Recomendações

Recomendações 02/2020 sobre as garantias essenciais europeias relativas às medidas de vigilância

Adotadas em 10 de novembro de 2020

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

Índice

1. INTRODUÇÃO 4
2. INGERÊNCIAS NOS DIREITOS FUNDAMENTAIS 6
3. GARANTIAS ESSENCIAIS EUROPEIAS 8
Garantia A – O tratamento deve basear-se em regras claras, precisas e acessíveis 9
Garantia B – É necessário demonstrar a necessidade e a proporcionalidade em relação aos objetivos legítimos prosseguidos 10
Garantia C – Mecanismo de supervisão independente 12
Garantia D – É necessário que as pessoas disponham de vias de recurso eficazes 13
4. OBSERVAÇÕES FINAIS 15

O Comité Europeu para a Proteção de Dados,

Tendo em conta o artigo 70.º, n.º 1, alínea e), 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 designado por «RGPD»)[1],

Tendo em conta o Acordo EEE e, nomeadamente, os seus Anexo XI e Protocolo 37, com a redação que lhe foi dada pela Decisão n.º 154/2018 do Comité Misto do EEE, de 6 de julho de 2018[2],

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

Tendo em conta o documento de trabalho do Grupo de Trabalho do Artigo 29.º sobre a justificação das ingerências nos direitos fundamentais à privacidade e à proteção de dados través de medidas de vigilância aquando da transferência de dados pessoais (garantias essenciais europeias, a seguir designadas por «GEE»), WP237,

ADOTOU AS SEGUINTES RECOMENDAÇÕES:

1. INTRODUÇÃO

1. Na sequência do acórdão Schrems I, as autoridades de proteção de dados da UE reunidas no Grupo de Trabalho 29 recorreram à jurisprudência para identificar as garantias essenciais europeias, que devem ser respeitadas para garantir que as ingerências nos direitos à privacidade e à proteção dos dados pessoais através de medidas de vigilância aquando da transferência de dados pessoais não ultrapassam o que é necessário e proporcionado numa sociedade democrática.

2. O CEPD gostaria de salientar que as garantias essenciais europeias se baseiam na jurisprudência do Tribunal de Justiça da União Europeia (a seguir designado por «TJUE») relativa aos artigos 7.º, 8.º, 47.º e 52.º da Carta dos Direitos Fundamentais da UE (a seguir designada por «Carta») e, se for caso disso, na jurisprudência do Tribunal Europeu dos Direitos do Homem (a seguir designado por «TEDH») relativa ao artigo 8.º da Convenção Europeia dos Direitos do Homem (a seguir designada por «CEDH») sobre questões de vigilância nos Estados partes na CEDH[3].

[1] O presente documento não contempla situações de transferências ou partilhas ulteriores que estejam abrangidas pelo âmbito da Diretiva sobre a Proteção de Dados na Aplicação da Lei [Diretiva (UE) 2016/680].

[2] As referências a «Estados membros» no presente documento devem ser entendidas como referências a «Estados membros do EEE».

[3] Nas presentes recomendações, o termo «direitos fundamentais» é derivado da Carta dos Direitos Fundamentais da UE. No entanto, é também utilizado para abranger os «direitos humanos» na aceção da Convenção Europeia dos Direitos do Homem.

3. A atualização do presente documento pretende promover o desenvolvimento das garantias essenciais europeias originalmente concebidas em resposta ao acórdão Schrems I [4], refletindo os esclarecimentos prestados pelo TJUE (e pelo TEDH) desde a sua publicação inicial, em especial no seu acórdão de referência Schrems II[5].

4. No seu acórdão Schrems II, o TJUE declarou que o exame da Decisão 2010/87/UE da Comissão, relativa a cláusulas contratuais-tipo aplicáveis à transferência de dados pessoais para subcontratantes estabelecidos em países terceiros nos termos da Diretiva, à luz dos artigos 7.º, 8.º e 47.º da Carta, não revelou nenhum elemento suscetível de afetar a validade dessa decisão, mas declarou inválida a Decisão BPD, relativa ao Escudo de Proteção da Privacidade. O TJUE considerou que a Decisão BPD era incompatível com o artigo 45.º, n.º 1, do RGPD, à luz dos artigos 7.º, 8.º e 47.º da Carta. O acórdão pode, assim, servir de exemplo quando as medidas de vigilância num país terceiro (neste caso, a secção 702 da FISA e o Decreto Executivo n.º 12 333 dos EUA) não são suficientemente limitadas nem criam um recurso efetivo à disposição dos titulares de dados para fazerem valer os seus direitos, conforme exigido pela legislação da UE para considerar que o nível de proteção num país terceiro é «essencialmente equivalente» ao assegurado na União Europeia, na aceção do artigo 45.º, n.º 1, do RGPD.

5. As razões para a declaração de invalidade do Escudo de Proteção também têm implicações para outros instrumentos [6]de transferência. Embora o Tribunal de Justiça tenha interpretado o artigo 46.º, n.º 1, do RGPD no contexto da validade das cláusulas contratuais-tipo (a seguir designadas por CCT), a sua interpretação aplica-se a qualquer transferência para países terceiros que se baseie em qualquer dos instrumentos referidos no artigo 46.º do RGPD [7].

6. Em última análise, incumbe ao TJUE avaliar se as ingerências num direito fundamental podem ser justificadas. No entanto, na ausência de tal acórdão e em aplicação da jurisprudência assente, as autoridades de proteção de dados são obrigadas a apreciar os casos individuais, quer oficiosamente, quer na sequência de uma queixa, e a remeter o caso para um tribunal nacional, se suspeitarem que a transferência não cumpre o disposto no artigo 45.º, quando existe uma decisão de adequação, ou a suspender ou proibir a transferência, se considerarem que o artigo 46.º do RGPD não pode ser respeitado e que a proteção dos dados transferidos exigida pela legislação da UE não pode ser assegurada por outros meios.

7. O objetivo das garantias essenciais europeias atualizadas é fornecer elementos para verificar se as medidas de vigilância que permitem o acesso a dados pessoais pelas autoridades públicas de um país terceiro, quer sejam agências de segurança nacional ou autoridades competentes para a aplicação da lei, podem ou não ser consideradas como uma ingerência justificável.

8. Com efeito, as garantias essenciais europeias fazem parte da avaliação a realizar para determinar se um país terceiro proporciona um nível de proteção essencialmente equivalente ao garantido na UE, mas não têm por objetivo, por si só, definir todos os elementos que são necessários para considerar que um

[4] Acórdão do TJUE, de 6 de outubro de 2015, Maximillian Schrems c. Data Protection Commissioner, C-362/14, UE:C:2015:650 (a seguir designado por acórdão Schrems I).

[5] Acórdão do TJUE de 16 de julho de 2020, Data Protection Commissioner c. Facebook Ireland Ltd e Maximillian Schrems, C-311/18, ECLI:EU:C:2020:559 (a seguir designado por acórdão Schrems II).

[6] Ver n.º 105 do acórdão Schrems II.

[7] Ver n.º 92 do acórdão Schrems II.

país terceiro proporciona esse nível de proteção em conformidade com o artigo 45.º do RGPD. Do mesmo modo, tão pouco têm por objetivo, por si só, definir todos os elementos que possam ser necessários para avaliar se o regime jurídico de um país terceiro impede o exportador de dados e o importador de dados de assegurarem salvaguardas adequadas, em conformidade com o artigo 46.º do RGPD.

9. Por conseguinte, os elementos apresentados no presente documento devem ser vistos como as garantias essenciais que devem ser encontradas no país terceiro ao avaliar a ingerência decorrente das medidas de vigilância de um país terceiro nos direitos à privacidade e à proteção de dados, em vez de como uma lista de elementos que demonstram que o regime jurídico de um país terceiro, no seu todo, proporciona um nível de proteção essencialmente equivalente.

10. O artigo 6.º, n.º 3, do Tratado da União Europeia estabelece que os direitos fundamentais consagrados na CEDH fazem parte, enquanto princípios gerais, do direito da União. No entanto, tal como o TJUE recorda na sua jurisprudência, esta não constitui, enquanto a União Europeia não lhe aderir, um instrumento jurídico formalmente integrado na ordem jurídica da União [8]. Assim, o nível de proteção dos direitos fundamentais exigido pelo artigo 46.º, n.º 1, do RGPD deve ser determinado com base nas disposições desse regulamento, lidas à luz dos direitos fundamentais consagrados na Carta. Dito isto, nos termos do artigo 52.º, n.º 3, da Carta, os direitos nela contidos que correspondam aos direitos garantidos pela CEDH têm o mesmo sentido e âmbito que os conferidos por essa Convenção e, por conseguinte, tal como recordado pelo TJUE, a jurisprudência do TEDH relativa aos direitos que também estão previstos na Carta dos Direitos Fundamentais da UE deve ser tida em conta como limiar mínimo de proteção para interpretar os direitos correspondentes na Carta[9]. No entanto, nos termos do último período do artigo 52.º, n.º 3, da Carta, «[e]sta disposição não obsta a que o direito da União confira uma proteção mais ampla».

11. Por conseguinte, o conteúdo das garantias essenciais continuará a basear-se parcialmente na jurisprudência do TEDH, na medida em que a Carta, tal como interpretada pelo TJUE, não prevê um nível de proteção mais elevado que prescreva requisitos diferentes dos estabelecidos na jurisprudência do TEDH.

12. O presente documento explica os antecedentes e descreve mais pormenorizadamente as quatro garantias essenciais europeias.

2. INGERÊNCIAS NOS DIREITOS FUNDAMENTAIS

13. Os direitos fundamentais ao respeito pela vida privada e familiar, incluindo as comunicações, e à proteção dos dados pessoais estão consagrados nos artigos 7.º e 8.º da Carta e aplicam-se a todas as pessoas. Além disso, o artigo 8.º estabelece condições para a licitude do tratamento dos dados pessoais, reconhece o direito de acesso e retificação, e impõe que essas regras estejam sujeitas a fiscalização por parte de uma autoridade independente.

[8] Ver n.º 98 do acórdão Schrems II.

[9] Ver n.º 124 do acórdão C-511/18, C-512/18 e C-520/18, La Quadrature du Net e o. (a seguir designado por acórdão La Quadrature du Net e o.).

14. «[A] operação que consiste na transferência de dados pessoais de um Estado-Membro para um país terceiro constitui, enquanto tal, um tratamento de dados pessoais»[10]. Assim, os artigos 7.º e 8.º da Carta aplicam-se a esta operação específica e a sua proteção abrange os dados transferidos, razão pela qual as pessoas cujos dados pessoais são transferidos para um país terceiro devem beneficiar de um nível de proteção substancialmente equivalente ao garantido na União Europeia[11].

15. Segundo o TJUE, quando o direito fundamental ao respeito da vida privada consagrado no artigo 7.º da Carta é afetado, por meio do tratamento de dados pessoais, o direito à proteção de dados é igualmente afetado, uma vez que esse tratamento é abrangido pelo âmbito de aplicação do artigo 8.º da Carta e, por conseguinte, deve necessariamente respeitar as exigências de proteção de dados previstas no referido artigo[12].

16. Por conseguinte, no que se refere a uma eventual ingerência nos direitos fundamentais consignados no direito da União, a obrigação imposta aos prestadores de serviços de comunicações eletrónicas de conservarem os dados de tráfego para, se for caso disso, os disponibilizarem às autoridades nacionais competentes coloca questões relativas ao respeito dos artigos 7.º e 8.º da Carta[13].. O mesmo se aplica relativamente a outros tipos de tratamento de dados, como a transmissão de dados a pessoas distintas dos utilizadores ou o acesso a esses dados tendo em vista a sua utilização[14], o que implica, portanto, uma ingerência nesses direitos fundamentais. Além disso, de acordo com a jurisprudência constante, o acesso aos dados por uma autoridade pública constitui uma ingerência suplementar[15].

17. Para detetar uma ingerência, não importa «se as informações relativas à vida privada em questão têm ou não caráter sensível, ou se os interessados sofreram ou não eventuais inconvenientes em razão dessa ingerência»[16]. O TJUE sublinhou igualmente que é irrelevante o facto de os dados conservados serem ou não objeto de utilização ulterior[17].

18. Todavia, os direitos consagrados nos artigos 7.º e 8.º da Carta não são prerrogativas absolutas, antes devendo ser tomados em consideração relativamente à sua função na sociedade[18].

19. A Carta inclui um teste da necessidade e da proporcionalidade para enquadrar as restrições aos direitos que protege. O artigo 52.º, n.º 1, da Carta especifica o âmbito de eventuais restrições aos artigos 7.º e 8.º, ao estabelecer que «qualquer limitação ao exercício dos direitos e liberdades reconhecidos pela presente Carta deve ser prevista por lei e respeitar a essência desses direitos e liberdades. Na observância do princípio da proporcionalidade, essas restrições só podem ser introduzidas se forem necessárias e corresponderem efetivamente a objetivos de interesse geral reconhecidos pela União, ou à necessidade de proteção dos direitos e liberdades de terceiros.»

[10] Acórdão do TJUE, Schrems II, n.º 83.
[11] Acórdão do TJUE, Schrems II, n.º 96.
[12] Acórdão do TJUE, Schrems II, n.ºs 170 e 171.
[13] Acórdão do TJUE, C-623/17, Privacy International (a seguir designado por acórdão Privacy International), n.º 60.
[14] Acórdão do TJUE, Privacy International, n.º 61.
[15] Acórdãos do TEDH, Leander, n.º 48; Rotaru, n.º 46; acórdão do TJUE, Digital Rights Ireland, n.º 35.
[16] Acórdão do TJUE, Schrems II, n.º 171, incluindo a jurisprudência citada.
[17] Acórdão do TJUE, Schrems II, n.º 171, incluindo a jurisprudência citada.
[18] Acórdão do TJUE, Privacy International, n.º 63.

20. O TJUE reiterou que a legislação da UE que envolva uma ingerência nos direitos fundamentais garantidos pelos artigos 7.º e 8.º da Carta «deve prever normas claras e precisas que regulem o âmbito e a aplicação da medida em causa e impor requisitos mínimos, de modo que as pessoas cujos dados foram conservados disponham de garantias suficientes que permitam proteger eficazmente os seus dados pessoais contra os riscos de abuso», em especial quando os dados pessoais são submetidos a um tratamento automatizado e «quando existe um risco significativo de acesso ilícito a tais dados»[19].

21. De acordo com o TJUE, a proteção do direito à privacidade exige que as derrogações e restrições ao direito à proteção de dados «ocorram na estrita medida do necessário». Além disso, um objetivo de interesse geral deve ser conciliado com os direitos fundamentais abrangidos pela medida, «efetuando uma ponderação equilibrada» entre esse objetivo e os direitos em causa[20].

22. Por conseguinte, o acesso, a conservação e a posterior utilização de dados pessoais pelas autoridades públicas no âmbito das medidas de vigilância não podem exceder os limites do estritamente necessário, avaliados à luz da Carta, caso contrário «não pode[m] ser considerad[os] justificad[os], numa sociedade democrática»[21].

23. As quatro garantias essenciais europeias, tal como são desenvolvidas no próximo capítulo, pretendem especificar mais aprofundadamente a forma de avaliar o nível de ingerência nos direitos fundamentais à privacidade e à proteção de dados no contexto das medidas de vigilância por parte das autoridades públicas de um país terceiro, aquando da transferência de dados pessoais, e quais os requisitos legais que devem, por conseguinte, ser aplicados para avaliar se tais ingerências seriam aceitáveis nos termos da Carta.

3. GARANTIAS ESSENCIAIS EUROPEIAS

24. Na sequência da análise da jurisprudência, o CEPD considera que os requisitos legais aplicáveis para justificar as restrições à proteção de dados e aos direitos à privacidade reconhecidos pela Carta podem ser resumidos em quatro garantias essenciais europeias:

A. O tratamento deve basear-se em regras claras, precisas e acessíveis
B. É necessário demonstrar a necessidade e a proporcionalidade em relação aos objetivos legítimos prosseguidos
C. Deve existir um mecanismo de supervisão independente
D. É necessário que os indivíduos disponham de vias de recurso eficazes

25. As garantias baseiam-se nos direitos fundamentais à privacidade e à proteção de dados que se aplicam a todas as pessoas, independentemente da sua nacionalidade.

[19] Acórdão do TJUE, Privacy International, n.º 68 e jurisprudência citada.
[20] Acórdão do TJUE, Privacy International, n.º 68 e jurisprudência citada.
[21] Acórdão do TJUE, Privacy International, n.º 81.

Garantia A – O tratamento deve basear-se em regras claras, precisas e acessíveis

26. Nos termos do artigo 8.º, n.º 2, da Carta, os dados pessoais devem, nomeadamente, ser tratados «para fins específicos e com o consentimento da pessoa interessada ou com outro fundamento legítimo previsto por lei»[22], conforme recordou o TJUE no acórdão Schrems II. De acordo com o artigo 52.º, n.º 1, da Carta, qualquer restrição ao exercício dos direitos e liberdades reconhecidos pela Carta deve ser prevista por lei. Deste modo, uma ingerência justificável tem de estar em conformidade com a lei.

27. Esta base jurídica deve estabelecer regras claras e precisas sobre o âmbito e a aplicação da medida em questão, e impor salvaguardas mínimas[23]. Além disso, o Tribunal recordou que «[a] regulamentação deve ser vinculativa no direito interno»[24]. A este respeito, o TJUE esclareceu que a avaliação da legislação aplicável de países terceiros deve centrar-se na possibilidade de ser invocada pelos indivíduos perante um tribunal[25]. O Tribunal de Justiça refere, portanto, que os direitos conferidos aos titulares dos dados são por estes oponíveis; nos casos em que não são conferidos às pessoas direitos oponíveis contra as autoridades públicas, o nível de proteção concedido não pode ser considerado essencialmente equivalente ao que resulta da Carta, contrariamente ao requisito previsto no artigo 45.º, n.º 2, alínea a), do RGPD[26].

28. Além disso, o Tribunal de Justiça salientou que a lei aplicável deve indicar em que circunstâncias e sob que condições pode ser adotada uma medida que preveja o tratamento de tais dados[27] (ver adiante, no tocante à Garantia B, a relação entre estes requisitos e os princípios da necessidade e da proporcionalidade).

29. Além disso, o TJUE referiu também que «a exigência segundo a qual qualquer limitação ao exercício de direitos fundamentais deve ser prevista por lei implica que a própria base jurídica que permite a ingerência nesses direitos deve definir o alcance da limitação do exercício do direito em causa»[28].

30. Por último, o Tribunal Europeu dos Direitos do Homem «não considera que exista qualquer motivo para aplicar diferentes princípios quanto à acessibilidade e clareza das regras que regem, por um lado, a interceção de comunicações individuais e, por outro, os programas de vigilância mais gerais»[29]. O TEDH esclareceu igualmente que a base jurídica deveria incluir, pelo menos, uma definição das categorias de pessoas que podem ser sujeitas a vigilância, um limite de duração da medida, o procedimento a seguir para o exame, utilização e armazenamento dos dados obtidos, e as precauções a tomar na comunicação dos dados a outras partes[30].

---

[22] Ver n.º 173 do acórdão Schrems II.

[23] Ver n.º 175 e n.º 180 do acórdão Schrems II, e Parecer 1/15 do Tribunal de Justiça (acordo PNR UE-Canadá), de 26 de julho de 2017, n.º 139 e jurisprudência citada.

[24] Ver n.º 68 do acórdão Privacy International. Deve também ficar claro que, na versão francesa do acórdão, o Tribunal de Justiça utiliza a palavra «réglementation», que abrange mais do que apenas os atos do parlamento.

[25] Ver n.º 181 do acórdão Schrems II (neste número, o TJUE faz referência à Presidential Policy Directive 28 dos EUA).

[26] Ver n.º 181 do acórdão Schrems II.

[27] Ver n.º 68 do acórdão Privacy International, em relação ao direito dos Estados membros.

[28] Ver acórdão Schrems II, n.º 175 e jurisprudência citada, bem como acórdão Privacy International, n.º 65.

[29] Acórdão do TEDH, Liberty, n.º 63.

[30] Acórdão do TEDH, Weber e Saravia, n.º 95.

31. Por último, a ingerência deve ser previsível quanto ao seu efeito para o indivíduo, a fim de lhe proporcionar uma proteção adequada e eficaz contra as ingerências arbitrárias e o risco de abuso. Por conseguinte, o tratamento deve assentar numa base jurídica precisa, clara, mas também acessível (ou seja, pública)[31]. O TEDH, relativamente a esta questão, recordou no processo Zakharov que «a referência à "previsibilidade" no contexto da interceção de comunicações não pode ser a mesma que em muitos outros domínios». Especificou que, no contexto de medidas secretas de vigilância, como a interceção de comunicações, «a previsibilidade não pode significar que um indivíduo seja capaz de prever quando será provável que as autoridades intercetem as suas comunicações para que possa adaptar a sua conduta em conformidade». No entanto, considerando que neste tipo de situações os riscos de arbitrariedade são evidentes, «é essencial dispor de regras claras e pormenorizadas sobre a interceção das comunicações telefónicas, especialmente porque a tecnologia que pode ser utilizada está a tornar-se cada vez mais sofisticada. A legislação nacional deve ser suficientemente clara para proporcionar aos cidadãos uma indicação adequada das circunstâncias e das condições em que as autoridades públicas têm o direito de recorrer a tais medidas»[32].

Garantia B – É necessário demonstrar a necessidade e a proporcionalidade em relação aos objetivos legítimos prosseguidos

32. Nos termos do artigo 52.º, n.º 1, primeiro período, da Carta, qualquer restrição ao exercício dos direitos e liberdades reconhecidos pela Carta deve respeitar o conteúdo essencial desses direitos e liberdades. Nos termos do segundo período do n.º 1 do artigo 52.º da Carta, na observância do princípio da proporcionalidade, essas restrições só podem ser aplicadas a tais direitos e liberdades se forem necessárias e corresponderem efetivamente a objetivos de interesse geral reconhecidos pela União, ou à necessidade de proteção dos direitos e liberdades de terceiros[33].

33. No que se refere ao **principio da proporcionalidade**, o Tribunal de Justiça considerou, em relação à legislação dos Estados membros, que a questão de saber se uma restrição dos direitos à vida privada e à proteção de dados pode ser justificada deve ser avaliada, por um lado, através da avaliação da **gravidade da ingerência** inerente a essa restrição[34] e, por outro, através da verificação de que a **importância do objetivo de interesse público** prosseguido pela referida restrição é proporcional a essa gravidade [35].

34. No acórdão La Quadrature du Net e o., pode observar-se que o TJUE decidiu, em relação à legislação de um Estado-Membro e não de um país terceiro, que o objetivo de salvaguardar a segurança nacional é, devido à sua importância, capaz de justificar medidas que impliquem ingerências mais graves nos direitos fundamentais do que aquelas que poderiam ser justificadas por outros objetivos, como o

[31] Acórdão do TEDH, Malone, n.ºs 65 e 66.

[32] Acórdão do TEDH, Zakharov, n.º 229.

[33] Acórdão Schrems II, n.º 174.

[34] Neste contexto, o Tribunal de Justiça salientou, por exemplo, que «a ingerência resultante da recolha de dados em tempo real que permite a localização dos equipamentos terminais parece ser particularmente grave, uma vez que esses dados fornecem às autoridades nacionais competentes um meio para acompanhar de forma precisa e permanente os movimentos dos utilizadores de telefones móveis [...].» (Acórdão La Quadrature du Net e o., n.º 187, incluindo a jurisprudência citada).

[35] Acórdão La Quadrature du Net e o., n.º 131.

combate à criminalidade. Concluiu, porém, que isso se verifica enquanto existirem motivos suficientemente sólidos para considerar que o Estado em causa se vê confrontado com uma ameaça grave à segurança nacional que se revela genuína, atual ou previsível e que está sujeito ao cumprimento dos outros requisitos estabelecidos no artigo 52.º, n.º 1, da Carta[36].

35. A este respeito, de acordo com a jurisprudência constante do Tribunal de Justiça, as derrogações à proteção de dados pessoais e as suas limitações devem ocorrer na estrita medida do necessário[37]. Para satisfazer este requisito, além de prever regras claras e precisas sobre o alcance e a aplicação da medida em causa, a legislação em questão deve impor salvaguardas mínimas, de modo a que as pessoas cujos dados foram transferidos tenham garantias suficientes de proteção eficaz dos seus dados pessoais contra o risco 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 limite ao estritamente necessário. A necessidade de dispor destas garantias é ainda mais importante quando os dados pessoais são sujeitos a um tratamento automatizado»[38].

36. No acórdão Schrems II, o TJUE salientou que a legislação de um país terceiro que não revela de forma alguma a existência de limitações ao poder que confere com vista à execução dos programas de vigilância para efeitos de obtenção de informações externas não pode garantir um nível de proteção essencialmente equivalente ao garantido pela Carta. Com efeito, segundo a jurisprudência, a própria base jurídica que permite ingerências nos direitos fundamentais deve, para satisfazer o princípio da proporcionalidade, definir o alcance da limitação do exercício do direito em causa[39].

37. No que se refere ao **princípio da necessidade**, o TJUE deixou claro que as legislações que «autoriza[m] de modo generalizado a conservação da totalidade dos dados pessoais de todas as pessoas cujos dados foram transferidos da União [...] sem qualquer diferenciação, limitação ou exceção em função do objetivo prosseguido e sem que esteja previsto um critério objetivo que permita delimitar o acesso das autoridades públicas aos dados e a sua utilização posterior para fins precisos, estritamente limitados e suscetíveis de justificar a ingerência que tanto o acesso como a utilização desses dados comportam» não respeitam aquele princípio[40]. Em particular, uma regulamentação que permita às

[36] N.ºs 136 e 137. Ver também o acórdão Privacy International, em que o Tribunal de Justiça especificou que tais ameaças podem ser distinguidas, pela sua natureza e particular gravidade, do risco geral de ocorrência de tensões ou de perturbações, ainda que graves, na segurança pública. N.º 75: Por exemplo, no acórdão La Quadrature du Net e o., o Tribunal de Justiça observou que a análise automatizada dos dados de tráfego e de localização que abrangem de forma geral e indiscriminada os dados das pessoas que utilizam sistemas de comunicações eletrónicas constitui uma ingerência particularmente grave, de modo que tal medida só pode satisfazer o requisito da proporcionalidade em situações em que o Estado membro em causa enfrenta uma ameaça grave para a segurança nacional que se revela genuína e atual ou previsível e, entre outras condições, desde que a duração da conservação seja limitada ao estritamente necessário (n.ºs 174 a 177).

[37] Acórdão Schrems II, n.º 176, incluindo a jurisprudência citada.

[38] Acórdão Schrems II, n.º 175.

[39] Acórdão Schrems II, n.º 180.

[40] Acórdão Schrems II, n.º 93, com referências adicionais. Ver (no entanto, desta vez em relação à legislação de um Estado-Membro e não à de um país terceiro) o acórdão Privacy International, n.º 71, incluindo a jurisprudência citada. Neste caso, o Tribunal de Justiça declarou que uma legislação de um Estado-Membro que exige aos fornecedores de serviços de comunicações eletrónicas que divulguem dados de tráfego e dados de localização às agências de segurança e de informações através de uma transmissão geral e indiscriminada excede os limites do estritamente necessário e não pode ser considerada justificada, numa sociedade democrática, como exige a Diretiva relativa à privacidade e às comunicações eletrónicas, lida à luz da Carta (n.º 81).

autoridades públicas aceder de modo generalizado ao conteúdo das comunicações eletrónicas deve ser considerada lesiva do conteúdo essencial do direito fundamental ao respeito da vida privada, tal como é garantido pelo artigo 7.º da Carta[41].

38. De igual modo (no entanto, desta vez, ao avaliar o direito de um Estado-Membro e não o direito de um país terceiro), o TJUE defendeu no acórdão La Quadrature du Net e o. que «a legislação que exige a conservação de dados pessoais deve sempre respeitar critérios objetivos que estabeleçam uma ligação entre os dados conservados e o objetivo prosseguido»[42]. No mesmo contexto, no acórdão Privacy International, o TJUE considerou igualmente que o legislador «deve basear-se em critérios objetivos para definir as circunstâncias e as condições nas quais deve ser concedido às autoridades nacionais competentes o acesso aos dados em causa»[43].

Garantia C – Mecanismo de supervisão independente

39. O CEPD lembra que ocorre uma ingerência no momento da recolha dos dados, mas também no momento em que os dados são objeto de acesso por uma autoridade pública para posterior tratamento. O TEDH especificou várias vezes que qualquer ingerência no direito à privacidade e à proteção de dados deve ser sujeita a um sistema de supervisão eficaz, independente e imparcial que deve ser assegurado quer por um juiz, quer por outro organismo independente[44] (por exemplo, uma autoridade administrativa ou um órgão parlamentar). A supervisão independente da aplicação das medidas de vigilância foi também tida em conta pelo TJUE no acórdão Schrems II[45].

40. O TEDH especifica que, embora a autorização prévia (judicial) das medidas de vigilância constitua uma importante salvaguarda contra a arbitrariedade, deve igualmente ser tido em conta o funcionamento efetivo do sistema de interceção, incluindo os controlos e equilíbrios relativos ao exercício do poder, e a existência ou ausência de abuso efetivo[46]. No processo Schrems II, o TJUE tomou igualmente em consideração o âmbito do controlo exercido pelo mecanismo de supervisão, que não abrangia as medidas de vigilância individuais[47].

---

[41] Acórdão Schrems II, n.º 94.

[42] Acórdão La Quadrature du Net e o., n.º 133. Neste contexto, o Tribunal de Justiça confirmou que as medidas legislativas que preveem, a título preventivo, a conservação geral e indiscriminada de dados relativos ao tráfego e à localização são excluídas pela Diretiva relativa à privacidade e às comunicações eletrónicas, lida à luz da Carta. Em contrapartida, o Tribunal de Justiça decidiu que, em situações de ameaça grave à segurança nacional que se revele genuína e atual ou previsível, o legislador pode permitir, para salvaguardar a segurança nacional, o recurso a uma instrução que exija que os fornecedores de serviços de comunicações eletrónicas conservem, de um modo geral e indiscriminado, os dados relativos ao tráfego e à localização. Essas medidas devem, no entanto, satisfazer condições específicas. Em especial, a instrução só pode ser dada por um período limitado no tempo ao estritamente necessário, que pode ser prorrogado se essa ameaça persistir (n.º 168).

[43] Acórdão Privacy International, n.º 78, incluindo a jurisprudência citada. No acórdão Privacy International, no que diz respeito ao acesso de uma autoridade aos dados pessoais fornecidos ao abrigo da legislação de um Estado-Membro, o Tribunal de Justiça decidiu que «um acesso generalizado a todos os dados conservados, na falta de qualquer relação, mesmo indireta, com o objetivo prosseguido, não pode ser considerado limitado ao estritamente necessário» (n.ºs 77 e 78).

[44] Acórdão do TEDH, Klass, n.ºs 17 e 51.

[45] Acórdão Schrems II, n.ºs 179 e 183.

[46] Acórdão do TEDH, Big Brother Watch, em sede de recurso, n.ºs 319 e 320.

[47] Acórdão Schrems II, n.º 179.

41. No que se refere ao direito dos Estados membros, o TJUE identificou um conjunto de medidas que só são conformes com o direito da UE se forem objeto de um controlo efetivo por parte de um tribunal ou de uma autoridade administrativa independente cuja decisão é vinculativa. O objetivo dessa revisão é verificar se existe uma situação que justifique a medida e se são respeitadas as condições e garantias que devem ser estabelecidas[48]. Relativamente à recolha em tempo real de dados relativos ao tráfego e à localização, a revisão deverá permitir verificar «ex ante», nomeadamente, se a sua autorização se limita ao estritamente necessário. Em casos de urgência devidamente justificados, as medidas podem ser tomadas sem esse reexame prévio; no entanto, o Tribunal de Justiça continua a exigir que a revisão subsequente se realize num curto espaço de tempo[49].

42. Quanto à independência dos mecanismos de supervisão em relação à vigilância, poderiam ser tidas em conta as conclusões do TJUE sobre a independência de um organismo no contexto da reparação (ver adiante, em relação à garantia D). Além disso, a jurisprudência do TEDH pode oferecer elementos adicionais. O TEDH já manifestou a sua preferência quanto a um juiz ser o responsável pela manutenção da supervisão. No entanto, não é de excluir que outro organismo possa ser responsável, «desde que seja suficientemente independente do executivo»[50] e «das autoridades que exercem a vigilância, e que tenha poderes e competências suficientes para exercer um controlo efetivo e contínuo»[51]. O TEDH acrescentou que «o modo de nomeação e o estatuto jurídico dos membros do órgão de supervisão»[52] devem ser tidos em conta na avaliação da independência. Estão aqui incluídas as «pessoas habilitadas a exercer funções judiciais, nomeadas pelo parlamento ou pelo primeiro-ministro. Em contrapartida, um ministro dos assuntos internos – que não só era um nomeado político e um membro do executivo, mas também estava diretamente envolvido na contratação de meios especiais de vigilância – foi considerado insuficientemente independente»[53]. O TEDH também «observa que é essencial que o órgão de supervisão tenha acesso a todos os documentos relevantes, incluindo materiais fechados[54]». Por último, o TEDH tem em conta «se as atividades do órgão de supervisão estão abertas ao controlo público»[55].

Garantia D – É necessário que as pessoas disponham de vias de recurso eficazes

43. A última garantia essencial europeia está relacionada com os direitos de recurso do indivíduo. Cada pessoa deve dispor de um meio de recurso eficaz para fazer valer os seus direitos quando considerar que não são ou não foram respeitados. Além disso, o TJUE observou que «uma regulamentação que não preveja nenhuma possibilidade de o particular recorrer a vias de direito 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, tal como é consagrado no artigo 47.º da Carta. Com efeito, o artigo 47.º, primeiro parágrafo, da Carta exige que

[48] Acórdão do TJUE, La Quadrature du Net e o., n.ºs 168 e 189.

[49] Acórdão do TJUE, La Quadrature du Net e o., n.º 189.

[50] Acórdãos do TEDH, Zakharov, n.º 258, Iordachi e o./Moldávia, n.ºs 40 e 51 e Dumitru Popescu/Roménia, n.ºs 70 a 73.

[51] Acórdãos do TEDH, Klass, n.º 56 e Big Brother Watch, em sede de recurso, n.º 318.

[52] Acórdão do TEDH, Zakharov, n.º 278.

[53] Acórdão do TEDH, Zakharov, n.º 278.

[54] Acórdão do TEDH, Zakharov, n.º 281.

[55] Acórdão do TEDH, Zakharov, n.º 283.

qualquer pessoa cujos direitos e liberdades garantidos pelo direito da União tenham sido violados tenha direito a uma ação perante um tribunal nos termos previstos nesse artigo»[56].

44. Ao apreciar a legislação de um Estado-Membro que permite a recolha em tempo real de dados relativos ao tráfego e à localização, o Tribunal de Justiça considerou que a notificação é necessária «para permitir que as pessoas afetadas exerçam os seus direitos, nos termos dos artigos 7.º e 8.º da Carta, de solicitar o acesso aos seus dados pessoais que tenham sido objeto dessas medidas e, se for caso disso, de solicitar que estes sejam retificados ou apagados, bem como para exercerem, nos termos do primeiro parágrafo do artigo 47.º da Carta, o direito a uma ação perante um tribunal»[57]. No entanto, o TJUE reconheceu igualmente que a notificação das pessoas cujos dados foram recolhidos ou analisados deve ocorrer apenas na medida em que e logo que a notificação deixe de pôr em perigo as tarefas pelas quais essas autoridades são responsáveis[58].

45. Também para o TEDH, a questão de um recurso efetivo está indissociavelmente ligada à notificação de uma medida de vigilância ao indivíduo, uma vez terminada a vigilância. Em especial, o TEDH considerou que «em princípio, a pessoa em causa tem pouca margem para recorrer aos tribunais, a menos que seja informada das medidas tomadas sem o seu conhecimento e possa assim contestar a sua legalidade retrospetivamente ou, a título subsidiário, a menos que qualquer pessoa que suspeite que as suas comunicações estão a ser ou foram intercetadas possa recorrer aos tribunais, de modo a que a competência dos tribunais não dependa da notificação ao destinatário da interceção de que foi objeto de uma interceção das suas comunicações» [59]. O TEDH reconheceu assim que, em alguns casos, pode não haver notificação, mas é necessário prever uma solução eficaz. Neste caso, o TEDH deixou claro, por exemplo, no caso Kennedy, que um tribunal oferece possibilidades de recurso suficientes se preencher uma série de critérios, ou seja, se for um órgão independente e imparcial, se tiver adotado o seu próprio regulamento interno, se for composto por membros que exercem ou exerceram um elevado cargo judicial ou são juristas experientes, e se não for necessário satisfazer um ónus de prova para apresentar um pedido ao tribunal[60]. Ao proceder ao exame das queixas apresentadas por indivíduos, o tribunal deverá ter acesso a todas as informações relevantes[61], incluindo os materiais fechados. Por último, o tribunal deve ter poderes para impor a sanação do incumprimento[62].

[56] Acórdão do TJUE, Schrems I, n.º 95.
[57] Ver n.º 190 do acórdão La Quadrature du Net e o. e Parecer 1/15 do TJUE, n.º 220.
[58] Ver n.º 191.º do acórdão La Quadrature du Net e o.
[59] Acórdão do TEDH, Zakharov, n.º 234.
[60] Acórdão do TEDH, Kennedy, n.º 190.
[61] O CEPD observa que o Comissário para os Direitos Humanos do Conselho da Europa considera que a chamada regra dos «terceiros» – segundo a qual as agências de informações de um país que fornecem dados a agências de informações de outro país podem impor às agências de acolhimento a obrigação de não divulgar os dados transferidos a terceiros – não deve aplicar-se aos organismos de supervisão, a fim de não comprometer a possibilidade de um recurso efetivo (documento temático sobre a supervisão democrática e eficaz dos serviços de segurança nacionais).
[62] Acórdão do TEDH, Kennedy, n.º 167.

46. A versão em inglês do artigo 47.º da Carta faz referência a um órgão jurisdicional, ainda que em versões linguísticas diferentes do inglês seja dada preferência à palavra «tribunal» [63], enquanto a CEDH apenas impõe aos Estados membros que garantam que «qualquer pessoa cujos direitos e liberdades reconhecidos na presente Convenção tiverem sido violados tem direito a recurso perante uma instância nacional» [64], que não tem necessariamente de ser uma autoridade judiciária[65].

47. O TJUE, no contexto do acórdão Schrems II, ao avaliar a adequação do nível de proteção de um país terceiro, reiterou que «os particulares devem dispor da possibilidade de utilizar medidas jurídicas corretivas eficazes num tribunal independente e imparcial para ter acesso a dados pessoais que lhes digam respeito, ou para obter a retificação ou a supressão desses dados» [66]. No mesmo contexto, o TJUE considera que uma proteção judicial eficaz contra tais ingerências pode ser assegurada não só por um tribunal, mas também por um órgão [67] que ofereça garantias essencialmente equivalentes às exigidas pelo artigo 47.º da Carta. No seu acórdão Schrems II, o TJUE sublinhou que a independência do tribunal ou do órgão deve ser assegurada, em especial em relação ao executivo, com todas as garantias necessárias, nomeadamente no que se refere às condições de destituição ou de anulação da nomeação [68], e que os poderes que devem ser atribuídos a um tribunal devem ser conformes com os requisitos do artigo 47.º da Carta. A este respeito, o órgão [69] deve ter poderes para adotar decisões que sejam vinculativas para os serviços de informações, em conformidade com as salvaguardas jurídicas que os titulares dos dados podem invocar [70].

4. OBSERVAÇÕES FINAIS

48. As quatro garantias essenciais europeias devem ser vistas como elementos fundamentais a encontrar na avaliação do nível de ingerência nos direitos fundamentais à privacidade e à proteção de dados. Não devem ser avaliadas de forma independente, uma vez que estão estreitamente interligadas, mas, em termos globais, na análise da legislação pertinente em matéria de medidas de vigilância, do nível mínimo de salvaguardas para a proteção dos direitos dos titulares dos dados e das vias de recurso previstas na legislação nacional do país terceiro.

49. Estas garantias exigem um certo grau de interpretação, especialmente porque a legislação de países terceiros não tem de ser idêntica ao quadro jurídico da UE.

50. Tal como afirmou o TEDH no acórdão Kennedy, «uma avaliação depende de todas as circunstâncias do caso, tais como a natureza, o âmbito e a duração das medidas possíveis, os motivos exigidos para as ordenar, e as autoridades competentes para as autorizar, executar e supervisionar, bem como o tipo de recurso previsto no direito nacional» [71].

---

[63] O termo inglês «tribunal» é, por exemplo, traduzido por «Gericht» em alemão e por «gerecht» em neerlandês.
[64] Artigo 13.º da CEDH.
[65] Acórdão do TEDH, Klass, n.º 67.
[66] Ver n.º 194 do acórdão Schrems II.
[67] Ver n.º 197 do acórdão Schrems II, em que o Tribunal de Justiça utiliza expressamente este termo.
[68] Ver n.º 195 do acórdão Schrems II.
[69] Ver n.º 197 do acórdão Schrems II, em que o Tribunal de Justiça utiliza expressamente este termo.
[70] Ver n.º 196 do acórdão Schrems II.
[71] Acórdão do TEDH, Kennedy, n.º 153.

51. Por conseguinte, a avaliação das medidas de vigilância de países terceiros por comparação com as garantias essenciais europeias pode conduzir a duas conclusões:

- A legislação do país terceiro em questão não garante os requisitos das garantias essenciais europeias: neste caso, a legislação do país terceiro não ofereceria um nível de proteção essencialmente equivalente ao garantido na UE.

- A legislação do país terceiro em questão satisfaz as garantias essenciais europeias.

52. Ao avaliar a adequação do nível de proteção, nos termos do artigo 45.º do RGPD, a Comissão terá de avaliar se as garantias essenciais europeias são satisfeitas como parte dos elementos a considerar para garantir que a legislação do país terceiro, no seu conjunto, oferece um nível de proteção essencialmente equivalente ao garantido na UE.

53. Quando os exportadores de dados confiam, juntamente com os importadores de dados, em garantias adequadas nos termos do artigo 46.º do RGPD, tendo em conta os requisitos da legislação do país terceiro especificamente aplicável aos dados transferidos, deverão assegurar que seja efetivamente alcançado um nível de proteção essencialmente equivalente. Em especial, nos casos em que a legislação do país terceiro não cumpre os requisitos das garantias essenciais europeias, isso implicaria que a lei em causa não colidisse com as garantias e salvaguardas aplicáveis à transferência, de modo que um nível de proteção essencialmente equivalente ao garantido na UE continuasse a ser assegurado.

54. O CEPD emitiu outras orientações e recomendações a ter em conta para proceder à avaliação, em função do instrumento de transferência a utilizar e da necessidade de fornecer garantias adequadas, incluindo, se for caso disso, medidas suplementares [72].

55. Além disso, é de notar que as garantias essenciais europeias se baseiam no que é exigido por lei. O CEPD sublinha que as garantias essenciais europeias se baseiam nos direitos fundamentais aplicáveis a todas as pessoas, independentemente da sua nacionalidade.

56. O CEPD reitera que as garantias essenciais europeias constituem uma norma de referência para a avaliação da ingerência inerente às medidas de vigilância de países terceiros, no contexto das transferências internacionais de dados. Estas normas decorrem do direito da UE e da jurisprudência do TJUE e do TEDH, que é vinculativa para os Estados membros.

[72] Referencial de adequação do CEPD, WP 254 rev. 01, revisto e adotado em 6 de fevereiro de 2018; Recomendações 01/2020 do CEPD sobre medidas que complementam os instrumentos de transferência para garantir o cumprimento do nível de proteção de dados pessoais da UE, 10 de novembro de 2020.