REVISTA ELECTRÓNICA DE DIREITO

RED

Faz sentido que uma empresa transfira a sua sede ou estabelecimento por causa do Regulamento Geral sobre a Proteção de Dados?

Does it make sense for a company to move its headquarters or establishment because of the General Data Protection Regulation?

Benedita Cunha Pinto

Advogada na PTCS – Pinheiro Torres, Cabral, Sousa e Silva & Associados

Avenida da Boavista, 2300, 2.º, 4100-118, Porto, Portugal

beneditacfcunhapinto@gmail.com

https://orcid.org/0000-0002-6754-469X

Setembro de 2021

RESUMO: O presente artigo tem como objetivo averiguar se a transferência de sede, ou mesmo de estabelecimento, se pode justificar por causa do Regulamento Geral sobre a Proteção de Dados (Regulamento (UE) 2016/679, de 27 de abril de 2016). Numa primeira fase, abordamos em detalhe o âmbito de aplicação territorial do RGPD de acordo com o critério do estabelecimento e critério da destinação. Em seguida, apontamos algumas limitações de execução do referido Regulamento bem como algumas motivações que podem levar uma empresa a ponderar transferir a sua sede social para um país fora do Espaço Económico Europeu (EEE) ou optar, simplesmente, por recorrer à migração do estabelecimento. Neste contexto, aproveitaremos para abordar dois mecanismos de execução do RGPD – Designação de um Representante no EEE e Cláusulas Contratuais-tipo – por se revelarem matérias de grande interesse prático para as empresas. Por fim, faremos algumas propostas no sentido de prevenir possíveis cenários de transferência de estabelecimento.

PALAVRAS-CHAVE: Forum Shopping; Proteção de Dados; Âmbito Territorial; Estabelecimento; Cláusulas Contratuais-tipo; Representante.

ABSTRACT: The article aims to make an analysis of the issue of the transfer of headquarters or even of the establishment because of the General Data Protection Regulation (Regulation (EU) 2016/679 of 27 April 2016). In a first phase we approach in detail the territorial scope of the GDPR in accordance with the establishment criterion and the targeting criterion. Then, we point out some limitations related to the execution of the aforementioned Regulation, as well as some reasons that may lead a company to consider transferring its registered office to a country outside the European Economic Area (EEA) or, simply, opting to resort to establishment migration. In this context, we use to address two mechanisms for implementing the GDPR – Designation of a Representative in the EEE and Standard Contractual Clauses – as they reveal matters of great practical interest to companies. Finally, we will make some proposals towards a possible prevention of establishment migration.

KEY WORDS: Forum Shopping; Data Protection; Territorial Scope; Establishment; Standard Contractual Clauses; Representative.

SUMÁRIO:

1. Introdução. Formulação do problema

O progresso tecnológico foi o grande impulsionador para a criação de um regime europeu unificado relativo à proteção de dados – Regulamento Geral sobre a Proteção de Dados (adiante apenas "*RGPD*"[1] ou "*Regulamento*"). A tecnologia, especialmente aquela que se baseia na Internet, constitui o veículo facilitador da "*galopante*" transmissão de dados a pessoas não autorizadas, numa fração de segundo e muitas vezes sem que os seus titulares tenham conhecimento. Afinal, a Internet não conhece limites territoriais.

O RGPD visa, sobretudo, proteger os dados das pessoas singulares do tratamento que é feito por duas grandes categorias de sujeitos[2]: Estado e Empresas[3]. No século XXI, a ameaça aos direitos fundamentais não vem apenas do Estado. Nesse sentido, é dada grande importância à regulação das relações entre privados, nomeadamente a relação entre titulares de dados e pessoas coletivas privadas. Por outro lado, as empresas procuram gerir riscos e, nalguns casos, escapar à aplicação efetiva do RGPD. Nas páginas que se seguem procuraremos perceber em que medida faz sentido que as pessoas coletivas transfiram a sua sede ou mobilizem o seu estabelecimento para contornar a aplicabilidade do RGPD.

Como ponto de partida averiguaremos a questão da transferência de sede. É sabido que, as operações de transferência de sede ocorrem tipicamente como forma de uma empresa se subtrair à aplicação do Direito do Estado de origem, por razões fiscais, regulatórias ou, mesmo, em busca de mão-de-obra e tecnologia a preços mais acessíveis. Resta apurar se o RGPD também constitui mais um motivo para tal operação de mobilidade.

O que está em causa é essencialmente saber: Será permitida a transferência de sede? O RGPD oferece motivos para que uma Empresa queira transferir a sua sede? E motivos para a transferência de estabelecimento? Se sim, quais os motivos? Incluem-se entre estes a *"fuga"* à aplicação do RGPD? Nomeadamente, poder escolher estar sujeita a uma determinada Autoridade de Controlo (adiante apenas "ADC")? Ou então escolher a Lei Nacional de execução do RGPD que lhe seja mais favorável?

[1] Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados).
[2] Sem prescindir, lembramos que a proteção do RGPD não se circunscreve ao tratamento feito por estas duas categorias. Tem um âmbito mais alargado designadamente aquele que é feito por pessoas singulares ou jurídicas que processem dados pessoais que não se encontrem excluídos pelo artigo 2.º/2 do RGPD.
[3] Art. 4.º, n.º 18 RGPD: "*«Empresa», uma pessoa singular ou coletiva que, independentemente da sua forma jurídica, exerce uma atividade económica, incluindo as sociedades ou associações que exercem regularmente uma atividade económica*".

2. *Forum Shopping*. Breve enquadramento

A primeira interrogação prende-se com saber se o sistema económico europeu admite ou não *forum shopping* (em sentido amplo[4]).

Não apresento qualquer novidade ao responder afirmativamente a esta questão: o sistema europeu admite operações de mobilidade societária em busca do quadro normativo que melhor se adeque aos seus interesses. Aliás, o conceito "*forum shopping*" deixou de ter a carga negativa que outrora lhe era atribuída. Facto é que estas deslocações para um Estado que ofereça um regime legal mais favorável passaram a ser analisadas como operações assentes na autonomia privada, na liberdade de circulação e liberdade de estabelecimento (cfr. art. 49.º e 54.º do TFUE). Isto constitui jurisprudência consolidada como resulta, entre outros, dos acórdãos *Cartesio*[5], *National Grud Indus*[6], *Vale*[7] e *Polbud*[8].

Em todo o caso, o RGPD não dá relevância à sede, mas, sim, ao local onde se situa o estabelecimento que efetivamente realiza a atividade que justifica o tratamento de dados (independentemente de coincidir com a sede ou não). Acontece que, em muitas empresas, é na sede[9] que algumas vezes acaba por se realizar este real tratamento de dados e onde são tomadas as decisões sobre as finalidades de tratamento. Pelo que, nestes casos, poderá fazer sentido transferir a sede (*forum shopping*). Dito com rigor: averiguaremos a eventual utilidade da migração do estabelecimento, pelo que apenas em alguns casos poderá haver lugar a *forum shopping*.

3. A aplicabilidade direta do RGPD. O âmbito territorial (art. 3.º)

3.1. Critério do estabelecimento

Conforme disposto no n.º 1 do artigo 3.º do RGPD[10]: "*O presente regulamento aplica-se ao tratamento de dados pessoais efetuado no contexto das atividades de um estabelecimento de*

[4] Em rigor: não nos referiremos apenas a *forum shopping* em sentido estrito, mas em sentido amplo, incluindo *law shopping*. De forma simples, podemos definir *forum shopping* em sentido amplo como: a circunstância de uma sociedade transferir a sua sede para outro Estado Membro ou mesmo ter sido constituída num determinado Estado Membro, de acordo com a legislação ou jurisdição que seja mais favorável às pretensões da sociedade.
[5] Acórdão do TJUE C-210/06, 16.12.2008 (ECLI:EU:C:2008:723), parágrafo 123.
[6] Acórdão do TJUE C-371/10, 29.11.2011, (ECLI:EU:C:2011:785), parágrafo 84.
[7] Acórdão do TJUE C-378/10, 12.07.2012, (ECLI:EU:C:2012:440), parágrafo 62.
[8] Acórdão do TJUE C-106/16, 25.10.2017 (ECLI:EU:C:2017:804), parágrafo 3; Veja-se ainda EUROPEAN PARLIAMENT, "The Polbud judgment and the freedom of establishment for companies in the European Union: problems and perspectives", *in* STUDY For the JURI Committee, Policy Department for Citizens' Rights and Constitutional Affairs Directorate General for Internal Policies of the Union, PE 608.833 - October 2018, *in* https://www.europarl.europa.eu/RegData/etudes/STUD/2018/608833/IPOL_STU(2018)608833_EN.pdf .
[9] Talvez ocorra maioritariamente nos casos em que a sede corresponde à sede real e, portanto, ao centro de administração e controlo.
[10] Quanto a este artigo 3.º, n.º 1 poderemos dizer que permanece igual ao já disposto na Diretiva 95/46/CE. Contudo, a diferença estará no facto de ter sido alargado aos subcontratantes (*processors*) – e não apenas à figura dos responsáveis (*controllers*) – que passarão a estar diretamente vinculados às obrigações previstas no RGPD.

um responsável pelo tratamento ou de um subcontratante situado no território da União, independentemente de o tratamento ocorrer dentro ou fora da União." [sublinhado nosso]

Resulta, pois, que qualquer estabelecimento situado na União estará obrigado a respeitar o Regulamento, independentemente de um determinado tratamento de dados ocorrer a nível nacional, transfronteiriço ou internacional[11]. Portanto, é requisito bastante para a aplicação do RGPD que o estabelecimento esteja situado em território da União, mesmo que o titular de dados se encontre num Estado Terceiro à União Europeia[12].

Apesar de o conceito de "*estabelecimento*"[13] não estar definido no artigo 4.º do Regulamento ("*Definições*"), o considerando 22 acaba por esclarecer que este não tem que coincidir com a sede social[14]. Poderá tratar-se de qualquer sucursal ou mesmo filial que faça um concreto tratamento de dados. O *estabelecimento* pressupõe o exercício efetivo de uma atividade com base numa instalação estável, sendo que a forma jurídica de tal estabelecimento não releva para o efeito[15].

A título de exemplo: Uma empresa com sede nos EUA tem uma filial em Portugal (UE). Apesar de ter sede nos EUA, é a filial que faz todo o tratamento de dados dos seus clientes, tanto para efeitos de execução dos contratos com os mesmos, como ainda para efeitos de envio de comunicações de marketing. A filial situada no território da União é um "*estabelecimento*" nos termos do artigo 3.º, n.º 1 – pelo que terá que ficar sujeita ao cumprimento das regras do RGPD.

---

[11] GUIDELINES 3/2018 on the territorial scope of the GDPR (Article 3) Version 2.1,12.11.2019, p. 5, in https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_3_2018_territorial_scope_after_public_consultation_en_1.pdf .

[12] Por uma questão de facilidade para o leitor acompanhar as disposições do RGPD, referir-me-ei muitas vezes apenas à "União Europeia". Contudo, em rigor, embora a letra do RGPD faça referência à União Europeia, o seu âmbito foi alargado por acordo ao Espaço Económico Europeu. O Espaço Económico Europeu (EEE) visa alargar o mercado interno da UE aos países da Zona Europeia de Comércio Livre (EFTA). Os atuais países da EFTA não pretendem aderir à UE. No entanto, a legislação da União Europeia relativa ao mercado interno passa a fazer parte da legislação dos países do EEE, *in* https://www.europarl.europa.eu/factsheets/pt/sheet/169/the-european-economic-area-eea-switzerland-and-the-north - Noruega, Liechenstein e Islândia.

[13] Cons. 22 do RGPD: O "estabelecimento" pressupõe o "exercício efetivo e real de uma atividade com base numa instalação estável". O estabelecimento desdobra-se em 3 elementos: i) estabilidade da instalação; ii) efetividade do exercício de uma atividade; iii) no contexto do exercício dessas atividades.

[14] PAUL VOIGT ET AL., *The EU General Data Protection Regulation (GDPR), A Practical Guide*, *in* Springer International Publishing, Switzerland, 2017, p. 22 ss*: "Flexible Concept of Establishment: Establishment implies the effective and real exercise of activity through stable arrangements*"; Acórdão do TJUE C-210/16, Wirtschaftsakademie, de 5.06.2018, (ECLI:EU:C:2018:388), parágrafo 54: *"estabelecimento (...) pressupõe o exercício efetivo e real de uma atividade mediante uma instalação estável e que a forma jurídica de tal estabelecimento, quer se trate de uma simples sucursal ou de uma filial com personalidade jurídica, não é determinante (Acórdão de 1 de outubro de 2015, Weltimmo, C-230/14, EU:C:2015:639, n.º 28 e jurisprudência aí referida).*"; Acórdão do TJUE C-230/14, Weltimmo, de 1.10.2015, (EU:C:2015:639), parágrafo 28 *"No que respeita, em primeiro lugar, ao conceito de «estabelecimento», há que recordar que o considerando 19 da Diretiva 95/46 enuncia que o estabelecimento no território de um Estado-Membro pressupõe o exercício efetivo e real de uma atividade mediante uma instalação estável e que a forma jurídica de tal estabelecimento, quer se trate de uma simples sucursal ou de uma filial com personalidade jurídica, não é determinante (acórdão Google Spain e Google, C-131/12, EU:C:2014:317, n.º 48). Este considerando precisa, por outro lado, que, quando no território de vários Estados-Membros estiver estabelecido um único responsável pelo tratamento, deve assegurar-se, nomeadamente para evitar que a legislação seja contornada, que cada um dos estabelecimentos cumpra as* obrigações impostas pela legislação nacional aplicável às respetivas atividades".

[15] Por esta razão, para efeitos deste estudo optei pelos termos "empresa" e "estabelecimento" ao invés de "sociedade" porque a forma jurídica do estabelecimento não é relevante nos termos do RGPD (cons. 22 RGPD).

Pensemos agora no seguinte caso: Uma empresa portuguesa desenvolveu um *software* dirigido a clientes do Brasil. A empresa portuguesa tratará dos dados destes titulares que se encontram fora da União no âmbito da prestação do serviço. Muito embora estes titulares não se encontrem na UE, o simples facto de existir um estabelecimento que faz tratamento de dados no território da União é razão para a aplicação do RGPD, nos termos do artigo 3.º, n.º 1.

Além disso, o RGPD aplica-se ao tratamento de dados pessoais por um responsável estabelecido, já não na União, mas num lugar em que se aplique o Direito de um Estado Membro por força do direito internacional público (art. 3.º, n.º 3 RGPD)[16].

Contudo, como veremos de seguida, o RGPD é aplicável diretamente, também, a determinados casos cujo estabelecimento não se encontre situado na União (art. 3.º, n.º 2 do RGPD).

3.2. Critério da destinação (*targeting*)

Os titulares de dados são pessoas singulares cuja informação pessoal *identificada ou identificável*[17] é merecedora de proteção. Assim sendo, estes sujeitos serão também titulares de direitos[18]. Contudo, o legislador não densifica o conceito de *titulares de dados*[19].

Para densificá-lo cumpre perceber quem é que o RGPD visa proteger. Estarão protegidos pelo RGPD todos os cidadãos de um Estado Membro da União? Estarão protegidos pelo RGPD todos aqueles que residam habitualmente num Estado Membro da União?

De forma simplificada, os titulares de dados que o RGPD visa proteger são:

a) Todas as pessoas singulares, independentemente de nacionalidade, estatuto, domicílio ou localização, cujo tratamento de dados seja efetuado por um responsável/subcontratante com estabelecimento *"situado no território da União"* (art. 3.º, n.º 1 RGPD);

b) Todas as pessoas singulares *"que se encontrem no território da União"* cujo tratamento de dados esteja relacionado com i) 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, e ii) o controlo do seu comportamento (art. 3.º, n.º 2 RGPD). [sublinhado nosso]

Relativamente ao critério do artigo 3.º, n.º 1 já aqui foi exposto o essencial. Cumpre agora analisar o critério encontrado no artigo 3.º, n.º 2. Pois bem, conforme mencionado no artigo 3.º, n.º 2, o RGPD também protege os dados dos *titulares que se encontrem no território da*

[16] Como exemplo: um posto consular de um Estado Membro da União que faça tratamento de dados é considerado um estabelecimento situado no território da União.
[17] Art 4.º, n.º 1 RGPD.
[18] Capítulo III – Direitos do Titular de Dados - do RGPD.
[19] O legislador limita-se a dar algumas orientações nos considerandos 23 e 24, embora de forma insuficiente.

União[20]. Dito isto, torna-se claro que o legislador não optou pelo *critério da nacionalidade*, nem pelo *critério da residência habitual*.

No entanto, este novo critério oferece problemas, não é simples e a dificuldade de aplicação prática é reveladora disso mesmo. Ora, se o *critério da residência habitual* é mais difuso do que o *critério da nacionalidade*, então, mais difuso e indefinido será o *critério dos que se encontrem no território da União*.

O legislador foi mais longe do que o critério da nacionalidade e do que o *critério da residência habitual*[21]. Um turista canadiano que passe um fim-de-semana no Algarve estará abrangido. A ambição do legislador seria encontrar um critério que incluísse, também, o *critério da residência habitual* e da *nacionalidade*. Mas, não foi feliz na sua redação e acabou por "*deixar escapar"* situações como as que abaixo se descrevem.

De facto, o *critério dos que se encontrem no território da União*[22] é bem mais abrangente do que o *critério da residência habitual*, tendo em conta que a generalidade dos que residem no território da União, em princípio, também se encontrarão neste território. Assim, o legislador quis abranger todos os *"residentes (temporários e permanentes), turistas, trabalhadores temporários, apátridas e quaisquer outros sujeitos"*[23] – v.g. o caso de um cidadão canadiano que vem passar dez dias de férias a Portugal (país da União). Nestes dias forneceu os seus dados a diversas empresas situadas em Portugal. O cidadão canadiano está protegido pelo RGPD, pois é um titular de dados que se encontra em território da União.

No que diz respeito ao *critério da nacionalidade*, não podemos afirmar que seja absorvido pelo critério apresentado pelo Regulamento, uma vez que nem todos os nacionais de um Estado da União se encontram no seu território – v.g. um cidadão Português que resida nos EUA (Estado Terceiro) e fornece os seus dados a empresas americanas. Neste caso, o simples facto de ser cidadão de um país da União não lhe confere qualquer proteção nos termos do RGPD.

Em rigor, no artigo 3.º, n.º 2, não existe uma conexão do titular de dados com a lei que mais se ajusta à sua identidade, mas, sim, uma conexão jurídico-económica entre o titular e o responsável[24]. Repare-se que o tratamento de dados tem que estar relacionado com a oferta de bens ou serviços e com o controlo de comportamentos. Portanto, este critério serve precisamente para proteger o funcionamento do mercado da UE. Isto, cada vez mais baseado

[20] Mais uma vez, irei referir-me à "União" por uma questão de facilidade, por proximidade à redação utilizada pelo legislador europeu. No entanto, não se esqueça que o conceito de "titulares de dados" para efeitos do RGPD foi alargado a todos os titilares de dados que se encontrem no EEE.
[21] LUÍS LIMA PINHEIRO, *Direito Internacional Privado, Direito de Conflitos – parte especial*, Vol. II, 4.ª Edição Refundida, Coimbra, Almedina, 2018, p. 42: "(...) tanto a nacionalidade, como o domicílio ou a residência habitual são elementos de conexão que, em princípio, exprimem uma ligação estreita com a pessoa em causa e asseguram uma continuidade das qualidades e situações jurídicas do estatuto pessoal*"*.
[22] Deixo aqui a nota de que inicialmente na versão portuguesa e espanhola podia ler-se: "*Residentes no território da União"* e "*que residan en la Unión*". Traduções erradas e que foram emendadas (a 19 de abril de 2018) em consonância com o que estava (e está) disposto nas restantes versões e que corresponde à redação que conhecemos hoje.
[23] A. BARRETO MENEZES CORDEIRO, *Direito da Proteção de Dados à Luz do RGPD e da lei n.º 58/2019*, Coimbra, Almedina, 2020, p. 96.
[24] PAUL CRAIG ET AL., "The Foundations of EU Data Protection Law*", Oxford Studies in European Law,* Orla Lynskey, *in* Oxford University Press, 2015, p. 51ss: *"Prioritizing Market integration*".

numa ideia de que o mercado europeu, para conciliar a *competitividade e segurança*, tem que: integrar uma dimensão digital e, a par disso, suscitar confiança, estabilidade e ainda proteção quanto ao tratamento dos dados dos titulares que são objeto do tratamento por parte daqueles estabelecimentos que com o mercado europeu queiram contratar[25].

O RGPD exige que as empresas sediadas fora da União apliquem as mesmas regras a que estão sujeitas as empresas sediadas na União, caso ofereçam bens e serviços relacionados com dados pessoais ou monitorizem o comportamento dos indivíduos na União. Pense-se na seguinte hipótese prática[26]: Uma cadeia de hotéis situada em Moçambique (estabelecimentos situados fora da UE) oferece os seus serviços através do seu *site* que está disponível em alemão. Apesar de não podermos qualificar como estabelecimento nos termos do artigo 3.º, n.º 1 – por não se situar em território da União – esta cadeia terá que atuar de acordo com o RGPD por dirigir os seus serviços a *titulares que se encontrem em território da União*[27] (3.º, n.º 2).

Podemos, pois, questionar a possibilidade de um Estado Europeu querer impor o Direito Europeu a comportamentos adotados por um Estado Terceiro cujos comportamentos afetem o direito à proteção de dados de um titular que se encontre na União (*princípio dos efeitos*).

[25] Muitas vezes estes titulares de dados coincidirão com o conceito de "*consumidor*" (cfr. art. 2.º Lei da Defesa do Consumidor; art. 1.º-B, al. b) da Lei 67/2003; art. 1.º/2/a) Diretiva 99/44/CE; cons. 21 e art. 2.º/2 da nova Diretiva 2019/771). A recente Diretiva 2019/770, 20 de Maio de 2019 – sobre certos aspetos relativos aos contratos de fornecimento de conteúdos e serviços digitais – é o espelho desta importante relação entre proteção de dados e o mercado europeu; Repare-se ainda no que escreve ALESSANDRA SILVEIRA/PEDRO FROUFE, "*Do mercado interno à cidadania de direitos, A proteção de dados pessoais como a questão jus-fundamental identitária dos nossos tempos" in UNIO, Eu Law Journal*, Vol. 4, N.º 2, Julho.2018: "Neste texto procuraremos demonstrar por que razão a proteção de dados pessoais converteu-se na questão jus-fundamental identitária dos nossos tempos. A proteção de dados pessoais adquiriu centralidade jurídico-constitucional não apenas porque o Mercado Único Digital converteu-se num interesse público primário a prosseguir – e a desejada circulação de pessoas, mercadorias, serviços e capitais implica o aumento do fluxo transfronteiriço de dados. Também não foi apenas porque a finalização do Mercado Único Digital requer um ambiente jurídico estável que estimule a inovação, combata a fragmentação do mercado e permita a competitividade em condições justas e equilibradas. Tal protagonismo jurídico-constitucional também não se prende apenas com a estimativa, certamente impressionante, de que o valor da economia dos dados subirá para 739 mil milhões de EUR até 2020, correspondendo a 4 % do PIB total da eu (ou seja, mais do dobro do valor atual) e o número de profissionais no setor dos dados passará de 6 milhões em 2016 para mais de 10 milhões até 2020.14 Então porquê? Ora, a proteção de dados pessoais converteu-se na questão jus-fundamental identitária dos nossos tempos para que o projeto do humanismo não se torne irrelevante*".*

[26] Este exemplo foi adaptado das Guidelines 3/2018 on the territorial scope of the GDPR (Article 3) Version 2.1, 12.November.2019, p. 7.

[27] Acórdão TJUE C-131/12, *Google Spain SL e Google Inc. contra Agencia Española de Protección de Datos (AEPD) e Mario Costeja González*, de 13.05.2014, (ECLI:EU:C:2014:317): podemos encontrar alguns indícios para determinar a intenção de fornecer serviços na UE: a) Utilização de referências específicas; b) Língua, moeda, possibilidade de encomendar na mesma língua, referência a clientes/utilizadores da União; As Guidelines 3/2018 on the territorial scope of the GDPR (Article 3) Version 2.1, 12.November.2019 (p. 18) também apresentam alguns indícios de uma atividade direcionada para o mercado europeu, como: a) a utilização de um nome de domínio que não seja o do País Terceiro em que a empresa está estabelecida, por exemplo, "*.de*" ou o uso de nomes de domínio neutros de nível superior, como "*.eu*", ou b) o responsável oferecer a entrega de mercadorias nos Estados-Membros da UE. Ainda com a seguinte ressalva: "*however, they should each be taken into account in any in concreto analysis in order to determine whether the combination of factors relating to the data controller's commercial activities can together be considered as an offer of goods or services directed at data subjects in the Union.*"; A propósito, note-se ainda que o "*targeting criterion*", assim denominado pelas das Guidelines 3/2018 on the territorial scope of the GDPR (Article 3) Version 2.1, 12.November.2019, não corresponde ao mesmo "*targeting criteria*" referido em diferentes decisões em matéria de Propriedade Intelectual. Em contraste do que consta no RGPD: a simples disponibilidade de acesso por um website de uma empresa de um Estado Terceiro a utilizadores de um Estado da UE não constitui violação de um direito protegido pela legislação vigente no Estado Terceiro.

Neste ponto, diria, antes, que o que se pretende é vincular as empresas que, por regra, tratam de dados pessoais com origem na UE ao Direito Europeu. Tudo assenta numa lógica de destino das atividades que tenham como *alvo a UE*.

E repare-se que esta solução de âmbito territorial com efeitos extraterritoriais parece estar a tornar-se uma tendência para legislador europeu. Olhemos, por exemplo, para o artigo 2.º da recente Proposta de Regulamento sobre as Regras de Harmonização da Inteligência Artificial[28]. Esta proposta também prevê a sua aplicação relativamente aos prestadores de serviços ou fornecedores de sistemas de Inteligência Artificial que atuem no mercado da União, independentemente de estas empresas estarem estabelecidas na União ou num País Terceiro. Ou o *Digital Services Act* – artigo 2.º. Afigura-se claro que esta tendência legislativa visa essencialmente garantir que a UE seja *líder mundial*[29] no desenvolvimento de um mercado digital *seguro, fiável e ético*[30] *[tradução nossa]*.

Especificamente, no caso do regime europeu de proteção de dados pretende-se assegurar que, quando os dados são processados por um estabelecimento fora da União, este regime os acompanha, se estende, para lá das fronteiras europeias. Atenta a realidade global em que vivemos – especialmente no que diz respeito às operações que ocorrem na Internet, desde motores de busca, *marketing*, comércio eletrónico e redes sociais – este acompanhamento dos dados por parte do regime europeu assume enorme relevância.

O objetivo é evitar que as pessoas singulares sejam privadas da proteção pelo simples facto de uma empresa ter estabelecimento fora da UE[31]. Chegou-se à conclusão que a estabilidade e segurança no mercado só é conseguida através desta extensão territorial que pretende cingir o acesso aos operadores de um País Terceiro que apresentem um nível de proteção de dados adequado e não sejam fonte de riscos para os titulares de dados da União.

---

[28] Brussels, 21.4.2021 COM(2021) 206 final, 2021/0106 (COD), Proposal for a Regulation of the European Parliament and of the Council, Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts, SEC(2021) 167 final - SWD(2021) 84 final - SWD(2021) 85 final.

[29] Expressão retirada *in* Brussels, 21.4.2021 COM(2021) 206 final, 2021/0106 (COD), Proposal for a Regulation of the European Parliament and of the Council, Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts, SEC(2021) 167 final - SWD(2021) 84 final - SWD(2021) 85 final, (p. 18) e utilizada no contexto do European Council, Special meeting of the European Council (1 and 2 October 2020) – Conclusions, EUCO 13/20, 2020, p. 6.

[30] Expressão retirada *in* Brussels, 21.4.2021 COM(2021) 206 final, 2021/0106 (COD), Proposal for a Regulation of the European Parliament and of the Council, Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts, SEC(2021) 167 final - SWD(2021) 84 final - SWD(2021) 85 final, p. 18. E que é transversal à segurança no desenvolvimento do Mercado Único Digital.

[31] GUIDELINES 3/2018 on the territorial scope of the GDPR (Article 3), Version 2.1, 12.November.2019, p. 4: "Article 3 of the GDPR reflects the legislator's intention to ensure comprehensive protection of the rights of data subjects in the EU and to establish, in terms of data protection requirement, a level playing field for companies active on the EU markets, in a context of worldwide data flows"; A este propósito leis-se também PEDRO ALBERTO DE MIGUEL ASENSIO, "Competencia y Derecho Aplicable em el Regulamento General sobre Protección de Datos de la Unión Europeia", *Revista Española de Derecho Internacional (REDI)*, Vol. 69 (1), Madrid, 2017, *in* http://www.revistaredi.es/wpcontent/uploads/2018/01/3_estudios_miguel_asensio_competencia_dcho_aplicable_en_reglamento_general.pdf .

3.3. Algumas conclusões

Nas palavras de Graça Canto Moniz[32]: *"(...) o artigo 3.º do RGPD pressupõe que o responsável pelo tratamento tem uma ligação substancial à UE, seja porque ali tem um estabelecimento seja porque trata os dados pessoais de titulares de dados aí localizados e as suas atividades são direcionadas para os mesmos ou, melhor dizendo, para o mercado da UE, para os seus consumidores ou para a "comunidade comercial da UE"*.

Por todo o exposto, fica, pois, demonstrado o vasto âmbito de aplicação direta do RGPD, que apenas depende da verificação do *critério do estabelecimento situado no território da União* – onde for efetuado o exercício real do tratamento, independentemente de corresponder ou não à sede social – ou do *critério dos titulares dos dados que se encontrem no território da União*[33].

Deste modo, não é uma deslocalização de sede ou mesmo de estabelecimento que permitirá uma empresa escapar ao amplo âmbito de aplicação do RGPD[34], sempre que uma empresa trate de dados de titulares que se encontrem na UE. [sublinhado nosso]

Ainda assim, vemos apenas um caso em que poderá ter interesse a mobilidade daquele estabelecimento que efetivamente realiza a atividade que justifica o tratamento de dados. Pelo que, como já vimos, pode passar ou não por uma transferência da sede social (*forum shopping*). Curiosamente, o caso a que nos referiremos não diz respeito ao artigo 3.º, n.º 2, nem tão pouco a casos que envolvam transferências internacionais subsequentes.

Relembremos aqui o caso da empresa portuguesa que desenvolve um software dirigido a clientes do Brasil (ponto 3.1.) e que, por sua vez, acaba por transferir estes dados para os seus parceiros também situados na União. Ora, temos um estabelecimento situado na UE, que processa dados de titulares que não se encontram na UE e que, frequentemente, realiza transferências transfronteiriças desses mesmos dados (transferências entre dois Estados Membros da UE). [sublinhado nosso] É sabido que este estabelecimento está sujeito à aplicação direta do RGPD, por via do artigo 3.º, n.º 1, só pelo simples facto de estar situado na UE. Numa situação como essa, a empresa portuguesa deve considerar a hipótese de uma

[32] GRAÇA CANTO MONIZ, "Finalmente: coerência no âmbito de aplicação do regime da União Europeia de proteção de dados pessoais! - O fim do enigma linguístico do artigo 3.º, n.º 2 do RGPD", *UNIO, Eu Law Journal*, Vol. 4, No. 2, Julho 2018, p. 127.

[33] Nas palavras de ALESSANDRA SILVEIRA/PEDRO FROUFE, "Do mercado interno à cidadania de direitos, A proteção de dados pessoais como a questão jus fundamental identitária dos nossos tempos", *in UNIO, EU Law Journal*, Vol. 4, No. 2, Julho 2018: "Ora, tem de ser assim porque a Internet não conhece limites territoriais – e a proteção de dados só resulta se for exercida de forma tendencialmente universal. Pode parecer exagerado – mas esta é a Europa que desejamos".

[34] V.g.: Um grupo empresarial com estabelecimento na Alemanha e nos EUA. O grupo empresarial apenas faz tratamento na UE. O grupo pondera transferir a sede da Alemanha (UE) para os EUA para que não se lhe aplique o RGPD. Contudo, conclui-se que é indiferente transferir a sua sede na medida em que o RGPD ser-lhe-á sempre aplicável. Se a sede fosse transferida para EUA (3.º/2) continuaria a dirigir os seus serviços a "titulares que se *encontrem na UE"*. Portanto, a transferência de sede pouco serve para que se não aplique o RGPD. Estando em causa dados de pessoas que se encontrem na UE este aplicar-se-á sempre.

operação de mobilidade do seu estabelecimento para um País Terceiro à União. Só assim o RGPD deixará de lhe ser aplicável[35].

4. A amplitude do âmbito de aplicação (*jurisdiction to prescribe*) e a limitação da execução do RGPD (*jurisdiction to execute*)

4.1. Jurisdiction to execute

Reconheça-se, em todo o caso, que a manifestação da extraterritorialidade[36] através de atos legislativos (*jurisdiction to prescribe*) e atos executivos (*jurisdiction to execute*) podem não *andar de braço dado*. Quero com isto dizer que a amplitude do âmbito de aplicação do Regulamento poderá levar a problemas de exequibilidade prática. Um Estado pode não ter capacidade para fazer respeitar as suas leis, ainda que estas se considerem aplicáveis.

Por essa razão e seguindo a lógica da proteção além-fronteiras, o RGPD prevê uma série de ferramentas para compensar a eventual ausência de um nível de proteção de dados adequado por parte de um País Terceiro[37]. Assim, o RGPD estabelece que cada empresa situada fora da União tem que designar um representante na União quando tenha intenções de operar no mercado europeu (arts. 4.º, n.º 17, 27.º, 58.º, n.º 2 e 83.º do RGPD)[38] – mecanismo relacionado com os casos de aplicabilidade direta do RGPD por força da extraterritorialidade presente no artigo 3.º, n.º 2 do RGPD – e ainda existe um regime de transferências internacionais de dados (art. 44.º e ss do RGPD) – mecanismo relativo à aplicabilidade indireta do RGPD – que pretende assegurar que as exigências de licitude, a proporcionalidade do

[35] E, claro, não é por vir a situar-se num País Terceiro e realizar transferências internacionais, ao invés de transfronteiriças, que estas transferências para os seus parceiros situados na UE terão que ser reguladas pelas cláusulas contratuais-tipo, uma vez que estas apenas dizem respeito a transferências de dentro para fora da UE.
[36] CHRISTOPHER KUNER, entre outros autores, entendem que o carácter extraterritorial do RGPD não se trata propriamente de uma novidade deste Regulamento. Basta para tanto pensar que já o Acórdão Google Spain e Google Inc contra AEPD e Mario Costeja (ECLI:EU:C:2014:317) – proferido ao tempo da Diretiva 95/46/CE – acabou por demonstrar a existência de uma natural extraterritorialidade (efeitos extraterritoriais) inerente à regulação em matéria de proteção de dados; Atenta à realidade em análise encontra-se um paralelismo com o direito da concorrência e o direito ambiental, assentes também no princípio dos efeitos; Leia-se também CHRISTOPHER KUNER, "Extraterritoriality and regulation of international data transfers in EU data protection law", *in International Data Privacy Law*, 5, 2015, p. 2-14.
[37] CHRISTOPHER KUNER, "Territorial Scope and Data Transfer Rules in the GDPR: Realising the EU's Ambition of Borderless Data Protection", *in Legal Studies Research Paper Series*, University of Cambridge, Faculty of Law, PAPER NO. 20/2021, APRIL 2021, p. 4: "EU data protection law has significant global influence, and territorial scope and data transfer rules have an impact on data processing in third countries".
[38] A obrigação de designar um representante corresponde a casos de aplicação direta do art. 3.º, n.º 2 do RGPD; O representante tem que executar as suas tarefas de acordo com o mandato recebido do responsável/subcontratante (fora da UE), nomeadamente no que respeita à cooperação com a Autoridade de Controlo competente. Tem que atuar de acordo com o mandato recebido pelo responsável/subcontratante fora da UE. O conceito de representante foi introduzido precisamente com o objetivo de facilitar a ligação e garantir a aplicação efetiva do RGPD contra responsáveis/subcontratantes não situados na EU, mas abrangidos pelo artigo 3.º, n.º 2 do RGPD. Facto que permite às Autoridades de Controlo iniciar um processo de execução através de um representante.

tratamento e os direitos dos titulares, se mantêm, mesmo quando os dados são transferidos para um País Terceiro[39].

Como se perceberá, aproveitamos para fazer uma breve nota sobre estes dois mecanismos, com especial destaque para o mecanismo do representante no EEE. Este mecanismo tem sido pouco estudado[40], embora tenha ganho alguma visibilidade nos últimos tempos com a saída do Reino Unido do EEE. Nomeadamente, mostra-se necessário esclarecer algumas empresas relativamente à necessidade de designar um representante na União, por terem um estabelecimento num País Terceiro ou, eventualmente, por terem intenção de vir a expandir o seu mercado.

4.2. Designação de Representante no EEE

Em primeiro lugar, importa reter que a figura do representante na UE (cons. 80 e art. 27.º do RGPD) aparece para facilitar as comunicações com:

a) os titulares de dados que se encontrem na UE (art. 12.º, 13.º e 14.º do RGPD), e;

b) as Autoridades de Controlo (art. 4, n.º21, 30.º e 51.º e ss do RGPD).

O legislador europeu quis desta forma garantir que os titulares dos dados que se encontrem no EEE e a ADC competente conseguem entrar em contacto com o estabelecimento que se encontre fora do EEE. E assim, eliminar eventuais barreiras territoriais de comunicação e aplicação de medidas por parte de uma ADC. Através da via da representação, uma empresa com estabelecimento num País Terceiro, que trata de dados de titulares que se encontram no território da União, poderá ser responsabilizada em caso de incumprimento do RGPD.

O n.º 1 do artigo 27.º do RGPD[41] deixa claro que, quando for aplicável o n.º 2 do artigo 3.º do RGPD, o responsável pelo tratamento ou o subcontratante está obrigado[42] a designar um

[39] Por sua vez, a utilização das cláusulas contratuais-tipo não corresponde a casos de aplicação direta do art. 3.º, n.º 2 do RGPD, mas, sim, a casos de transferências de dados pessoais para entidades que vão fazer tratamentos de dados não abrangidos pelo 3.º, n.º2; Note-se que a relação de tratamento de dados não aparece apenas sobre a forma de relação entre titular e responsável, mas pode aparecer sobre outras formas como, por exemplo, entre responsável e subcontratante.

[40] Segundo CHRISTOPHER KUNER a designação de um representante no EEE tem-se revelado um mecanismo ineficaz de aplicação do RGPD a Países Terceiros (cfr. CHRISTOPHER KUNER, "Extraterritoriality and regulation of international data transfers in EU data protection law*", in International Data Privacy Law*, 5, 2015, p.12 e 28). Contudo, julgamos que a realidade prática ainda não permite avaliar a real pertinência desta figura. É certo que a Diretiva 95/46 já previa a designação de um representante. No entanto, em moldes diversos dos estabelecidos no RGPD.

[41] Artigo 27.º: "*1. Se for aplicável o artigo 3.º, n.º 2, o responsável pelo tratamento ou o subcontratante designa por escrito um representante seu na União.*
2. A obrigação a que se refere o n.º 1 do presente artigo não se aplica: a) Às operações de tratamento que sejam ocasionais, não abranjam o tratamento, em grande escala, de categorias especiais de dados a que se refere o artigo 9.º, n.º 1, ou o tratamento de dados pessoais relativos a condenações penais e infrações referido no artigo 10.º, e não seja suscetível de implicar riscos para os direitos e liberdades das pessoas singulares, tendo em conta a natureza, o contexto, o âmbito e as finalidades do tratamento; ou b) Às autoridades ou organismos públicos;" [sublinhado nosso].

[42] Apesar do artigo 27.º, n.º 1 do RGPR referir apenas a palavra *"designa"* e a versão inglesa ser utilizada a expressão "*shall designate*" - *deve designar* [tradução nossa] - trata-se de uma verdadeira obrigação. Conclusão que pode ser retirada do n.º 2 do mesmo artigo. Este número parece ser esclarecedor referindo-se à designação

representante na União. Por sua vez, o n.º 2 do mesmo artigo estipula duas exceções, em que a obrigação do número anterior não será aplicável.

Um estabelecimento que esteja sujeito à mencionada obrigação poderá designar tanto uma pessoa singular como uma pessoa coletiva para o efeito. O representante é *"designado por um mandato*[43] *do responsável pelo tratamento ou do subcontratante, emitido por escrito*[44]*, que permita ao representante agir em seu nome no que diz respeito às obrigações que lhes são impostas (...)"*[45]. Este processo de designação do representante constitui, acima de tudo, um processo interno da própria empresa visto que não é preciso notificar a ADC competente. Contudo, a ADC e os titulares de dados terão sempre conhecimento da existência do representante designado, bem como acesso aos seus dados de contacto, uma vez que estas informações devem estar permanentemente acessíveis[46]. Nomeadamente devem constar na política de privacidade da empresa ou grupo empresarial.

Um estabelecimento situado fora da União pode ainda designar um só representante para todo o EEE. Ou seja, aquele estabelecimento que direcione os seus bens ou serviços a vários países do EEE não precisará de designar tantos representantes quantos os Estados Membros onde atue fazendo tratamento de dados dos titulares que se encontrem no EEE.

Outras questões relativas à designação do representante podem ser colocadas. Entre as quais, saber se um DPO[47] (Encarregado de Proteção de Dados) poderá ou não acumular a função de representante na mesma empresa. De facto, o RGPD não impede que um DPO seja designado como representante. Contudo, também não vemos que o acumular de funções seja desejável. Julgamos aconselhável a clara distinção entre ambas as funções para evitar potenciais situações de conflito de interesses[48].

Alertamos para o facto de os elementos de avaliação da necessidade de designar um representante (artigo 27.º do RGPD) não se confundirem com os elementos para avaliar a nomeação de um DPO (artigo 37.º do RGPD). Isto porque os artigos alusivos a estas duas figuras, não só são substancialmente diferentes, como partem de premissas distintas. Por outro lado, basta pensar que, caso o legislador quisesse que os elementos para avaliar a necessidade de designar um representante fossem os mesmos elementos utilizados para

---

do representante no EEE como uma "*obrigação*": "*A obrigação a que se refere o n.º 1 do presente artigo não se aplica (...)" ou "The obligation laid down in paragraph 1 of this Article shall not apply to (...)"* [sublinhado nosso].

[43] A. BARRETO MENEZES CORDEIRO, *Comentário ao Regulamento Geral de Proteção de Dados e à Lei n.º 58/2019*, Coimbra, Almedina, 2021, p. 250: "Na sua base, porém, à luz do direito português, estará, além daquela, um contrato de mandato com representação (artigos 262.º/1 e 1157.º do CC)".

[44] A este propósito, o RGPD não deixa claro se o mandato para designação do representante pode ser celebrado por email ou carta, em vez de ser celebrado um contrato de mandato sob a forma escrita.

[45] Cons. 80 do RGPD.

[46] CHRISTOPHER KUNER ET AL., *The EU General Data Protection Regulation (GDPR), A Commentary*, OXFORD, 2020, p. 596.

[47] Sigla utilizada por referência à expressão inglesa "*Data Protection Officer*".

[48] Veja-se ainda, CHRISTOPHER KUNER ET AL., "*The EU General Data Protection Regulation (GDPR), A Commentary"*, *in* Oxford, 2020, p. 596; Na mesma linha, leia-se THOMAS SHAW, "How do the DPO and EU representative interplay?*"*, *in IAPP*, 23.01.2018, disponível em https://iapp.org/news/a/how-do-the-dpo-and-eu-representative-interplay/ : "Due to the potential for conflicts, the DPC, while noting that there is no express prohibition on the same person fulfilling both roles, advises caution and notes it is the controller's responsibility to ensure that the DPO does not take on other tasks that result in a conflict".

avaliar a necessidade de nomear um DPO, o mesmo teria poupado algum trabalho e teria feito remissão entre os dois artigos – mas não o fez.

Pondo de lado os casos em que o tratamento de dados é efetuado por uma autoridade ou organismo público, a avaliação da necessidade de um DPO depende da avaliação dos dados que são tratados no âmbito da *"atividade principal"*[49] de uma empresa[50]. Já o artigo 27.º depende da avaliação de todos os dados que são processados por um determinado estabelecimento que se encontra fora do EEE. Portanto, a avaliação da necessidade de designar um representante inclui não só os dados tratados por um determinado estabelecimento fora do EEE no âmbito da atividade principal, como inclui os dados tratados no âmbito das atividades auxiliares desse estabelecimento – v.g. dados tratados para efeitos de *marketing*.

Como referido acima, estes dois artigos partem de premissas diferentes. Da letra da lei podemos constatar que a necessidade de nomear um DPO só se verifica caso se encontrem preenchidos todos os requisitos estabelecidos no artigo 37.º, n.º 1 do RGPD.

Em contraste, pelo artigo 27.º percebemos que o legislador assumiu que existe obrigação de nomear um representante na União sempre que o estabelecimento em análise é um estabelecimento fora do EEE que processa dados de pessoas que se encontram no território da União. Só em casos excecionais – elencados intencionalmente em separado no n.º 2 do mesmo artigo – é que haverá dispensa de designar um representante na UE. Parece claro que o legislador quis ser mais cauteloso e tomar uma medida preventiva nos casos em que uma empresa tenha estabelecimento num País Terceiro. Afinal, o legislador assume que, em princípio, todo o tratamento de dados efetuado fora da União assume maior risco do que quando tratado em território europeu.

Embora possa causar alguma estranheza, do exposto compreendemos que podem existir casos em que uma empresa está obrigada a designar um representante na União, mas já não obrigada a nomear um DPO. O contrário já não parece ser verdade.

A avaliação da necessidade de um representante tem que ser feita caso a caso e muitas vezes não é tarefa simples. Designadamente, podem surgir dúvidas – v.g. Será que um estabelecimento no Reino Unido (estabelecimento fora da UE) que pertence a um grupo empresarial com estabelecimentos em Portugal, Espanha e França (estabelecimentos da UE) está obrigado a designar um representante na UE? E que dizer se a sede desse grupo empresarial for num Estado Membro da UE, por exemplo em Portugal? Ou mesmo, que dizer no caso de esse estabelecimento do Reino Unido ser detido pela empresa portuguesa (estabelecimento da UE)? Essa obrigação mantém-se? Justificar-se-á, nestes casos, a designação de um representante?

[49] Art. 37.º, n.º 1 RGPD.
[50] Ou grupo empresarial.

Os poucos artigos escritos são tendencialmente da opinião de que todas estas ligações são motivo bastante para afastar a necessidade de designar um representante na União[51]. Mas creio que este entendimento não colhe. Não colhe, em primeiro lugar, porque como já foi dito anteriormente, o RGPD não dá relevância à sede, mas, sim, ao local do estabelecimento onde é feito o real tratamento de dados. Pegando no exemplo do parágrafo anterior, a avaliação da necessidade de designar um representante tem que ser feita à luz do tratamento de dados que é efetivamente levado a cabo pelo estabelecimento do Reino Unido, independentemente de a sede estar localizada ou não na UE.

Além do mais, nunca podemos perder de vista a letra e a teleologia da norma. Repare-se que a letra da lei não estabelece qualquer exceção caso o estabelecimento pertença a um grupo empresarial com outros estabelecimentos no território da União. No artigo 27.º do RGPD o legislador limitou-se a fazer referência ao artigo 3.º, n.º 2 do RGPD, sem qualquer outra indicação. Por fim, seguindo a teleologia da norma, será caso para dizer que se persistir dúvida em saber se um caso concreto cabe numa das exceções do n.º 2 do artigo 27.º do RGPD, é preferível seguir a perspetiva cautelosa do legislador e optar por designar um representante.

4.3. Cláusulas Contratuais-tipo

Analisemos agora as cláusulas contratuais-tipo: mecanismo que irá obrigar as empresas fora da UE a um nível de proteção de dados, não por via direta (art. 3.º, n.º 1 e 2), mas por via indireta. De forma simplificada, deixamos de estar num plano "*titular-estabelecimento*" para passarmos a analisar as transferências subsequentes no plano "*estabelecimento-estabelecimento*".

Nos termos do considerando 57 e do artigo 46.º, n.º 1 e 2, só podem ser realizadas transferências internacionais se o País Terceiro apresentar um nível de proteção adequado. Mas como garantir este nível de proteção quando os dados são transferidos para um País Terceiro? Uma das formas são as cláusulas-tipo de proteção de dados aprovadas pela Comissão Europeia[52] (*standard contractual clauses*) – previstas no artigo 46.º, n.º 2, c) do RGPD. Este mecanismo permite transferências internacionais de dados entre pessoas coletivas e, dada a sua relevância prática no dia-a-dia das empresas, revela-se ilustrativo do efeito do RGPD fora do EEE.

[51] Como exemplo: LOTHER DETERMANN, IAPP Member Contributor, "Representatives under Art. 27 of the GDPR: All your questions answered", 12.06.2018, IAPP, *in* https://iapp.org/news/a/representatives-under-art-27-of-the-gdpr-all-your-questions-answered/ e VINCENT REZZOUK-HAMMACHI/ALEX WILLIAM/ CLARA CLARK NEVOLA, "Brexit deal agreed: The need to appoint an EU and/or UK representative for #GDPR or UK data protection law purposes remains", 12.2020, Bird & Bird, *in* https://www.twobirds.com/en/news/articles/2019/uk/article-27-representative--do-you-need-to-appoint-an-eu-representative-a-uk-representative-or-both . Note-se que estes artigos são pouco explicativos no que respeita a esta questão, limitando-se a lançar conclusões sem escrutinar os elementos interpretativos da norma.

[52] Cláusulas-tipo de proteção de dados adotadas pela Comissão pelo procedimento de exame referido no artigo 93.º, n.º 2 do RGPD.

De forma breve, trata-se de um instrumento contratual com o objetivo de garantir que uma empresa num País Terceiro que recebe dados de uma empresa europeia irá apresentar o mesmo nível de proteção de dados que o regime europeu apresenta.

Pense-se numa empresa italiana que irá organizar um evento em Itália. Com efeito, recolheu dados de determinados participantes inscritos e irá transferir esses mesmos dados para uma empresa norte-americana que patrocinará o evento e usará esses mesmos dados para efeitos de marketing. A empresa italiana tem que garantir que está a contratar com uma empresa norte-americana que irá tratar dos dados nos termos do RGPD. Neste caso, a empresa italiana nos termos do n.º 1 do artigo 3.º, está abrangida pelo RGPD. E a empresa norte-americana, também, conforme disposto no n.º 2 do mesmo artigo. Contudo, para assegurar que as regras de proteção de dados são efetivamente cumpridas por uma empresa de um Estado Terceiro, a empresa italiana terá que assinar um contrato com a empresa norte-americana com essas mesmas regras (*standard contractual clauses*) para garantir a executividade do RGPD no território Estado Terceiro. A lei torna-se numa cláusula dum contrato. Será a via contratual que irá assegurar que aquela empresa situada num Estado Terceiro cumprirá o tratamento nos termos do regime europeu[53] bem como aceita estar sujeito à supervisão das autoridades de controlo[54]. Aqui a empresa situada no território de um País Terceiro estará a obrigar-se a um nível de segurança e responsabilidade, não através da lei, mas pela via contratual.

4.4. Limitações de execução

Apesar de todo o exposto: serão as regras de transferências internacionais ainda assim suficientemente eficazes? Serão efetivamente respeitadas e executadas na prática?

Julgo que o regime europeu de proteção de dados continua a apresentar limitações. Nomeadamente quanto à efetiva execução dos poderes das ADC, incapazes de concretizar os seus comandos num País Terceiro. Esta constatação passa, justamente, por admitir que a abrangência oferecida pelo artigo 3.º, n.º 2 (extraterritorialidade) não está em consonância com o disposto no artigo 55.º RGPD, que revela uma (real) limitação territorial das ADC: *"As autoridades de controlo são competentes para prosseguir as atribuições e exercer os poderes que lhes são conferidos pelo presente regulamento no território do seu próprio Estado-Membro".* [sublinhado nosso]

Bem vistas as coisas, será, com certeza, aliciante transferir a sede, ou mesmo a alteração do estabelecimento, para um País Terceiro quando se pretende tratar dados pessoais de titulares

[53] Claro que, caso não aceite assinar tais disposições contratuais, a empresa italiana poderá ser responsabilizada por contratar com uma empresa que não oferece garantias suficientes.
[54] A. BARRETO MENEZES CORDEIRO, *Comentário ao Regulamento Geral de Proteção de Dados e à Lei n.º 58/2019*, Coimbra, Almedina, 2021, p. 333: "Ao realizar transferências baseadas em cláusulas-tipo, o exportador e o importador encontram-se sujeitos à supervisão das autoridades de controlo. As autoridades de controlo podem suspender ou proibir a transmissão de dados caso o responsável pelo tratamento de dados violar as cláusulas-tipo de proteção de dados".

que se encontrem na União. Afinal, ainda que existam as medidas acima mencionadas para transferências internacionais, como pode uma ADC impor coimas a uma empresa estabelecida fora da UE que não cumpra o RGPD? Como se garante o cumprimento de sanções? Como podem ser realizadas auditorias a empresas não europeias a operar na União? Será que o direito da União consegue impor as suas regras a uma sociedade estabelecida num País Terceiro perante comportamentos lesivos de dados pessoais de titulares que se encontrem na UE? Será que um Estado Terceiro reconhece autoridade a uma ADC (Europeia)? A figura do representante na UE será eficaz em termos de responsabilização de uma sociedade num um País Terceiro que trate de dados pessoais com origem no território da União?

A estes problemas, acresce o facto de os poderes das ADC estarem muitas vezes limitados aos escassos recursos financeiros. Problema que se coloca dentro da UE. Sem dúvida que as limitações financeiras podem ser um impedimento para que uma ADC realize as suas tarefas. Circunstância, diga-se, muito conveniente às sociedades que não apresentem um nível adequado de proteção/respeito pelo RGPD.

Não se estranha, portanto, que, se estas limitações de execução não conseguirem ser ultrapassadas, as sociedades encontram terreno fértil para recorrerem à mobilidade de estabelecimento. Vejamos.

5. Transferência de sede como meio de escolha de uma determinada ADC

Poderíamos, pois, ficar por aqui, não fosse conveniente averiguar em detalhe se a transferência de estabelecimento (que pode corresponder em alguns casos à transferência de sede) poderá ser útil para "escapar" ao escrutínio de uma ADC.

O objetivo é claro: perceber como determinar a ADC competente e até onde vão os seus poderes. Se, da seguinte análise, constatarmos que as ADC se veem incapacitadas de realizar os seus poderes por a) falta de financiamento, ou b) perante Países Terceiros por falta de reconhecimento da sua autoridade, não restará outra alternativa, se não, concluir que fica aberto caminho para a mobilidade de estabelecimento e, em alguns casos, para o *forum shopping*.

5.1. Determinação da ADC competente

Qualquer empresa terá que saber qual a sua ADC competente, quanto mais não seja para cumprir a obrigação de notificar a ADC competente perante a ocorrência de uma violação de dados pessoais (art. 33.º RGPD).

No que respeita a tratamentos nacionais, não temos dúvida: a ADC competente corresponderá à ADC nacional daquele Estado Membro onde se encontra o(s) estabelecimento(s). Basta para tanto ter presente o artigo 55.º RGPD: cada Estado Membro tem que nomear uma ADC para fiscalizar as atividades de tratamento no seu território.

Questão diferente colocar-se-á quando um responsável/subcontratante faz um tratamento transfronteiriço. Refiro-me ao tratamento de dados pessoais que ocorre no contexto das atividades de: a) "*estabelecimentos em mais do que um Estado-Membro de um responsável pelo tratamento ou um subcontratante na União, caso o responsável pelo tratamento ou o subcontratante esteja estabelecido em mais do que um Estado-Membro*", ou; b) "*um único estabelecimento de um responsável pelo tratamento ou de um subcontratante, mas que afeta substancialmente, ou é suscetível de afetar substancialmente, titulares de dados em mais do que um Estados-Membro"* (art. 4.º, n.º 23 do RGPD). Nestes casos, seguindo a lógica anterior, correríamos o risco de nos depararmos com diferentes decisões emitidas por várias ADC. Diga-se: *"seria uma valente confusão"*[55].

Para que isto não suceda, o RGPD encontrou solução no chamado "*Sistema do Balcão Único*"[56]. Este sistema tem por base duas categorias de ADC: a) a ADC principal e b) as ADC interessadas. Ou seja, para os referidos tratamentos transfronteiriços, será competente uma ADC principal encarregue de decidir e coordenar as várias ADC interessadas. Já as ADC interessadas ficarão destacadas para prestar assistência sobre qualquer informação solicitada por parte da ADC principal. Em suma: apenas uma única ADC (ADC principal) será competente para controlar o tratamento transfronteiriço, ainda que coadjuvada por outas ADC.

Este sistema tem que ser seguido *"step by step"*. Com efeito, só será útil equacionar a migração de um estabelecimento se uma determinada empresa ou organização souber qual a ADC principal que ficará competente para agir com autoridade perante uma violação de dados. Como determinar qual a ADC principal? Nos termos do artigo 56.º RGPD, a ADC principal corresponde à ADC do território onde se situe o estabelecimento principal.

Anuncia-se uma próxima etapa: como determinar qual o estabelecimento principal/único? O conceito de "*estabelecimento principal"* encontra-se definido no n.º 16 do artigo 4.º do RGPD: o local onde são tomadas as decisões sobre as finalidades e os meios de tratamento ou onde são efetivamente exercidas as principais atividades de tratamento de dados, pelo que muitas vezes corresponderá à sede real, onde se encontra o centro de administração e controlo[57].

[55] As alíneas a) e b) encontram-se explicados com algum detalhe nas Orientações do Grupo de Trabalho do Art. 29 (que foi assumida pelo Comité) - WP242 rev.01 sobre os critérios de determinação da autoridade de controlo competente.
[56] MARTA PORTOCARRERO/PATRÍCIA FRAGOSO MARTINS, "O mecanismo de coerência e o contencioso da União: Reflexões a respeito das decisões do Comité ao abrigo do Regulamento Europeu de Proteção de Dados", *Revista Forum de Proteção de Dados*, n.º 5, Novembro.2018, p. 11.
[57] Ou seja, o conceito de estabelecimento principal é funcionalizado, trata-se apenas de estabelecimento principal na perspectiva das actividades relevantes para o RGPD.

5.2. Limitações. Motivos para a mobilidade de estabelecimento

Retomo, aqui, o raciocínio acima referenciado (ponto 4.4) sobre a falta de meios humanos, técnicos e financeiros que impossibilitam que as ADC consigam dar execução às suas atribuições.

Dispõe o n.º 4 do artigo 52.º do RGPD: *"Os Estados-Membros asseguram que cada autoridade de controlo disponha dos recursos humanos, técnicos e financeiros, instalações e infraestruturas necessários à prossecução eficaz das suas atribuições e ao exercício dos seus poderes, incluindo as executadas no contexto da assistência mútua, da cooperação e da participação no Comité."*

Graça Canto Moniz, na sua tese de doutoramento[58], entende que *"o ponto frágil deste modelo de supervisão reside na inexistência de recursos humanos e financeiros em algumas das autoridades de controlo para o desempenho bem-sucedido dos seus poderes"*.

Ou seja, os escassos recursos acabam por gerar uma discrepância entre as ADC. Facto que favorece empresas cujo escrutínio é feito por autoridades com poucos meios, bem como pode constituir um estímulo para a mobilidade de estabelecimento.

Penso, em concreto, em casos semelhantes ao da ADC irlandesa, que até há bem pouco tempo era um atrativo para determinadas empresas transferirem o seu estabelecimento[59]. Em contraste, temos certas ADC com muitos meios para desempenhar escrupulosamente as suas funções. Circunstância que pode gerar a retirada de alguns estabelecimentos ou, em alguns casos, a transferência de sede deste país.

Não posso deixar de concordar com TJ Mcintyre[60] que defendia que a Irlanda violava o RGPD pelo facto de, em tempos, não ter dotado a sua ADC de meios suficientes.

A esta conclusão chegou o TJUE no conhecido *Acórdão Schrems*[61] afirmando que o Estado irlandês tinha que dotar a sua ADC de recursos suficientes. Por isso mesmo, a ADC irlandesa teve um reforço de meios para desempenhar as suas funções.

Em todo o caso, um país que não venha a dotar a sua ADC desses meios está a violar o Direito da UE, mais especificamente, o artigo 52.º, n.º 4 do RGPD. Com efeito, nestes casos poderá mesmo haver a responsabilidade civil do Estado por violação do Direito da União[62].

---

[58] GRAÇA CANTO MONIZ, *A Extraterritorialidade do Regime Geral de Proteção de Dados Pessoais da União Europeia: Manifestações e Limites*, Faculdade de Direito, Universidade Nova de Lisboa, Novembro 2018, p. 101.
[59] Pense-se no caso da Amazon e Microsoft que se encontram estabelecidas na Irlanda. É certo que o principal motivo são razões fiscais, mas têm, igualmente, vindo a beneficiar de um escrutínio *"mais brando"* quanto ao tratamento de dados.
[60] TJ MCINTYRE, "Regulating the Information Society: Data Protection and Ireland's Internet Industry", *in The Oxford Handbook of Irish Politics* (Oxford University Press, forthcoming 2020, P. 14.
[61] Acórdão do TJUE C-362/14, 6.10. 2015 (ECLI:EU:C:2015:650).
[62] SOFIA OLIVEIRA PAIS, *Princípios Fundamentais de Direito da União Europeia – Uma abordagem jurisprudencial*, 2.ª Edição, Coimbra, Almedina, 2012, p. 107 ss.

No sentido de averiguar esta responsabilidade vejam-se os Acórdãos *Francovich*[63] e *Almelo*[64]. Em todas estas decisões estava em discussão a responsabilidade civil do Estado por violação de Direito da União e que tem por base o princípio da cooperação leal dos Estados Membros assim como o princípio da proteção dos direitos dos particulares.

Elucidados estes aspetos, impõe-se averiguar os três requisitos para verificação da condenação de um Estado Membro a pagar uma indemnização aos particulares afetados:

> a) A norma violada tem que conferir direitos aos particulares;
>
> b) A violação em causa tem que ser suficientemente caracterizada (entenda-se uma violação manifesta e grave);
>
> c) E, por fim, a existência de um nexo de causalidade entre a violação e o dano sofrido pelo particular.

Claro que esta averiguação tem de ser feita caso a caso. Contudo, julgo que a omissão de facultar meios para que uma ADC prossiga as suas atribuições constitui uma violação do artigo 52.º, n.º 4 do RGPD, pondo em causa o direito à proteção dos dados dos titulares (art. 1.º RGPD e art. 8.º da Carta dos Direitos Fundamentais da União Europeia).

Problema diverso é o que se segue: saber se uma ADC tem mecanismos para fazer com que uma empresa com estabelecimento principal num País Terceiro cumpra as suas orientações, sanções ou a realização de auditorias[65].

Tentar responder a esta questão não é fácil. Ultrapassar a barreira territorial torna-se tarefa árdua. Seja como for, destaco a constante tentativa dos Estados Membros em realizar acordos de cooperação internacional.

De acordo com o artigo 50.º do RGPD, o cumprimento de instruções e decisões de uma ADC, bem como a realização de auditorias e determinadas diligências procedimentais e de fiscalização num País Terceiro, está dependente do cumprimento voluntário por parte da empresa em causa ou dependente da celebração de acordos internacionais.

A realização de acordos de cooperação internacionais e de assistência mútua é que acabam por reconhecer autoridade a uma determinada ADC aos olhos de um País Terceiro. Pelo que a execução extraterritorial está entregue à sorte da celebração destas convenções. Concluo que a inexistência de acordos de cooperação pode ser motivo bastante para que uma empresa equacione transferir o seu estabelecimento para um País Terceiro.

---

[63] Acórdão do TJUE C-6/90, 19.11.1991 (ECLI:EU:C:1991:428).
[64] Acórdão do TJUE C-470/04, 7.09.2006 (ECLI:EU:C:2006:525).
[65] BENJAMIN GREZE, "The extra-territorial enforcement of the GDPR, A genuine issue and the quest for alternatives", *in International Data Privacy Law*, 2019, Vol. 0, No. 0, p. 3: "Yet, the extra-territorial reach of the GDPR and more particularly Article 3(2) neglects the enforcement aspect. The greatest challenge to the extra-territorial dimension of the GDPR is undoubtedly the effectiveness of its enforcement, which is at the core of its success. In that regard, the extra-territorial enforcement issue was regularly mentioned,18 and in some cases very shortly after the publication of the initial proposal of the GDPR.19 It was thus anticipated that data protection authorities would initiate very few actions—or perhaps no action at all—outside the EU territory. While much ink has been spilled over the extra-territorial scope of EU data protection law in the legal literature from a prescriptive and adjudicative perspective, the problem of enforcement does not generally move centre-stage so that there is no comprehensive study un- der the prism of enforcement jurisdiction in the area of data protection law".

Ainda a este propósito, não é menos importante destacar que, mesmo na ausência das referidas convenções, as empresas de Países Terceiros acabam por cumprir ordens de uma ADC, porque bem percebem que o rótulo de *"incumpridor"* traz desvantagens na relação com o mercado europeu. A má reputação de uma empresa fora da União pode trazer desconfiança tanto por parte dos titulares de dados como por parte de outras empresas europeias que com ela queiram contratar. Por isto, há empresas que acabam por cumprir voluntariamente as indicações de uma ADC, principalmente empresas estrangeiras fortemente direcionadas para o mercado europeu.

Também, por esta razão, tem havido uma crescente necessidade – note-se, com algum trabalho de sensibilização e persuasão das ADC – para que haja uma harmonização de proteção de dados a nível mundial. Desde logo, assiste-se a um fenómeno em cadeia de produção legislativa inspirada no regime europeu de proteção de dados. É o caso do Japão, do Brasil, da Nova Zelândia, Austrália, Índia e da Coreia do Sul. Não há dúvida que, com a progressiva harmonização legislativa, eventuais casos de transferência de estabelecimento por motivos relacionados com a proteção dos dados acabarão por caminhar numa relação proporcionalmente inversa.

5.3. Alternativas à transferência de sede com vista à escolha de uma determinada ADC

A presente análise não ficaria, porém, completa sem pensarmos noutras alternativas à transferência de estabelecimento que também permitam a escolha de uma determinada ADC.

a) Cláusula de submissão a uma determinada ADC?

Pense-se no contrato entre duas empresas em que as partes acordam submeter-se a uma determinada ADC. Tal situação poderia acontecer, por exemplo, no âmbito de uma relação entre uma empresa responsável pelo tratamento e uma empresa subcontratada que processa dados por conta da empresa responsável[66] (art. 28.º, n.º 3 RGPD).

Não há dúvida que o Regulamento Roma I[67] dá relevância à vontade das partes em matéria contratual. Todavia, o Regulamento Roma I só é aplicável às obrigações contratuais, em

[66] Ainda assim, note-se que a mesma hipótese poderá ocorrer não apenas entre responsável e subcontratante, mas também no âmbito de um contrato entre dois responsáveis independentes.
[67] Regulamento (CE) N.º 593/2008 do Parlamento Europeu e do Conselho, de 17 de Junho de 2008, sobre a lei aplicável às obrigações contratuais (Roma I).

matéria civil e comercial que impliquem um conflito de leis, ficando de fora a liberdade para escolha de uma entidade administrativa – uma ADC (art. 1.º, n.º 1 Regulamento Roma I)[68].

De todo o modo, as normas relativas à determinação da ADC competente não parecem ser supletivas, mas injuntivas. Pelo que uma ADC não poderá ser afastada por vontade das partes. Sendo assim, existe sempre um carácter vinculativo à ADC competente.

b) Cláusula de escolha da lei competente para reger o contrato?

Já que a hipótese anterior oferece obstáculos: que pensar, agora, da hipótese de duas empresas celebrarem um contrato com uma cláusula escolhendo uma determinada lei nacional aplicável ao contrato com o objetivo de beneficiar da competência da ADC desse mesmo Estado?

Acompanhe-se o seguinte exemplo: duas empresas, uma portuguesa e outra irlandesa, submetem o contrato à Lei Irlandesa. Imaginemos, por conseguinte, que a empresa portuguesa viola o RGPD. Em princípio a ADC competente será a ADC portuguesa. No entanto, como as partes escolheram a lei Irlandesa para reger aquele contrato, poderá ser a ADC irlandesa competente?

Neste caso, como as partes escolheram apenas a lei que rege aquele contrato – e não uma entidade administrativa – o Regulamento Roma I não oferece qualquer impedimento (art. 1.º e 3.º do Regulamento Roma I).

Porém, mais uma vez, as normas de determinação da ADC competente não parecem ser passíveis de afastamento pelo mesmo argumento que acima foi exposto no ponto 5.3.a). Perante o que antes se explicou, o caso que aqui se coloca não terá sucesso. Ainda assim, como esta foi uma possibilidade que coloquei quando pensei nesta exposição, nada como ficar escrito para que não restem dúvidas.

Não se julgue, por isto, que esta questão será completamente desprovida de sentido. Afinal, esta questão poderia ter lógica, na medida em que, se aquelas empresas se dedicassem na sua maioria ao mercado irlandês – tratassem de dados de pessoas que se encontrem na Irlanda – a escolha da ADC irlandesa[69] poderia ter sido, porventura, uma solução (razoável) encontrada pelo legislador europeu – mas não foi o caso.

[68] Também cfr. LUÍS LIMA PINHEIRO, *Direito Internacional Privado, Direito de Conflitos – parte especial*, Vol. II, 4.ª Edição Refundida, Coimbra, Almedina, 2018, p. 315.
[69] Claro que nada disto invalida que a ADC irlandesa seja parte interessada nos termos do art. 4.º, n.º 22 RGPD.

c) Outras alternativas

Já concluímos que as normas para determinar a ADC competente são imperativas, não podendo, à partida, ser afastadas por vontade dos responsáveis.

Mas encontram-se duas formas de contornar esta aparente vinculatividade, evitando, assim, alguns casos de mobilidade de estabelecimento como *"fuga"* a uma ADC.

Em primeiro lugar, se duas empresas tratarem de dados enquanto responsáveis conjuntos[70] (art. 26.º RGPD) existe a possibilidade de entre elas acordarem sobre qual é o estabelecimento principal. O Estado onde se encontrar o estabelecimento principal escolhido corresponderá, então, à ADC daquele Estado[71]. Portanto, ao escolherem o estabelecimento principal, estarão a escolher a ADC competente, *in casu*.

Em segundo lugar, o artigo 4.º, n.º 16 do RGPD deu, igualmente, espaço aos grupos empresarias para determinar qual é o seu estabelecimento principal para efeitos de tratamento de dados pessoais (pode não ser a sede). A escolha do estabelecimento principal determinará, mais uma vez, a ADC competente[72].

6. Transferência de sede como meio de escolha de uma lei nacional de execução do RGPD?

Parece-nos que a Lei de execução de cada país não será motivo suficiente para uma operação de transferência de sede, nem mesmo mobilidade de estabelecimento.

É sabido que o RGPD é diretamente aplicável em todos os Estados Membros (art. 99.º do RGPD) e o legislador apenas deu espaço a estes Estados para legislarem a nível nacional sobre determinados aspetos específicos e dentro das "balizas" enunciadas pelo legislador[73].

[70] Não se confunda com tratamento de dados entre responsável e um subcontratante. A este propósito leia-se o artigo de MAFALDA MIRANDA BARBOSA que explica a diferença entre as relações controller-processor (relação de subcontratação), controller-controller (relação de controlo paralelo/independent controllers) e controller-controller (relação de controlo conjunto/joint controllers). (MAFALDA MIRANDA BARBOSA, "Data controllers e data processors: da responsabilidade pelo tratamento de dados à responsabilidade civil", *in Revista de Direito Comercial*, 15.03.2018).

[71] Orientações do Grupo de Trabalho do Art. 29 (que foi assumida pelo Comité) - WP244 rev.01.

[72] Mesmo assim, julgo que a escolha do estabelecimento principal não é vinculativa. Se uma determinada ADC se achar competente e duvidar de que, de facto, o estabelecimento identificado pelo responsável/subcontratante não corresponde ao estabelecimento onde
se decide o efetivo tratamento de dados, seguir-se-á, por regra, o procedimento do art. 56.º e, eventualmente a ADC poderá reclamar para si essa competência após pedido de evidências de que é naquele local que tratamento ocorre; Cfr. Orientações do Grupo de Trabalho do Art. 29 (que foi assumida pelo Comité) - WP244 rev.01, p. 7.

[73] Em Portugal, a lei de execução corresponde à Lei n.º 58/2019, de 8 de Agosto - lei que foi objeto de várias críticas pela CNPD. Tanto que a recente Deliberação/2019/498 veio considerar alguns preceitos da Lei n.º 58/2019 violadoras do RGPD – a CNPD deliberou desaplica-las em futuros casos concretos. Note-se que o RGPD tem carácter geral e obrigatório e é diretamente aplicável aos Estados Membros, cabendo aos mesmos apenas especificar a aplicação das regras e adaptar ao contexto nacional, sem extravasar o seu âmbito de aplicação.

Uma vez verificados os pressupostos previstos nos números 1 ou 2, do artigo 3.º, o RGPD sempre se aplicará e os aspetos que o legislador deixou à disposição dos Estados Membros não são de maior relevância para as empresas. Mas tudo dependerá da análise casuística da questão.

7. Conclusão. Como evitar a mobilidade de estabelecimento ou casos de fórum shopping?

Em face do exposto e prevenindo alguns possíveis cenários de transferência de estabelecimento (que podem coincidir ou não com a transferência de sede) proponho o seguinte:

i) Os Estados devem continuar o seu trabalho de cooperação internacional e harmonização legislativa;

ii) Os Estados Membros devem dotar as ADC dos recursos necessários para prosseguirem as suas atribuições. Caso contrário, os Estados Membros terão que ser responsabilizados por violarem o Direito da UE;

iii) Os grupos empresariais, bem como os responsáveis conjuntos, devem privilegiar a escolha de um estabelecimento principal ao invés de optarem pela transferência de estabelecimento;

iv) Sempre que possível, as empresas devem optar por estratégias tecnológicas de anonimização de dados (cons. 26 RGPD). Na verdade, a melhor forma para acabar com um problema criado pela tecnologia é fazer uso da própria tecnologia. Desta forma, se uma empresa conseguir anonimizar determinados dados, estes deixam de ter um carácter pessoal e, por conseguinte, deixam de ser abrangidos pelo âmbito de aplicação material do RGPD. Ou seja, passam a ser informações que não dizem respeito a uma *pessoa singular identificada ou identificável*, deixando de se colocar qualquer necessidade de transferência de estabelecimento.

Bibliografia citada

CORDEIRO, A. BARRETO MENEZES, *Comentário ao Regulamento Geral de Proteção de Dados e à Lei n.º 58/2019*, Coimbra, Almedina, 2021

CORDEIRO, A. BARRETO MENEZES, *Direito da Proteção de Dados à Luz do RGPD e da lei n.º 58/2019*, Coimbra, Almedina, 2020

SILVEIRA, ALESSANDRA/FROUFE, PEDRO, *"Do mercado interno à cidadania de direitos, A proteção de dados pessoais como a questão jus-fundamental identitária dos nossos tempos"*, *in* UNIO, EU

Law Journal, Vol. 4, No. 2, Julho 2018, in http://www.unio.cedu.direito.uminho.pt/Uploads/UNIO%204%20.%20Vol%201/Unio%204%20n.%202%20PT/Alessandra%20Silveira%20&%20Pedro%20Froufe.pdf

GREZE, BENJAMIN, "The extra-territorial enforcement of the GDPR: a genuine issue and the quest for alternatives", *in International Data Privacy Law*, 2019, Vol. 0, No. 0

KUNER, CHRISTOPHER ET AL., *The EU General Data Protection Regulation (GDPR), A Commentary*, Oxford, 2020

KUNER, CHRISTOPHER, "Territorial Scope and Data Transfer Rules in the GDPR: Realising the EU's Ambition of Borderless Data Protection", *in Legal Studies Research Paper Series*, University of Cambridge, Faculty of Law, PAPER NO. 20/2021, APRIL 2021

Kuner, Christopher, "Extraterritoriality and regulation of international data transfers in EU data protection law", *in International Data Privacy Law*, 5, 2015, *in* https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2644237

MONIZ, GRAÇA CANTO, *A Extraterritorialidade do Regime Geral de Proteção de Dados Pessoais da União Europeia: Manifestações e Limites,* Faculdade de Direito, Universidade Nova de Lisboa, Novembro 2018, *in* https://run.unl.pt/bitstream/10362/89180/1/Fonseca_2019.pdf

MONIZ, GRAÇA CANTO, "Finalmente: coerência no âmbito de aplicação do regime da União Europeia de proteção de dados pessoais! - O fim do enigma linguístico do artigo 3.º, n.º 2 do RGPD", *in UNIO, Eu Law Journal*, Vol. 4, No. 2, Julho 2018

GT29 OPINION 8/2010 on applicable law (WP 179): https://ec.europa.eu/newsroom/article29/items/640614/en

GUIDELINES 3/2018 on the territorial scope of the GDPR (Article 3) Version 2.1, 12.November.2019 https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_3_2018_territorial_scope_after_public_consultation_en_1.pdf

PINHEIRO, LUÍS LIMA, *Direito Internacional Privado, Direito de Conflitos – parte especial*, Vol. II, 4.ª Edição Refundida, Coimbra, Almedina, 2018

PORTOCARRERO, MARTA/MARTINS, PATRÍCIA FRAGOSO, "O mecanismo de coerência e o contencioso da União: Reflexões a respeito das decisões do Comité ao abrigo do Regulamento Europeu de Proteção de Dados", *in Revista Forum de Proteção de Dados*, n.º 5, Novembro.2018

BARBOSA, MAFALDA MIRANDA, "Data controllers e data processors: da responsabilidade pelo tratamento de dados à responsabilidade civil", *in Revista de Direito Comercial*, 15.03.2018, *in* https://static1.squarespace.com/static/58596f8a29687fe710cf45cd/t/5aaacd451ae6cf02516c4b66/1521143111492/2018-10.pdf

CRAIG, PAUL ET AL., "The Foundations of EU Data Protection Law", *in Oxford Studies in European Law*, Orla Lynskey, Oxford University Press, 2015

VOIGT, PAUL ET AL., *The EU General Data Protection Regulation (GDPR), A Practical Guide*, Springer International Publishing, Switzerland, 2017

ASENSIO, PEDRO ALBERTO DE MIGUEL*, Derecho Privado de Internet*, Quinta Edicion, Civitas, 2015

ASENSIO, PEDRO ALBERTO DE MIGUEL, "Competencia y Derecho Aplicable em el Regulamento General sobre Protección de Datos de la Unión Europeia*", in Revista Española de Derecho Internacional* (REDI*)*, Volumen 69 (1), Madrid, 2017, *in* http://www.revista-redi.es/wp-content/uploads/2018/01/3_estudios_miguel_asensio_competencia_dcho_aplicable_en_reglamento_general.pdf

PAIS, SOFIA OLIVEIRA, *Princípios Fundamentais de Direito da União Europeia – Uma abordagem jurisprudencial*, 2.ª Edição, Coimbra, Almedina, 2012

MCINTYRE, TJ, *"Regulating the Information Society: Data Protection and Ireland's Internet Industry"*, *in* SRN, The Oxford Handbook of Irish Politics (Oxford University Press), 9.02.2020, *in* https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3520101

REZZOUK-HAMMACHI, VINCENT/WILLIAM, ALEX/ NEVOLA, CLARA CLARK, *Brexit deal agreed: The need to appoint an EU and/or UK representative for #GDPR or UK data protection law purposes remains*, 12.2020, Bird & Bird, *in* https://www.twobirds.com/en/news/articles/2019/uk/article-27-representative--do-you-need-to-appoint-an-eu-representative-a-uk-representative-or-both

EUROPEAN PARLIAMENT*,* "The Polbud judgment and the freedom of establishment for companies in the European Union: problems and perspectives", *in STUDY For the JURI Committee*, Policy Department for Citizens' Rights and Constitutional Affairs Directorate General for Internal Policies of the Union, PE 608.833 - October 2018, *in* https://www.europarl.europa.eu/RegData/etudes/STUD/2018/608833/IPOL_STU(2018)608833_EN.pdf

SHAW, THOMAS, CIPP/E, CIPP/US, IAPP Member contributor, "How do the DPO and EU representative interplay*?*", *in IAPP*, 23.01.2018: https://iapp.org/news/a/how-do-the-dpo-and-eu-representative-interplay/

DETERMANN, LOTHAR, IAPP Member Contributor, "Representatives under Art. 27 of the GDPR: All your questions answered", 12.06.2018, *IAPP*, *in* https://iapp.org/news/a/representatives-under-art-27-of-the-gdpr-all-your-questions-answered/

Jurisprudência

Acórdão C-362/14, 6.10.2015 (ECLI:EU:C:2015:650).

Acórdão C-131/12, 13.05.2014 (ECLI:EU:C:2014:317).

Acórdão C-6/90, 19.11.1991 (ECLI:EU:C:1991:428).

Acórdão C-470/04, 7.09.2006 (ECLI:EU:C:2006:525).

Acórdão C-210/06, 16.12.2008 (ECLI:EU:C:2008:723).

Acórdão C-371/10, 29.11.2011 (ECLI:EU:C:2011:785).

Acórdão C-378/10, 12.07.2012 (ECLI:EU:C:2012:440).

Acórdão C-106/16, 25.10.2017 (ECLI:EU:C:2017:804).

Acórdão C-210/16, 5.06.2018 (ECLI:EU:C:2018:388).

(texto submetido a 28.09.2021 e aceite para publicação a 14.01.2022)