COMISSÃO
EUROPEIA

Bruxelas, 29.5.2019
COM(2019) 250 final

COMUNICAÇÃO DA COMISSÃO AO PARLAMENTO EUROPEU E AO CONSELHO

Orientações sobre o regulamento relativo a um quadro para o livre fluxo de dados não pessoais na União Europeia

Índice

O presente documento é disponibilizado pela Comissão Europeia unicamente para fins informativos. Não contém qualquer interpretação vinculativa do Regulamento (UE) 2018/1807 do Parlamento Europeu e do Conselho, de 14 de novembro de 2018, relativo a um regime para o livre fluxo de dados não pessoais na União Europeia e não constitui uma decisão ou posição da Comissão Europeia. Não afeta eventuais decisões ou posições da Comissão Europeia nem as competências do Tribunal de Justiça da União Europeia para interpretar o regulamento em conformidade com os Tratados da UE.

1 Introdução

Numa economia cada vez mais baseada em dados, os fluxos de dados estão no centro dos processos operacionais de empresas de todas as dimensões e em todos os setores. As novas tecnologias digitais geram oportunidades para o público em geral, para as empresas e para as administrações públicas na União Europeia (a seguir designada por «UE»).

Com vista a aumentar o intercâmbio transfronteiriço de dados e impulsionar a economia dos dados, o Parlamento Europeu e o Conselho adotaram, em novembro de 2018, o Regulamento (UE) 2018/1807, relativo a um regime para o livre fluxo de dados não pessoais na União Europeia[1] (a seguir designado por «Regulamento Livre Fluxo de Dados Não Pessoais»), com base numa proposta da Comissão Europeia (a seguir designada por «Comissão»). O regulamento é aplicável a partir de 28 de maio de 2019. O princípio da livre circulação de dados pessoais já se encontra estabelecido no Regulamento (UE) 2016/679 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 «Regulamento Geral sobre a Proteção de Dados»)[2]. Consequentemente, existe agora um quadro abrangente para um espaço comum europeu de dados e a livre circulação de todos os dados na União Europeia[3].

O Regulamento Livre Fluxo de Dados Não Pessoais cria segurança jurídica para que as empresas possam escolher onde pretendem tratar os seus dados na UE, aumenta a confiança nos serviços de tratamento de dados e contraria as práticas de vinculação a um prestador de serviços. Tal aumentará as possibilidades de escolha dos clientes, melhorará a eficiência e incentivará a adoção de tecnologias de computação em nuvem, conduzindo a poupanças significativas para as empresas na UE. Um estudo mostra que as empresas da UE podem poupar entre 20 % e 50 % dos seus custos informáticos se optarem pela migração para a nuvem[4].

Graças aos dois regulamentos supramencionados, os dados podem circular livremente entre os Estados-Membros, permitindo aos utilizadores de serviços de tratamento de dados utilizar os dados recolhidos em diferentes mercados da UE para melhorar a sua produtividade e competitividade. Os utilizadores podem, assim, tirar pleno partido das economias de escala proporcionadas pelo grande mercado da UE, melhorando a sua competitividade a nível mundial e aumentando a interconectividade da economia europeia dos dados.

---

[1] Regulamento (UE) 2018/1807 do Parlamento Europeu e do Conselho, de 14 de novembro de 2018, relativo a um regime para o livre fluxo de dados não pessoais na União Europeia (JO L 303 de 28.11.2018, p. 59).

[2] 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).

[3] O Regulamento Geral sobre a Proteção de Dados abrange também o Espaço Económico Europeu (EEE), que inclui a Islândia, o Listenstaine e a Noruega. Além disso, o Regulamento Livre Fluxo de Dados Não Pessoais é considerado relevante para efeitos do EEE.

[4] Deloitte: *Measuring the economic impact of cloud computing in Europe*, SMART 2014/0031, 2016. Disponível no seguinte endereço: http://ec.europa.eu/newsroom/document.cfm?doc_id=41184.

O Regulamento Livre Fluxo de Dados Não Pessoais apresenta três particularidades importantes:

- Proíbe, regra geral, os Estados-Membros de impor requisitos sobre a localização dos dados. As exceções a esta regra só podem ser justificadas por razões de segurança pública, em conformidade com o princípio da proporcionalidade.
- Estabelece um mecanismo de cooperação para garantir que as autoridades competentes continuam a poder exercer os seus eventuais direitos de acesso a dados que estão a ser tratados noutro Estado-Membro.
- Prevê incentivos para que a indústria, com o apoio da Comissão, elabore códigos de conduta de autorregulação sobre a mudança de prestador de serviços e a portabilidade de dados.

Objetivo do presente documento de orientação

O presente documento dá cumprimento ao disposto no artigo 8.º, n.º 3, do Regulamento Livre Fluxo de Dados Não Pessoais, que exige que a Comissão publique orientações sobre a interação entre este regulamento e o Regulamento Geral sobre a Proteção de Dados, «nomeadamente no que se refere aos conjuntos compostos por dados pessoais e não pessoais».

As presentes orientações visam ajudar os utilizadores — especialmente as pequenas e médias empresas — a compreender a interação entre o Regulamento Livre Fluxo de Dados Não Pessoais e o Regulamento Geral sobre a Proteção de Dados[5]. Por conseguinte, o documento aborda, em especial: i) os conceitos de dados não pessoais e dados pessoais, ii) os princípios da livre circulação de dados e a proibição do estabelecimento de requisitos de localização de dados no âmbito dos dois regulamentos, iii) a noção de portabilidade de dados ao abrigo do Regulamento Livre Fluxo de Dados Não Pessoais. Trata igualmente dos requisitos de autorregulação estabelecidos nos dois regulamentos.

O Regulamento Livre Fluxo de Dados Não Pessoais abrange apenas «dados que não sejam dados pessoais», na aceção do Regulamento Geral sobre a Proteção de Dados. O Regulamento Geral sobre a Proteção de Dados rege o tratamento de dados pessoais, que constitui uma parte essencial do quadro de proteção de dados da UE[6]. Este regulamento entrou em vigor nos

[5] Considerando 37 do Regulamento (UE) 2018/1807 do Parlamento Europeu e do Conselho, de 14 de novembro de 2018, relativo a um regime para o livre fluxo de dados não pessoais na União Europeia.

[6]
- 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).
- Regulamento (UE) 2018/1725 do Parlamento Europeu e do Conselho, de 23 de outubro de 2018, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas instituições e pelos órgãos e organismos da União e à livre circulação desses dados, e que revoga o Regulamento (CE) n.º 45/2001 e a Decisão n.º 1247/2002/CE (JO L 295 de 21.11.2018, p. 39).
- Diretiva (UE) 2016/680 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

Estados-Membros em 25 de maio de 2018 e estabelece regras harmonizadas para proteger as pessoas na UE/no EEE no que diz respeito ao tratamento dos seus dados pessoais e à livre circulação desses dados. O Regulamento Geral sobre a Proteção de Dados: i) especifica que informações constituem dados pessoais, ii) estabelece fundamentos jurídicos para o seu tratamento, iii) define os direitos e as obrigações a observar aquando do tratamento desses dados[7], entre outras disposições. No que se refere ao princípio da livre circulação de dados pessoais, o artigo 1.º, n.º 3, do Regulamento Geral sobre a Proteção de Dados estabelece que a «[a] livre circulação de dados pessoais no interior da União não é restringida nem proibida por motivos relacionados com a proteção das pessoas singulares no que respeita ao tratamento de dados pessoais».

Na maior parte das situações reais, é muito provável que um conjunto de dados seja composto por dados pessoais e não pessoais. Um conjunto de dados com estas características é frequentemente designado por «conjunto misto de dados». A secção 2.2 infra explica mais pormenorizadamente a interação entre o Regulamento Livre Fluxo de Dados Não Pessoais e o Regulamento Geral sobre a Proteção de Dados no que respeita aos conjuntos mistos de dados.

Por razões de clareza, sublinha-se que não existem obrigações contraditórias decorrentes do Regulamento Geral sobre a Proteção de Dados e da livre circulação de dados não pessoais.

---

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 (JO L 119 de 4.5.2016, p. 89).

– Diretiva 2002/58/CE do Parlamento Europeu e do Conselho, de 12 de julho de 2002, relativa ao tratamento de dados pessoais e à proteção da privacidade no setor das comunicações eletrónicas (Diretiva relativa à privacidade e às comunicações eletrónicas) (JO L 201 de 31.7.2002, p. 37) — atualmente em revisão.

[7] Para mais orientações sobre diversos aspetos 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 (Regulamento Geral sobre a Proteção de Dados) e sobre a legislação europeia em matéria de proteção de dados, consultar a página Web do Comité Europeu para a Proteção de Dados, que emitiu uma série de orientações em conformidade com o artigo 70.º do Regulamento Geral sobre a Proteção de Dados, disponíveis em: https://edpb.europa.eu/our-work-tools/general-guidance/gdpr-guidelines-recommendations-best-practices_pt. A referida página Web também disponibiliza o acesso a orientações, recomendações e outros documentos elaborados pelo antecessor do Comité Europeu para a Proteção de Dados — Grupo de Trabalho do Artigo 29.º Além disso, com o objetivo de sensibilizar os cidadãos e as empresas para o conteúdo 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 (Regulamento Geral sobre a Proteção de Dados), a Comissão publicou uma comunicação sobre a proteção de dados — Orientações da Comissão relativas à aplicação direta do RGPD [COM(2018) 43 final], disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?qid=1517578296944&uri=CELEX%3A52018DC0043

2 Interação entre o Regulamento Livre Fluxo de Dados Não Pessoais e o Regulamento Geral sobre a Proteção de Dados — conjuntos mistos de dados.

2.1 O conceito de dados não pessoais no Regulamento Livre Fluxo de Dados Não Pessoais

O Regulamento Livre Fluxo de Dados Não Pessoais[8] visa assegurar o livre fluxo de dados que não sejam dados pessoais. Em todo o seu texto, o regulamento utiliza o termo «dados», que deve ser entendido como «dados que não sejam dados pessoais na aceção do artigo 4.º, ponto 1, do Regulamento (UE) 2016/679 [Regulamento Geral sobre a Proteção de Dados]»[9]. Esses dados, também referidos como «**dados não pessoais**» no presente documento, são definidos por oposição (*a contrario*) aos dados pessoais, tal como descritos no Regulamento Geral sobre a Proteção de Dados.

Dados pessoais

De acordo com o Regulamento Geral sobre a Proteção de Dados, entende-se por: «"[d]ados pessoais", informação relativa a uma pessoa singular identificada ou identificável ("titular dos dados"); é considerada identificável uma pessoa singular que possa ser identificada, direta ou indiretamente, em especial por referência a um identificador, como por exemplo um nome, um número de identificação, dados de localização, identificadores por via eletrónica ou a um ou mais elementos específicos da identidade física, fisiológica, genética, mental, económica, cultural ou social dessa pessoa singular».

A definição lata de dados pessoais é intencional e permaneceu essencialmente inalterada no Regulamento Geral sobre a Proteção de Dados, em comparação com a legislação anterior[10]. Diversos aspetos da definição de dados pessoais, como «[qualquer] informação», «relativa a», «identificada ou identificável», já foram analisados pelo Grupo de Trabalho do Artigo 29.º[11] no seu Parecer 4/2007 sobre o conceito de dados pessoais, adotado em 20 de junho de 2007 (WP 136).

---

8 Artigo 1.º do Regulamento (UE) 2018/1807 do Parlamento Europeu e do Conselho, de 14 de novembro de 2018, relativo a um regime para o livre fluxo de dados não pessoais na União Europeia.

9 Ver o artigo 3.º, ponto 1, do Regulamento (UE) 2018/1807 do Parlamento Europeu e do Conselho, de 14 de novembro de 2018, relativo a um regime para o livre fluxo de dados não pessoais na União Europeia.

10 Ver o artigo 2.º, alínea a), da 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 (data de fim de validade: 24 de maio de 2018, revogada pelo Regulamento Geral sobre a Proteção de Dados). Consultar igualmente a jurisprudência do Tribunal de Justiça relativa à definição de dados pessoais, que reconhece a interpretação lata desse conceito, por exemplo o Acórdão do Tribunal de Justiça de 29 de janeiro de 2009 no processo C-275/06, Productores de Música de España (Promusicae)/Telefónica de España SAU, ECLI:EU:C:2008:54; o Acórdão do Tribunal de Justiça de 24 de novembro de 2011 no processo C-70/10, Scarlet Extended SA/Société belge des autores, compositeurs et éditeurs SCRL (SABAM), ECLI:EU:C:2011:771; o Acórdão do Tribunal de Justiça de 19 de outubro de 2016 no processo C-582/14, Patrick Breyer/Bundersrepublik Deutschland, ECLI:EU:C:2016:779.

11 O Grupo de Trabalho do Artigo 29.º foi um órgão consultivo que prestou aconselhamento à Comissão em matéria de proteção de dados e que contribuiu para a elaboração de políticas harmonizadas de proteção de dados na UE. Após o início da aplicabilidade do Regulamento Geral sobre a Proteção de Dados, em 25 de maio de 2018, o Grupo de Trabalho do Artigo 29.º foi substituído pelo Comité Europeu para a Proteção de Dados.

Em domínios como a investigação, é prática comum pseudonimizar os dados pessoais a fim de encobrir a identidade de uma pessoa. A **pseudonimização** é o tratamento de dados pessoais de forma a que não seja possível atribuí-los a uma pessoa específica sem recorrer a informações adicionais. Estas informações adicionais são mantidas separadamente e protegidas por meio de medidas organizacionais ou técnicas (por exemplo, cifragem)[12,13]. No entanto, os dados pseudonimizados continuam a ser considerados informações sobre uma pessoa identificável se puderem ser atribuídos a essa pessoa mediante a utilização de informações adicionais[14]. Esses dados **constituem dados pessoais** na aceção do Regulamento Geral sobre a Proteção de Dados.

Dados não pessoais

Todos os dados que não sejam «dados pessoais», na aceção do Regulamento Geral sobre a Proteção de Dados, são **dados não pessoais**. Os dados não pessoais podem ser classificados segundo a origem:

- Desde o início — dados originalmente não relacionados com uma pessoa singular identificada ou identificável, tais como dados sobre as condições meteorológicas gerados por sensores instalados em turbinas eólicas ou dados sobre as necessidades de manutenção de máquinas industriais.

- Em segunda fase — dados inicialmente pessoais, mas posteriormente **anonimizados**[15]. A «anonimização» de dados pessoais é diferente da pseudonimização (ver supra), uma vez que os dados devidamente anonimizados não podem ser atribuídos a uma determinada pessoa, nem sequer pela utilização de dados adicionais[16], pelo que se tratam de dados não pessoais.

---

12 Ver o artigo 4.º, ponto 5, 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 (Regulamento Geral sobre a Proteção de Dados), que define «pseudonimização».

13 Por exemplo, pode considerar-se que um estudo de investigação dos efeitos de um novo medicamento recorre à pseudonimização, se os dados pessoais dos participantes no estudo forem substituídos por atributos únicos (por exemplo, um número ou código) na documentação de investigação e forem mantidos separadamente, com os atributos únicos atribuídos, num documento protegido (por exemplo, uma base de dados protegida por senha).

14 Ver o considerando 26 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 (Regulamento Geral sobre a Proteção de Dados).

15 Ver o considerando 26 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 (Regulamento Geral sobre a Proteção de Dados), segundo o qual os «princípios da proteção de dados não deverão, pois, aplicar-se às informações anónimas, ou seja, às informações que não digam respeito a uma pessoa singular identificada ou identificável nem a dados pessoais tornados de tal modo anónimos que o seu titular não seja ou já não possa ser identificado».

16 Ver o Acórdão do Tribunal de Justiça de 19 de outubro de 2016 no processo C-582/14, Patrick Breyer/Bundersrepublik Deutschland, ECLI:EU:C:2016:779. O Tribunal de Justiça considerou que o endereço de protocolo Internet (IP) dinâmico pode constituir um dado pessoal mesmo que um terceiro (por exemplo, um fornecedor de serviços de Internet) disponha de dados adicionais que lhe permitam identificar a pessoa em causa. A possibilidade de identificar a pessoa deve constituir meios suscetíveis de serem razoavelmente utilizados para identificar a pessoa, direta ou indiretamente.

Aferir da correta anonimização dos dados depende de circunstâncias específicas e únicas de cada caso[17]. Os vários exemplos detetados de reidentificação de conjuntos de dados supostamente anonimizados demonstraram que essa avaliação pode ser exigente[18]. Para determinar se uma pessoa é identificável, é necessário ter em conta todos os meios suscetíveis de serem razoavelmente utilizados por um responsável pelo tratamento ou qualquer outra pessoa para identificar uma pessoa direta ou indiretamente[19].

Exemplos de dados não pessoais:

- Dados agregados a um nível em que acontecimentos individuais (tais como viagens de indivíduos ao estrangeiro ou padrões de viagem que possam constituir dados pessoais) já não são identificáveis podem ser considerados dados anónimos[20]. Os dados anónimos são utilizados, por exemplo, em estatísticas ou em relatórios de vendas (por exemplo, para aferir a popularidade de um produto e das suas características).
- Dados de negociação de alta frequência no setor financeiro, ou dados sobre a agricultura de precisão, que ajudam a monitorizar e otimizar a utilização de pesticidas, nutrientes e água.

No entanto, se determinados dados não pessoais puderem ser associados a uma pessoa de qualquer forma, tornando-os direta ou indiretamente identificáveis, devem ser considerados dados pessoais.

Por exemplo, se um relatório de controlo da qualidade sobre uma linha de produção permitir relacionar os dados com trabalhadores da fábrica específicos (por exemplo, os que fixam os parâmetros de produção), os dados serão considerados dados pessoais e o Regulamento Geral sobre a Proteção de Dados será forçosamente aplicável. Aplicam-se as mesmas regras quando

---

17 A anonimização de dados deve ser sempre realizada utilizando as mais recentes técnicas avançadas.

18 Para exemplos de reidentificação de dados supostamente anonimizados, consultar o estudo sobre os futuros fluxos de dados realizado para a Comissão ITRE do Parlamento Europeu por Blackman, C., Forge, S.: *Data Flows — Future Scenarios: In-Depth Analysis for the ITRE Committee*, 2017, p. 22, caixa de texto 2. Disponível no seguinte endereço: http://www.europarl.europa.eu/RegData/etudes/IDAN/2017/607362/IPOL_IDA(2017)607362_EN.pdf.

19 Ver o considerando 26 do Regulamento (UE) 2016/679 (Regulamento Geral sobre a Proteção de Dados), segundo o qual «[p]ara determinar se há uma probabilidade razoável de os meios serem utilizados para identificar a pessoa singular, importa considerar todos os fatores objetivos, como os custos e o tempo necessário para a identificação, tendo em conta a tecnologia disponível à data do tratamento dos dados e a evolução tecnológica».

20 Conforme referido pelo Grupo de Trabalho do Artigo 29.º no documento *Parecer 05/2014 sobre técnicas de anonimização*, adotado em 10 de abril de 2014 (WP 216), p. 9: «[a]penas quando o responsável pelo tratamento de dados agrega os dados a um nível em que cada evento deixa de ser identificável é que o conjunto de dados daí resultante pode ser classificado como anónimo. Por exemplo: se uma organização recolher dados sobre os movimentos de viagem de uma pessoa singular, os padrões de viagem dessa pessoa a nível de evento continuariam a ser classificados como dados pessoais para qualquer parte enquanto o responsável pelo tratamento dos dados (ou qualquer outra parte) continuar a ter acesso aos dados brutos originais, mesmo que os identificadores diretos tenham sido retirados do conjunto fornecido a terceiros. Porém, se o responsável pelo tratamento de dados eliminar os dados brutos e apenas fornecer estatísticas agregadas a terceiros a um nível elevado, tais como "nas segundas-feiras, na trajetória X há mais 160 % de passageiros do que nas terças-feiras", estas informações serão consideradas como dados anónimos».

a evolução da tecnologia e da análise de dados torna possível a conversão de dados anonimizados em dados pessoais. [21]

Uma vez que a definição de dados pessoais se refere a «pessoas singulares», os conjuntos de dados que contêm nomes e contactos de pessoas coletivas são, em princípio, dados não pessoais[22]. No entanto, em determinadas situações podem ser considerados dados pessoais[23]. Será o caso, por exemplo, de uma pessoa coletiva cujo nome seja o mesmo de uma pessoa singular que a detenha ou cujas informações que estejam relacionadas com uma pessoa singular identificada ou identificável[24].

2.2 Conjuntos mistos de dados

O Regulamento Livre Fluxo de Dados Não Pessoais e o Regulamento Geral sobre a Proteção de Dados abordam a livre circulação de dados na UE de duas perspetivas diferentes.

O Regulamento Livre Fluxo de Dados Não Pessoais estabelece uma proibição geral dos requisitos de localização de dados para os dados não pessoais. O artigo 4.º, n.º 1, do regulamento proíbe os requisitos de localização de dados, salvo quando justificados por motivos de segurança pública e no respeito do princípio da proporcionalidade.

O Regulamento Geral sobre a Proteção de Dados, além de assegurar um elevado nível de proteção dos dados pessoais, garante a livre circulação de dados pessoais. Nos termos do artigo 1.º, n.º 3, do referido regulamento, a livre circulação de dados pessoais «não é restringida nem proibida por motivos relacionados com a proteção das pessoas singulares no que respeita ao tratamento de dados pessoais». Em conjunto, os dois regulamentos possibilitam a livre circulação de «todos» os dados no interior da UE. As disposições específicas são abordadas mais aprofundadamente nos pontos 3.1 e 3.2.

Um conjunto misto de dados é composto por dados pessoais e não pessoais. Os conjuntos mistos de dados representam a maioria dos conjuntos de dados utilizados na economia dos

[21] Se os dados pessoais forem tratados ilegalmente ou se o seu tratamento infringir o Regulamento Geral sobre a Proteção de Dados, os titulares dos dados (pessoas singulares) têm o direito de apresentar reclamação, ao abrigo do referido regulamento, a uma autoridade de controlo nacional (autoridade de proteção de dados) na UE, ou a intentar ação judicial junto de um tribunal nacional. As funções, competências e poderes das autoridades de controlo nacionais estão estabelecidas no capítulo VI, secção 2, do Regulamento Geral sobre a Proteção de Dados.

[22] Ver o considerando 14 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 (Regulamento Geral sobre a Proteção de Dados), segundo o qual «[o] presente regulamento não abrange o tratamento de dados pessoais relativos a pessoas coletivas, em especial a empresas estabelecidas enquanto pessoas coletivas, incluindo a denominação, a forma jurídica e os contactos da pessoa coletiva». No entanto, este considerando deve ser lido tendo em conta a definição dados pessoais estabelecida no artigo 4.º, ponto 1, do mesmo regulamento.

[23] Ver o Acórdão do Tribunal de Justiça de 9 de novembro de 2010 nos processos apensos C-92/09, Volker und Markus Schecke GbR/Land Hessen, e C-93/09, Hartmut Eifert/Land Hessen, ECLI:EU:C:2010:662, n.º 52.

[24] https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/application-regulation/do-data-protection-rules-apply-data-about-company_en.

dados e são comuns devido a resultados da evolução tecnológica como sejam a Internet das coisas (ou seja, a ligação digital entre objetos), a inteligência artificial e as tecnologias que permitem a análise de megadados.

Exemplos de conjuntos mistos de dados:

- Registo fiscal de uma empresa, com menção do nome e do número de telefone do seu diretor executivo;
- Conjuntos de dados num banco, especialmente os que contêm informações sobre os clientes e dados relativos a transações, tais como serviços de pagamento (cartões de crédito e de débito), aplicações de gestão de relacionamento com parceiros e acordos de empréstimo, documentos que misturam dados relativos a pessoas singulares e coletivas;
- Dados estatísticos anonimizados de uma instituição de investigação e os dados brutos recolhidos inicialmente, tais como as respostas de cada inquirido às perguntas do inquérito estatístico;
- A base de dados de conhecimentos de uma empresa sobre problemas informáticos e respetivas soluções, criada a partir de relatórios individuais de incidentes informáticos;
- Dados relacionados com a Internet das coisas, em que alguns dos dados permitem formular hipóteses sobre indivíduos identificáveis (por exemplo, presença numa determinada morada e padrões de utilização);
- Análise dos registos de dados operacionais de equipamento de fabrico no setor transformador.

Exemplo: serviços de gestão de relacionamento com clientes

Alguns bancos recorrem a serviços de gestão de relacionamento com clientes (CRM) fornecidos por terceiros que exigem a disponibilização de dados dos clientes no ambiente de CRM. Os dados conservados no serviço de CRM incluirão todas as informações necessárias para gerir eficazmente a interação com os clientes, tais como os seus endereços postais e eletrónicos, os seus números de telefone, os produtos e serviços que adquirem e os relatórios de vendas, incluindo dados agregados. Assim, estes dados podem incluir dados pessoais e não pessoais dos clientes.

No que diz respeito aos conjuntos mistos de dados, o Regulamento Livre Fluxo de Dados Não Pessoais[25] estabelece que:

«No caso de um conjunto de dados compostos por dados pessoais e não pessoais, o presente regulamento aplica-se aos dados não pessoais do conjunto de dados. Caso os dados pessoais e não pessoais de um conjunto de dados estejam indissociavelmente ligados, o presente regulamento não prejudica a aplicação do Regulamento (UE) 2016/679.»

[25] Artigo 2.º, n.º 2.

Isto significa que, no caso de um conjunto de dados compostos por dados pessoais e não pessoais:

- O Regulamento Livre Fluxo de Dados Não Pessoais se aplica aos dados não pessoais do conjunto de dados.
- A disposição do Regulamento Geral sobre a Proteção de Dados relativa à liberdade de circulação[26] se aplica aos dados pessoais do conjunto de dados;
- Se os dados não pessoais e os dados pessoais estiverem «indissociavelmente ligados», os direitos e obrigações em matéria de proteção de dados decorrentes do Regulamento Geral sobre a Proteção de Dados se aplicam plenamente a todo o conjunto misto de dados, mesmo que os dados pessoais representem apenas uma pequena parte do conjunto de dados[27].

Esta interpretação está em consonância com o direito à proteção dos dados pessoais garantido pela Carta dos Direitos Fundamentais da União Europeia[28] e com o considerando 8 do Regulamento Livre Fluxo de Dados Não Pessoais[29]. O considerando 8 estabelece que o «regime jurídico sobre a proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais […], nomeadamente [o Regulamento Geral sobre a Proteção de Dados] e as Diretivas (UE) 2016/680 e 2002/58/CE […], não são afetados pelo presente regulamento».

Exemplo prático:

Uma empresa que opera na UE oferece os seus serviços através de uma plataforma. As empresas (clientes) carregam os seus documentos, que contêm conjuntos mistos de dados, na plataforma. Na qualidade de «responsável pelo tratamento», a empresa que carrega os documentos tem de se certificar de que o tratamento está em conformidade com o Regulamento Geral sobre a Proteção de Dados. Ao tratar o conjunto de dados por conta do responsável pelo tratamento, a empresa que oferece os serviços (o «subcontratante») necessita de armazenar e tratar os dados em conformidade com o Regulamento Geral sobre a Proteção de Dados, por exemplo para garantir um nível adequado de segurança dos dados, incluindo por via da cifragem.

O conceito de «indissociavelmente ligados» não é definido em nenhum dos regulamentos em causa[30]. Para efeitos práticos, pode referir-se a uma situação em que um conjunto de dados

[26] Artigo 1.º, n.º 3, 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 (Regulamento Geral sobre a Proteção de Dados). Ver também o ponto 3.2 infra.

[27] Tal como referido no documento de trabalho dos serviços da Comissão intitulado «Avaliação de impacto que acompanha o documento "proposta de Regulamento do Parlamento Europeu e do Conselho relativo a um regime para o livre fluxo de dados não pessoais na União Europeia"» [SWD(2017) 304 final], parte 1/2, p. 3: «independentemente da quantidade de dados pessoais incluídos num conjunto misto de dados, o RGPD [Regulamento Geral sobre a Proteção de Dados] tem de ser plenamente respeitado no atinente aos dados pessoais incluídos no conjunto».

[28] Carta dos Direitos Fundamentais da União Europeia (JO C 362 de 26.10.2012, p. 391).

[29] Considerando 8.

[30] O Regulamento Livre Fluxo de Dados Não Pessoais e o Regulamento Geral sobre a Proteção de Dados.

contém dados pessoais e dados não pessoais, e em que a separação dos dois tipos é impossível ou é considerada economicamente ineficiente ou tecnicamente inviável pelo responsável pelo tratamento. Por exemplo, aquando da aquisição de sistemas de CRM e de elaboração de relatórios de vendas, a empresa teria de duplicar os seus custos com *software* mediante a aquisição de *software* separado para sistemas de CRM (dados pessoais) e sistemas de elaboração de relatórios de vendas (dados agregados/não pessoais) baseados em dados do sistema de CRM.

A separação do conjunto de dados é também suscetível de reduzir significativamente o seu valor. Além disso, a natureza evolutiva dos dados (ver ponto 2.1) dificulta a distinção clara e, por conseguinte, a separação entre diferentes categorias de dados.

É importante destacar que nenhum dos regulamentos obriga as empresas a separar os conjuntos de dados por cujo tratamento são responsáveis, incluindo na qualidade de subcontratante.

Por conseguinte, um conjunto misto de dados estará, em geral, sujeito às obrigações dos responsáveis pelo tratamento de dados e subcontratantes e terá de respeitar os direitos dos titulares dos dados estabelecidos pelo Regulamento Geral sobre a Proteção de Dados.

Tratamento dos dados relativos à saúde

Um conjunto misto de dados pode incluir dados relativos à saúde. A título de exemplo, destacam-se os registos de saúde eletrónicos, os ensaios clínicos ou os conjuntos de dados recolhidos por diversas aplicações de saúde e bem-estar móvel (por exemplo aplicações que analisam o estado de saúde de modo a recordar o seu utilizador da toma de medicamentos ou para registar a evolução da condição física)[31]. A divisão exata entre dados pessoais e não pessoais nestes conjuntos de dados está a tornar-se cada vez mais ténue, devido à evolução tecnológica. Consequentemente, o seu tratamento deve cumprir o disposto no Regulamento Geral sobre a Proteção de Dados, em especial (visto que os dados relativos à saúde constituem uma categoria especial de acordo com o referido regulamento) no artigo 9.º, que estabelece a proibição geral de tratar categorias especiais de dados, bem como exceções a essa proibição.

Os dados contidos em conjuntos mistos de dados que incluem dados relativos à saúde podem ser uma fonte valiosa de informação, por exemplo para efeitos de investigação médica, medição dos efeitos secundários de medicamentos prescritos, análise estatística de doenças ou desenvolvimento de novos serviços ou tratamentos de saúde. No entanto, o Regulamento Geral sobre a Proteção de Dados deve ser respeitado, quer durante as operações iniciais de tratamento de dados como durante as operações de tratamento adicionais. Assim, qualquer

[31] O desenvolvimento e a utilização de aplicações de saúde móvel exigem o cumprimento estrito das normas estabelecidas no Regulamento Geral sobre a Proteção de Dados. Estes requisitos serão especificados mais pormenorizadamente no código de conduta sobre a privacidade nas aplicações de saúde móvel, atualmente em elaboração. Para mais informações sobre o progresso da elaboração, consultar: https://ec.europa.eu/digital-single-market/en/privacy-code-conduct-mobile-health-apps.

tratamento de dados relativos à saúde deve ter um fundamento jurídico válido[32] e uma justificação adequada, ser seguro e incluir as salvaguardas suficientes.

Por fim, é essencial que as pessoas e as empresas tenham segurança jurídica e confiem no tratamento dos dados. Essas condições são igualmente cruciais para a economia dos dados. Os dois regulamentos garantem esses objetivos e visam a inexistência de entraves à livre circulação de dados.

3 Livre fluxo de dados e eliminação dos requisitos de localização de dados

A presente secção explica mais pormenorizadamente o conceito de «requisitos de localização de dados», no âmbito do Regulamento Livre Fluxo de Dados Não Pessoais, e o «princípio da livre circulação», constante do Regulamento Geral sobre a Proteção de Dados. Embora estas disposições visem os Estados-Membros, podem ajudar as empresas a ter uma ideia mais exata de como os dois regulamentos contribuem para a livre circulação de todos os dados na UE.

3.1 Livre fluxo de dados não pessoais

O Regulamento Livre Fluxo de Dados Não Pessoais[33] estabelece que os «requisitos de localização de dados são proibidos, salvo quando justificados por motivos de segurança pública e no respeito do princípio da proporcionalidade».

Os **requisitos de localização de dados** são definidos[34] como «uma obrigação, proibição, condição, limitação ou outra exigência, prevista nas disposições legislativas, regulamentares ou administrativas de um Estado-Membro, ou resultante de práticas administrativas gerais e coerentes de um Estado-Membro e de organismos regidos pelo direito público, nomeadamente no domínio dos contratos públicos, sem prejuízo do disposto na Diretiva 2014/24/UE, que exige o tratamento de dados no território de um Estado-Membro específico ou restringe o tratamento de dados em qualquer outro Estado-Membro[35]».

A definição demonstra como as medidas que restringem a livre circulação de dados na UE podem assumir diversas formas. Podem ser estabelecidas na legislação ou em regulamentos e disposições de caráter administrativo ou até resultar de práticas administrativas gerais e sistemáticas. Além disso, a proibição dos requisitos de localização de dados abrange medidas suscetíveis de restringir direta ou indiretamente a livre circulação de dados não pessoais.

---

32 Ver o artigo 6.º, n.º 1, 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 (Regulamento Geral sobre a Proteção de Dados).

33 Artigo 4.º, n.º 1.

34 Artigo 3.º, ponto 5, do Regulamento (UE) 2018/1807 do Parlamento Europeu e do Conselho, de 14 de novembro de 2018, relativo a um regime para o livre fluxo de dados não pessoais na União Europeia.

35 Note-se que a incerteza jurídica quanto ao alcance dos requisitos legítimos e ilegítimos em matéria de localização dos dados restringem ainda mais as opções disponíveis para os intervenientes no mercado e o setor público, no que se refere à localização do tratamento dos dados [ver o considerando 4 do Regulamento (UE) 2018/1807 do Parlamento Europeu e do Conselho, de 14 de novembro de 2018, relativo a um regime para o livre fluxo de dados não pessoais na União Europeia].

Os **requisitos diretos de localização de dados** podem consistir, por exemplo, na obrigação de armazenar dados numa localização geográfica específica (por exemplo, a obrigação de os servidores estarem localizados num determinado Estado-Membro) ou a obrigação de cumprir requisitos técnicos nacionais únicos (por exemplo, a obrigação de os dados utilizarem formatos nacionais específicos).

Os **requisitos indiretos de localização de dados**, que podem restringir o tratamento de dados não pessoais noutro Estado-Membro, podem assumir diversas formas. Podem incluir a obrigação de utilizar meios tecnológicos certificados ou aprovados num determinado Estado-Membro ou outras obrigações cujos efeitos tornem mais difícil o tratamento de dados fora de uma zona geográfica ou território específico na União Europeia[36,37].

O processo de aferir se uma determinada medida representa um requisito indireto de localização de dados deve ter em conta as circunstâncias específicas de cada caso.

O Regulamento Livre Fluxo de Dados Não Pessoais[38] remete para o conceito de **segurança pública**, tal como interpretado pelo Tribunal de Justiça da União Europeia. Este conceito «abrange tanto a segurança interna como a segurança externa de um Estado-Membro[39], bem como questões atinentes à proteção pública, nomeadamente a fim de facilitar a investigação, a deteção e a repressão de infrações penais. O conceito de "segurança pública" pressupõe a existência de uma ameaça real e suficientemente grave que afete um interesse essencial da sociedade[40], como, por exemplo, uma ameaça ao funcionamento das instituições e serviços públicos essenciais e à sobrevivência da população, assim como o risco de uma perturbação grave das relações externas ou da coexistência pacífica das nações, ou um risco para os interesses militares».

Além disso, qualquer requisito de localização de dados justificado por razões de segurança pública deve ser proporcionado. De acordo com a jurisprudência do Tribunal de Justiça da

---

[36] Considerando 4 do Regulamento (UE) 2018/1807 do Parlamento Europeu e do Conselho, de 14 de novembro de 2018, relativo a um regime para o livre fluxo de dados não pessoais na União Europeia.

[37] Ver dois estudos sobre requisitos de localização de dados realizados antes da adoção do Regulamento Livre Fluxo de Dados Não Pessoais: 1) Godel, M. *et al.*: *Facilitating cross border data flows in the Digital Single Market*, número SMART: 2015/0016. Disponível no seguinte endereço: http://ec.europa.eu/newsroom/document.cfm?doc_id=41185; 2) Time.lex, Spark Legal Network e Tech4i2: *Cross-border data flow in the digital single market: study on data localisation restrictions*, número SMART: 2015/0054. Disponível no seguinte endereço: http://ec.europa.eu/newsroom/dae/document.cfm?doc_id=46695.

[38] Considerando 19.

[39] Ver, por exemplo, o Acórdão do Tribunal de Justiça de 23 de novembro de 2010 no processo C-145/09, Land Baden-Württemberg/Panagiotis Tsakouridis. ECLI:EU:C:2010:708, n.º 43, e o Acórdão do Tribunal de Justiça de 4 de abril de 2017 no processo C-544/15, Sahar Fahimian/Bundesrepublik Deutschland, ECLI:EU:C:2017:225, n.º 39.

[40] Ver, por exemplo, o Acórdão do Tribunal de Justiça de 22 de dezembro de 2008 no processo C-161/07, Comissão das Comunidades Europeias/República da Áustria, ECLI:EU:C:2008:759, n.º 35, e jurisprudência nele referida, e o Acórdão do Tribunal de Justiça de 26 de março de 2009 no processo C-326/07, Comissão das Comunidades Europeias/República Italiana, ECLI:EC:C:2009:193, n.º 70, e jurisprudência nele referida.

União Europeia, o princípio da proporcionalidade exige que as medidas adotadas sejam adequadas à realização do objetivo em causa e não vão além do necessário para esse fim[41].

Por razões de clareza, sublinha-se que a proibição dos requisitos de localização de dados não prejudica restrições já em vigor estabelecidas pela legislação da UE[42].

Acresce a isto que o Regulamento Livre Fluxo de Dados Não Pessoais não impõe quaisquer obrigações às empresas nem limita a sua liberdade contratual no atinente à decisão do local de tratamento dos seus dados.

Os Estados-Membros são obrigados a disponibilizar publicamente, num **ponto de informação nacional em linha único** (sítios Web nacionais), informações pormenorizadas sobre todos os requisitos de localização de dados aplicáveis no seu território. Os Estados-Membros devem manter os respetivos pontos únicos de informação atualizados ou fornecer informações atualizadas a um ponto de informação central estabelecido ao abrigo de outro ato da UE[43]. Para conveniência das empresas e a fim de lhes disponibilizar o fácil acesso a informações pertinentes a nível da UE, a Comissão publicará ligações para estes pontos de informação no portal Your Europe[44].

3.2 Livre fluxo de dados pessoais

O Regulamento Geral sobre a Proteção de Dados[45] estabelece que «[a] livre circulação de dados pessoais não é restringida nem proibida por motivos relacionados com a proteção das pessoas singulares no que respeita ao tratamento de dados pessoais».

Se um Estado-Membro impuser requisitos de localização de dados pessoais por motivos que não a proteção de dados pessoais, estes requisitos terão de ser avaliados à luz das disposições relativas às liberdades fundamentais e às justificações para derrogações a essas liberdades que

41 Ver, por exemplo, o Acórdão do Tribunal de Justiça de 8 de julho de 2010 no processo C-343/09, Afton Chemical Limited/Secretary of State for Transport, ECLI:EU:C:2010:419, n.º 45, e jurisprudência nele referida.

42 Ver, por exemplo, o artigo 245.º, n.º 2, da Diretiva 2006/112/CE, de 28 de novembro de 2006, relativa ao sistema comum do imposto sobre o valor acrescentado, segundo o qual «[o]s Estados-Membros podem impor aos sujeitos passivos estabelecidos no seu território a obrigação de lhes comunicarem o local de armazenagem das faturas, quando este se situar fora do seu território». No entanto, esta obrigação deve ser lida em conjunto com o artigo 249.º, segundo o qual «[q]uando um sujeito passivo armazene as faturas emitidas ou recebidas por uma via eletrónica que garanta o acesso em linha aos dados e o local de armazenagem das faturas esteja situado num Estado-Membro diferente daquele em que está estabelecido, as entidades competentes do Estado-Membro em que o sujeito passivo está estabelecido têm, para efeitos da presente diretiva, o direito de aceder a essas faturas por via eletrónica, de as carregar e de as utilizar, dentro dos limites fixados pela regulamentação do Estado-Membro de estabelecimento do sujeito passivo e na medida em que necessitem de o fazer para efeitos de controlo».

43 Artigo 4.º, n.º 4, do Regulamento (UE) 2018/1807 do Parlamento Europeu e do Conselho, de 14 de novembro de 2018, relativo a um regime para o livre fluxo de dados não pessoais na União Europeia.

44 https://europa.eu/youreurope/index.htm.

45 Artigo 1.º, n.º 3, 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 (Regulamento Geral sobre a Proteção de Dados).

constam do Tratado sobre o Funcionamento da União Europeia[46,47] e na legislação pertinente da UE, tal como a Diretiva Serviços[48] e a Diretiva Comércio Eletrónico[49].

Exemplo:

Um ato legislativo nacional exige que as contas de salários estejam localizadas num determinado Estado-Membro por motivos relacionados o controlo regulamentar, por exemplo parte da autoridade fiscal nacional. Essa disposição nacional estaria excluída do âmbito de aplicação do artigo 1.º, n.º 3, do Regulamento Geral sobre a Proteção de Dados, visto que os motivos em causa são diversos da proteção de dados pessoais. Em vez disso, teria de ser avaliada à luz das disposições relativas às liberdades fundamentais e às justificações para derrogações a essas liberdades que constam do Tratado sobre o Funcionamento da União Europeia.

O Regulamento Geral sobre a Proteção de Dados[50] reconhece que os Estados-Membros podem impor condições, incluindo limitações, no que respeita ao tratamento de dados genéticos, dados biométricos ou dados relativos à saúde. No entanto, tal como referido no considerando 53, essas limitações nacionais não devem impedir a livre circulação de dados pessoais na UE, quando essas condições se aplicam ao tratamento transfronteiriço desses dados. Tal está em consonância com o artigo 16.º do Tratado sobre o Funcionamento da União Europeia, que constitui a base legal para a adoção de regras relativas ao direito à proteção de dados pessoais e à livre circulação desses dados.

3.3 Âmbito de aplicação do Regulamento Livre Fluxo de Dados Não Pessoais

Como já referido, o Regulamento Livre Fluxo de Dados Não Pessoais visa assegurar o livre fluxo de dados não pessoais «na União»[51]. Por conseguinte, não se aplica a operações de

[46] Versão consolidada do Tratado sobre o Funcionamento da União Europeia (JO C 326 de 26.10.2012, p. 47).

[47] Ver também o Acórdão do Tribunal de Justiça de 19 de junho de 2008 no processo C-319/06, Comissão das Comunidades Europeias/Grão-Ducado do Luxemburgo, ECLI:EU:C:2008:350, n.os 90 e 91: o Tribunal considerou que uma obrigação de manter à disposição e de conservar determinados documentos num Estado-Membro específico constitui uma restrição à livre prestação de serviços, não sendo suficiente a justificação de que essa obrigação permite «facilitar em geral o cumprimento da missão de fiscalização das autoridades».

[48] Diretiva 2006/123/CE do Parlamento Europeu e do Conselho, de 12 de Dezembro de 2006 , relativa aos serviços no mercado interno (JO L 376 de 27.12.2006, p. 36).

[49] Diretiva 2000/31/CE do Parlamento Europeu e do Conselho, de 8 de junho de 2000, relativa a certos aspetos legais dos serviços da sociedade de informação, em especial do comércio eletrónico, no mercado interno («Diretiva sobre o comércio eletrónico») (JO L 178 de 17.7.2000, p. 1).

[50] Artigo 9.º, n.º 4, 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 (Regulamento Geral sobre a Proteção de Dados).

[51] Ver o artigo 1.º do Regulamento (UE) 2018/1807 do Parlamento Europeu e do Conselho, de 14 de novembro de 2018, relativo a um regime para o livre fluxo de dados não pessoais na União Europeia.

tratamento realizadas fora da UE nem a requisitos de localização de dados relacionados com esse tratamento[52,53].

Por conseguinte, o âmbito de aplicação do regulamento limita-se, de acordo com o artigo 2.º, n.º 1, ao tratamento de dados eletrónicos que não sejam dados pessoais na UE:

a) Prestado como um serviço a utilizadores residentes ou estabelecidos na UE, independentemente de o prestador de serviços estar ou não estabelecido na UE; ou
b) Realizado por uma pessoa singular ou coletiva com residência ou estabelecimento na UE para as suas necessidades próprias.

Exemplos:

Artigo 2.º, n.º 1, alínea a), do Regulamento Livre Fluxo de Dados Não Pessoais:

- Um prestador de serviços de computação em nuvem estabelecido nos EUA presta os seus serviços de tratamento de dados a clientes com residência ou estabelecimento na UE. O prestador de serviços de computação em nuvem gere as suas atividades por intermédio de servidores localizados no território da UE, onde são armazenados ou tratados os dados dos seus clientes europeus. O prestador de serviços de computação em nuvem não tem obrigatoriamente de possuir infraestruturas situadas na UE, podendo, por exemplo, alugar espaço em servidores na UE. O Regulamento Livre Fluxo de Dados Não Pessoais é aplicável a esse tratamento de dados.
- Um prestador de serviços de computação em nuvem estabelecido no Japão disponibiliza os seus serviços a clientes europeus. As capacidades de tratamento do prestador de serviços, onde decorrem todas as atividades de tratamento de dados, estão localizadas no Japão. O Regulamento Livre Fluxo de Dados Não Pessoais não é aplicável neste caso, visto que todas as atividades de tratamento de dados decorrem fora da UE[54].

[52] Ver o considerando 15 do Regulamento (UE) 2018/1807 do Parlamento Europeu e do Conselho, de 14 de novembro de 2018, relativo a um regime para o livre fluxo de dados não pessoais na União Europeia.

[53] O conceito de «tratamento» é definido em termos gerais [artigo 3.º, ponto 2, do Regulamento (UE) 2018/1807 do Parlamento Europeu e do Conselho, de 14 de novembro de 2018, relativo a um regime para o livre fluxo de dados não pessoais na União Europeia] e, como realçado no considerando 17, o regulamento deverá aplicar-se ao tratamento de dados no sentido mais lato, englobando a utilização de todos os tipos de sistemas informáticos.

[54] Note-se que o Regulamento (UE) 2018/1807 do Parlamento Europeu e do Conselho, de 14 de novembro de 2018, relativo a um regime para o livre fluxo de dados não pessoais na União Europeia, não diz respeito a requisitos de localização de dados impostos pelos Estados-Membros ao armazenamento de dados não pessoais em países terceiros, pelo que os ordenamentos jurídicos nacionais podem incluir requisitos desse tipo. Por razões de clareza, sublinha-se que o Regulamento Geral sobre a Proteção de Dados se aplica ao tratamento de dados pessoais cujos titulares estejam na UE, efetuado por um responsável pelo tratamento ou subcontratante não estabelecido na UE, se as atividades de tratamento estiverem relacionadas com: a) a oferta de bens ou serviços a esses titulares de dados na União, independentemente da exigência de os titulares dos dados procederem a um pagamento; b) o controlo do seu comportamento, desde que esse comportamento tenha lugar na União (ver artigo 3.º, n.º 2, do Regulamento Geral sobre a Proteção de Dados).

Artigo 2.º, n.º 1, alínea b), do Regulamento Livre Fluxo de Dados Não Pessoais:

- Uma pequena empresa europeia em fase de arranque, situada no Estado-Membro A, decide alargar a sua atividade abrindo um estabelecimento no Estado-Membro B. Para minimizar os custos, essa empresa decide centralizar o armazenamento e o tratamento de dados do novo estabelecimento no seu servidor que está localizado no Estado-Membro A. Os Estados-Membros não podem proibir esses esforços de centralização informática, salvo quando tal se justifique por motivos de segurança pública e no respeito do princípio da proporcionalidade.

Embora o Regulamento Livre Fluxo de Dados Não Pessoais não seja aplicável se todas as atividades de tratamento de dados não pessoais forem realizadas fora da UE, o Regulamento Geral sobre a Proteção de Dados deve ser respeitado quando os conjuntos de dados incluem dados pessoais. Em particular, as regras em matéria de transferência de dados pessoais para países terceiros ou organizações internacionais previstas no Regulamento Geral sobre a Proteção de Dados têm de ser sempre respeitadas[55].

3.4 Atividades relacionadas com a organização interna dos Estados-Membros

O Regulamento Livre Fluxo de Dados Não Pessoais não obriga os Estados-Membros a externalizar a prestação de serviços relacionados com dados não pessoais que os próprios pretendam prestar ou organizar por meios que não contratos públicos[56].

O artigo 2.º, n.º 3, segundo parágrafo, do Regulamento Livre Fluxo de Dados Não Pessoais refere que:

«O presente regulamento é aplicável sem prejuízo das disposições legislativas, regulamentares e administrativas relativas à **organização interna** dos Estados-Membros e que atribuem às autoridades públicas e aos organismos regidos pelo direito público definidos no artigo 2.º, n.º 1, ponto 4, da Diretiva 2014/24/UE[57] poderes e responsabilidades para o **tratamento de**

[55] No respeitante às transferências de dados pessoais para países terceiros, consultar a página Web da Comissão — https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/obligations/what-rules-apply-if-my-organisation-transfers-data-outside-eu_pt; e a Comunicação da Comissão ao Parlamento Europeu e ao Conselho — Intercâmbio e proteção de dados pessoais num mundo globalizado (COM/2017/07 final), disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX:52017DC0007. No que respeita ao Japão, a Comissão adotou a sua decisão de adequação em 23 de janeiro de 2019, a qual permite a livre circulação de dados pessoais entre as duas economias, assente em sólidas garantias quanto à sua proteção.

[56] Considerando 14 do Regulamento (UE) 2018/1807 do Parlamento Europeu e do Conselho, de 14 de novembro de 2018, relativo a um regime para o livre fluxo de dados não pessoais na União Europeia.

[57] O artigo 2.º, n.º 1, ponto 4, da Diretiva 2014/24/UE do Parlamento Europeu e do Conselho, de 26 de fevereiro de 2014, relativa aos contratos públicos e que revoga a Diretiva 2004/18/CE (JO L 94 de 28.3.2014, p. 65) define «organismos de direito público» como «organismos que apresentem todas as seguintes características: a) [f]oram criados para o fim específico de satisfazer necessidades de interesse geral, sem caráter industrial ou comercial; b) [t]êm personalidade jurídica; e c) [s]ão maioritariamente financiados pelo Estado, por autoridades regionais ou locais ou por outros organismos de direito público, ou a sua gestão está sujeita a controlo por parte dessas autoridades ou desses organismos, ou mais de metade dos membros nos seus órgãos de

dados sem remuneração contratual do setor privado, nem das disposições legislativas, regulamentares e administrativas dos Estados-Membros que preveem a aplicação desses poderes e dessas responsabilidades.»[58]

Podem existir interesses legítimos que justifiquem a opção pela prestação de serviços de tratamento de dados «por si próprio», tais como a «internalização» ou acordos mútuos entre administrações públicas. São exemplos típicos a utilização de uma «nuvem governamental» ou a designação, por parte de um governo, de uma agência informática centralizada responsável pela prestação de serviços de tratamento de dados às instituições e aos organismos públicos.

Todavia, o Regulamento Livre Fluxo de Dados Não Pessoais incentiva os Estados-Membros a ter em conta a eficiência económica e outros benefícios decorrentes do recurso a prestadores de serviços externos[59,60]. Assim que as autoridades nacionais decidam «externalizar» o tratamento de dados com remuneração contratual do setor privado, e esse tratamento tenha lugar na UE, o mesmo passa a estar abrangido pelo Regulamento Livre Fluxo de Dados Não Pessoais, o que significa que o princípio do livre fluxo de dados não pessoais é aplicável às práticas gerais e administrativas das autoridades nacionais. Nomeadamente, estas devem abster-se de impor restrições em matéria de localização de dados, por exemplo, em procedimentos de concursos públicos[61].

4 Estratégias de autorregulação que apoiam o livre fluxo de dados

A autorregulação contribui para a inovação e a confiança entre os intervenientes no mercado e tem características que lhe permitem responder melhor às alterações do mercado. A presente secção apresenta uma panorâmica das iniciativas de autorregulação para o tratamento de dados pessoais e não pessoais.

4.1 Portabilidade de dados e mudança entre prestadores de serviços de computação em nuvem

Um dos objetivos do Regulamento Livre Fluxo de Dados Não Pessoais é evitar práticas de vinculação a um prestador de serviços. Estas práticas ocorrem quando os utilizadores não podem mudar de prestador de serviços porque os seus dados estão «bloqueados» no sistema

administração, direção ou fiscalização são designados pelo Estado, pelas autoridades regionais ou locais ou por outros organismos de direito público».

[58] O considerando 13 do Regulamento (UE) 2018/1807 do Parlamento Europeu e do Conselho, de 14 de novembro de 2018, relativo a um regime para o livre fluxo de dados não pessoais na União Europeia refere que o regulamento não prejudica o disposto na Diretiva 2014/24/UE.

[59] Considerando 14 do Regulamento (UE) 2018/1807 do Parlamento Europeu e do Conselho, de 14 de novembro de 2018, relativo a um regime para o livre fluxo de dados não pessoais na União Europeia.

[60] Entende-se por «prestador de serviços externo» uma entidade que não seja um «organismos de direito público», na aceção do artigo 2.º, n.º 1, ponto 4, da Diretiva 2014/24/UE do Parlamento Europeu e do Conselho, de 26 de fevereiro de 2014, relativa aos contratos públicos e que revoga a Diretiva 2004/18/CE (JO L 94 de 28.3.2014, p. 65).

[61] Considerando 13 do Regulamento (UE) 2018/1807 do Parlamento Europeu e do Conselho, de 14 de novembro de 2018, relativo a um regime para o livre fluxo de dados não pessoais na União Europeia.

de um determinado prestador, por exemplo devido a formatos específicos dos dados ou acordos contratuais, não podendo ser transferidos para fora do sistema informático do prestador de serviços em causa. A ausência de entraves à portabilidade de dados é importante para permitir aos utilizadores a livre escolha entre prestadores de serviços de tratamento de dados e, assim, garantir a concorrência efetiva no mercado.

A portabilidade de dados entre empresas está a tornar-se cada vez mais importante numa vasta gama de indústrias digitais, incluindo os serviços de computação em nuvem.

Nos termos do artigo 6.º do Regulamento Livre Fluxo de Dados Não Pessoais, a Comissão deve incentivar e viabilizar a elaboração de códigos de conduta de autorregulação a nível da UE («códigos de conduta»), a fim de contribuir para uma economia dos dados competitiva. O artigo constitui uma base para que o setor elabore códigos de conduta de autorregulação relativos à mudança de prestador de serviços e à portabilidade de dados entre diferentes sistemas informáticos.

Há um conjunto de aspetos a ter em conta na elaboração desses códigos de conduta relativos à portabilidade de dados, nomeadamente:

- As **melhores práticas** para facilitar a mudança de prestador de serviços e a portabilidade de dados num formato estruturado, comum e legível por máquina;
- Os **requisitos mínimos de informação** para garantir que os utilizadores profissionais recebam, antes de assinarem um contrato de tratamento de dados, informações suficientemente pormenorizadas e claras relativamente aos processos, requisitos técnicos, prazos e encargos aplicáveis no caso de um utilizador profissional pretender mudar para outro prestador de serviços ou aplicar a portabilidade dos dados para os seus próprios sistemas informáticos;
- As **abordagens relativas a sistemas de certificação** que permitam uma melhor comparação entre serviços de computação em nuvem; e
- Os **roteiros de comunicação** que sensibilizem para a existência dos códigos de conduta.

No atinente ao mercado de serviços de computação em nuvem, a Comissão começou por facilitar os trabalhos dos grupos de trabalho de partes interessadas nos serviços de computação em nuvem no mercado único digital, os quais reúnem peritos e utilizadores profissionais desses serviços, incluindo pequenas e médias empresas. Nesta fase, um subgrupo está a elaborar códigos de conduta de autorregulação relativos à portabilidade de dados e à mudança de prestador de serviços de computação em nuvem (grupo de trabalho SWIPO)[62], e um outro está a trabalhar no sentido de criar um regime de certificação da segurança dos serviços de computação em nuvem (grupo de trabalho CSPCERT)[63].

[62] Grupo de trabalho para a mudança de prestador de serviços de computação em nuvem e a portabilidade de dados.

[63] Grupo de trabalho para a certificação europeia de prestadores de serviços de computação em nuvem. Ver também o ponto 4.3.

O grupo de trabalho SWIPO está a elaborar códigos de conduta que abrangem todo o espetro de serviços de computação em nuvem: infraestrutura como serviço (IaaS), plataforma como serviço (PaaS) e *software* como serviço (Saas).

A Comissão prevê que os diferentes códigos de conduta sejam complementados por **cláusulas contratuais modelo**[64]. Estas permitiriam a necessária especificidade técnica e jurídica durante a adoção e aplicação prática dos códigos de conduta, o que seria sobremaneira importante para as pequenas e médias empresas. Prevê-se que a redação das cláusulas contratuais modelo se siga à elaboração dos códigos de conduta (que deverão estar prontos em 29 de novembro de 2019).

Em consonância com o artigo 8.º do Regulamento Livre Fluxo de Dados Não Pessoais, a Comissão avaliará a execução do regulamento até 29 de novembro de 2022. Esse exercício permitirá avaliar: i) o impacto do regulamento no livre fluxo de dados na Europa, ii) a aplicação do regulamento, especialmente no tocante aos conjuntos mistos de dados, iii) a magnitude da revogação efetiva, por parte dos Estados-Membros, de restrições injustificadas em matéria de localização de dados, iv) o efeito útil no mercado dos códigos de conduta no domínio da portabilidade de dados e da mudança de prestador de serviços de computação em nuvem.

Conceito de portabilidade e interação com o Regulamento Geral sobre a Proteção de Dados

Ambos os regulamentos[65] se referem à portabilidade de dados e ao objetivo de facilitar essa portabilidade entre ambientes informáticos, ou seja, entre sistemas de diferentes prestadores de serviços ou para sistemas locais. Tal evita a vinculação a um prestador de serviços e promove a concorrência entre prestadores de serviços. No entanto, os regulamentos divergem na sua abordagem à portabilidade no que se refere à relação entre os grupos de interesse visados e à natureza jurídica das disposições.

O direito à portabilidade de dados pessoais, tal como estabelecido no artigo 20.º do Regulamento Geral sobre a Proteção de Dados, centra-se na relação entre o titular dos dados e o responsável pelo tratamento. Diz respeito aos direitos do titular dos dados, nomeadamente de receber os dados pessoais que tenha fornecido ao responsável pelo tratamento, num formato estruturado, de uso corrente e de leitura automática, e de os transmitir a outro responsável pelo tratamento ou de os transferir para as suas próprias capacidades de armazenamento, sem que o responsável a quem os dados pessoais foram fornecidos o possa

64 Ver o considerando 30 do Regulamento (UE) 2018/1807 do Parlamento Europeu e do Conselho, de 14 de novembro de 2018, relativo a um regime para o livre fluxo de dados não pessoais na União Europeia.

65 Artigo 6.º do Regulamento (UE) 2018/1807 do Parlamento Europeu e do Conselho, de 14 de novembro de 2018, relativo a um regime para o livre fluxo de dados não pessoais na União Europeia, e artigo 20.º 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 (Regulamento Geral sobre a Proteção de Dados).

impedir[66]. Habitualmente, nesta relação os titulares dos dados são consumidores de diversos serviços em linha que pretendem mudar para outro prestador desses serviços.

O artigo 6.º do Regulamento Livre Fluxo de Dados Não Pessoais não estabelece o direito de os utilizadores profissionais aplicarem a portabilidade de dados, mas segue uma abordagem de autorregulação, assente em códigos de conduta adotados pela indústria. Simultaneamente, visa situações em que um utilizador profissional tenha externalizado o tratamento dos seus dados a um terceiro que presta serviços de tratamento de dados[67]. Nos termos do artigo 3.º, ponto 8, do Regulamento Livre Fluxo de Dados Não Pessoais, o conceito de «utilizador profissional» engloba pessoas singulares ou coletivas, incluindo autoridades públicas ou organismos regidos pelo direito público, que utilizem ou solicitem um serviço de tratamento de dados para fins relacionados com as suas atividades comerciais, empresariais ou artesanais, ou com as suas tarefas profissionais.

Na prática, o conceito de portabilidade utilizado no artigo 6.º do Regulamento Livre Fluxo de Dados Não Pessoais diz respeito às interações a nível empresarial entre um utilizador profissional (o qual, nos casos que incluem o tratamento de dados pessoais, pode ser considerado um «responsável pelo tratamento» na aceção do Regulamento Geral sobre a Proteção de Dados) e um prestador de serviços (de igual modo passível de ser considerado «subcontratante» nesses casos).

Apesar das diferenças, podem surgir situações em que a portabilidade de dados estará abrangida simultaneamente pelo Regulamento Livre Fluxo de Dados Não Pessoais e pelo Regulamento Geral sobre a Proteção de Dados, no respeitante a conjuntos mistos de dados.

Exemplo:

Uma empresa que utiliza um serviço de computação em nuvem decide mudar de prestador desses serviços e aplicar a portabilidade de todos os dados para o novo prestador de serviços. O contrato celebrado entre o cliente e o prestador de serviços de computação em nuvem prevê cláusulas relativas à mudança de prestador de serviços e à portabilidade de dados. Se o prestador inicial de serviços de computação em nuvem adotar os códigos de conduta elaborados ao abrigo do Regulamento Livre Fluxo de Dados Não Pessoais, a portabilidade de dados terá de ser aplicada em conformidade com os requisitos especificados nesses códigos.

Se os conjuntos de dados a transmitir incluírem dados pessoais, o processo de portabilidade terá de respeitar todas as disposições pertinentes do Regulamento Geral sobre a Proteção de

[66] Conforme referido pelo Grupo de Trabalho do Artigo 29.º no documento *Orientações sobre o direito à portabilidade dos dados* (WP 242 rev.01), adotado em 13 de dezembro de 2016, com a última redação que lhe foi dada em 5 de abril de 2017.

[67] Ver o considerando 29 do Regulamento (UE) 2018/1807 do Parlamento Europeu e do Conselho, de 14 de novembro de 2018, relativo a um regime para o livre fluxo de dados não pessoais na União Europeia, segundo o qual: «[e]mbora os consumidores individuais beneficiem do direito da União em vigor [ou seja, o Regulamento Geral sobre a Proteção de Dados], a possibilidade de mudar de prestador de serviços não é facilitada aos utilizadores no exercício das suas atividades comerciais ou profissionais».

Dados, nomeadamente garantindo que o novo prestador de serviços de computação em nuvem cumpre os requisitos aplicáveis, por exemplo em matéria de segurança[68].

Exemplo:

Se um banco decidir mudar de prestador de serviços de gestão de relacionamento com clientes (CRM), é possível que seja necessário transferir alguns dados (pessoais e não pessoais) do anterior prestador de serviços para o novo. Esses dados ficariam, então, sujeitos a diversos requisitos regulamentares, alguns decorrentes do Regulamento Geral sobre a Proteção de Dados e outros do Regulamento Livre Fluxo de Dados Não Pessoais.

4.2 Códigos de conduta e sistemas de certificação relativos à proteção dos dados pessoais

Podem ser utilizados códigos de conduta e sistemas de certificação para demonstrar conformidade com as obrigações decorrentes do Regulamento Geral sobre a Proteção de Dados (ver artigo 24.º, n.º 3, e artigo 28.º, n.º 5).

De acordo com o artigo 40.º, n.º 1, e o artigo 42.º, n.º 1, do Regulamento Geral sobre a Proteção de Dados, os Estados-Membros, as autoridades de controlo, o Comité Europeu para a Proteção de Dados e a Comissão devem promover a elaboração de códigos de conduta e a criação de procedimentos de certificação em matéria de proteção de dados por parte da indústria.

As associações e outros organismos que representem uma categoria específica de responsáveis pelo tratamento ou de subcontratantes podem preparar um código de conduta para o seu setor. Deve ser apresentado um projeto do código à respetiva autoridade de controlo competente, para aprovação[69]. Se o projeto de código de conduta estiver relacionado com atividades de tratamento efetuadas em diversos Estados-Membros, a autoridade de controlo tem de o apresentar ao Comité Europeu para a Proteção de Dados antes de o aprovar. O Comité emitirá o seu parecer sobre a conformidade do projeto de código com o Regulamento Geral sobre a Proteção de Dados.

O Comité Europeu para a Proteção de Dados publicou as suas Orientações 1/2019 sobre códigos de conduta e organismos de supervisão no âmbito do Regulamento Geral sobre a Proteção de Dados[70]. Este documento inclui informações sobre a elaboração de códigos de

[68] Conforme referido pelo Grupo de Trabalho do Artigo 29.º no documento *Parecer 05/2012 sobre a computação em nuvem*, adotado em 1 de julho de 2012 (WP 196), que especifica a posição e as obrigações dos utilizadores e prestadores de serviços de computação em nuvem no que respeita ao tratamento de dados pessoais.

[69] Ver o artigo 40.º, n.º 5, e o artigo 55.º 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 (Regulamento Geral sobre a Proteção de Dados).

[70] Comité Europeu para a Proteção de Dados: *Orientações 1/2019 sobre códigos de conduta e organismos de supervisão no âmbito do Regulamento (UE) 2016/679*, adotadas em 12 de fevereiro de 2019; versão para

conduta, os critérios para a sua aprovação e outras informações úteis. De igual modo, o Comité Europeu para a Proteção publicou as Orientações 1/2018 sobre a certificação e a seleção de critérios de certificação em conformidade com os artigos 42.º e 43.º do Regulamento Geral sobre a Proteção de Dados, que disponibilizam informações sobre os procedimentos de certificação no âmbito do referido regulamento, bem como sobre a elaboração e aprovação de critérios de certificação[71].

Exemplos de códigos de conduta elaborados pelo setor da computação em nuvem:

O **Código de Conduta para a Computação em Nuvem na UE**, cuja preparação foi facilitada pela Comissão, foi elaborado em colaboração com o Grupo Seleto da Indústria de Computação em Nuvem (C-SIG) com base na Diretiva Proteção de Dados[72] e, posteriormente, no Regulamento Geral sobre a Proteção de Dados. O Código de Conduta para a Computação em Nuvem na UE abrange todo o espetro de serviços de computação em nuvem: *software* como serviço (Saas), plataforma como serviço (PaaS) e infraestrutura como serviço (IaaS)[73].

O **Código de Conduta dos Prestadores de Serviços de Infraestruturas para a Computação em Nuvem na Europa (CISPE)**[74] centra-se nos prestadores de IaaS. O Código de Conduta dos CISPE é composto por requisitos relativos aos prestadores de IaaS que atuam como subcontratantes para o tratamento de dados no âmbito do Regulamento Geral sobre a Proteção de Dados. Estabelece igualmente disposições sobre a estrutura de governação para a adoção e aplicação do código.

O **Código de Conduta para o Cumprimento do RGPD, da Cloud Security Alliance**, visa todas as partes interessadas do setor da computação em nuvem e abrangidas pela legislação europeia em matéria de dados pessoais, tais como prestadores, clientes e potenciais clientes, auditores e corretores de serviços de computação em nuvem. O código de conduta abrange todo o espetro de prestadores de serviços de computação em nuvem[75].

---

consulta pública, disponível em linha no seguinte endereço: https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-12019-codes-conduct-and-monitoring-bodies-under_pt.

[71] Comité Europeu para a Proteção de Dados: *Orientações 1/2018 sobre a certificação e a seleção de critérios de certificação em conformidade com os artigos 42.º e 43.º do Regulamento (UE) 2016/679*, adotadas em 23 de janeiro de 2019, disponíveis em linha no seguinte endereço: https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-12018-certification-and-identifying-certification_pt.

[72] 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 (data de fim de validade: 24 de maio de 2018).

[73] Para mais informações sobre o Código de Conduta para a Computação em Nuvem na UE, consultar: https://eucoc.cloud/en/home.html.

[74] Para mais informações sobre o Código de Conduta dos CISPE, consultar: https://cispe.cloud/code-of-conduct/.

[75] Para mais informações sobre o Código de Conduta da CSA, consultar: https://gdpr.cloudsecurityalliance.org/.

4.3 Promover a confiança no tratamento transfronteiriço de dados — certificação da segurança

Tal como referido no considerando 33 do Regulamento Livre Fluxo de Dados Não Pessoais, a promoção da confiança na segurança do tratamento transfronteiriço de dados deverá reduzir a tendência dos intervenientes no mercado e do setor público para utilizar a localização de dados como fator de salvaguarda dos dados. Juntamente com o pacote Cibersegurança proposto pela Comissão em 2017[76], o grupo de trabalho CSPCERT está a preparar recomendações para efeitos do estabelecimento de um sistema europeu de certificação de serviços de computação em nuvem, que apresentará à Comissão. Esse sistema tem potencial para facilitar a livre circulação de dados, permitir uma melhor comparabilidade entre serviços de computação em nuvem e promover a adoção desses serviços. A Comissão poderá incumbir a ENISA — Agência da União Europeia para a Cibersegurança de elaborar uma proposta de sistema, em conformidade com as disposições pertinentes do Regulamento Cibersegurança[77]. Esse sistema pode visar dados pessoais e dados não pessoais. Além do Regulamento Cibersegurança, e tal como salientado no ponto 4.2, é igualmente possível utilizar o RGPD para demonstrar a existência de salvaguardas adequadas em matéria de segurança dos dados[78].

Observações finais

A segurança jurídica e a confiança no tratamento de dados são fatores essenciais para que a UE seja capaz de explorar ao máximo o potencial de utilização dos dados, criando cadeias de valor entre setores e além-fronteiras. Os dois regulamentos garantem esses objetivos e visam permitir a livre circulação de dados. Em conjunto, o Regulamento Livre Fluxo de Dados Não Pessoais e o Regulamento Geral sobre a Proteção de Dados constituem a base para o livre fluxo de todos os dados no interior da União Europeia e para uma economia europeia dos dados altamente competitiva.

[76] Para mais informações, consultar: https://ec.europa.eu/digital-single-market/en/cyber-security.

[77] Regulamento do Parlamento Europeu e do Conselho, de 17 de abril de 2019, relativo à ENISA, a «Agência da União Europeia para a Cibersegurança», e à certificação da cibersegurança das tecnologias da informação e comunicação, e que revoga o Regulamento (UE) n.º 526/2013 («Regulamento Cibersegurança»).

[78] Ver o considerando 74 do Regulamento Cibersegurança.