Parecer do Comité [artigo 70.º, n.º1, alínea s)]

Parecer 28/2018

relativo à proposta de decisão de execução da Comissão Europeia

sobre a proteção adequada dos dados pessoais no Japão

Adotado em 5 de dezembro de 2018

Translations proofread by EDPB Members.
This language version has not yet been proofread.

Índice

O Comité Europeu para a Proteção de Dados

Tendo em conta o artigo 70.º, n.º 1, alínea s), do 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 (a seguir «Regulamento Geral sobre a Proteção de Dados»),

Tendo em conta o Acordo EEE e, nomeadamente, o seu anexo XI e o seu Protocolo n.º 37, com a redação que lhe foi dada pela Decisão do Comité Misto do EEE n.º 154/2018, de 6 de julho de 2018,

Tendo em conta o artigo 12.º e o artigo 22.º do seu Regulamento de Processo, de 25 de maio de 2018,

ADOTOU O PRESENTE PARECER:

1 SUMÁRIO EXECUTIVO

1. A Comissão Europeia aprovou o seu projeto de decisão de execução em matéria de proteção adequada dos dados pessoais pelo Japão, em conformidade com o Regulamento Geral sobre a Proteção de Dados (a seguir designado GDPR)[1] em 5 de setembro de 2018[2]. Em seguida, a Comissão Europeia deu início ao procedimento para a sua adoção formal.

2. Em 25 de setembro de 2018, a Comissão Europeia solicitou o parecer do Comité Europeu para a Proteção de Dados («CEPD»)[3]. A Comissão foi convidada a fornecer ao CEPD toda a documentação necessária no que diz respeito a este país, incluindo toda a correspondência pertinente com o governo do Japão.

3. À luz dos debates realizados com o CEPD, a Comissão Europeia alterou duas vezes o seu projeto de decisão de adequação, tendo enviado a sua última versão em 13 de novembro de 2018[4] O CEPD baseou o seu presente parecer na sua versão mais recente do projeto de decisão de execução (a seguir «projeto de decisão de adequação»).

4. A avaliação pelo CEPD do nível de proteção assegurado pela decisão de adequação da Comissão foi realizada com base na análise da própria decisão, bem como na análise da documentação disponibilizada[5] pela Comissão.[6]

5. O CEPD centrou-se na avaliação dos aspetos comerciais do projeto de decisão de adequação e do acesso do governo aos dados pessoais transferidos da UE para efeitos de aplicação da lei e de

[1] 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.
[2] Ver comunicado de imprensa http://europa.eu/rapid/press-release_IP-18-5433_pt.htm.
[3] Nos termos do artigo 70.º, n.º 1, alínea s), do RGPD.
[4] Ver o anexo I do parecer do CEPD para a versão atualizada do projeto de decisão de execução da Comissão Europeia.
[5] Ver o anexo II do parecer do CEPD relativo à lista de documentos não fornecidos pela Comissão Europeia ao CEPD.
[6] O CEPD baseou a sua análise nas traduções apresentadas pelas autoridades japonesas verificadas pela Comissão Europeia

segurança nacional, incluindo as vias de recurso legal disponíveis para os cidadãos da UE. O CEPD também avaliou se as garantias previstas no quadro jurídico japonês são aplicadas e eficazes.

6. O CEPD utilizou como principal referência para este trabalho o seu referencial de adequação[7] adotado em fevereiro de 2018.

1.1 Domínios de convergência

7. O principal objetivo do CEPD consiste em dar um parecer à Comissão Europeia sobre o nível de proteção concedido às pessoas no quadro japonês. É importante reconhecer que o CEPD não espera que o quadro jurídico japonês reproduza a legislação europeia em matéria de proteção de dados.

8. No entanto, o CEPD recorda que, para se considerar que é concedido um nível de proteção adequado, a jurisprudência do TJUE, bem como o artigo 45.º do RGPD, exigem que a legislação do país terceiro esteja conforme a essência dos princípios fundamentais consagrados no RGPD. Nos domínios da proteção de dados, o CEPD observa ainda que existem áreas fundamentais de alinhamento entre o quadro do RGPD e o quadro japonês no que diz respeito a determinadas disposições fundamentais, como a exatidão e a minimização dos dados, a limitação da conservação, a segurança dos dados, a limitação das finalidades e uma autoridade de controlo independente, a Comissão de Proteção das Informações Pessoais (CPP).

9. Adicionalmente, o CEPD congratula-se com os esforços envidados pela Comissão Europeia e pelas autoridades japonesas para garantir que o Japão conceda um nível de proteção adequado ao do RGPD, nomeadamente preenchendo as lacunas entre o RGPD e o quadro japonês de proteção de dados mediante a adoção de regras adicionais por parte da CPP aplicáveis apenas aos dados pessoais transferidos da UE para o Japão, as normas complementares. Por exemplo, o CEPD observa que a CPP concordou em tratar outras categorias de dados como dados sensíveis (os dados sensíveis ao abrigo da legislação japonesa não incluem a orientação sexual nem a filiação sindical). Além disso, as normas complementares garantem que os direitos dos titulares dos dados serão aplicados a todos os dados pessoais transferidos a partir da UE, independentemente do seu período de conservação (enquanto o sistema jurídico japonês prevê que os direitos dos titulares dos dados não se aplicam aos dados pessoais que devem ser apagados no prazo de seis meses).

10. O CEPD observa igualmente os esforços da Comissão Europeia para reforçar a decisão de adequação em resposta às preocupações manifestadas pelo CEPD.

1.2 Desafios gerais

11. Não obstante, subsistem desafios e o CEPD sugere as áreas a seguir como as principais que devem ser reforçadas e cuidadosamente acompanhadas no sistema japonês.

12. O primeiro desafio diz respeito à monitorização desta nova arquitetura de adequação, que combina um quadro jurídico existente com normas complementares específicas para assegurar que será um sistema sustentável e fiável que não levantará **questões práticas relacionadas com o cumprimento concreto e eficiente** por parte das entidades japonesas e com a execução por parte da CPP.

13. Em segundo lugar, o CEPD regista os repetidos compromissos e garantias da Comissão Europeia e das autoridades japonesas no que respeita à natureza vinculativa e executória das normas complementares, convidando simultaneamente a Comissão Europeia a **acompanhar de forma contínua o seu caráter vinculativo e a sua aplicação efetiva no Japão**, uma vez que o seu valor jurídico é um elemento absolutamente essencial da adequação UE – Japão. No que diz respeito às orientações

[7] GT254, referencial de adequação, 6 de fevereiro de 2018.

da CPP, o CEPD gostaria de receber esclarecimentos no projeto de decisão de adequação em relação **ao seu caráter vinculativo e solicita à Comissão que acompanhe atentamente este aspeto**[8].

1.3 Aspetos comerciais específicos

14. No domínio dos aspetos comerciais do projeto de decisão de adequação UE – Japão, o CEPD tem algumas preocupações específicas e gostaria de solicitar esclarecimentos relativamente a algumas questões importantes.

1.3.1 Preocupações do CEPD no que diz respeito aos princípios fundamentais em matéria de proteção de dados

15. O CEPD congratula-se com o facto de as normas complementares excluírem os dados pessoais transferidos da UE que são posteriormente transferidos para um país terceiro com base no sistema de normas transnacionais de proteção da privacidade da APEC. Além disso, o CEPD reconhece que, no seu novo projeto de decisão de adequação, a Comissão Europeia se comprometeu a suspender a decisão de adequação quando as transferências subsequentes já não asseguram a continuidade da proteção.

16. Ao abrigo da legislação japonesa, uma das bases jurídicas para as transferências subsequentes é o reconhecimento de um país terceiro como estando a proporcionar um nível de proteção adequado ao do Japão. No entanto, a avaliação de um país terceiro como adequado pelo Japão não parece incluir as «normas complementares» negociadas entre a Comissão Europeia e a CPP, que se aplicam apenas aos dados pessoais da UE para assegurar um nível de proteção essencialmente equivalente ao das normas do RGPD. Por conseguinte, os dados pessoais da UE transferidos do Japão para outro país terceiro não reconhecido como tendo um quadro de proteção de dados essencialmente equivalente ao RGPD com base numa adequação do Japão deixarão de beneficiar da proteção específica dos dados pessoais da UE.

17. **No entanto, deve ter-se em conta que podem ocorrer transferências subsequentes de dados pessoais para países terceiros que sejam objeto de uma eventual decisão de adequação japonesa posterior. Estes países terceiros não podem ter sido objeto de uma avaliação prévia ou de constatação de adequação da UE. Nesta fase, a Comissão deve assumir o seu papel de controlo e assegurar que se mantém o nível de proteção dos dados da UE ou ponderar a suspensão desta decisão de adequação.**

18. Além disso, o CEPD exprime reservas quanto às **obrigações de consentimento e transparência** dos responsáveis pelo tratamento de dados (PIIHBO). O CEPD procedeu a uma verificação cuidadosa destes elementos, uma vez que, de uma forma diferente da legislação europeia em matéria de proteção de dados, a utilização do consentimento como base para o tratamento e para as transferências tem um papel central no sistema jurídico japonês. Por exemplo, o CEPD tem dúvidas quanto ao conceito de consentimento, que não está definido de forma a incluir o direito de retirada, um elemento essencial ao abrigo da legislação da UE para garantir o verdadeiro controlo do titular dos dados sobre os seus dados pessoais. No que diz respeito às obrigações de transparência de um PIHBO, existem dúvidas quanto ao facto de serem prestadas informações proativas aos titulares dos dados.

19. O CEPD está preocupado com o facto de o **sistema de recurso japonês** poder não ser de acesso fácil aos cidadãos da UE que necessitam de apoio ou que pretendam apresentar uma denúncia, tendo em conta o facto de o apoio da CPP se encontrar disponível apenas através da linha de apoio e apenas em japonês. Existe a mesma questão com o serviço de mediação prestado pela CPP, uma vez que o sistema não é publicitado na versão inglesa do sítio Web da CPP, ao passo que os documentos informativos

[8] Ver secção 1.3.4 do presente parecer para mais informações.

importantes, como as perguntas frequentes relativamente à LPDP, também estão disponíveis apenas em japonês. A este respeito, o CEPD veria com bons olhos que a Comissão debatesse com a CPP a possibilidade de criar um serviço em linha, pelo menos em inglês, destinado a prestar apoio e a tratar as denúncias de indivíduos na UE – semelhante ao previsto no anexo II da presente decisão de adequação. A Comissão Europeia terá também de acompanhar de perto a eficácia das sanções e das vias de recurso pertinentes.

1.3.2 Necessidade de clarificação

20. O CEPD gostaria de receber garantias relativamente a alguns aspetos do projeto de decisão de adequação que necessitam de mais esclarecimentos.

21. Trata-se, por exemplo, de alguns conceitos fundamentais da legislação japonesa. Mais especificamente, verifica-se uma falta de clareza relativamente ao **estatuto do chamado «administrador fiduciário»**- um termo que se assemelha ao subcontratante do RGPD, mas cuja capacidade para determinar e alterar as finalidades e os meios de tratamento dos dados pessoais permanece ambígua.

22. O CEPD necessitará igualmente de garantias devido à falta de documentos pertinentes no que diz respeito às **restrições aos direitos dos indivíduos** (em especial, os direitos de acesso, retificação e objeção) serem ou não necessárias e proporcionadas numa sociedade democrática e respeitarem a essência dos direitos fundamentais.

23. O CEPD espera também que a Comissão Europeia acompanhe de perto a proteção eficaz dos **dados pessoais transferidos da UE para o Japão, com base no projeto de decisão de adequação, ao longo de todo o seu «ciclo de vida»**, apesar de a legislação japonesa impor uma obrigação de conservação de registos da origem dos dados por um período máximo de três anos.

1.4 Relativamente ao acesso das autoridades públicas aos dados transferidos para o Japão

24. O CEPD analisou também o quadro jurídico aplicável às entidades governamentais japonesas aquando do acesso aos dados pessoais transferidos da UE para o Japão para efeitos de aplicação da lei ou de segurança nacional. Embora reconhecendo as garantias fornecidas pelo governo japonês, referidas como o anexo II do projeto de decisão de adequação, o CEPD identificou vários aspetos preocupantes e que necessitam de esclarecimento, dos quais se destacam os apresentados a seguir.

25. No domínio da aplicação da lei, o CEPD observa que os princípios jurídicos aplicáveis aos dados de acesso parecem frequentemente ser semelhantes aos da UE, na medida em que estejam disponíveis. No entanto, a falta de traduções disponíveis de vários textos jurídicos e de jurisprudência relevante torna difícil concluir que todos os procedimentos de acesso aos dados são necessários e proporcionados e que a aplicação de tais princípios é feita de forma «essencialmente equivalente» ao direito da União.

26. No domínio da segurança nacional, o CEPD reconhece que o governo japonês reafirmou que as informações apenas podem ser obtidas a partir de fontes de acesso livre ou através de divulgação voluntária por parte das empresas, e que não recolhe informações sobre o público em geral. No entanto, está ciente das preocupações expressas pelos peritos e nos meios de comunicação social e gostaria de receber mais esclarecimentos no que diz respeito às medidas de vigilância por parte das entidades governamentais japonesas.

27. No que diz respeito à reparação legal dos cidadãos da UE, no domínio da aplicação da lei e da segurança nacional, o CEPD congratula-se com o facto de a Comissão Europeia e o governo japonês terem

negociado um mecanismo adicional para que os cidadãos da UE lhes proporcionem uma via de recurso adicional, alargando assim os poderes da autoridade responsável pela proteção de dados japonesa. No entanto, um aspeto que suscita preocupação continua a ser o facto de este novo mecanismo não compensar totalmente as deficiências da supervisão e das vias de recurso ao abrigo da legislação japonesa. O CEPD procura, assim, mais esclarecimentos para garantir que este novo mecanismo compensa plenamente tais deficiências.

1.5 Conclusão

28. O CEPD considera que esta decisão de adequação é de importância primordial. Desde a entrada em vigor do RGPD, a primeira decisão de adequação constituirá **um precedente para futuros pedidos de adequação, bem como para a revisão das decisões de adequação proferidas ao abrigo da Diretiva 95/46[9].** É igualmente importante sublinhar que as pessoas estão cada vez mais conscientes do impacto da globalização na sua vida privada e recorrem às suas autoridades de supervisão para assegurar que estão previstas garantias adequadas quando os seus dados pessoais são transferidos para o estrangeiro. Face a estas implicações, o CEPD considera que a Comissão Europeia deve assegurar que não existem deficiências na proteção oferecida pela adequação UE-Japão e que este tipo específico de adequação está em consonância com os requisitos do artigo 45.º do RGPD.

29. O CEPD congratula-se com os esforços envidados pela Comissão Europeia e pela CPP japonesa para alinhar tanto quanto possível o quadro jurídico japonês com o quadro jurídico europeu. **As melhorias** introduzidas pelas normas complementares para colmatar algumas das diferenças entre os dois quadros são muito importantes e bem recebidas.

30. No entanto, na sequência de uma análise cuidadosa do projeto de decisão de adequação da Comissão, bem como do quadro japonês de proteção de dados, o CEPD verifica que **subsistem algumas preocupações, associadas à necessidade de esclarecimentos adicionais**. Adicionalmente, este tipo específico de adequação, que combina um quadro nacional existente com regras específicas adicionais, suscita também questões sobre a sua execução operacional. Tendo em conta o que precede, o CEPD recomenda à Comissão Europeia que dê resposta às preocupações e pedidos de esclarecimento apresentados pelo CEPD e forneça mais provas e explicações no que diz respeito às questões suscitadas. O CEPD convida igualmente a Comissão Europeia a proceder a uma revisão desta constatação de adequação pelo menos de dois em dois anos e não de quatro em quatro anos como sugerido no atual projeto de decisão de adequação.

2 INTRODUÇÃO

2.1 Quadro japonês em matéria de proteção de dados

31. O quadro japonês relativo à proteção de dados foi muito recentemente modernizado, em 2017. Este quadro inclui vários pilares, em que existe um direito comum geral, a Lei da Proteção de Dados Pessoais (LPDP). Outro elemento importante da legislação é a resolução ministerial de entrada em vigor da LPDP («Resolução ministerial»), que especifica determinados princípios fundamentais da LPDP.

32. Com base numa decisão do Concelho de Ministros, adotada em 12 de junho de 2018[10], e no artigo 6.º da LPDP, que delega na CPP o poder de «*tomar as medidas necessárias para colmatar as diferenças*

[9] Diretiva n.º 95/46/CE do Parlamento Europeu e do Conselho, de 24 de outubro de 1995, relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados.
[10] O CEPD observa que, de acordo com o projeto de decisão de adequação, esta decisão do Conselho de Ministros foi adotada em 12 de junho de 2018. No entanto, o CEPD recebeu apenas o projeto de decisão do Concelho de Ministros, com data de abril de 2018.

entre os sistemas e operações entre o Japão e o país estrangeiro em causa, a fim de assegurar o tratamento adequado dos dados pessoais recebidos desse país»[11]. A decisão do Concelho de Ministros sugere igualmente que as regras adotadas pela CPP que complementem e vão além das estabelecidas na LPDP seriam vinculativas e aplicáveis aos operadores comerciais japoneses[12].

33. Por conseguinte, a CPP encetou negociações com a Comissão Europeia e adotou, em junho de 2018, regras mais rigorosas do que as da LPDP e da resolução ministerial que devem ser aplicadas aos dados transferidos da UE. Estas são as normas complementares ao abrigo da lei da proteção de dados pessoais para o tratamento dos dados pessoais transferidos da UE com base numa decisão de adequação, a seguir designadas por «normas complementares»[13]. Estas normas complementares são igualmente anexadas ao projeto de decisão de execução da Comissão publicado em julho de 2018.

34. É importante notar que as normas complementares só são aplicáveis aos dados pessoais transferidos da União Europeia para o Japão com base na decisão de adequação e visam reforçar a proteção aplicável a esses dados. Como tal, não são aplicáveis a dados pessoais de pessoas no Japão ou provenientes de outros países que não os do EEE.

35. Além disso, o CEPD gostaria de chamar a atenção para o facto de a LPDP alterada ter entrado em vigor em 30 de maio de 2017 e a CPP, na sua forma atual, ter sido criada em 2016. Além disso, as normas complementares negociadas pela CPP com a Comissão Europeia ainda não entraram em vigor, uma vez que tal dependerá do reconhecimento do Japão pela Comissão Europeia como uma jurisdição adequada à da UE.

2.2 Âmbito da avaliação do CEPD

36. O projeto de decisão de adequação da Comissão Europeia é o resultado de uma avaliação das regras japonesas relativas à proteção dos dados, seguida de negociações com as autoridades japonesas. O resultado destas negociações está refletido, nomeadamente, nos dois anexos anexados ao projeto de decisão de adequação: o primeiro prevê proteções adicionais que os operadores comerciais japoneses terão de aplicar ao tratamento de dados pessoais transferidos da UE, enquanto o segundo contém garantias e compromissos do governo japonês relativamente ao acesso das autoridades públicas aos dados.

37. O CEPD analisou o quadro japonês de proteção de dados, as normas complementares negociadas pela Comissão Europeia e as garantias e compromissos do governo japonês. O CEPD deverá emitir um parecer independente sobre as constatações da Comissão Europeia, identificar insuficiências no quadro de adequação, se for caso disso, e procurar propor alterações para resolvê-las.

38. Tal como mencionado no referencial de adequação do CEPD, *«as informações fornecidas pela Comissão Europeia devem ser exaustivas e colocar o CEPD em posição de proceder a uma avaliação própria do nível de proteção de dados no país terceiro»[14].*

39. No entanto, o CEPD recebeu a maioria dos documentos traduzidos para inglês, mencionados no projeto de decisão de adequação, que constituem uma parte essencial do sistema jurídico japonês. Por conseguinte, o CEPD disponibiliza o presente parecer com base na análise dos documentos em inglês. O CEPD considerou o quadro aplicável em matéria de proteção de dados na União Europeia,

[11] Decisão do Conselho de Ministros de 25 de abril de 2018.
[12] Ver Secção 1.3.4 infra para mais informações.
[13] Normas complementares, anexo I da Decisão de Execução da Comissão de XXXX, nos termos do Regulamento (CE) n.º 2016/679 do Parlamento Europeu e do Conselho sobre o nível de proteção adequado concedido pelo Japão aos dados pessoais, enviadas ao CEPD em setembro de 2018.
[14] GT254, p.3.

nomeadamente o artigo 8.º da Convenção Europeia dos Direitos do Homem (a seguir designado por «CEDH») que protege o direito à vida privada e familiar, bem como os artigos 7.º, 8.º e 47.º da Carta dos Direitos Fundamentais da União Europeia (a seguir designada por «Carta»), os quais consagram, respetivamente, o direito à proteção da vida privada e familiar, o direito à proteção dos dados pessoais e o direito à ação e a um tribunal imparcial. Além do acima referido, o CEPD considerou os requisitos do RGPD, bem como a jurisprudência relevante.

40. O objetivo deste exercício é assegurar que o quadro japonês de proteção de dados é essencialmente equivalente ao da União Europeia. O conceito de «nível de proteção adequado», que já existia ao abrigo da Diretiva 95/46, foi aprofundado pelo TJUE. É importante recordar a norma estabelecida pelo TJUE no acórdão Schrems, ou seja, que, embora o «nível de proteção» no país terceiro deva ser «essencialmente equivalente» ao garantido na UE, «a este respeito, os meios a que esse país terceiro recorre para efeitos desse nível de proteção podem diferir dos que são utilizados na [UE]»[15]. Por conseguinte, o objetivo não é refletir a legislação europeia, mas definir os requisitos essenciais da legislação em apreço. A adequação pode ser alcançada através de uma combinação de direitos para os titulares dos dados e de obrigações relativamente aos que tratam dados ou que exercem controlo sobre esse tratamento e supervisão por órgãos independentes. No entanto, as regras relativas à proteção de dados só são eficazes se forem executórias e forem seguidas na prática. Por conseguinte, para além do conteúdo das regras aplicáveis aos dados pessoais transferidos para um país terceiro ou uma organização internacional, é necessário considerar também o sistema em vigor para garantir a eficácia dessas regras. A eficácia dos mecanismos de execução é fundamental para a eficácia das regras de proteção dos dados[16].

2.3 Observações e preocupações gerais

2.3.1 Especificidades deste tipo de decisão de adequação

41. A adequação UE-Japão é a primeira a ser analisada relativamente ao novo cenário jurídico do RGPD. Tal torna o trabalho do CEPD mais importante à luz dos efeitos deste projeto de decisão de adequação nos pedidos de adequação futuros.

42. A adequação UE-Japão também seria a primeira mútua. Quando e se a UE reconhecer que o Japão proporciona um nível de proteção essencialmente equivalente ao do RGPD, o Japão emitirá também a sua própria decisão de adequação nos termos do artigo 24.º da LPDP, reconhecendo que a UE oferece um nível de proteção adequado ao abrigo do quadro japonês de proteção de dados. Assim, esta adequação UE-Japão prevista é de natureza específica que o CEPD considerou na sua avaliação. Tal como acima referido, a CPP japonesa negociou com a Comissão Europeia regras específicas e mais rigorosas, aplicáveis apenas aos dados pessoais transferidos da UE. Estas regras mais rigorosas são vinculativas e aplicáveis em conformidade com a decisão do Conselho de Ministros e devem ser respeitadas por todos os operadores de empresas responsáveis pelo tratamento de dados pessoais (a seguir designados «PIIHBO») no Japão aquando do tratamento de dados pessoais provenientes da UE ao abrigo do presente projeto de decisão de adequação.

43. Por conseguinte, a Comissão Europeia baseou a sua constatação de adequação não apenas no atual quadro geral japonês de proteção de dados, mas também nas regras específicas em vigor. O facto de as normas complementares terem de complementar a LPDP é indicativo do facto de a Comissão

[15] Processo C362/14, Maximillian Schrems contra Data Protection Commissioner, de 6 de outubro de 2015 (n.os 73 e 74).
[16] GT254, p.2.

Europeia reconhecer que a legislação japonesa em matéria de proteção de dados não é, por si só, equivalente ao RGPD.

44. **À luz das questões acima referidas, o CEPD convida a Comissão Europeia a assegurar que esta nova arquitetura de adequação, a primeira a ser adotada ao abrigo do RGPD, com base nas normas complementares, será um sistema sustentável e fiável que não levantará problemas práticos relacionados com o cumprimento concreto e eficiente por parte das entidades japonesas e a execução por parte da CPP.**

2.3.2 Segurança das traduções

45. Tal como a Comissão Europeia, o CEPD trabalhou com base nas traduções em inglês fornecidas pelas autoridades japonesas[17]. O CEPD insta a Comissão Europeia a esclarecer que baseou o seu projeto de decisão de adequação nas traduções em inglês recebidas e a verificar regularmente a qualidade e a segurança dessas traduções.

2.3.3 Adequação setorial

46. A constatação de adequação deste projeto de decisão de adequação limita-se à proteção das informações pessoais por parte dos PIHBO, nos termos da LPDP. Tal significa que a adequação é setorial, uma vez que apenas se aplica ao setor privado, excluindo do seu âmbito as transferências de dados pessoais entre autoridades e órgãos públicos. Atualmente, a Comissão Europeia faz uma breve referência a esta especificidade do âmbito da adequação no considerando 10 do projeto de decisão de adequação.

47. **O CEPD convida a Comissão Europeia a mencionar explicitamente a natureza setorial desta constatação de adequação no título da decisão de execução, bem como no seu artigo 1.º em conformidade com o artigo 45.º, n.º 3, do RGPD.**

2.3.4 Natureza vinculativa das normas complementares e das orientações da CPP

48. Nos termos do artigo 6.º da LPDP, «o Governo... deve tomar as medidas legislativas e outras medidas necessárias para poder tomar as medidas necessárias para assegurar a proteção dos dados pessoais que, em particular, exigem que seja assegurada a aplicação rigorosa do seu tratamento adequado para obter uma proteção reforçada dos direitos e interesses de um indivíduo, e tomar as medidas necessárias em colaboração com os governos de outros países para criar um sistema de dados pessoais adaptável a nível internacional através do fomento da cooperação com uma organização internacional e outro quadro internacional». Embora o governo esteja claramente identificado no presente artigo da LPDP como competente para a adoção de tal ação legal, não se refere diretamente à CPP como órgão competente para adotar regras específicas.[18] Devido a limitações de tempo, o CEPD não conseguiu reunir, analisar e examinar os elementos de prova que possam ser apresentados sobre esta questão.

49. **Tendo em conta a importância desta questão, o CEPD toma nota dos repetidos compromissos e garantias da Comissão Europeia e das autoridades japonesas no que respeita à natureza vinculativa e executória das normas complementares. O CEPD convida a Comissão Europeia a monitorizar**

[17] A Comissão Europeia verificou essas traduções.

[18] De acordo com um artigo publicado em julho de 2018, quando as normas complementares se encontravam em fase de projeto, o caráter vinculativo das presentes normas era suscetível de ser objeto de debate interno no país. Ver Fujiwara S., Comparison between the EU and Japan's Data Protection Legal Frameworks', Jurist, vol. 1521 (julho 2018): p. 19.

continuamente o seu caráter vinculativo e a sua aplicação eficaz no Japão, uma vez que o seu valor jurídico é um elemento essencial da adequação UE – Japão.

50. Além disso, a Comissão Europeia faz referência em várias secções do seu projeto de decisão de adequação às orientações da CPP (Orientações).

51. Embora a Comissão Europeia clarifique que as orientações fornecem uma interpretação vinculativa da LPDP no considerando 16 do seu projeto de decisão de adequação, no mesmo considerando faz referência ao caráter vinculativo das presentes orientações: «Segundo as informações recebidas da CPP, consideram-se as orientações normas vinculativas que formam parte integrante do quadro jurídico, que devem ser lidas em conjunto com o texto da LPDP, da resolução ministerial, das normas da CPP e de um conjunto de PeR elaborado pela CPP.»[19]

52. No entanto, a perceção do CEPD, com base nas mesmas informações prestadas pela CPP, é que as orientações não são juridicamente vinculativas. Em vez disso, fornecem uma «interpretação vinculativa» da lei. A CPP alega que as orientações são seguidas, na prática, pelos PIHBDO, utilizadas pela CPP para a aplicação da lei contra os PIHBO e utilizadas pelos tribunais para a sua apreciação. No entanto, estes elementos não constituem prova suficiente de que as orientações são normas juridicamente vinculativas.

53. **O CEPD gostaria de receber esclarecimentos na decisão de adequação em relação ao caráter vinculativo das orientações relativas à CPP e solicita à Comissão Europeia que acompanhe atentamente este aspeto.**

54. De acordo com a CPP, as orientações são, todavia, seguidas na prática uma vez que são um costume local. A CPP refere que os tribunais japoneses utilizam as orientações da CPP para proferir os seus acórdãos aquando da aplicação das normas da LPDP. A Comissão Europeia faz referência a uma decisão judicial[20], que data de 2006, para apresentar provas de que os tribunais japoneses se baseiam em orientações para as suas constatações. Apesar de o CEPD não ter recebido esta decisão judicial, o CEPD agradece que a Comissão Europeia forneça, se disponível, uma decisão judicial mais recente, quer no domínio da proteção de dados, quer noutro setor em que os tribunais japoneses tenham utilizado as orientações da CPP ou outras orientações semelhantes como base para a sua decisão.

2.3.5 Revisão periódica da constatação de adequação

55. O artigo 45.º, n.º 3, do RGPD prevê uma revisão periódica, pelo menos, de quatro em quatro anos. De acordo com referencial de adequação do CEPD[21], trata-se de um prazo geral, que deve ser ajustado a cada país terceiro ou organização internacional com uma decisão de adequação. Em função das circunstâncias específicas em causa, pode justificar-se um ciclo de revisão mais curto. Adicionalmente, os incidentes ou outras informações ou alterações do quadro jurídico do país terceiro ou da organização internacional em questão podem desencadear a necessidade de uma revisão antes do prazo previsto. Afigura-se igualmente adequado proceder em breve a uma primeira revisão de uma

[19] Decisão de Execução da Comissão de XXXX, nos termos do Regulamento (CE) n.º 2016/679 do Parlamento Europeu e do Conselho sobre o nível de proteção adequado concedido pelo Japão aos dados pessoais, enviadas ao CEPD em 13 de novembro de 2018, Considerando 16.

[20] Decisão de Execução da Comissão de XXXX, nos termos do Regulamento (CE) n.º 2016/679 do Parlamento Europeu e do Conselho sobre o nível de proteção adequado concedido pelo Japão aos dados pessoais, enviadas ao CEPD em 13 de novembro de 2018, página 5, nota de rodapé 16, «Tribunal distrital de Osaka, decisão de 19 de maio de 2006, Hanrei Jiho, Vol. 1948, p. 122.

[21] GT254, p.3.

decisão de adequação inteiramente nova e ajustar gradualmente o ciclo de revisão em função do resultado.

56. Tendo em conta uma série de fatores, incluindo o facto de a LPDP ter entrado em vigor em 2017, de a CPP ter sido criada em 2016 e de não haver informações nem elementos de prova da aplicação prática das normas complementares, **o CEPD convida a Comissão Europeia a proceder a uma revisão dessa constatação da adequação (pelo menos) de dois em dois anos e não de quatro em quatro anos, tal como sugerido no atual projeto de decisão de adequação.**

2.3.6 Compromissos internacionais assumidos pelo Japão

57. Em conformidade com o artigo 45.º, n.º 2, alínea c), do RGPD e com o referencial de adequação[22], aquando da avaliação da adequação do nível de proteção de um país terceiro, a Comissão Europeia deve considerar, entre outros, os compromissos internacionais assumidos pelo país terceiro, ou outras obrigações decorrentes da participação do país terceiro em sistemas multilaterais ou regionais, em especial no que se refere à proteção dos dados pessoais, bem como o cumprimento de tais obrigações. Adicionalmente, há que ter em conta a adesão do país terceiro em causa à Convenção do Conselho da Europa para a proteção das pessoas relativamente ao tratamento automatizado de dados de caráter pessoal, de 28 de janeiro de 1981 («Convenção 108+[23]»), e respetivo Protocolo Adicional.

58. **A este respeito, o CEPD observa que o Japão é um observador do Comité Consultivo da Convenção 108+.**

2.3.7 Poderes das autoridades de proteção de dados (APD)[24] para intentar ações relativas à validade de uma decisão de adequação perante um tribunal

59. O CEPD sublinha que, embora o considerando 179 do projeto de decisão de adequação apenas mencione casos em que uma APD recebeu uma denúncia que põe em causa a compatibilidade de uma decisão de adequação com os direitos fundamentais dos indivíduos à privacidade e à proteção de dados, esta declaração deve ser entendida como um exemplo de situações em que uma APD pode recorrer a um tribunal nacional, o que também pode ser possível na ausência de uma denúncia, e não como uma restrição dos poderes conferidos às APD ao abrigo do RGPD e das legislações nacionais dos Estados-Membros nesta matéria. Com efeito, as disposições do RGPD incluem tanto o poder de suspender as transferências de dados, mesmo quando baseadas numa decisão de adequação, como de intentar uma ação relativa à validade de uma decisão de adequação, não se limitam aos casos em que tenham recebido uma denúncia, caso a sua legislação nacional lhes confira o poder de o fazer de forma mais ampla e independente de uma denúncia, em conformidade com as disposições pertinentes do RGPD.

60. **O CEPD convida a Comissão Europeia a esclarecer, no seu projeto de decisão de adequação, que o poder de as autoridades de controlo intentarem uma ação contra a validade de uma decisão de adequação na sequência de uma denúncia é apenas um exemplo dos poderes mais amplos das autoridades de proteção de dados decorrentes do RGPD, que incluem o poder de suspender transferências e intentar uma ação relativa à validade de uma decisão de adequação na ausência de uma denúncia caso a sua legislação nacional o preveja.**

[22] GT254, p.2.

[23] Convenção para a proteção das pessoas relativamente ao tratamento automatizado de dados de caráter pessoal, Convenção 108+, de 18 de maio de 2018.

[24] Processo C362/14, Maximillian Schrems contra Data Protection Commissioner, de 6 de outubro de 2015.

3 ASPETOS COMERCIAIS

3.1 Princípios fundamentais

61. O capítulo 3 do referencial de adequação dedica-se aos «princípios de conteúdo». O sistema de um país terceiro ou de uma organização internacional deve incluí-los de forma a ter em conta o nível de proteção assegurado como essencialmente equivalente ao garantido pela legislação da UE. O CEPD reconhece que o sistema jurídico japonês segue uma abordagem diferente da do RGPD de forma a dar cumprimento ao direito à privacidade. Embora o direito à privacidade não esteja consagrado, por si só, na Constituição japonesa, foi reconhecido como um direito constitucional através da jurisprudência, como também mencionado na decisão da Comissão Europeia[25].

62. Devido, em especial, ao facto de a abordagem japonesa ser claramente diferente da abordagem europeia, há que observar cuidadosamente se, em última análise, o sistema no seu conjunto, não apenas os aspetos individuais, proporciona um nível de proteção «essencialmente equivalente». Isto significa que as potenciais «lacunas» relativas a um princípio de conteúdo podem ser compensadas por outros aspetos que proporcionem controlos e equilíbrios adequados.

3.1.1 Conceitos

63. Com base no referencial de adequação, devem existir conceitos e/ou princípios básicos de proteção dos dados no quadro jurídico do país terceiro. Embora não tenham de refletir a terminologia do RGPD, devem refletir e ser coerentes com os conceitos consagrados na legislação europeia em matéria de proteção de dados. Por exemplo, o RGPD inclui os seguintes conceitos importantes: «dados pessoais», «tratamento de dados pessoais», «responsável pelo tratamento», «subcontratante», «destinatário» e «dados sensíveis»[26].

64. A LPDP inclui igualmente uma série de definições, tais como, entre outras, as de «informações pessoais», «dados pessoais», «operador de empresas de tratamento de dados pessoais». **No entanto, parece que a LPDP não inclui uma definição do termo «tratamento de dados pessoais» que seja semelhante à expressão «processamento de dados pessoais».**

65. No que diz respeito à definição da expressão «tratamento de dados pessoais», a CPP respondeu por escrito à pergunta do CEPD sobre esta definição. A Comissão Europeia citou a resposta ao projeto de decisão da Comissão *«Embora a LPDP não utilize o termo «processamento», baseia-se no conceito equivalente de «tratamento» que, de acordo com as informações recebidas pela CPP, abrange «qualquer ato relativo a dados pessoais» que inclua a aquisição, a introdução, a acumulação, a organização, o armazenamento, a edição/tratamento, a renovação, a produção, a segurança, a utilização ou o fornecimento de informações pessoais.»*[27]

66. No entanto, uma vez que o texto de referência para esta definição não foi apresentado, o CEPD convida **a Comissão Europeia a acompanhar de perto de forma a garantir que a definição do conceito acima mencionada é efetivamente seguida na prática, tal como fornecida pela CPP.**

---

[25] O CEPD não recebeu a tradução para inglês desta decisão do Tribunal. Ver Decisão de Execução da Comissão de XXXX, nos termos do Regulamento (CE) n.º 2016/679 do Parlamento Europeu e do Conselho sobre o nível de proteção adequado concedido pelo Japão aos dados pessoais, enviadas ao CEPD em 13 de novembro de 2018, nota de rodapé 9

[26] GT254, p.4.

[27] Decisão de Execução da Comissão de XXXX, nos termos do Regulamento (CE) n.º 2016/679 do Parlamento Europeu e do Conselho sobre o nível de proteção adequado concedido pelo Japão aos dados pessoais, enviadas ao CEPD em 13 de novembro de 2018, Considerando 17.

3.1.1.1 Conceito de subcontratante e obrigações de um «administrador»

67. Como acima mencionado, o referencial de adequação exige a existência dos conceitos e/ou princípios básicos de proteção dos dados no quadro jurídico do país terceiro.

68. A LPDP inclui uma definição de «operador de empresas de tratamento de dados pessoais» que, de acordo com a Comissão Europeia, inclui os termos de um responsável pelo tratamento de dados e de um subcontratante, tal como previsto pelo RGPD, e não faz uma distinção entre ambos[28]. No entanto, a LPDP inclui também um termo «administrador» no seu artigo 22.º que, em alguns casos, se assemelha ao termo «subcontratante» no âmbito do RGPD.

69. Tal como explicado pela CPP nas suas respostas fornecidas ao CEPD, e também incluído no projeto de decisão de adequação da Comissão Europeia, um administrador é considerado o equivalente a um subcontratante ao abrigo do RGPD – responsável pelo tratamento de dados pessoais por um PIHBO. Este administrador tem as mesmas obrigações e direitos que qualquer PIHBO, incluindo as normas complementares aplicáveis aos dados pessoais transferidos da UE. O PIHBO, que confia o tratamento de dados pessoais a um administrador, é obrigado a «exercer a supervisão necessária e adequada»[29] do administrador.

70. **O CEPD convida a Comissão Europeia a explicar o estatuto e as obrigações do administrador quando o administrador alterar as finalidades e os meios de tratamento e esclarecer se o consentimento do titular dos dados continua a ser uma condição necessária para essa mudança de finalidade ou de determinação dos meios[30].**

3.1.1.2 Conceito de dados pessoais conservados

71. A LPDP contém o conceito de «dados pessoais conservados», que é considerado uma subcategoria de dados pessoais. Segundo a LPDP, as disposições relativas aos direitos do titular dos dados aplicam-se[31]apenas aos dados pessoais conservados. A definição de dados pessoais conservados é incluída no artigo 2.º, n.º 7, da LPDP.

72. Os dados pessoais conservados são os dados pessoais que não os que i) devem ser apagados num prazo máximo de 6 meses[32] ou que ii) são abrangidos pelas exceções previstas no artigo 4.º da resolução ministerial que são suscetíveis de prejudicar os interesses públicos ou outros, caso a sua presença ou ausência seja dada a conhecer.

73. A norma complementar 2) prevê que «*os dados pessoais recebidos da UE com base numa decisão de adequação devem ser tratados como dados pessoais conservados, independentemente do período em que devam ser suprimidos.*»

74. No entanto, os dados pessoais abrangidos pelas exceções previstas no artigo 4.º da resolução ministerial não serão tratados como dados pessoais conservados e os direitos dos titulares dos dados não serão aplicáveis.

75. O artigo 23.º do RGPD prevê que, tal como o artigo 4.º da ordem ministerial, o direito da União ou o direito do Estado-Membro a que o responsável pelo tratamento/subcontratante está sujeito, podem

[28] Decisão de Execução da Comissão de XXXX, nos termos do Regulamento (CE) n.º 2016/679 do Parlamento Europeu e do Conselho sobre o nível de proteção adequado concedido pelo Japão aos dados pessoais, enviadas ao CEPD em 13 de novembro de 2018, Considerando 35.
[29] Artigo 22.º da Lei da Proteção de Dados Pessoais (LPDP) alterada, em vigor desde 30 de maio de 2017.
[30] Artigo 23.º, n.º 5, alínea i), LPDP. Ver também a secção relativa ao princípio de transparência infra.
[31] Artigo 27.º a 30.º. da LPDP.
[32] Alteração à resolução ministerial para aplicação do artigo 5.º da Lei da Proteção de Dados Pessoais (LPDP) alterada, em vigor desde 30 de maio de 2017.

restringir o âmbito das obrigações que lhe são aplicáveis e os direitos à disposição do titular dos dados. Tal pode ser feito através de uma medida legislativa. Estas restrições devem respeitar a essência do direito e das liberdades fundamentais e constituem uma medida necessária e proporcionada numa sociedade democrática.

76. No que diz respeito à substância das exceções previstas no artigo 4.º da resolução ministerial, o CEPD não recebeu documentação suficiente sobre estas limitações ou elementos adicionais para clarificar o âmbito de aplicação destas disposições[33]. O CEPD não está em condições de avaliar se estas limitações aos direitos dos titulares dos dados se limitam ao que seria considerado estritamente necessário e proporcional ao abrigo da legislação da UE e, por conseguinte, seriam essencialmente equivalentes aos direitos fornecidos aos titulares dos dados da UE.

77. **Devido à falta de alguns documentos relevantes, o CEPD gostaria igualmente de receber garantias dadas pela Comissão Europeia, se as restrições aos direitos dos indivíduos (em especial, os direitos de acesso, retificação e objeção) forem necessárias e proporcionadas numa sociedade democrática e respeitam a essência dos direitos fundamentais.**

78. Um requisito essencial no âmbito do RGPD é que os dados pessoais sejam protegidos ao longo de todo o seu «ciclo de vida».

79. Tendo em conta o facto de as normas complementares apenas se aplicarem aos dados pessoais transferidos da UE, o CEPD gostaria de receber mais informações sobre a aplicação na prática destas regras por parte dos PIHBDO, em especial quando esses dados são ainda comunicados a outro PIHBO após a sua primeira transmissão ao Japão.

80. No considerando 15 do seu projeto de decisão de adequação, a Comissão Europeia esclareceu que os PIHBO que recebem e/ou tratam posteriormente dados pessoais da UE terão a obrigação legal de cumprir as normas complementares e que, para tal, terão de garantir que podem identificar tais dados pessoais ao longo de todo o seu «ciclo de vida».

81. Nas suas respostas, a CPP[34]explicou que essa identificação será feita através de métodos técnicos (marcação) ou métodos organizacionais (armazenamento de dados provenientes da UE numa base de dados específica).

82. Na nota de rodapé 14 do seu projeto de decisão de adequação, a Comissão Europeia explica que os PIHBO devem registar as informações sobre a origem dos dados da UE durante o tempo necessário para poderem cumprir as normas complementares. Tal encontra-se igualmente consagrado no artigo 26.º, n.^{os} 1, 3 e 4, da LPDP, que estabelece que um PIHBO tem a obrigação de confirmar e registar a fonte desses dados e todas as circunstâncias que envolveram a aquisição desses dados.

83. No entanto, o CEPD observa que o artigo 18.º das normas da CPP[35] especifica que as obrigações de conservação de registos dos PIHBO estão limitadas a um máximo de três anos para os casos que não são abrangidos pelos métodos específicos de conservação de registos descritos no artigo 16.º das regras da CPP (utilizando um documento escrito, um registo eletromagnético ou um microfilme). Tal é igualmente afirmado pela Comissão Europeia no considerando 71 do seu projeto de decisão de

[33] O CEPD não recebeu as decisões do Supremo Tribunal mencionadas no considerando 53 do projeto de decisão de adequação.

[34] Anexo III do presente parecer.

[35] Normas de execução para a Lei da Proteção de Dados Pessoais (Regras da CPP), em vigor desde 30 de maio de 2017, artigo 16.º.

adequação: «*Tal como especificado no artigo 18.º das regras da CPP, esses registos devem ser conservados por um período de um a três anos, consoante as circunstâncias.*»

84. Mesmo que, como afirma a Comissão Europeia na nota de rodapé 14 do seu projeto de decisão de adequação, os PIHBO não estejam proibidos de manter registos relativos à origem dos dados por um período superior a três anos para poderem cumprir as suas obrigações nos termos da norma complementar 2), tal não está claramente refletido na legislação japonesa nem nas normas complementares. O CEPD considera que existe o risco de os PIHBO respeitarem, de facto, o artigo 18.º das regras da CPP, mesmo quando tratam dados provenientes da UE. Tal deve-se principalmente ao facto de, atualmente, à luz do CEPD e com base nos documentos disponíveis, não existir qualquer disposição que obrigue os PIHBO a cumprir as normas complementares. Tal resultaria na transferência de dados da UE para deixarem de estar protegidos pelas proteções adicionais incluídas nas normas complementares.

85. **O CEPD convida a Comissão Europeia a acompanhar de perto a proteção eficaz dos dados pessoais transferidos da UE para o Japão, com base no projeto de decisão de adequação, ao longo de todo o seu «ciclo de vida», apesar de a legislação japonesa impor uma obrigação de conservação de registos da origem dos dados por um período máximo de três anos.**

3.1.2 Fundamentações para o tratamento lícito e equitativo para fins legítimos

86. De acordo com o referencial de adequação, em conformidade com o RGPD, os dados devem ser tratados de forma lícita, leal e legítima[36]. A base jurídica, segundo a qual os dados pessoais podem ser tratados de forma lícita, equitativa e legítima, deve ser estabelecida de forma suficientemente clara. O quadro europeu reconhece várias fundamentações legítimas como, por exemplo, as disposições do direito nacional, o consentimento do titular dos dados, a execução de um contrato ou o interesse legítimo do responsável pelo tratamento ou de um terceiro que não prevalece sobre os interesses do indivíduo.

87. No âmbito da LPDP, o consentimento desempenha um papel central no sistema jurídico japonês de proteção de dados. O consentimento é a base jurídica central para o tratamento de dados pessoais no Japão e também uma das principais bases jurídicas para as transferências de dados pessoais do Japão para um país terceiro. Adicionalmente, é necessário consentimento para uma alteração da finalidade do tratamento.

88. De acordo com a norma complementar 3), a base jurídica para o tratamento de dados pessoais transferidos da UE para o Japão será a base jurídica para a qual os dados são transferidos para o Japão. Se o PIHBO pretender continuar a tratar tais dados com uma finalidade diferente, deve obter o consentimento prévio do titular dos dados.

89. O CEPD considera que a qualidade do consentimento, especialmente devido ao seu papel central no quadro jurídico japonês, deve cumprir os requisitos fundamentais da noção de consentimento, ou seja, de acordo com o direito da UE, uma «*indicação livre, específica, informada e inequívoca do desejo do titular dos dados...*». O titular dos dados pode retirar esse consentimento como uma garantia essencial para garantir o livre arbítrio do titular dos dados durante o período em causa[37]. O direito de retirada, enquanto elemento obrigatório do consentimento, parece estar em falta no quadro jurídico japonês.

[36] GT254, p.4.

[37] RGPD, artigo 4.º, n.º 11. Para mais informações, ver também as orientações relevantes do CEPD sobre o consentimento do GT259, de 10 de abril de 2018.

Com efeito, de acordo com as orientações da CPP[38], a retirada é apenas «desejável» e depende das «características, dimensão e situação da atividade».

3.1.3 O princípio da transparência

90. Com base no artigo 5.º do RGPD, a transparência é um princípio fundamental do sistema de proteção de dados da UE.[39] O referencial de adequação menciona explicitamente a «transparência» como um dos princípios a considerar na avaliação do nível de proteção essencialmente equivalente previsto por um país terceiro. O princípio da transparência e da equidade esforça-se por assegurar que o titular dos dados tenha controlo sobre os seus dados e, para o efeito, por regra, deve ser fornecida informação de forma proativa. No caso do Escudo de Proteção da Privacidade, no seu parecer 1/2016, o Grupo do artigo 29.º para a Proteção de Dados[40] fez referência ao anexo II, secção II, n.º 1, alínea b), do acordo relativo ao Escudo de Proteção da Privacidade (comunicação ao indivíduo) e declarou que, se os dados não forem recolhidos diretamente, a organização deve notificar o titular dos dados «quando os dados são registados pela organização aderente» (secção 2.2.1.a). A política de privacidade disponível ao público constitui um critério adicional (ver secção 2.2.1.b). Assim, já nos termos da Diretiva 95/46/CE considerou-se necessário informar diretamente o titular dos dados.

91. Uma primeira preocupação diz respeito à modalidade de informação fornecida ao titular dos dados no âmbito da LPDP. Nos termos do artigo 27.º, n.º 1, da LPDP, um PIHBO é obrigado a fornecer as informações descritas no artigo 27.º, n.º 1, da LPDP, colocando-o «num Estado onde um mandante possa ter conhecimento». No entanto, esta redação não esclarece em que medida o PIHBO tem de tomar medidas positivas para informar efetivamente o titular dos dados.

92. **O CEPD convida a Comissão a esclarecer o significado do termo «pode ter conhecimento» e se a LPDP prevê, em regra, a obrigação de informar genuinamente os titulares dos dados.**

93. Além disso, de acordo com o referencial de adequação, podem existir restrições relativamente às informações a fornecer ao titular dos dados, à semelhança do disposto no artigo 23.º do RGPD. Na mesma linha, o artigo 14.º, n.º 5, do RGPD prevê uma exceção ao direito de ser informado quando a informação é suscetível de tornar impossível ou prejudicar gravemente a realização do tratamento. No entanto, mesmo neste caso, o responsável pelo tratamento deve fornecer algum tipo de informação, por exemplo, tornando públicas as informações «generalizadas». Além disso, quando o risco deixa de existir, o titular dos dados deve ser notificado[41]. Estes aspetos são importantes para garantir o princípio fundamental da equidade.

94. Nos termos do artigo 23.º da LPDP, o PIHBO tem geralmente de prestar antecipadamente informações ao titular dos dados sobre o fornecimento dos seus dados a terceiros, quer implicitamente, quando obtém o seu consentimento, quer expressamente através de uma notificação de autoexclusão. O CEPD

[38] Data Protection Legal and Technical Research and Analysis Consortium (DPC), An assessment of the level of protection of personal data provided under Japanese law, p. 46: «Além disso, do ponto de vista da proteção dos direitos e interesses de um mandante como os consumidores, é desejável que, caso se receba um pedido de dados pessoais conservados por parte de um mandante, se cumpra o pedido do mandante através da suspensão, etc., do envio de mensagens diretas ou do preenchimento voluntário de uma interrupção da utilização, etc., tendo em conta as características, a dimensão e a situação da atividade».

[39] GT254, capítulo 3, ponto 7, p. 5; ver também o considerando 39) do RGPD.

[40] Este Grupo de Trabalho foi instituído ao abrigo do artigo 29.º da Diretiva 95/46/CE. Trata-se de um órgão consultivo europeu independente em matéria de proteção de dados e de privacidade. As suas funções estão descritas no artigo 30.º da Diretiva 95/46/CE e no artigo 15.º da Diretiva 2002/58/CE. O GT29 passa a ser o CEPD.

[41] Tele2, Processos apensos C 203/15 e C 698/15, Acórdão do Tribunal, 21 de dezembro de 2016, cons. 121 e Digital Rights Ireland, Processos apensos C-293/12 e C-594/12, Acórdão do Tribunal de Justiça, de 8 de abril de 2014, cons. 54-62.

compreende que não existe qualquer notificação ao titular dos dados a informá-lo de que os seus dados não são conservados no âmbito da LPDP, uma vez que estão abrangidos pelas exceções previstas no artigo 4.º da resolução ministerial. Consequentemente, não poderão beneficiar plenamente dos seus direitos. Os titulares dos dados também não são informados nos casos do artigo 18.º, n.º 4, da LPDP.

95. **O CEPD reconhece que os direitos podem ser restringidos para objetivos legítimos prosseguidos pelo PIHBO e pelas autoridades estatais Ao mesmo tempo, o CEPD considera que deve haver, pelo menos, uma informação de caráter geral sobre a possibilidade de limitação dos direitos para os objetivos a que se refere a lei e que o titular dos dados deve ser notificado quando deixam de existir os riscos para os quais a informação é restringida.**

96. Por último, desenvolvem-se mais adiante outros aspetos da transparência. Estes referem-se aos riscos inerentes à transferência para um país terceiro[42] e à informação sobre a lógica do tratamento no contexto do processo automatizado de tomada de decisões, incluindo a definição de perfis.[43]

3.1.4 Restrições relativas a transferências subsequentes

97. O CEPD congratula-se com os esforços envidados pelas autoridades japonesas e pela Comissão Europeia para melhorar o nível de proteção das transferências subsequentes na norma complementar 4), o que exclui que os dados pessoais transferidos da UE sejam posteriormente transferidos para um país terceiro com base nas normas transnacionais de proteção da privacidade da APEC. Além disso, o CEPD reconhece que, nos considerandos 177 e 184 do seu novo projeto de decisão de adequação, a Comissão Europeia se comprometeu a suspender a decisão de adequação quando as transferências subsequentes já não asseguram a continuidade da proteção. No entanto, o CEPD gostaria de apresentar dois pontos no que diz respeito a estas transferências de dados pessoais da UE provenientes do Japão para países terceiros.

98. **A utilização do consentimento como base para as transferências de dados do Japão para um país terceiro no sistema jurídico japonês suscita preocupações, uma vez que o CEPD considera que as informações fornecidas ao titular dos dados antes do seu consentimento não parecem ser exaustivas.**

99. O artigo 24.º da LPDP proíbe a transferência de dados pessoais para terceiros fora do território do Japão sem o consentimento prévio do titular dos dados. A norma complementar 4), estipula que os titulares dos dados da UE devem receber informações sobre as circunstâncias relacionadas com a transferência necessária para tomar uma decisão sobre o seu consentimento.

100. A Comissão Europeia conclui, no seu projeto de decisão de adequação, que a norma suplementar n.º 4, garante um consentimento específico bem informado do titular dos dados da UE[44], uma vez que será informado do facto de os dados serem transferidos para o estrangeiro e do país de destino específico. Tal permitiria ao titular dos dados avaliar o risco para a privacidade associado à transferência.

101. De acordo com o princípio da transparência do referencial de adequação, deve assegurar-se um certo grau de equidade quando se informa os indivíduos. No contexto de transferências ulteriores com base no consentimento, o CEPD considera que, para garantir esse grau adequado de equidade, os titulares

[42] Ver a secção 2.1.4.
[43] Ver a secção 2.1.6.
[44] Decisão de Execução da Comissão de XXXX, nos termos do Regulamento (CE) n.º 2016/679 do Parlamento Europeu e do Conselho sobre o nível de proteção adequado concedido pelo Japão aos dados pessoais, enviadas ao CEPD em 13 de novembro, Considerando 76.

dos dados devem ser explicitamente informados dos eventuais riscos de tais transferências decorrentes da ausência de proteção adequada no país terceiro e da ausência de garantias adequadas antes do consentimento. Esse aviso deve incluir, por exemplo, a informação de que, no país terceiro, podem não existir autoridades de controlo e/ou os princípios de tratamento de dados e/ou os direitos dos titulares dos dados podem não estar previstos no país terceiro[45]. Para o CEPD, o fornecimento desta informação é essencial para que o titular dos dados dê o seu consentimento com pleno conhecimento destes factos específicos da transferência[46].

102. O consentimento informado é igualmente importante no que respeita às exclusões setoriais. A decisão de adequação não abrange determinados tipos de tratamento por parte de determinados órgãos, como as universidades, para o tratamento de dados pessoais para fins académicos. A preocupação do CEPD diz respeito ao cenário específico em que os dados transferidos da UE ao abrigo da decisão de adequação – por exemplo, os dados de RH dos estudantes Erasmus no Japão – são depois utilizados para uma finalidade diferente, que não se insere no âmbito da decisão de adequação (por exemplo, fins de investigação), com o consentimento do titular dos dados, e, por conseguinte, já não são abrangidos pela proteção adicional prevista nas normas complementares.

103. No considerando 38 do seu projeto de decisão de adequação, a Comissão Europeia afirma que esse cenário será abrangido pelo contexto das transferências ulteriores e que, caso tal aconteça, o PIHBO tem de fornecer ao titular dos dados todas as informações necessárias antes de obter o seu consentimento, incluindo que as informações pessoais não seriam abrangidas pela proteção das regras da LPDP.

104. A norma complementar 4), requer que o PIHBO obtenha o consentimento do titular dos dados após receber informações sobre as circunstâncias relacionadas com a transferência necessária para que o mandante tome uma decisão sobre o seu consentimento.

105. **O CEPD convida a Comissão Europeia a assegurar que as informações a fornecer ao titular dos dados «sobre as circunstâncias relacionadas com a transferência» devem incluir as informações sobre os eventuais riscos de transferências decorrentes da ausência de proteção adequada no país terceiro e a ausência de garantias adequadas, ou, no caso de exclusões setoriais, da ausência de proteções das normas complementares e da LPDP.**

106. **As transferências ulteriores de dados pessoais podem ocorrer em países terceiros que sejam objeto de uma eventual decisão de adequação japonesa posterior.**

107. Sem prejuízo das derrogações previstas no artigo 23.º, n.º 1, da LPDP, os dados inicialmente transferidos da UE para o Japão podem ser transferidos do Japão para um país terceiro sem consentimento em dois casos:

- Se o PIHBO e o terceiro destinatário tiverem implementado em conjunto medidas que proporcionem um nível de proteção equivalente ao da LPDP, juntamente com as normas complementares por meio de um contrato, outras formas de acordos vinculativos ou de acordos vinculativos no âmbito de um grupo empresarial[47].

[45] Orientações do CEPD 2/2018 relativas às derrogações do artigo 49.º do Regulamento (CE) n.º 2016/679, de 25 de maio de 2018, p. 8.
[46] Orientações do CEPD 2/2018 relativas às derrogações do artigo 49.º do Regulamento (CE) n.º 2016/679, de 25 de maio de 2018, p. 7.
[47] Norma complementar 4), alínea ii).

- Se a CPP tiver reconhecido o país terceiro nos termos do artigo 24.º da LPDP e do artigo 11.º das Regras da CPP[48] como proporcionando um nível de proteção equivalente ao garantido no Japão.

108. O Comité Europeu para a Proteção de Dados avalia a LPDP, artigo 24.º, como a regra mais específica, que contém uma derrogação à regra geral prevista na LPDP, artigo 23.º. Por conseguinte, o CEPD não partilha a avaliação da Comissão Europeia na última frase do considerando 78 do projeto de decisão de adequação, declarando que, mesmo nesses casos, a transferência para o terceiro continua sujeita à exigência de um consentimento nos termos do artigo 23.º, n.º 1, da LPDP.

109. Nos termos do artigo 11.º, n.º 1, das regras da CPP, uma decisão de adequação por parte da CPP exige normas substantivas equivalentes à LPDP cuja aplicação está assegurada no país terceiro e que são supervisionadas de forma eficaz por uma autoridade de execução independente. Além disso, a CPP pode impor condições necessárias para proteger os direitos e interesses de pessoas singulares no Japão, de acordo com o artigo 11.º, n.º 2, das regras da CPP.

110. A norma complementar 4) estabelece que os dados pessoais da UE podem ser transferidos para um país terceiro sujeito a uma decisão de adequação japonesa sem mais restrições. Mas o artigo 44.º do RGPD regulamenta que qualquer transferência de dados pessoais para um país terceiro tem de cumprir as condições estabelecidas no capítulo V do RGPD, incluindo transferências ulteriores do país terceiro para outro país terceiro. O nível de proteção das pessoas singulares cujos dados sejam transferidos não deve ser posto em causa pela transferência ulterior[49]. Embora esta interpretação seja, em princípio, também partilhada pela Comissão Europeia no seu projeto de decisão de adequação[50], não parece ser seguida integralmente. A Comissão Europeia negociou a proibição da transferência de dados provenientes da UE para um país terceiro com base nas normas transnacionais de proteção da privacidade da APEC. À luz do instrumento comparativo desenvolvido em 2014 no âmbito da diretiva da UE entre o BCR e o CBPR, que mostra os requisitos de ambos os sistemas, as suas convergências e diferenças (Parecer 02/2014 do GT29), o CEPD tem dúvidas quanto à utilização das normas transnacionais de proteção da privacidade como instrumento de transferência ulterior de dados pessoais transferidos da UE para países fora do Japão.

111. Em contrapartida, as transferências ulteriores de dados pessoais transferidos da UE para o Japão com base numa decisão de adequação do Japão parecem ser aceites pela Comissão Europeia, sem a possibilidade de a CPP impor as normas complementares como condições para proteger os direitos e interesses dos cidadãos da UE, se necessário. O CEPD deduz do artigo 44.º do Regulamento Geral sobre a Proteção de Dados que o reforço da proteção dos dados transferidos da UE para o Japão previsto nas normas complementares tem sempre de ser prorrogado quando os dados pessoais transferidos da UE para o Japão são posteriormente transferidos para um país terceiro, se o quadro de proteção de dados nesse país não for reconhecido como essencialmente equivalente ao RGPD.

112. **Por conseguinte, o CEPD convida a Comissão Europeia a assumir o seu papel de controlo e a assegurar que se mantém o nível de proteção dos dados da UE ou a considerar a suspensão desta decisão de adequação se os dados pessoais transferidos da UE para o Japão forem posteriormente transferidos para países terceiros sujeitos a uma eventual decisão de adequação japonesa, quando**

[48] Normas de execução para a Lei da Proteção de Dados Pessoais, 30 de maio de 2017. A Comissão Europeia comunicou ao CEPD uma tradução em inglês do novo artigo 11.º, mas este artigo ainda não foi publicado.
[49] GT254, p.5.
[50] Decisão de Execução da Comissão de XXXX, nos termos do Regulamento (CE) n.º 2016/679 do Parlamento Europeu e do Conselho sobre o nível de proteção adequado concedido pelo Japão aos dados pessoais, enviadas ao CEPD em 13 de novembro, Considerando 75.

esses países terceiros não tiverem sido objeto de uma avaliação prévia ou de uma constatação de adequação da UE.

3.1.5 Comercialização direta

113. De acordo com a regra complementar 3), um PIHBO está proibido de tratar os dados para efeitos de comercialização direta se tiverem sido transferidos da União Europeia para outra finalidade e se o titular dos dados da UE não tiver dado o seu consentimento para a alteração da finalidade de utilização.

114. De acordo com o referencial de adequação segundo o qual os dados sejam tratados para tais fins de comercialização direta, o titular dos dados deve poder opor-se a qualquer momento sem que os seus dados sejam tratados para tais fins. Nos termos do artigo 16.º da LPDP, um PIHBO está apenas autorizado a tratar informações pessoais se o titular dos dados der o seu consentimento. A retirada do consentimento pode proporcionar o mesmo resultado que o direito privilegiado de oposição à comercialização direta.

115. O quadro japonês de proteção de dados não proporciona um direito privilegiado de oposição e, tal como explicado anteriormente na secção relativa ao consentimento, a retirada do consentimento ao abrigo das orientações da CPP é meramente desejável e condicional, não podendo, por conseguinte, ser equiparada a um direito de oposição em qualquer altura, tal como solicitado no âmbito do referencial de adequação. **O CEPD convida a Comissão Europeia a dar garantias quanto ao direito de retirar o consentimento e a controlar os casos relacionados com a comercialização direta.**

3.1.6 Decisão e definição de perfis automatizada

116. De acordo com o referencial de adequação, as decisões baseadas exclusivamente no tratamento automatizado (decisões individuais automatizadas), incluindo a definição de perfis, que produza efeitos na sua esfera jurídica ou que afete significativamente o titular dos dados, apenas podem ser tomadas em determinadas condições estabelecidas no quadro jurídico do país terceiro. Por conseguinte, sempre que é tomada uma decisão automatizada e realizada a definição de perfis nas circunstâncias acima referidas, tem de existir um fundamento jurídico para o efeito.

117. No quadro europeu, as condições para a decisão automatizada incluem, por exemplo, a necessidade de obter o consentimento explícito[51] do titular dos dados ou a necessidade de tal decisão para a celebração de um contrato. Se a decisão não cumprir as condições estabelecidas no quadro jurídico do país terceiro, o titular dos dados deve ter o direito de não lhe estar sujeito. Além disso, a legislação do país terceiro deve, em todo o caso, providenciar as garantias necessárias, nomeadamente o direito de ser informado sobre os motivos específicos subjacentes à decisão e a lógica subjacente à retificação de informações inexatas ou incompletas, bem como de contestar a decisão, caso esta tenha sido adotada numa base factual incorreta.

118. A decisão da Comissão diz apenas respeito ao setor bancário onde se aplicariam as regras setoriais[52] relativas às decisões automatizadas. As Orientações Gerais para a supervisão dos principais bancos mencionadas no considerando 93 do projeto de decisão de adequação indicam que as pessoas em causa devem receber explicações específicas sobre os motivos da rejeição de um pedido de celebração de um contrato de crédito.

[51] Para observações críticas ao conceito de consentimento no quadro jurídico japonês em matéria de proteção de dados, consultar: 2.1. Generalidades e 2.2.8. Comercialização direta.

[52] Estas regras setoriais não foram apresentadas ao CEPD.

119. As argumentações da Comissão Europeia relativas ao projeto de decisão de adequação (Considerando 94), segundo as quais a ausência de regras específicas sobre a decisão automatizada na LPDP é pouco suscetível de afetar o nível de proteção, não parece (por exemplo) ter em conta o caso em que os dados pessoais transferidos da UE são posteriormente tratados por outro responsável pelo tratamento de dados japonês (diferente do importador de dados inicial japonês original).

120. Afigura-se, por conseguinte, que não existem regras gerais aplicáveis em todos os setores do Japão que regem a decisão e definição de perfis automatizada.

121. **O CEPD convida a Comissão Europeia a acompanhar os casos relacionados com a decisão e definição de perfis automatizada.**

3.2 Mecanismos processuais e de aplicação efetiva

122. Com base nos critérios estabelecidos no referencial de adequação, o CEPD analisou os seguintes aspetos da proteção de dados e do quadro jurídico japonês abrangidos pelo projeto de decisão de adequação: a existência e o funcionamento efetivo de uma autoridade de controlo independente; a existência de um sistema que garanta um bom nível de cumprimento e um sistema de acesso aos mecanismos de recurso adequados que dotem os indivíduos da UE dos meios necessários para exercerem os seus direitos e procurarem obter reparação sem se depararem com entraves morosos ao recurso administrativo e judicial.

123. Com base nos parâmetros estabelecidos pelo TJUE no processo Schrems[53] e nos descritos no considerando 104 e no artigo 45.º do RGPD, o CEPD considera que, embora exista um sistema coerente com o sistema europeu no Japão, este sistema pode ser de difícil acesso, na prática, por parte dos cidadãos da UE, cujos dados serão transferidos ao abrigo da presente decisão de adequação à luz da existência de barreiras linguísticas e institucionais.

124. As secções que se seguem analisarão os aspetos acima mencionados do quadro japonês antes de apresentarem algumas recomendações dirigidas à Comissão.

3.2.1 Autoridade de controlo independente competente

125. A CPP foi criada em 1 de janeiro de 2016, na sequência das alterações da LPDP de 2015, substituindo a sua predecessora – a Comissão de Proteção individual das Informações Pessoais (criada em 2013 ao abrigo da Lei My Number). Apesar de uma organização jovem, desde a sua criação, a CPP envidou esforços consideráveis no sentido de construir a infraestrutura necessária para ter em conta a aplicação da LPDP alterada. Entre eles está o estabelecimento das regras da CPP, as orientações da CPP para orientar os PIHBO relativamente à interpretação da LPDP, a publicação de um documento de PeR[54] da CPP e a criação de uma linha telefónica de apoio para aconselhar os operadores comerciais e os cidadãos sobre as disposições em matéria de proteção de dados, bem como de um serviço de mediação para tratar as denúncias.

126. A criação e o funcionamento da CPP encontram-se regulados no capítulo V da LPDP. Embora a CPP seja abrangida pela jurisdição do Primeiro-Ministro, o artigo 62.º prevê que a CPP exerça a sua função de forma independente. O CEPD congratula-se com o esclarecimento feito pela Comissão Europeia no projeto alterado da decisão de adequação, divulgado em 13 de novembro de 2018, a fim de descrever de forma mais pormenorizada a medida em que a CPP está isenta de influências internas e externas.

[53] Processo 362/14 (2015), Maximillian Schrems contra Data Protection Commissioner, (n.os 73 e 74).
[54] Este documento não foi fornecido pela Comissão Europeia ao CEPD em inglês.

3.2.2 O sistema de proteção de dados deve garantir um bom nível de conformidade

127. O projeto de decisão de adequação realiza um exame exaustivo dos poderes que a CPP possui ao abrigo da LPDP, artigos 40.º, 41.º e 42.º, para assegurar o controlo e a aplicação da legislação. O artigo 40.º autoriza a CPP a solicitar ao PIHBO a apresentação de relatórios e documentação relativos às operações de tratamento, bem como a realização de inspeções no local. Nos termos do artigo 42.º, a CPP tem o poder de, quando reconhecer a necessidade de proteger os direitos individuais ou verificar uma violação das disposições da lei, emitir recomendações e, em caso de incumprimento, ordens para que os PIHBO suspendam o ato de violação ou tomem as medidas necessárias para retificar a violação.

128. Em outubro de 2018, a CPP adotou uma das suas primeiras ações ao abrigo do artigo 41.º da LPDP alterada e emitiu «orientações» para um PIHBO, aconselhando a empresa a reforçar as suas medidas de segurança e a supervisionar eficazmente os fornecedores de aplicações, dando simultaneamente esclarecimentos claros e de fácil compreensão aos utilizadores sobre a forma como os seus dados pessoais são utilizados, e obter o consentimento prévio quando as informações são partilhadas com terceiros, bem como responder adequadamente ao pedido de apagamento das suas informações por parte dos utilizadores. Nas respostas ao CEPD[55], os agentes da CPP informaram que a empresa anunciou que iria cooperar e que, quando não o fizer, apresentarão à empresa uma «recomendação» ao abrigo do artigo 42.º, n.º 1, da LPDP.

129. O inquérito realizado pela CPP sobre o PIHBO acima mencionado é um indicador muito positivo dos esforços da autoridade de controlo japonesa para garantir um bom nível de conformidade no país.

130. Embora existam melhorias no que diz respeito ao quadro em vigor antes das alterações de 2015, o CEPD observa que a CPP possui menos poderes do que a APD europeia ao abrigo do RGPD, especialmente no que diz respeito à sua **aplicação**. As coimas[56], por exemplo, são bastante suaves. No considerando 108, a decisão da Comissão Europeia salienta que, em casos de incumprimento ou de algumas violações da LPDP, estão em vigor sanções penais e que o presidente da CPP pode encaminhar os casos para o Ministério Público. No entanto, a decisão da Comissão Europeia não tem em conta o facto de a ação pública no Japão ser discricionária e estar, por vezes, sujeita a processos de revisão morosos[57]. Além disso, a pena de prisão (com ou sem trabalho voluntário) associada às violações da LPDP nos termos do disposto no capítulo VII pode ser difícil de executar, porque é dirigida a pessoas singulares e, de qualquer modo, não pune o PIHBO como entidade jurídica que não exerce as suas obrigações de responsabilização.

131. **Tendo em conta o que precede, o CEPD convida a Comissão Europeia a acompanhar de perto a eficácia das sanções e das vias de recurso pertinentes no sistema japonês de proteção de dados.**

3.2.3 O sistema de proteção de dados deve prestar apoio e assistência aos titulares dos dados no exercício dos seus direitos e mecanismos de reparação adequados.

132. A CPP fornece informações e orientações exaustivas no seu sítio Web destinadas a aumentar a sensibilização dos PIHBO no que diz respeito às suas obrigações e responsabilidades no âmbito do quadro de proteção de dados, bem como uma linha telefónica de apoio para prestar informações e

[55] Anexo III.

[56] Estas são apresentadas no capítulo VII da proposta. A sanção máxima é prevista pelo artigo 83.º (disposição ou utilização abusiva de uma base de dados de dados pessoais para fins próprios ou lucros ilegais de terceiros) e equivale a uma pena de prisão de um ano com trabalho ou a uma multa não superior a 500,000 ienes (cerca de 3 900 EUR). De acordo com as explicações fornecidas pela Comissão, as coimas são cumulativas por infração. Embora possa ser este o caso, o CEPD observa que, mesmo que se apliquem coimas cumulativas, o montante total deverá manter-se consideravelmente baixo em comparação com as normas europeias.

[65] Oda H., legislação japonesa, Oxford University Press (edição III), 2009: 439 – 440.

apoio aos cidadãos japoneses sobre os seus direitos individuais no âmbito da LPDP. O sítio Web também tem uma secção denominada «Sala de Crianças», que visa explicitamente um público de crianças e jovens. O CEPD observa que esta informação, juntamente com o apoio da linha telefónica de apoio, as orientações e a documentação de PeR, está disponível em japonês[58]. Por conseguinte, o CEPD acredita firmemente que seria benéfico que a CPP fornecesse uma página específica na versão inglesa do seu sítio Web destinada a fornecer informações sobre os seus direitos individuais ao abrigo do quadro japonês de proteção de dados e ao abrigo das normas complementares aos cidadãos da UE cujos dados serão transferidos para o Japão ao abrigo da decisão de adequação da Comissão Europeia.

133. O CEPD congratula-se com a clarificação feita pela Comissão Europeia no considerando 104 do projeto de decisão de adequação alterado distribuído em 13 de novembro de 2018 no que diz respeito ao serviço de mediação gerido pela CPP nos termos do artigo 61.º, alínea ii), da LPDP. No entanto, o CEPD gostaria de apresentar três pontos em relação a esta questão. Em primeiro lugar, o serviço de mediação não é publicitado na versão inglesa do sítio Web da CPP. Em segundo lugar, o serviço está disponível apenas por telefone e em japonês. Por último, a mediação é apenas um processo facilitador que não conduz a um acordo vinculativo entre as partes, o que tem implicações na eficácia das opções de recurso disponíveis para os titulares dos dados[59].

134. Por último, o CEPD observa que o projeto de decisão de adequação coloca a tónica nas vias de recurso disponíveis através de ações cíveis, bem como em processos penais, mas não reconhece a existência de **barreiras institucionais ao litígio** no Japão, tais como as custas judiciais (as custas judiciais são divididas em partes iguais entre o requerente e o requerido, independentemente de quem é condenado no processo[60]), falta de advogados no país[61], o facto de os advogados estrangeiros não estarem autorizados a praticar o direito nacional, bem como o ónus da prova ao abrigo da responsabilidade civil. O CEPD receia que estes fatores possam, na prática, impedir o acesso dos indivíduos à justiça e comprometer o seu direito a intentar rapidamente vias de recurso judicial e sem suportar custos proibitivos.

135. Face ao exposto, **o CEPD está preocupado com o risco de os indivíduos da UE poderem ter dificuldades no acesso a vias de recurso administrativo e judicial** e, por conseguinte, veria com bons olhos que a Comissão Europeia debatesse com a CPP a possibilidade de criar um serviço em linha, pelo menos em inglês, **destinado a prestar apoio e a tratar as denúncias dos cidadãos da UE[62]**. Adicionalmente, o CEPD acolheria com agrado a possibilidade de permitir que as APD da UE atuassem como intermediários para a apresentação de denúncias dos titulares de dados da UE com as organizações que operam no Japão e a CPP.

[58] https://www.ppc.go.jp/en/contactus/piinquiry/.

[59] Kojima T., *Civil Procedure and ADR in Japan*, Chuo University Press, 2004; e Menkel-Meadow C., *Dispute Processing and Conflict Resolution: Theory, Practice and Policy*, Ashgate (2003) (ed.).

[60] Wagatsuma (2012), «Recent Issues of Cost and Fee Allocation in Japanese Civil Procedure» em Reimann (ed.), Cost and Taxa Allocation in Civil Procedure — Ius Gentium; «Comparative Perspetives on Law and Justice», vol. 11, pp. 195-200.

[61] De acordo com os dados mais recentes, o número de advogados no Japão é de 38 980 (aproximadamente 290 advogados por milhão de pessoas [Japan Federation of Bar Association] (2017), White Paper on Attorneys: p. 8 – 9.

[62] Semelhante ao previsto no anexo II da presente decisão de adequação para as denúncias de residentes na UE relativas ao acesso aos seus dados por parte das autoridades públicas japonesas.

4 ACESSO DAS AUTORIDADES PÚBLICAS AOS DADOS TRANSFERIDOS PARA O JAPÃO

136. A intenção da Comissão consiste em reconhecer, através da decisão de adequação, que «o Japão assegura um nível adequado de proteção dos dados pessoais transferidos da União Europeia para os operadores de empresas de tratamento de dados pessoais no Japão», tal como referido no artigo 1.º do projeto de decisão de adequação. Em conformidade com o artigo 45.º, n.º 2, do Regulamento Geral sobre a Proteção de Dados, a Comissão analisou igualmente as limitações e garantias no que respeita ao acesso a dados pessoais por parte das autoridades públicas. O presente capítulo centra-se na avaliação do acesso aos dados pessoais pelas autoridades responsáveis pela aplicação da lei e por outras entidades públicas para efeitos de segurança nacional. A análise do CEPD baseia-se no projeto de decisão de adequação, no seu anexo II, no qual o governo japonês fornece uma visão geral do quadro jurídico relevante e dos textos jurídicos japoneses, na medida em que estes foram fornecidos pela Comissão. Por conseguinte, no contexto específico da presente avaliação, o CEPD teve em conta elementos relativos às leis japonesas que não fazem parte das constatações da Comissão Europeia, mas que são relevantes para avaliar as condições e garantias que permitem às autoridades públicas japonesas aceder aos dados pessoais transferidos da União Europeia.

4.1 Acesso aos dados por parte das autoridades responsáveis pela aplicação da lei

4.1.1 Procedimentos de acesso aos dados no domínio do direito penal

137. O projeto de decisão de adequação apresenta três formas previstas no direito japonês para que as autoridades responsáveis pela aplicação da lei possam aceder aos dados no Japão:

4.1.1.1 Pedidos de acesso com um mandado judicial

138. O projeto de decisão de adequação estabelece que, para o acesso governamental no Japão e, em especial, para que as autoridades responsáveis pela aplicação da lei em matéria penal possam aceder a elementos de prova eletrónicos no contexto de investigações criminais, devem sempre obter um mandado, a menos que utilizem o procedimento de divulgação voluntária – ver infra.

4.1.1.1.1 Requisito de «causa adequada», necessidade e proporcionalidade das garantias

139. O CEPD reconhece que, nos termos da Constituição japonesa, qualquer recolha de dados pessoais por meios obrigatórios deve basear-se num mandado judicial. Mais especificamente, o projeto de decisão de adequação indica que, em todos os casos de «buscas e apreensões», os mandados judiciais devem ser emitidos com uma «causa adequada», que o Supremo Tribunal considera existir apenas quando a pessoa em causa (suspeita ou arguida) é considerada como tendo cometido uma infração e a busca e apreensão são necessárias para a investigação criminal. A Comissão remete aqui para o acórdão do Supremo Tribunal de 18 de março de 1969, processo n.º 100 (1968(Shi)).). O CEPD recorda que, nos termos da jurisprudência do TJUE[63], apenas um tribunal, e não os delegados do Ministério Público, por exemplo, pode autorizar a recolha de dados relativos ao tráfego e à localização em particular.

140. Também à luz da jurisprudência do TJUE, segundo a qual o acesso aos dados pode ser sujeito a um mandado, tal como na Tele2, o CEPD lamenta que não tenham sido fornecidas informações adicionais para avaliar a forma como os critérios para avaliar a necessidade de um mandado – a gravidade da infração e a forma como foi cometida; valor e importância dos materiais apreendidos como elementos de prova; probabilidade de ocultação ou destruição de materiais apreendidos; extensão das desvantagens causadas por uma apreensão; outras condições conexas – e o conceito de «causa

[63] Ver processos 203/15, C 293/12 e C 594/12 do TJUE.

adequada» derivado da Constituição são aplicados na prática. Por conseguinte, o CEPD convida a Comissão a verificar se a emissão de mandados cumpre os critérios estabelecidos na prática pelo TJUE.

4.1.1.1.2 Tipos de crimes para os quais podem ser emitidos mandados

141. O procedimento do mandado aplica-se apenas quando for efetuada uma «investigação obrigatória». Em princípio, estes mandados apenas podem ser emitidos nos casos em que tenha ocorrido uma violação da lei. A este respeito, o CEPD toma nota da «Lei sobre o crime organizado e o controlo do crime organizado» recentemente adotada em 15 de junho de 2017 no contexto da adesão do Japão à Convenção das Nações Unidas contra a Criminalidade Organizada Transnacional (UNTOC, *UN international Convention on Transnational Crime*)[64]. Na ausência de uma versão inglesa disponível desta legislação, e tendo em conta o requisito da legislação da UE de que alguns dados são recolhidos apenas no contexto da investigação, deteção ou repressão de crimes graves[65], bem como as preocupações expressas por vários comentadores, incluindo o relator especial da ONU, Joseph Cannrataci[66], relativas ao vasto âmbito de aplicação, e que se baseia numa definição de «grupo criminoso organizado» alegadamente vago e demasiado amplo, o CEPD não está em condições de concluir que o acesso a elementos de prova eletrónicos ao abrigo da legislação japonesa aplicável se limita aos limiares previstos na legislação da UE.

142. É também de salientar que, para alguns tipos de infrações, a polícia provincial é competente e possui os seus decretos policiais específicos. O CEPD não dispunha das regras internas aplicáveis à polícia provincial.

143. De acordo com o projeto de decisão de adequação, a recolha de informações eletrónicas no domínio da aplicação do direito penal é da responsabilidade da polícia provincial.

4.1.1.2 Mandados de escutas telefónicas

144. O anexo II do projeto de adequação indica que a Lei relativa às escutas telefónicas no âmbito de investigação penal prevê especificidades para a interceção de comunicações. Esta legislação foi apresentada muito tardiamente, o que não permitiu uma análise aprofundada. Por conseguinte, embora pareçam existir muitas garantias neste quadro jurídico, o CEPD não está em condições de avaliar se as condições previstas no presente texto legislativo estão rodeadas de garantias substancialmente equivalentes às exigidas na UE, tanto pela Carta conforme interpretada pelo Tribunal de Justiça da União Europeia (TJUE) e pela CEDH, tal como interpretado pelo Tribunal de Estrasburgo.

4.1.1.3 Procedimento de «divulgação voluntária» com base na ficha de consulta

145. Esta forma de cooperação não obrigatória permite que as autoridades públicas solicitem aos responsáveis pelo tratamento (com exceção das empresas de telecomunicações) que lhes forneçam os dados de que dispõem. A não conformidade com o pedido não pode ser executada. Continua por esclarecer que autoridades podem utilizar este tipo de procedimento, mas parece limitado às que estão a investigar crimes.

4.1.1.3.1 Condições para a emissão de «fichas de inquérito»

146. O CEPD reconhece que o Supremo Tribunal japonês, por referência à Constituição, desenvolveu limitações à utilização de «divulgações voluntárias»[67]. Do projeto de decisão de adequação resulta que

[64] Ver: https://www.unodc.org/unodc/en/organized-crime/intro/UNTOC.html .
[65] Ver processos apensos C 293/12, C 594/12 e C 203/15.
[66] Relator especial da ONU sobre o direito à privacidade, bem como Graham Greenleaf, investigador em direito da UNSW.
[67] Ver Anexo II, página 8.

as autoridades competentes podem apenas solicitar uma «divulgação voluntária» através da emissão de uma «ficha de consulta». O envio de uma «ficha de consulta» é admissível apenas no âmbito de uma investigação criminal e, por conseguinte, pressupõe sempre uma suspeita concreta de um crime já cometido. Tais investigações são geralmente efetuadas pela polícia provincial, onde são aplicáveis as limitações previstas no artigo 2.º, n.º 2, da regulamentação relativa às forças de segurança pública, o que significa que deve ser relevante para as atividades de polícia. No entanto, o CEPD procura obter esclarecimentos adicionais sobre os contornos concretos dos critérios que permitem a emissão de uma ficha de consulta (como a jurisprudência que ilustra a aplicação destes critérios) e a relação entre o procedimento de divulgação voluntária e a apreensão de dados com base num mandado. Com efeito, mesmo nos casos em que não foi possível obter os dados através do procedimento voluntário, estes ainda poderiam ser obtidos com um mandado, se tal for indispensável para as autoridades de investigação[68].

4.1.1.3.2 Jurisprudência disponível sobre as limitações à utilização da divulgação voluntária de informações

147. Os casos mencionados no projeto de decisão de adequação[69] para ilustrar as limitações à utilização de procedimentos de divulgação voluntária de informações dizem respeito a casos, em que a pessoa acusada foi fotografada ou filmada no espaço público diretamente pela polícia e, por conseguinte, fornecem indicações limitadas quanto a situações em que as autoridades competentes podem solicitar ao responsável pelo tratamento de dados a divulgação de dados, em especial no que diz respeito aos critérios enumerados no anexo II, relativamente à «adequação dos métodos», o que parece abranger a avaliação sobre se a investigação voluntária é «adequada» ou razoável, com vista a alcançar o objetivo da investigação. O mesmo sucede em relação aos critérios gerais de «se pode ser considerado razoável, em conformidade com as convenções socialmente aceites», para avaliar a legalidade dos inquéritos voluntários. Além disso, a Agência Nacional de Polícia, a autoridade federal responsável por todas as questões relativas à polícia judiciária, emitiu instruções à polícia provincial sobre a «utilização adequada em questões de investigação». Entre outros aspetos, o investigador principal deve receber a aprovação interna de um alto funcionário. O CEPD não dispõe de informações se essas instruções forem vinculativas. No entanto, o CEPD estabelece que o recurso a este procedimento deve ser proporcionado ou necessário.

4.1.1.3.3 Direitos e obrigações dos responsáveis pelo tratamento de dados no contexto da divulgação voluntária de informações

148. Além disso, incumbe aos responsáveis pelo tratamento de dados dar o seu consentimento à disponibilização de dados (embora pareça não existir qualquer tipo de obrigatoriedade em obter o consentimento dos titulares dos dados ou em informá-los), desde que esses pedidos não entrem em conflito com outras obrigações legais (por exemplo, obrigações de confidencialidade). O relatório apresentado pela Comissão Europeia parece indicar que, após uma elevada taxa de conformidade, os responsáveis pelo tratamento de dados começaram a ter em conta a proteção de dados dos seus clientes, pelo que começaram a responder com menos frequência a estes pedidos.

149. Além disso, permanece pouco claro se os responsáveis pelo tratamento de dados têm qualquer incentivo para cumprir os pedidos (por exemplo, se tiverem uma vantagem no cumprimento ou se estiverem exonerados de sanções, etc.). Em especial, não é feita qualquer menção a um princípio, como por exemplo, o «princípio da não autoincriminação».

[68] Ver Anexo II, página 7.

[69] Ver anexo II, página 8 — duas decisões do Supremo Tribunal de 24 de dezembro de 1969 (1965 [A] n.º 1187) e de 15 de abril de 2008 (2007 [A] n.º 839).

150. O CEPD gostaria de receber informações adicionais, se disponíveis, sobre o número e o tipo de pedidos, bem como sobre as respostas solicitadas pelos responsáveis pelo tratamento de dados. Na ausência de jurisprudência e números, o CEPD convida a Comissão a monitorizar a eficiência e a aplicação concreta deste procedimento na prática.

151. No entanto, a AEPD não tem jurisprudência nem números sobre este procedimento para estabelecer estes elementos. Por conseguinte, o CEPD não está em condições de apresentar uma avaliação da eficiência e da aplicação concreta deste procedimento sem mais elementos relativos à prática.

4.1.1.4 Conclusão sobre os procedimentos de acesso aos dados para efeitos de aplicação da lei

152. Em conclusão, o CEPD reconhece que o princípio segundo o qual os dados pessoais podem ser acedidos pelas autoridades competentes apenas quando necessário e proporcionalmente ao objetivo, e com base num mandado, corresponde às principais garantias essenciais previstas na legislação da UE e da CEDH. Na sequência das conclusões acima referidas, o CEPD solicita à Comissão que acompanhe o âmbito destas medidas, o âmbito do procedimento de divulgação voluntária de informações e a aplicação deste princípio pela polícia provincial e pelos tribunais, na jurisprudência relevante, e que controle igualmente, se o quadro jurídico japonês fornece as garantias essenciais exigidas pelo TJUE com base na Carta e na CEDH com base na Convenção.

4.1.2 Supervisão no domínio do direito penal

153. O projeto de decisão de adequação, bem como o anexo II, apresentam quatro tipos de supervisão realizados junto das forças policiais, dos ministérios e das agências públicas.

4.1.2.1 Supervisão judicial

4.1.2.1.1 Nos casos em que as informações eletrónicas são obrigatoriamente recolhidas (busca e apreensão)

154. De acordo com o projeto de decisão de adequação, em todos os casos em que as informações eletrónicas são recolhidas por meios obrigatórios (busca e apreensão), a polícia deve obter um mandado judicial prévio. Existe, no entanto, uma exceção a esta regra.[70]. Com efeito, o artigo 220.º, n.º 1, do Código do Processo Penal permite a um procurador do Ministério Público, ao seu adjunto ou a um agente da polícia judiciária confiscar ou apreender informação eletrónica no local da detenção de um suspeito. Nesta situação, é possível excluir essas informações como meio de prova por um juiz.

155. O CEPD está ciente de que também existem exceções semelhantes ao abrigo da legislação da UE. Observa que nem sempre existe um controlo judicial nos casos em que as informações eletrónicas são recolhidas por meios obrigatórios, tal como estipulado no projeto de decisão de adequação. Neste contexto, o CEPD recorda a jurisprudência da CEDH sobre os controlos judiciais a posteriori.[71]

4.1.2.1.2 No caso de pedidos de divulgação voluntária de informações

156. De acordo com o projeto de decisão de adequação, no caso dos pedidos de divulgação voluntária, não existe controlo *ex ante* por parte de um juiz. Nesse caso, a polícia provincial funciona sob a supervisão do procurador do Ministério Público. O projeto de decisão de adequação refere os artigos 192.º, n.º 1, e 246.º relativos à cooperação e coordenação mútuas dos procuradores, à Comissão Municipal de Segurança Pública e aos funcionários da Polícia Judiciária e ao intercâmbio de informações entre eles. Adicionalmente, é feita referência ao artigo 193.º, n.º 1, segundo o qual o procurador do Ministério Público pode dar as instruções necessárias à polícia judiciária, bem como estabelecer normas para uma investigação equitativa. Por último, é mencionado o artigo 194.º relativo às medidas disciplinares

[70] Ver anexo II.
[71] TEDH, Modestou c. Grécia, N.º 51693/13.

exercidas pela Comissão Nacional ou Provincial de Segurança Pública contra a polícia judiciária por não respeitar os procuradores do Ministério Público.

157. O CEPD reconhece o estabelecimento das medidas anteriores e a supervisão conduzida pela Comissão Nacional ou Municipal de Segurança Pública no que concerne polícia judiciária (ver infra).

4.1.2.2 Supervisão pelas Comissões de Segurança Pública da polícia

158. De acordo com o anexo II do projeto de decisão de adequação, dois tipos de comissões estão a exercer uma supervisão da polícia. Ambos visam garantir a gestão democrática e a neutralidade política da administração da polícia.

4.1.2.2.1 Supervisão exercida pela Comissão Nacional de Segurança Pública

159. O anexo II do projeto de decisão de adequação mencionava a supervisão efetuada pela Comissão Nacional de Segurança Pública na NPA. A regulamentação relativa às forças de segurança pública fornece uma lista das funções da Comissão da qual emanam os seus poderes de supervisão (ver o artigo 5.º).

160. Nos termos do artigo 4.º da regulamentação relativa às forças de segurança pública, a Comissão Nacional de Segurança Pública é constituída sob a jurisdição do primeiro-ministro e é composta por um presidente e cinco membros. O artigo 7.º estabelece algumas limitações quanto à nomeação dos membros da Comissão. A duração do mandato dos membros da Comissão é de cinco anos, podendo ser prorrogada apenas uma vez, em conformidade com o artigo 8.º. Além disso, a Dieta parece ter um forte poder sobre a nomeação e o despedimento do membro da Comissão, o que assegura a independência da Comissão Nacional de Segurança Pública.

161. Estas disposições jurídicas reforçam a neutralidade política da Comissão Nacional de Segurança Pública.

4.1.2.2.2 Supervisão exercida pelas Comissões Municipais de Segurança Pública

162. A polícia provincial está sujeita à fiscalização das Comissões Municipais de Segurança Pública estabelecida em cada província. Nos termos do artigo 2.º e do artigo 36.º, n.º 2, da regulamentação relativa às forças de segurança pública, as Comissões Municipais de Segurança Pública são responsáveis pela «proteção dos direitos e da liberdade de uma pessoa». O artigo 38.º, bem como o artigo 42.º, da regulamentação relativa às forças de segurança pública, enumeram os deveres das comissões municipais de segurança pública. As referidas Comissões têm igualmente por objetivo garantir a gestão democrática e a neutralidade política da administração policial, tal como indicado no artigo 43.º, n.º 2, através da emissão à polícia provincial de casos individuais sempre que o considerem necessário no contexto de uma inspeção das atividades da polícia provincial ou de uma conduta indevida do seu pessoal.

163. No entanto, não é claro se tais Comissões têm outros poderes para além do controlo do comportamento da polícia. O CEPD interroga-se se a expressão «conduta indevida» abrange o acesso ilegal a dados e, nesse caso, se as Comissões podem, ou não, ordenar o apagamento dos dados.

164. No que diz respeito à neutralidade e à independência das Comissões, tal como indicado no projeto de decisão de adequação[72], as Comissões Municipais de Segurança Pública são estabelecidas sob a jurisdição do governador, que tem de nomear membros da Comissão com o consentimento da assembleia municipal. Os membros da Comissão Municipal de Segurança Pública têm um mandato de três anos e podem ser renomeados até duas vezes. O artigo 39.º da regulamentação relativa às forças de segurança pública revelou limitações quanto à nomeação dos membros. O projeto de decisão de

[72] Ver projeto de decisão de adequação, p. 31.

adequação também menciona a supervisão da polícia provincial por assembleia local, fazendo referência ao artigo 100.º da Lei sobre os contratos públicos. No entanto, este ato não foi concedido ao Comité Europeu para a Proteção de Dados[73].

165. Além disso, nos termos do artigo 42.º, n.os 2 e 3, da regulamentação relativa às forças de segurança pública, «nenhum membro da Comissão passa a ser simultaneamente membro da assembleia ou do pessoal das entidades públicas locais a tempo inteiro ou contratado a tempo parcial ao abrigo do disposto no artigo 28.º, n.º 5, da lei relativa ao serviço público local.

166. De acordo com os elementos acima referidos e tendo em conta a colaboração entre as Comissões Municipais de Segurança Pública e a Comissão Nacional de Segurança Pública, o CEPD concorda com o projeto de decisão de adequação e congratula-se com a neutralidade e a independência dos membros das Comissões Municipais de Segurança Pública. O CEPD entende que as Comissões Municipais de Segurança apenas têm o poder de investigar o comportamento da polícia e que não dispõem de outros poderes de supervisão, incluindo o apagamento de dados recolhidos pela polícia provincial. Por conseguinte, afigura-se necessário clarificar se a supervisão exercida pelas Comissões Municipais de Segurança Pública é suficiente, de acordo com as normas estabelecidas ao abrigo da legislação da UE.

4.1.2.2.3 Supervisão exercida pela Dieta

167. O projeto de decisão de adequação[74] e o anexo II[75] fornecem algumas informações sobre a supervisão exercida pela Dieta em relação ao governo, nomeadamente no que diz respeito à legalidade da recolha de informações de dados pela polícia. Efetivamente, ambos referem o artigo 62.º da Constituição, segundo o qual a Dieta pode solicitar a apresentação de documentos e o depoimento de testemunhas. Ambos contêm também disposições legais da legislação da Dieta, em especial do artigo 104.º, relativas aos poderes da Dieta, bem como do artigo 74.º, relativas à apresentação de inquéritos escritos, que devem ser respondidos pelo Conselho de Ministros, por escrito, no prazo de sete dias, como previsto no artigo 75.º. O projeto de decisão de adequação acrescenta igualmente: «O papel da Dieta na supervisão do órgão executivo é apoiado por obrigações de comunicação de informações, por exemplo, nos termos do artigo 29.º da Lei sobre as escutas telefónicas».

168. O CEPD reconhece o envolvimento da Dieta na supervisão do governo e da polícia no que concerne a legalidade da recolha de dados.

4.1.2.2.4 Supervisão exercida pelo órgão executivo

169. De acordo com o anexo II do projeto de adequação, o ministério ou o chefe de cada ministério ou organismo tem, por um lado, a autoridade de supervisão e controlo do cumprimento com base na APPIHAO[76]. Por outro lado, o Ministro dos Assuntos Internos e das Comunicações (MIC) tem um poder de investigação relativo à aplicação da APPIHAO por todos os outros ministérios, incluindo o Ministério da Justiça para a Polícia, tal como mencionado no projeto de decisão de adequação[77].

170. O ministério pode solicitar ao chefe de um órgão de administração a apresentação de materiais e explicações sobre o tratamento de dados pessoais pelo órgão de administração em causa, com base no artigo 50.º da APPIHAO. É possível solicitar uma revisão das medidas sempre que se suspeite da ocorrência de uma infração ou de um funcionamento inadequado da lei, bem como emitir pareceres

[73] Ver projeto de decisão de adequação, p. 33.
[74] Ver projeto de decisão de adequação, p. 30.
[75] Ver anexo II, p. 12.
[76] Ver anexo II, p. 10.
[77] Ver anexo II, p. 11.

relativos ao tratamento de dados pessoais pelo órgão administrativo em causa, nos termos dos artigos 50.º e 51.º da APPIHAO.

171. O projeto de decisão de adequação e o anexo II mencionam igualmente a criação de 51 centros de informação abrangente que «asseguram a correta aplicação da presente lei», em conformidade com o artigo 47.º da APPIHAO. O CEPD salienta que a APPIHAO não explica o papel e os poderes desses centros de informação, mas que o projeto de decisão de adequação fornece algumas elucidações.

172. Por conseguinte, o CEPD congratula-se com o facto de haver um controlo sobre o poder executivo no respeito pela APPIHAO, nos ministérios e nos órgãos administrativos, por parte do MIC.

173. Em conclusão, a legislação da UE e a CEDH, na jurisprudência dos respetivos tribunais, estão a criar normas e garantias segundo as quais a supervisão deve ser completa, neutra e independente. O CEPD observa que a CPP não dispõe de poderes de supervisão em questões relacionadas com a aplicação da lei. Além disso, se a supervisão exercida pela Dieta, pela Comissão Nacional e pela Comissão Municipal de Segurança parecer ser neutra e independente, são necessários mais esclarecimentos sobre os poderes de supervisão das Comissões Municipais de Segurança Pública.

4.1.3 Reparação no domínio do direito penal

174. O projeto de decisão de adequação, complementado pelo anexo II, apresenta várias vias através das quais os indivíduos podem apresentar as suas denúncias, tanto perante as autoridades independentes como perante os juízes.

175. Estas vias e os principais elementos destes procedimentos decorrentes da documentação disponível são apresentados após uma breve panorâmica dos direitos disponíveis para esclarecer o que os titulares dos dados podem esperar das autoridades públicas no contexto do tratamento de dados, no domínio dos processos penais.

4.1.3.1 Direitos dos titulares dos dados disponíveis no âmbito de processos penais

176. Para obterem reparação, os titulares dos dados devem ter direitos, ao abrigo da lei, de forma a poderem alegar que não foram respeitados. Por conseguinte, o CEPD avaliou igualmente os direitos disponíveis no contexto dos processos penais apresentados no projeto de decisão de adequação.

4.1.3.1.1 Limitações gerais dos direitos dos titulares dos dados ao abrigo da APPIHAO

177. No seu projeto de decisão de adequação, a Comissão remete para os princípios gerais de proteção de dados que as autoridades públicas devem respeitar assim que recolherem dados pessoais. Estes princípios são também descritos de forma mais pormenorizada no anexo II, de modo a que o Comité Europeu para a Proteção de Dados tenha decidido comentar as mesmas.

178. No que diz respeito aos direitos disponíveis, o CEPD observa que, de acordo com o anexo II do projeto de decisão de adequação, alguns dos direitos gerais fornecidos aos titulares dos dados no contexto dos dados tratados pelos órgãos administrativos continuam igualmente disponíveis no contexto de investigações criminais. No entanto, as limitações adicionais no que se refere à recolha e ao tratamento posterior das informações pessoais neste contexto decorrem também da própria APPIHAO.

179. Estas limitações, que também parecem aplicar-se tanto no contexto dos dados recolhidos com base em mandado, como com base numa ficha de inquérito no contexto da divulgação voluntária, suscitam questões relativas a vários aspetos.

180. No que se refere ao princípio da limitação da finalidade, embora, em princípio, os órgãos administrativos sejam obrigados a especificar a finalidade para a qual conservam dados pessoais e não

os conservam para além do âmbito necessário para a consecução do objetivo de utilização especificado, podem alterar o objetivo se for «o que pode razoavelmente ser considerado adequadamente relevante para o fim inicial».

181. A APPIHAO também prevê o princípio da não divulgação, segundo o qual um funcionário não pode revelar as informações pessoais adquiridas a outra pessoa sem uma justificação válida, ou utilizar essas informações para uma finalidade injusta. No entanto, não são fornecidas informações adicionais relativamente à interpretação do que um «motivo justificável» ou «objetivo sem causa» poderia abranger, de modo que seriam necessários esclarecimentos adicionais para a avaliação.

182. A APPIHAO, artigo 8.º, n.º 1, estabelece igualmente a proibição de utilizar ou divulgar dados «salvo disposição em contrário das leis e regulamentos». No entanto, embora esta disposição não seja, em princípio, contrária ao nível de proteção proporcionado pela legislação da UE, o CEPD carece de elementos adicionais no que respeita à medida em que qualquer supervisão ou controlo é exercido quando a divulgação é efetuada por leis ou regulamentos. Além disso, nos termos do artigo 8.º, n.º 2, aplicam-se exceções adicionais a esta regra se «essa divulgação excecional não for suscetível de prejudicar gravemente os direitos e interesses do titular dos dados ou de um terceiro». Sem quaisquer outros elementos a este respeito, esta exceção, que se baseia na noção pouco clara de danos «injustos», necessita de um maior esclarecimento, caso seja suficientemente limitada.

183. Por último, a APPIHAO, artigo 9.º, prevê restrições adicionais quanto à finalidade ou ao método de utilização ou quaisquer outras restrições, que devem ser impostas pelo chefe de um órgão de administração quando as informações pessoais retidas sejam fornecidas a outra pessoa. Como as noções de «quaisquer outras restrições necessárias» e «fornecidas a outra pessoa» são muito amplas, estas restrições adicionais aos direitos das pessoas em causa suscitam preocupações sem esclarecimentos adicionais sobre o âmbito desta disposição.

184. Embora o CEPD esteja plenamente consciente de que os direitos de acesso e outros princípios de proteção de dados também são limitados no âmbito de processos penais ao abrigo da legislação da UE, são previstas salvaguardas adicionais quando essas limitações estão previstas, nomeadamente em termos de supervisão, fiscalização e recurso. Na ausência de uma jurisprudência suficiente sobre estas limitações ou elementos adicionais para clarificar o âmbito de aplicação destas disposições, o CEPD não está em condições de avaliar se estas limitações aos direitos dos titulares dos dados se limitam ao que seria considerado estritamente necessário e proporcional ao abrigo da legislação da UE e, por conseguinte, seriam essencialmente equivalentes aos direitos que os titulares dos dados da UE teriam.

4.1.3.1.2 Limitações adicionais aos direitos da APPIHAO decorrentes do Código de Processo Penal e dos decretos da polícia provincial

185. O CEPD observa que, embora a APPIHAO pareça ser aplicável a todo o tratamento por órgãos administrativos do Japão, algumas limitações importantes aos direitos dos titulares dos dados decorrem de legislações específicas. Nomeadamente, o artigo 53.º, n.º 2, do Código do Processo Penal[78] prevê que «as informações pessoais registadas em documentos relativos a ensaios e artigos apreendidos» estão excluídas do âmbito de aplicação dos direitos individuais no capítulo IV da APPIHAO. Concretamente, o CEPD entende, por conseguinte, que, no contexto dos processos penais, os titulares dos dados não beneficiam dos direitos de informação, de acesso, de retificação ou de apagamento de dados pessoais registados em documentos relativos a ensaios e artigos apreendidos.

[78] Disponível aqui http://www.japaneselawtranslation.go.jp/law/detail/?printID=&id=2283&re=02&vm=02 e citado no anexo II do projeto de decisão de adequação, nota de rodapé 25.

186. No que diz respeito a estas limitações, o CEPD entende que se aplicam no contexto dos dados recolhidos com base em mandados, bem como no contexto dos dados recolhidos no âmbito da divulgação voluntária através de fichas de inquérito (ver infra). Com efeito, a base jurídica dos dois procedimentos para aceder aos dados (através de um mandado e através de uma ficha de informação) é apresentada no código do processo penal. O artigo 53.º, n.º 2, deste Código parece aplicar-se a ambos os tipos de recolha. No entanto, uma vez que o artigo 53.º, n.º2, se refere aos artigos «apreendidos», pode ser esclarecido se as limitações aos direitos previstos ao abrigo desta disposição também se aplicam no contexto da divulgação voluntária.

187. O CEPD lamenta não receber a legislação da Polícia Provincial, que alegadamente protege as informações pessoais, os direitos e as obrigações equivalente à APPIHAO. Tendo em conta, por um lado, as ambiguidades relativas à interpretação da APPIHAO e, por outro, a indisponibilidade das forças policiais provinciais, o CEPD interroga-se se os direitos concedidos aos indivíduos neste contexto, bem como os mecanismos de controlo e/ou reparação adicionais, são suficientes para compensar a ausência de direitos.

4.1.3.2 Recurso através das autoridades independentes

4.1.3.2.1 Recurso administrativo

188. O CEPD observa que os órgãos administrativos responsáveis pela recolha de dados, tais como a polícia provincial, são competentes para tratar os pedidos das pessoas relativamente aos seus direitos — limitados — no que diz respeito aos seus dados recolhidos no âmbito de investigações criminais (ver supra, relativamente aos direitos disponíveis), que parecem incluir tanto a recolha de dados com base num mandado como em fichas de inquérito. Concretamente, estes direitos parecem estar limitados a princípios gerais, tais como a necessidade de conservação de dados em ligação com o objetivo (ver artigo 3.1.º da APPIHAO), o princípio da limitação da finalidade (artigo 4.º) ou a exatidão dos dados (artigo 5.º), enquanto os direitos individuais, como o direito à informação, ao acesso, à retificação ou ao apagamento, estão excluídos dos dados pessoais registados em documentos relativos a ensaios e artigos apreendidos[79]. Embora estes órgãos não possam ser considerados independentes e, por conseguinte, como uma tutela ou um controlo independentes, o CEPD congratula-se com esta possibilidade. No entanto, salienta-se que as denúncias apresentadas neste contexto continuam a ser limitadas a um número muito reduzido de direitos dos titulares dos dados, tendo em conta as limitações dos direitos que lhe são conferidos pela APPIHAO.

189. Além disso, uma vez que as «informações pessoais registadas em documentos relativos a ensaios e artigos apreendidos» estão excluídas do âmbito de aplicação dos direitos individuais constantes do capítulo IV da APPIHAO em conformidade com os artigos 53-2.º do Código do Processo Penal, as possibilidades de solicitar o acesso a informação pessoal estão igualmente limitadas aos procedimentos previstos noutras disposições do presente Código do Processo Penal. Aparentemente, apenas as vítimas, as pessoas suspeitas ou acusadas podem intervir neste contexto e, ainda assim, dependendo da fase do processo penal. Por conseguinte, o CEPD está preocupado com o facto de os titulares dos dados não terem o direito geral de acesso e/ou de retificação ou de apagamento de informações ao abrigo da legislação japonesa no contexto do processo penal, e de todas as vias de recurso disponíveis implicarem que o sujeito seja uma vítima (caso em que a pessoa saberá provavelmente que os seus dados foram recolhidos) ou um suspeito ou acusado, ou a demonstração de um dano, ao passo que os titulares dos dados também devem ter o direito de aceder aos seus dados e de, eventualmente, pedir a retificação ou o apagamento dos seus dados quando não sofrem danos

[79] Ver supra as limitações à APPIHAO e, em particular, o artigo 53.º, n.º 2, do Código do Processo Penal (não previsto, mas citado no anexo II do projeto de decisão de adequação, nota de rodapé 25).

(contudo, possível) e/ou quando não são uma vítima, um suspeito ou um acusado, mas testemunhas, por exemplo.

4.1.3.2.2 Recurso administrativo através das comissões municipais de segurança pública

190. Além disso, as comissões municipais de segurança pública parecem ser competentes para tratar as denúncias. Com base no artigo 79.º da regulamentação relativa às forças de segurança pública a que se refere o projeto de decisão de adequação, os indivíduos podem recorrer contra qualquer comportamento ilegal ou inadequado de um agente no exercício das suas funções.

191. O CEPD solicita esclarecimentos sobre se o tratamento «ilegal» de dados pessoais pode ser considerado um «comportamento ilícito ou inadequado de um agente» e sobre se demonstra uma desvantagem que parece ser exigida ao titular dos dados. Com efeito, a comunicação da ANE às Comissões Municipais de Segurança Pública e à Polícia sobre o correto tratamento de denúncias relativas à execução de tarefas por agentes policiais limita as denúncias a pedidos concretos de «correção de eventuais desvantagens específicas que tenham sido infligidas por um agente da polícia na sequência de um comportamento ilegal ou inadequado, ou da não adoção das medidas necessárias por parte de um agente da polícia», bem como a possibilidade de «apresentar denúncia/descontentamento em relação a um modo inadequado de execução de funções por um agente da polícia». É expressamente clarificado que devem ser excluídas as «denúncias contra o incumprimento de um agente da polícia relativamente a qualquer matéria que não seja considerada como estando sob o dever de um oficial de polícia, bem como as que expressam um parecer geral ou uma proposta que não afeta diretamente a própria parte requerente».

192. No que diz respeito aos requisitos processuais para apresentar uma denúncia, embora devam ser apresentados por escrito, o CEPD observa que a assistência para escrever a denúncia é apresentada neste contexto ao abrigo da legislação japonesa, incluindo para os estrangeiros. Além disso, o Governo japonês também parece ter confiado à CPP o dever de prestar assistência aos titulares dos dados da UE para tratar e resolver denúncias neste domínio, que o CEPD acolhe favoravelmente. O CEPD sublinha que, no seu entender, neste contexto, a CPP só funcionará como ponto de contacto entre os titulares dos dados da UE e as autoridades competentes do Japão.

193. Os resultados da Comissão Municipal da Segurança Pública na sequência de uma denúncia não são detetados nos casos enumerados no artigo 79.º, n.º 2, da regulamentação relativa às forças de segurança pública, o que inclui o caso em que o atual «residente do autor da denúncia é desconhecido». O CEPD reconhece que a referência ao residente não implica que, em todos os casos, os titulares dos dados da UE sejam, por conseguinte, excluídos da notificação dos resultados das suas denúncias com base no facto de não residirem no Japão.

4.1.3.2.3 Mecanismo ad hoc incluindo a CPP

194. Tendo em conta as conclusões acima descritas, o CEPD congratula-se com o facto de o Governo japonês e a Comissão da UE terem acordado um mecanismo adicional de recurso que proporciona aos cidadãos da UE uma via adicional de reparação no Japão através do qual as pessoas podem igualmente procurar obter reparação contra inquéritos ilegais ou inadequados por parte das autoridades públicas. Além disso, o CEPD observa e congratula-se com o facto de os pedidos poderem ser apresentados junto da CPP, em vez de serem apresentados junto de outro oficial do governo, alargando assim o âmbito de competência da CPP ao domínio da aplicação da lei e da segurança nacional.

195. Aquando da análise do novo mecanismo, o CEPD tem-se centrado em compreender os poderes que a CPP tem neste contexto.

196. Embora não seja totalmente claro, o CEPD compreende que o mecanismo de recurso adicional não exige «um padrão», no sentido em que o requerente não é obrigado a demonstrar que os seus dados pessoais são suscetíveis de ter sido objeto de vigilância por parte de uma autoridade japonesa. O CEPD gostaria ainda de solicitar a confirmação por parte da Comissão.

197. Em consonância com a sua avaliação do mecanismo do Provedor de Justiça, criado ao abrigo do Escudo de Proteção da Privacidade, o CEPD salienta a necessidade de poderes efetivos do destinatário do pedido, neste caso a CPP, a fim de considerar o mecanismo de recurso como essencialmente equivalente a um recurso efetivo na aceção do artigo 47.º da Carta dos Direitos Fundamentais.

198. Ao explicar o mecanismo de recurso, o Governo japonês remete para o artigo 6.º, o artigo 61.º, alínea ii), e o artigo 80.º, e estabelece estes poderes no anexo II. O CEPD considera que o procedimento descrito no anexo II especifica ou alarga os poderes do PPC, uma vez que a linguagem utilizado no artigo 6.º, no artigo 61.º, alínea ii), e no artigo 80.º, é bastante vaga e geral. Na medida em que o anexo II especifica ou alarga os poderes da CPP, o CEPD gostaria de solicitar esclarecimentos sobre a vinculação das outras agências do governo japonês.

199. Com base no procedimento constante do anexo II, o CEPD observa que as autoridades públicas competentes do Japão devem cooperar com a CPP, «nomeadamente fornecendo-lhes as informações necessárias e material relevante, de modo a que a CPP possa avaliar se a recolha ou a subsequente utilização de dados pessoais foram efetuadas em conformidade com as regras aplicáveis». Para a avaliação da eficácia do sistema, é, pois, importante referir novamente os poderes que as autoridades competentes, com o que a CPP coopera, têm. Na opinião do CEPD, esses poderes não seriam alargados através das garantias previstas no anexo II.

200. O CEPD observa igualmente que, se tiver sido identificada uma violação das regras, «a cooperação das autoridades públicas em causa com a CPP inclui a obrigação de sanar a violação», o que inclui expressamente o apagamento dos dados recolhidos em violação das regras aplicáveis. O CEPD considera que as obrigações da autoridade competente decorrem da «cooperação com a CPP», em vez de uma decisão da CPP.

201. Por último, a CPP informará o requerente relativamente ao «resultado da avaliação, incluindo quaisquer medidas corretivas eventualmente tomadas». Além disso, a CPP informará o requerente da «possibilidade de obter uma confirmação dos resultados da autoridade pública competente e da autoridade à qual deve ser apresentado um pedido de confirmação».

202. Além disso, a CPP comprometeu-se a auxiliar o requerente a propor novas ações ao abrigo da legislação japonesa, caso o requerente não concorde com o resultado do procedimento.

203. Tendo em conta a necessidade de dispor de um mecanismo de recurso eficaz, essencialmente equivalente às normas da UE, o CEPD pergunta, no entanto, se a CPP tem quaisquer poderes específicos para além de avaliar se a recolha ou a subsequente utilização de informação pessoal teve lugar em conformidade com as regras aplicáveis e insta as autoridades competentes a utilizarem os respetivos poderes e a tratarem as denúncias que lhes sejam enviadas pela CPP. Se a CPP apenas atuar como ponto de contacto para os cidadãos da UE, o CEPD considera este facto insuficiente para prever um mecanismo de recurso eficaz, essencialmente equivalente às normas da UE. O CEPD insta, por conseguinte, a Comissão a prestar esclarecimentos sobre os pontos mencionados no presente subcapítulo, em especial sobre se e de que forma o mecanismo alarga as obrigações das autoridades competentes, de que forma estão vinculadas, e a forma como a CPP pode efetivamente assegurar o cumprimento e não só atuar como ponto de contacto para os cidadãos da UE.

4.1.3.3 Recurso judicial

4.1.3.3.1 Mecanismo quase alternativo para a apresentação de denúncias

204. O chamado procedimento de «quase-denúncia» permite agir contra a recolha coerciva de informação com base num mandado de apreensão ou alteração de uma apreensão ilegal.

205. Esta via implica que a pessoa tem conhecimento da apreensão dos dados. No entanto, o CEPD compreende que o procedimento de recolha de dados com base num mandado não é notificado ao titular dos dados. Do mesmo modo, compreende que a divulgação voluntária não implica que as empresas solicitadas tenham a obrigação de informar as pessoas em causa dos pedidos recebidos e cumpridos. Por conseguinte, embora seja sublinhado no anexo II que «esse desafio pode ser interposto sem que o indivíduo tenha de esperar pela conclusão do processo», na prática, para além dos mandados que autorizam a realização de escutas telefónicas, em relação às quais é indicado que a lei prevê uma obrigação de notificação[80], esta via parece estar efetivamente disponível apenas quando o titular dos dados tiver conhecimento da recolha através de um processo intentado contra o mesmo.

4.1.3.3.2 Ação inibitória

206. Adicionalmente, para obter o apagamento dos dados recolhidos através de um processo penal (a chamada «reparação injuntiva»), ou para obter uma indemnização, os indivíduos podem também intentar ações cíveis perante um juiz.

207. No que diz respeito à compensação, o CEPD observa que o procedimento parece estar circunscrito às situações em que um funcionário público, no exercício das suas funções, casou danos, ilegalmente e com culpa (deliberadamente ou por negligência), à pessoa em causa. No entendimento do CEPD, os danos parecem incluir danos morais. No entanto, não está definido de forma mais pormenorizada o que deve ser demonstrado pelo indivíduo que sofreu um dano. O Comité Europeu para a Proteção de Dados não estava em condições de avaliar a jurisprudência relativa à concessão de uma compensação e, por conseguinte, não pôde avaliar se esta via prevê um recurso efetivo em caso de danos.

208. No que diz respeito à «ação inibitória», o CEPD nota igualmente que, para apresentar um pedido, a pessoa em causa deve ter primeiro conhecimento de que os seus dados foram recolhidos e que continuam a ser mantidos. Por conseguinte, tendo em conta os direitos limitados de informação e de acesso das pessoas singulares no contexto das investigações e dos procedimentos penais, a eficiência do procedimento parece ser demasiado limitada.

4.1.3.4 Avaliação global das vias de recurso

209. Na sequência da avaliação de todas as vias de recurso em aberto para os indivíduos ao abrigo da legislação japonesa, bem como para os titulares dos dados da UE perante a CPP, o CEPD congratula-se com o mecanismo ad hoc de resolução de litígios que envolve a CPP. Tem um valor acrescentado para os titulares dos dados da UE, em especial porque lhes permite compreender as vias disponíveis para obter reparação e/ou compensação, bem como apresentar os seus pedidos em conformidade com os requisitos processuais aplicáveis ao abrigo da legislação japonesa. No entanto, são necessários esclarecimentos adicionais, em particular sobre se e de que forma o mecanismo alarga as obrigações das autoridades competentes, de que forma estão vinculadas, e como a CPP pode, efetivamente, assegurar o cumprimento, a fim de garantir que este novo mecanismo estabelece vias de recurso eficazes.

[80] O artigo 23.º da Lei de escutas telefónicas é mencionado na página 33 do projeto de decisão de adequação, mas o CEPD não recebeu este texto, pelo que não é capaz de avaliar em que medida esta obrigação de notificação é aplicável e em que casos pode ser limitada.

210. Esta avaliação mostra que nenhum mecanismo de recurso no direito japonês parece permitir o acesso, a retificação ou o apagamento de dados para os titulares dos dados que não sejam vítimas, suspeitos ou arguidos no âmbito de um processo penal, por exemplo, para corrigir a recolha ou conservação ilegal dos seus dados. Além disso, mostra que todos os procedimentos e mecanismos de recurso e compensação disponíveis ao abrigo da legislação japonesa para as vítimas, suspeitos ou arguidos implicam o conhecimento da recolha de dados, que parece ser limitada na prática, uma vez que lhes são facultados direitos de acesso e de informação limitados. Além disso, afigura-se necessária uma clarificação adicional sobre a demonstração de um comportamento ilegal por parte das autoridades, em especial se esse comportamento inclui qualquer tratamento ilegal de dados pessoais ou um dano sofrido pelo indivíduo.

211. Por conseguinte, sem mais documentação e elementos, o CEPD está preocupado em saber se a reparação prevista na legislação japonesa e no projeto de decisão de adequação é suficientemente eficaz em comparação com as normas da legislação da UE.

4.2 Acesso para fins de segurança nacional

4.2.1 Âmbito de supervisão

212. No projeto de decisão de adequação, o capítulo sobre «acesso e utilização pelas autoridades públicas japonesas para efeitos de segurança nacional» é introduzido por uma declaração geral, em consonância com a garantia prestada pelo governo japonês no anexo II, segundo a qual nenhuma lei japonesa permitiria «pedidos de informação ou "escutas administrativas" fora do âmbito das investigações penais». Em suma, afirma-se que «apenas é possível obter as informações relativas aos motivos de segurança nacional a partir de uma fonte de informação acessível gratuitamente por qualquer pessoa ou por divulgação voluntária. Tal exclui quaisquer atividades de vigilância discreta neste domínio. Os operadores de empresas que recebem um pedido de cooperação voluntária (sob a forma de divulgação de informações eletrónicas) não estão juridicamente obrigados a prestar essas informações.»[81]

213. Dentro destas limitações, estão enumeradas quatro entidades públicas que têm o poder de recolher informações eletrónicas na posse de operadores comerciais japoneses por motivos de segurança nacional. No que diz respeito ao Ministério da Defesa, na qualidade de uma destas quatro entidades, diz-se que o mesmo «tem autoridade apenas para recolher informações (eletrónicas) através de divulgações voluntárias».[82]

214. Com vista a avaliar a configuração geral da recolha de dados para efeitos de segurança nacional, o CEPD recorda a primeira das quatro chamadas «garantias essenciais», segundo as quais «o tratamento deve basear-se em regras claras, precisas e acessíveis»[83]. Mais especificamente, a CEDH foi muito clara quanto ao facto de os programas de vigilância estarem apenas «em conformidade com a legislação» se as medidas de vigilância «tiverem alguma base no direito nacional». O tribunal esclareceu que a compatibilidade com o Estado de direito exige que a lei que autoriza a medida seja acessível e previsível quanto aos seus efeitos. Remetendo para o risco de arbitrariedade, o tribunal tem exigido «regras claras e circunstanciadas em matéria de medidas de vigilância secreta»; «suficientemente

[81] Decisão de adequação, n.º 151.
[82] Decisão de adequação, n.º 153.
[83] GT29, GT 237: Documento de trabalho 01/2016 sobre a justificação das interferências com os direitos fundamentais à privacidade e à proteção de dados através de medidas de vigilância quando da transferência de dados pessoais (garantias essenciais europeias).

claras para dar aos cidadãos uma indicação adequada das circunstâncias e das condições em que as autoridades públicas estão habilitadas a recorrer a qualquer uma dessas medidas».[84]

215. Para a aplicação destas garantias essenciais ao sistema jurídico do Japão, o CEPD está ciente não só do facto de, em matéria de segurança nacional, os Estados disporem de uma ampla margem de apreciação, reconhecida pelo Tribunal Europeu dos Direitos do Homem. Adicionalmente, os poderes de segurança nacionais refletem as experiências históricas das nações. O CEPD entende, por conseguinte, que, tal como salientado pelo Governo japonês, após a Segunda Guerra Mundial, as agências nacionais de informação do Japão têm sido dotadas de poderes mais limitados do que noutros Estados.

216. Na leitura do CEPD, o projeto de decisão sobre o nível de proteção adequado, em consonância com as garantias dadas pelo Governo japonês, sugere que as entidades do Governo japonês não realizam programas, que controlam estrategicamente a comunicação em termos gerais (Internet). Tal como acima referido, o governo japonês deu garantias, numa carta assinada pelo Ministro da Justiça, de que «apenas é possível obter as informações relativas aos motivos de segurança nacional a partir de uma fonte de informação acessível gratuitamente por qualquer pessoa ou por divulgação voluntária».

217. Quanto à base jurídica do Ministério da Defesa, o CEPD observa que o projeto de decisão de adequação inclui informações gerais sobre os seus poderes e cita a sua missão de «levar a cabo os assuntos relacionados com a mesma a fim de garantir a paz e a independência a nível nacional e a segurança da nação». No entanto, o CEPD não recebeu uma tradução para inglês da base jurídica.

218. Ao mesmo tempo, o CEPD tem conhecimento dos relatórios publicados em diferentes meios de comunicação social, sugerindo que os programas de vigilância são geridos pela Direção da Informação sobre Transmissões do Ministério da Defesa (MD)[85] do Japão. No relatório, alega-se igualmente que, ao recusar o debate específico do relatório, o Ministério da Defesa japonês «reconheceu que o Japão possui "gabinetes em todo o país" que intercetam comunicações» e que esses «se centrarão em atividades militares e em "ciberameaças"» e «não recolhem as informações do público em geral». Esta última afirmação (que o MD não recolhe informações sobre o público em geral) faz parte da reexpressão pelo governo japonês.

219. Significa que o governo japonês reafirmou, numa carta assinada pelo Ministro da Justiça, que o MD não recolhe informações sobre o público em geral.

220. É uma tarefa que vai além do âmbito do CEPD proceder a uma avaliação geral das capacidades de vigilância possíveis do governo japonês. Estas atividades são importantes apenas para a sua avaliação se forem relevantes para a transferência de dados pessoais entre a UE e o Japão. Neste contexto, o CEPD gostaria de reafirmar a sua abordagem já adotada pelo seu antecessor quando solicitou que se optasse pelo Escudo de Proteção da Privacidade UE-EUA. Ao emitir um parecer sobre o Escudo de Proteção da Privacidade, o GT29 incluiu na sua análise os poderes e os limites dos EUA para a vigilância dos dados «a caminho» dos EUA[86]. Aplicando a mesma norma que fora aplicada para a decisão de

[84] Ver, por exemplo, o caso de Big Brother Watch e outros contra o Reino Unido, n.º 305.

[85] Em maio de 2018, a publicação em linha «The Intercept» publicou um relatório intitulado «The untold story of Japan's secret spy agency» (A história desconhecida da agência secreta de espionagem do Japão).

[86] Ver GT255, Escudo de Proteção da Privacidade UE-EUA – Primeira reapreciação conjunta anual, adotada em 28 de novembro de 2017, p. 16: «O GT29 considera que a análise da legislação do país terceiro em relação à qual a adequação é considerada não se deve limitar à legislação e prática que permite a vigilância dentro das fronteiras físicas desse país, mas deve também incluir uma análise das bases jurídicas da legislação desse país terceiro que lhe permita efetuar a vigilância fora do seu território no que diz respeito aos dados da UE. Tal como já sublinhado no seu parecer anterior, «deve ficar claro que os princípios do Escudo de Proteção da Privacidade

adequação relativa ao Japão, o CEPD considera relevantes as informações sobre os poderes das autoridades japonesas para controlar os dados «a caminho» do Japão. Se estes poderes de vigilância existirem, a decisão de Big Brother Watch por parte da CEDH parece sugerir que tais poderes teriam de ser regulados de acordo com as normas estabelecidas pela CEDH.

221. Consequentemente, se as interceções se limitarem à «assistência de uma ação militar», podem não ser relevantes para a avaliação da decisão de adequação. É, portanto, do interesse do CEPD receber esclarecimentos relativamente às medidas de vigilância das entidades governamentais japonesas. A este respeito, tal esclarecimento seria bem-vindo para determinar se os dados objeto de transferência ao abrigo deste quadro de adequação poderiam ser objeto de acesso por parte das autoridades competentes japonesas para efeitos de segurança nacional.

4.2.2 Divulgação voluntária em caso de segurança nacional

222. O projeto de decisão de adequação estabelece que as quatro entidades públicas apenas têm autoridade para recolher informações (eletrónicas) através da divulgação voluntária. De acordo com o projeto de decisão e com o anexo II, existem algumas limitações por motivos regulamentares, o que significa que a recolha de dados se encontra limitada ao necessário para a execução das tarefas pelas entidades.

223. No domínio do direito penal, tal como mencionado na secção relativa à aplicação da lei, apenas é permitida a divulgação voluntária no âmbito de uma investigação criminal, pelo que pressupõe uma suspeita concreta de um crime já cometido. As investigações no domínio da segurança nacional diferem das investigações no domínio da aplicação da lei. O CEPD reconhece que, de acordo com o anexo II, os princípios centrais da «necessidade de investigação» e da «adequação do método» são igualmente aplicáveis no domínio da segurança nacional e devem ser respeitados, tendo devidamente em conta as circunstâncias específicas de cada caso[87]. Lamenta que a aplicação não seja esclarecida, nomeadamente através de uma referência mais aprofundada à jurisprudência. No entanto, o CEPD estabelece que o recurso a este procedimento deve ser proporcionado ou necessário.

224. De acordo com o projeto de decisão, quando a informação pessoal tiver sido recolhida («obtida»), o tratamento é regulado pela APPIHAO, com exceção da polícia provincial[88]. O Anexo II refere que o tratamento de dados pessoais pela polícia provincial é regido por decretos provinciais que estabelecem os princípios para a proteção de dados pessoais, direitos e obrigações equivalentes aos do APPIHAO[89]. Uma vez que não existem traduções em inglês para estes decretos, o CEPD não se encontra em condições de avaliar se os princípios são equivalentes aos do APPIHAO.

225. Para as outras observações relativamente à divulgação voluntária, é feita referência à secção relativa à aplicação da lei.

4.2.3 Supervisão

4.2.3.1 Aspetos gerais

226. As quatro entidades governamentais com poderes para recolher informações eletrónicas detidas por operadores comerciais japoneses por motivos de segurança nacional são: i) o Gabinete de Investigação e Informações (CIRO, *Cabinet Intelligence & Research Office*); ii) o Ministério da Defesa («MD»); iii) a

serão aplicáveis a partir do momento em que é realizada a transferência de dados, o que significa que devem ser incluídos os dados "a caminho" desse país.»

[87] Ver anexo II, pp. 23.

[88] Decisão de adequação, n.os 118 e 157.

[89] Ver anexo II, pp. 3.

polícia (tanto a Agência de Polícia Nacional (NPA, *National Police Agency*)[90] como a polícia provincial); e iv) a Public Security Intelligence Agency («PSIA»).

227. De acordo com o projeto de decisão de adequação, estas entidades públicas estão sujeitas a vários níveis de supervisão por parte de três ramos do governo[91]. O CEPD observa que existe um mecanismo de controlo no âmbito do ramo legislativo (Dieta japonesa) e do poder executivo (Office of Legal Compliance (Gabinete de Conformidade Legal) do Inspetor-geral (OIG), das Comissões Municipais de Segurança Pública e da Comissão de Análise da Segurança Pública). O CEPD salienta que a Comissão deve esclarecer o controlo judicial (*ex officio*/garantia C do GT 237; no que diz respeito à reparação, existe um capítulo separado no projeto de decisão e uma garantia adicional no GT 237) dos órgãos governamentais acima mencionados, uma vez que não é claro se existe tal controlo judicial na área da recolha de dados pessoais para fins de segurança nacional sem meios obrigatórios.

4.2.3.2 Supervisão pela Dieta japonesa

228. O CEPD observa que a Dieta japonesa pode realizar investigações relacionadas com as atividades das autoridades públicas e, por conseguinte, também para todas as entidades governamentais acima mencionadas. Além disso, a dieta pode também solicitar a apresentação de documentos e o depoimento de testemunhas (*Constituição japonesa, artigo 62.º, Lei relativa à Dieta, artigo 104.º*). O CEPD observa também que, de acordo com a *Lei relativa à Dieta, artigos 74.º e 75.º*, os membros da Dieta podem colocar perguntas por escrito ao Gabinete que pode terminar numa resposta do mesmo (*Lei relativa à Dieta, artigo 75.º*). Por último, é de notar também que existem obrigações de comunicação específicas para, por exemplo, a Public Security Intelligence Agency (PSIA) (SAPA, artigo 36.º/ACO, artigo 31.º), através de um relatório anual entregue à Dieta. Este relatório não foi entregue ao CEPD.

4.2.3.3 Controlo pelo Office of Legal Compliance (Gabinete de Conformidade Legal) do Inspetor-geral (OIG)

229. O CEPD observa que existe um organismo de supervisão para o MD designado OIG. O CEPD não recebeu a lei relativa ao estabelecimento do MD (Lei relativa ao estabelecimento do MD), mas sim apenas as representações constantes do anexo II do projeto de decisão. Nos termos do anexo II, o OIG é uma entidade independente no MD, que se encontra sob a supervisão direta do Ministro da Defesa, em conformidade com o artigo 29.º da Lei relativa ao estabelecimento do MD. O OIG tem poderes para efetuar inspeções de cumprimento de leis e regulamentos por funcionários do Ministério da Defesa («Inspeções de Defesa»), em todo o ministério, incluindo as Forças de Autodefesa.

230. Em conformidade com o anexo II, o OIG exerce as suas funções de forma independente dos serviços operacionais do MD. O CEPD observa que o OIG é um organismo de supervisão *interno*.

231. As inspeções deram origem a constatações e, com a intenção de garantir o cumprimento, a medidas diretamente comunicadas ao Ministro da Defesa. Com base no relatório do OIG, o Ministro da Defesa pode emitir ordens de execução das medidas necessárias para corrigir a situação. O Vice-Ministro da Defesa é responsável pela aplicação destas medidas e deve informar o Ministro da Defesa relativamente à situação dessa aplicação.

232. Analisando o anexo II, sem estar previsto nas disposições legais (Lei relativa ao estabelecimento do MD) destas considerações, o CEPD congratula-se com a possibilidade de ordenar as medidas de

[90] No entanto, de acordo com as informações recebidas, o papel principal da NPA consiste em coordenar as investigações realizadas pelos diferentes departamentos da polícia provincial e as suas atividades de recolha de informações limitam-se às trocas com autoridades estrangeiras.
[91] Ver anexo II, pp. 39.

conformidade necessárias para corrigir a situação. No entanto, o CEPD suscita dúvidas quanto à independência do OIG, uma vez que se trata de um gabinete no Ministério da Defesa e está sob a supervisão direta do Ministro da Defesa, nos termos do anexo II (de acordo com o *GT 237, «independência funcional não basta, por si só, para resguardar a referida autoridade de fiscalização de qualquer influência externa»*).

233. Em conformidade com a jurisprudência da CEDH e o *GT 237*, respetivamente, na sequência das considerações do anexo II, o Inspetor-Geral pode solicitar os relatórios do gabinete em questão (documentos, sítios Web, explicações). O CEPD requer clarificação no que diz respeito aos gabinetes em questão serem ou não obrigados a dar seguimento a estes pedidos e se os documentos solicitados incluem ou não materiais fechados, como o *GT 237* faz referência ou não.

234. Embora o CEPD se congratule com o facto de peritos em questões jurídicas superiores (ex-promotor superintendente) liderarem o OIG, afigura-se necessário clarificar as modalidades de nomeação deste organismo de supervisão.

4.2.3.4 Supervisão pela Comissão de Análise da Segurança Pública

235. De acordo com o anexo II (página 25), a PSIA realiza inspeções regulares e especiais às operações das suas agências e gabinetes (Serviços de Informação de Segurança Pública [Public Security Intelligence Bureau], Gabinetes de Informação de Segurança Pública [Public Security Intelligence Offices] e Subgabinetes, etc.). Para efeitos da inspeção regular, um Diretor-Geral Adjunto e/ou um diretor são designados inspetores. Essas inspeções devem abranger igualmente a gestão de dados pessoais.

236. Nos termos do considerando 163 do projeto de decisão, a Comissão de Análise da Segurança Pública funciona como organismo independente de supervisão *ex ante* da PSIA, no que diz respeito às questões da ACO[92] e SAPA[93]. O CEPD congratula-se com esse facto.

237. Embora o sítio Web do Ministério da Justiça japonês forneça algumas informações[94], o CEPD não está em condições de avaliar cuidadosamente a independência da Comissão de Análise da Segurança Pública, uma vez que não lhe foi fornecida a lei relativa à instituição da Comissão de Análise da Segurança Pública[95] e às regras da Comissão de Análise da Segurança Pública[96].

4.2.3.5 Supervisão por parte da Comissão Nacional de Segurança Pública, das Comissões Municipais de Segurança Pública e da APPIHAO (executivo)

238. Ver 3.1.2.2.1 (Comissão Nacional de Segurança Pública), 3.1.2.2.2. (Comissões Municipais de Segurança Pública) e 3.1.2.2.4. (Executivo).

4.2.3.6 Supervisão pela CPP

239. O CEPD convida a Comissão a mencionar, no considerando 164, que a CPP não é um organismo de supervisão para as entidades governamentais acima mencionadas e que apenas é competente para a

---

[92] Lei relativa ao controlo das organizações que tenham cometido atos de assassínio em massa indiscriminados (Lei n.º 147 de 7 de dezembro de 1999).

[93] Lei de prevenção de atividades subversivas (Lei n.º 240 de 21 de julho de 1952).

[94] Consultar http://www.moj.go.jp/ENGLISH/MEOM/meom-01.html (setembro de 2018): o órgão extra-ministerial «*é composto por um presidente e seis membros. São selecionados de entre pessoas com bom caráter e capazes de proferir uma decisão justa no que diz respeito ao controlo de organizações e de pessoas que dispõem de uma vasta experiência tanto em matéria de direito como da sociedade. São nomeados pelo Primeiro-Ministro e devem ser aprovados por ambas as câmaras da Dieta. No que diz respeito à aplicação da legislação anteriormente mencionada (SAPA/ACO), os membros desempenham as suas funções de forma bastante independente, sem qualquer orientação ou controlo por parte do Primeiro-Ministro ou do Ministro da Justiça.*»

[95] http://www.japaneselawtranslation.go.jp/law/detail_main?re=&vm=2&id=613 (setembro de 2018).

[96] Artigo 28.º ACO.

reparação dos indivíduos ou para transferir a passagem no considerando 164 para a secção «reparação individual».

4.2.4 Mecanismo de recurso

240. Para a análise do mecanismo de recurso negociado recentemente, é feita referência à secção relativa à aplicação da lei.

241. Além disso, é de salientar que a legislação japonesa prevê uma via de recurso individual específica disponível no domínio da segurança nacional. O CEPD considera que todos os indivíduos, incluindo os cidadãos da UE, podem, de uma forma geral, pedir a divulgação, a correção (incluindo o apagamento) ou a suspensão da utilização dos órgãos administrativos, também se estes forem tratados para efeitos de segurança nacional. No caso de um pedido desta natureza ser «rejeitado devido ao facto de a informação em causa não ser considerada acessível», pode ser interposto um recurso e consultado o «Comité de Exame da Informação e da Proteção de Informações Pessoais ». O Comité é composto por membros nomeados pelo Primeiro-Ministro com o consentimento de ambas as câmaras, com poderes de investigação, e conclui com um relatório escrito para a pessoa em causa, que não é juridicamente vinculativo, mas quase sempre seguido[97]. De acordo com o anexo II, apenas em dois casos de um total de 2000 casos uma autoridade administrativa adotou uma decisão diferente da conclusão do Comité.[98]

242. Decorre da explicação desde que a revisão não esteja disponível, se a informação pode ser «divulgada», mas o indivíduo não está satisfeito com o resultado. O CEPD reconhece esta possibilidade de recurso, mas gostaria de pedir esclarecimentos adicionais relativamente a este último aspeto, que limitaria significativamente o seu âmbito de aplicação.

O Comité Europeu para a Proteção de Dados

A presidente

(Andrea Jelinek)

[97] Anexo II, p. 25, 26. Ato para a criação do Comité de Exame da Informação e da Proteção de Informações Pessoais, artigos 4.º, 9.º e 11.º.
[98] Anexo II, nota de rodapé 35.