Recomendações 01/2021 sobre os critérios de referência para a adequação no quadro da Diretiva sobre a Proteção de Dados na Aplicação da Lei

Adotadas em 2 de fevereiro de 2021

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 51.º, n.º 1, alínea b), da Diretiva (UE) 2016/680 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas autoridades competentes para efeitos de prevenção, investigação, deteção ou repressão de infrações penais ou execução de sanções penais, e à livre circulação desses dados, e que revoga a Decisão-Quadro 2008/977/JAI do Conselho[1],

Tendo em conta o artigo 12.º e o artigo 22.º do seu Regulamento Interno,

ADOTOU AS SEGUINTES RECOMENDAÇÕES

1. INTRODUÇÃO

1. O Grupo de Trabalho do Artigo 29.º publicou um documento de trabalho[2] relativo aos critérios de referência para a adequação no quadro do Regulamento Geral sobre a Proteção de Dados (RGPD)[3]. Tal documento de trabalho foi aprovado pelo Comité Europeu para a Proteção de Dados (CEPD) na sua primeira sessão plenária.

2. Tal como referido na declaração n.º 21 anexada ao Tratado de Lisboa, atendendo à especificidade dos domínios em causa, poderão ser necessárias disposições específicas sobre proteção de dados pessoais e sobre a livre circulação desses dados, nos domínios da cooperação judiciária em matéria penal e da cooperação policial, com base no artigo 16.º do Tratado sobre o Funcionamento da União Europeia (TFUE).

3. Nesta base, o legislador da UE adotou a Diretiva (UE) 2016/680 (Diretiva sobre a Proteção de Dados na Aplicação da Lei), que estabelece regras específicas no que diz respeito ao tratamento de dados pessoais pelas autoridades competentes para efeitos de **prevenção, investigação, deteção ou repressão de infrações penais ou execução de sanções penais, incluindo a salvaguarda e prevenção de ameaças à segurança pública**.

4. A Diretiva sobre a Proteção de Dados na Aplicação da Lei determina os motivos que permitem a transferência de dados pessoais para um país terceiro ou para uma organização internacional neste contexto. Um dos motivos para tal transferência é a determinação da Comissão Europeia de que o país terceiro ou a organização internacional em causa assegura um nível de proteção adequado.

---

1 JO L 119 de 4.5.2016, p. 89.

2 WP 254 rev.01 adotado pelo Grupo de Trabalho do Artigo 29.º em 28 de novembro de 2017, última redação revista e adotada em 6 de fevereiro de 2018. Atualiza o capítulo I do documento de trabalho «Transferência de dados pessoais para países terceiros: aplicação dos artigos 25.º e 26.º da Diretiva comunitária relativa à proteção dos dados», WP 12, adotado pelo Grupo de Trabalho do Artigo 29.º em 24 de julho de 1998.

3 Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados) (JO L 119 de 4.5.2016, p. 1).

5. Enquanto o documento de trabalho WP 254 rev.01 sobre os critérios de referência para a adequação visa facultar orientações à Comissão Europeia relativas ao nível de proteção de dados em países terceiros e organizações internacionais nos termos do RGPD, o presente documento visa facultar orientações semelhantes nos termos da Diretiva sobre a Proteção de Dados na Aplicação da Lei. Neste contexto, estabelece os princípios centrais da proteção de dados que devem ser incluídos no quadro normativo de um país terceiro ou organização internacional a fim de assegurar uma equivalência substancial em relação ao quadro normativo da UE no âmbito da Diretiva sobre a Proteção de Dados na Aplicação da Lei (ou seja, para o tratamento de dados pessoais pelas autoridades competentes para efeitos de prevenção, investigação, deteção ou repressão de infrações penais ou execução de sanções penais). Além disso, pode servir para orientar os países terceiros e as organizações internacionais interessados em alcançar a adequação.

6. O presente documento centra-se unicamente nas decisões de adequação. Trata-se de atos de execução da Comissão Europeia de acordo com o artigo 36.º, n.º 3, da Diretiva sobre a Proteção de Dados na Aplicação da Lei.

2. CONCEITO DE ADEQUAÇÃO

7. A Diretiva sobre a Proteção de Dados na Aplicação da Lei estabelece as regras para a transferência de dados pessoais para países terceiros e organizações internacionais, na medida em que tais transferências sejam abrangidas pelo seu âmbito. As regras relativas às transferências internacionais de dados pessoais são estabelecidas no capítulo V da Diretiva sobre a Proteção de Dados na Aplicação da Lei, em especial nos seus artigos 35.º a 39.º.

8. Nos termos do artigo 36.º da Diretiva sobre a Proteção de Dados na Aplicação da Lei, as transferências de dados para um país terceiro ou uma organização internacional podem ser efetuadas se um país terceiro, um território ou uma organização internacional, assegurarem um nível de proteção adequado. Decorre da jurisprudência[4] do Tribunal de Justiça da União Europeia (TJUE) que esta disposição deva ser lida à luz do artigo 35.º da Diretiva sobre a Proteção de Dados na Aplicação da Lei, intitulado «Princípios gerais das transferências de dados pessoais», que estabelece que «todas as disposições [do capítulo V da Diretiva sobre a Proteção de Dados na Aplicação da Lei] são aplicadas de forma a assegurar que não fique comprometido o nível de proteção das pessoas singulares assegurado pela presente diretiva».

9. Caso a Comissão Europeia decida que tal nível de proteção adequado está assegurado, as transferências de dados pessoais para esse país terceiro, território, setor ou organização internacional podem ocorrer, sem ser necessário obter qualquer autorização específica, exceto caso outro Estado-Membro do qual os dados foram obtidos tenha de dar a sua autorização para a transferência, tal como estabelecido nos artigos 35.º e 36.º e no considerando 66 da Diretiva sobre a Proteção de Dados na Aplicação da Lei. Tal não prejudica a necessidade, para o tratamento dos dados, de as autoridades dos Estados-Membros em causa cumprirem as disposições nacionais adotadas nos termos da Diretiva (UE) 2016/680.

[4] Processo C-311/18, *Data Protection Commissioner* contra *Facebook Ireland Ltd* e *Maximillian Schrems*, 16 de julho de 2020, ECLI:EU:C:2020:559, n.º 92 (Schrems II).

10. Este conceito de «nível de proteção adequado», que já existia nos termos da Diretiva 95/46/CE[5] e da Decisão-Quadro 2008/977/JAI do Conselho[6], foi desenvolvido pelo TJUE neste contexto e, recentemente, no quadro do RGPD.

11. Tal como especificado pelo TJUE, 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 recorre para assegurar tal nível de proteção possam ser diferentes dos implementados dentro da União», mas «tais meios devem, todavia, revelar-se efetivos, na prática»[7]. Por conseguinte, o padrão de adequação não exige a imitação ponto por ponto da legislação da UE, mas sim o estabelecimento do essencial – os principais requisitos dessa legislação.

12. Neste contexto, o tribunal esclareceu igualmente que a decisão de adequação da Comissão deve conter alguma referência à existência, no país terceiro, de normas adotadas por este país terceiro destinadas a limitar as eventuais ingerências nos direitos fundamentais das pessoas cujos dados pessoais sejam transferidos da União Europeia para este país terceiro, ingerências essas que as autoridades públicas deste país seriam *autorizadas* a praticar quando prosseguem objetivos legítimos, tais como a segurança nacional[8].

13. A finalidade das decisões de adequação da Comissão Europeia é confirmar formalmente, com efeitos vinculativos para os Estados-Membros[9], incluindo para as respetivas autoridades competentes de proteção de dados[10], que o nível de proteção de dados de um país terceiro ou organização internacional é substancialmente equivalente ao nível de proteção de dados da União Europeia. Este deverá dar garantias de assegurar um nível adequado de proteção, essencialmente equivalente ao assegurado na União, em particular quando os dados são tratados num ou em vários setores específicos[11].

14. A adequação pode ser alcançada através de uma combinação de direitos conferidos aos titulares dos dados e de deveres impostos a quem trata os dados ou quem exerce o controlo sobre esse tratamento e supervisão por organismos independentes. Contudo, as normas relativas à proteção de dados só são eficazes se tiverem caráter executório e forem aplicadas na prática. Por conseguinte, é necessário ter em conta não apenas o conteúdo das normas aplicáveis aos dados pessoais transferidos para um país terceiro ou organização internacional, mas também o sistema existente para assegurar a eficácia dessas normas. A existência de mecanismos executórios eficientes é extremamente importante para a eficácia das normas de proteção de dados[12].

---

5 Diretiva 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, JO L 281 de 23.11.1995, p. 31.

6 Decisão-Quadro 2008/977/JAI do Conselho, de 27 de novembro de 2008, relativa à proteção dos dados pessoais tratados no âmbito da cooperação policial e judiciária em matéria penal, JO L 350 de 30.12.2008, p. 60.

7 Processo C−362/14, *Maximillian Schrems* contra *Data Protection Commissioner*, 6 de outubro de 2015, ECLI:EU:C:2015:650, n.os 73 e 74 (*Schrems I*).

8 *Schrems I*, n.º 88.

9 Artigo 288.º, n.º 2, do TFUE.

10 *Schrems I*, n.º 52.

11 Considerando 67 da Diretiva sobre a Proteção de Dados na Aplicação da Lei.

12 *Schrems I*, n.os 72 a 74, e Parecer 1/15 relativo ao projeto de acordo entre o Canadá e a União Europeia, 26 de julho de 2017, ECLI:EU:C:2017:592 (Parecer 1/15), n.º 134: «Este direito à proteção dos dados pessoais exige, nomeadamente, que a continuidade do nível elevado de proteção das liberdades e dos direitos fundamentais conferido pelo direito da União seja assegurada em caso de transferência de dados pessoais da União para um país terceiro. Mesmo que os meios destinados a garantir esse nível de proteção possam ser diferentes dos implementados na União a fim de garantir o respeito dos requisitos decorrentes

3. ASPETOS PROCESSUAIS DAS DECISÕES DE ADEQUAÇÃO NO QUADRO DA DIRETIVA SOBRE A PROTEÇÃO DE DADOS NA APLICAÇÃO DA LEI

15. A fim de cumprir as funções de aconselhamento à Comissão Europeia de acordo com o artigo 51.º, n.º 1, alínea g), da Diretiva sobre a Proteção de Dados na Aplicação da Lei, o CEPD deve receber toda a documentação pertinente, incluindo correspondência pertinente e conclusões formuladas pela Comissão Europeia. É absolutamente necessário que todos os documentos pertinentes sejam traduzidos para inglês e transmitidos com a devida antecedência ao CEPD, a fim de permitir discussões informadas e úteis previamente à adoção final das decisões de adequação. Se o quadro normativo for complexo, importa incluir qualquer relatório preparado sobre o nível de proteção de dados do país terceiro ou organização internacional. Em todo o caso, as informações da Comissão Europeia devem ser exaustivas e permitir que o CEPD possa avaliar a análise realizada pela Comissão sobre o nível de proteção de dados no país terceiro ou na organização internacional.

16. O CEPD emitirá um parecer sobre as conclusões da Comissão Europeia em tempo útil, identificará eventuais insuficiências no âmbito da adequação e apresentará possíveis recomendações, se necessário.

17. De acordo com o artigo 36.º, n.º 4, da Diretiva sobre a Proteção de Dados na Aplicação da Lei, cabe à Comissão Europeia controlar, de forma continuada, os desenvolvimentos que possam prejudicar a aplicação de uma decisão de adequação.

18. O artigo 36.º, n.º 3, da Diretiva sobre a Proteção de Dados na Aplicação da Lei prevê a realização de uma avaliação periódica, no mínimo de quatro em quatro anos. Contudo, trata-se de um intervalo temporal geral que deve ser ajustado a cada país terceiro ou organização internacional com uma decisão de adequação. Dependendo das circunstâncias específicas em causa, pode justificar-se um ciclo de revisão mais curto. Além disso, alguns incidentes ou outras informações ou alterações do quadro normativo do país terceiro ou organização internacional em causa podem levar à necessidade de proceder a uma revisão antes da data prevista. Parece também ser adequado realizar a primeira revisão de uma decisão de adequação totalmente nova bastante cedo e, gradualmente, ajustar o ciclo de revisão em função dos resultados.

19. Atendendo à sua função de dar à Comissão Europeia um parecer quanto ao facto de um país terceiro, um território ou um ou mais setores específicos desse país terceiro, ou uma organização internacional, ter deixado de garantir um nível adequado de proteção, o CEPD deve, oportunamente, receber informações úteis em relação ao seguimento, por parte da Comissão Europeia, dos desenvolvimentos nesse país terceiro ou organização internacional. Como tal, o CEPD deve ser informado de qualquer processo de revisão e missão de revisão no país terceiro ou organização internacional. O CEPD recomenda que seja convidado a participar nestes processos e missões de revisão, tal como foi previsto na decisão do Escudo de Proteção da Privacidade e está previsto na decisão de adequação relativa ao Japão.

20. Deve notar-se igualmente que, de acordo com o artigo 36.º, n.º 5, da Diretiva sobre a Proteção de Dados na Aplicação da Lei, a Comissão Europeia tem o poder, caso o país terceiro ou a organização

do direito da União, esses meios devem, contudo, na prática, ser efetivos, a fim de assegurar uma proteção substancialmente equivalente à garantida na União».

internacional deixe de assegurar um nível de proteção adequado, de revogar, alterar ou suspender as decisões de adequação existentes. O procedimento de revogação, alteração ou suspensão envolve o CEPD, ao solicitar o seu parecer, de acordo com o artigo 51.º, n.º 1, alínea g), da Diretiva sobre a Proteção de Dados na Aplicação da Lei.

21. Além disso, sem prejuízo dos poderes das autoridades responsáveis pela aplicação da lei, as autoridades de controlo deverão ainda dispor do poder de levar as violações à presente diretiva ao conhecimento das autoridades judiciais e de intentar processos judiciais[13]. Em especial, decorre do acórdão *Schrems I* do TJUE que as autoridades de proteção de dados devem poder intervir num processo judicial perante os órgãos jurisdicionais nacionais, se considerarem fundadas as críticas apresentadas por uma pessoa contra uma decisão de adequação[14]. O acórdão *Schrems II* confirmou esta apreciação[15].

4. NORMAS DA UE PARA A ADEQUAÇÃO DA COOPERAÇÃO POLICIAL E JUDICIÁRIA EM MATÉRIA PENAL

22. Quanto à substância, as decisões de adequação devem centrar-se na avaliação da legislação existente do país terceiro em causa no seu todo, em teoria e na prática, à luz dos critérios de avaliação estabelecidos no artigo 36.º da Diretiva sobre a Proteção de Dados na Aplicação da Lei. O sistema de um país terceiro ou de uma organização internacional deve conter os seguintes princípios e mecanismos básicos gerais relativos aos requisitos processuais e de execução em matéria de proteção de dados.

23. O artigo 36.º, n.º 2, da Diretiva sobre a Proteção de Dados na Aplicação da Lei estabelece os elementos que a Comissão Europeia deve ter em conta ao avaliar a adequação do nível de proteção num país terceiro ou organização internacional.

24. Em especial, a Comissão terá em consideração o Estado de direito, o respeito pelos direitos humanos e pelas liberdades fundamentais[16], a legislação pertinente, bem como a execução de tal

---

13 Ver o artigo 47.º, n.º 5, e o considerando 82 da Diretiva sobre a Proteção de Dados na Aplicação da Lei.

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

15 Ver *Schrems II*, n.º 120: «Mesmo perante uma decisão de adequação da Comissão, a autoridade nacional de controlo competente à qual uma pessoa tenha apresentado uma reclamação relativa à proteção dos seus direitos e liberdades no que diz respeito ao tratamento dos seus dados pessoais deve poder examinar, com total independência, se a transferência desses dados respeita as exigências estabelecidas pelo RGPD e, sendo caso disso, intentar uma ação nos órgãos jurisdicionais nacionais para que estes últimos, caso partilhem das dúvidas dessa autoridade quanto à validade da decisão de adequação, procedam a um reenvio prejudicial para efeitos da apreciação dessa validade».

16 Ao avaliar o quadro normativo do país terceiro, deve ser tida em consideração a possibilidade de a pena de morte ou de qualquer forma de tratamento cruel e desumano poder ser imposta com base em dados transferidos da UE. Com efeito, se tal pena ou tratamento forem previstos na legislação do país terceiro, devem ser encontradas garantias adicionais no quadro normativo do país terceiro, a fim de assegurar que os dados transferidos da UE não seriam utilizados para requerer, aplicar ou executar uma pena de morte ou qualquer forma de tratamento cruel e desumano (por exemplo, um acordo internacional que imponha condições a respeito da transferência, um compromisso do país terceiro de não impor a pena de morte ou qualquer forma de tratamento cruel e desumano com base nos dados transferidos da UE, ou uma moratória à pena de morte).

legislação, os direitos efetivos e oponíveis dos titulares dos dados e as vias de recurso eficazes, administrativas e judiciais, dos titulares cujos dados pessoais são transferidos, a existência e o funcionamento eficaz de uma ou várias autoridades de controlo independentes e os compromissos internacionais assumidos pelo país terceiro ou pela organização internacional.

25. Por conseguinte, fica claro que qualquer análise significativa do nível de proteção adequado deve englobar dois elementos básicos: o conteúdo das normas aplicáveis e a forma como é assegurada a sua execução efetiva na prática. Cabe à Comissão Europeia verificar, periodicamente, se as normas vigentes são eficazes na prática.

26. O essencial dos princípios gerais no que toca à proteção de dados e dos requisitos processuais e de execução, que pode ser visto como um requisito mínimo para a proteção de dados ser adequada, advém da Carta dos Direitos Fundamentais da UE (Carta) e da Diretiva sobre a Proteção de Dados na Aplicação da Lei. A existência de disposições gerais de proteção de dados e privacidade no país terceiro não é suficiente. Pelo contrário, o quadro normativo do país terceiro ou organização internacional deve incluir disposições específicas que regulem concretamente o direito à proteção de dados no domínio da aplicação da lei. O país terceiro deve dar garantias para assegurar um nível adequado de proteção essencialmente equivalente ao assegurado na União. Estas disposições devem ter caráter executório.

27. Além disso, no que diz respeito ao princípio da proporcionalidade[17], o TJUE considerou, em relação à legislação dos Estados-Membros, que a possibilidade de justificarem uma limitação aos direitos à privacidade e à proteção de dados deve ser apreciada através da medição da **gravidade da ingerência** que tal limitação implica[18], por um lado, e da verificação de que a **importância do objetivo geral** prosseguido por esta limitação está relacionada com essa gravidade, por outro lado[19].

28. De acordo com a jurisprudência do TJUE, a própria base jurídica que permite ingerências nos direitos fundamentais deve, para satisfazer o princípio da proporcionalidade, definir o alcance da restrição ao exercício do direito em causa[20]. As derrogações à proteção de dados pessoais e as suas restrições devem ocorrer na estrita medida do necessário[21]. Para satisfazer este requisito, para além de prever regras claras e precisas que regulem o alcance e a aplicação da medida em causa, a regulamentação em causa deve impor requisitos mínimos, de modo que as pessoas cujos dados foram transferidos disponham de garantias suficientes que permitam proteger eficazmente os seus dados pessoais contra os riscos de abuso. «Essa regulamentação deve, em especial, indicar em que circunstâncias e em que condições se pode adotar uma medida que preveja o tratamento desses dados, garantindo, assim, que a ingerência se limita ao estritamente necessário. A necessidade de dispor destas garantias é ainda mais importante quando os dados pessoais são sujeitos a um tratamento automatizado[22].»

---

17 Artigo 52.º, n.º 1, da Carta.

18 O tribunal observou, por exemplo, que «a ingerência que comporta a recolha em tempo real de dados que permitam localizar um equipamento terminal afigura-se particularmente grave, uma vez que estes dados fornecem às autoridades nacionais competentes um meio de acompanhamento preciso e permanente das deslocações dos utilizadores dos telefones móveis [...]» (processos apensos C-511/18, C-512/18 e C-520/18, *La Quadrature du Net e o.*, 6 de outubro de 2020, ECLI:EU:C:2020:791, n.º 187, incluindo a jurisprudência citada).

19 *La Quadrature du Net e o.*, n.º 131.

20 *Schrems II*, n.º 180.

21 *Schrems II*, n.º 176, incluindo a jurisprudência citada.

22 *Schrems II*, n.º 176, incluindo a jurisprudência citada.

29. O CEPD adotou recomendações, que identificam as garantias essenciais que refletem a jurisprudência do TJUE e do Tribunal Europeu dos Direitos Humanos (TEDH) no domínio da vigilância, que devem ser encontradas na legislação do país terceiro ao avaliar a ingerência decorrente de tais medidas de vigilância de países terceiros nos direitos dos titulares dos dados, no caso de os dados serem transferidos para esse país terceiro nos termos do RGPD[23]. A fim de avaliar se as condições do artigo 36.º, n.º 2, alínea a), da Diretiva sobre a Proteção de Dados na Aplicação da Lei são preenchidas, o CEPD considera que as garantias estabelecidas nestas recomendações devem ser tidas em conta ao avaliar, nos termos da Diretiva sobre a Proteção de Dados na Aplicação da Lei, a adequação de um país terceiro no domínio da vigilância, tendo em mente condições específicas adicionais no domínio da vigilância, neste contexto.

30. Em relação ao requisito do artigo 36.º, n.º 2, alínea b), o país terceiro deverá não apenas garantir o controlo efetivo e independente da proteção dos dados, mas também estabelecer mecanismos de cooperação com as autoridades de proteção de dados dos Estados-Membros[24].

31. Em relação ao requisito do artigo 36.º, n.º 2, alínea c), além dos compromissos internacionais assumidos pelo país terceiro ou pela organização internacional, deverão igualmente ser tidas em conta as obrigações decorrentes da participação do país terceiro ou da organização internacional nos sistemas multilaterais ou regionais, em especial no que diz respeito à proteção dos dados pessoais, bem como o cumprimento de tais obrigações. Em especial, há que ter em conta a adesão do país terceiro a outros acordos internacionais em matéria de proteção de dados, por exemplo, 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, e respetivo Protocolo Adicional[25] (Convenção 108 e a respetiva versão modernizada, Convenção 108+). Pode ser igualmente tida em conta a conformidade do país terceiro com os princípios consagrados em documentos internacionais, tais como o «*Practical Guide on the use of personal data in the police sector*: *how to protect personal data while combatting crime*» (Guia prático a respeito da utilização de dados pessoais no setor policial: como proteger os dados pessoais ao combater a criminalidade) do Conselho da Europa.

32. Uma decisão de adequação deve assegurar que, por meio da substância dos direitos à privacidade e à proteção dos dados e da sua efetiva execução, controlo e aplicação, o sistema estrangeiro na sua totalidade proporciona o nível de proteção exigido, incluindo para os dados em trânsito para este país terceiro. Tal como sublinhado pelo TJUE no acórdão *Schrems II*, o elevado nível de proteção concedido deve ser igualmente assegurado em caso de transferência de dados pessoais para um país terceiro[26].

33. Finalmente, ao adotar uma decisão de adequação unicamente a respeito de um território ou um setor específico num país terceiro, a Comissão Europeia deverá ter em conta critérios claros e objetivos, tais como atinentes às atividades de tratamento específicas ou ao âmbito das normas jurídicas aplicáveis, bem como a legislação em vigor no país terceiro[27].

A. Princípios gerais e garantias

23 Ver Recomendações 02/2020 do CEPD sobre as garantias essenciais europeias relativas às medidas de vigilância, adotadas em 10 de novembro de 2020.
24 Considerando 67 da Diretiva sobre a Proteção de Dados na Aplicação da Lei.
25 Considerando 68 da Diretiva sobre a Proteção de Dados na Aplicação da Lei.
26 Ver n.º 93.
27 Considerando 67 da Diretiva sobre a Proteção de Dados na Aplicação da Lei.

a) Conceitos

34. Devem existir conceitos básicos em matéria de proteção de dados. Estes não têm de imitar a terminologia da Diretiva sobre a Proteção de Dados na Aplicação da Lei, mas devem refletir e ser coerentes com os conceitos consagrados na legislação europeia em matéria de proteção de dados. A título de exemplo, a Diretiva sobre a Proteção de Dados na Aplicação da Lei inclui os seguintes conceitos importantes: «dados pessoais», «tratamento de dados pessoais», «autoridades competentes», «responsável pelo tratamento», «subcontratante», «destinatário», «dados sensíveis», «exatidão», «definição de perfis», «proteção de dados desde a conceção e por defeito», «autoridade de controlo» e «pseudonimização».

b) Licitude e lealdade do tratamento dos dados pessoais (artigo 4.º, considerando 26)

35. Nos termos do artigo 8,º, n.º 2, da Carta, os dados pessoais devem, nomeadamente, ser objeto de um tratamento «para fins específicos e com o consentimento da pessoa interessada ou com outro fundamento legítimo previsto por lei»[28]. Todavia, no contexto da aplicação da lei, deve notar-se que o exercício das funções de prevenção, investigação, deteção ou repressão de infrações penais conferidas institucionalmente por lei às autoridades competentes permite-lhes exigir que as pessoas singulares cumpram o que lhes é solicitado. Neste caso, o consentimento do titular dos dados não deverá constituir um fundamento jurídico do tratamento de dados pessoais pelas autoridades competentes[29].

36. Esta base jurídica deve prever regras claras e precisas que regulem o alcance e a aplicação das operações de tratamento de dados pertinentes e impor requisitos mínimos[30]. Além disso, o TJUE recordou que esta «regulamentação deve ser vinculativa no direito interno»[31].

37. A fim de ser lícito, o tratamento de dados[32] deverá ser necessário para a execução de uma missão por uma autoridade competente para efeitos de prevenção, investigação, deteção ou repressão de infrações penais ou execução de sanções penais, incluindo as garantias e a prevenção de ameaças à segurança pública[33]. Estes efeitos devem ser previstos no direito nacional.

38. Os dados pessoais devem ser objeto de um tratamento leal. A lealdade de tratamento, que constitui um dos princípios da proteção de dados, é uma noção distinta do direito a um tribunal

---

28 Ver *Schrems II*, n.º 173.

29 O considerando 35 da Diretiva sobre a Proteção de Dados na Aplicação da Lei declara igualmente que «Caso seja obrigado a cumprir uma obrigação legal, o titular dos dados não tem verdadeira liberdade de escolha, pelo que a sua reação não poderá ser considerada uma livre manifestação da sua vontade. Tal não deverá obstar a que os Estados-Membros prevejam por lei a possibilidade de o titular dos dados consentir que os seus dados pessoais sejam tratados para as finalidades previstas na presente diretiva, nomeadamente que sejam efetuados testes de ADN no âmbito de investigações penais ou controlada a sua localização por meio de etiquetas eletrónicas tendo em vista a execução de sanções penais».

30 Ver *Schrems II*, n.º 175 e n.º 180, e Parecer 1/15, n.º 139 e a jurisprudência citada.

31 Ver processo C-623/17, *Privacy International* contra *Secretary of State for Foreign and Commonwealth Affairs e o.*, 6 de outubro de 2020, ECLI:EU:C:2020:790, n.º 68 – Deve ficar igualmente claro que na versão francesa do acórdão, o TJUE utiliza a palavra *réglementation*, que é mais ampla do que unicamente leis do Parlamento.

32 O tratamento de dados pessoais por meios total ou parcialmente automatizados, bem como o tratamento por meios distintos dos meios automatizados de dados pessoais contidos em ficheiros ou a eles destinados.

33 As autoridades competentes são qualquer autoridade pública competente para tais efeitos ou qualquer outro organismo ou entidade autorizados por lei a exercer autoridade pública e poderes públicos para tais efeitos.

imparcial, tal como definido no artigo 47.º da Carta e no artigo 6.º da Convenção Europeia para a Proteção dos Direitos do Homem e das Liberdades Fundamentais (CEDH)[34].

c) O princípio da limitação das finalidades (artigo 4.º)

39. Os efeitos específicos do tratamento deverão ser explícitos e legítimos, e deverão estar determinados no momento da recolha dos dados pessoais[35].

40. Os dados devem ser tratados para uma finalidade determinada, explícita e legítima, para efeitos de prevenção, investigação, deteção ou repressão de infrações penais ou execução de sanções penais[36], nomeadamente a salvaguarda e a prevenção de ameaças à segurança pública no país terceiro, e posteriormente utilizados para qualquer destes efeitos, na medida em tal não seja incompatível com a finalidade original do tratamento (por exemplo, para processos paralelos de execução ou arquivos de interesse público, utilização científica, estatística ou histórica para tais finalidades) e sujeitos a garantias adequadas para os direitos e liberdades dos titulares dos dados. Se os dados pessoais forem tratados, pelo mesmo ou por outro responsável pelo tratamento (autoridade competente[37]), para uma finalidade de prevenção, investigação, deteção ou repressão de infrações penais ou execução de sanções penais que não aquela para a qual foram recolhidos, esse tratamento deverá ser permitido, na condição de que esse tratamento seja autorizado em conformidade com as disposições legais aplicáveis e necessário e proporcionado para a prossecução dessa outra finalidade[38]. Deve ser igualmente tida em conta a existência de um mecanismo que vise informar as autoridades competentes dos Estados-Membros pertinentes a respeito de tal tratamento posterior[39]. Além disso, em qualquer caso, o nível de proteção das pessoas singulares assegurado na União pela Diretiva sobre a Proteção de Dados na Aplicação da Lei deverá continuar a ser garantido, inclusive nos casos em que os dados pessoais são transmitidos a partir do país terceiro para responsáveis pelo tratamento, ou subcontratantes desse país terceiro[40].

d) Condições específicas para o tratamento posterior para outras finalidades (artigo 9.º)

41. No que respeita ao tratamento posterior, ou à divulgação de dados transferidos da UE para outras finalidades que não as de aplicação da lei, tais como finalidades de segurança nacional, deve ser igualmente previsto por lei, necessário e proporcionado. Deve ser igualmente tida em conta a existência de um mecanismo que vise informar as autoridades competentes dos

---

34 Considerando 26 da Diretiva sobre a Proteção de Dados na Aplicação da Lei.

35 Considerando 26 da Diretiva sobre a Proteção de Dados na Aplicação da Lei.

36 Inclui «atividades policiais sem conhecimento prévio de que um incidente constitui ou não uma infração penal. Estas funções podem incluir o exercício da autoridade através de medidas coercivas, tais como as atividades da polícia em manifestações, grandes eventos desportivos e distúrbios. Essas funções incluem também a manutenção da ordem pública enquanto atribuição da polícia ou de outras autoridades de aplicação da lei, quando necessárias para a salvaguarda e prevenção de ameaças à segurança pública e aos interesses fundamentais da sociedade protegidos por lei, e à prática de infrações penais» (considerando 12 da Diretiva sobre a Proteção de Dados na Aplicação da Lei). Deve distinguir-se de uma finalidade de segurança nacional ou de atividades inseridas no âmbito de aplicação do título V, capítulo 2, do Tratado da União Europeia (TUE) (considerando 14 da Diretiva sobre a Proteção de Dados na Aplicação da Lei).

37 Ver nota 33.

38 Considerando 29 da Diretiva sobre a Proteção de Dados na Aplicação da Lei.

39 Tal mecanismo poderia ser, por exemplo, a utilização de códigos de tratamento mutuamente acordados, uma obrigação de notificação nos termos de um instrumento internacional, incluindo eventuais notificações automatizadas, ou outras medidas de transparência semelhantes.

40 Considerando 64 da Diretiva sobre a Proteção de Dados na Aplicação da Lei.

Estados-Membros pertinentes a respeito de tal tratamento posterior[41]. Igualmente neste caso, depois de tratados ou divulgados, os dados devem beneficiar do mesmo nível de proteção que quando foram inicialmente tratados pela autoridade competente que os recebeu.

e) O princípio da minimização dos dados

42. Os dados devem ser adequados, pertinentes e não excessivos relativamente às finalidades para que são tratados. Em especial, deve ser tida em conta a aplicação da proteção de dados desde a conceção e por defeito, tais como campos de introdução limitada (comunicações estruturadas) ou verificações da qualidade automatizadas e não automatizadas.

f) O princípio da exatidão dos dados

43. Os dados devem ser exatos e, se necessário, atualizados. Não obstante, é conveniente aplicar o princípio da exatidão dos dados tendo em conta a natureza e a finalidade do tratamento em causa. Especialmente quando se trata de processos judiciais, as declarações que contêm dados pessoais são baseadas em perceções subjetivas da pessoa singular e nem sempre são verificáveis. Este princípio não deve, portanto, aplicar-se à exatidão da própria declaração, mas simplesmente ao facto de tal declaração ter sido feita[42].

44. Deve assegurar-se que não sejam transmitidos nem disponibilizados dados pessoais incorretos, incompletos ou desatualizados[43] e que sejam previstos procedimentos a fim de retificar ou apagar dados inexatos. Em especial, deve ser tido em conta qualquer sistema de classificação da informação tratada, quanto à fiabilidade da fonte e quanto ao nível de verificação dos factos[44].

g) O princípio da conservação de dados

45. Os dados não devem ser conservados mais tempo do que o necessário para as finalidades para as quais são tratados. Devem ser previstas regras adequadas para o apagamento dos dados pessoais; pode tratar-se de um prazo fixo ou de uma avaliação periódica da necessidade de os conservar (ou uma combinação de ambos: prazo máximo fixo e avaliação periódica, a determinados intervalos)[45]. Os dados pessoais conservados durante prazos mais longos a fim de fazerem parte de arquivos de interesse público ou de serem utilizados para fins científicos, estatísticos ou históricos devem estar sujeitos a garantias adequadas (por exemplo, no que respeita ao acesso)[46].

h) O princípio da segurança e da confidencialidade (artigo 29.º, considerandos 28 e 71)

46. Qualquer entidade que proceda ao tratamento de dados pessoais deve assegurar que os dados são tratados de uma forma que garanta a sua segurança, designadamente ao evitar o acesso a dados pessoais e equipamentos utilizados para o seu tratamento ou a sua utilização por pessoas não autorizadas. Tal inclui a proteção contra o tratamento ilícito, bem como a perda, a destruição e os danos acidentais, por meio da utilização de medidas técnicas e organizativas adequadas para lhes fazer face. Ao determinar o nível de segurança, deve ter-se em conta as técnicas mais avançadas, os custos da sua aplicação, e a natureza, o âmbito, o contexto e as finalidades do

41 Ver nota 39.
42 Considerando 30 da Diretiva sobre a Proteção de Dados na Aplicação da Lei.
43 Considerando 32 da Diretiva sobre a Proteção de Dados na Aplicação da Lei.
44 Por exemplo, grelhas 4x4 para avaliações da fiabilidade e códigos de tratamento.
45 Artigo 5.º da Diretiva sobre a Proteção de Dados na Aplicação da Lei.
46 Considerando 26 da Diretiva sobre a Proteção de Dados na Aplicação da Lei.

tratamento dos dados, bem como o risco decorrente do tratamento para os direitos e liberdades das pessoas singulares, cuja probabilidade e gravidade podem ser variáveis.

47. Devem garantir-se canais seguros de comunicação entre as autoridades dos Estados-Membros que transferem os dados pessoais e as autoridades dos Estados terceiros que os recebem.

i) O princípio da transparência (artigo 13.º, considerandos 26, 39, 42, 43, 44 e 46)

48. As pessoas singulares deverão ser alertadas para os riscos, regras, garantias e direitos associados ao tratamento dos seus dados pessoais e para os meios de que dispõem para exercer os seus direitos relativamente ao tratamento desses dados[47].

49. Devem ser disponibilizadas às pessoas singulares as informações a respeito de todos os principais elementos do tratamento dos seus dados pessoais. Tais informações devem ser de fácil acesso e compreensão, utilizando uma linguagem clara e simples. As referidas informações devem incluir a finalidade do tratamento, a identidade do responsável pelo tratamento de dados, os direitos à sua disposição[48] e outras informações, uma vez que tal é necessário para assegurar a lealdade.

50. Podem existir algumas exceções a este direito à informação. Todavia, tal limitação deve ser permitida por uma medida legislativa e ser necessária e proporcionada, a fim de evitar prejudicar os inquéritos, investigações ou procedimentos oficiais ou judiciais, de evitar prejudicar a prevenção, a investigação, a deteção ou a repressão de infrações penais, ou a execução de sanções penais, de salvaguardar a segurança pública ou a segurança nacional ou ainda de proteger os direitos e as liberdades de terceiros, desde que tal limitação, parcial ou total, constitua uma medida necessária e proporcionada numa sociedade democrática, tendo devidamente em conta os direitos fundamentais e os interesses legítimos da pessoa singular em causa. Tais restrições devem ser igualmente tidas em consideração e avaliadas tendo em conta a possibilidade de apresentar uma reclamação a uma autoridade de controlo ou de procurar uma via de recurso. Em todo o caso, qualquer eventual restrição deve ser temporária e não genérica e deve ser enquadrada por condições, garantias e limitações semelhantes às exigidas nos termos da Carta e do TEDH, tal como interpretadas na jurisprudência do TJUE e pelo TEDH, respetivamente, e, em especial, respeitar a essência desses direitos e liberdades.

j) O direito de acesso, de retificação e de apagamento (artigos 14.º e 16.º)

51. O titular dos dados deve ter o direito de obter a confirmação de que os dados pessoais que lhe digam respeito são ou não objeto de tratamento e, se for esse o caso, de ter acesso a esses dados. Tal direito deve incluir, no mínimo, determinadas informações a respeito do tratamento, tais como as finalidades e o fundamento jurídico do tratamento, o direito de apresentar reclamação à autoridade de controlo e as categorias de dados pessoais em causa[49], o que é particularmente importante no caso de a transparência ser alcançada por meio de uma notificação geral (por exemplo, informações no sítio Web da autoridade).

52. O titular dos dados deve ter o direito de obter a retificação dos seus dados por razões específicas, por exemplo quando estes estiverem incorretos ou incompletos. O titular dos dados deve igualmente ter o direito ao apagamento dos seus dados pessoais quando, por exemplo, o seu tratamento deixar de ser necessário ou for ilícito.

---

47 Considerando 26 da Diretiva sobre a Proteção de Dados na Aplicação da Lei.

48 Tanto os direitos substantivos (direito de acesso, de retificação, etc.) como o direito de recurso.

49 Artigo 14.º da Diretiva sobre a Proteção de Dados na Aplicação da Lei.

53. O exercício desses direitos não deve ser excessivamente complexo para o titular dos dados.

k) Limitações dos direitos dos titulares dos dados

54. Podem existir eventuais limitações a estes direitos, a fim de evitar prejudicar os inquéritos, investigações ou procedimentos oficiais ou judiciais, de evitar prejudicar a prevenção, a investigação, a deteção ou a repressão de infrações penais, ou a execução de sanções penais, de salvaguardar a segurança pública ou a segurança nacional ou ainda de proteger os direitos e as liberdades de terceiros, desde que tal limitação, parcial ou total, constitua uma medida necessária e proporcionada numa sociedade democrática, tendo devidamente em conta os direitos fundamentais e os interesses legítimos da pessoa singular em causa. Tais restrições devem igualmente ser tidas em consideração e avaliadas tendo em conta a possibilidade de apresentar uma reclamação a uma autoridade de controlo ou de intentar uma ação judicial.

l) Limitação relativa a transferências ulteriores (artigo 35.º, considerandos 64 e 65)

55. As transferências ulteriores de dados pessoais pelo destinatário inicial para outro país terceiro ou organização internacional não devem prejudicar o nível de proteção, previsto na União, das pessoas singulares cujos dados são transferidos. Por conseguinte, tais transferências ulteriores de dados devem ser permitidas unicamente se for assegurada a continuidade do nível de proteção conferido pelo direito da UE[50]. Em especial, o destinatário seguinte (ou seja, o destinatário da transferência ulterior) deve ser uma autoridade competente para efeitos de aplicação da lei[51] e tais transferências ulteriores de dados só podem ocorrer para finalidades limitadas e específicas, e desde que existam fundamentos jurídicos para o tratamento em causa.

56. Deve ser igualmente tida em conta a existência de um mecanismo que vise informar as autoridades competentes dos Estados-Membros pertinentes e autorizar tal transferência ulterior de dados. O destinatário inicial dos dados transferidos da UE deve ser responsável e estar em condições de provar que a autoridade competente pertinente do Estado-Membro autorizou a transferência ulterior[52] e que estão previstas garantias adequadas para as transferências ulteriores de dados na ausência de uma decisão de adequação relativa ao país terceiro para o qual os dados seriam ulteriormente transferidos[53].

m) O princípio da responsabilidade (artigo 4.º, n.º 4)

57. O responsável pelo tratamento deve ser responsável pelos princípios da proteção de dados constantes do artigo 4.º da Diretiva sobre a Proteção de Dados na Aplicação da Lei e estar em condições de demonstrar a conformidade com os mesmos.

---

50 Ver também o parecer 1/15.

51 Ver nota 33.

52 Neste contexto, deve ser tida em conta a existência de uma obrigação ou de um compromisso de aplicar os códigos de tratamento pertinentes definidos pelas autoridades dos Estados-Membros que efetuam a transferência.

53 Os requisitos acima referidos não prejudicam as condições específicas para transferências ulteriores para um país adequado, estabelecidas na Diretiva sobre a Proteção de Dados na Aplicação da Lei [artigo 35.º, n.º 1, alíneas c) e e)].

B. Exemplos de princípios adicionais que devem ser aplicados a tipos específicos de tratamento

a) Categorias especiais de dados (artigo 10.º e considerando 37)

58. Devem existir garantias específicas aplicáveis a «categorias especiais de dados»[54] relativas a riscos específicos[55]. Estas categorias devem refletir as que se encontram previstas no artigo 10.º da Diretiva sobre a Proteção de Dados na Aplicação da Lei. O tratamento de categorias especiais de dados deve, por conseguinte, estar sujeito a garantias específicas e ser permitido unicamente quando é estritamente necessário, sob determinadas condições, por exemplo, a fim de proteger o interesse vital de uma pessoa singular.

b) Decisões automatizadas e definição de perfis (artigo 11.º e considerando 38)

59. As decisões baseadas unicamente no tratamento automatizado (decisões individuais automatizadas), incluindo definição de perfis, que produzem efeitos jurídicos adversos ou afetam significativamente o titular dos dados, devem ser tomadas unicamente nas condições fixadas no quadro normativo do país terceiro[56].

60. No quadro da União Europeia, tais condições incluem, por exemplo, informação específica ao titular dos dados e o direito de obter a intervenção humana da parte do responsável pelo tratamento e, em especial, de manifestar o seu ponto de vista, de obter uma explicação sobre a decisão tomada na sequência dessa avaliação ou de contestar a decisão.

61. Em qualquer caso, o direito do país terceiro deve prever as garantias necessárias para os direitos e liberdades do titular dos dados. A este respeito, deve ser igualmente tida em conta a existência de um mecanismo que vise informar as autoridades competentes do Estado-Membro pertinente a respeito de qualquer tratamento posterior, tal como a utilização dos dados transferidos para a definição de perfis em grande escala.

c) Proteção de dados desde a conceção e por defeito (artigo 20.º)

62. Ao avaliar a adequação, deve ser dada atenção à existência da obrigação de os responsáveis pelo tratamento adotarem políticas internas e aplicarem medidas que cumpram os princípios em matéria de proteção de dados desde a conceção e por defeito, tendo em conta as técnicas mais avançadas e os custos da sua aplicação e a natureza, o âmbito, o contexto e as finalidades do tratamento, bem como os riscos de probabilidade e gravidade variáveis que representa para os direitos e liberdades das pessoas singulares, a fim de adotarem, tanto no momento da definição dos meios de tratamento como no momento do próprio tratamento, as medidas técnicas e organizativas — como a pseudonimização — concebidas para aplicar de forma eficaz os princípios da proteção de dados, como a minimização dos dados, e para integrar as garantias necessárias no tratamento.

---

54 Tais categorias especiais são designadas também como «dados sensíveis» no considerando 37 da Diretiva sobre a Proteção de Dados na Aplicação da Lei.

55 Tais garantias adicionais poderiam ser, por exemplo, medidas de segurança específicas, direitos de acesso limitados para o pessoal, limitações a respeito do tratamento posterior, decisões automatizadas, partilha ulterior ou transferências ulteriores.

56 Parecer 1/15, n.º 173.

C. Mecanismos processuais e de aplicação efetiva

63. Embora os meios aos quais o país terceiro recorre para assegurar um nível de proteção adequado possam diferir dos meios empregues na União Europeia[57], um sistema coerente com o europeu deve caracterizar-se pela existência dos seguintes elementos:

a) Autoridade de controlo competente e independente (artigos 36.º, n.º 2, alínea b), e 36.º, n.º 3, e considerando 67)

64. Deve existir uma ou mais autoridades de controlo independentes, responsáveis por assegurar e aplicar a conformidade com as disposições de proteção de dados e privacidade no país terceiro. A autoridade de controlo deve atuar com total independência e imparcialidade quando desempenha as suas funções e exerce os seus poderes, não devendo procurar nem aceitar instruções para o fazer. Nesse contexto, a autoridade de controlo deve ter todos os poderes de aplicação da lei adequados para assegurar eficazmente a conformidade com os direitos ligados à proteção de dados e promover a sensibilização. Importa também ter em conta o pessoal e o orçamento da autoridade de controlo. A autoridade de controlo deve igualmente ter meios para realizar inquéritos por iniciativa própria. Deve igualmente ser responsável por prestar assistência e aconselhamento aos titulares dos dados no exercício dos seus direitos (ver também o ponto c) abaixo). As decisões de adequação devem identificar, se aplicável, a autoridade ou as autoridades de controlo e os mecanismos de cooperação com as autoridades de controlo dos Estados-Membros para a aplicação das regras em matéria de proteção de dados.

b) Aplicação eficaz das regras relativas à proteção de dados

65. O sistema do país terceiro deve assegurar um nível elevado de sensibilização entre os responsáveis pelo tratamento e aqueles que tratam dados pessoais em seu nome em relação aos seus deveres, funções e responsabilidades, bem como entre os titulares dos dados em relação aos seus direitos e aos modos de exercício desses direitos. A existência de sanções efetivas e dissuasivas é uma forma importante de assegurar o cumprimento das normas, assim como os sistemas de controlo direto por autoridades, auditores ou funcionários independentes encarregados da proteção de dados.

66. O quadro de proteção de dados do país terceiro deve obrigar os responsáveis pelo tratamento dos dados ou aqueles que tratam dados pessoais em seu nome a cumprir esse mesmo quadro e conseguir comprovar esse cumprimento, em especial junto da autoridade de controlo competente. Tais medidas devem incluir a conservação de registos ou arquivos das operações de tratamento de dados durante um prazo adequado. Podem incluir igualmente, por exemplo, a avaliação de impacto sobre a proteção de dados, a designação de um responsável pela proteção de dados ou a proteção de dados desde a conceção e por defeito.

c) O sistema de proteção de dados deve facilitar o exercício dos direitos do titular dos dados (artigos 12.º, 17.º e 46.º da Diretiva sobre a Proteção de Dados na Aplicação da Lei)

67. O quadro de proteção de dados do país terceiro deve obrigar os responsáveis pelo tratamento dos dados a facilitar o exercício dos direitos do titular dos dados nos termos da secção A, ponto j), *supra* e prever que a respetiva autoridade de controlo, se lhe for solicitado, preste informações a qualquer titular de dados sobre o exercício dos seus direitos[58].

---

57 *Schrems I*, n.º 74.

58 O exercício dos direitos dos titulares dos dados pode ser direto ou indireto.

d) O sistema de proteção de dados deve prever mecanismos de recurso adequados

68. Embora atualmente não exista jurisprudência a respeito da adequação do sistema jurídico de um país terceiro nos termos da Diretiva sobre a Proteção de Dados na Aplicação da Lei, o TJUE interpretou o direito fundamental à tutela judicial efetiva como consagrado no artigo 47.º da Carta. O primeiro parágrafo do artigo 47.º da Carta exige que qualquer pessoa cujos direitos e liberdades garantidos pelo direito da União Europeia tenham sido violados tenha direito a uma ação perante um tribunal[59] nos termos previstos no referido artigo.

69. De acordo com a jurisprudência consagrada do TJUE, a própria existência de uma fiscalização jurisdicional efetiva destinada a assegurar o cumprimento das disposições do direito da União é inerente à existência de um Estado de direito. Assim, uma regulamentação que não preveja nenhuma possibilidade de o particular recorrer a medidas jurídicas corretivas eficazes para ter acesso aos dados pessoais que lhe dizem respeito, ou para obter a retificação ou a supressão de tais dados, não respeita o conteúdo essencial do direito fundamental a uma proteção jurisdicional efetiva[60].

70. As pessoas singulares devem ter acesso a vias de recurso para fazer valer os seus direitos rápida e eficazmente, e sem custos proibitivos, bem como assegurar a conformidade.

71. Para tal, devem existir mecanismos de controlo que permitam a realização de investigações independentes acerca das reclamações e a identificação e punição de quaisquer violações do direito à proteção de dados e respeito pela vida privada.

72. Se as regras não forem cumpridas, o titular dos dados cujos dados pessoais são transferidos para o país terceiro deve também dispor de vias de recurso eficazes, administrativas e judiciais no país terceiro, incluindo indemnizações em resultado do tratamento ilícito dos seus dados pessoais. Trata-se de um elemento crucial, que pressupõe um sistema de apreciação independente ou de arbitragem, que possa decidir a atribuição de uma indemnização e a eventual aplicação de sanções.

59 O TJUE considera que uma tutela judicial efetiva pode ser assegurada não apenas por um tribunal, mas também por um órgão que ofereça garantias substancialmente equivalentes às exigidas no artigo 47.º da Carta (ver *Schrems II*, n.º 197). Tal pode ser pertinente em especial para organizações internacionais.

60 Schrems II, n.os 187 e 194, incluindo a jurisprudência citada.