pessoais tem de cumprir os requisitos da Lei relativa à proteção de informações pessoais. A este respeito, o artigo 58.º, n.º 1, ponto 2, da Lei relativa à proteção de informações pessoais prevê que os Capítulos III a VII não se aplicam às informações pessoais recolhidas ou solicitadas para a análise de informações relacionadas com a segurança nacional. Por conseguinte, esta exceção parcial aplica-se ao tratamento de informações pessoais para fins de segurança nacional.

Ao mesmo tempo, o capítulo I (Disposições gerais), o capítulo II (Estabelecimento de políticas de proteção de informações pessoais, etc.), o capítulo VIII (Ação coletiva por violação de dados), o capítulo IX (Disposições complementares) e o capítulo X (Disposições sancionatórias) da Lei relativa à proteção de informações pessoais aplicam-se ao tratamento de tais informações pessoais. Tal inclui os princípios gerais em matéria de proteção de dados estabelecidos no artigo 3.º (Princípios em matéria de proteção de informações pessoais) e os direitos individuais garantidos pelo artigo 4.º da Lei relativa à proteção de informações pessoais (Direitos dos titulares de dados).

Além disso, o artigo 58.º, n.º 4, da Lei relativa à proteção de informações pessoais prevê que tais informações devem ser tratadas na medida mínima necessária para atingir a finalidade prevista e durante o período mínimo; por outro lado, exige que o responsável pelo tratamento das informações pessoais aplique as medidas necessárias para assegurar uma gestão segura dos dados e um tratamento adequado, tais como garantias técnicas, de gestão e físicas, bem como medidas para o tratamento adequado de reclamações individuais.

Por último, aplicam-se as disposições que regem as tarefas e os poderes da Comissão de Proteção de Informações Pessoais (incluindo os artigos 60.º a 65.º da Lei relativa à proteção de informações pessoais sobre o tratamento de reclamações e a adoção de recomendações e medidas corretivas), bem como as disposições sobre sanções administrativas e penais (artigo 70.º e seguintes da Lei relativa à proteção de informações pessoais). Nos termos do artigo 7.º-8, n.º 1, pontos 3 e 4, e do artigo 7.º-9, n.º 1, ponto 5, da Lei relativa à proteção de informações pessoais, estes poderes de investigação e correção, incluindo quando exercidos no contexto do tratamento de reclamações, abrangem também possíveis infrações às regras contidas em leis específicas que estabelecem as limitações e garantias no que respeita à recolha de informações pessoais, nomeadamente as leis relativas à segurança nacional. Dados os requisitos do artigo 3.º, n.º 1, da Lei relativa à proteção de informações pessoais relativos à recolha lícita e leal de informações pessoais, essa infração constitui uma violação da «presente lei» na aceção dos artigos 63.º e 64.º, permitindo à Comissão de Proteção de Informações Pessoais realizar uma investigação e tomar medidas corretivas. ([11]) O exercício destes poderes pela Comissão de Proteção de Informações Pessoais complementa, mas não substitui, os poderes da Comissão Nacional dos Direitos Humanos ao abrigo da Lei relativa à Comissão dos Direitos Humanos.

A aplicação dos princípios, direitos e obrigações fundamentais da Lei relativa à proteção de informações pessoais ao tratamento de informações pessoais para fins de segurança nacional reflete as garantias consagradas na Constituição relativas à proteção do direito das pessoas singulares de controlar as suas próprias informações pessoais. Como reconhecido pelo Tribunal Constitucional, tal inclui o direito de uma pessoa singular ([12]) «a decidir quando, a quem ou por quem, e em que medida as suas informações serão divulgadas ou utilizadas. Trata-se de um direito básico ([13]), […], que existe para proteger a liberdade de decisão pessoal contra o risco causado pelo alargamento das funções do Estado e da tecnologia de informação e comunicação». Qualquer restrição a esse direito, nomeadamente, quando necessário para a proteção da segurança nacional, exige um equilíbrio entre os direitos e interesses da pessoa singular e o interesse público pertinente e não pode afetar a essência do direito (artigo 37.º, n.º 2, da Constituição).

([11]) No que diz respeito a medidas corretivas nos termos do artigo 64.º, ver também o ponto 5 supra.
([12]) Acórdão do Tribunal Constitucional de 26 de maio de 2005, 99HunMa513, 2004HunMa190.
([13]) Acórdão do Tribunal Constitucional de 21 de julho de 2005, 2003HunMa282.

Por conseguinte, ao tratar informações pessoais para fins de segurança nacional, o responsável pelo tratamento (por exemplo, o Serviço Nacional de Informações) deve, nomeadamente:

1) Especificar explicitamente as finalidades para as quais as informações pessoais são tratadas e recolher informações pessoais de forma lícita e leal, na medida mínima necessária para tais finalidades (artigo 3.º, n.º 1, da Lei relativa à proteção de informações pessoais); em concreto, só deve recolher e tratar subsequentemente as informações pessoais para a finalidade de desempenhar funções ao abrigo da legislação pertinente, como a Lei relativa ao Serviço Nacional de Informações;

2) Tratar as informações pessoais na medida mínima necessária e pelo período mínimo necessário para atingir o objetivo pretendido (artigo 58.º, n.º 4, da Lei relativa à proteção de informações pessoais); uma vez cumprida a finalidade do tratamento, o responsável pelo tratamento deve destruir irreversivelmente as informações pessoais, a menos que a conservação subsequente seja especificamente mandatada por lei, caso em que as informações pessoais pertinentes serão conservadas e geridas separadamente de outras informações pessoais, não serão utilizadas para outros fins distintos dos especificados na lei e serão destruídas no final do período de conservação;

3) Tratar as informações pessoais de forma adequada e necessária para os fins para os quais as informações pessoais são tratadas, não devendo utilizá-las para além dessas finalidades (artigo 3.º, n.º 2, da Lei relativa à proteção de informações pessoais);

4) Assegurar que as informações pessoais sejam exatas, completas e atualizadas na medida necessária em para as finalidades para que são tratadas (artigo 3.º, n.º 3, da Lei relativa à proteção de informações pessoais);

5) O responsável pelo tratamento das informações pessoais deve gerir com segurança as informações pessoais de acordo com os métodos de tratamento, tipos, etc. de informações pessoais, tendo em conta a possibilidade de violação dos direitos do titular dos dados e a gravidade dos riscos pertinentes (artigo 3.º, n.º 4, da Lei relativa à proteção de informações pessoais);

6) Tornar pública a sua política de privacidade e outras questões relacionadas com o tratamento das informações pessoais (artigo 3.º, n.º 5, da Lei relativa à proteção de informações pessoais);

7) Tratar as informações pessoais de forma a minimizar a possibilidade de violação da privacidade do titular dos dados (artigo 3.º, n.º 6, da Lei relativa à proteção de informações pessoais).

ii) Em conformidade com o artigo 58.º, n.º 4, da Lei relativa à proteção de informações pessoais, o responsável pelo tratamento (por exemplo, as autoridades competentes em matéria de segurança nacional como o Serviço Nacional de Informações) deve tomar as disposições necessárias, como a criação de garantias técnicas, de gestão e físicas, a fim de assegurar o cumprimento destes princípios e o tratamento adequado das informações pessoais. Estas disposições podem, por exemplo, incluir medidas específicas para garantir a segurança das informações pessoais, tais como restrições ao acesso a informações pessoais, controlos de acesso, registos, formação específica dos funcionários sobre o tratamento de informações pessoais, etc.

Além disso, nos termos do artigo 3.º, n.º 5, e do artigo 4.º da Lei relativa à proteção de informações pessoais, os titulares dos dados terão, entre outros, os seguintes direitos no que respeita às informações pessoais tratadas para fins de segurança nacional:

1) O direito de obter confirmação sobre se as suas informações pessoais estão ou não a ser tratadas, bem como de obter informações sobre o tratamento e aceder a essas informações, incluindo o fornecimento de cópias (artigo 4.º, n.ºs 1 e 3, da Lei relativa à proteção de informações pessoais);

2) O direito de suspender o tratamento e de solicitar a retificação, apagamento e destruição dessas informações (artigo 4.º, n.º 4 da Lei relativa à proteção de informações pessoais).

iii) o titular dos dados pode apresentar, no exercício destes direitos, um pedido diretamente ao responsável pelo tratamento ou indiretamente através da Comissão de Proteção, e pode autorizar o seu representante a fazê-lo. Se o titular dos dados apresentar um pedido, o responsável pelo tratamento deve garantir esse direito sem demora, desde que possa, no entanto, retardar, limitar ou negar o direito, se especificamente previsto ou inevitável para cumprir outra legislação, na medida e durante o tempo necessário e proporcionado para proteger um objetivo importante de interesse público (por exemplo, na medida e durante o tempo em que a concessão do direito possa pôr em risco uma investigação em curso ou ameaçar a segurança nacional), ou quando a concessão do direito possa lesar vida ou a integridade física de um terceiro ou resultar numa infração injustificada da propriedade e de outros interesses de terceiros. Se o pedido for recusado ou restringido, o titular dos dados deve ser notificado sem demora dos motivos. O responsável pelo tratamento deve elaborar o método e o procedimento para permitir aos titulares de dados apresentar pedidos, e deve anunciá-los publicamente, de modo que os titulares de dados possam tomar conhecimento dos mesmos.

Além disso, nos termos do artigo 58.º, n.º 4, da Lei relativa à proteção de informações pessoais (requisito para assegurar o tratamento adequado de queixas individuais) e do artigo 4.º, n.º 5, da Lei relativa à proteção de informações pessoais (direito à reparação adequada de quaisquer danos resultantes do tratamento de informações pessoais, através de um procedimento rápido e justo), os titulares dos dados terão o direito de obter reparação. Tal inclui o direito de denunciar uma alegada violação ao centro de denúncia de violações das informações pessoais (em conformidade com o artigo 62.º, n.º 3, da Lei relativa à proteção de informações pessoais), apresentar uma queixa à Comissão de Proteção de Informações Pessoais nos termos do artigo 62.º da Lei relativa à proteção de informações pessoais sobre qualquer violação dos direitos ou interesses relacionados com as informações pessoais de uma pessoa singular e obter reparação judicial contra decisões ou inação da Comissão de Proteção de Informações Pessoais ao abrigo da Lei relativa ao contencioso administrativo. Além disso, os titulares dos dados podem obter reparação judicial ao abrigo da Lei relativa ao contencioso administrativo se tiver ocorrido uma violação dos seus direitos ou interesses devido a um ato ou omissão por parte do responsável pelo tratamento (por exemplo, recolha ilícita de dados pessoais), ou obter compensação por danos em conformidade com a Lei relativa às Indemnizações do Estado. Estas vias de recurso estão disponíveis tanto no caso de possíveis infrações às regras contidas em leis específicas que estabelecem as limitações e garantias no que respeita à recolha de informações pessoais, como as leis relativas à segurança nacional, como da Lei relativa à proteção de informações pessoais.

Uma pessoa singular da UE pode apresentar uma reclamação à Comissão de Proteção de Informações Pessoais através da respetiva autoridade nacional responsável pela proteção de dados, e a Comissão de Proteção de Informações Pessoais notificará essa pessoa singular através da autoridade nacional responsável pela proteção de dados, após a conclusão da investigação e da medida corretiva (se aplicável).

ANEXO II

18 de maio de 2021.

Sua Excelência, Didier Reynders, Comissário da Justiça da Comissão Europeia

Ex.mo Senhor Comissário,

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

Na sequência do pedido formulado pela Comissão Europeia ao Governo da Coreia, 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 da Coreia.

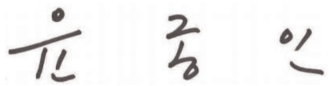
O referido documento diz respeito a diversos ministérios e agências do Governo da Coreia. Quanto ao seu teor, os ministérios e agências competentes (Comissão de Proteção de Informações Pessoais, Ministério da Justiça, Serviço Nacional de Informações, Comissão Nacional dos Direitos Humanos da Coreia, Centro Nacional de Luta contra o Terrorismo, Unidade de Informações Financeiras da Coreia) 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 de Informações Pessoais 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.

Com os melhores cumprimentos,

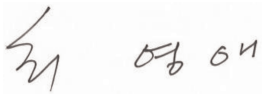


Yoon Jong In
Presidente da Comissão de Proteção de Informações Pessoais

O presente documento foi elaborado pela Comissão de Proteção de Informações Pessoais e pelos ministérios e agências competentes a seguir indicados.

Park Jie Won
Presidente (Diretor), Serviço Nacional de Informações

Lee Jung Soo
Diretor-Geral, Ministério da Justiça



Choi Young Ae
Presidente, Comissão Nacional dos Direitos Humanos da Coreia

Kim Hyuck Soo
Diretor, Centro Nacional de Luta contra o Terrorismo

Kim, Jeong Kag
Comissário, Unidade de Informações Financeiras da Coreia

Quadro jurídico para a recolha e utilização de dados pessoais pelas autoridades públicas coreanas para efeitos de aplicação da lei e de segurança nacional

O documento que se segue apresenta uma panorâmica do quadro jurídico para a recolha e utilização de dados pessoais pelas autoridades públicas coreanas para efeitos de aplicação do direito penal e de segurança nacional (a seguir designado por «*acesso governamental*»), em especial no que diz respeito às bases jurídicas disponíveis, às condições (limitações) e às garantias aplicáveis, incluindo o controlo independente e as possibilidades de reparação individual.

1. PRINCÍPIOS GERAIS DO DIREITO APLICÁVEIS AO ACESSO GOVERNAMENTAL

1.1. Quadro constitucional

A Constituição da República da Coreia estabelece o direito à privacidade em geral (artigo 17.º) e o direito à privacidade da correspondência em particular (artigo 18.º). O Estado tem o dever de garantir estes direitos fundamentais ([1]). A Constituição estipula ainda que os direitos e liberdades dos cidadãos só podem ser limitados por lei e quando necessário por razões de segurança nacional ou de manutenção da lei e da ordem pública ([2]). Mesmo quando são impostas, tais restrições não podem afetar a essência da liberdade ou do direito ([3]). Os tribunais coreanos têm aplicado estas disposições em casos de interferência governamental na privacidade. Por exemplo, o Supremo Tribunal considerou que a vigilância de civis violou o direito fundamental à privacidade, salientando que os cidadãos têm «o direito à autodeterminação das informações pessoais» ([4]). Num outro caso, o Tribunal Constitucional considerou que a privacidade é um direito fundamental que proporciona proteção contra a intervenção e a observação por parte do Estado na vida privada dos cidadãos ([5]).

A Constituição coreana garante ainda que nenhuma pessoa pode ser presa, detida, revistada ou interrogada, nem os seus bens apreendidos, exceto nos casos previstos na lei ([6]). Além disso, as buscas e apreensões só podem ser conduzidas com base num mandado emitido por um juiz, mediante pedido de um procurador e no respeito pelas garantias processuais ([7]). Em circunstâncias excecionais, isto é, quando o suspeito de um crime é detido durante a comissão de um crime (flagrante delito), ou quando existe o risco de uma pessoa suspeita de ter cometido um crime punível com pena de prisão igual ou superior a três anos poder escapar ou destruir provas, as autoridades de investigação podem conduzir uma busca ou apreensão sem mandado, caso em que devem solicitar um mandado *ex post* ([8]). Estes princípios gerais são desenvolvidos mais aprofundadamente em leis específicas que tratam do processo penal e da proteção das comunicações (ver uma descrição mais pormenorizada *infra*).

No que respeita aos nacionais estrangeiros, a Constituição estipula que o seu estatuto é garantido nos termos do direito e dos tratados internacionais ([9]). Vários acordos internacionais em que a Coreia é parte garantem direitos à privacidade, nomeadamente, o Pacto Internacional sobre os Direitos Civis e Políticos (artigo 17.º), a Convenção sobre os Direitos das Pessoas com Deficiência (artigo 22.º) e a Convenção sobre os Direitos da Criança (artigo 16.º). Além disso, embora a Constituição se refira, em princípio, aos direitos dos «*cidadãos*», o Tribunal Constitucional decidiu que também assistem aos nacionais estrangeiros direitos fundamentais ([10]). Em especial, o Tribunal declarou que a proteção da dignidade e do valor da pessoa como ser humano, bem como o direito à felicidade, são direitos de qualquer ser humano e não apenas

([1]) Artigo 10.º da Constituição da República da Coreia, promulgada em 17 de julho de 1948 (a seguir designada por «Constituição»).
([2]) Artigo 37.º, n.º 2, da Constituição.
([3]) Artigo 37.º, n.º 2, da Constituição.
([4]) Decisão n.º 96DA42789 do Supremo Tribunal, de 24 de julho de 1998.
([5]) Decisão n.º 2002Hun-Ma51 do Tribunal Constitucional, de 30 de outubro de 2003. Da mesma forma, na Decisão n.º 99Hun-Ma513 e 2004Hun-Ma190 (consolidada), de 26 de maio de 2005, o Tribunal Constitucional esclareceu que «o direito de controlar as próprias informações pessoais constitui um direito do titular das informações de decidir pessoalmente quando, a quem ou por quem, e em que medida, as suas informações são divulgadas ou utilizadas. Trata-se de um direito básico, embora não especificado na Constituição, que existe para proteger a liberdade de decisão pessoal contra o risco causado pelo alargamento das funções do Estado e da tecnologia de informação e comunicação».
([6]) Artigo 12.º, n.º 1, primeiro período, da Constituição.
([7]) Artigo 16.º e artigo 12.º, n.º 3, da Constituição.
([8]) Artigo 12.º, n.º 3, da Constituição.
([9]) Artigo 6.º, n.º 2, da Constituição.
([10]) Decisão n.º 93Hun-MA120 do Tribunal Constitucional, de 29 de dezembro de 1994. Ver também, por exemplo, a Decisão n.º 2014Hun-Ma346 do Tribunal Constitucional (31 de maio de 2018), em que o Tribunal considerou que foi violado o direito constitucional de um nacional sudanês detido no aeroporto de receber assistência de um advogado de defesa. Num outro caso, o Tribunal Constitucional considerou que a liberdade de escolher o local de trabalho legal está intimamente relacionada com o direito de procurar a felicidade, bem como o direito à dignidade e ao valor humano, pelo que não está reservada apenas aos cidadãos, mas pode também ser garantida aos estrangeiros legalmente empregados na República da Coreia (Decisão n.º 2007Hun-Ma1083 do Tribunal Constitucional, de 29 de setembro de 2011).

dos cidadãos ([11]). O Tribunal esclareceu igualmente que o direito de controlar a informação pessoal é considerado um direito básico, fundamentado no direito à dignidade e à busca da felicidade e no direito à vida privada ([12]). Embora até à data a jurisprudência não tenha tratado especificamente do direito à privacidade dos nacionais não coreanos, é contudo amplamente aceite entre os académicos que os artigos 12.º a 22.º da Constituição (que incluem o direito à privacidade, bem como à liberdade pessoal) estabelecem «*direitos dos seres humanos*».

Por último, a Constituição também prevê o direito de reclamar uma justa indemnização junto das autoridades públicas ([13]). Além disso, com base na Lei relativa ao Tribunal Constitucional, qualquer pessoa cujos direitos fundamentais garantidos pela Constituição sejam violados pelo exercício do poder governamental (excluindo os acórdãos dos tribunais) pode apresentar uma queixa constitucional junto do Tribunal Constitucional ([14]).

1.2. **Regras gerais sobre a proteção de dados**

A lei geral sobre a proteção de dados na República da Coreia, a Lei relativa à proteção de informações pessoais, aplica-se tanto ao setor privado como ao setor público. No que respeita às autoridades públicas, a Lei relativa à proteção de informações pessoais refere-se especificamente à obrigação de formular políticas para prevenir «o abuso e a utilização indevida de informações pessoais, a vigilância e o rastreamento indiscretos, etc., e para reforçar a dignidade dos seres humanos e a privacidade individual» ([15]).

O tratamento de dados pessoais para fins de aplicação da lei está sujeito à totalidade dos requisitos da Lei relativa à proteção de informações pessoais, o que significa, por exemplo, que as autoridades responsáveis em matéria de aplicação do direito penal devem cumprir as obrigações de tratamento lícito, ou seja, recorrer a uma das bases jurídicas enumeradas na Lei relativa à proteção de informações pessoais para a recolha, utilização ou fornecimento de informações pessoais (artigos 15.º a 18.º da Lei relativa à proteção de informações pessoais), bem como os princípios de limitação das finalidades (artigo 3.º, n.ºs 1 e 2, da Lei relativa à proteção de informações pessoais), de proporcionalidade/minimização dos dados (artigo 3.ºs, n.º 1 e 6, da Lei relativa à proteção de informações pessoais), de conservação limitada dos dados (artigo 21.º da Lei relativa à proteção de informações pessoais), de segurança dos dados, incluindo a notificação de violações dos dados (artigo 3.º, n.º 4, e artigos 29.º e 34.º da Lei relativa à proteção de informações pessoais), e de transparência (artigo 3.º, n.ºs 1 e 5, e artigos 20.º, 30.º e 32.º da Lei relativa à proteção de informações pessoais). Aplicam-se garantias específicas no que respeita à informação sensível (artigo 23.º da Lei relativa à proteção de informações pessoais). Além disso, em conformidade com o artigo 3.º, n.º 5, e os artigos 4.º e 35.º a 39.º-2 da Lei relativa à proteção de informações pessoais, as pessoas singulares podem exercer os seus direitos de acesso, retificação, apagamento e suspensão junto das autoridades responsáveis pela aplicação da lei.

Por conseguinte, embora se aplique plenamente ao tratamento de dados pessoais para fins de aplicação do direito penal, a Lei relativa à proteção de informações pessoais inclui uma exceção quando os dados pessoais são tratados para efeitos de segurança nacional. Nos termos do artigo 58.º, n.º 1, ponto 2, da Lei relativa à proteção de informações pessoais, os artigos 15.º a 50.º da Lei relativa à proteção de informações pessoais não se aplicam às informações pessoais recolhidas ou solicitadas para a análise de informações relacionadas com a segurança nacional ([16]). Em contrapartida, o capítulo I (Disposições gerais), o capítulo II (Estabelecimento de políticas de proteção de informações pessoais, etc.), o capítulo VIII (Ação coletiva por violação de dados), o capítulo IX (Disposições complementares) e o capítulo X (Disposições sancionatórias) da Lei relativa à proteção de informações pessoais continuam a ser aplicáveis. Tal inclui os princípios gerais em matéria de proteção de dados estabelecidos no artigo 3.º (Princípios em matéria de proteção de informações pessoais) e os direitos individuais garantidos pelo artigo 4.º da Lei relativa à proteção de informações pessoais (Direitos dos titulares de dados). Tal significa que os princípios e direitos essenciais são também garantidos neste domínio. Além disso, o artigo 58.º, n.º 4, da Lei relativa à proteção de informações pessoais prevê que tais informações devem ser tratadas na medida mínima necessária para atingir a finalidade prevista e durante o período mínimo; por outro lado, exige que o responsável pelo tratamento das informações pessoais aplique as medidas necessárias para assegurar uma gestão segura e um tratamento adequado dos dados, nomeadamente, garantias técnicas, de gestão e físicas, bem como medidas para o tratamento adequado de queixas individuais.

Na Notificação n.º 2021-1 sobre as normas complementares para a interpretação e aplicação da Lei relativa à proteção de informações pessoais, a Comissão de Proteção de Informações Pessoais clarificou melhor a forma como a Lei relativa à proteção de informações pessoais se aplica ao tratamento de dados pessoais para efeitos de segurança nacional, à luz desta isenção parcial ([17]). Tal inclui em particular os direitos das pessoas singulares (acesso, retificação, suspensão e apagamento) e os fundamentos, bem como as limitações, de possíveis restrições aos mesmos. Nos termos da notificação, a aplicação dos princípios, direitos e obrigações fundamentais da Lei relativa à proteção de informações pessoais ao tratamento de informações pessoais para fins de segurança nacional reflete as garantias consagradas na Constituição

([11]) Decisão n.º 99HeonMa494-Ma51 do Tribunal Constitucional, de 29 de novembro de 2001.
([12]) Ver, por exemplo, a Decisão n.º 99HunMa513 do Tribunal Constitucional.
([13]) Artigo 29.º, n.º 1, da Constituição.
([14]) Artigo 68.º, n.º 1, da Lei relativa ao Tribunal Constitucional.
([15]) Artigo 5.º, n.º 1, da Lei relativa à proteção de informações pessoais.
([16]) Artigo 58.º, n.º 1, ponto 2, da Lei relativa à proteção de informações pessoais.
([17]) Notificação n.º 2021-1 da Comissão de Proteção de Informações Pessoais relativa às normas complementares para a interpretação e aplicação da Lei relativa à proteção de informações pessoais, secção III, n.º 6.

relativas à proteção do direito das pessoas singulares de controlar as suas próprias informações pessoais. Qualquer restrição a esse direito, nomeadamente, quando necessário para a proteção da segurança nacional, exige um equilíbrio entre os direitos e interesses da pessoa singular e o interesse público pertinente e não pode afetar a essência do direito (artigo 37.º, n.º 2, da Constituição).

2. ACESSO GOVERNAMENTAL PARA FINS DE APLICAÇÃO DO DIREITO PENAL

2.1. **Autoridades públicas competentes em matéria de aplicação da lei**

Com base na Lei relativa ao processo penal, na Lei relativa à proteção da privacidade das comunicações e na Lei relativa às atividades de telecomunicações, a polícia, os procuradores e os tribunais podem recolher dados pessoais para efeitos de aplicação do direito penal. Na medida em que a Lei relativa ao Serviço Nacional de Informações confere este poder também ao Serviço Nacional de Informações, este tem de cumprir as leis supramencionadas ([18]). Por último, a Lei relativa à comunicação e utilização de informações específicas sobre transações financeiras fornece uma base jurídica para as instituições financeiras divulgarem informações à Unidade de Informações Financeiras da Coreia para efeitos de prevenção do branqueamento de capitais e do financiamento do terrorismo. Esta agência especializada pode, por sua vez, fornecer essas informações às autoridades responsáveis pela aplicação da lei. No entanto, estas obrigações de divulgação aplicam-se apenas aos responsáveis pelo tratamento de dados que tratam informações pessoais de crédito nos termos da Lei relativa às informações de crédito e sujeitos ao controlo da Comissão dos Serviços Financeiros. Uma vez que o tratamento de informações pessoais de crédito por tais responsáveis pelo tratamento está excluído do âmbito de aplicação da decisão de adequação, as limitações e garantias aplicáveis ao abrigo da ARUSFTI não são descritas em maior pormenor no presente documento.

2.2. **Bases jurídicas e limitações**

A Lei relativa ao processo penal (ver 2.2.1), a Lei relativa à proteção da privacidade das comunicações (ver 2.2.2) e a Lei relativa às atividades de telecomunicações (ver 2.2.3) estabelecem as bases jurídicas para a recolha de informações pessoais para efeitos de aplicação da lei e definem as limitações e garantias aplicáveis.

2.2.1. *Buscas e apreensões*

2.2.1.1. Base jurídica

Os procuradores e os agentes superiores da polícia judiciária só podem inspecionar artigos, revistar pessoas ou apreender artigos 1) se uma pessoa for suspeita de ter cometido um crime (um suspeito de um crime), 2) se for necessário para a investigação e 3) se os artigos a inspecionar, as pessoas a revistar e quaisquer artigos apreendidos forem considerados como estando relacionados com o processo ([19]). Do mesmo modo, os tribunais podem realizar buscas e apreender quaisquer artigos destinados a servir de prova ou suscetíveis de apreensão, desde que tais artigos ou pessoas sejam considerados como estando relacionados com um processo específico ([20]).

2.2.1.2. Limitações e garantias

Como obrigação geral, os procuradores e os agentes da polícia judiciária devem respeitar os direitos humanos do suspeito de um crime, bem como os direitos de qualquer outra pessoa envolvida ([21]). Além disso, só podem ter tomadas medidas obrigatórias para cumprir a finalidade da investigação quando previsto explicitamente na Lei relativa ao processo penal e na medida do necessário ([22]).

As buscas, inspeções ou apreensões por agentes da polícia ou procuradores no âmbito de uma investigação criminal só podem ser realizadas com base num mandado emitido por um tribunal ([23]). A autoridade que solicita um mandado deve apresentar elementos que demonstrem os motivos para suspeitar que uma pessoa cometeu um crime, que a busca, inspeção ou apreensão são necessárias, e que os artigos pertinentes a apreender existem ([24]). Quanto ao mandado, este deve conter, entre outros elementos, os nomes do suspeito de crime e a infração, o local, a pessoa ou os artigos a sujeitar à busca, ou os artigos a apreender, a data de emissão e o período efetivo de aplicação ([25]). Da mesma forma, quando, no âmbito de processos judiciais em curso, forem efetuadas buscas e apreensões que não sejam públicas, deverá ser obtido previamente um mandado emitido por um tribunal ([26]). A pessoa em causa e o seu advogado de defesa são previamente notificados da busca ou apreensão e podem estar presentes durante a execução do mandado ([27]).

([18]) Ver o artigo 3.º da Lei relativa ao Serviço Nacional de Informações (Lei n.º 12948), que se refere a investigações penais de determinados crimes, tais como insurreição, rebelião e crimes relacionados com a segurança nacional (por exemplo, espionagem). Os procedimentos da Lei relativa ao processo penal relativos a buscas e apreensões aplicar-se-ão neste contexto, ao passo que a Lei relativa à proteção da privacidade das comunicações regerá a recolha de dados de comunicação (ver parte 3 sobre as disposições relativas ao acesso às comunicações para efeitos de segurança nacional).
([19]) Artigo 215.º, n.os 1 e 2, da Lei relativa ao processo penal.
([20]) Artigo 106.º, n.º 1, artigo 107.º e artigo 109.º da Lei relativa ao processo penal.
([21]) Artigo 198.º, n.º 2, da Lei relativa ao processo penal.
([22]) Artigo 199.º, n.º 1, da Lei relativa ao processo penal.
([23]) Artigo 215.º, n.os 1 e 2, da Lei relativa ao processo penal.
([24]) Artigo 108.º, n.º 1, do Regulamento de Processo Penal.
([25]) Artigo 114.º, n.º 1, da Lei relativa ao processo penal, em conjugação com o artigo 219.º da Lei relativa ao processo penal.
([26]) Artigo 113.º da Lei relativa ao processo penal.
([27]) Artigo 121.º e artigo 122.º, da Lei relativa ao processo penal.

Aquando da condução de buscas e apreensões e caso a busca diga respeito a um disco de um computador ou a outro suporte de armazenamento de dados, em princípio, só serão apreendidos os dados (copiados ou impressos) e não todo o suporte ([28]). O suporte de armazenamento de dados só poderá ser apreendido quando for considerado substancialmente impossível imprimir ou copiar separadamente os dados necessários, ou quando for considerado substancialmente impraticável realizar a finalidade da busca de outra forma ([29]). A pessoa singular em causa deve ser notificada da apreensão sem demora ([30]). Nos termos da Lei relativa ao processo penal, não existem exceções a este requisito de notificação.

As buscas, inspeções e apreensões sem mandado só podem ser realizadas em situações limitadas. Em primeiro lugar, é este o caso quando é impossível obter um mandado por motivo de urgência no local de uma infração ([31]). No entanto, um mandado deve ser subsequentemente obtido sem demora ([32]). Em segundo lugar, as buscas e inspeções sem mandado podem ser realizadas no local quando o suspeito de um crime é preso ou detido ([33]). Por último, um procurador ou agente superior da polícia judiciária pode apreender um artigo sem mandado quando o artigo tiver sido abandonado pelo suspeito de um crime ou por um terceiro ou tiver sido apresentado voluntariamente ([34]).

As provas que tenham sido obtidas em violação da Lei relativa ao processo penal serão consideradas inadmissíveis ([35]). Além disso, o Código Penal estipula que as buscas ilegais de pessoas ou do seu local de residência, de um edifício vigiado, de uma estrutura, veículo automóvel, navio, avião ou sala ocupada, são puníveis com pena de prisão por um máximo de três anos ([36]). Esta disposição também se aplica, por conseguinte, quando são apreendidos objetos, como dispositivos de armazenamento de dados, durante uma busca ilegal.

2.2.2. *Recolha de informações sobre comunicações*

2.2.2.1. Base jurídica

A recolha de informações sobre comunicações é regida por uma lei específica, a Lei relativa à proteção da privacidade das comunicações. Em particular, a Lei relativa à proteção da privacidade das comunicações estipula a proibição de qualquer pessoa censurar qualquer correspondência, realizar escutas telefónicas, fornecer dados de confirmação da comunicação ou gravar ou escutar qualquer conversa entre outras pessoas que não sejam tornadas públicas, exceto com base na Lei relativa ao processo penal, na Lei relativa à proteção da privacidade das comunicações ou na Lei relativa ao Tribunal Militar ([37]). O termo «*comunicação*» na aceção da Lei relativa à proteção da privacidade das comunicações abrange tanto a correspondência normal como as telecomunicações ([38]). A este respeito, a Lei relativa à proteção da privacidade das comunicações distingue entre «medidas de restrição das comunicações» ([39]) e a recolha de «dados de confirmação da comunicação».

O conceito de medidas de restrição das comunicações abrange a «*censura*», ou seja, a recolha do conteúdo da correspondência postal tradicional, bem como «*escutas telefónicas*», ou seja, a interceção direta (aquisição ou gravação) do conteúdo das telecomunicações ([40]). O conceito de dados de confirmação das comunicações abrange «*dados sobre os registos das telecomunicações*», o que inclui a data das telecomunicações, a respetiva hora de início e fim, o número de chamadas efetuadas e recebidas, bem como o número de assinante da outra parte, a frequência de utilização, os ficheiros de registo relativos à utilização dos serviços de telecomunicações e informações de localização (por exemplo, das torres de transmissão onde os sinais são recebidos) ([41]).

([28]) Artigo 106.º, n.º 3, da Lei relativa ao processo penal.
([29]) Artigo 106.º, n.º 3, da Lei relativa ao processo penal.
([30]) Artigo 219.º da Lei relativa ao processo penal, em conjugação com o artigo 106.º, n.º 4, da Lei relativa ao processo penal.
([31]) Artigo 216.º, n.º 3, da Lei relativa ao processo penal.
([32]) Artigo 216.º, n.º 3, da Lei relativa ao processo penal.
([33]) Artigo 216.º, n.os 1 e 2, da Lei relativa ao processo penal.
([34]) Artigo 218.º da Lei relativa ao processo penal. No que respeita às informações pessoais, esta disposição apenas abrange a apresentação voluntária pela própria pessoa em causa, e não por um responsável pelo tratamento das informações pessoais que detenha essas informações (o que exigiria uma base jurídica específica ao abrigo da Lei relativa à proteção de informações pessoais). Os artigos apresentados voluntariamente só são admitidos como prova em processos judiciais se não houver dúvidas razoáveis quanto à natureza voluntária da divulgação, facto que cabe ao procurador demonstrar. Ver Decisão n.º 2013Do11233 do Supremo Tribunal, de 10 de março de 2016.
([35]) Artigo 308.º-2 da Lei relativa ao processo penal.
([36]) Artigo 321.º do Código Penal.
([37]) Artigo 3.º da Lei relativa à proteção da privacidade das comunicações. Em princípio, a Lei relativa ao Tribunal Militar rege a recolha de informações sobre o pessoal militar e só pode ser aplicada a civis num número limitado de casos (por exemplo, se o pessoal militar e os civis cometerem um crime em conjunto, ou se uma pessoa cometer um crime contra as forças armadas, o processo pode ser intentado junto de um tribunal militar; ver o artigo 2.º da Lei relativa ao Tribunal Militar). As disposições gerais que regem as buscas e as apreensões são idênticas às da Lei relativa ao processo penal; ver, por exemplo, os artigos 146.º a 149.º e 153.º a 156.º da Lei relativa ao Tribunal Militar. Por exemplo, a correspondência postal só pode ser recolhida quando necessário para conduzir uma investigação e com base num mandado do Tribunal Militar. Caso sejam recolhidas comunicações eletrónicas, aplicar-se-ão as limitações e garantias da Lei relativa à proteção da privacidade das comunicações.
([38]) Artigo 2.º, n.º 1, da Lei relativa à proteção da privacidade das comunicações, «*transmissão ou receção de todo o tipo de sons, palavras, símbolos ou imagens, por fio ou sem fio, fibra ótica ou outro sistema eletromagnético, incluindo telefone, correio eletrónico, serviço de informação por subscrição, fax e radiochamada*».
([39]) Artigo 2.º, n.º 7, e artigo 3.º, n.º 2, da Lei relativa à proteção da privacidade das comunicações.
([40]) A «censura» é definida como «*a abertura de correspondência sem o consentimento da parte interessada ou a aquisição de conhecimento sobre o respetivo conteúdo, bem como o registo ou a retenção do mesmo, por outros meios*» (artigo 2.º, n.º 6, da Lei relativa à proteção da privacidade das comunicações). «Escutas telefónicas» refere-se à «aquisição ou gravação do conteúdo de telecomunicações através da escuta ou da leitura coletiva dos sons, das palavras, dos símbolos ou das imagens das comunicações através de dispositivos eletrónicos e mecânicos, sem o consentimento da parte interessada ou interferência na sua transmissão e receção» (artigo 2.º, n.º 7, da Lei relativa à proteção da privacidade das comunicações).
([41]) Artigo 2, n.º 11, da Lei relativa à proteção da privacidade das comunicações.

A Lei relativa à proteção da privacidade das comunicações estabelece as limitações e garantias para a recolha de ambos os tipos de dados, e o não cumprimento de vários destes requisitos é passível de sanções penais ([42]).

2.2.2.2. Limitações e garantias aplicáveis à recolha do conteúdo das comunicações (medidas de restrição das comunicações)

A recolha do conteúdo das comunicações só pode ocorrer como meio complementar para facilitar uma investigação criminal (ou seja, como medida de último recurso) e devem ser desenvolvidos esforços para minimizar a interferência com o sigilo de comunicação pessoal ([43]). De acordo com este princípio geral, as medidas de restrição das comunicações só podem ser aplicadas quando for difícil impedir a prática de um crime, prender o criminoso ou recolher as provas ([44]). Os serviços responsáveis pela aplicação da lei que recolhem o conteúdo das comunicações devem deixar imediatamente de o fazer quando o acesso continuado deixar de ser considerado necessário, assegurando assim que a violação da privacidade das comunicações seja tão limitada quanto possível ([45]).

Além disso, as medidas de restrição das comunicações só podem ser utilizadas quando houver motivos substanciais para suspeitar que certos crimes graves especificamente enumerados na Lei relativa à proteção da privacidade das comunicações estão a ser planeados ou estão a ser ou foram cometidos. Estes incluem crimes como insurreição, crimes relacionados com drogas ou crimes que envolvam explosivos, bem como crimes relacionados com a segurança nacional, relações diplomáticas ou bases e instalações militares ([46]). O alvo de uma medida de restrição das comunicações deve consistir em envios postais ou telecomunicações específicos enviados ou recebidos pelo suspeito, ou envios postais ou telecomunicações enviados ou recebidos pelo suspeito durante um período de tempo determinado ([47]).

Mesmo quando estes requisitos são cumpridos, a recolha de dados sobre conteúdos só pode ser realizada com base num mandado emitido por um tribunal. Em particular, um procurador pode solicitar ao tribunal que permita a recolha de dados sobre conteúdos relativos ao suspeito ou à pessoa sob investigação ([48]). Da mesma forma, um agente da polícia judiciária pode pedir autorização a um procurador, que por sua vez pode solicitar um mandado ao tribunal ([49]). Um pedido de mandado deve ser efetuado por escrito e conter elementos específicos. Em especial, deve indicar 1) as razões substanciais para suspeitar que um dos crimes enumerados está planeado, está a ser ou foi cometido, bem como quaisquer elementos que estabeleçam uma presunção de suspeita *prima facie*; 2) as medidas de restrição das comunicações, bem como o seu alvo, âmbito, objetivo e período efetivo; e 3) o local onde as medidas seriam executadas e a forma como seriam levadas a cabo ([50]).

Quando os requisitos legais forem satisfeitos, o tribunal pode conceder autorização escrita para a execução de medidas de restrição das comunicações relativamente ao suspeito ou à pessoa sob investigação ([51]). Este mandado especifica os tipos de medidas, bem como o seu alvo, âmbito, período efetivo, local de execução e a forma como devem ser executadas ([52]).

As medidas de restrição das comunicações só podem ser executadas por um período de dois meses ([53]). Se o objetivo das medidas for atingido mais cedo durante esse período, as medidas devem ser imediatamente interrompidas. Em contrapartida, se continuarem a verificar-se as condições exigidas, poderá ser apresentado um pedido de prorrogação do período efetivo das medidas de restrição das comunicações dentro do prazo limite de dois meses. Tal pedido tem de incluir elementos que estabeleçam uma presunção *prima facie* para a prorrogação das medidas ([54]). O período prorrogado não pode exceder, no total, um ano ou três anos no caso de determinados crimes especialmente graves (nomeadamente, crimes de insurreição, agressão estrangeira, segurança nacional, etc.) ([55]).

As autoridades responsáveis pela aplicação da lei podem obrigar a assistência dos operadores de comunicações, facultando-lhes a autorização escrita do tribunal ([56]). Os operadores de comunicações são obrigados a cooperar e a manter a autorização recebida nos seus ficheiros ([57]). Podem recusar a cooperação quando as informações sobre a pessoa visada, indicada na autorização escrita do tribunal (por exemplo, o número de telefone da pessoa), estiverem incorretas. Além disso, estão proibidos, em todas as circunstâncias, de divulgar as palavras-passe utilizadas nas telecomunicações ([58]).

([42]) Artigos 16.º e 17.º da Lei relativa à proteção da privacidade das comunicações. Tal aplica-se, por exemplo, à recolha sem mandado, à não manutenção de registos, à não interrupção da recolha quando uma emergência deixa de existir ou à não notificação da pessoa em causa.
([43]) Artigo 3, n.º 2, da Lei relativa à proteção da privacidade das comunicações.
([44]) Artigo 5, n.º 1, da Lei relativa à proteção da privacidade das comunicações.
([45]) Artigo 2.º do Decreto de Execução da Lei relativa à proteção da privacidade das comunicações.
([46]) Artigo 5, n.º 1, da Lei relativa à proteção da privacidade das comunicações.
([47]) Artigo 5, n.º 2, da Lei relativa à proteção da privacidade das comunicações.
([48]) Artigo 6, n.º 1, da Lei relativa à proteção da privacidade das comunicações.
([49]) Artigo 6, n.º 2, da Lei relativa à proteção da privacidade das comunicações.
([50]) Artigo 6.º, n.º 4, da Lei relativa à proteção da privacidade das comunicações e artigo 4.º, n.º 1, do Decreto de Execução da Lei relativa à proteção da privacidade das comunicações.
([51]) Artigo 6.º, n.ºs 5 e 8, da Lei relativa à proteção da privacidade das comunicações.
([52]) Artigo 6, n.º 6, da Lei relativa à proteção da privacidade das comunicações.
([53]) Artigo 6, n.º 7, da Lei relativa à proteção da privacidade das comunicações.
([54]) Artigo 6, n.º 7, da Lei relativa à proteção da privacidade das comunicações.
([55]) Artigo 6, n.º 8, da Lei relativa à proteção da privacidade das comunicações.
([56]) Artigo 9, n.º 2, da Lei relativa à proteção da privacidade das comunicações.
([57]) Artigo 15.º-2 da Lei relativa à proteção da privacidade das comunicações e artigo 12.º do Decreto de Execução da Lei relativa à proteção da privacidade das comunicações.
([58]) Artigo 9, n.º 4, da Lei relativa à proteção da privacidade das comunicações.

Qualquer pessoa que execute medidas de restrição das comunicações ou seja solicitada a cooperar deve manter registos que especifiquem os objetivos das medidas, a sua execução, a data em que a cooperação foi prestada e o respetivo alvo ([59]). As autoridades responsáveis pela aplicação da lei que executem medidas de restrição das comunicações devem também manter registos que incluam os pormenores e os resultados obtidos ([60]). Os agentes da polícia judiciária devem fornecer estas informações por meio de um relatório ao procurador quando encerram uma investigação ([61]).

Quando um procurador deduz uma acusação em relação a um processo, em que foram utilizadas medidas de restrição das comunicações, ou emite uma disposição de não acusação ou detenção da pessoa em causa (ou seja, não apenas uma suspensão do procedimento penal), o procurador deve notificar a pessoa objeto das medidas de restrição das comunicações do facto de que tais medidas foram executadas, bem como indicar a agência de execução e o período de execução. Tal notificação deve ser efetuada por escrito no prazo de 30 dias a contar da disposição ([62]). A notificação pode ser diferida quando for suscetível de pôr seriamente em perigo a segurança nacional ou perturbar a segurança e a ordem públicas, ou quando for suscetível de resultar em danos materiais para a vida e a integridade física de terceiros ([63]). Sempre que pretenda adiar a notificação, o procurador ou o agente da polícia judiciária deve obter a aprovação do diretor da procuradoria distrital ([64]). Assim que deixarem de existir motivos para o diferimento, a notificação deve ser efetuada no prazo de 30 dias a partir dessa data ([65]).

A Lei relativa à proteção da privacidade das comunicações também estabelece um procedimento específico para a recolha do conteúdo das comunicações em situações de emergência. Em particular, os serviços responsáveis pela aplicação da lei podem recolher o conteúdo das comunicações no caso de o planeamento ou a execução de um crime organizado ou de outro crime grave, que possa causar diretamente a morte ou ferimentos graves, ser iminente e se existir uma emergência que impossibilite o seguimento do procedimento regular (conforme estabelecido supra) ([66]). Em tal emergência, um agente da polícia ou procurador pode tomar medidas de restrição das comunicações sem autorização judicial prévia, mas deve apresentar um pedido de autorização judicial imediatamente após a execução. Se o serviço responsável pela aplicação da lei não obtiver autorização judicial no prazo de 36 horas a partir do momento em que as medidas de emergência foram aplicadas, a recolha deve ser imediatamente interrompida, normalmente seguida da destruição das informações recolhidas ([67]). Os agentes da polícia que realizam a vigilância de emergência fazem-no sob o controlo de um procurador ou, caso seja impossível receber antecipadamente as instruções do procurador devido à necessidade de agir com urgência, a polícia deve obter a aprovação de um procurador imediatamente após o início da execução ([68]). As regras anteriormente descritas sobre a notificação da pessoa aplicam-se também à recolha do conteúdo das comunicações em situações de emergência.

A recolha de informações em situações de emergência deve ser sempre efetuada em conformidade com uma «*declaração de censura/escutas telefónicas de emergência*», e a autoridade responsável pela recolha deve manter um registo de todas as medidas de emergência ([69]). O pedido a um tribunal para que conceda autorização para medidas de emergência deve ser acompanhado de um documento escrito indicando as medidas de restrição das comunicações necessárias, o alvo, o assunto, o âmbito, o período, o local de execução, o método, e uma explicação sobre como as medidas de restrição das comunicações em causa cumprem o artigo 5.º, n.º 1, da Lei relativa à proteção da privacidade das comunicações ([70]), juntamente com documentos de apoio.

Nos casos em que as medidas de emergência são realizadas num curto espaço de tempo, excluindo assim a autorização judicial (por exemplo, se o suspeito for detido imediatamente após o início da interceção, que, por conseguinte, cessa), o diretor da procuradoria competente envia uma notificação da medida de emergência ao tribunal competente ([71]). A notificação deve estabelecer o objetivo, alvo, âmbito, período, local de execução e método de recolha, bem como os fundamentos para não apresentar um pedido de autorização judicial ([72]). Esta notificação permite que o tribunal de receção examine a legalidade da recolha e deve ser inscrita num registo de notificações de medidas de emergência.

([59]) Artigo 9, n.º 3, da Lei relativa à proteção da privacidade das comunicações.
([60]) Artigo 18.º, n.º 1, do Decreto de Execução da Lei relativa à proteção da privacidade das comunicações.
([61]) Artigo 18.º, n.º 2, do Decreto de Execução da Lei relativa à proteção da privacidade das comunicações.
([62]) Artigo 9.º-2, n.º 1, da Lei relativa à proteção da privacidade das comunicações.
([63]) Artigo 9.º-2, n.º 4, da Lei relativa à proteção da privacidade das comunicações.
([64]) Artigo 9.º-2, n.º 5, da Lei relativa à proteção da privacidade das comunicações.
([65]) Artigo 9.º-2, n.º 6, da Lei relativa à proteção da privacidade das comunicações.
([66]) Artigo 8, n.º 1, da Lei relativa à proteção da privacidade das comunicações.
([67]) Artigo 8, n.º 2, da Lei relativa à proteção da privacidade das comunicações.
([68]) Artigo 8.º, n.º 3, da Lei relativa à proteção da privacidade das comunicações e artigo 16.º, n.º 3, do Decreto de Execução da Lei relativa à proteção da privacidade das comunicações.
([69]) Artigo 8, n.º 4, da Lei relativa à proteção da privacidade das comunicações.
([70]) Ou seja, que há uma razão substancial para suspeitar que certos crimes graves estão a ser planeados ou cometidos, ou foram cometidos, e é impraticável de outra forma impedir a prática de um crime, prender o criminoso, ou recolher provas.
([71]) Artigo 8, n.º 5, da Lei relativa à proteção da privacidade das comunicações.
([72]) Artigo 8.º, n.ºs 6 e 7, da Lei relativa à proteção da privacidade das comunicações.

Como requisito geral, o conteúdo das comunicações adquiridas através da execução de medidas de restrição das comunicações com base na Lei relativa à proteção da privacidade das comunicações só pode ser utilizado para investigar, instaurar ação penal ou prevenir os crimes específicos acima enumerados, em processos disciplinares pelos mesmos crimes, em pedidos de indemnização apresentados por uma parte nas comunicações ou quando tal for permitido por outras leis ([73]).

Aplicam-se garantias específicas sempre que sejam recolhidas telecomunicações transmitidas através da Internet ([74]). Tais informações só podem ser utilizadas para investigar os crimes graves enumerados no artigo 5.º, n.º 1, da Lei relativa à proteção da privacidade das comunicações. Para conservar as informações, deve ser obtida aprovação do tribunal que autorizou as medidas de restrição das comunicações ([75]). Um pedido de conservação deve conter informações sobre as medidas de restrição das comunicações, um resumo dos resultados das medidas, as razões para a conservação (juntamente com materiais de apoio) e as telecomunicações a conservar ([76]). Na ausência de tal pedido, as telecomunicações adquiridas devem ser eliminadas no prazo de 14 dias após o termo das medidas de restrição das comunicações ([77]). Se um pedido for rejeitado, as telecomunicações devem ser destruídas no prazo de sete dias ([78]). Sempre que forem eliminadas telecomunicações, deve ser apresentado um relatório no prazo de sete dias junto do tribunal que autorizou as medidas de restrição das comunicações, indicando as razões para a eliminação, bem como os respetivos pormenores e data.

Em termos mais gerais, as informações obtidas ilegalmente através de medidas de restrição das comunicações não são admitidas como elementos de prova em processos judiciais ou disciplinares ([79]). Além disso, a Lei relativa à proteção da privacidade das comunicações proíbe qualquer pessoa que tome medidas de restrição das comunicações de divulgar informações confidenciais obtidas no decurso da implementação dessas medidas e de utilizar as informações obtidas para prejudicar a reputação das pessoas abrangidas pelas mesmas ([80]).

2.2.2.3. Limitações e garantias aplicáveis à recolha de informações de confirmação das comunicações

Com base na Lei relativa à proteção da privacidade das comunicações, as autoridades responsáveis pela aplicação da lei podem solicitar aos operadores de telecomunicações que forneçam dados de confirmação das comunicações quando necessário para conduzir uma investigação ou executar uma sentença ([81]). Ao contrário da recolha de dados sobre os conteúdos, a possibilidade de recolher dados de confirmação das comunicações não se limita a determinados crimes específicos. Contudo, tal como no caso dos dados sobre conteúdos, a recolha de dados de confirmação das comunicações requer autorização prévia por escrito de um tribunal, sujeita às mesmas condições anteriormente descritas ([82]). Quando, por motivos de urgência, seja impossível obter autorização judicial, os dados de confirmação das comunicações podem ser recolhidos sem um mandado, caso em que a autorização deve ser obtida imediatamente após o pedido dos dados e deve ser comunicada ao fornecedor de telecomunicações ([83]). Se não for obtida qualquer autorização subsequente, as informações recolhidas devem ser destruídas ([84]).

Os procuradores, os agentes da polícia judiciária e os tribunais devem manter registos dos pedidos de dados de confirmação das comunicações ([85]). Além disso, os fornecedores de telecomunicações devem informar duas vezes por ano o Ministro da Ciência e das TIC sobre a divulgação de dados de confirmação das comunicações e devem manter registos dos mesmos durante sete anos a partir da data em que os dados tenham sido divulgados ([86]).

Em princípio, as pessoas são notificadas do facto de que os dados de confirmação das comunicações foram recolhidos ([87]). O prazo dessa notificação depende das circunstâncias da investigação ([88]). Uma vez tomada uma decisão de (não) instaurar ação penal, a notificação deve ser enviada no prazo de 30 dias. Em contrapartida, se a dedução de acusação for suspensa, a notificação deve ser enviada no prazo de 30 dias após um ano depois de essa decisão ter sido tomada. Em qualquer caso, a notificação deve ser enviada no prazo de 30 dias após um ano depois de as informações terem sido recolhidas.

A notificação pode ser diferida se for suscetível de 1) pôr em perigo a segurança nacional, a segurança e a ordem públicas, 2) causar a morte ou lesões corporais, 3) impedir um processo judicial justo (por exemplo, levando à

([73]) Artigo 12.º da Lei relativa à proteção da privacidade das comunicações.
([74]) Artigo 12.º- 2 da Lei relativa à proteção da privacidade das comunicações.
([75]) O procurador ou agente da polícia que executa as medidas de restrição das comunicações tem de selecionar as telecomunicações a reter no prazo de 14 dias após o termo das medidas e solicitar a aprovação do tribunal (no caso de uma proposta da polícia, o pedido deve ser apresentado a um procurador que, por sua vez, o apresenta ao tribunal); ver o artigo 12.º-2, n.os 1 e 2, da Lei relativa à proteção da privacidade das comunicações.
([76]) Artigo 12.º-2, n.º 3, da Lei relativa à proteção da privacidade das comunicações.
([77]) Artigo 12.º-2, n.º 5, da Lei relativa à proteção da privacidade das comunicações.
([78]) Artigo 12.º-2, n.º 5, da Lei relativa à proteção da privacidade das comunicações.
([79]) Artigo 4.º da Lei relativa à proteção da privacidade das comunicações.
([80]) Artigo 11.º, n.º 2, do Decreto de Execução da Lei relativa à proteção da privacidade das comunicações.
([81]) Artigo 13, n.º 1, da Lei relativa à proteção da privacidade das comunicações.
([82]) Artigo 13.º e artigo 6.º da Lei relativa à proteção da privacidade das comunicações.
([83]) Artigo 13, n.º 2, da Lei relativa à proteção da privacidade das comunicações. Tal como no caso de medidas urgentes de restrição das comunicações, deve ser elaborado um documento em que os pormenores do processo (o suspeito, as medidas a tomar, o crime suspeito, bem como a urgência) sejam especificados. Ver o artigo 37.º, n.º 5, do Decreto de Execução da Lei relativa à proteção da privacidade das comunicações.
([84]) Artigo 13, n.º 3, da Lei relativa à proteção da privacidade das comunicações.
([85]) Artigo 13.º, n.os 5 e 6, da Lei relativa à proteção da privacidade das comunicações.
([86]) Artigo 13, n.º 7, da Lei relativa à proteção da privacidade das comunicações.
([87]) Ver o artigo 13.º-3, n.º 7, em conjugação com o artigo 9.º-2 da Lei relativa à proteção da privacidade das comunicações.
([88]) Artigo 13.º-3, n.º 1, da Lei relativa à proteção da privacidade das comunicações.

destruição de elementos de prova ou ameaçando testemunhas), ou 4) difamar o suspeito, as vítimas ou outras pessoas relacionadas com o processo, ou invadir a sua privacidade ([89]). A notificação efetuada com base num dos motivos supramencionados requer a autorização do diretor de uma procuradoria distrital competente ([90]). Assim que deixarem de existir motivos para o diferimento, a notificação deve ser efetuada no prazo de 30 dias a partir dessa data ([91]).

As pessoas notificadas podem apresentar um pedido por escrito ao procurador ou agente da polícia judiciária relativamente aos motivos da recolha dos dados de confirmação das comunicações ([92]). Nesse caso, o procurador ou o agente da polícia judiciária deve apresentar os motivos por escrito no prazo de 30 dias após a receção do pedido, a menos que se aplique um dos motivos acima mencionados (exceções para diferimento da notificação) ([93]).

2.2.3. *Divulgação voluntária pelos operadores de atividades de telecomunicações*

O artigo 83.º, n.º 3, da Lei relativa às atividades de telecomunicações permite que os operadores de atividades de telecomunicações cumpram voluntariamente um pedido (feito em apoio de um julgamento criminal, investigação ou execução de uma sentença) de um tribunal, procurador ou diretor de uma agência de investigação, para revelar «dados de comunicações». No contexto da Lei relativa às atividades de telecomunicações, os «*dados de comunicações*» incluem o nome, o número de registo de residente, o endereço e o número de telefone dos utilizadores, as datas em que os utilizadores subscrevem ou cancelam a sua subscrição, bem como os códigos de identificação dos utilizadores (ou seja, os códigos utilizados para identificar o utilizador legítimo dos sistemas informáticos ou das redes de comunicação) ([94]). Para efeitos da Lei relativa às atividades de telecomunicações, só são considerados utilizadores as pessoas que contratam diretamente serviços a um fornecedor de telecomunicações coreano ([95]). Como consequência, as situações em que pessoas da UE cujos dados tenham sido transferidos para a República da Coreia seriam consideradas utilizadores ao abrigo da Lei relativa às atividades de telecomunicações são provavelmente muito limitadas, uma vez que essas pessoas não celebrariam normalmente um contrato direto com um operador de telecomunicações coreano.

Os pedidos de obtenção de dados de comunicações com base na Lei relativa às atividades de telecomunicações devem ser efetuados por escrito e indicar as razões do pedido, a ligação ao utilizador em causa e o âmbito dos dados solicitados ([96]). Em caso de impossibilidade de apresentar um pedido por escrito devido a uma urgência, o pedido escrito deve ser apresentado logo que o motivo da urgência deixe de existir ([97]). Os operadores de atividades de telecomunicações que satisfazem pedidos de divulgação de dados de comunicações devem manter livros que incluam registos indicando que os dados de comunicações foram fornecidos, bem como materiais conexos, como o pedido por escrito ([98]). Além disso, os operadores de atividades de telecomunicações devem informar, duas vezes por ano, o Ministro da Ciência e das TIC sobre o fornecimento de dados de comunicações ([99]).

Não existe qualquer obrigação para os operadores de atividades de telecomunicações de cumprir os pedidos de divulgação de dados de comunicações com base na Lei relativa às atividades de telecomunicações. Cada pedido deve, por conseguinte, ser avaliado pelo operador à luz dos requisitos de proteção de dados aplicáveis no âmbito da Lei relativa à proteção de informações pessoais. Em especial, um operador de atividades de telecomunicações deve ter em conta os interesses do titular dos dados e não pode divulgar as informações se estas forem suscetíveis de infringir injustamente os interesses da pessoa ou de um terceiro ([100]). Além disso, em conformidade com a Notificação n.º 2021--1 relativa às normas complementares para a interpretação e aplicação da Lei relativa à proteção de informações pessoais, a pessoa afetada tem de ser notificada da divulgação. Em situações excecionais, essa notificação pode ser diferida, em particular se e na medida em que a notificação possa comprometer uma investigação penal em curso ou seja suscetível de prejudicar a vida ou a integridade física de outra pessoa, sempre que esses direitos ou interesses sejam manifestamente superiores aos direitos do titular dos dados ([101]).

Em 2016, o Supremo Tribunal confirmou que o fornecimento voluntário de dados de comunicações por operadores de atividades de telecomunicações sem um mandado, com base na Lei relativa às atividades de telecomunicações, não viola, enquanto tal, o direito à autodeterminação informativa do utilizador do serviço de telecomunicações. Ao mesmo tempo, o Tribunal esclareceu que se verificaria tal violação se fosse manifestamente evidente que o organismo requerente abusou da sua autoridade para solicitar a divulgação de dados de comunicações, violando assim os interesses da pessoa em causa ou de um terceiro ([102]). Em termos mais gerais, qualquer pedido de divulgação voluntária por uma autoridade responsável pela aplicação da lei deve respeitar os princípios da legalidade, da necessidade e da proporcionalidade decorrentes da Constituição coreana (artigo 12.º, n.º 1, e artigo 37.º, n.º 2).

([89]) Artigo 13.º-3, n.º 2, da Lei relativa à proteção da privacidade das comunicações.
([90]) Artigo 13.º-3, n.º 3, da Lei relativa à proteção da privacidade das comunicações.
([91]) Artigo 13.º-3, n.º 4, da Lei relativa à proteção da privacidade das comunicações.
([92]) Artigo 13.º-3, n.º 5, da Lei relativa à proteção da privacidade das comunicações.
([93]) Artigo 13.º-3, n.º 6, da Lei relativa à proteção da privacidade das comunicações.
([94]) Artigo 83.º, n.º 3, da Lei relativa às atividades de telecomunicações.
([95]) Artigo 2.º, n.º 9, da Lei relativa às atividades de telecomunicações.
([96]) Artigo 83.º, n.º 4, da Lei relativa às atividades de telecomunicações.
([97]) Artigo 83.º, n.º 4, da Lei relativa às atividades de telecomunicações.
([98]) Artigo 83.º, n.º 5, da Lei relativa às atividades de telecomunicações.
([99]) Artigo 83.º, n.º 6, da Lei relativa às atividades de telecomunicações.
([100]) Artigo 18.º, n.º 2, da Lei relativa à proteção de informações pessoais.
([101]) Notificação n.º 2021-1 da Comissão de Proteção de Informações Pessoais relativa às normas complementares para a interpretação e aplicação da Lei relativa à proteção de informações pessoais, secção III, n.º 2, alínea iii).
([102]) Decisão n.º 2012Da105482 do Supremo Tribunal, de 10 de março de 2016.

2.3. **Supervisão**

A supervisão das autoridades responsáveis pela aplicação do direito penal é efetuada através de diferentes mecanismos, tanto internamente como por organismos externos.

2.3.1. *Auditoria interna*

Em conformidade com a Lei relativa a auditorias do setor público, as autoridades públicas são incentivadas a criar um órgão próprio de auditoria interna, cuja tarefa consiste, entre outras, em proceder ao controlo da legalidade ([103]). Deve ser garantida a maior independência possível aos diretores destes órgãos de auditoria ([104]). Mais especificamente, são nomeados externamente à autoridade em causa (por exemplo, antigos juízes, professores) por um período de dois a cinco anos e só podem ser destituídos por motivos justificados (por exemplo, quando incapazes de desempenhar funções devido a uma perturbação mental ou física, quando objeto de ação disciplinar) ([105]). Da mesma forma, os auditores são nomeados com base em condições específicas estabelecidas na lei ([106]). Os relatórios de auditoria podem incluir recomendações ou pedidos de compensação ou correção, bem como repreensões e recomendações ou pedidos de ação disciplinar ([107]). Estes relatórios são notificados ao diretor da autoridade pública objeto da auditoria, bem como à Comissão de Auditoria e Inspeção (ver ponto 2.3.2) no prazo de 60 dias após a conclusão da auditoria ([108]). A autoridade em causa deve implementar as medidas exigidas e comunicar os resultados à Comissão de Auditoria e Inspeção ([109]). Além disso, os resultados da auditoria são geralmente disponibilizados ao público ([110]). A recusa ou obstrução de uma auditoria interna está sujeita a coimas ([111]). No domínio da aplicação do direito penal, a fim de cumprir a legislação supramencionada, a Agência Nacional de Polícia opera um sistema de inspetores-gerais para tratar das auditorias internas, incluindo no que diz respeito a possíveis violações dos direitos humanos ([112]).

2.3.2. *Comissão de Auditoria e Inspeção*

A Comissão de Auditoria e Inspeção pode inspecionar as atividades das autoridades públicas e, com base nessas inspeções, emitir recomendações, solicitar ações disciplinares ou apresentar uma queixa-crime ([113]). A Comissão de Auditoria e Inspeção é criada sob a égide do Presidente da República da Coreia, mas mantém um estatuto independente no que diz respeito às suas funções ([114]). Além disso, a Lei que cria a Comissão de Auditoria e Inspeção exige que esta conceda plena independência, na medida máxima possível, no que respeita à nomeação, destituição e organização do seu pessoal, bem como à elaboração do seu orçamento ([115]). O presidente da Comissão de Auditoria e Inspeção é nomeado pelo Presidente da República, mediante aprovação da Assembleia Nacional ([116]). Os seis comissários restantes são nomeados pelo Presidente da República, mediante recomendação do presidente, para um mandato de quatro anos ([117]). Os comissários (incluindo o presidente) têm de reunir os requisitos específicos previstos na lei ([118]) só podem ser demitidos em caso de impugnação, condenação a prisão ou incapacidade para desempenhar as suas funções devido a deficiências mentais ou físicas crónicas ([119]). Além disso, os comissários estão proibidos de participar em atividades políticas e de exercer simultaneamente funções na Assembleia Nacional, em serviços administrativos, organizações sujeitas a auditorias e inspeções realizadas pela Comissão de Auditoria e Inspeção ou qualquer outro serviço ou cargo remunerado ([120]).

A Comissão de Auditoria e Inspeção realiza uma auditoria geral anualmente, mas também pode realizar auditorias específicas sobre questões de especial interesse. A Lei relativa à Comissão de Auditoria e Inspeção pode solicitar a apresentação de documentos no decurso de uma inspeção e solicitar a presença de determinadas pessoas ([121]). No âmbito de uma auditoria, a Comissão de Auditoria e Inspeção examina as receitas e despesas do Estado, mas também

([103]) Artigos 3.º e 5.º da Lei relativa a auditorias do setor público.
([104]) Artigo 7.º da Lei relativa a auditorias do setor público.
([105]) Artigos 8.º a 11.º da Lei relativa a auditorias do setor público.
([106]) Artigo 16.º e seguintes da Lei relativa a auditorias do setor público.
([107]) Artigo 23.º, n.º 2, da Lei relativa a auditorias do setor público.
([108]) Artigo 23.º, n.º 1, da Lei relativa a auditorias do setor público.
([109]) Artigo 23.º, n.º 3, da Lei relativa a auditorias do setor público.
([110]) Artigo 26.º da Lei relativa a auditorias do setor público.
([111]) Artigo 41.º da Lei relativa a auditorias do setor público.
([112]) Ver, em particular, as divisões sob responsabilidade do diretor-geral de auditoria e inspeção: https://www.police.go.kr/eng/knpa/org/org01.jsp.
([113]) Artigos 24.º e 31.º a 35.º da Lei relativa à Comissão de Auditoria e Inspeção.
([114]) Artigo 2.º, n.º 1, da Lei relativa à Comissão de Auditoria e Inspeção.
([115]) Artigo 2.º, n.º 2, da Lei relativa à Comissão de Auditoria e Inspeção.
([116]) Artigo 4.º, n.º 1, da Lei relativa à Comissão de Auditoria e Inspeção.
([117]) Artigo 5.º, n.º 1, e artigo 6.º da Lei relativa à Comissão de Auditoria e Inspeção.
([118]) Nomeadamente, terem servido como juízes, procuradores públicos ou advogados durante, pelo menos, dez anos, terem trabalhado no funcionalismo público ou terem sido professores ou ocupado uma posição superior numa universidade durante, pelo menos, oito anos, ou terem trabalhado numa empresa cotada em bolsa ou numa instituição com capitais públicos (dos quais, pelo menos, cinco anos como diretores executivos); ver o artigo 7.º da Lei relativa à Comissão de Auditoria e Inspeção.
([119]) Artigo 8.º da Lei relativa à Comissão de Auditoria e Inspeção.
([120]) Artigo 9.º da Lei relativa à Comissão de Auditoria e Inspeção.
([121]) Ver, por exemplo, o artigo 27.º da Lei relativa à Comissão de Auditoria e Inspeção.

fiscaliza o cumprimento geral das obrigações das autoridades públicas e dos funcionários públicos, com vista a melhorar o funcionamento da administração pública ([122]). Por conseguinte, a sua supervisão excede os aspetos orçamentais e inclui ainda um controlo da legalidade.

2.3.3. *Assembleia Nacional*

A Assembleia Nacional pode investigar e inspecionar as autoridades públicas ([123]). Durante uma investigação ou inspeção, a Assembleia Nacional pode solicitar a divulgação de documentos e obrigar à comparência de testemunhas ([124]). Qualquer pessoa que cometa perjúrio durante uma investigação da Assembleia Nacional está sujeita a sanções penais (pena de prisão até dez anos) ([125]). O processo e os resultados das inspeções podem ser tornados públicos ([126]). Se a Assembleia Nacional constatar a existência de atividade ilegal ou imprópria, pode solicitar que a autoridade pública competente tome medidas corretivas, incluindo a atribuição de indemnizações, a adoção de medidas disciplinares e a melhoria dos seus procedimentos internos ([127]). Na sequência de tal pedido, a autoridade deve agir sem demora e comunicar o resultado à Assembleia Nacional ([128]).

2.3.4. *Comissão de Proteção de Informações Pessoais*

A Comissão de Proteção de Informações Pessoais exerce supervisão sobre o tratamento de informações pessoais pelas autoridades responsáveis pela aplicação do direito penal, em conformidade com a Lei relativa à proteção de informações pessoais. Além disso, nos termos do artigo 7.º-8, n.º 3, e do artigo 7.º-9, n.º 5, da Lei relativa à proteção de informações pessoais, a supervisão da Comissão de Proteção de Informações Pessoais abrange também possíveis infrações às normas que estabelecem as limitações e garantias respeitantes à recolha de informações pessoais, incluindo as contidas nas leis específicas que regulam a recolha de elementos de prova (eletrónicos) para efeitos de aplicação do direito penal (ver ponto 2.2). Dados os requisitos do artigo 3.º, n.º 1, da Lei relativa à proteção de informações pessoais sobre a recolha lícita e leal de informações pessoais, tal infração constitui uma violação da referida lei, permitindo à Comissão de Proteção de Informações Pessoais realizar uma investigação e tomar medidas corretivas ([129]).

No exercício da sua função de supervisão, a Comissão de Proteção de Informações Pessoais tem acesso a todas as informações pertinentes ([130]). A Comissão de Proteção de Informações Pessoais pode aconselhar as autoridades responsáveis pela aplicação da lei a que melhorem o nível de proteção das informações pessoais das suas atividades de tratamento, impor medidas corretivas (por exemplo, suspender o tratamento de dados ou tomar as medidas necessárias para proteger informações pessoais) ou aconselhar a autoridade a que tome medidas disciplinares ([131]). Por último, estão previstas sanções penais para determinadas violações da Lei relativa à proteção de informações pessoais, tais como a utilização ou divulgação ilícita de informações pessoais a terceiros ou o tratamento ilícito de informações sensíveis ([132]). A este respeito, a Comissão de Proteção de Informações Pessoais pode remeter a questão para o organismo de investigação competente (incluindo um procurador) ([133]).

2.3.5. *Comissão Nacional dos Direitos Humanos*

A Comissão Nacional dos Direitos Humanos, um organismo independente encarregado de proteger e promover os direitos fundamentais ([134]), tem o poder de investigar e reparar as violações dos artigos 10.º a 22.º da Constituição, que incluem os direitos à privacidade e à privacidade da correspondência. A Comissão Nacional dos Direitos Humanos é composta por 11 comissários, designados após nomeação pela Assembleia Nacional (quatro), pelo Presidente (quatro) e pelo juiz presidente do Supremo Tribunal (três) ([135]). Para ser nomeado, um comissário tem de 1) ter servido durante, pelo menos, dez anos numa universidade ou num instituto de investigação autorizado, pelo menos como professor associado; 2) ter exercido as funções de juiz, procurador ou advogado durante, pelo menos, dez anos; 3) ter estado envolvido em atividades relacionadas com os direitos humanos durante, pelo menos, dez anos (por exemplo, numa organização não governamental ou internacional sem fins lucrativos); ou 4) ter sido recomendado por grupos da sociedade civil ([136]). O seu presidente é nomeado pelo Presidente da República de entre os comissários e deve ser

([122]) Artigo 20.º e artigo 24.º da Lei relativa à Comissão de Auditoria e Inspeção.
([123]) Artigo 128.º da Lei relativa à Assembleia Nacional e artigos 2.º, 3.º e 15.º da Lei relativa à inspeção e investigação da administração do Estado. Esta inclui inspeções anuais de assuntos governamentais, no seu conjunto, e investigações de questões específicas.
([124]) Artigo 10.º, n.º 1, da Lei relativa à inspeção e investigação da administração do Estado. Ver também os artigos 128.º e 129.º da Lei relativa à Assembleia Nacional.
([125]) Artigo 14.º da Lei relativa a depoimentos, apreciação, etc. perante a Assembleia Nacional.
([126]) Artigo 12.º-2, da Lei relativa à inspeção e investigação da administração do Estado.
([127]) Artigo 16.º, n.º 2, da Lei relativa à inspeção e investigação da administração do Estado.
([128]) Artigo 16.º, n.º 3, da Lei relativa à inspeção e investigação da administração do Estado.
([129]) Ver a Notificação n.º 2021-1 relativa às normas complementares para a interpretação e aplicação da Lei relativa à proteção de informações pessoais.
([130]) Artigo 63.º da Lei relativa à proteção de informações pessoais.
([131]) Artigo 61.º, n.º 2, artigo 65.º, n.ºs 1 e 2 e artigo 64.º, n.º 4, da Lei relativa à proteção de informações pessoais.
([132]) Artigos 70.º a 74.º da Lei relativa à proteção de informações pessoais.
([133]) Artigo 65.º, n.º 1, da Lei relativa à proteção de informações pessoais.
([134]) Artigo 1.º da Lei relativa à Comissão Nacional dos Direitos Humanos.
([135]) Artigo 5.º, n.ºs 1 e 2, da Lei relativa à Comissão Nacional dos Direitos Humanos.
([136]) Artigo 5.º, n.º 3, da Lei relativa à Comissão Nacional dos Direitos Humanos.

confirmado pela Assembleia Nacional ([137]). Os Comissários (incluindo o presidente) são nomeados por um período renovável de três anos e só podem ser demitidos quando forem condenados a penas de prisão ou já não conseguirem desempenhar as suas funções devido a deficiências físicas ou mentais crónicas (caso em que dois terços dos comissários têm de concordar com a destituição) ([138]). Além disso, os Comissários da Comissão Nacional dos Direitos Humanos estão proibidos de exercer um mandato simultâneo na Assembleia Nacional, nos conselhos locais ou em qualquer governo estatal ou local (na qualidade de funcionários públicos) ([139]).

A Comissão Nacional dos Direitos Humanos pode iniciar uma investigação por sua própria iniciativa ou com base numa petição de uma pessoa singular. No âmbito da sua investigação, a Comissão Nacional dos Direitos Humanos pode solicitar a apresentação de materiais pertinentes, realizar inspeções e convocar pessoas para testemunhar ([140]). Na sequência de uma investigação, a Comissão Nacional dos Direitos Humanos pode emitir recomendações para melhorar ou corrigir políticas e práticas específicas, e pode torná-las públicas ([141]). As autoridades públicas devem notificar a Comissão Nacional dos Direitos Humanos de um plano para implementar essas recomendações no prazo de 90 dias após a sua receção ([142]). Além disso, no caso de as recomendações não serem implementadas, a autoridade em causa deve informar a Comissão desse facto ([143]). A Comissão Nacional dos Direitos Humanos pode, por sua vez, comunicar essa omissão à Assembleia Nacional e/ou torná-la pública. Em geral, as autoridades públicas cumprem as recomendações da Comissão Nacional dos Direitos Humanos e têm um forte incentivo para o fazer, uma vez que esse cumprimento foi apreciado no âmbito de uma avaliação geral conduzida pelo Gabinete de Coordenação das Políticas Governamentais, sob a autoridade do Gabinete do Primeiro-Ministro.

2.4. **Vias de recurso individuais**

2.4.1. *Mecanismos de recurso previstos na Lei relativa à proteção de informações pessoais*

No âmbito da Lei relativa à proteção de informações pessoais, as pessoas singulares podem exercer os seus direitos de acesso, retificação, apagamento e suspensão das informações pessoais tratadas pelas autoridades responsáveis pela aplicação do direito penal. O acesso pode ser solicitado diretamente à autoridade competente, ou indiretamente através da Comissão de Proteção de Informações Pessoais ([144]). A autoridade competente só pode limitar ou negar o acesso quando a lei preveja essa possibilidade, quando o mesmo for suscetível de causar danos à vida ou à integridade física de um terceiro ou quando for suscetível de resultar numa violação injustificada do direito de propriedade e de outros interesses de outra pessoa (ou seja, quando os interesses da outra pessoa forem superiores aos interesses da pessoa que apresenta o pedido) ([145]). Se um pedido de acesso for recusado, a pessoa deve ser informada das razões para essa recusa e das vias de recurso ([146]). Da mesma forma, um pedido de retificação ou apagamento pode ser recusado quando tal estiver previsto noutras leis, caso em que a pessoa deve ser informada das razões subjacentes e da possibilidade de apresentar recurso ([147]).

No que diz respeito às vias de recurso, as pessoas singulares podem apresentar uma reclamação junto da Comissão de Proteção de Informações Pessoais, incluindo através do centro de atendimento para a privacidade, gerido pela Agência de Internet e Segurança da Coreia ([148]). Além disso, uma pessoa pode obter mediação através do Comité de Mediação de Litígios de Informações Pessoais ([149]). Estas vias de recurso estão disponíveis tanto no caso de possíveis infrações às regras contidas em leis específicas que estabelecem as limitações e garantias no que respeita à recolha de informações pessoais (ponto 2.2), como à Lei relativa à proteção de informações pessoais. Além disso, as pessoas podem contestar as decisões ou a inação da Comissão de Proteção de Informações Pessoais ao abrigo da Lei relativa ao contencioso administrativo (ver ponto 2.4.3).

([137]) Artigo 5.º, n.º 5, da Lei relativa à Comissão Nacional dos Direitos Humanos.
([138]) Artigo 7.º, n.º 1, e artigo 8.º da Lei relativa à Comissão Nacional dos Direitos Humanos.
([139]) Artigo 10.º da Lei relativa à Comissão Nacional dos Direitos Humanos.
([140]) Artigo 36.º da Lei relativa à Comissão Nacional dos Direitos Humanos. Nos termos do artigo 36.º, n.º 7, da lei, a apresentação de materiais ou artigos pode ser rejeitada se prejudicar a confidencialidade do Estado suscetível de afetar substancialmente a segurança do Estado ou as relações diplomáticas ou constituir um sério obstáculo a uma investigação penal ou a um julgamento pendente. Nesses casos, se necessário para verificar se a recusa em fornecer as informações é justificada, a Comissão pode solicitar informações adicionais ao diretor da agência em causa (que tem de cumprir esse requisito de boa-fé).
([141]) Artigo 25.º, n.º 1, da Lei relativa à Comissão Nacional dos Direitos Humanos.
([142]) Artigo 25.º, n.º 3, da Lei relativa à Comissão Nacional dos Direitos Humanos.
([143]) Artigo 25.º, n.º 4, da Lei relativa à Comissão Nacional dos Direitos Humanos.
([144]) Artigo 35.º, n.º 2, da Lei relativa à proteção de informações pessoais.
([145]) Artigo 35.º, n.º 4, da Lei relativa à proteção de informações pessoais.
([146]) Artigo 42.º, n.º 2, do Decreto de Execução da Lei relativa à proteção de informações pessoais.
([147]) Artigo 36.º, n.ºs 1 e 2, da Lei relativa à proteção de informações pessoais e artigo 43.º, n.º 3, do Decreto de Execução da Lei relativa à proteção de informações pessoais.
([148]) Artigo 62.º da Lei relativa à proteção de informações pessoais.
([149]) Artigos 40.º a 50.º da Lei relativa à proteção de informações pessoais e artigos 48.º-2 a 57.º do Decreto de Execução da Lei relativa à proteção de informações pessoais.

2.4.2. *Vias de recurso junto da Comissão Nacional dos Direitos Humanos*

A Comissão Nacional dos Direitos Humanos trata de reclamações apresentadas por pessoas singulares (tanto coreanas como estrangeiras) relativas a violações dos direitos humanos cometidas por autoridades públicas ([150]). Não existe qualquer requisito de legitimidade de as pessoas singulares apresentarem uma reclamação à Comissão Nacional dos Direitos Humanos ([151]). Como consequência, uma reclamação será tratada pela Comissão Nacional dos Direitos Humanos mesmo que a pessoa em causa não possa demonstrar um dano de facto na fase de admissibilidade. No contexto da recolha de dados pessoais para fins de aplicação do direito penal, uma pessoa não será, por conseguinte, obrigada a demonstrar que as autoridades públicas coreanas de facto acederam às suas informações para que a reclamação seja admissível perante a Comissão Nacional dos Direitos Humanos. Uma pessoa singular pode também solicitar a resolução da reclamação através de mediação ([152]).

Para investigar uma reclamação, a Comissão Nacional dos Direitos Humanos pode utilizar as suas competências de investigação, nomeadamente solicitar a apresentação de materiais pertinentes, realizar inspeções e convocar pessoas para testemunhar ([153]). Se a investigação revelar que ocorreu uma violação das leis pertinentes, a Comissão Nacional dos Direitos Humanos pode recomendar a aplicação de medidas corretivas ou a retificação ou melhoria de qualquer lei, política ou prática pertinente ([154]). As medidas corretivas propostas podem incluir mediação, cessação da violação dos direitos humanos, compensação por danos e medidas que previnam a recorrência das mesmas violações ou de violações semelhantes ([155]). Em caso de recolha ilegal de informações pessoais no quadro das regras aplicáveis, as medidas corretivas podem incluir o apagamento das informações pessoais recolhidas. Caso se considere altamente provável que a violação continue a verificar-se e se considere provável que, se deixada sem vigilância, sejam causados danos difíceis de reparar, a Comissão Nacional dos Direitos Humanos poderá adotar medidas de reparação urgentes ([156]).

Embora a Comissão Nacional dos Direitos Humanos não disponha do poder de obrigar, as suas decisões (por exemplo, uma decisão de não prosseguir a investigação de uma reclamação ([157])) e recomendações podem ser contestadas junto dos tribunais coreanos ao abrigo da Lei relativa ao contencioso administrativo (ver ponto 2.4.3 *infra*) ([158]). Além disso, se as conclusões da Comissão Nacional dos Direitos Humanos revelarem que os dados pessoais foram recolhidos ilegalmente por uma autoridade pública, uma pessoa singular pode procurar outras vias de recurso junto dos tribunais coreanos contra essa autoridade pública, por exemplo, contestando a recolha ao abrigo da Lei relativa ao contencioso administrativo, apresentando uma queixa constitucional ao abrigo da Lei relativa ao Tribunal Constitucional, ou solicitando uma indemnização por danos ao abrigo da Lei relativa às indemnizações do Estado (ver ponto 2.4.3 *infra*).

2.4.3. *Recurso judicial*

As pessoas singulares podem invocar as limitações e garantias descritas nos pontos anteriores para obter reparação perante os tribunais coreanos através de diferentes vias de recurso.

Em primeiro lugar, em conformidade com a Lei relativa ao processo penal, a pessoa em causa e o seu advogado podem estar presentes quando um mandado de busca ou apreensão é executado e, por conseguinte, podem também levantar uma objeção no momento da sua execução ([159]). Além disso, a Lei relativa ao processo penal prevê um mecanismo que permite às pessoas singulares solicitar ao tribunal competente a anulação ou alteração de uma disposição tomada por um procurador ou agente da polícia relativamente a uma apreensão ([160]). Desta forma, as pessoas singulares podem contestar as medidas tomadas para executar um mandado de apreensão.

([150]) Embora o artigo 4.º da Lei relativa à Comissão Nacional dos Direitos Humanos se refira a cidadãos e estrangeiros residentes na República da Coreia, o termo «residente» reflete um conceito de jurisdição e não de território. Por conseguinte, se os direitos fundamentais de um estrangeiro fora da Coreia forem violados por instituições nacionais na Coreia, essa pessoa pode apresentar uma reclamação junto da Comissão Nacional dos Direitos Humanos. Ver, por exemplo, a pergunta correspondente na página de perguntas mais frequentes da Comissão Nacional dos Direitos Humanos, disponível em https://www.humanrights.go.kr/site/ /program/board/basicboard/list?boardtypeid=7025&menuid=002004005001&pagesize=10&currentpage=2. Tal seria o caso se as autoridades públicas coreanas acedessem ilegalmente aos dados pessoais de um estrangeiro transferidos para a Coreia.

([151]) Em princípio, uma reclamação tem de ser apresentada no prazo de um ano a contar da data da violação, mas a Comissão Nacional dos Direitos Humanos pode ainda decidir investigar uma reclamação apresentada após esse prazo, desde que o período de prescrição ao abrigo do direito penal ou civil não tenha expirado (artigo 32.º, n.º 1, ponto 4, da Lei relativa à Comissão Nacional dos Direitos Humanos).

([152]) Artigo 42.º e seguintes da Lei relativa à Comissão Nacional dos Direitos Humanos.

([153]) Artigo 36.º e artigo 37.º da Lei relativa à Comissão Nacional dos Direitos Humanos.

([154]) Artigo 44.º da Lei relativa à Comissão Nacional dos Direitos Humanos.

([155]) Artigo 42.º, n.º 4, da Lei relativa à Comissão Nacional dos Direitos Humanos.

([156]) Artigo 48.º da Lei relativa à Comissão Nacional dos Direitos Humanos.

([157]) Por exemplo, se a Comissão Nacional dos Direitos Humanos não puder, a título excecional, inspecionar determinados materiais ou instalações porque dizem respeito a segredos de Estado suscetíveis de terem um efeito substancial na segurança do Estado ou nas relações diplomáticas, ou se a inspeção apresentar um sério obstáculo a uma investigação criminal ou a um julgamento pendente (ver nota de rodapé 166), e se tal impedir a Comissão Nacional dos Direitos Humanos de realizar a investigação necessária para avaliar os méritos da petição recebida, deve informar a pessoa singular das razões pelas quais a queixa foi rejeitada, em conformidade com o artigo 39.º da Lei relativa à Comissão Nacional dos Direitos Humanos. Nesse caso, a pessoa poderia contestar essa decisão ao abrigo da Lei relativa ao contencioso administrativo.

([158]) Ver, por exemplo, a Decisão n.º 2007NU27259 do Tribunal Superior de Seul, de 18 de abril de 2008, confirmada pela Decisão n.º 2008Du7854 do Supremo Tribunal, de 9 de outubro de 2008; e a Decisão n.º 2017NU69382 do Tribunal Superior de Seul, de 2 de fevereiro de 2018.

([159]) Artigos 121.º e 219.º da Lei relativa ao processo penal.

([160]) Artigo 417.º da Lei relativa ao processo penal, em conjugação com o artigo 414.º, n.º 2, da Lei relativa ao processo penal. Ver também a Decisão n.º 97Mo66 do Supremo Tribunal, de 29 de setembro de 1997.

Além disso, as pessoas singulares podem obter uma indemnização por danos nos tribunais coreanos. Com base na Lei relativa às indemnizações do Estado, as pessoas singulares podem requerer uma indemnização por danos infligidos por funcionários públicos no exercício das suas funções oficiais, em violação da lei ([161]). Um pedido de indemnização ao abrigo da referida lei pode ser apresentado a um «Conselho de Indemnizações» especializado, ou diretamente aos tribunais coreanos ([162]). Se a vítima for um nacional estrangeiro, a Lei relativa às indemnizações do Estado aplica-se desde que o seu país de origem garanta igualmente uma indemnização do Estado aos nacionais coreanos ([163]). De acordo com a jurisprudência, esta condição é preenchida se os requisitos para solicitar uma indemnização no outro país «não forem significativamente desequilibrados entre a Coreia e o outro país» e «não forem geralmente mais rigorosos do que os determinados pela Coreia, não diferindo destes de forma material e substantiva» ([164]). O Código Civil rege a responsabilidade do Estado pela indemnização e, como consequência, a responsabilidade do Estado também abrange os danos não patrimoniais (por exemplo, sofrimento mental) ([165]).

Nos casos de violação das regras de proteção de dados, está prevista uma via de recurso adicional ao abrigo da Lei relativa à proteção de informações pessoais. Nos termos do artigo 39.º da Lei relativa à proteção de informações pessoais, qualquer pessoa singular que sofra danos em resultado de uma violação da Lei relativa à proteção de informações pessoais ou de uma perda, roubo, divulgação, falsificação, alteração ou dano das suas informações pessoais pode obter uma indemnização por danos junto dos tribunais. Não existe qualquer requisito de reciprocidade semelhante ao previsto na Lei relativa às indemnizações do Estado.

Para além da indemnização por danos, pode ser obtida reparação administrativa contra atos ou omissões de serviços administrativos ao abrigo da Lei relativa ao contencioso administrativo. Qualquer pessoa pode contestar um ato (isto é, o exercício ou recusa ao exercício do poder público num caso específico) ou omissão (a não emissão prolongada por parte de um serviço administrativo de um determinado ato, não obstante a sua obrigação legal de o fazer), o que pode levar à revogação/alteração de um ato ilegal, a uma conclusão de nulidade (isto é, a conclusão de que o ato não tem efeito legal ou é inexistente na ordem jurídica) ou a uma conclusão de que uma omissão é ilegal ([166]). Para que seja possível contestá-la, uma disposição administrativa deve ter um impacto direto nos direitos e obrigações civis ([167]). Tal inclui medidas para recolher dados pessoais, seja diretamente (por exemplo, através da interceção de comunicações), seja através de um pedido de divulgação (por exemplo, a um fornecedor de serviços).

As ações supramencionadas podem ser interpostas, em primeiro lugar, junto de comissões de recurso administrativo criadas ao abrigo de determinadas autoridades públicas (por exemplo, o Serviço Nacional de Informações, a Comissão Nacional dos Direitos Humanos) ou junto da Comissão Central de Recursos Administrativos, criada ao abrigo da Comissão de Combate à Corrupção e dos Direitos Civis ([168]). Um recurso administrativo deste tipo proporciona uma via alternativa e mais informal para contestar uma disposição ou omissão de uma autoridade pública. No entanto, também é possível intentar uma ação diretamente nos tribunais coreanos ao abrigo da Lei relativa ao contencioso administrativo.

Um pedido de revogação/alteração de um ato ao abrigo da Lei relativa ao contencioso administrativo pode ser apresentado por qualquer pessoa que tenha um interesse jurídico em solicitar a revogação/alteração ou em ter os seus direitos restabelecidos através da revogação/alteração no caso de o ato ter deixado de produzir efeitos ([169]). Da mesma forma, uma pessoa com um interesse jurídico nessa afirmação pode instaurar uma ação para afirmar a nulidade, enquanto qualquer pessoa, que tenha apresentado um pedido de emissão de um ato e tenha um interesse jurídico em procurar que a ilegalidade da omissão seja afirmada, pode instaurar uma ação para afirmar a ilegalidade de uma omissão ([170]). De acordo com a jurisprudência do Supremo Tribunal, o «interesse jurídico» é interpretado como um «interesse protegido juridicamente», ou seja, um interesse direto e específico protegido pelas disposições legislativas e regulamentares em que se baseiam os atos administrativos (ou seja, não se trata de interesses gerais, indiretos e abstratos do público) ([171]). Por conseguinte, as pessoas têm um interesse jurídico em caso de violação das limitações e garantias aplicáveis à recolha dos seus dados pessoais para efeitos de aplicação do direito penal (ao abrigo de leis específicas ou da Lei relativa à proteção de informações pessoais). Uma decisão transitada em julgado nos termos da Lei relativa ao contencioso administrativo é vinculativa para as partes ([172]).

Um pedido de revogação/alteração de um ato e um pedido de confirmação da ilegalidade de uma omissão devem ser apresentados no prazo de 90 dias a contar da data em que a pessoa toma conhecimento do ato ou omissão

([161]) Artigo 2.º, n.º 1, da Lei relativa às indemnizações do Estado.

([162]) Artigo 9.º e artigo 12.º da Lei relativa às indemnizações do Estado. A lei cria Conselhos Distritais (presididos pelo procurador-adjunto da procuradoria regional correspondente), um Conselho Central (presidido pelo vice-ministro da Justiça) e um Conselho Especial (presidido pelo vice-ministro da Defesa Nacional, encarregado dos pedidos de indemnização por danos infligidos por militares ou funcionários civis das forças armadas). Os pedidos de indemnização são, em princípio, tratados pelos Conselhos Distritais que, em determinadas circunstâncias, têm de transmitir os casos ao Conselho Central/Especial, por exemplo, se a indemnização exceder um determinado montante ou no caso de um indivíduo se candidatar a uma nova deliberação. Todos os Conselhos são compostos por membros nomeados pelo ministro da Justiça (por exemplo, entre os funcionários públicos do Ministério da Justiça, oficiais de justiça, advogados e pessoas com conhecimentos especializados relacionados com indemnizações do Estado) e estão sujeitos a regras específicas em matéria de conflitos de interesses (ver artigo 7.º do Decreto de Execução da Lei relativa às indemnizações do Estado).

([163]) Artigo 7.º da Lei relativa às indemnizações do Estado.

([164]) Decisão n.º 2013Da208388 do Supremo Tribunal, de 11 de junho de 2015.

([165]) Ver o artigo 8.º da Lei relativa às indemnizações do Estado, bem como o artigo 751.º do Código Civil.

([166]) Artigo 2.º e artigo 4.º da Lei relativa ao contencioso administrativo.

([167]) Decisão n.º 98Du18435 do Supremo Tribunal, de 22 de outubro de 1999, Decisão n.º 99Du1113 do Supremo Tribunal, de 8 de setembro de 2000, e Decisão n.º 2010Du3541 do Supremo Tribunal, de 27 de setembro de 2012.

([168]) Artigo 6.º da Lei relativa aos recursos administrativos e artigo 18.º, n.º 1, da Lei relativa ao contencioso administrativo.

([169]) Artigo 12.º da Lei relativa ao contencioso administrativo.

([170]) Artigos 35.º e 36.º da Lei relativa ao contencioso administrativo.

([171]) Decisão n.º 2006Du330 do Supremo Tribunal, de 26 de março de 2006.

([172]) Artigo 30.º, n.º 1, da Lei relativa ao contencioso administrativo.

e, em princípio, o mais tardar um ano a contar da data em que o ato é emitido ou em que a omissão ocorreu, salvo se existirem razões justificáveis ([173]). De acordo com a jurisprudência do Supremo Tribunal, o conceito de «razões justificáveis» deve ser interpretado em sentido lato e exige que se avalie se é socialmente aceitável permitir uma reclamação tardia à luz de todas as circunstâncias do processo ([174]). Tal inclui, nomeadamente, razões para o atraso pelas quais a parte em causa não pode ser responsabilizada (ou seja, situações que escapam ao controlo do autor da reclamação, por exemplo, quando este não foi notificado da recolha das suas informações pessoais) ou motivos de força maior (por exemplo, uma catástrofe natural ou uma guerra).

Por último, as pessoas podem igualmente apresentar uma queixa constitucional junto do Tribunal Constitucional ([175]). Com base na Lei relativa ao Tribunal Constitucional, qualquer pessoa cujos direitos fundamentais garantidos pela Constituição sejam violados pelo exercício, ou pelo não exercício, do poder governamental (excluindo os acórdãos dos tribunais) pode solicitar uma decisão sobre uma queixa constitucional. Se existirem outras vias de recurso, estas devem ser esgotadas em primeiro lugar. De acordo com a jurisprudência do Tribunal Constitucional, os estrangeiros podem apresentar uma queixa constitucional na medida em que os seus direitos fundamentais sejam reconhecidos pela Constituição coreana (ver explicações do ponto 1.1) ([176]). As queixas constitucionais têm de ser apresentadas no prazo de 90 dias a contar da data em que a pessoa tiver tomado conhecimento da infração e no prazo de um ano após a sua ocorrência. Dado que o procedimento da Lei relativa ao contencioso administrativo é aplicado aos litígios ao abrigo da Lei relativa ao Tribunal Constitucional ([177]), uma queixa continuará a ser admissível se existirem «razões justificáveis», tal como interpretadas em conformidade com a jurisprudência do Supremo Tribunal descrita anteriormente.

Se for necessário esgotar outras vias de recurso primeiro, a queixa constitucional deve ser apresentada no prazo de 30 dias a contar da decisão final sobre esse recurso ([178]). O Tribunal Constitucional pode invalidar o exercício do poder governamental que causou a infração ou confirmar a inconstitucionalidade de uma determinada omissão ([179]). Nesse caso, a autoridade competente é obrigada a tomar medidas para cumprir a decisão do Tribunal.

3. ACESSO GOVERNAMENTAL POR MOTIVOS DE SEGURANÇA NACIONAL

3.1. Autoridades públicas competentes em matéria de segurança nacional

A República da Coreia tem dois serviços de informações específicos: o Serviço Nacional de Informações e o Comando de Apoio à Segurança da Defesa. Além destes, a polícia e o Ministério Público também podem recolher informações pessoais para efeitos de segurança nacional.

O Serviço Nacional de Informações é criado pela Lei relativa ao Serviço Nacional de Informações e funciona diretamente sob a jurisdição e supervisão do Presidente ([180]). Em especial, o Serviço Nacional de Informações recolhe, compila e distribui informações sobre países estrangeiros (e sobre a Coreia do Norte) ([181]), informações relacionadas com o combate à espionagem (incluindo espionagem militar e industrial), o terrorismo e as atividades das organizações criminosas internacionais, informações sobre certos tipos de crimes contra a segurança pública e nacional (por exemplo, insurreição interna, agressão estrangeira) e informações relacionadas com a garantia da cibersegurança e a prevenção ou combate a ciberataques e ameaças ([182]). A Lei relativa ao Serviço Nacional de Informações, que cria este serviço e define as suas funções, também define princípios gerais que enquadram todas as suas atividades. Como princípio geral, o Serviço Nacional de Informações deve manter a neutralidade política e proteger a liberdade e os direitos individuais ([183]). Cabe ao presidente do Serviço Nacional de Informações desenvolver orientações gerais que estabelecem os princípios, o âmbito e os procedimentos para o desempenho das suas funções em matéria de recolha e utilização de informações, e tem de comunicá-los à Assembleia Nacional ([184]). A Assembleia Nacional (através do seu Comité de Informações) pode exigir que as orientações sejam corrigidas ou complementadas, se considerar que são ilegais ou injustas. Em termos mais gerais, no exercício das suas funções, o diretor e o pessoal do Serviço Nacional de Informações não podem obrigar nenhuma instituição, organização ou pessoa singular a fazer algo que não seja obrigada a fazer, nem obstruir o exercício dos direitos de qualquer pessoa, abusando da sua autoridade oficial ([185]). Além disso, qualquer censura de correspondência, interceção de telecomunicações, recolha de informações de localização, recolha de dados de confirmação de

([173]) Artigo 20.º da Lei relativa ao contencioso administrativo. Este prazo também se aplica a uma ação para afirmar a ilegalidade de uma omissão; ver o artigo 38.º, n.º 2, da Lei relativa ao contencioso administrativo.
([174]) Decisão n.º 90Nu6521 do Supremo Tribunal, de 28 de junho de 1991.
([175]) Artigo 68.º, n.º 1, da Lei relativa ao Tribunal Constitucional.
([176]) Decisão n.º 99HeonMa194-Ma51 do Tribunal Constitucional, de 29 de novembro de 2001.
([177]) Artigo 40.º da Lei relativa ao Tribunal Constitucional.
([178]) Artigo 69.º da Lei relativa ao Tribunal Constitucional.
([179]) Artigo 75.º, n.º 3, da Lei relativa ao Tribunal Constitucional.
([180]) Artigo 2.º e artigo 4.º, n.º 2, da Lei relativa ao Serviço Nacional de Informações.
([181]) Este conceito não abrange informações relativas a pessoas singulares, mas sim informações gerais relativas a países estrangeiros (tendências, evoluções) e às atividades de intervenientes estatais de países terceiros.
([182]) Artigo 3.º, n.º 1, da Lei relativa ao Serviço Nacional de Informações.
([183]) Artigo 3.º, n.º 1, artigo 6.º, n.º 2, e artigos 11.º e 21.º. Ver também as regras em matéria de conflitos de interesses, em especial os artigos 10.º e 12.º.
([184]) Artigo 4.º, n.º 2, da Lei relativa ao Serviço Nacional de Informações.
([185]) Artigo 13.º da Lei relativa ao Serviço Nacional de Informações.

comunicações ou a gravação ou escuta de comunicações privadas pelo Serviço Nacional de Informações deve estar em conformidade com a Lei relativa à proteção da privacidade das comunicações, a Lei relativa às informações de localização ou a Lei relativa ao processo penal ([186]). Qualquer abuso de poder ou recolha de informações em violação destas leis é passível de sanções penais ([187]).

O Comando de Apoio à Segurança da Defesa é um serviço de informações militares, estabelecida sob a tutela do Ministério da Defesa. É responsável por questões de segurança nas Forças Armadas, investigações criminais militares (sujeitas à Lei relativa ao Tribunal Militar) e informações militares. Em geral, o Comando de Apoio à Segurança da Defesa não efetua a vigilância de civis, a menos que esta seja necessária para o desempenho das suas funções militares. As pessoas que podem ser investigadas são o pessoal militar, os funcionários civis das forças armadas, as pessoas em formação militar, reserva militar ou recrutamento militar e os prisioneiros de guerra ([188]). Ao recolher informações sobre comunicações para efeitos de segurança nacional, o Comando de Apoio à Segurança da Defesa está sujeito às limitações e garantias estabelecidas pela Lei relativa à proteção da privacidade das comunicações e pelo seu decreto de execução.

3.2. **Bases jurídicas e limitações**

A Lei relativa à proteção da privacidade das comunicações, a Lei antiterrorismo para a proteção dos cidadãos e da segurança pública e a Lei relativa às atividades de telecomunicações definem as bases jurídicas para a recolha de informações pessoais para efeitos de segurança nacional e estabelecem as limitações e garantias aplicáveis ([189]). Estas limitações e garantias, descritas nos pontos seguintes, garantem que a recolha e o tratamento de informações se limitem ao estritamente necessário para alcançar um objetivo legítimo. Por conseguinte, encontra-se excluída a recolha maciça e indiscriminada de informações pessoais por razões de segurança nacional.

3.2.1. *Recolha de informações sobre comunicações*

3.2.1.1. Recolha de informações sobre comunicações pelos serviços de informações

3.2.1.1.1. Base jurídica

A Lei relativa à proteção da privacidade das comunicações habilita os serviços de informações a recolher dados sobre comunicações e exige que os prestadores de serviços de comunicação cooperem com as solicitações desses serviços ([190]). Conforme descrito no ponto 2.2.2.1, a Lei relativa à proteção da privacidade das comunicações distingue entre a recolha do conteúdo das comunicações (ou seja, «*medidas de restrição das comunicações*» tais como «*escutas telefónicas*» ou medidas de «*censura*» ([191])) e a recolha de «*dados de confirmação das comunicações*» ([192]).

O limiar para a recolha destes dois tipos de informações difere, mas os procedimentos e garantias aplicáveis são, em grande medida, idênticos ([193]). A recolha de dados de confirmação das comunicações (ou metadados) pode ser realizada com a finalidade de prevenir ameaças à segurança nacional ([194]). Aplica-se um limiar mais elevado à execução de medidas de restrição das comunicações (ou seja, para recolher o conteúdo das comunicações), que só podem ser tomadas quando se prevê que a segurança nacional seja colocada em perigo grave e a recolha de informações seja necessária para prevenir esse perigo (ou seja, se houver um risco grave para a segurança nacional e a recolha for necessária para o prevenir) ([195]). Além disso, o acesso ao conteúdo das comunicações só pode ser efetuado como medida de último recurso para garantir a segurança nacional, e devem ser envidados esforços para minimizar a violação da privacidade das comunicações ([196]). Mesmo quando tiver sido obtida a devida aprovação/autorização, tais medidas devem ser imediatamente interrompidas logo que deixem de ser necessárias, assegurando assim que qualquer violação dos segredos de comunicação da pessoa singular seja limitada ao mínimo ([197]).

3.2.1.1.2. Limitações e garantias aplicáveis à recolha de informações sobre comunicações que envolva, pelo menos, um nacional coreano

A recolha de informações sobre comunicações (tanto conteúdos como metadados) em que uma ou ambas as pessoas envolvidas na comunicação sejam nacionais coreanos só pode ser realizada com a autorização de um juiz presidente do

([186]) Artigo 14.º da Lei relativa ao Serviço Nacional de Informações.
([187]) Artigos 22.º e 23.º da Lei relativa ao Serviço Nacional de Informações.
([188]) Artigo 1.º da Lei relativa ao Tribunal Militar.
([189]) Na investigação de crimes relacionados com a segurança nacional, a polícia e o Serviço Nacional de Informações atuam com base na Lei relativa ao processo penal, enquanto o Comando de Apoio à Segurança da Defesa está sujeito à Lei relativa ao Tribunal Militar.
([190]) Artigo 15.º- 2 da Lei relativa à proteção da privacidade das comunicações.
([191]) Artigo 2.º, n.ºs 6 e 7, da Lei relativa à proteção da privacidade das comunicações.
([192]) Artigo 2, n.º 11, da Lei relativa à proteção da privacidade das comunicações.
([193]) Ver também o artigo 13.º-4, n.º 2, da Lei relativa à proteção da privacidade das comunicações e o artigo 37.º, n.º 4, do respetivo decreto de execução, que estabelecem que os procedimentos aplicáveis à recolha do conteúdo das comunicações se aplicam, com as devidas adaptações, à recolha de dados de confirmação das comunicações.
([194]) Artigo 13.º- 4 da Lei relativa à proteção da privacidade das comunicações.
([195]) Artigo 7, n.º 1, da Lei relativa à proteção da privacidade das comunicações.
([196]) Artigo 3, n.º 2, da Lei relativa à proteção da privacidade das comunicações.
([197]) Artigo 2.º do Decreto de Execução da Lei relativa à proteção da privacidade das comunicações.

Supremo Tribunal ([198]). O pedido do serviço de informações deve ser efetuado por escrito a um procurador ou a uma Procuradoria Superior ([199]). Deve indicar as razões da recolha (ou seja, que é previsível que a segurança nacional seja posta em grave perigo, ou que a recolha seja necessária para prevenir ameaças à segurança nacional), juntamente com os materiais que apoiam essas razões e estabelecem uma presunção *prima facie*, bem como os pormenores do pedido [ou seja, os objetivos, a(s) pessoa(s) visada(s), o âmbito, o período efetivo de recolha, bem como a forma e o local em que a recolha será realizada] ([200]). Por sua vez, o procurador/Procuradoria Superior solicita a autorização de um juiz presidente do Supremo Tribunal ([201]). O juiz presidente do Supremo Tribunal só pode conceder autorização por escrito quando considerar o pedido justificado e rejeitará o pedido quando o considerar infundado ([202]). O mandado especifica o tipo, objetivo, alvo, âmbito e período efetivo de recolha, a forma e o local em que a recolha poderá ser realizada ([203]).

Aplicam-se regras específicas no caso de a medida visar a investigação de um ato de conspiração que ameace a segurança nacional e de existir uma emergência que impossibilite a realização dos procedimentos supramencionados ([204]). Sempre que estas condições estejam reunidas, os serviços de informações podem levar a cabo medidas de vigilância sem aprovação judicial prévia ([205]). No entanto, imediatamente após a execução das medidas de emergência, o serviço de informações deve solicitar a autorização do tribunal. Se a autorização não for obtida no prazo de 36 horas a partir do momento em que as medidas são tomadas, estas devem ser imediatamente suspensas ([206]). A recolha de informações em situações de emergência deve ser sempre efetuada em conformidade com uma «declaração de censura/escutas telefónicas de emergência», e o serviço de informações responsável pela recolha deve manter um registo de todas as medidas de emergência ([207]).

Nos casos em que a vigilância é concluída num curto espaço de tempo, excluindo a autorização do tribunal, o chefe da Procuradoria Superior competente tem de enviar uma notificação da medida de emergência elaborada pelo serviço de informações ao presidente do tribunal competente que mantém o registo de medidas de emergência ([208]). Deste modo, o tribunal fica habilitado a examinar a legalidade da recolha.

3.2.1.1.3. Limitações e garantias aplicáveis à recolha de informações sobre comunicações que envolva apenas nacionais não coreanos

Para recolher informações sobre comunicações exclusivamente entre nacionais não coreanos, os serviços de informações devem obter a aprovação prévia por escrito do Presidente ([209]). Tais comunicações só serão recolhidas para fins de segurança nacional se se enquadrarem numa das várias categorias enumeradas, ou seja, comunicações entre funcionários governamentais ou outras pessoas singulares de países hostis à República da Coreia, agências, grupos ou nacionais estrangeiros suspeitos de envolvimento em atividades contra a Coreia ([210]), ou membros de grupos na Península da Coreia efetivamente fora da soberania da República da Coreia e dos seus grupos de coordenação estabelecidos em países estrangeiros ([211]). Inversamente, se uma parte de uma comunicação for de nacionalidade coreana e a outra de nacionalidade não coreana, será necessária a aprovação do tribunal em conformidade com o procedimento descrito no ponto 3.2.1.1.2.

O chefe de um serviço de informações deve apresentar ao diretor do Serviço Nacional de Informações um plano das medidas a tomar ([212]). O diretor do Serviço Nacional de Informações analisa se o plano é adequado e, se for esse o caso, submete-o à aprovação do Presidente ([213]). As informações que devem ser incluídas no plano são as mesmas que as informações exigidas para um pedido de autorização judicial para recolher informações de nacionais coreanos (conforme descrito supra) ([214]). Deve, em especial, indicar as razões da recolha (ou seja, que é previsível que a segurança nacional

([198]) Artigo 7.º, n.º 1, ponto 1, da Lei relativa à proteção da privacidade das comunicações. O tribunal competente é o tribunal superior com jurisdição sobre o local de residência ou sede de uma ou ambas as partes objeto de vigilância.
([199]) Artigo 7.º, n.º 3, do Decreto de Execução da Lei relativa à proteção da privacidade das comunicações.
([200]) Artigo 7.º, n.º 3, e artigo 6.º, n.º 4, da Lei relativa à proteção da privacidade das comunicações.
([201]) Artigo 7.º, n.º 4, do Decreto de Execução da Lei relativa à proteção da privacidade das comunicações. O pedido do procurador ao tribunal deve expor os principais motivos de suspeita e, caso solicitadas várias autorizações em simultâneo, a respetiva justificação (ver artigo 4.º do Decreto de Execução da Lei relativa à proteção da privacidade das comunicações).
([202]) Artigo 7.º, n.º 3, e artigo 6.º, n.ºs 5 e 9, da Lei relativa à proteção da privacidade das comunicações.
([203]) Artigo 7.º, n.º 3, e artigo 6.º, n.º 6, da Lei relativa à proteção da privacidade das comunicações.
([204]) Artigo 8.º da Lei relativa à proteção da privacidade das comunicações.
([205]) Artigo 8, n.º 1, da Lei relativa à proteção da privacidade das comunicações.
([206]) Artigo 8, n.º 2, da Lei relativa à proteção da privacidade das comunicações.
([207]) Artigo 8, n.º 4, da Lei relativa à proteção da privacidade das comunicações. Ver o ponto 2.2.2.2 anterior relativamente às medidas de emergência no contexto da aplicação da lei.
([208]) Artigo 8.º, n.ºs 5 e 7, da Lei relativa à proteção da privacidade das comunicações. Esta notificação tem de indicar o objetivo, o alvo, o âmbito, o período, o local de execução e o método de vigilância, bem como os motivos para não apresentar um pedido antes de tomar a medida (artigo 8.º, n.º 6, da Lei relativa à proteção da privacidade das comunicações).
([209]) Artigo 7.º, n.º 1, ponto 2, da Lei relativa à proteção da privacidade das comunicações.
([210]) Tal refere-se a atividades que ameaçam a existência e a segurança da nação, a ordem democrática ou a sobrevivência e liberdade do povo.
([211]) Além disso, se uma parte for uma pessoa descrita no artigo 7.º, n.º 1, ponto 2, da Lei relativa à proteção da privacidade das comunicações e a outra for desconhecida ou não puder ser especificada, aplica-se o procedimento previsto no artigo 7.º, n.º 1, ponto 2.
([212]) Artigo 8.º, n.º 1, do Decreto de Execução da Lei relativa à proteção da privacidade das comunicações. O diretor do Serviço Nacional de Informações é nomeado pelo Presidente mediante confirmação do Parlamento (artigo 7.º da Lei relativa ao Serviço Nacional de Informações).
([213]) Artigo 8.º, n.º 2, do Decreto de Execução da Lei relativa à proteção da privacidade das comunicações.
([214]) Artigo 8.º, n.º 3, do Decreto de Execução da Lei relativa à proteção da privacidade das comunicações, em conjugação com o artigo 6.º, n.º 4, da Lei relativa à proteção da privacidade das comunicações.

seja posta em grave perigo, ou que a recolha seja necessária para prevenir ameaças à segurança nacional), os principais motivos de suspeita, juntamente com os materiais que apoiam essas razões e estabelecem uma presunção *prima facie*, bem como os pormenores do pedido [ou seja, os objetivos, a(s) pessoa(s) visada(s), o âmbito, o período efetivo de recolha, bem como a forma e o local em que a recolha será realizada]. Sempre que forem solicitadas várias autorizações, os respetivos motivos e finalidade ([215]).

Em situações de emergência ([216]), deve ser obtida a aprovação prévia do ministro que tutela o serviço de informações em causa. No entanto, neste caso, o serviço de informações deve solicitar a aprovação do Presidente imediatamente após a tomada das medidas de emergência. Se um serviço de informações não obtiver a aprovação no prazo de 36 horas a partir do momento em que o pedido é efetuado, a recolha deve ser imediatamente interrompida ([217]). Nesses casos, as informações recolhidas serão sempre destruídas.

3.2.1.1.4. Limitações e garantias gerais

Quando solicitam a cooperação de entidades privadas, os serviços de informações têm de fornecer ao tribunal o mandado judicial/a autorização presidencial ou uma cópia da capa de uma declaração de censura de emergência, que a entidade visada deve conservar nos seus arquivos ([218]). As entidades a quem é solicitada a divulgação de informações aos serviços de informações com base na Lei relativa à proteção da privacidade das comunicações podem recusar fazê-lo quando a autorização ou a declaração de censura de emergência se refere a um identificador errado (por exemplo, um número de telefone pertencente a uma pessoa diferente da pessoa identificada). Além disso, em todos os casos, as palavras-passe utilizadas nas comunicações não podem ser divulgadas ([219]).

Os serviços de informações podem confiar a aplicação de medidas de restrição das comunicações ou a recolha de informações de confirmação das comunicações a uma estação de correios ou a um prestador de serviços de telecomunicações (como definido pela Lei relativa às atividades de telecomunicações) ([220]). Tanto o serviço de informações em causa como o fornecedor que recebe um pedido de cooperação devem manter registos que indiquem o objetivo do pedido das medidas, a data de execução ou cooperação, e o objeto das medidas (por exemplo, correspondência, telefone, correio eletrónico) durante três anos ([221]). Os prestadores de serviços de telecomunicações que fornecem dados de confirmação das comunicações têm de manter informações sobre a frequência da recolha nos seus ficheiros durante sete anos e apresentar relatórios duas vezes por ano ao ministro da Ciência e das TIC ([222]).

Os serviços de informações têm de comunicar ao diretor do Serviço Nacional de Informações as informações recolhidas e os resultados da atividade de vigilância ([223]). No que respeita aos dados de confirmação das comunicações, devem ser mantidos registos do facto de que foi apresentado um pedido desses dados, bem como do próprio pedido escrito e da instituição que o invocou ([224]).

A recolha do conteúdo das comunicações e dos dados de confirmação das comunicações só pode durar um período máximo de quatro meses e deve ser imediatamente interrompida se o objetivo visado for alcançado mais cedo ([225]). Se as condições de autorização persistirem, o período pode ser prolongado até quatro meses, mediante autorização do tribunal ou a aprovação do Presidente. O pedido de autorização para a prorrogação das medidas de vigilância tem de ser apresentado por escrito, indicando as razões pelas quais a prorrogação é solicitada e fornecendo materiais de apoio ([226]).

Dependendo da base jurídica para a recolha, as pessoas singulares são geralmente notificados quando as suas comunicações são recolhidas. Em especial, independentemente de a informação recolhida dizer respeito ao conteúdo das comunicações ou aos dados de confirmação das comunicações e independentemente de a informação ter sido obtida através do procedimento ordinário ou numa situação de emergência, o diretor do serviço de informações deve notificar a pessoa em causa por escrito da medida de vigilância no prazo de 30 dias a contar da data em que a vigilância terminou ([227]). A notificação tem de incluir 1) o facto de as informações terem sido recolhidas, 2) o serviço de execução e 3) o período de execução. Contudo, se for provável que a notificação ponha em risco a segurança nacional ou cause

([215]) Artigos 8.º, n.º 3, e artigo 4.º do Decreto de Execução da Lei relativa à proteção da privacidade das comunicações.

([216]) Ou seja, nos casos em que a medida visa um ato de conspiração que ameaça a segurança nacional, em que não há tempo suficiente para obter a aprovação do Presidente e em que a não adoção de medidas de emergência pode prejudicar a segurança nacional (artigo 8.º, n.º 8, da Lei relativa à proteção da privacidade das comunicações).

([217]) Artigo 8, n.º 9, da Lei relativa à proteção da privacidade das comunicações.

([218]) Artigo 9.º, n.º 2, da Lei relativa à proteção da privacidade das comunicações e artigo 12.º do Decreto de Execução da Lei relativa à proteção da privacidade das comunicações.

([219]) Artigo 9, n.º 4, da Lei relativa à proteção da privacidade das comunicações.

([220]) Artigo 13.º do Decreto de Execução da Lei relativa à proteção da privacidade das comunicações.

([221]) Artigo 9.º, n.º 3, da Lei relativa à proteção da privacidade das comunicações e artigo 17, n.º 2, do Decreto de Execução da Lei relativa à proteção da privacidade das comunicações. Este prazo não se aplica aos dados de confirmação das comunicações (ver artigo 39.º do Decreto de Execução da Lei relativa à proteção da privacidade das comunicações).

([222]) Artigo 13.º, n.º 7, da Lei relativa à proteção da privacidade das comunicações e artigo 39.º do Decreto de Execução da Lei relativa à proteção da privacidade das comunicações.

([223]) Artigo 18.º, n.º 3, do Decreto de Execução da Lei relativa à proteção da privacidade das comunicações.

([224]) Artigo 13.º, n.º 5, e artigo 13.º-4, n.º 3, da Lei relativa à proteção da privacidade das comunicações.

([225]) Artigo 7, n.º 2, da Lei relativa à proteção da privacidade das comunicações.

([226]) Artigo 7.º, n.º 2, da Lei relativa à proteção da privacidade das comunicações e artigo 5.º do Decreto de Execução da Lei relativa à proteção da privacidade das comunicações.

([227]) Artigo 9.º-2, n.º 3, da Lei relativa à proteção da privacidade das comunicações. Nos termos do artigo 13.º-4 da Lei relativa à proteção da privacidade das comunicações, tal aplica-se tanto à recolha do conteúdo das comunicações como aos dados de confirmação das comunicações.

danos à vida e à segurança física das pessoas, a notificação pode ser diferida ([228]). A notificação deve ser apresentada no prazo de 30 dias, assim que os motivos para o diferimento deixarem de existir ([229]).

Este requisito de notificação apenas se aplica à recolha de informações em que, pelo menos, uma das partes seja um nacional coreano. Consequentemente, os nacionais não coreanos só serão notificados quando as suas comunicações com nacionais coreanos forem recolhidas. Por conseguinte, não há lugar a qualquer requisito de notificação quando são recolhidas comunicações exclusivamente entre nacionais não coreanos.

O conteúdo de quaisquer comunicações, bem como os dados de confirmação das comunicações, adquiridos através de vigilância com base na Lei relativa à proteção da privacidade das comunicações, só podem ser utilizados 1) para fins de investigação, ação penal ou prevenção de certos crimes, 2) para processos disciplinares, 3) para processos judiciais em que uma parte relacionada com a comunicação os invoque num pedido de indemnização ou 4) com base noutras leis ([230]).

3.2.1.2. Recolha de informações sobre comunicações pela polícia/procuradores para efeitos de segurança nacional

A polícia/procurador pode recolher informações sobre comunicações (tanto o conteúdo das comunicações como os dados de confirmação das comunicações) para fins de segurança nacional nas mesmas condições descritas no ponto 3.2.1.1. Quando atua em situações de emergência ([231]), o procedimento aplicável é o descrito anteriormente em relação à recolha do conteúdo das comunicações para fins de aplicação da lei em situações de emergência (ou seja, o artigo 8.º da Lei relativa à proteção da privacidade das comunicações).

3.2.2. *Recolha de informações sobre suspeitos de terrorismo*

3.2.2.1. Base jurídica

A Lei antiterrorismo autoriza o diretor do Serviço Nacional de Informações a recolher informações sobre suspeitos de terrorismo ([232]). «*Suspeito de terrorismo*» define-se como um membro de um grupo terrorista ([233]), uma pessoa que tenha feito propaganda a um grupo terrorista (promovendo e divulgando ideias ou táticas de um grupo terrorista), angariado ou contribuído com fundos para o terrorismo ([234]), ou tenha estado envolvida noutras atividades de preparação, conspiração, propaganda ou instigação do terrorismo, ou uma pessoa sobre quem existam bons motivos para suspeitar que tenha conduzido tais atividades ([235]). Como regra geral, qualquer funcionário público que aplique a Lei antiterrorismo tem de respeitar os direitos básicos consagrados na Constituição coreana ([236]).

A Lei antiterrorismo não estabelece por si só poderes específicos, limitações e garantias para a recolha de informações sobre suspeitos de terrorismo, mas remete para os procedimentos previstos noutras leis. Em primeiro lugar, com base na Lei antiterrorismo, o diretor do Serviço Nacional de Informações pode recolher 1) informações sobre a entrada e a saída da República da Coreia, 2) informações sobre transações financeiras e 3) informações sobre comunicações. Consoante o tipo de informações solicitadas, os requisitos processuais pertinentes são indicados na Lei relativa à imigração e no Código Aduaneiro, na Lei relativa à comunicação e utilização de informações específicas sobre transações financeiras ou na Lei relativa à proteção da privacidade das comunicações, respetivamente ([237]). No caso da recolha de informações sobre a entrada e a saída da Coreia, a Lei antiterrorismo remete para os procedimentos estabelecidos na Lei relativa à imigração e no Código Aduaneiro. No entanto, estas leis não preveem atualmente tais poderes. No caso da recolha de informações sobre comunicações e transações financeiras, a Lei antiterrorismo remete para as limitações e garantias previstas na Lei relativa à proteção da privacidade das comunicações (especificadas mais adiante) e na Lei relativa à

([228]) Artigo 9.º-2, n.º 4, da Lei relativa à proteção da privacidade das comunicações.
([229]) Artigo 13.º-4, n.º 2, e artigo 9.º-2, n.º 6, da Lei relativa à proteção da privacidade das comunicações.
([230]) Artigo 5.º, n.ºs 1 e 2, e artigos 12.º e 13.º-5 da Lei relativa à proteção da privacidade das comunicações.
([231]) Ou seja, quando a medida visa um ato de conspiração que ameaça a segurança nacional e existe uma emergência que torna impossível passar pelo procedimento ordinário de aprovação (artigo 8.º, n.º 1, da Lei relativa à proteção da privacidade das comunicações).
([232]) Artigo 9.º da Lei antiterrorismo.
([233]) «*Grupo terrorista*» define-se como um grupo de terroristas conforme designado pelas Nações Unidas (artigo 2.º, n.º 2, da Lei antiterrorismo).
([234]) «*Terrorismo*» é definido no artigo 2.º, n.º 1, da Lei antiterrorismo como um comportamento levado a cabo com a finalidade de impedir o exercício da autoridade do Estado, de um governo local ou de um governo estrangeiro (incluindo governos locais e organizações internacionais), ou com a finalidade de o obrigar a conduzir qualquer atividade que não tenha a obrigação legal de conduzir, ou de ameaçar o público. O referido comportamento inclui a) matar uma pessoa ou colocar em risco a sua vida ao causar-lhe lesões corporais ou prender, confinar, raptar uma pessoa ou tomá-la como refém; b) determinados tipos de conduta que visam uma aeronave (por exemplo, despenhar, sequestrar ou danificar uma aeronave em voo); c) determinados tipos de conduta relacionados com um navio (por exemplo, apreender um navio ou estrutura marítima em operação, destruir um navio ou estrutura marítima em operação ou infligir-lhe danos a um nível que ponha em perigo a sua segurança, incluindo danificar a carga a bordo de um navio ou estrutura marítima em operação); d) colocar, detonar ou utilizar de qualquer outra forma uma arma ou dispositivo bioquímico, explosivo ou incendiário com a intenção de causar a morte, ferimentos graves ou danos materiais graves ou que tenha esse efeito em certos tipos de veículos ou instalações (por exemplo, comboios, elétricos, veículos automóveis, parques e estações públicos, instalações de fornecimento de eletricidade, gás e telecomunicações, etc.); e) determinados tipos de conduta relacionados com materiais nucleares, materiais radioativos ou instalações nucleares (por exemplo, lesar a vida humana, a integridade física ou bens, ou de outra forma perturbar a segurança pública, destruindo um reator nuclear ou manipulando indevidamente materiais radioativos, etc.).
([235]) Artigo 2.º, n.º 3, da Lei antiterrorismo.
([236]) Artigo 3.º, n.º 3, da Lei antiterrorismo.
([237]) Artigo 9.º, n.º 1, da Lei antiterrorismo.

comunicação e utilização de informações específicas sobre transações financeiras (que, tal como explicado na secção 2.1, não é pertinente para efeitos da avaliação da decisão de adequação).

Além disso, o artigo 9.º, n.º 3, da Lei antiterrorismo especifica que o diretor do Serviço Nacional de Informações pode solicitar informações pessoais ou informações sobre a localização de um suspeito de terrorismo a um responsável pelo tratamento de informações pessoais ([238]) ou a um fornecedor de informações de localização ([239]). Esta possibilidade é limitada aos pedidos de divulgação voluntária, aos quais os responsáveis pelo tratamento de informações pessoais e os fornecedores de informações de localização não são obrigados a responder e, em qualquer caso, só podem fazê-lo em conformidade com a Lei relativa à proteção de informações pessoais e a Lei relativa às informações de localização (ver ponto 3.2.2.2 *infra*).

3.2.2.2. Limitações e salvaguardas aplicáveis à divulgação voluntária nos termos da Lei relativa à proteção de informações pessoais e da Lei relativa às informações de localização

Os pedidos de cooperação voluntária ao abrigo da Lei antiterrorismo devem ser limitados a informações sobre suspeitos de terrorismo (ver ponto 3.2.2.1 *supra*). Qualquer pedido do Serviço Nacional de Informações neste sentido deve respeitar os princípios da legalidade, da necessidade e da proporcionalidade decorrentes da Constituição coreana (artigo 12.º, n.º 1, e artigo 37.º, n.º 2) ([240]), bem como os requisitos da Lei relativa à proteção de informações pessoais para a recolha de informações pessoais (artigo 3.º, n.º 1, da Lei relativa à proteção de informações pessoais; ver ponto 1.2 *supra*). A Lei relativa ao Serviço Nacional de Informações especifica ainda que este serviço não pode obrigar nenhuma instituição, organização ou pessoa singular a fazer algo que não seja obrigada a fazer, nem obstruir o exercício dos direitos de qualquer pessoa, abusando da sua autoridade oficial ([241]). Uma violação desta proibição pode ser passível de sanções penais ([242]).

Os responsáveis pelo tratamento de informações pessoais e os fornecedores de informações de localização que recebem pedidos do Serviço Nacional de Informações com base na Lei antiterrorismo não são obrigados a satisfazer tais pedidos. Podem satisfazê-los voluntariamente, mas só estão autorizados a fazê-lo em conformidade com a Lei relativa à proteção de informações pessoais e a Lei relativa a informações de localização. No respeitante à conformidade com a Lei relativa à proteção de informações pessoais, o responsável pelo tratamento deve ter em especial conta os interesses do titular dos dados e não pode divulgar as informações se estas forem suscetíveis de infringir injustamente os interesses da pessoa singular ou de um terceiro ([243]). Além disso, em conformidade com a Notificação n.º 2021-1 relativa às normas complementares para a interpretação e aplicação da Lei relativa à proteção de informações pessoais, a pessoa afetada tem de ser notificada da divulgação. Em situações excecionais, essa notificação pode ser diferida, em particular se e na medida em que a notificação possa comprometer uma investigação penal em curso ou seja suscetível de prejudicar a vida ou a integridade física de outra pessoa, sempre que esses direitos ou interesses sejam manifestamente superiores aos direitos do titular dos dados ([244]).

3.2.2.3. Limitações e garantias nos termos da Lei relativa à proteção da privacidade das comunicações

Com base na Lei antiterrorismo, os serviços de informações só podem recolher informações sobre comunicações (tanto o conteúdo das comunicações como os dados de confirmação das comunicações) quando necessário para atividades de combate ao terrorismo, ou seja, atividades relacionadas com a prevenção do terrorismo e contramedidas contra o terrorismo. Os procedimentos da Lei relativa à proteção da privacidade das comunicações descritos no ponto 3.2.1 aplicam-se à recolha de informações de comunicação para fins de combate ao terrorismo.

3.2.3. *Divulgação voluntária pelos operadores de atividades de telecomunicações*

Com base na Lei relativa às atividades de telecomunicações, os operadores de atividades de telecomunicações podem dar cumprimento a um pedido de divulgação de «dados sobre comunicações» de um serviço de informações que pretenda recolher as informações com vista a prevenir uma ameaça para a segurança nacional ([245]). Qualquer pedido neste sentido deve respeitar os princípios da legalidade, da necessidade e da proporcionalidade decorrentes da Constituição coreana (artigo 12.º, n.º 1, e artigo 37.º, n.º 2) ([246]), bem como os requisitos da Lei relativa à proteção de informações pessoais para a recolha de informações pessoais (artigo 3.º, n.º 1, da Lei relativa à proteção de informações pessoais; ver ponto 1.2 *supra*). Além disso, aplicam-se as mesmas limitações e garantias que em relação à divulgação voluntária para fins de aplicação da lei (ver ponto 2.2.3) ([247]).

([238]) Conforme definido no artigo 2.º da Lei relativa à proteção de informações pessoais, ou seja, uma instituição pública, pessoa coletiva, organização, pessoa singular, etc. que trata informações pessoais, direta ou indiretamente, a fim de gerir os ficheiros de informações pessoais para fins oficiais ou comerciais.

([239]) Conforme definido no artigo 5.º da Lei relativa à proteção, utilização, etc. de informações de localização (a seguir designada por «Lei relativa a informações de localização»), ou seja, qualquer pessoa que tenha obtido autorização da Comissão das Comunicações da Coreia para se envolver numa atividade de informações de localização.

([240]) Ver também o artigo 3.º, n.ºs 2 e 3, da Lei antiterrorismo.

([241]) Artigo 11.º, n.º 1, da Lei relativa ao Serviço Nacional de Informações.

([242]) Artigo 19.º da Lei relativa Serviço Nacional de Informações.

([243]) Artigo 18.º, n.º 2, da Lei relativa à proteção de informações pessoais.

([244]) Notificação n.º 2021-1 da Comissão de Proteção de Informações Pessoais relativa às normas complementares para a interpretação e aplicação da Lei relativa à proteção de informações pessoais, secção III, n.º 2, alínea iii).

([245]) Artigo 83.º, n.º 3, da Lei relativa às atividades de telecomunicações.

([246]) Ver também o artigo 3.º, n.ºs 2 e 3, da Lei antiterrorismo.

([247]) Em especial, o pedido deve ser efetuado por escrito e indicar as respetivas razões, bem como a ligação ao utilizador em causa e o âmbito das informações solicitadas, e o fornecedor de serviços de telecomunicações deve manter registos e informar o ministro da Ciência e das TIC duas vezes por ano.

Um operador de serviços de telecomunicações não é obrigado a satisfazer o pedido, mas pode fazê-lo numa base voluntária e apenas em conformidade com a Lei relativa à proteção de informações pessoais. A este respeito, as mesmas obrigações, incluindo no que respeita à notificação da pessoa singular, são aplicáveis aos operadores de atividades de telecomunicações quando recebem pedidos das autoridades responsáveis pela aplicação do direito penal, tal como explicado em maior pormenor na secção 2.2.3.

3.3. **Supervisão**

Diferentes organismos supervisionam as atividades dos serviços de informações coreanos. A supervisão do Comando de Apoio à Segurança da Defesa é conduzida pelo Ministério da Defesa Nacional, em conformidade com a Diretiva do Ministério relativa à Implementação da Auditoria Interna. O Serviço Nacional de Informações está sujeito à supervisão do executivo, da Assembleia Nacional e de outros organismos independentes, como se explica em mais pormenor a seguir.

3.3.1. *Responsável pela proteção dos direitos humanos*

Quando os serviços de informações recolhem informações sobre suspeitos de terrorismo, a Lei antiterrorismo prevê a supervisão pela Comissão de Luta contra o Terrorismo e pelo responsável pela proteção dos direitos humanos ([248]).

Nomeadamente, a Comissão de Luta contra o Terrorismo desenvolve políticas relativas às atividades de luta contra o terrorismo e supervisiona a aplicação de medidas antiterrorismo, bem como as atividades das diferentes autoridades competentes no domínio do combate ao terrorismo ([249]). A Comissão é presidida pelo primeiro-ministro e composta por vários ministros e diretores de agências governamentais, incluindo os ministros dos Negócios Estrangeiros, da Justiça, da Defesa Nacional e do Interior e da Segurança, o diretor do Serviço Nacional de Informações, o comissário-geral da Agência Nacional de Polícia e o presidente da Comissão dos Serviços Financeiros ([250]). Na condução de investigações antiterroristas e na deteção de suspeitos de terrorismo para recolher informações ou materiais necessários às atividades antiterroristas, o diretor do Serviço Nacional de Informações deve informar o presidente da Comissão de Luta contra o Terrorismo (ou seja, o primeiro-ministro) ([251]).

Além disso, a Lei antiterrorismo cria o responsável pela proteção dos direitos humanos com vista a proteger os direitos fundamentais das pessoas singulares contra violações causadas pelas atividades de combate ao terrorismo ([252]). O responsável pela proteção dos direitos humanos é nomeado pelo presidente da Comissão de Luta contra o Terrorismo de entre pessoas que reúnam as qualificações enumeradas no Decreto de Execução da Lei antiterrorismo [ou seja, qualquer pessoa qualificada como advogado com, pelo menos, dez anos de experiência profissional, ou com conhecimentos especializados no domínio dos direitos humanos e que esteja ou tenha estado ao serviço (pelo menos) como professor associado durante, pelo menos, dez anos, ou como funcionário público superior em organismos estatais ou administrações locais, ou com, pelo menos, dez anos de experiência profissional no domínio dos direitos humanos, por exemplo, numa organização não governamental] ([253]). O responsável pela proteção dos direitos humanos é nomeado por dois anos (com possibilidade de renovação do mandato) e só pode ser destituído por motivos específicos e limitados e justa causa, por exemplo, quando acusado num processo penal relacionado com as suas funções, quando divulga informações confidenciais, ou devido a incapacidade mental ou física prolongada ([254]).

Em termos de competências, o responsável pela proteção dos direitos humanos pode emitir recomendações para melhorar a proteção dos direitos humanos por parte dos serviços envolvidos em atividades antiterroristas, bem como processar petições civis (ver ponto 3.4.3) ([255]). Quando seja possível estabelecer razoavelmente a existência de uma violação dos direitos humanos no exercício de funções oficiais, o responsável pela proteção dos direitos humanos pode recomendar ao diretor do serviço responsável que corrija tal violação ([256]). Por seu turno, o serviço responsável tem de notificar o responsável pela proteção dos direitos humanos das medidas tomadas para aplicar essa recomendação ([257]). Se um serviço não aplicar uma recomendação do responsável pela proteção dos direitos humanos, a questão será elevada à Comissão, incluindo ao seu presidente, o primeiro-ministro. Até à data, não se verificaram situações em que as recomendações do responsável pela proteção dos direitos humanos não tenham sido aplicadas.

3.3.2. *Assembleia Nacional*

Conforme descrito no ponto 2.3.2, a Assembleia Nacional pode inspecionar as autoridades públicas e, nesse contexto, pode solicitar a divulgação de documentos e obrigar à comparência de testemunhas. No que diz respeito a assuntos da jurisdição do Serviço Nacional de Informações, esta supervisão parlamentar é levada a cabo pelo Comité de Informações da Assembleia Nacional ([258]). O diretor do Serviço Nacional de Informações, que supervisiona o desempenho de funções

([248]) Artigo 7.º da Lei antiterrorismo.
([249]) Artigo 5.º, n.º 3, da Lei antiterrorismo.
([250]) Artigo 3.º, n.º 1, do Decreto de Execução da Lei antiterrorismo.
([251]) Artigo 9.º, n.º 4, da Lei antiterrorismo.
([252]) Artigo 7.º da Lei antiterrorismo.
([253]) Artigo 7.º, n.º 1, do Decreto de Execução da Lei antiterrorismo.
([254]) Artigo 7.º, n.º 3, do Decreto de Execução da Lei antiterrorismo.
([255]) Artigo 8.º, n.º 1, do Decreto de Execução da Lei antiterrorismo.
([256]) Artigo 9.º, n.º 1, do Decreto de Execução da Lei antiterrorismo. O responsável pela proteção dos direitos humanos tem autonomia para decidir sobre a adoção de recomendações, mas tem de as comunicar ao presidente da Comissão de Luta contra o Terrorismo.
([257]) Artigo 9.º, n.º 2, do Decreto de Execução da Lei antiterrorismo.
([258]) Artigo 36.º e artigo 37.º, n.º 1, ponto 16, da Lei relativa à Assembleia Nacional.

por parte do serviço, responde perante o Comité de Informações (bem como perante o Presidente) ([259]). O próprio Comité de Informações pode também solicitar um relatório sobre uma matéria específica, a que o diretor do Serviço Nacional de Informações é obrigado a responder sem demora ([260]). O diretor só pode recusar-se a responder ou a testemunhar perante o Comité de Informações no que respeita a segredos de Estado relativos a questões militares, diplomáticas ou relacionadas com a Coreia do Norte em que o conhecimento público possa ter um impacto grave no destino nacional ([261]). Neste caso, o Comité de Informações pode solicitar uma explicação ao primeiro-ministro. Se tal explicação não for apresentada no prazo de sete dias após a apresentação do pedido, a resposta ou testemunho deixa de poder ser recusado.

Se a Assembleia Nacional determinar que ocorreu atividade ilegal ou imprópria, pode solicitar que a autoridade pública competente tome medidas corretivas, incluindo a atribuição de indemnizações, a adoção de medidas disciplinares e a melhoria dos seus procedimentos internos ([262]). Na sequência de tal pedido, a autoridade deve agir sem demora e comunicar o resultado à Assembleia Nacional. Existem regras específicas relativas à supervisão parlamentar no que diz respeito à utilização de medidas de restrição das comunicações (ou seja, a recolha do conteúdo das comunicações) nos termos da Lei relativa à proteção da privacidade das comunicações ([263]). No que se refere a esta última, a Assembleia Nacional pode solicitar aos diretores dos serviços de informações um relatório sobre qualquer medida específica de restrição das comunicações. Além disso, pode conduzir inspeções no local dos equipamentos de escuta telefónica. Por último, os serviços de informações que tenham recolhido informações sobre conteúdos e os operadores que as tenham divulgado para fins de segurança nacional têm de apresentar um relatório sobre essa divulgação, a pedido da Assembleia Nacional.

3.3.3. *Comissão de Auditoria e Inspeção*

A Comissão de Auditoria e Inspeção desempenha as mesmas funções de supervisão em relação aos serviços de informações que no domínio da aplicação do direito penal (ver ponto 2.3.2) ([264]).

3.3.4. *Comissão de Proteção de Informações Pessoais*

No que respeita ao tratamento de dados para fins de segurança nacional, incluindo a fase de recolha, a Comissão de Proteção de Informações Pessoais conduz supervisão adicional. Conforme explicado em mais pormenor no ponto 1.2, tal inclui os princípios e obrigações gerais estabelecidos no artigo 3.º e no artigo 58.º, n.º 4, da Lei relativa à proteção de informações pessoais, bem como o exercício dos direitos individuais garantidos pelo artigo 4.º da Lei relativa à proteção de informações pessoais. Além disso, nos termos do artigo 7.º-8, n.ºs 3 e 4, e do artigo 7.º-9, n.º 5, da Lei relativa à proteção de informações pessoais, a supervisão da Comissão de Proteção de Informações Pessoais também abrange possíveis infrações às regras contidas em leis específicas que estabelecem as limitações e garantias relativas à recolha de informações pessoais, tais como a Lei relativa à proteção da privacidade das comunicações, a Lei antiterrorismo e a Lei relativa às atividades de telecomunicações. Por força dos requisitos previstos no artigo 3.º, n.º 1, da Lei relativa à proteção de informações pessoais para a recolha lícita e leal de informações pessoais, qualquer infração a essas leis constitui uma violação da Lei relativa à proteção de informações pessoais. A Comissão de Proteção de Informações Pessoais tem assim o poder de investigar ([265]) violações das leis que regem o acesso aos dados para fins de segurança nacional, bem como das regras de tratamento estabelecidas na Lei relativa à proteção de informações pessoais, e de emitir recomendações de melhoria, impor medidas corretivas, recomendar ação disciplinar e remeter potenciais infrações às autoridades de investigação pertinentes ([266]).

3.3.5. *Comissão Nacional dos Direitos Humanos*

A supervisão por parte da Comissão Nacional dos Direitos Humanos aplica-se nos mesmos moldes aos serviços de informações e a outras autoridades governamentais (ver ponto 2.3.2).

3.4. **Vias de recurso individuais**

3.4.1. *Recurso junto do responsável pela proteção dos direitos humanos*

No que diz respeito à recolha de informações pessoais no contexto de atividades de luta contra o terrorismo, o responsável pela proteção dos direitos humanos representa uma via de recurso específica, estabelecida no âmbito da Comissão de Luta contra o Terrorismo. O responsável pela proteção dos direitos humanos trata de petições civis relacionadas com a violação dos direitos humanos decorrente das atividades de luta contra o terrorismo ([267]). Pode recomendar medidas corretivas e o serviço em causa deve comunicar ao responsável quaisquer medidas tomadas para aplicar essa recomendação. Não existe qualquer requisito de legitimidade de as pessoas singulares apresentarem uma reclamação junto do responsável pela proteção dos direitos humanos. Consequentemente, o responsável pela proteção dos direitos humanos tratará uma reclamação mesmo que a pessoa em causa não possa demonstrar um dano de facto na fase de admissibilidade.

([259]) Artigo 18.º da Lei relativa Serviço Nacional de Informações.

([260]) Artigo 15.º, n.º 2, da Lei relativa ao Serviço Nacional de Informações.

([261]) Artigo 17.º, n.º 2, da Lei relativa ao Serviço Nacional de Informações. Os «segredos de Estado» são definidos como «*os factos, bens ou conhecimentos classificados como segredos de Estado, cujo acesso é apenas permitido a um número limitado de pessoas e que não devem ser divulgados a nenhum outro país ou organização, a fim de evitar qualquer desvantagem grave para a segurança nacional*»; ver o artigo 13.º, n.º 4, da Lei relativa ao Serviço Nacional de Informações.

([262]) Artigo 16.º, n.º 2, da Lei relativa à inspeção e investigação da administração do Estado.

([263]) Artigo 15.º da Lei relativa à proteção da privacidade das comunicações.

([264]) Como no caso do Comité de Informações da Assembleia Nacional, o diretor do Serviço Nacional de Informações só pode recusar responder à Comissão de Auditoria e Inspeção relativamente a matérias que constituam segredos de Estado e na eventualidade de o seu conhecimento público vir a ter um impacto grave na segurança nacional (artigo 13.º, n.º 1, da Lei relativa ao Serviço Nacional de Informações).

([265]) Artigo 63.º da Lei relativa à proteção de informações pessoais.

([266]) Artigo 61.º, n.º 2, artigo 65.º, n.ºs 1 e 2 e artigo 64.º, n.º 4, da Lei relativa à proteção de informações pessoais.

([267]) Artigo 8.º, n.º 1, ponto 2, do Decreto de Execução da Lei antiterrorismo.

3.4.2. *Mecanismos de recurso previstos na Lei relativa à proteção de informações pessoais*

No âmbito da Lei relativa à proteção de informações pessoais, as pessoas singulares podem exercer os seus direitos de acesso, retificação, apagamento e suspensão das informações pessoais tratadas para efeitos de segurança nacional ([268]). Os requerimentos para exercer estes direitos podem ser diretamente apresentados ao serviço de informações ou indiretamente através da Comissão de Proteção de Informações Pessoais. O serviço de informações só pode retardar, limitar ou recusar o exercício do direito na medida e durante o tempo necessário e proporcionado para proteger um objetivo importante de interesse público (por exemplo, na medida e durante o tempo em que a concessão do direito possa pôr em risco uma investigação em curso ou ameaçar a segurança nacional), ou quando a concessão do direito possa lesar vida ou a integridade física de um terceiro. Se o pedido for recusado ou restringido, a pessoa deve ser notificada sem demora dos motivos.

Além disso, nos termos do artigo 58.º, n.º 4, da Lei relativa à proteção de informações pessoais (requisito para assegurar o tratamento adequado de queixas individuais) e do artigo 4.º, n.º 5, da Lei relativa à proteção de informações pessoais (direito à reparação adequada de quaisquer danos resultantes do tratamento de informações pessoais, através de um procedimento rápido e justo), as pessoas singulares têm o direito de obter reparação. Este inclui o direito de denunciar uma alegada violação junto do centro de atendimento para a privacidade, gerido pela Agência de Internet e Segurança da Coreia e de apresentar uma queixa junto da Comissão de Proteção de Informações Pessoais ([269]). Estas vias de recurso estão disponíveis tanto no caso de possíveis infrações às regras contidas em leis específicas que estabelecem as limitações e garantias no que respeita à recolha de informações pessoais para efeitos de segurança nacional como da Lei relativa à proteção de informações pessoais. Conforme explicado na Notificação n.º 2021-1, uma pessoa singular da UE pode apresentar uma denúncia à Comissão de Proteção de Informações Pessoais através da sua autoridade nacional responsável pela proteção de dados. Nesse caso, a Comissão de Proteção de Informações Pessoais notificará a pessoa através da autoridade nacional responsável pela proteção de dados uma vez concluída a investigação (incluindo, se for caso disso, informações sobre as medidas corretivas impostas). É possível recorrer contra as decisões ou a inação por parte da Comissão de Proteção de Informações Pessoais perante os tribunais coreanos ao abrigo da Lei relativa ao contencioso administrativo.

3.4.3. *Vias de recurso junto da Comissão Nacional dos Direitos Humanos*

A possibilidade de obter reparação individual junto da Comissão Nacional dos Direitos Humanos aplica-se nos mesmos moldes aos serviços de informações e a outras autoridades governamentais (ver ponto 2.4.2).

3.4.4. *Recurso judicial*

Tal como no caso das atividades das autoridades de aplicação do direito penal, as pessoas singulares podem obter reparação judicial contra os serviços de informações relativamente às violações das limitações e garantias supramencionadas através de diferentes vias.

Em primeiro lugar, as pessoas singulares podem obter uma indemnização por danos nos termos da Lei relativa às indemnizações do Estado. Num caso específico, por exemplo, a indemnização foi concedida relativamente à vigilância ilegal por parte do Comando de Apoio à Defesa (o predecessor do Comando de Apoio à Segurança da Defesa) ([270]).

Em segundo lugar, a Lei relativa ao contencioso administrativo permite que as pessoas singulares contestem atos e omissões por parte de serviços administrativos, incluindo os serviços de informações ([271]).

Por último, as pessoas singulares podem apresentar uma queixa constitucional junto do Tribunal Constitucional contra medidas tomadas pelos serviços de informações com base na Lei relativa ao Tribunal Constitucional.

([268]) Artigo 3.º, n.º 5, e artigo 4.º, n.ºs 1, 3 e 4, da Lei relativa à proteção de informações pessoais.
([269]) Artigo 62.º e artigo 63.º, n.º 2, da Lei relativa à proteção de informações pessoais.
([270]) Decisão n.º 96Da42789 do Supremo Tribunal, de 24 de julho de 1998.
([271]) Artigos 3.º e 4.º da Lei relativa ao contencioso administrativo.