Maria da Graça Almeida de Eça do Canto Moniz Adão da Fonseca

A EXTRATERRITORIALIDADE DO REGIME GERAL DE PROTEÇÃO DE DADOS PESSOAIS DA UNIÃO EUROPEIA: MANIFESTAÇÕES E LIMITES

Dissertação com vista à obtenção do grau de Doutora em Direito na especialidade de Direito Público

Orientadora: Doutora Filipa Calvão, Professora Associada da Faculdade de Direito da Universidade Católica

Novembro 2018

Maria da Graça Almeida de Eça do Canto Moniz Adão da Fonseca

A EXTRATERRITORIALIDADE DO REGIME GERAL DE PROTEÇÃO DE DADOS PESSOAIS DA UNIÃO EUROPEIA: MANIFESTAÇÕES E LIMITES

Dissertação com vista à obtenção do grau de Doutora em Direito na especialidade de Direito Público

Orientadora: Doutora Filipa Calvão, Professora Associada da Faculdade de Direito da Universidade Católica

Novembro 2018

Declaração anti plágio

Declaro que o texto que apresento é da minha autoria, sendo exclusivamente responsável pelo respetivo conteúdo e citações efetuadas. Toda a utilização de contributos ou textos alheios está devidamente referenciada.

Maria da Graça Almeida de Eça do Canto Moniz Adão da Fonseca
1 de novembro de 2018

Agradecimentos

O primeiro agradecimento é dirigido à Cita e ao Luís: obrigada por tudo o que me ensinaram e ensinam ainda hoje. Quero agradecer particularmente ao meu marido, entre tantas outras coisas, pela sua alegria a qualquer hora e pelo seu exemplo de força e persistência na adversidade. Não esqueço também a Benedita, nomeadamente a companhia e a preciosa orientação a estudar algumas matérias.

Além disto, uma palavra de sentida gratidão é devida à minha orientadora, a Professora Doutora Filipa Calvão. Agradeço-lhe toda a disponibilidade, opiniões, sabedoria e as conversas que tivemos ao longo destes anos e que me ajudaram a aperfeiçoar este trabalho. Não posso deixar de mencionar o Professor Doutor Francisco Pereira Coutinho, pelo interesse na minha investigação, pela sua disponibilidade e pelos vários desafios que me tem apresentado.

Agradeço ainda ao Professor Doutor Jorge Pereira da Silva, à Dra. Clara Guerra e ao Martinho Lucas Pires pela troca de impressões na fase final deste trabalho.

Por fim, devo destacar que esta tese foi subsidiada pela Fundação para a Ciência e Tecnologia, através da concessão de uma bolsa de doutoramento que financiou a minha estadia na Universidade de Georgetown, nos EUA, e na Universidade de Tilburg, na Holanda.

Lista de abreviaturas

ADIRC – Académie de Droit International. Recueil des Cours
AEPD – Agencia Española de Protección de Datos
AFDI – Annuaire français de droit international
AFIPS – American Federation of Information Processing Societies
AJCL – American Journal of Comparative Law
AJICL – Arizona Journal of International & Comparative Law
AJIL – American Journal of International Law
AJST - Albany Law Journal of Science and Technology
ALJ – Antitrust Law Journal
AmCham EU – American Chamber of Commerce to the European Union
Art. – Artigo
BCICLR – Boston College International and Comparative Law Review
BFDUC – Boletim da Faculdade de Direito da Universidade de Coimbra
BJIL – Brooklyn Journal of International Law
BMJ – Boletim do Ministério da Justiça
BYIL – British Yearbook of International Law
CalLR – California Law Review
CDFUE – Carta dos Direitos Fundamentais da União Europeia
CDI – Comissão de Direito Internacional Público das Nações Unidas
CILJ – Cornell International Law Journal
CJIL – Connecticut Journal of International Law
CJoL – Chicago Journal of International Law
CJTL – Columbia Journal of Transnational Law
CKJIP – Chicago-Kent Journal of Intellectual Property
CL – Communications Law
CLAR – Columbia Law Review
CLJ – Computer Law Journal
CLR – Cornell Law Review
CLSR – Computer Law & Security Review
CMLR – Common Market Law Review
CNIL – Commission Nationale de l'Informatique et des Libertés
COM – Comissão Europeia
CPS – Comparative Political Studies
DA – Droit Administratif
DGVR – Deutsche Gesellschaft fur Volkerrecht
DJCIL – Duke Journal of Comparative and International Law
DPC – Data Protection Commissioner
DPLP – Data Protection Law & Policy
ECLaR - Electronic Communication Law Review
ECLR – European Constitutional Law Review
EDILR – Electronic Data Interchange Law Review
EDPL – European Data Protection Law Review
EDR – Edinburgh Law Review
EFAR – European Foreign Affairs Review
EHRLR – European Human Rights Law Review
EIPLR – European Intellectual Property Law Review
EILR – Emory International Law Review

EJIL – European Journal of International Law
EJIR – European Journal of International Relations
EJL – European Journal Law
EJLT – European Journal of Law and Technology
EJRR – European Journal of Risk Regulation
ELR – European Law Review
EM – Estado-Membro
EmLR – Emory Law Review
EP – ePública. Revista de Direito Público
EUA – Estados Unidos da América
EUP – European Union Politics
FDPD – Fórum de Proteção de Dados
FILJ – Fordham International Law Journal
FIPMELJ – Fordham Intellectual Property, Media and Entertainment Law Journal
FJIL – Florida Journal of International Law
FOIA – Freedom of Information Act
GeJIL - Georgetown Journal of International Law
GJIA – Georgetown Journal of International Affairs
GJIL – Groningen Journal of International Law
GIELR – Georgetown International Environmental Law Review
GLJ – German Law Journal
GYUL – German Yearbook of International Law
GSULR – Georgia State University Law Review
GWILR – George Washington International Law Review
G29 – Grupo de Trabalho do Artigo 29
HILJ – Harvard International Law Journal
HJIL – Houston Journal of International Law
HJLT - Harvard Journal of Law and Technology
HLR – Houston Law Review
HYIL– Hague Yearbook of International Law
ICLQ – International and Comparative Law Quarterly
IDPL – International Data Privacy Law
IJGLS - Indiana Journal of Global Legal Studies
IJLIT – International Journal of Law and Information Technology
IL – International Lawyer
ILJ – Indiana Law Journal
ILR – Iowa Law Review
IO – International Organisation
IOLR – International Organisations Law Review
IPSR - International Political Science Review
IRLCT – International Review of Law, Computers & Technology
IRLE – International Review of Law and Economics
JCMS – Journal of Common Market Studies
JCRDL – Journal of Contemporary Roman-Dutch Law
JDIP – Journal du Droit International Privé
JEPP – Journal of European Public Policy
JICLT – Journal of International Commercial Law and Technology
JICJ – Journal of International Criminal Justice
JMJCIL – John Marshall Journal of Computer and Information Law
LCLP – Law and Contemporary Legal Problems

LCP – Law and Contemporary Problems
LLR – Louisiana Law Review
LPIB – Law & Policy International Business
LPIB – Law & Policy International Business
MALR – Maine Law Review
MILR - Minnesota Law Review
MIJIL – Michigan Journal of International Law
MJECL – Maastricht Journal of European and Comparative Law
MJIL – Minnesota Journal of International Law
MLR – Maryland Law Review
MUJLT – Masaryk University Journal of Law and Technology
NWULR – Northwestern University Law Review
NYULR – New York University Law Review
NZULR – New Zealand Universities Law Review
OCDE – Organização para a Cooperação e Desenvolvimento Económico
OI – Organização Internacional
OIAC – Organização Internacional da Aviação Civil
OLR – Oslo Law Review
OMC – Organização Mundial do Comércio
OPC – Office of the Privacy Commissioner of Canada
OSLJ – Ohio State Law Journal
PDP – Privacy & Data Protection
PE – Parlamento Europeu
PLBIR – Privacy Laws & Business International Report
PLPR – Privacy Law and Policy Reporter
RCADI – Recueil des Cours de l'Academie de droit international
RCCS – Revista Crítica de Ciências Sociais
RCDIP – Revue Critique de Droit International Privé
RDI – Revista de Direito Intelectual
RDIPP – Rivista di diritto internazionale private e processuale
RIDC – Revue International de Droit Comparé
RIDP – Revista de Internet, Derecho y Politica
REDI – Revista española de Derecho internacional
RFDUSP – Revista da Faculdade de Direito da Universidade de São Paulo
RGPD – Regulamento Geral de Proteção de Dados Pessoais
RIDPC – Rivista italina di diritto pubblico comunitário
RIS – Review of International Studies
RMCUE – Revue du Marché Commun et de l'Union Européenne
ROA – Revista da Ordem dos Advogados
RTDE – Revue trimestrelle de droit européen
RTDP – Rivista Trimestrale di Diritto Pubblico
SCJ – Supreme Court of the United States of America
SEPD – Supervisor Europeu de Proteção de Dados
SJICL – Singapore Journal of International & Comparative Law
SJIL – Standford Journal of International Law
SLR – Stanford Law Review
SLRew – Southwestern Law Review
SSL – Scandinavian Studies in Law
STLR – Stanford Technology Law Review
SYIL – Spanish Yearbook of International Law

TEDH – Tribunal Europeu dos Direitos do Homem
TEJIL – The European Journal of International Law
TEL – Transnational Environmental Law
TICLJ – Temple International and Comparative Law Journal
TIJ – Tribunal Internacional de Justiça
TIJMCL – The International Journal of Marine and Coastal Law
TJUE – Tribunal de Justiça da União Europeia
TLR – The Tulane Law Review
TPIAJ – Tribunal Penal Internacional para a antiga Jugoslávia
TPA – Tribunal Permanente de Arbitragem
TSCJ – The Sedona Conference Journal
UCLR – University of Cincinnati Law Review
UE – União Europeia
UJIEL – Utrecht Journal of International and European Law
ULR – Utrecht Law Review
UPJIL – University of Pennsylvania Journal of International Law
UPJIEL – University of Pennsylvania Journal of International Economic Law
UPLR – University of Pennsylvania Law Review
UPLRw – University of Pittsburgh Law Review
USCASC – United States Court of Appeals for the Second Circuit
VancJIL – Vancouver Journal of International Law
VJIL – Virginia Journal of International Law
YLJ – Yale Law Journal
WILJ – Wisconsin International Law Journal

Declaração de carateres

849550

Resumos

Resumo: as questões colocadas pela extraterritorialidade e, em geral, pelo exercício de jurisdição do Estado não são novas. Contudo, nos últimos tempos suscitaram o interesse por parte da doutrina, sobretudo em relação à União Europeia, um sujeito que, no plano internacional, ocupa uma posição particular. Nesse sentido, o regime geral de proteção de dados pessoais ("regime") configura um objeto de estudo dessa posição da União Europeia e do modo como exerce jurisdição extraterritorial.

O presente trabalho visa, assim, (i) aferir em que medida se poderá afirmar que este regime goza de vocação extraterritorial e (ii) quais as manifestações e os limites da mesma. Para cumprir este duplo desiderato, na primeira parte da tese precisa-se o que se entende por extraterritorialidade, quem a exerce, em que termos e com que limites.

Delimitado este conceito, na segunda parte da tese procede-se à sua aplicação no domínio específico da proteção de dados pessoais. Este exercício não se alargará a toda a matéria da proteção de dados pessoais, mas apenas ao regime geral da União Europeia, em especial às novidades 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 ("RGPD") e que revoga a Diretiva 95/46/CE do Parlamento Europeu e do Conselho, de 24 de outubro de 1995, relativa à proteçao das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados ("Diretiva" ou Diretiva de 95"). Começo por apresentar e caraterizar esse regime, delimitando as suas fontes, o processo de "europeização" da proteção de dados pessoais que o mesmo implementa, a complexidade da sua natureza e, por fim, aponto as suas caraterísticas distintivas. Feito este enquadramento, procedo à identificação das manifestações de extraterritorialidade propriamente ditas no regime delimitado, em especial analisando o seu âmbito de aplicação e a configuração do regime das transferências de dados pessoais.

A terceira parte desta investigação incide sobre os limites das manifestações de extraterritorialidade anteriormente elencadas. Além de enunciar os obstáculos ao sucesso integral das pretensões da UE, aponto as soluções para os contornar que, em certos casos, já se encontram presentes no RGPD mas carecem de melhorias, ao passo que outras hipóteses não foram ainda consideradas pelo legislador.

Resumo em inglês: the questions posed by extraterritoriality and by the exercise of state jurisdiction are not new but have attracted a great deal of attention from the literature, especially in relation to the European Union, a subject in a particular position in the international landscape. The general regime for the protection of personal data constitutes an excellent object to study this practice of the European Union.

The purpose of this work is precisely that: to assess the extent to which that regime enjoys an extraterritorial reach and what are its limits. For this purpose, it is necessary to specify, in the first part of this thesis, what is meant by extraterritoriality, who exercises it, in what terms and with what restrictions.

After presenting the concept of extraterritoriality, I proceed to its application in the specific domain of personal data protection in the second part of the thesis. This exercise will not extend to all matters relating to the protection of personal data in the European Union, but only to the general regime focusing on the recent developments in the framework of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of individuals with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46 / EC ("GDPR").

Firstly, I present and characterize this regime, delimiting its sources, highlighting the process of "europeanization" of the protection of personal data, the complexity of its nature and, finally, pointing out its distinctive characteristics. Once this framework has been drawn up, I will identify the manifestations of extraterritoriality, specially by analyzing its scope and the configuration of the data transfers regime.

The third part of this investigation focuses on the limits of the extraterritoriality previously identified. In addition to stating these obstacles I will propose solutions, considering that some of these hypotheses are already present in the GDPR but need improvement, while others have not yet been considered by the European Union legislator.

Introdução. Enquadramento da questão e sequência

Desde 1995 que se multiplicam na doutrina estrangeira, segundo diferentes designações, reflexões sobre o tema que proponho tratar neste trabalho: "âmbito de aplicação amplo", "impacto" ou "efeito" extraterritorial, "extraterritorialidade", "jurisdição extraterritorial", "dimensão internacional" do "regime" ou do "direito" de proteção de dados pessoais da UE, entre outras[1]. Em Portugal, salvo raras exceções[2], este tema não tem merecido grande atenção por parte da doutrina. Além disto, sem prejuízo da publicação das obras estrangeiras, não se conhece uma investigação sistematizada sobre as manifestações e os limites da extraterritorialidade no campo da proteção de dados pessoais que, ao longo do tempo, apenas foram sendo enunciados pela doutrina de forma dispersa. É desta lacuna, da tentativa de a preencher, que nasce este trabalho.

Adicionalmente, este é um tema que ganhou uma importância renovada com o surgimento de um novo enquadramento normativo da proteção de dados pessoais por

[1] Brendan VAN ALSENOY, "Reconciling the (extra)territorial reach of the GDPR with public international law", Gert VERMEULEN & Eva LIEVENS (eds.), *Transatlantic tensions, EU surveillance, and big data,* Maklu, 2017, p. 77 e ss.; Christopher KUNER, "Extraterritoriality and regulation of international data transfers in EU data protection law", *IDPL,* vol. 5, n.º 4, 2015; US House of Representatives, "The EU Data Protection Directive: Implications for the US Privacy Debate", *Hearing before the Subcommittee on Commerce, Trade and Consumer Protection of the Committee on Energy and Commerce*, 8 de Março, 2001, n.º de série 107-19; Dan SVANTESSON, *Extraterritoriality in Data Privacy Law,* Ex Tuto, 2013, p. 89 e ss. e, do mesmo autor, "Extraterritoriality and targeting in EU data privacy law: the weak spot undermining the regulation", *IDPL,* vol. 5, n.º 4, 2015, p. 226 e ss.., "Article 4(1)(a) "establishment of the controller" in EU data privacy law – time to rein in this expanding concept", *IDPL,* vol. 6, n.º 3, 2016, p. 210 e ss. e "The Extraterritoriality of EU Data Privacy Law – Its Theoretical Justification and Its Practical Effect on U.S. Businesses", *SJIL,* n.º 50, 2014; Eduardo USTARAN, "The Scope of Application of EU data protection law and its extraterritorial reach", Noriswadi ISMAIL e Edwin CIEH (eds.), *Beyond Data Protection – Strategic Case Studies and Practical Guidance,* Springer, 2013, p. 144 e ss.; Joshua BAUCHNER, "State Sovereignty and the Globalizing Effects of the Internet: A Case Study of the Privacy Debate", *BJIL,* n.º 26, 2000-2001, p. 696 e ss.; Lee BYGRAVE, "Determining Applicable law pursuante to European Data Protection Legislation", *CLSR,* n.º 16, 2000, p. 252 e ss.; Liane COLONNA, *Legal Implications of Data Mining,* Ragulka, 2016 e, da mesma autora, "Article 4 of the EU Data Protection Directive and the irrelevance of the EU-US Safe Harbour Program?", *IDPL,* n.º 4, 2014, p. 203 e ss.; Lokke MOEREL, "Back to basics: when does EU data protection law apply?", *IDPL,* vol. 1, n.º 2, 2011, p. 97 e ss. e, da mesma autora, "The long arm reach of EU data protection law: Does the Data Protection Directive apply to processing of personal data of EU citizens by websites worldwide?", *IDPL,* vol. 1, n.º 1, 2011, p. 30 e ss.; Merlin GOMANN, "The new territorial scope of EU data protection law: deconstructing a revolutionary achievement", *CMLR*, n.º 54, 2017, p. 567 e ss.; Orla LYNSKEY, *The Foundations of EU Data Protection Law,* Oxford University Press, 2015, p. 41; Pedro ASENSIO, "Competencia y Derecho aplicable en el Reglamento General sobre Protección de Datos de la Unión", *REDI*, n.º 69, vol. 1, 2017, p. 75 e ss.; Paul De HERT e Michael CZERNIAWSKI, "Expanding the European data protection scope beyond territory: Article 3 of the General Data Protection Regulation in its wider context", *IDPL,* vol. 6, n.º 3, 2016, p. 234 e ss.; Yves POULLET, "Transborder Data Flows and Extraterritoriality: the European Position", *JICLT,* n.º 2, 2007, p. 141 e ss..

[2] Anabela De Sousa GONÇALVES, "The extraterritorial application of the EU Directive on data protection", *SYIL,* n.º 19, 2015, p. 195 e ss..

ocasião da entrada em vigor 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 ("RGPD") e que revoga a 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 ("Diretiva" ou "Diretiva de 95"). O RGPD é fruto de uma reforma legislativa, iniciada em 2009, pela Comissão Europeia, que culminou, em 2012, com a apresentação de uma primeira proposta de revisão da Diretiva através de um Regulamento[3].

Como qualquer trabalho de investigação, o tratamento do tema que se apresenta pressupõe esclarecimentos conceptuais prévios e, naturalmente, conhece limites. Haverá, desde logo, que perguntar, o que é a "extraterritorialidade"? Nos autores que se debruçam sobre esta questão é frequente a constação de que num mundo cada vez mais interdependente, caraterizado pela internacionalização da vida quotidiana e das relações humanas, e pela globalização, o recurso à extraterritorialidade se banalizou. Porém, esta constatação nem sempre é acompanhada por um exercício de compreensão daquele instituto, pela identificação das razões que o mobilizam, das condições e limites que o balizam, dos seus efeitos e dos problemas práticos que coloca. São estes aspetos do "ADN" da extraterritorialidade que apresento na Parte I, uma antecâmara do tratamento na especialidade daquele instituto. Esta caraterização prévia do instituto da extraterritorialidade é essencial para cumprir o objetivo desta investigação: identificar, sistematizar e caraterizar, na Parte II e III, as manifestações e os limites da extraterritorialidade no domínio específico do regime de proteção de dados pessoais da UE.

Mas aí impõe-se uma nova delimitação do campo de investigação desta tese: a que realidade aplicar o conceito definido na Parte I? Quais as fontes do regime de proteção de dados pessoais da UE? Respondo a estas perguntas no Capítulo 1, da Parte II, onde procuro enunciar os contornos deste regime, explorando as suas dimensões, natureza e caraterísticas distintivas. Os Capítulos 2 e 3, seguimentos lógicos e cronológicos do precedente, centram-se na identificação, caraterização e sistematização das manifestações

[3] Foi em 2012 que a COM apresentou a primeira versão do que viria a ser o RGPD. Por esta razão optei por designar este processo legislativo "reforma de 2012". Antecede-lhe um longo processo de consulta pública, decorrido entre junho e dezembro de 2009, cuja informação e documentação se encontra disponível em https://ec.europa.eu/home-affairs/what-is-new/public-consultation/2009/consulting_0003_en, consultado no dia 30 de setembro de 2018.

de extraterritorialidade do regime previamente delimitado. Pretendo estudar a evolução destas manifestações desde a Diretiva de 95 até ao RGPD.

No Capítulo 2 ocupo-me do âmbito de aplicação do regime em apreço já que, a meu ver, deve ser esse o primeiro elemento a apreciar para verificar se o legislador da UE pretendeu atribuir apenas alcance territorial aos seus comandos. O Capítulo seguinte incide sobre o regime das transferências de dados pessoais para países terceiros cujas hipotéticas implicações extraterritoriais são sugeridas logo neste enunciado linguístico com a alusão aos "países terceiros". Em ambos os Capítulos interessa-me, sobretudo, salientar o que há de novo no RGPD.

Finalmente, na última Parte desta dissertação, na Parte III, procedo a um levantamento dos limites às manifestações de extraterritorialidade anteriormente sistematizadas, problematizando-os e discutindo soluções para alcançar uma aplicação adequada e eficaz daquelas.

Enfim, em jeito de síntese, com a margem de generalidade que se impõe numa introdução, são estas as principais questões que coloco e para as quais procurarei respostas em cada parte deste trabalho:

(1) O que é a extraterritorialidade, quem a exerce, em que termos, com que balizas e quais os seus efeitos (Parte I)?
(2) Existem manifestações de extraterritorialidade no regime geral de proteção de dados pessoais da UE (Parte II)?
(3) Se sim, quais são, qual a sua razão de ser e que limites conhecem (Parte III)?

Delimitado o objeto desta dissertação e exposto o caminho que pretendo trilhar, merece uma palavra o método que usarei. O acolhimento de contributos interdisciplinares é cada vez mais relevante em todas as áreas do Direito e sê-lo-á também para a análise do tema que me ocupa. Com efeito, o mesmo não tem uma sede dogmática própria o que me obriga a recorrer a várias disciplinas distintas, como o Direito Internacional Público e Privado, o Direito da União Europeia, o Direito Constitucional, os Direitos Fundamentais ou o Direito Administrativo (nacional e internacional). Desde logo, o tratamento da extraterritoralidade pode ser sediado no Direito Internacional Público ou Privado, enquanto que a regulação da proteção de dados pessoais foi fortemente influenciada pelo Direito da União Europeia, pelo Direito Constitucional e pelos Direitos Fundamentais. Em todo o caso, centrarei a minha análise, sobretudo, no Direito

Internacional Público, para o estudo da extraterritorialidade, como tem sido a prática[4], e no Direito da União Europeia, no que à proteção de dados pessoais diz respeito.

Para responder às perguntas enunciadas utilizarei o método da ciência jurídica, isto é, parto da interpretação do direito positivo, bem como da doutrina e da jurisprudência que geralmente lhe estão associadas. Adicionalmente, merece referência uma fonte específica do domínio em apreço que tomarei em conta: as deliberações, opiniões e pareceres das autoridades de controlo e, em particular, do Grupo do Artigo 29 ("G29"), constituído ao abrigo do artigo 29.º da Diretiva e que, como ali se pode ler, tinha como atribuição, *inter alia,* analisar questões relativas à aplicação do regime de proteção de dados pessoais "com vista a contribuir para a sua aplicação uniforme". Ao abrigo dos artigos 68.º e seguintes do RGPD, sucede ao G29 o Comité Europeu de Proteção de Dados Pessoais, cujas orientações, pareceres e demais posições foram analisadas. Sublinho que as fontes consultadas para este trabalho, em especial daquele Comité, bem como as decisões judiciais estudadas, limitam-se àquelas publicadas até à data de finalização da investigação para este trabalho, o dia 30 de setembro de 2018.

Por fim, a riqueza do objeto deste estudo revelou ser o seu principal desafio. A bem da legibilidade e inteligibilidade do mesmo, centrei-me nos pontos essenciais para conceptualizar e discutir a extraterritorialidade do regime geral de proteção de dados pessoais da UE. Por esta razão, ficam de fora vários assuntos e temas parcelares, como o da territorialidade da jurisdição, da soberania do Estado, ou até uma análise comparativa do regime da UE com o de outras latitudes que, sem prejuízo da sua relevância, dariam azo a excursos dilatórios, paralelos e de pouco valor à luz dos contributos doutrinais já existentes. De facto, o grosso destes temas foi, no passado, exaustivamente tratado por outros autores pelo que me esforcei para deles extrair apenas o que poderia ser relevante para as minhas conclusões.

[4] G29, "Documento de trabalho sobre a determinação da aplicação internacional da legislação da UE em matéria de proteção de dados ao tratamento de dados pessoais na Internet efetuado por sites não europeus", 30 de maio de 2002, p. 2 e Christopher KUNER, "Data Protection Law and International Jurisdiction on the Internet (Part 1)", *IJLIT,* vol. 18, n.º 2, 2010, p. 184.

Parte I – A teoria e a prática da extraterritorialidade

A reflexão sobre a teoria e a prática da extraterritorialidade, de natureza sintética e referencial, arranca no Capítulo 1, com a procura de respostas para o *quê*, o *quem* e o *como* da extraterritorialidade: o que é (1.1), quem a pode exercer ou titular (1.2.) e como se manifesta (1.3.)?

O Capítulo 2 é direcionado para o funcionamento na prática da extraterritorialidade, para os interesses que a mobilizam (2.1), os limites do direito internacional público que a balizam (2.2) e os efeitos do seu exercício (2.3).

Capítulo 1 – Definição, titulares e categorias

1.1.Definição

Uma marca genética deste conceito é a pluralidade significativa, bem visível na doutrina que dele cuida. Entre nós D. LOPES refere-se à "jurisdição extraterritorial do Estado" como o "conjunto de situações em que o Estado está habilitado, usualmente por via unilateral, a dizer o direito aplicável a situações internacionais"[5]. Por seu turno F. LOUREIRO BASTOS explica que a "extraterritorialidade determina que as normas de uma determinada ordem jurídica possam vir a produzir efeitos no espaço geográfico de uma ordem jurídica distinta"[6]. No estrangeiro C. RYNGAERT enquadra neste conceito as situações "em que um Estado regula assuntos que, tendo uma ligação com outro Estado, não são de preocupação exclusivamente doméstica"[7]. Muito próximas desta definição encontram-se as seguintes: de A. BIANCHI ("situações em que o Estado regula assuntos de natureza não exclusivamente doméstica ou, por outras palavras, assuntos que apresentam ligações, mais ou menos significativas, com outras ordens jurídicas"[8]), a proposta de B. STERN ("situações em que uma parte ou a totalidade do processo de

[5] Dulce LOPES, *Eficácia, Reconhecimento e Execução de Atos Administrativos Estrangeiros,* Policopiado, 2015, p. 38.
[6] Fernando Loureiro BASTOS, "Algumas notas sobre globalização e extraterritorialidade", *Liber Amicorum Fausto de Quadros,* vol. I, 2016, p. 442.
[7] Cedric RYNGAERT, *Jurisdiction in International Law,* Oxford University Press, 2015, p. 6.
[8] Andreas BIANCHI, "Reply to Professor Maier", Karl MEESSEN (ed.), *Extraterritorial Jurisdiction in Theory and Practice,* Brill, 1996, p. 74 e ss..

aplicação [das normas] se desenrola fora do território que as adotou"[9]), a sugestão de P. DEMARET, ("quando a autoridade legislativa, governamental, judicial ou administrativa de um Estado dirige a um sujeito uma imposição de fazer ou não fazer que será executada no todo ou em parte no território de outro Estado"[10]) e a hipótese de A. GUZMAN, ("a capacidade de um país governar a atividade ocorrida em países estrangeiros"[11]).

Diante desta dispersão de definições a CDI, cuja função é contribuir para o desenvolvimento do DIP[12], procedeu a um estudo sobre a extraterritorialidade no qual apresentou a seguinte definição: o "exercício de jurisdição extraterritorial por um Estado é uma tentativa de regular, através de atos legislativos, judiciais ou executivos, a conduta de pessoas, bens ou atos, além das suas fronteiras, que afetam os seus interesses na ausência de regulação pelo DIP" [13]. Como se vê, esta definição decompõe-se em vários elementos: (i) o exercício de jurisdição por um Estado (ii) através de uma tentativa regulatória manifestada em diferentes tipos de atos (iii) incidentes sobre a conduta de pessoas, bens ou atos, além das fronteiras do respetivo território, mas que afetam os interesses do Estado (iv) na ausência de regulação do DIP.

Porém, apesar desta tentativa da CDI para fixar os termos de uma definição de jurisdição extraterritorial ou de extraterritorialidade[14], a mesma continua, na prática, a gerar confusões conceptuais[15] e, com o passar do tempo, foi sendo atualizada em vários dos seus elementos, nomeadamente no que respeita aos *titulares*[16].

---

[9] Brigitte STERN, "L'extraterritorialité 'revisitée': où il est question des affaires *Alvarez-Machain, Pâte Bois* et de quelques autres", *AFDI,* vol. 38, n.º 1, 1992, p. 239 e 242.

[10] Paul DEMARET, L'extraterritorialité des lois et les relations transatlantiques: une question de droit ou de diplomatie?", *RTDE,* vol. 21, n.º 1, 1985, p. 1 e ss..

[11] Andrew GUZMAN, "Is International Antitrust Possible?", *NYULR,* n.º 73, 1998, p. 1506.

[12] Patrícia G. TELES, "O contributo das Nações Unidas e da Comissão de Direito Internacional para a formação do Direito Internacional: breve balanço por ocasião do 70.º aniversário da organização das Nações Unidas", *Themis,* ano XVII, n.º 30/31, 2016, p. 15 e ss..

[13] CDI, "Report on the Work of its Fifty-Eight Session", 1 May-9 June and 3 July-11 August 2006, UN Doc. A/61/10, Annex E, n.º 2, disponível em http://legal.un.org/ilc/documentation/english/reports/a_61_10.pdf, consultado no dia 30 de setembro de 2018.

[14] Ao longo deste trabalho, para simplificar a sua linguagem e facilitar a sua leitura, usarei os dois termos como sinónimos, à semelhança de outros autores, v. Menno KAMMINGA, "Extraterritoriality", *The Max Planck Encyclopedia of Public International Law,* Vol. III, Oxford University Press, 2012.

[15] C. RYNGAERT, *Jurisdiction* cit., p. 7 e Parte I, Capítulo 2, ponto 2.2.2. sobre "os princípios da jurisdição extraterritorial".

[16] Procedendo a essa atualização no âmbito da jurisdição penal do Estado, v. Pedro CAEIRO, *Da Jurisdição Penal do Estado,* Coimbra Editora, 2010, p. 10 e ss..

1.2.Titularidade ativa e passiva

A definição avançada pela CDI refere-se ao exercício de jurisdição extraterritorial pelo Estado*,* apresentando-o como titular *exclusivo* daquela. Mas, afinal, o que é a *jurisdição*, quem, nos dias de hoje, a pode exercer (*titularidade ativa)* e quais os seus destinatários (*titularidade passiva*)?

A palavra "jurisdição" é utilizada em várias aceções, sendo a mais frequente a de poder atribuído ao conjunto dos tribunais de um Estado ou a uma determinada categoria de tribunais. Contudo, para o propósito deste trabalho esta é uma variante limitada na medida em que o mesmo não incide sobre os tribunais. Por conseguinte, não me afastando excessivamente da etimologia deste termo no Latim, que corresponde a *ius* ou *juris* (direito) e *dicere* (dizer)[17], proponho a sua utilização numa outra aceção mais aberta, flexível e menos rígida: o "poder de resolver problemas"[18].

Com efeito, este é o entendimento que melhor se ajusta à realidade internacional na medida em que nem sempre são os Estados a resolver os problemas globais nem a "dizer o direito" [19] aplicável aos mesmos como, aliás, evidenciam as novas formas de normatividade que extravasam o DIP e o direito estadual, as novas "jurisdições" fora do Estado[20]. A doutrina tem-se-lhes reportado, por exemplo, em relação aos sujeitos de âmbito internacional com poderes de autoridade e regulatórios[21], como é o caso do ICANN[22] – *Internet Corporation for Assigned Names and Numbers* – uma empresa privada norte-americana que gere os aspetos técnico-administrativos dos nomes dos domínios na Internet, e da ISO – *International Standardization Organization* – que

---

[17] Costas DOUZINAS, "The Metaphysics of Jurisdiction"*,* Shaun MCVEIGH, *Jurisprudence of Jurisdiction,* Routledge, 2007, p. 21.

[18] Phillip JESSUP, *Transnational Law,* Yale University Press, 1956, p. 35 e ss. e, entre nós, D. LOPES, *Eficácia* cit., p. 39.

[19] Frederick MANN, "The doctrine of jurisdiction in international law", *ADIRC,* n.º 111, I, 1964, p. 9 e ss., reimpresso em *Studies in International Law,* Clarendon Press Oxford, 2008, p. 11 e ss. e, do mesmo autor, "The doctrine of international jurisdiction revisited after twenty years", *ADIRC,* n.º 186, III, 1984, p. 13 e ss.; Maarten HEIJER e Rick LAWSON, "Extraterritorial Human Rights and the Concept of 'Jurisdiction', Malcolm LANGFORD *et alii* (eds.), *Global Justice, State Duties – The Extraterritorial Scope of Economic, Social and Cultural Rights in International Law,* Cambridge University Press, 2013, p. 153 e ss..

[20] No domínio do ciberespaço, v. Alexandre PEREIRA, *Direitos de Autor e Liberdade de Informação*, Almedina, 2008, p. 321. Em geral, v. Cristina QUEIROZ, *Direito Constitucional Internacional,* Coimbra Editora, 2011, p. 38.

[21] Giacinto CANANEA, "I pubblici poteri nello spazio giuridico globale", *RTDP,* n.º 1, 2003, p. 1 e ss.; Jorge SAMPAIO, *O Acto Administrativo Pela Estrada Fora*, Associação Académica da Faculdade de Direito de Lisboa, 2014, p. 41; Miguel Prata ROQUE, *A Dimensão Transnacional do Direito Administrativo*, AAFDL, 2014, p. 868, nota de rodapé 2381; Pedro GONÇALVES, *Entidades Privadas com Poderes Públicos,* Almedina, 2005, p. 103 e ss.;

[22] Joachim ZEKOLL, "Jurisdiction in Cyberspace", Gunther HANDL *et alii*, *Beyond Territoriality. Transnational Legal Authority in an Age of Globalization,* Martinus Nijhoff Publisher, 2012, p. 369.

desempenha um papel central na uniformização de prescrições técnicas transnacionais e na criação de procedimentos de certificação[23]. Nesse sentido constata-se toda uma constelação de sujeitos no cenário internacional, "novos agentes do poder político"[24], que flexibilizam o conceito de jurisdição a reboque de outras noções, como a de personalidade jurídica internacional[25].

É certo que, paralelamente, se colocam problemas jusfilosóficos sobre o que *é o direito* neste contexto. Como sublinha A. SANTOS CAMPOS, a "matriz de entendimento do direito tendeu em décadas recentes a perder um referente sócio-político, em virtude de a entrada no século XXI trazer um conjunto de desafios concretos de várias índoles ao âmbito da normatividade jurídica. Numa palavra, esses desafios decorrem da chamada *globalização,* neste caso das próprias fontes de direito"[26].

A refração mais óbvia à estadualidade da jurisdição, e aquela que neste particular mais releva, é a própria UE enquanto produtora de instrumentos jurídicos não reconduzíveis às formas canónicas do DIP ou do direito estadual[27]. À luz da sua originalidade, autonomia e autoridade, conciliadas com uma noção de "soberania funcional", a UE posiciona-se lado a lado com os Estados no contexto internacional[28]. Por conseguinte, a UE encontra-se sujeita, nos domínios da sua competência, às mesmas regras e limites de DIP que os Estados quando exercem jurisdição extraterritorial. O tema tem sido aflorado, de forma consensual, pelos autores que se debruçam sobre os vários domínios nos quais a UE tem adotado legislação com vocação extraterritorial, designadamente o direito da

[23] Sobre o papel da ISO em matéria de proteção de dados pessoais, v. Working Party for Information and Security and Privacy (WPISP), *The evolving privacy landscape: 30 years after the OECD Privacy Guidelines,* Directorate for Science, Technology and Industry – Committee for Information, Computer and Communications Policy, 2011, p. 113.

[24] M. Prata ROQUE, *A Dimensão* cit., p. 201.

[25] D. LOPES, *Eficácia, Reconhecimento e* cit., p. 85. Relatando exemplos de jurisdição penal de entidades não-estatais v. P. CAEIRO, *Da Jurisdição* cit., p. 67 e ss..

[26] Com efeito, a matriz de entendimento do direito até então assentava nos chamados "teste de *pedigree"* concebidos num contexto de associação de um sistema jurídico à produção normativa imputável a um Estado (mesmo que por várias fontes ligadas de alguma maneira a esse Estado). Desenvolvendo, v. André SANTOS CAMPOS, *Glosas Abertas de Filosofia do Direito. Um tronco comum para juristas e filósofos,* Quid Juris, 2013, p. 316 e ss..

[27] Além da UE, P. CAEIRO aponta outros exemplos de jurisdições não estatais no domínio do direito penal, v. P. CAEIRO, *Da Jurisdição ...* cit., p. 67 e ss..

[28] Bernard OXMAN, "Jurisdiction of States", *The Max Planck Encyclopedia of Public International Law,* vol. IV, Oxford University Press, 2012, p. 548; Christiana ALHBORN, "The Rules of International Organizations and the Law of International Responsibility", *IOLR,* vol. 8, n.º 2, 2011, p. 397 e, entre nós, D. LOPES, *Eficácia, Reconhecimento e* cit., p. 66; Violeta MORENO-LAX e Cathryn COSTELO, "The extraterritorial application of the EU Charter of Fundamental Rights: from territoriality to facticity, the effectiveness model", Steve PEERS *et alii*, *The EU Charter of Fundamental Rights: A Commentary,* Hart Publishing, 2014, p. 1663 citando Michael P. SCHARF, *The Law of International Organisations,* Carolina Academic Press, 2007.

concorrência e o direito do ambiente[29]. De resto, a própria instância da União tem sublinhado que aquela é "obrigada a reiterar o direito internacional na sua totalidade"[30].

Portanto, e no que respeita à titularidade da extraterritorialidade, os sujeitos *ativos* ou quem a exerce, podem ser entidades estaduais ou não estaduais, como a UE, que doravante designarei genericamente como "entidade do foro ou de origem". Por seu turno, no que respeita aos sujeitos *passivos* ou destinatários do exercício da extraterritorialidade, a resposta é facetada, distinguindo-se entre destinatários *diretos*, as pessoas singulares ou coletivas visadas pelos comandos da entidade do foro, ou *indiretos*, podendo ser outros Estados ou a própria UE, que doravante designarei por "entidade *ad quem* ou de destino".

1.3.Categorias

A definição apresentada pela CDI, à semelhança de outras, não reporta um conceito monolítico ou unitário, antes se desdobrando em vários atos que permitem enunciar as três categorias da jurisdição extraterritorial: prescritiva, adjudicativa e de execução[31].

A jurisdição prescritiva corresponde ao poder de disciplinar juridicamente uma determinada matéria através da criação de normas de conduta. Encontramo-la associada,

---

[29] Christopher KUNER, "The European Union and the Search for an International Data Protection Framework", *GJIL,* vol. 2, n.º 2, 2014, p. 55 e ss. e, do mesmo autor, "The Internet and the global reach of EU law", LSE Law Working Paper Series 04/2017, University of Cambridge Faculty of Law, Research Paper No. 24/2017; Cedric RYNGAERT, "Whither Territoriality? The European Union's Use of Territoriality to Set Norms with Universal Effects", *What's Wrong with International Law,* Brill, 2015, p. 434 e ss.; Elaine FAHEY, *The Global Reach of EU Law,* Routledge, 2017, p. 2 e ss.; Joanne SCOTT, "Extraterritoriality and Territorial Extension of EU Law", *AJCL*, vol. 62, n.º 1, 2014, p. 88 e, da mesma autora, "The New EU 'Extraterritoriality'", *CMLR,* vol. 51, 2014, p. 1343 e ss.; "Contingent Unilateralism: International Aviation in the European Emissions Trading Scheme", Bart VAN VOOREN *et alii* (eds.), *The EU Role in Global Governance: The Legal Dimension,* Oxford University Press, 2013; "Developments in the Law-Extraterritoriality", *HLR,* n.º 124, 2011, p. 1226 e ss.; Joanne SCOTT e Lavanya RAJAMANI, "EU Climate Change Unilateralism", *EJIL*, vol. 23, n.º 2, p. 469.

[30] Acórdão do TJ, Air Transport Association of America *et alii* c. Secretary of State for Energy and Climate Change*,* C-366/10, 21 de dezembro de 2011, n.º 101 e 123, citando várias decisões anteriores.

[31] Esta diferenciação encontra-se nos trabalhos da CDI, "Report …" cit., n.º 5 e, nos EUA, no influente *Restatement of the Law Third, The Foreign Relations Law of the United States*, § 401. Este instrumento, da autoria do *American Law Institute*, resume o direito internacional aplicável aos EUA, v. *Restatement of the Law Third, The Foreign Relations Law of the United States*, American Law Institute, 1987. Entre nós, v. Jónatas MACHADO, *Direito Internacional: do paradigma clássico ao pós-11 de setembro,* Coimbra Editora, 2013, p. 232; Luís LIMA PINHEIRO, *Direito Internacional Privado,* vol. I, Almedina, 2003, p. 329; M. Prata ROQUE, *A Dimensão* cit., p. 1064; P. CAEIRO, *Da Jurisdição ...* cit., p. 41; Rui MOURA RAMOS, *Da Lei Aplicável ao Contrato de Trabalho Internacional,* Almedina, 1991, p. 15 e 16. No estrangeiro, Anthony COLANGELO, "Constitutional Limits on extraterritorial jurisdiction: Terrorism and the intersection of national and international law*", HILJ*, n.º 48, 2007, p. 126; v. B. OXMAN, "Jurisdiction …" cit., p. 547; C. KUNER, "Data Protection Law ..." cit., p. 186; D. SVANTESSON, *Extraterritoriality in* cit., p. 67; François RIGAUX, "Refléxions sur les rapports entre le droit international privé et le droit des gens", *Estudios de Derecho Internacional – Homenaje a D. Antonio de Luna,* Instituto Francisco Vitoria, 1968, p. 575; Hannah BUXBAUM, "Territory, territoriality and the resolution of jurisdictional conflict", *AJCL*, n.º 3, 2009, p. 632; Roger O'KEEFE, "Universal Jurisdiction. Clarifying the basic concept", *JICJ*, n.º 2, 2004, p. 736;

em alguma doutrina, a uma "competência legislativa ou poder legislativo"[32] ou "jurisdição legislativa"[33]. A jurisdição adjudicativa, por seu lado, traduz o poder de apreciar, decidir e julgar determinada situação da vida pelo poder judicial. O terceiro e último sentido – a jurisdição de execução – corresponde ao momento de concretização do direito (ou dever), o poder de adotar medidas de caráter punitivo para assegurar o cumprimento das normas, reagir contra o incumprimento e realizar atos de coerção material[34].

Esta categorização merece dois apontamentos que dizem respeito à sua utilidade analítica e à natureza aberta de cada categoria. Em primeiro lugar, há quem proponha um conceito amplo de jurisdição de execução e questione a necessidade de autonomizar a jurisdição adjudicativa, já que a atividade desenvolvida pelos tribunais pode ser enquadrada na jurisdição prescritiva (nos sistemas de *common law* ou quando as decisões são meramente declarativas) ou na jurisdição de execução (quando engloba os poderes dos tribunais de adotar medidas de caráter punitivo)[35]. Acresce, como sublinha D. LOPES, que o "poder de apreciar, decidir e julgar determinada situação da vida" é da responsabilidade de outros órgãos, designadamente administrativos, que "também procedem a uma tarefa *adjudicativa* do direito"[36]. O segundo apontamento, ao qual voltarei adiante, respeita à própria natureza da jurisdição de execução: a territorialidade da coercividade dos poderes públicos estaduais[37].

[32] M. Prata ROQUE, *A Dimensão* cit., p. 601 e 1064.
[33] A. COLANGELO, "What is ..." cit., p. 1310; P. CAEIRO, *Da Jurisdição Penal* cit., p. 42; Willis REESE, "Legislative Jurisdiction", *CLAR,* n.º 78, n.º 8, December, 1978, p. 1587.
[34] D. SVANTESSON, *Extraterritoriality* cit., p. 68.
[35] B. OXMAN, "Jurisdiction …", nota 4, p. 55; P. CAEIRO, *Da Jurisdição Penal* cit., p. 41 e R. O'KEEFE, "Universal Jurisdiction. Clarifying…" cit., p. 736 e ss.; Alex MILLS, "Rethinking Jurisdiction in International Law", *BYIL,* vol. 84, n.º 1, 2014, p. 195; Antonio CASSESE, *International Law,* Oxford University Press 2005, p. 49 e ss.; Marko MILANOVIC, *Extraterritorial Application of Human Rights Treaties. Law, Principles and Policy,* Oxford University Press, 2011, p. 23; Michael AKEHURST, "Jurisdiction in International Law", *BYIL*, n.º 46, 1972-1973, p. 145 e ss.; Robert JENNINGS e Arthur WATTS, *Oppenheim's International Law,* 9ª edição, vol. I, Peace, 1992, p. 456; Vaughan LOWE, "Jurisdiction", M. EVANS (ed.) *International Law,* Oxford University Press, 2006, p. 338 e ss..
[36] D. LOPES, *Eficácia* cit., p. 41, nota de rodapé 43.
[37] Hans KELSEN, *General Theory of Law and State,* The Law Book Exchange Ltd, 1945 e, do mesmo autor, *Teoria Pura do Direito,* Vol. I, 2ª ed., Arménio Amado Editor, 1962, p. 64 e ss..

Capítulo 2 – A extraterritorialidade na prática

2.1. Os interesses prosseguidos

O "fenómeno da extraterritorialidade", como lhe chama I. JALLES[38], não é de agora. Há muito que os Estados intervêm, unilateralmente, no contexto internacional, munidos de normas de particular intensidade valorativa, como é o caso das "leis de aplicação imediata"[39]. Por outro lado, o âmbito da jurisdição da entidade do foro é "amplo e fluído"[40] sendo frequentemente instrumentalizado para "assegurar o desempenho e autonomia estatais, permitindo que os Estados cumpram todas as funções que lhes competem, ramificando a sua intervenção externa, se necessário"[41]. Com efeito, a jurisdição da entidade do foro não se compreende apenas por referência a um território. Cabem ali elementos pessoais (dos indivíduos vinculados às normas daquela) e elementos funcionais, em especial quando o exercício de autoridade procura alcançar certos *efeitos*[42]*,* esfumando-se a componente territorial como sucede quando a entidade do foro assume jurisdição com base na mera convicção de que a eficácia de uma regra ou de um regime jurídico depende da sua aplicação fora de portas ou que certos atos cometidos além-fronteiras violam normas imperativas nacionais e internacionais ou têm implicações sérias no território nacional[43]. Assim, se nunca vigorou uma regra estrita de territorialidade, como parece suceder[44], a evolução das relações "internacionais" ou "transnacionais", a frequência e a intensidade dos desafios que se colocam à capacidade de a entidade do foro manter a sua autoridade, proteger os indivíduos, e se projetar no exterior, são fatores que obrigam, se não à recusa radical daquela regra, pelo menos a uma reinvenção ou adaptação da mesma[45].

Cada vez mais o termo "independência" não faz jus às vulnerabilidades experimentadas pela entidade do foro a eventos que ocorrem fora do seu território o que impulsiona o recurso à jurisdição extraterritorial. Daí a distinção entre a conceção clássica

---

[38] Isabel JALLES, *Extraterritorialidade e Comércio Internacional. Um Exercício de Direito Americano,* Universidade Católica, 1986, p. 37.
[39] Dando nota desta tendência no Direito Público, v. M. Prata ROQUE, *A Dimensão* cit., p. 139.
[40] D. LOPES, *Eficácia* cit., p. 41.
[41] *Ibidem*.
[42] D. LOPES, *Eficácia* cit., p. 40.
[43] Armand MESTRAL, "The Extraterritorial Extension of Laws: How Much as Changed?", *AJICL,* vol. 31, n.º 1, 2014, p. 46.
[44] V., *inter alia,* Saskia SASSEN, *Losing Control – Sovereignty in na Age of Globalization,* Columbia University Press, 1996, p. 4. Entre nós v. D. LOPES, *Eficácia* cit., p. 38; M. Prata ROQUE, *A Dimensão* cit., p. 62 e ss..
[45] R. MOURA RAMOS, *Da Lei ...* cit., p. 279.

da extraterritorialidade e as suas manifestações *contemporâneas*[46] presentes em cada vez mais domínios: concorrência[47], ambiente[48], imigração[49] e, de enorme relevância para este trabalho, a Internet[50]. Sem pretender apresentar um mapeamento exaustivo dos interesses subjacentes a estas manifestações contemporâneas da extraterritorialidade, identifico e exemplifico dois tipos de interesses que a jurisdição extraterritorial visa prosseguir: de natureza *interna,* ligados à entidade do foro, e de natureza *externa*, ligados à comunidade internacional. Como procurarei demonstrar, ao contrário do que sugere a definição da CDI, a extraterritorialidade vem sendo usada para prosseguir interesses da entidade do foro *e* da comunidade internacional.

2.1.1. Interesses ligados à entidade do foro

A interdependência crescente das economias por via do comércio internacional, a força centrípeta da globalização[51], as vulnerabilidades das entidades do foro em face da "sociedade aberta"[52], são fatores que instigam o exercício da jurisdição extraterritorial[53]. S. BATTINI considera que a interdependência internacional em áreas como a economia e o ambiente converte a extraterritorialidade num fenómeno não excecional, alegando que a extraterritorialidade *de iure* visa contrariar efeitos de uma extraterritorialidade *de facto,* sendo por isso um fenómeno crescente e inevitável[54]. Já A. NEWMAN e R. POSNER concluem que as regras aplicáveis aos mercados financeiros não são adotadas através de consensos internacionais, mas resultam, com frequência, da extraterritorialidade prescritiva de "hiper-reguladores" como é o caso da UE[55]. Em sentido semelhante, a CDI deu nota de que "a globalização da economia global leva os Estados a exercerem

[46] M. Prata ROQUE, *A Dimensão* cit., p. 208.
[47] *Idem*, p. 205.
[48] CDI, "Report ..." cit., Anexo E, nota de rodapé 18.
[49] *Ibidem*.
[50] Sobre a extraterritorialidade na Internet, v. Chris REED, *Making Laws for Cyberspace,* Oxford University Press, 2012, p. 34 e Utah KOHL, "Eggs, Jurisdiction, and the Internet", *ICLQ*, vol. 51, n.º 3, 2002, p. 579.
[51] Proceder a uma caraterização consensual da já tantas vezes apregoada globalização não é uma tarefa fácil nem cabe neste meu propósito, bem mais modesto, para o qual importa apenas destacar, a propósito do tema da globalização, a sua natureza transformacionista e o seu caráter promotor de mudanças económicas, sociais e políticas rápidas, indutoras da reengenharia dos poderes públicos.
[52] Jurgen BASEDOW, *The Law of Open Societies. Private Ordering and Public Regulation in the Conflict of Laws,* Brill/Nijhoff, 2012, p. 36.
[53] Gareth DAVIES, "International Trade, Extraterritorial Power, and Global Constitutionalism: A Perspective from Constitutional Pluralism", *GLJ,* vol. 13, n.º 11, 2012, p. 1203.
[54] Stefano BATTINI, "Globalisation and Extraterritoriality: an Unexceptional Exception", Gordon ANTHONY *et alii* (eds.), *Values in Global Administrative Law,* Hart Publishing, 2011, cit., p. 67.
[55] Abraham NEWMAN e Elliot POSNER, "International interdependence and regulatory power: Authority, mobility and markets", *EJIR,* vol. 17, n.º 4, 2011.

jurisdição extraterritorial para proteção dos seus interesses económicos *vis-à-vis* empresas multinacionais e outros atores globais"[56].

Em segundo lugar, no quadro da "sociedade de risco global"[57], as entidades do foro são confrontadas com um "aumento exponencial de situações de relevância internacional que carecem de uma intervenção ou reação pronta"[58]. O exercício de jurisdição extraterritorial poderá corresponder a uma tentativa de intervir, reagir ou defender, no plano externo, interesses nacionais, direitos e posições jurídicas individuais [59]. É essa a conclusão que resulta da evolução dos princípios da jurisdição extraterritorial adiante apresentados: tanto a "teoria dos efeitos" como o princípio da universalidade fundam-se nos "direitos dos indivíduos", como "fundamentos últimos"[60], correspondendo a formas de "proximidade desterritorializada" entre uma parte estrangeira e um indivíduo (exemplos: consumidor, vítima de um crime)[61]. Por outro lado, segundo a teoria dos deveres de proteção de direitos fundamentais, em especial as considerações a propósito dos "perigos com conexões internacionais", isto é, "diretamente causados por Estados estrangeiros ou com origem nos respetivos territórios"[62], vigora um relativo consenso quanto à tese de que a entidade do foro não se deve demitir do dever de proteção apenas porque a *fonte* da ameaça ou perigo se encontra no estrangeiro pelo que se tem pugnado pela aplicação de um "princípio da irrelevância da origem da ameaça"[63]. Cabe sempre à entidade do foro ponderar a utilidade social e económica de atividades perigosas (mesmo quando a sua origem é no estrangeiro) com as probabilidades de estas causarem danos jusfundamentais de difícil mensuração e valoração, mesmo que tal implique decidir,

---

[56] CDI, "Report …" cit., n.º 23.
[57] João LOUREIRO, "Da sociedade técnica de massas à sociedade de risco – Prevenção, precaução e tecnociência: algumas questões juspublicístas", *Estudos em homenagem ao Prof. Doutor Rogério Soares,* Coimbra Editora, 2001; Ulrich BECK, *La sociedade del riesgo global,* Siglo XXI, 2006 e, do mesmo autor, *La sociedade del riesgo: Hacia una nueva modernidade,* Paidos Iberica, 2006.
[58] D. LOPES, *Eficácia* cit., p. 41.
[59] *Idem*, p. 42.
[60] *Ibidem*; A. MILLS, "Rethinking Jurisdiction …" cit., p. 187 e ss..
[61] Cedric RYNGAERT, *Universal Jurisdiction and Global Values,* eleven international publishing, 2015, p. 78 e 79.
[62] Jorge Pereira da SILVA, *Deveres do Estado de Proteção de Direitos Fundamentais,* Universidade Católica, 2015, p. 271.
[63] *Idem*, p. 222 e 272. Segundo este princípio, "o importante não está tanto em saber de onde vêm uns e outros, mas sobretudo para onde se dirigem" e, além disto, "a intencionalidade e a direção dos deveres de proteção de direitos fundamentais convergem no sentido de conceder uma garantia de amparo tão extensa quanto possível a todos os bens e liberdades que dela careçam, não sendo legítimo adotar um sistema de segregação dos diferentes perigos e riscos em função das suas origens (...) A vida humana é sempre a vida humana, independentemente da origem do perigo ou do risco que a ameaça. O seu valor – bem como as razões para a proteger – não mudam ao sabor das caraterísticas particulares das agressões de que pode ser alvo".

isolada e unilateralmente, questões de elevada complexidade sem que a entidade do foro disponha de todos os dados e num ambiente de incerteza[64].

Como observa J. PEREIRA DA SILVA, "para ameaças que transcendem as fronteiras do Estado, torna-se necessário que este promova soluções institucionais e normativas que transcendam a escala puramente nacional"[65]. Idealmente essas soluções traduzem-se em esforços ao nível da cooperação internacional, diplomáticos e institucionais, e no *treaty making power*. Acontece que esta via nem sempre é a mais adequada num quadro em que se acentua a incapacidade da estrutura, do sistema e instituições do DIP clássico para resolver problemas de âmbito global ou transnacional[66]. Face a esta constatação N. KIRSCH[67] dá nota de uma ultrapassagem do "direito dos tratados" e de uma cadência crescente de atuações unilaterais dos sujeitos internacionais, com recurso à jurisdição extraterritorial, e de manifestações informais de normas internacionais[68]. Outros autores descrevem um ambiente normativo internacional socorrendo-se do enquadramento dado pelo *pluralismo jurídico* [69].

Seja qual for a perspetiva de análise, é pacífico afirmar que as entidades do foro recorrem crescentemente a vias de proteção dos seus interesses, vias que estão ao seu alcance no plano doméstico e que potenciem o seu papel na colmatação das falhas de uma comunidade internacional incapaz de se organizar para resolver os desafios com efeitos internos ou no seu território. De facto, recordando a definição da CDI, um dos elementos enunciados é a *subsidiariedade* da extraterritorialidade em relação ao DIP, isto é, quando vigora uma lacuna regulatória naquele com implicações para a entidade do foro[70].

---

[64] *Idem*, p. 18.
[65] *Idem*, p. 22.
[66] Nico KRISCH, "The Decay of Consent: International Law in an Age of Public Goods", *AJIL,* n.º 108, 2014, p. 7. Entre nós, sobre a dificuldade operativa de certas normas de DIP (auto-determinação, boa fé, entre outras), v. Francisco FERREIRA DE ALMEIDA, *Direito Internacional Público,* Coimbra Editora, 2003*,* p. 20.
[67] N. KRISCH, "The Decay …" cit., p. 8. e, do mesmo autor, "Pluralism in International Law and Beyond", Jean D'ASPREMONT e Sahib SINGH (eds.), *Fundamental Concepts for International Law: The Construction of a Discipline,* Edward Elgar Publishing, 2016 e *Beyond Constitutionalism. The Pluralist Structure of Postnational Law,* Oxford University Press, 2011.
[68] N. KRISCH, "The Decay …" cit., p. 26.
[69] Desenvolvendo este conceito v. António Manuel HESPANHA, *Pluralismo Jurídico e Direito Democrático. Perspetivas do direito no séc. XXI,* 2016; Kaarlo TUORI, "Transnational law: on legal hybrids and legal perspectivism", Miguel P. MADURO *et alii*, *Transnational Law. Rethinking European Law and Legal Thinking,* Cambridge University Press, 2014, p. 23; Paul BERMAN, *Global Legal Pluralism,* Cambridge University Press, 2012, p. 3 e ss..
[70] V. o Capítulo 1 desta tese sobre "Definição, titulares e categorias".

O exercício de jurisdição extraterritorial poderá ainda servir como instrumento de pacificação da comunidade da entidade do foro[71] ou até quando esta apenas pretende comunicar os seus valores à comunidade internacional[72].

2.1.2. Interesses ligados à comunidade internacional

O exercício de jurisdição extraterritorial poderá também servir interesses externos à entidade do foro ou, melhor dizendo, da comunidade internacional. Sobretudo depois do caso *Shrimp/Turtle*, resolvido no seio da OMC [73], vem-se firmando a tese de que a entidade do foro pode unilateralmente adotar medidas legislativas para a prossecução e proteção de valores e de bens e interesses de natureza universal ou potencialmente universal, designadamente quando a comunidade internacional haja falhado. Entende-se que, na ausência de um poder público global ou de um centro de imputação de produção legislativa "cosmopolita", a ação unilateral[74] poderá ser virtuosa se assumir uma vocação cosmopolita[75] ou uma "orientação internacionalista"[76]. Esta foi a argumentação da UE na sua intervenção no caso *Shrimp-Turtle* para subscrever a posição dos EUA no litígio: sem embargo do relevo da cooperação internacional, defendeu que, excecionalmente, medidas aplicadas por um Estado além do seu território podem ser oportunas para proteger certos

[71] Sugerindo esta hipótese no caso do exercício de jurisdição adjudicativa, v. Luís de LIMA PINHEIRO, "A triangularidade do direito internacional privado – Ensaio sobre a articulação entre o Direito de Conflitos, o Direito da Competência Internacional e o Direito de Reconhecimento", *Estudos em Homenagem à Professora Doutora Isabel de Magalhães Collaço,* vol. I, Almedina, 2002, p. 235.

[72] Tanto no caso do exercício de jurisdição adjudicativa como prescritiva, v. Dan SVANTESSON, *Solving the Internet Jurisdiction Puzzle,* Oxford University Press, 2017, p. 134.

[73] A extraterritorialidade prescritiva dos EUA justificou-se, no caso, como a única medida de proteção das tartarugas marítimas consideradas em risco de extinção na Convenção Internacional sobre o Comércio de Espécie Ameaçadas (CITES), v. OMC, "Dispute Panel Report on United States – Import Prohibition of Certain Shrimp and Shrimp Products", proc. n.º WT/DS58/R, para. 6.1., 15 de junho de 2001, disponível em https://www.wto.org/english/tratop_e/dispu_e/cases_e/ds58_e.htm, consultado no dia 30 de setembro de 2018.

[74] Por ação unilateral ou por unilateralismo entendo a tendência para o *opt out,* num contexto multilateral, (existente ou em discussão) ou a atuação isolada de um sujeito internacional em relação a um desafio de natureza global ou regional ao invés de participar numa atuação coletiva e concertada com os seus pares. Adotando uma definição semelhante, v. David MALONE Yuen KHONG, "Unilateralism and US Foreign Policy: International Perspective", David MALONE *et alii* (eds.), *Unilateralism and US Foreign Policy: International Perspective,* Lynne Rienner, 2003, p. 3 e J. SCOTT, "Territorial Sovereignty …" cit., p. 272. Destacando as virtudes do unilateralismo, v. Daniel BODANSKY, "What's So Bad About Unilateral Action to Protect the Environment?", *EJIL,* n.º 11, 2000, p. 339.

[75] C. RYNGAERT, *Universal Jurisdiction* cit., p. 10, descrevendo o "cosmopolitanismo" como "uma noção político-filosófica segundo a qual a comunidade internacional partilha uma moralidade e, os seus membros, sejam indivíduos ou Estados, têm deveres recíprocos".

[76] Bernhard JANSEN, "The Limits of Unilateralism from a European Perspective", *EJIL,* vol. 11, n.º 2, 2000, p. 311; Jacob SCHUMAN, "Extraterritoriality and International norm internalization", *HLR,* vol. 124, 2011, p. 1280 e ss. e J. SCOTT, "Extraterritoriality and Territorial …" cit., p. 89.

valores e interesses tendencialmente universais. A decisão do órgão de resolução de litígios da OMC subscreveu a validade das medidas legislativas adotadas pelos EUA como forma de exercer pressão política sobre países terceiros (no caso India, Paquistão, Malásia e Tailândia) para implementarem medidas de proteção de recursos naturais[77].

Do mesmo modo, em face do sucesso do acordo CORSIA[78], a jurisdição extraterritorial poderá também ser parte de uma tática de geração de normas internacionais que, partindo da fragmentação normativa, de lacunas na regulação, precede a cooperação e a convergência, atuando como instrumento temporário de pressão para despertar a comunidade internacional[79]. No passado encontram-se exemplos de certos impulsos unilaterais que contribuíram para o desenvolvimento do DIP como, no caso do Direito do Mar[80], além das reações unilaterais ao ilícito, "em especial quando destinadas à realização do direito em situações em que esteja em jogo a realização de interesses e aspirações comunitários"[81].

2.1.3. Exemplos: as "leis-garra", os "perigos externos com projeção interna" e a técnica legislativa da "extensão territorial"

Um caso de estudo de extraterritorialidade prescritiva para a prossecução de um interesse *interno* da entidade do foro é o das "leis-garra". O nome deve-se ao paralelismo

---

[77] Markus GEHRING e Alexandre GENEST, "Disputes on sustainable development in the WTO regime", Marie-Claire SEGGER e Christopher WEERAMANTRY, *Sustainable Development Principles in the Decisions of International Courts and Tribunals. 1992-2012,* Routledge, 2017, p. 365 e ss.; Tracy VARGHESE, "The WTO's *Shrimp-Turtle* Decisions: the Extraterritorial Enforcement of U.S. Environmental Policy via Unilateral Trade Embargos", *TEL,* vol. 8, n.º 2, 2001/2002, p. 421 e ss..

[78] Adotado em 2016 no âmbito da OIAC. Este acordo foi antecedido pelo exercício de jurisdição extraterritorial prescritiva da UE concretizada na criação de um regime para as emissões de gases com efeitos de estufa no setor da aviação. Este regime seria aplicável a todas as aeronaves, incluindo estrangeiras, que aterrassem no território da UE, v. Alasdair YOUNG, "The European Union as a Global Regulator? Context and Comparison", *JEPP,* vol. 22, 2015, p. 1233; Daniel KELEMEN, "Globalizing European Union Environmental policy", *JEPP*, vol. 17, n.º 3, 2010, p. 342 e ss.; Vicky BIRCHFIELD, "Coercion with Kid Gloves: The European Union's Role in Shaping a Global Regulatory Framework for Aircraft Emissions", *JEPP,* vol. 22, n.º 9, 2015, p. 1276 e ss..

[79] Austen PARRISH, "Reclaiming International from Extraterritoriality", *MiLR*, vol. 93, 2009, p. 815; C. RYNGAERT, *Jurisdiction* cit., p. 207; E. FAHEY, *The Global* cit, p. 147; Jennifer ZERK, "Extraterritorial Jurisdiction: Lessons from the Business and Human Rights Sphere from Six Regulatory Areas", *Harvard Corporate Social Responsibility Initiative Working Paper No. 59,* disponível em https://www.hks.harvard.edu/m-rcbg/CSRI/publications/workingpaper_59_zerk.pdf, consultado no 30 de setembro de 2018.

[80] Donald R. ROTHWELL e Tim STEPHEN, *The International Law of the Sea,* Hart Publishing, 2016. Analisando as fontes do Direito do Mar os autores destacam o papel de dois tipos de declarações unilaterais: as declarações dos Estados que pretendem gerar práticas novas neste domínio e as declarações unilaterais que firmam uma pretensão consistente com o direito vigente.

[81] José AZEREDO LOPES, *Entre Solidão e Intervencionismo. Direito de Autodeterminação dos povos e reações de estados terceiros,* Universidade Católica, 2003, p. 597 e ss..

com uma ave predadora que sobrevoa as presas que se aventuram no seu território, em busca de alimentação, para depois as agarrar sem hipótese de fuga[82].

A sua origem deve-se a vários fatores, como o incremento do comércio internacional, o maior intervencionismo na economia traduzido na regulação de aspetos como a produção de certos bens e a prestação de determinados serviços e, em especial, a possibilidade de "fuga generalizada" (*offshore regulation evasion*) dos agentes económicos transnacionais de ordenamentos jurídicos mais garantísticos do "interesse público" para "paraísos jurídicos" onde as exigências normativas são mais suaves[83]. O fenómeno verifica-se em vários domínios que cabem na chamada "regulação" [84], como o dos meios de comunicação, da Internet, da concorrência, entre outros[85]. Por conseguinte, os destinatários das "leis-garra" são agentes económicos transnacionais, cuja sede formal ou local de atuação principal é no país *x,* mas as suas atividades produzem efeitos no país *y*[86].

Ora, procurando preservar a integridade da regulação do país *y* e proteger os consumidores e outros interesses socioeconómicos[87], as "leis-garra" configuram uma medida "defensiva" da entidade do foro, adotada tanto na Europa[88] como nos EUA[89], em

---

[82] M. Prata ROQUE, *A Dimensão* cit., p. 722.

[83] *Idem,* p. 721; J. BASEDOW, *The Law of* cit., p. 74. Citando F. Loureiro BASTOS: "a globalização económica tem-se traduzido numa deslocalização de empresas, incentivada por baixos salários e pela existência de uma legislação local irrelevante ou muito pouco exigente ao nível do enquadramento jus-laboral e jus-ambiental", v. F. Loureiro BASTOS, "Algumas notas ..." cit., p. 444.

[84] Este conceito será tratado mais adiante.

[85] Jack GOLDSMITH, "The internet and the abiding significance of territorial sovereignty", *IJGLS,* n.º 2, 1998, p. 481 e M. Prata ROQUE, *A Dimensão* cit., p. 722.

[86] B. OXMAN, "Jurisdiction ..." cit., p. 56; Brigitte STERN, "Quelques observations sur les règles internationals relatives à l'application extraterritoriale du droit", *AFDI,* 1986, p. 30 e ss.; Chris BRUMMER, "Territoriality as a regulatory technique: notes from the finantial crisis", *UCLR,* vol. 79, n.º 2, 2011, p. 504 e ss.; G. DAVIES, "International Trade …" cit., p. 1207; I. JALLES, *Extraterritorialidade* cit., p. 51 e ss. e 259 e ss.; José MAGALHÃES, "A aplicação extraterritorial de leis nacionais", *RFDUSP,* vol. 80, 1985, p. 171 e ss.; Mika HAYASHI, "Objective Territorial Principle or Effects Doctrine? Jurisdiction and Cyberspace", *Law,* n.º 6, 2006, p. 284 e ss.; Stefano BATTINI, "Extraterritoriality: an Unexceptional Exception", *Séminaire de droit administrative, européen et global – Extraterritoriality and Administrative Law,* Charie M.A.D.P./SciencesPo, 2008, p. 5 e 6.

[87] CDI, "Report …" cit., n.º 23.

[88] Exemplo disto é o art. 2.º, n.º 2, da Lei de Defesa da Concorrência, aprovada pela Lei n.º 18/2012, de 8 de maio, bem como o art. 103.º, n.º 2 da GWB (Lei da Concorrência alemã). Sobre estas normas, v. M. Prata ROQUE, *A Dimensão* cit., p. 723.

[89] Nos EUA este tipo de legislação vigora no domínio do direito da concorrência, onde se estabelecem fortes restrições a práticas concertadas fora do território norte-americano mas nele repercutidas. Mas também no domínio laboral, veja-se por exemplo a adoção, por parte de alguns Estados (como Nova Iorque e Massachusetts) das *Antisweatshop Laws* que pretendem garantir o cumprimento de *core labor standards* aos trabalhadores envolvidos na produção de produtos destinados ao território norte-americano, estipulando inclusive exigências salariais mínimas. Por fim, este tipo de regimes jurídicos intensifica-se também como instrumento de pressão política internacional sobre outros Estados, designadamente pela adoção de medidas restritivas à importação de produtos provenientes de determinados Estados com os quais os EUA mantêm conflitos internacionais ou querelas diplomáticas. Cfr. M. Prata ROQUE, *A Dimensão* cit., p. 723.

vários domínios desde a concorrência ao direito laboral[90]. Estas soluções visam evitar que os agentes económicos transnacionais se subtraiam ao respeito pelos valores fundamentais de um determinado ordenamento jurídico, camuflando a sua atividade num "paraíso jurídico", em detrimento dos demais membros de uma comunidade que eventualmente serão afetados pelos efeitos da respetiva atividade[91].

Pode-se falar de uma manifestação de jurisdição extraterritorial prescritiva porquanto as "leis-garra" visam regular a conduta de pessoas formalmente estabelecidas além-fronteiras, com base no critério do "local da produção de efeitos" da atividade dessas pessoas no território da entidade do foro[92].

Outro exemplo da tutela de um interesse interno, oriundo do domínio dos direitos fundamentais, é a já aflorada reação da entidade do foro a "riscos externos com projeção interna" que, por seu turno, cabem dentro da categoria dos "riscos com conexões internacionais". Ocorrem, em geral, quando aquela é confrontada com uma ameaça a direitos fundamentais de indivíduos localizados no interior do seu território, mas a fonte da ameaça, o sujeito que a provoca, encontra-se fora dali[93]. Tipicamente, verificam-se em domínios tecnológicos específicos, como a pirataria informática transnacional, a vigilância eletrónica das comunicações e a Internet em geral[94].

Neste último caso multiplicam-se as afirmações de que a jurisdição meramente territorial é obsoleta na "era digital" equacionando-se um novo paradigma de jurisdição que põe de parte a "tirania da territorialidade"[95]. Este paradigma assenta em várias premissas, das quais destaco as seguintes:

(i) A soberania deve ser colocada ao serviço dos valores da democracia, do Estado de direito e dos direitos fundamentais e deve ser exercida de modo a evitar a consumação ou a mitigar as atividades que estrangeiros possam desenvolver no respetivo país de origem, mas cujos *efeitos* se façam sentir no território da entidade do foro;

[90] J. BASEDOW, *The Law,* cit., p. 75.
[91] *Idem*, p. 728, nota de rodapé 2063.
[92] M. Prata ROQUE, *A Dimensão* cit., p. 722. Mais adiante neste trabalho explico o princípio de jurisdiçao subjacente a este critério.
[93] J. Pereira da SILVA, *Deveres* cit., p. 286.
[94] *Ibidem*.
[95] D. SVANTESSON, *Solving the Internet* cit., p. 13 e ss..

(ii) O princípio da territorialidade, rigorosamente interpretado, não tem sido usado (nem é suficiente) para distribuir a jurisdição das entidades do foro em relação a atividades em linha, valendo aí o critério do "local de produção de efeitos", também designado de doutrina dos efeitos, e o princípio da nacionalidade;

(iii) O meio de transmissão do dano para a entidade do foro – a Internet – não deve ser determinante para travar um impulso protetor daquela;

(iv) A dificuldade ou mesmo impossibilidade de alcançar um consenso sob a forma de um Tratado Global, sendo uma necessidade reconhecida pela doutrina, não pode ser o fim das respostas da entidade do foro aos desafios colocados pela Internet[96].

Assim se compreendem opções legislativas como o Marco Civil, no Brasil[97], e decisões paradigmáticas como o caso que opôs a *Ligue contre le racism et l'antisémitisme et Union des étudiants juifs de France* à *Yahoo! Et Societé Yahoo! France (LICRE c. Yahoo),* decidido pelo Tribunal de Grande Instância de Paris ("TGIP"), em Maio e Novembro de 2000. Esta é a decisão mais discutida sobre a jurisdição extraterritorial adjudicativa em relação a atividades da Internet, além dos recentes casos envolvendo a *Google,* tanto a decisão do Supremo Tribunal do Canadá[98] como o caso *Google Spain,* decidido pelo TJ e tratado na Parte II[99].

---

[96] Brendan ALSENOY e Marieke KOEKKOEK, "Internet and Jurisdiction After Google Spain: The Extra-territorial Reach of the EU's 'Right to be Forgotten'", *IDPL,* n.º 5, 2015, p. 105 e ss.; Christopher KUNER *et alii*, "The (Data Privacy) Law hasn't Even Checked in when technology takes off", *IDPL,* n.º 4, 2014, p. 175 e ss.; C. REED, *Making Laws* cit., p. 29 e ss.; D. SVANTESSON, *Solving the Internet* cit., p. 29 e ss.; J. ZEKOLL, "Jurisdiction in…" cit., p. 346; J. GOLDSMITH, "The Internet and a…" cit., p. 479; O. POLLICINO e M. BASSINI, "The law …" cit., p. 361; P. De HERT e M. CZERNIAWSKI, "Expanding …" cit., p. 234; Uta KOHL, *Jurisdiction and the Internet – Regulatory Competence of Online Activity,* Cambridge University Press, 2007, p. 89.

[97] Veja-se a discussão no Brasil sobre o art. 11.º da Lei n.º 12965 de 23 de abril de 2014 em Francis MEDEIROS e Lee BYGRAVE, "Brazil's Marco Civil Da Internet: Does It Live up to the Hype?", *CLSR,* n.º 31, 2015, p. 127 e ss. e, ainda a propósito do mesmo, v. Nicolo ZINGALES, "Extraterritorial reach of the Marco Civil. A guide to the interpretation of article 11's key criteria", 30 de abril de 2015, disponível em http://pensando.mj.gov.br/marcocivil/pauta/extraterritorial-reach-of-the-marco-civil-a-guide-to-the-interpretation-of-article-11s-key-criteria/, consultado no dia 30 de setembro de 2018.

[98] Analisando esta decisão, v. D. SVANTESSON, *Solving the Internet* cit., p. 181 e ss..

[99] Sobre o caso *Yahoo*, entre outros, v. Alberto MIGLIO, "Back to Yahoo!? Regulatory clashes in cyberspace in the light of EU data protection law", Gert VERMEULEN & Eva LIEVENS (eds.), *Transatlantic tensions* cit., p. 101 e ss.; Catarina SANTOS BOTELHO, "Novo ou velho direito? – O Direito ao esquecimento e o princípio da proporcionalidade no constitucionalismo global", *AB Instantia,* vol. V, n.º 7, 2017, p. 49 e ss.; Jack GOLDSMITH e Tim WU, *Who Controls the Internet? Illusions of a Borderless World,* Oxford University

Por último, servindo interesses internos e externos, veja-se o exemplo da técnica da "extensão territorial" usada, maioritariamente, pela UE. Em áreas de regulação que operam num contexto de grande interdependência internacional, que incidem sobre operadores económicos transnacionais e nas quais a cooperação internacional é frágil e morosa (alterações climáticas[100], ambiente[101], proteção animal[102], transporte marítimo[103], transporte aéreo[104] e regulação financeira[105]), a doutrina salienta o uso recorrente de uma técnica legislativa caraterizada por três elementos centrais[106]:

(i) Parte de um nexo ou gancho territorial com a UE que pode resultar de vários fatores, como a introdução de um produto ou a prestação de serviços por um operador ou prestador estrangeiro no mercado interno, a sua presença temporária no território da UE, entre outros fatores;

(ii) A imposição de condições a esse acesso, ao mercado interno ou ao território da União, que passam pela apreciação da conformidade e respeito do DUE, quanto às operações e à atividade desenvolvidas no mercado interno da UE, mas também quanto à sua *performance* no estrangeiro;

Press, 2006; Paul Schiff BERMAN, "The Globalization of Jurisdiction", *PLR,* n.º 151, 2002, p. 311 e ss.; Thomas SCHULTZ, "Carving up the Internet: Jurisdiction, Legal Orders, and the Private/Public International Law Interface", *TEJIL,* vol. 19, n.º 4, 2008, p. 799 e ss..

[100] Diretiva 2008/101, de 19 de novembro de 2008, que altera a Diretiva 2003/87/CE de modo a incluir as atividades da aviação no regime de comércio de licenças de emissão de gases com efeito de estufa na Comunidade.

[101] Regulamento 995/2010 do Parlamento Europeu e do Conselho, de 20 de outubro de 2010, que fixa as obrigações dos operadores que colocam no mercado madeira e produtos de madeira.

[102] Regulamento 1007/2009 do PE e do Conselho, de 16 de setembro de 2009, relativo ao comércio de produtos derivados da foca.

[103] Diretiva 2008/106 do PE e do Conselho, de 19 de novembro de 2008, relativa ao nível mínimo de formação dos marítimo e Regulamento 391/2009 do PE e do Conselho, de 23 de abril de 2009, relativo às regras comuns para as organizações de vistoria e inspeção de navios.

[104] Regulamento de Execução 859/2011 da Comissão Europeia, de 25 de agosto de 2011, que altera o Regulamento 185/2010 que estabelece as medidas de execução das normas de base comuns sobre a segurança da aviação, no respeitante à carga e ao correio aéreos, entretanto substituído pelo Regulamento de Execução 2015/1998 da Comissão Europeia, de 5 de novembro de 2015, que estabelece as medidas de execução das normas de bas comuns sobre a segurança da aviação.

[105] Regulamento 1060/2009 do PE e do Conselho, de 16 de setembro de 2009, relativo às agências de notação de risco, e Diretiva 2011/61/EU, do Parlamento e do Conselho, de 8 de junho de 2011, relativa aos gestores de fundos de investimento alternativos e que altera as Diretivas 2003/41/CE e o Regulamento 1095/2010.

[106] C. RYNGAERT, "Whither Territoriality? …" cit., p. 434 e, do mesmo autor, *Jurisdiction* cit., p. 94 e "Core values beyond territories and borders: the internal and external dimension of EU regulation and enforcement", Ton BRINK *et alii* (eds.), *Sharing sovereignty in the European legal order?* Intersentia, 2015, p. 13; J. SCOTT, "Extraterritoriality and Territorial …" cit., p. 96 e 105.

(iii) A criação de "esferas concêntricas de intervenção regulatória" incidentes sobre vários níveis, três *externos*, micro (atividades económicas transnacionais), intermédio (o conteúdo do direito estrangeiro) e macro (a evolução do DIP) e um nível *interno*.

Daqui resulta que operadores económicos estrangeiros como negociantes de madeira, gestores de fundos de investimento, agências de notação de risco, inspetores de navios, organizações que realizam inquéritos, companhias aéreas, entre outros, apenas possam prestar serviços, comercializar bens e desenvolver as respetivas atividades no mercado interno da UE se a formação que receberam, os métodos que utilizam e a supervisão a que se sujeitam, tal como decorrem do direito vigente no país de origem, forem "equivalentes" ou "adequados" face às exigências do DUE[107].

Comparando com formas de unilateralismo tradicionais ou absolutas, associadas aos EUA[108], a utilização desta técnica pela UE posiciona-a como uma unilateralista relutante ou prudente, na medida em que a aplicação do DUE fora de portas não é cega ou absoluta[109]. Tal deve-se à utilização, em várias áreas de direito derivado da União, de "cláusulas de equivalência" ou de "adequação" em relação ao direito estrangeiro, com especial destaque para o setor financeiro e bancário[110].

[107] *Idem*, p. 96 e ss..

[108] Austen PARRISH, "Reclaiming International from Extraterritoriality", *MiLR*, vol. 93, 2009, p. 815; J. SCOTT, "Extraterritoriality and Territorial …" cit., p. 118 e John RUGGIE, "Doctrinal Unilateralism and its Limits: American and Global Governance in the New Century", David P. FORSYTHE *et alii* (eds.), *American Foreign Policy in a Globalized World,* 2006, p. 8 e ss..

[109] C. RYNGAERT, "Whither Territoriality? ..." cit., p. 448 e, do mesmo autor, *Jurisdiction* cit., p. 95; J. SCOTT, "Extraterritoriality and Territorial …" cit., p. 273 e, da mesma autora, "Territorial Sovereignty and Territorial Extension in an Inter-Connected World", Richard RAWLINGS *et alii* (eds), *Sovereignty and the Law. Domestic, European and International Perspectives,* Oxford University Press, 2013, p. 272.

[110] Como a cláusula de equivalência para as Agências de Notação de Risco estabelecidas em países terceiros e sem presença nem ligações à UE que são certificadas "após a Comissão ter apurado a equivalência do enquadramento legal e de supervisão de um país terceiro" aos requisitos do DUE (art. 4.º do Regulamento 1060/2009/UE do PE e do Conselho, de 16 de setembro de 2009 relativo às agências de notação de risco) ou a cláusula de equivalência prevista em relação a gestores de fundos de investimento alternativos (FIA's) "extra-UE" que pretendem gerir FIA's da UE ou comercializar FIA's na UE (art. 37.º da Diretiva 2011/61/UE do PE e do Conselho, de 8 de junho de 2011). Analisando esta tendência, v. Lucia QUAGLIA, "The politics of 'Third Country Equivalence' in Post-crisis Financial Services Regulation in the European Union", *WEP,* vol. 38, n.º 1, 2015, p. 167 e ss..

Segundo a COM[111] e o PE[112], os *objetivos* destas cláusulas são os seguintes:

(i) Encontrar o equilíbrio entre a estabilidade financeira, a proteção dos investidores e os benefícios em manter os mercados financeiros da UE globalmente abertos;

(ii) Promover a convergência regulatória e melhorar a cooperação da supervisão com outros parceiros.

Por seu turno, as *vantagens* enunciadas são várias:

(i) Reduzir ou eliminar as sobreposições regulatórias e facilitar a fiscalização;

(ii) Permitir a aplicação de um regime prudencial menos oneroso em relação a instituições da UE expostas a uma instituição equivalente de outro país;

(iii) Permitir o acesso a um conjunto amplo de serviços, produtos e opções de investimento, oriundos de outros países, mas que respeitam o DUE.

É a introdução destas cláusulas que transforma esta técnica legislativa em algo *mais* do que o simples exercício de jurisdição extraterritorial porquanto as mesmas potenciam a incidência regulatória da UE em várias das esferas ou níveis de intervenção já referenciados: três *externos* (micro, intermédio e macro) e um *interno*.

No plano externo, o nível micro incide sobre as práticas, a arquitetura de *governance* e as atividades de operadores económicos estrangeiros que pretendem atuar no mercado interno da UE. Com frequência, efetuada uma ponderação de custos e benefícios, estes operadores não abdicam daquele mercado e optam pelo padrão regulatório da UE para a

[111] Comissão Europeia, "Commission Staff Working Document. Equivalence decisions in financial services policy: an assessment", 27 de fevereiro de 2017, disponível em https://ec.europa.eu/info/sites/info/files/eu-equivalence-decisions-assessment-27022017_en.pdf, consultado no dia 30 de setembro de 2018.
[112] PE, "Briefing: Third-country equivalence in EU banking legislation", 12 de julho de 2017, disponível em http://www.europarl.europa.eu/RegData/etudes/BRIE/2016/587369/IPOL_BRI(2016)587369_EN.pdf, consultado no dia 30 de setembro de 2018.

sua atividade global[113]. Nesse sentido, não se pode dizer que sejam *forçados* a respeitar o DUE sendo apenas económica e indiretamente *incentivados* a fazê-lo[114].

A intervenção da UE faz-se sentir também a um nível intermédio. Na prática, as cláusulas de equivalência condicionam o acesso ao mercado interno para agentes económicos em cujos países de origem não vigoram regras equivalentes ou adequadas[115]. Ao sujeitar o acesso desses operadores económicos à verificação de uma equivalência, o legislador da UE promove uma assimetria negocial colocando aqueles operadores em desvantagem concorrencial no mercado europeu por força da legislação do seu país de origem[116]. Como sintetizam A. NEWMAN e R. POSNER, "as normas de equivalência incentivam empresas internacionalmente ativas a pressionar reformas regulatórias nos países de origem"[117]. Assim, a UE poderá instigar alterações no ordenamento jurídico de países terceiros, atuando como "catalisador de normas", já que a necessidade de cumprir o DUE tem o potencial de induzir pressão nos países terceiros no sentido de aproximar a legislação interna com a da UE [118].

Mas também ao nível macro ou global se faz sentir a extensão territorial do DUE, espoletando a realização de acordos bilaterais e multilaterais e influenciando o trajeto da normatividade internacional. O caso mais evidente é o acordo CORSIA, exemplificando a forma como o unilateralismo da UE pode criar um incentivo ou, pelo menos, acelerar a ação multilateral[119]. A doutrina sugere que a mesma estratégia de pressão da comunidade internacional foi acionada no que diz respeito ao transporte marítimo, no Regulamento 2015/757, de 29 de abril de 2015, relativo à monitorização, comunicação e verificação das emissões de dióxido de carbono provenientes do transporte marítimo e que altera a

---

[113] Volto a este ponto adiante. Cfr. C. RYNGAERT, "Whither Territoriality? …" cit., p. 437 e "Core values beyond …" cit., p. 14.

[114] Em sentido próximo, v. Laurens ANKERSMIT, Jessis LAWRENCE, e Garreth DAVIES, "Diverging EU and WTO Perspectives on Extraterritorial Process Regulation", *MJIL,* n.º 21, 2012, p. 25; Natalie DOBSON e Cedric RYNGAERT, "EU 'Extraterritorial' Regulation of Maritime Emissions", *ICLQ,* 2016, p. 295 e ss..

[115] Abraham NEWMAN e Elliot POSNER, "Putting the EU in its place: policy strategies and the global regulatory context", *JEPP*, vol. 22, n.º 9, 2015, p. 1316 e ss..

[116] Alasdair YOUNG, "Political Transfer and 'Trading up'? Transatlantic Trade in Genetically Modified Food and US Politics", *WP,* n.º 55, Julho, 2003, p. 457 e ss. e A. NEWMAN e E. POSNER, "Putting the EU …" cit., p. 1316 e ss..

[117] *Ibidem*.

[118] Fabian AMTENBRINK, "What Role for the European Union in Shaping Global Financial Governance", *The EU's Role in* cit., p. 256 e J. SCOTT, "Extraterritoriality and Territorial …" cit., p. 108.

[119] A medida legislativa da União que o antecedeu será tratada no ponto 2.3.1 deste capítulo quando enumerar as reações à mesma, v. Alasdair YOUNG, "The European Union as a Global Regulator? Context and Comparison", *JEPP,* vol. 22, 2015, p. 1233; Daniel KELEMEN, "Globalizing European Union Environmental policy, *JEPP*, vol. 17, n.º 3, 2010, p. 342 e ss.; Vicky BIRCHFIELD, "Coercion with Kid Gloves: The European Union's Role in Shaping a Global Regulatory Framework for Aircraft Emissions", *JEPP,* vol. 22, n.º 9, 2015, p. 1276 e ss..

Diretiva 2009/16/CE[120]. Através da assunção de jurisdição a UE estará a executar *standards internacionais*[121] que vinculam os seus Estados-Membros (como, por exemplo, o Protocolo de Quioto), pelo que a sua ação unilateral atua como um mecanismo para desenvolver ou dar eficácia ao DIP, caraterizado por uma estrutura "primitiva" e descentralizada, em que inexistem, ou mesmo escasseiam, órgãos superiores aos Estados, capazes de assegurar o controlo dos seus comportamentos.

De facto, o objeto da maioria dos exemplos de direito derivado que adotaram esta técnica incide sobre um problema previamente sinalizado ou discutido no âmbito internacional, seja em convenções – como no caso da madeira[122] ou do transporte marítimo[123] – ou em organizações internacionais – como no caso do bem-estar animal[124], da segurança do transporte aéreo[125], das agências de notação de risco[126] e da gestão de FIA[127]. Nestes domínios a UE como que atua numa posição de *subsidiariedade* da comunidade internacional dado o tradicional processo voluntário de formação da maior parte de normas jurídico-internacionais, algo que faz do DIP particularmente omisso em face da velocidade dos tempos atuais e dos desafios que colocam[128]. Este posicionamento da União está de acordo com um princípio que rege a sua atuação externa e que traduz um objetivo de longa data dos seus órgãos de incrementar a visibilidade e a eficácia da sua atuação internacional no sentido de fazer da UE uma "potência capaz de marcar

[120] E. FAHEY, *The Global* cit, p. 49.
[121] A expressão é de J. SCOTT, "Extraterritoriality and Territorial …" cit., p. 112, para descrever, genericamente, a utilização de padrões prescritos em acordos internacionais bem como em diplomas não vinculativos adotados por organizações inter-governamentais.
[122] O Regulamento 995/2010, no considerando 10, expressamente refere a Convenção sobre o Comércio Internacional das Espécies da Fauna e Flora Selvagens Ameaçadas de Extinção.
[123] A Diretiva 2008/106, no considerando 7, para determinar o nível mínimo de formação na UE toma por referência "normas de formação já acordadas a nível internacional" como a Convenção da Organização Marítima Internacional, de 1978, sobre Normas de Formação, de Certificação e de Serviço de Quartos para os Marítimos, revista em 1995.
[124] Na Estratégia da União para a proteção e o bem-estar dos animais 2012-1015, os critérios da Organização Mundial da Saúde Animal (OIE) e da Organização para a Alimentação e a Agricultura (FAO) serviram de ponto de partida sendo que ambas as organizações tomaram iniciativas em matéria de bem-estar dos animais e, em especial, a OIE adotou normas internacionais neste domínio, disponíveis em www.oie.int, consultado no dia 30 de setembro de 2018.
[125] O Regulamento 859/2011, no considerando 6, alude também à OMI.
[126] No Regulamento 1060/2009, sobre as agências de notação de risco, o considerando 8 remete para as conclusões alcançadas no âmbito da Organização Internacional das Comissões de Valores Imobiliários e nos códigos de conduta por esta produzidos.
[127] O considerando 89 da Diretiva 2011/61, relativa aos gestores de fundos de investimento, remete para as conclusões dos dirigentes do G20, de abril de 2009, e para os princípios definidos pela Organização Internacional de Comissões de Valores Imobiliários, de junho de 2009, de forma a orientar o desenvolvimento de uma regulamentação internacional coerente neste domínio.
[128] C. RYNGAERT, "Whither Territoriality? …" cit., p. 448. Em sentido próximo, Thomas BERNAUER, Robert GAMPFER e Aya KACHI, "European unilateralism and involuntary burden-sharing in global climate politics: A public opinion perspective from the other side", *EUP,* vol. 15, n.º 1, 2014, p. 132 e ss..

eticamente a globalização": o princípio da *responsabilidade*[129]. Trata-se de um princípio enunciado na Declaração de Laeken, em 2001, e acolhido pelo TL por via do elenco de objetivos da UE em matéria de atuação externa no art. 3.º, n.º 5 e no art. 21.º do TUE[130].

Por fim, no plano interno, a extensão territorial serve para proteger o funcionamento do mercado da União, garantir a sua estabilidade e integridade e condicionar o acesso de operadores económicos estrangeiros. Condicionando esse acesso, a UE protege interesses próprios (de consumidores, investidores, cidadãos e indivíduos em geral) sempre que os serviços e produtos estrangeiros comportem riscos para o valor ou interesse que mobilizou o legislador a conformar a atividade privada no seu espaço económico[131]. A criação de um mercado interno, dando origem a uma forma de *territorialidade interna*, e a efetividade da regulação aplicável a esse mercado, exigem a *externalização* do DUE sempre que o objetivo ou a integridade daquele possa ser contornado por agentes económicos transnacionais que ali atuem. Estes agentes podem, por exemplo, "expulsar" operadores situados no mercado interno ou compeli-los a uma relocalização para "paraísos jurídicos", assim dificultando a tutela de certos interesses da UE[132]. Neste nível interno, a explicação para a técnica legislativa da "extensão territorial" situa-se na bissetriz entre a garantia do comércio internacional, da livre concorrência e de acesso a utilidades económicas e a sujeição da atuação privada de âmbito transnacional a vinculações jurídico-públicas que garantam a preservação e a promoção de traços essenciais do ordenamento jurídico da União.

2.2. Os limites no direito internacional público

A jurisdição da entidade do foro é, como referi, ampla e fluída, no sentido em que não toma por referência apenas o território. Na verdade, "o poder de dizer o direito" ou de

[129] Maria J. RANGEL DE MESQUITA, *A Actuação Externa da União Europeia depois do Tratado de Lisboa,* Almedina, 2011, p. 184.
[130] Onde se pode ler, respetivamente, "Nas suas relações com o mundo, a União afirma e promove os seus valores e interesses e contribui para a proteção dos seus cidadãos. Contribui para a paz, a segurança, o desenvolvimento sustentável do planeta, a solidariedade e o respeito mútuo entre os povos, o comércio livre e equitativo, a erradicação da pobreza e a proteção dos direitos do Homem (...) bem como para a rigorosa observância e o desenvolvimento do direito internacional, incluindo o respeito dos princípios da Carta das Nações Unidas" e, *inter alia,* "A ação da União na cena internacional assenta nos princípios que presidiram à sua criação, desenvolvimento e alargamento, e que é seu objetivo promover em todo o mundo: democracia, Estado de direito, universalidade e indivisibilidade dos direitos do Homem e das liberdades fundamentais, respeito pela dignidade humana, princípios da igualdade e solidariedade e respeito pelos princípio da Carta das Nações Unidas e do direito internacional. (...)".
[131] G. DAVIES, "International Trade …" cit., p. 1208.
[132] C. RYNGAERT, "Core values …" cit., p. 13.

"resolver problemas" nunca se delimitou pelo "princípio da territorialidade", uma criação humana contingente que é apenas o "ponto de partida" das tarefas da entidade do foro[133]. O alargamento da jurisdição para fora de portas, secundado em geral pela doutrina[134], é ancorado na jurisprudência internacional, designadamente no caso *Lotus,* decidido pelo Tribunal Permanente de Justiça Internacional, que opôs a Turquia à França em 1927. Aqui se proclamou que, salvo proibições expressamente previstas em regras de DIP, cada Estado tem liberdade para exercer jurisdição nos termos que considerar mais adequados[135].

De resto, a ultrapassagem da territorialidade foi suscitada noutras decisões. Numa opinião conjunta no caso do Mandado de Detenção contra o Ministro dos Negócios Estrangeiros do Congo, decidido pelo TIJ, em 2002, os juízes HIGGINS, KOOIJMAN e BUERGENTHAL, apontaram "[u]m movimento gradual para princípios de jurisdição diferentes do território" e uma "mudança lenta mas firme para uma aplicação extensiva da jurisdição extraterritorial dos Estados"[136].

Além da jurisprudência internacional, outra evidência da fluidez da jurisdição é o chamado "direito transnacional". L. LIMA PINHEIRO refere que a regulamentação de situações internacionais tem sido *desestatiza,* podendo ser prosseguida pelo direito transnacional que é formado *sem qualquer ação dos órgãos do Estado*[137]. Do mesmo modo, a incidência do "direito transnacional" no direito público tem sido apontada pela doutrina. Por exemplo, a aplicação do conceito de "transnacionalidade" ao direito administrativo visa sinalizar, essencialmente, (i) a ultrapassagem da base territorial e

---

[133] D. LOPES, *Eficácia* cit., p. 34.; J. SAMPAIO, *O Acto* cit., p. 22; M. Prata ROQUE, *A Dimensão* cit., p. 208.
[134] A. COLANGELO, "Constitutional Limits ..." cit., p. 126 e, do mesmo autor, "What is Extraterritorial Jurisdiction?", *CLR*, vol. 99, 2014, p. 1303 e ss.; Derek BOWETT, "Jurisdiction: Changing Patterns of Authority over Activities and Resources", *BYIL*, vol. 53, 1982, p. 1 e ss.; D. LOPES, *Eficácia* cit., p. 41; F. RIGAUX, "Refléxions sur ..." cit., p. 569 e ss.; H. BUXBAUM, "Territory, territoriality ..." cit., p. 631 e ss.; I. JALLES, *Extraterritorialidade* cit., p. 33 e ss.; Malcolm SHAW, *International Law,* Cambridge University Press, 6ª edição, 2008, p. 645; M. Prata ROQUE, *A Dimensão* cit., p. 204 e ss.; M. AKEHURST, "Jurisdiction in …" cit., p. 145; M. MILANOVIC, *Extraterritorial Application ...* cit., p. 23; V. LOWE, "Jurisdiction …" cit., p. 335.
[135] Para uma análise compreensiva desta decisão, v. P. CAEIRO, *Da Jurisdição Penal do* cit., p. 300. Em extrema síntese, o autor conclui que o tribunal parte do princípio da liberdade de o Estado determinar os limites da respetiva jurisdição, cujas limitações "não se presumem" e que apenas decorrem do DIP "como bloco de controlo da validade das regras de aplicabilidade da lei (...) estatal (...)".
[136] Acórdão do TIJ, República Democrática do Congo c. Bélgica*,* Joint Separet Opinion of Judges Higgins, Kooijmans and Buergenthal, 14 de fevereiro de 2002, n.º 73 a 75.
[137] Luís LIMA PINHEIRO, "The 'Denationalization' of Transnational Relationships: Regulation of Transnational Relationships by Public International Law, European Community Law, and Transnational Law", *Estudos de Direito Internacional Privado – Direito de Conflitos, Competência Internacional e Reconhecimento de Decisões Estrangeiras,* Almedina, 2006, p. 189 e ss.. Sobre o "direito transnacional", v. K. TUORI, "Transnational law ..." cit., p. 19, sublinhando um acervo de normas que escapa ao controlo do Estado no momento da sua formação e aplicação.

populacional dos Estados isoladamente considerados; (ii) a aplicação das suas normas tanto a sujeitos privados como a Estados; e (iii) a abrangência de matérias com repercussão regional ou global, para além do interesse exclusivo de determinado Estado[138].

O alargamento funcional e pessoal da jurisdição é acompanhado por uma transição na noção de soberania. Em especial, sublinha-se a sua abertura a um conceito que não equivale a uma autoridade única e unívoca, responsável exclusiva pela criação e concretização do direito, e a novas formas de atuação e organização internacional que simbolizam "fenómenos de partilha de competência e de cooperação internacional"[139]. Este processo é visível em várias teorizações sobre aquela noção: "soberania de serviço"[140], "tardia"[141], "cosmopolita"[142] ou "partilhada"[143], entre outros[144]. Estas noções ajudam a explicar o recurso crescente à jurisdição extraterritorial, a concorrência de jurisdições, as novas formas de gerar e concretizar o direito, e acentuam uma conceção funcional de soberania, "de forma a explicar a sua partilha e expansão de 'poderes soberanos' a outros sujeitos internacionais"[145].

Não se sugere com isto uma substituição do Estado: este não deve deixar de atuar de forma responsável e como último garante dos princípios fundamentais por si eleitos ou a que se vinculou internacionalmente. As intervenções estaduais deverão ser "válvulas de escape de um sistema multidimensional", assegurando a paz, a dignidade da pessoa humana, o bem-estar económico e a segurança humana[146]. Neste contexto, a

---

[138] J. SAMPAIO, *O Acto* cit., p. 38 e 39 e nota de rodapé 107. Em sentido próximo, M. Prata ROQUE, *A Dimensão* cit., p. 861 e ss..

[139] D. LOPES, *Eficácia* cit., p. 103 e J. GOLDSMITH, "The Internet and …" cit., p. 475 e ss..

[140] Adriano MOREIRA, "Território, Fronteira e Soberania no Mundo Atual", *Estudos em Homenagem ao Prof. Doutor Martim de Albuquerque,* vol. I, Coimbra Editora, 2010, p. 29.

[141] Neil WALKER, "Late Sovereignty in the European Union", Neil WALKER (ed.), *Sovereignty in Transition,* Hart Publishing, 2003, p. 3 e ss..

[142] David HELD, "Law of States, Law of Peoples: Three Models of Sovereignty", *Legal Theory,* vol. 8, n.º 2, 2002, p. 1 e ss.. Particularmente importante a este propósito é a teorização desenvolvida por C. RYNGAERT em torno de uma jurisdição cosmopolita, do Estado e da UE, que legitima o unilateralismo (ou a jurisdição extraterritorial) preordenados e ao serviço da sociedade cosmopolita e do fornecimento de "bens públicos globais", v. C. RYNGAERT, *Unilateral Jurisdiction* cit., p. 10 e ss..

[143] J. MACHADO, *Direito Internacional* cit., p. 227; Oreste POLLICINO e Marco BASSINI, "The law of the Internet between Globalisation and localization", Miguel Poiares MADURO *et alii* (eds.), *Transnational Law: Rethinking European Law and Legal Thinking,* Cambridge University Press, 2014, p. 359.

[144] Para esse mapeamento, v. D. LOPES, *Eficácia* cit., p.103.

[145] *Idem*, p. 101.

[146] Na descrição de F. LUCAS PIRES o Estado atuará como uma "rede de segurança, lar no meio de uma casa comum" ou "valor refúgio", v. *Introdução à Ciência Política,* Universidade Católica Portuguesa, 1998, p. 77. Em sentido próximo v. John COHAN, "Sovereignty in a Postsovereign World", *FJIL,* n.º 18, 2006, p. 907 e ss. e Wladimir BRITO, *Responsabilidade de Proteger no Direito Internacional,* Almedina, 2016, p. 13.

extraterritorialidade funcionará como uma ferramenta útil na prossecução daquela tarefa. Resta saber em que termos pode ser usada e, sobretudo, se o DIP lhe impõe limites.

A doutrina é consensual na conclusão de que o DIP não contém em si um sistema específico de regras sobre a jurisdição da entidade do foro[147]. Não obstante, há princípios, diretrizes e soluções particulares que condicionam a conformação do âmbito daquela, por exemplo em matéria de imunidades de jurisdição em relação aos Estados estrangeiros, às organizações internacionais e aos agentes diplomáticos e consulares[148]. Entre aqueles princípios, o princípio da não ingerência nos assuntos internos e a *comity* são apontados pela CDI como limites ao exercício de jurisdição extraterritorial, tal como os chamados princípios da jurisdição extraterritorial ou a exigência de uma ligação da relação controvertida com a entidade do foro[149].

2.2.1. O princípio da não ingerência nos assuntos internos e a *comity*

Em relação ao primeiro, reconhece um domínio reservado dos Estados ou "uma área de autoridade interna que está fora do alcance do direito internacional"[150]. Tal como a CDI[151] e a doutrina[152] não tenho dúvidas quanto à sua utilidade em casos de exercício de jurisdição de *execução* quando a entidade do foro pratica um ato de coerção material no território da entidade *ad quem* sem o seu consentimento. Contudo, recordando as outras categorias de jurisdição extraterritorial, será possível falar-se de uma ingerência nos assuntos internos alheios?

Rigorosamente falando, os comandos dirigidos à "conduta de pessoas, bens ou atos" em território alheio pode constituir uma ingerência, na medida em que a entidade *ad quem* tem uma pretensão legítima de proteção do exercício de direitos no espaço sob sua jurisdição, livre de coação por parte de terceiros. Por outro lado, o entendimento quanto ao conceito de "ingerência" parece ser tão amplo como o que foi dado por WINFIELD:

---

[147] L. LIMA PINHEIRO, *Direito Internacional,* cit., p. 22.
[148] *Ibidem.*
[149] CDI, "Report …" cit., n.º 8 e n.º 45 e L. LIMA PINHEIRO, *Direito Internacional,* cit., p. 22 e 23.
[150] Anthony D'AMATO, "Domestic Jurisdiction", *Encyclopedia of Public International Law,* vol. I, 1992, p. 1090.
[151] CDI, "Report …" cit., n.º 5.
[152] Ian BROWNLIE, *Principles of International Law,* Clarendon Press, 4ª ed., 1990, p. 309, apontando para a necessidade do consentimento da entidade do foro e M. Prata ROQUE, *A Dimensão* cit., p. 1133.

"ingerência pode ser qualquer coisa: desde a partição da Polónia a um discurso de LORD PALMERSTON na Câmara dos Lordes"[153].

Porém, este princípio, pela sua própria natureza, não pode ser absoluto no atual contexto de imbricação das situações da vida e de globalização das mesmas. Nesse sentido, veja-se a sugestão de M. PRATA ROQUE, propondo a sua reinterpretação: não haverá uma intromissão nos "assuntos internos alheios" quando "uma situação da vida extravasa as fronteiras de um só Estado", e quando o que se pretende é "participar na solução de um problema mais vasto, de âmbito transnacional" [154]. Em sentido semelhante, H. LAUTERPACHT refere que o princípio da não ingerência não poderá ser invocado "relativamente a matérias que são essencialmente internacionais" à luz "das suas inevitáveis repercussões"[155].

Acresce que, sendo este um entre vários princípios estruturantes do DIP e dada a sua natureza relativa, tem de ser conciliado com outras referências comunitárias e outros princípios, como a proteção dos direitos fundamentais, pelo que pode ser alvo de uma compressão com vista à prossecução de deveres de salvaguarda dos mesmos[156]. E bem se compreende que assim seja atendendo à crescente valorização do indivíduo no DIP[157]. Por exemplo, no que respeita à proteção dos direitos dos estrangeiros, aliada à "proteção internacional dos direitos fundamentais independentemente de se tratar de nacionais ou estrangeiros", há quem defenda que a assunção de jurisdição não pode conduzir à denegação de justiça aos estrangeiros[158]. Essencial, como demonstrarei, é que a pretensão de jurisdição extraterritorial seja devidamente justificada ou fundamentada num princípio de jurisdição[159]. Se assim for, o argumento da ingerência não pode ser usado, *in abstracto,* para negar por si só a juridicidade da pretensão da entidade do foro[160].

Quanto à *comity*, também designada regra da cortesia ou moderação, significa que os Estados, o legislador, os tribunais e a administração pública, empreendam um esforço de

---

[153] Maria de Assunção do VALE PEREIRA, *A Intervenção Humanitária no Direito Internacional Contemporâneo,* Coimbra Editora, 2009, p. 374.
[154] M. Prata ROQUE, *A Dimensão* cit., p. 60. Parece também ser esta a sugestão de F. Loureiro BASTOS, "Algumas notas ..." cit., p. 453 e 602.
[155] Hersch LAUTERPACHT, "The International Protection of Human Rights", *RCADI,* vol. 70, 1947-I, p. 24.
[156] M. Prata ROQUE, *A Dimensão* cit., p. 603. Recordo o que referi no ponto 2.1.1. a propósito dos "interesses ligados à entidade do foro".
[157] M. VALE PEREIRA, *A Intervenção ...* cit., p. 374 e ss..
[158] L. LIMA PINHEIRO, *Direito Internacional* cit., p. 22.
[159] Em sentido semelhante, v. P. CAEIRO, *Da Jurisdição Penal* cit., p. 329 e 355.
[160] C. RYNGAERT, *Jurisdiction* cit., p. 40; Michael HENZELIN, *Le Principe de l'Universalité em droit penal international: droit et obligation pour les États de poursuivre et juger selon le principe de l'universalité,* Helbing & Lichtenhahn, 2001, p. 186; Note, "Predictability and Comity: Toward Commons Principles of Extraterritorial Jurisdiction", *HLR,* n.º 98, 1985, p. 1319.

contenção ou moderação no exercício de jurisdição. Devem, então, averiguar se a sua ligação com a situação é ou não a mais estreita e apurar os constrangimentos que a respetiva pretensão extraterritorial provoca nos seus pares[161]. Veja-se a opinião do juiz FITZMAURICE, no caso *Barcelona Traction*: "[do direito internacional] decorre uma obrigação de cada Estado exercer moderação ou contenção na assunção de jurisdição (…) de modo a evitar a usurpação indevida da jurisdição, mais adequada, de outro Estado"[162]. Sucintamente, a entidade do foro deve gizar as suas pretensões tendo presentes preocupações de *coordenação internacional*.

Este ponto de vista é secundado por uma boa parte da doutrina[163] que tem adotado outras designações para a mesma ideia: "princípio da boa fé" [164], "razoabilidade" [165], "interdição de abuso do direito" [166], "proporcionalidade ou proibição do abuso do direito" [167].

Todavia, a *comity* não é um limite que balize de forma precisa os termos da extraterritorialidade havendo quem o descreva como "uma fórmula vazia", ou quem aponte a ausência de uma prática uniforme pelos Estados e de uma metodologia coerente para apreciar os interesses em concurso, entre outras críticas[168]. A incerteza inerente a esta noção e a excessiva amplitude dos vários sentidos que adquire, dos quais é difícil extrair deveres concretos quanto ao exercício de jurisdição extraterritorial, retira-lhe utilidade e operatividade[169]. Aliás, como sublinha D. LOPES, certas conceções desta

[161] CDI, "Report ..." cit., Anexo E, n.º 45.
[162] Acórdão do TIJ, Bélgica c. Espanha, Separate Opinion of Judge Sir Gerald Fitzmaurice, 24 de Julho de 1984, n.º 70.
[163] C. RYNGAERT, *Jurisdiction* cit., p. 145; Dulce LOPES, "A jurisdição extraterritorial dos Estados: entre tradição e modernidade", *Estudos em Homenagem ao Conselheiro Presidente Rui Moura Ramos*, vol. 1, 2016, p. 1071 e ss.; Harold MAIER, "Extraterritorial Jurisdiction at a Crossroads: An Intersection between Public and Private International Law", *AJIL,* vol. 76, n.º 2, 1982, p. 280; Karl MEESSEN, "Conflicts of Jurisdiction under the new Restatement", *LCLP,* vol. 50, n.º 3, 1987, p. 47 e ss.; M. HENZELIN, *Le Principe* cit., p. 232 e M. AKEHURST, "Jurisdiction …" cit., p. 189.
[164] B. STERN, "L'extraterritorialité …" cit., p. 251 e 253 e "Quelques Observations..." cit., p. 45; F. MANN, "The doctrine …" cit., p. 48 a 50.
[165] I. BROWNLIE, *Principles* cit., p. 306; Rosalyn HIGGINS, "The Legal Basis of Jurisdiction", Cecil OLMSTEAD (eds.), *Extra-Territorial Application of Laws and Responses Thereto,* Oxford, 1984, p. 14.
[166] Robert JENNINGS, "Extraterritorial Jurisdiction and the United States Antitrust Laws", *BYIL*, n.º 33, 1957, p. 153.
[167] Alexander LAYTON e Angharad PARRY, "Extraterritorial Jurisdiction – European Responses", *HJIL,* vol. 26, n.º 2, 2004, p. 320.
[168] Andreas BIANCHI, "Extraterritoriality and Export Controls: Some Remarks on the Alleged Antinomy Between European and U.S. Approaches", *GYIL,* vol. 35, 1992, p. 377; D. LOPES, "A jurisdição extraterritorial ..." cit., p. 1094 e 1102; Editorial comment, "Extraterritorial Application of United States Law: The Case of Export Controls", *UPLR,* vol. 132, 1984, p. 380 e ss.; Harold MAIER, "Interest Balancing and Extraterritorial Jurisdiction", *AJCL,* vol. 31, n.º 4, Autumn, 1983, p. 581 e 894 e, do mesmo autor, "Extraterritorial Jurisdiction …" cit., p. 281; Piet VAN SLOT e Eric GRABANDT, "Extraterritoriality and Jurisdiction", *CMLR,* vol. 23, n.º 3, 1986, p. 553.
[169] D. LOPES, *Eficácia* cit., p. 420.

noção, ao invés de travarem o exercício de jurisdição extraterritorial alimentam-no porquanto rejeitam essa necessidade de contenção no momento prescritivo e sugerem um critério apenas para o momento da execução, através de um "espírito de cooperação" entre os Estados, sempre que assumem, de forma concorrente, jurisdição[170].

Mesmo estudos como o de J. ZERK, sobre a razoabilidade de uma legislação criada para produzir efeitos extraterritoriais, propondo dezasseis fatores relevantes para a testar, conferem uma ampla margem de manobra à entidade do foro[171].

2.2.2. Os princípios da jurisdição extraterritorial

Considerando a reduzida utilidade operativa daqueles dois princípios para apurar rigorosamente os limites da jurisdição extraterritorial, em especial nas suas categorias prescritiva e adjudicativa, a maioria dos autores conclui que o DIP não chega a delinear, com a reclamada certeza e exatidão, uma linha vermelha[172]. Como refere B. STERN, a proibição do exercício de poderes coercivos sem o consentimento do Estado *ad quem* é uma das poucas certezas existentes[173]. No campo da jurisdição extraterritorial o DIP parece viver a pulsão conflitual entre normas tradicionais e rígidas (*v.g.* soberania, jurisdição territorial) e novos conceitos e regimes permissivos do seu exercício que vão emergindo, como a doutrina dos efeitos e a jurisdição universal, que explicarei adiante.

Mas será que a entidade do foro pode exercer a sua jurisdição relativamente a todas as situações internacionais? Será que a constatação do recurso à jurisdição extraterritorial em cada vez mais domínios, acompanhada da conclusão sobre a imprecisão quanto aos seus limites, significam a sua extensão ilimitada e absoluta? Julgo que não.

Por um lado, vigora um *princípio de indeterminação dos fundamentos da jurisdição extraterritorial,* isto é, não há uma lista pré-determinada e taxativa de razões "boas" e/ou "más" para a assunção daquela. Por outro lado, a extraterritorialidade, nas suas dimensões prescritiva e adjudicativa, conhece um limite: a exigência de um elo suficientemente

---

[170] *Idem* p. 417.
[171] J. ZERK, "Extraterritorial …" cit., p. 2 e ss.. Entre esses fatores encontra-se, por exemplo, a existência de um consenso razoável sobre o conteúdo da legislação, a probabilidade de não gerar barreiras ao comércio internacional ou distorcer a concorrência, a sensibilidade da legislação aos interesses de outros Estados, entre outros elementos.
[172] António MARQUES DOS SANTOS, *As normas de aplicação imediata no Direito Internacional Privado – Esboço de uma teoria geral,* Vol. II, Almedina, 1991, p. 999; B. AUDIT, "Extraterritorialité ..." cit., p. 420; D. LOPES, *Eficácia* cit., p. 49; F. Loureiro BASTOS, "Algumas notas ..." cit., p. 443; L. LIMA PINHEIRO, *Direito Internacional Privado,* cit., p. 331; M. Prata ROQUE, *A Dimensão* cit., p. 527, nota de rodapé 1585; P. DEMARET, "L'extraterritorialité ..." cit., p. 24.
[173] B. STERN, "L'extraterritorialité …" cit., p. 247.

estreito e genuíno entre a entidade do foro e a situação que propõe regular[174]. Este será o principal limite à jurisdição, presente no caso *Nottebohm*[175], atuando como travão à discricionariedade da entidade do foro[176].

Esses elos foram designados pela CDI como "princípios de jurisdição extraterritorial"[177] paralelamente a outras designações doutrinais, como a de regra *none of your business* [178]. Entre nós, no contexto do direito administrativo transnacional, M. PRATA ROQUE invoca o "princípio da intransatividade" do qual retira um dever de abstenção da entidade do foro sempre que não seja possível identificar uma conexão "suficientemente estreita" (dimensão negativa) e o dever de aplicar o direito da entidade *ad quem*, sob pena de denegação de justiça (dimensão positiva)[179]. Deste modo, a jurisdição extraterritorial encontra-se condicionada por um critério de previsibilidade e de segurança jurídica que orienta a escolha do aplicador entre o direito nacional ou estrangeiro[180]. Em sentido próximo, J. SAMPAIO refere o princípio da "não transatividade" [181], enquanto P. CAEIRO[182] e R. MOURA RAMOS[183] aludem ao "princípio de proximidade". A lógica subjacente é a mesma: a qualquer facto só deve aplicar-se, em princípio, uma lei que com ele esteja em contacto, impondo uma ponderação em concreto da conexão entre a disposição normativa e a situação factual. O não acatamento deste princípio acarretaria o perigo de ofensa de direitos adquiridos ou de expetativas legítimas dos indivíduos, já que deixariam de poder antever os parâmetros normativos aplicáveis às suas atuações.

Não obstante, nem mesmo esta exigência de um "elo" é um limite absoluto ao exercício de jurisdição como denotam certas circunstâncias específicas, creditadas ao princípio da *universalidade* e explicadas de seguida.

---

[174] Benedetto CONFORTI, *International Law and the Role of Domestic Legal Systems,* Martinus Nijhoff, 1995, p. 133 e, do mesmo autor, "The Theory of Competence in Verdross", *EJIL*, vol. 5, 1994, p. 70 e ss.; C. RYNGAERT, *Jurisdiction* cit., p. 104; D. LOPES, *Eficácia* cit., p. 42; F. MANN, "The doctrine …" cit., p. 37; I. BROWNLIE, *Principles of* cit., p. 309; I. JALLES, *Extraterritorialidade* cit., p. 224; M. AKEHURST, "Jurisdiction …" cit., p. 152; Paul TORREMANS, "Extraterritorial Application of E.C. and U.S. Competition Law", *ELR,* vol. 21, 1996, p. 280; P. CAEIRO, *Da Jurisdição Penal* cit., p. 328.

[175] O TIJ considerou não ter sido demonstrado um vínculo suficiente para apurar a nacionalidade de Nottebohm em relação ao Estado do Lichtenstein, v. Acórdão do TIJ, Liechtenstein c. Guatemala, 6 de abril de 1955.

[176] D. LOPES, *Eficácia* cit., p. 44.

[177] CDI, "Report ..." cit., Anexo E, n.º 42.

[178] C. RYNGAERT, *Jurisdiction* cit., p. 39 e Michael RAMSEY, "Escaping 'International comity'", *ILR,* n.º 83, 1998, p. 920.

[179] M. Prata ROQUE, *A Dimensão* cit., p. 61 e 421 e ss...

[180] *Idem*, p. 699.

[181] J. SAMPAIO, *O Acto* cit., p. 58.

[182] P. CAEIRO, *Da Jurisdição Penal* cit., p. 233.

[183] R. MOURA RAMOS, *Da Lei Aplicável* cit., p. 170.

Os princípios da jurisdição extraterritorial surgiram essencialmente na área do direito penal, mas a CDI e a doutrina entendem que a sua função excede aquele âmbito específico[184]. E que função é essa? Não é a de indicar *a* entidade do foro que deve exercer jurisdição sobre uma determinada situação pois pode dar-se o caso de várias invocarem, para a mesma situação, princípios igualmente válidos originando um conflito de jurisdição[185]. Por conseguinte, os princípios da jurisdição extraterritorial apenas geram uma *presunção* de *bona fide* da pretensão extraterritorial de certa entidade do foro, reforçada pela invocação de mais do que um destes princípios num caso concreto[186].

De todos os princípios que de seguida enuncio nem todos apresentam a mesma importância nem a mesma aceitação. Há, desde o caso *Lotus,* divergências em torno da autonomia da doutrina dos efeitos em relação ao princípio da territorialidade objetiva, às quais não é indiferente o contexto em que surgem, nomeadamente nos EUA e na UE[187]. Acresce ainda que a aceitação de cada princípio no plano internacional depende, em grande medida, da proximidade com o *core* das funções da entidade do foro, pelo que, por exemplo, a mobilização do critério do território é conatural ao exercício da jurisdição do Estado[188]. Dito isto, compete à entidade do foro fundamentar a jurisdição num dos seguintes princípios: territorialidade objetiva e doutrina dos efeitos; nacionalidade ou personalidade ativa; personalidade passiva; universalidade e, por fim, proteção.

Segundo a CDI, nos dois primeiros há um nexo ainda territorial com a entidade do foro: o primeiro abarca as situações que ocorrem fora do território quando um elemento constitutivo da conduta ocorreu ali[189]; já a doutrina dos efeitos expandiu o critério da territorialidade, que deixa de abranger apenas os atos materialmente verificados em determinado território, cobrindo a jurisdição sobre comportamentos de estrangeiros, ocorridos fora do território da entidade do foro, que produzam efeitos acolá[190].

---

[184] C. RYNGAERT, *Jurisdiction* cit., p. 104 e ss.; CDI, "Report …" cit., n.º 23; D. LOPES, *Eficácia* cit., p. 44; I. JALLES, *Extraterritorialidade* cit., p. 224 e ss.; M. AKEHURST, "Jurisdiction ..." cit., p. 152 e ss.; M. Prata ROQUE, *A Dimensão* cit., p. 207.

[185] Sobre estes conflitos v. ponto 2.3.2. deste capítulo sobre "um sistema de concorrência de jurisdições".

[186] CDI, "Report ..." cit., Anexo E, n.º 43.

[187] Além da distinção realizada pela CDI, à qual já irei aludir, alguns autores diferenciam os dois fundamentos, v. Jurgen BASEDOW, "Souveraineté Territoriale et Globalisation des Marchés: Le Domaine d'Application des Lois contre Les Restrictions de la Concurrence", *RCADI,* vol. 264, 1997, p. 21, 135 e 140; P. VAN SLOT e E. GRABANDT, "Extraterritoriality and ..." cit, p. 549. Outros autores sustentam uma posição intermédia segundo a qual a doutrina dos efeitos apenas se autonomiza quando os efeitos – diretos, substanciais e razoavelmente previsíveis – se produzem num território, mas são imputáveis a um sujeito que se encontra integralmente fora dali, v. P. DEMARET, "L'Extraterritorialité ..." cit., p. 2.

[188] D. LOPES, *Eficácia* cit., p. 47.

[189] CDI, "Report ..." cit., Anexo E, n.º 11.

[190] *Idem*, n.º 12.

Intimamente próxima da territorialidade objetiva, a doutrina dos efeitos comporta uma diluição do nexo territorial já que não pressupõe que um elemento da conduta a regular ocorra no território da entidade do foro. Por conseguinte, estes dois princípios atestam a elasticidade e evolução do conceito de territorialidade à acomodação dos interesses internos e externos da entidade do foro[191].

Como se vê, enquanto fundamento da jurisdição, o território não foi (ainda) esquecido adaptando-se de modo a superar o teste do tempo[192]. É, aliás, a sua reconfiguração a origem de incertezas quanto aos termos precisos da jurisdição extraterritorial *pura,* ou seja, aquela que visa regular a conduta de pessoas, bens ou atos sem qualquer ligação ao território da entidade do foro. Essencialmente questiona-se o rigor da expressão *extra*territorialidade quando na mesma cabem formas *impuras,* isto é, casos de regulação de pessoas, bens ou atos assentes num nexo territorial com a entidade do foro. Com frequência a invocação de extraterritorialidade reflete pretensões da entidade do foro sobre violações de direito da concorrência ou de direito financeiro, ocorridas em países terceiros, provocadas por estrangeiros, mas com impacto naquela entidade (doutrina dos efeitos). Nestas situações o próprio impacto da conduta estrangeira na entidade do foro é ficcionado como um *impacto territorial*[193]. Por isso, há quem proponha a designação de jurisdição "não exclusivamente territorial"[194] e quem critique frontalmente o uso da expressão "extraterritorial"[195]. Por fim há ainda aqueles que, com base na pulverização das situações da vida contemporânea e na imbricação dos interesses económicos, rejeitam verdadeiros casos de extraterritorialidade[196]. Daí a distinção entre forma *puras* e formas *impuras* de extraterritorialidade, as primeiras reservadas para aquelas situações em que não existe qualquer conexão com o território da entidade do foro. Como refiro adiante é esse o caso do princípio da universalidade.

---

[191] Constatando esta evolução e declarando uma territorialidade desagregada (*unbundled territoriality*) como marca da pós-modernidade, v. John RUGGIE, "Territoriality and Beyond: Problematizing Modernity in International Relations", *IO,* vol. 47, n.º 1, Inverno, 1993, p. 139 e ss..

[192] Sublinhando uma "atenuação" do princípio da territorialidade, v. J. SAMPAIO, *O Acto* cit., p. 16.

[193] Como explica RYNGAERT: "Qualquer assunção de jurisdição extraterritorial visa defender os interesses do Estado enquanto entidade territorialmente definida, pelo que terá sempre um nexo territorial". O autor considera ainda que, sempre que não exista uma deslocação física dos poderes públicos da entidade do foro (do legislador, por exemplo) ao território estrangeiro, o exercício de extraterritorialidade será sempre territorialmente circunscrito, v. C. RYNGAERT, *Jurisdiction in* cit., p. 7 e 40.

[194] *Idem*, p. 7.

[195] François RIGAUX, "Droit économique et conflits de souverainetés", *Rabels Zeitschrift fur auslandisches und internationals Privatrecht,* Ano 52, vol.1/2, 1988, p. 112 e N. DOBSON e C. RYNGAERT, "EU 'Extraterritorial' ..." cit., p. 295 e ss..

[196] I. JALLES, *Extraterritorialidade* cit., p. 43.

Ao abrigo do princípio da nacionalidade a jurisdição não se firma somente nos casos de controlo físico, pela entidade do foro, sobre o seu nacional[197]. Aquele princípio fundamenta a jurisdição sobre as atividades e condutas de nacionais, incluindo empresas, aeronaves e barcos, independentemente da sua localização geográfica, isto é, dentro ou fora do território da entidade do foro. Numa época como a nossa, na qual assumem relevância enquanto agentes económicos empresas, transnacionais ou multinacionais, concebidos como centros de imputação de direitos e deveres, as questões mais duvidosas suscitadas pela aplicação deste princípio resultam da *ficção* que consiste em falar da nacionalidade de uma pessoa coletiva e da dificuldade em encontrar critérios de conexão que sejam suficientemente significativos e aceites por unanimidade.

Estes critérios são múltiplos e não se encontram hierarquizados: a sua estrutura jurídica varia largamente, entre o local da sede da pessoa coletiva – estatutária, social ou efetiva[198]– a nacionalidade da maioria dos membros, a sua incorporação[199] ou o local da constituição[200]. Em face desta entropia, a extraterritorialidade vem-se firmando em relação a empresas que não se encontram estatutariamente, com domicílio fiscal ou residência habitual, no território da entidade do foro.

O exemplo mais antigo vem do direito norte-americano[201], utilizando como critério a mera existência de algum controlo de uma pessoa coletiva por parte de nacionais dos EUA para impor prescrições àquela, uma solução cunhada como *doutrina do controlo*. Esta pressupõe uma negação ou, pelo menos, uma relativização, da personalidade jurídica da pessoa coletiva, rejeitando e pondo de parte o facto essencial de que ela constitui uma entidade jurídica, um sujeito de direito distinto dos membros que a constituem. A doutrina do controlo visa ultrapassar o rigor das construções jurídicas ou, pelo menos, abandonar o juridismo excessivo, para determinar quais os interesses económicos e/ou políticos

[197] *Idem*, p. 306.
[198] Em certos países entende-se por sede social a sede estatutária, isto é, a sede que é designada nos estatutos ou no pacto social, independentemente de a administração principal da sociedade se encontrar aí situada, enquanto em outros países a jurisprudência e a doutrina se pronunciam em favor da sede social *real,* isto é, não fictícia, séria ou não fraudulenta.
[199] A sociedade tem a nacionalidade de um país, se for constituída, criada, "incorporada", segundo o direito desse país. Para um Estado que adote este critério como único e exclusivo, são nacionais todas as sociedades que nascerem como pessoas jurídicas por força do direito desse Estado, qualquer que seja o lugar da sede social, do centro de exploração, do exercício da sua atividade comercial ou industrial, qualquer que seja a nacionalidade dos sócios, acionistas ou administradores, ou até mesmo qualquer que seja o lugar onde a sociedade foi constituída.
[200] M. Prata ROQUE, *A Dimensão* cit., p. 744. Sobre a conceção imprópria de "nacionalidade" em relação às pessoas coletivas privadas, v. António CORREIA, *Lições de Direito Internacional Privado,* vol. I, Almedina, 2000, p. 82; L. LIMA PINHEIRO, *Direito Internacional Privado,* vol. II, cit., p. 114 e ss..
[201] I. JALLES, *Extraterritorialidade* cit., p. 308 e ss..

reais que se perfilam – ou escondem – por detrás do ente coletivo[202]. Em sentido próximo, na UE, vigora uma teorização, já subscrita pelo TJ no domínio do direito da concorrência, designada *teoria da unidade económica*[203]. Como é sabido, por regra o legislador presume que as empresas que pertencem ao mesmo grupo, tendo personalidade jurídica, são sujeitos jurídicos autónomos. Porém, em certas circunstâncias, se a entidade do foro olha para o grupo como uma *unidade económica única* poderá assumir jurisdição sobre os seus membros situados além-fronteiras. O que estes exemplos sugerem é que a imprecisão da "nacionalidade" das pessoas coletivas flexibiliza o recurso à extraterritorialidade e alarga o substrato pessoal da jurisdição da entidade do foro.

O princípio da personalidade passiva é invocado para fundamentar a aplicação da lei nacional a condutas e atividades ocorridas no estrangeiro, danosas para os nacionais. O que oferece fundamento a este princípio é a necessidade, sentida pela entidade do foro, de proteger os seus nacionais. A CDI aponta a possibilidade deste princípio se diluir na doutrina dos efeitos, por se tratar de uma aplicação específica daquela e sublinha que, apesar de uma certa rejeição inicial, este princípio é cada vez mais aceite, sobretudo quando combinado com outros[204].

O princípio da universalidade, uma entorse à regra *none of your business*, confere jurisdição *pura,* ou seja, independentemente de qualquer conexão (territorial ou não) com a entidade do foro, em relação a certos crimes que, extravasando territórios, se convolam em assunto público da comunidade internacional[205]. A discussão à volta deste princípio ganhou a atenção da doutrina pelo menos em dois momentos: a propósito do caso *Eichmann,* um oficial do regime Nazi capturado na Argentina, por agentes israelitas e posteriormente julgado em Israel, e aquando da pronúncia da Câmara dos Lordes no âmbito do caso *Pinochet*[206].

Por último, o princípio da proteção ancora a jurisdição em relação a pessoas, bens e atos verificados no estrangeiro que constituem uma ameaça a interesses fundamentais da

---

[202] As suas preocupações são primacialmente económicas ou político-económicas, v. António MARQUES DOS SANTOS, *Algumas reflexões sobre a nacionalidade das sociedades em direito internacional privado e em direito internacional público,* Coimbra, 1985, p. 74.

[203] Carsten KOENING, "An Economic Analysis of the single economic entity doctrine in EU competition law", *JCLE,* vol. 13, n.º 2, junho de 2017, p. 281 e ss.; Okeoghene ODUDU e David BAILEY, "The single economic entity doctrine in EU competition law", *CMLR,* n.º 51, 2014, p. 1721 e ss.; Peter BEHRENS, "The extraterritorial reach of EU competition law revisited: The 'effects doctrine' before the ECJ", Discussion Paper, Europa-Kolleg Hamburg, n.º 3/16.

[204] CDI, "Report ..." cit., Anexo E, n.º 13.

[205] M. HENZELIN, *Le Principe* cit., p. 179 e CDI, "Report …" cit., n.º 16.

[206] Francisco FERREIRA DE ALMEIDA, *Os Crimes Contra a Humanidade no Actual Direito Internacional Penal,* Almedina, 2009, p. 171 e ss..

entidade do foro, nomeadamente ameaças estrangeiras à segurança nacional. Para a CDI a autonomia deste princípio é duvidosa sugerindo que se trata de uma aplicação específica da territorialidade objetiva ou da doutrina dos efeitos[207].

Deste elenco constata-se a porosidade dos critérios da territorialidade e da componente pessoal da jurisdição, possivelmente estendidos por força da pressão dos avanços da globalização, do surgimento de agentes económicos multinacionais ou transnacionais, dos *standards* internacionais de respeito pelos direitos fundamentais, entre outros fatores[208]. Não obstante, a territorialidade não foi abandonada e é ainda o principal "quadro de referência" do exercício do poder público[209]. Além disto, como já fui dizendo, o território desempenha ainda uma função relevante no que ao exercício de poderes coercivos diz respeito.

2.2.3. O *deficit* democrático das prescrições extraterritoriais

Paredes meias com o já referido problema (filosófico) da validade do direito no mundo do pluralismo jurídico[210] emerge outro: a *legitimidade* da intervenção de múltiplos atores, de natureza pública e privada, no contexto internacional. Ou, dito de outro modo, a necessidade de "os poderes políticos se pautarem, na sua atuação, por princípios ético-jurídicos aos quais a comunidade adira ou com os quais se identifique, de tal modo que aceite, generalizadamente, os atos autoritários provenientes daquelas autoridades"[211].

Paralelamente, com o crescimento das manifestações contemporâneas de extraterritorialidade, surge um debate sobre a legitimidade da entidade do foro para dirigir prescrições a destinatários estrangeiros (pessoas singulares e coletivas) sem representação, pondo em perigo um elementar princípio democrático. Com efeito, os estrangeiros não dispõem de mecanismos jurídico-constitucionais para influenciar a tomada de decisão legislativa primária. É este o argumento central das posições que sustentam um regresso ao territorialismo estrito, conjugadas com o pressuposto de que o avanço da extraterritorialidade aumenta a ineficácia das regulações internacionais e o risco de adjudicações inconsistentes[212].

---

[207] CDI, "Report …" cit., n.º 13.
[208] D. LOPES, *Eficácia* cit., p. 56.
[209] *Idem* p. 37.
[210] Deixado em aberto por A. SANTOS CAMPOS, *Glosas Abertas* cit., p. 315 e ss..
[211] D. LOPES, *Eficácia* cit., p. 107.
[212] Austen PARRISH, "The Effects Test: Extraterritoriality's Fifith Business", *VLR,* vol. 61, n.º 5, 2008, p. 1455 e ss. e, do mesmo autor, "Reclaiming …" cit., p. 865 e "Kiobel, Unilateralism, and the Retreat from

Em boa verdade, esta falha de legitimidade poderá ser equacionada em relação a situações hoje incontestadas, como a aplicação do direito estadual a estrangeiros que nele residem e que não participam, em regra, na formação das decisões que lhes são aplicáveis[213], bem como a casos mais recentes de subjetividade internacional, os novos sujeitos de DIP, sem representação e legitimidade democrática[214].

Em todo o caso, as críticas não têm sido unidirecionais havendo quem enfatize que a legitimidade deixou de ser um "dado adquirido" ou um "valor absoluto"[215] e, por conseguinte, o que é hoje relevante são as *condições de exercício de autoridade*; outros, em especial a propósito da UE, sublinham novas dimensões deste conceito, assentes em critérios de resultados ou *out-put legitimacy* para contrabalançar o défice da legitimação democrática[216]. Se, por exemplo, a aplicação de uma norma a estrangeiros sem representação corresponder a uma tentativa de proteger a economia da entidade do foro, o seu mercado ou os direitos dos indivíduos e consumidores que ali se encontram, equaciona-se a hipótese de consentimento tácito dos estrangeiros quanto às normas que se aplicam no mercado onde consabidamente atuam. Como sintetiza D. SVANTESSON, nestes casos, "cada parte decide por si qual o mercado onde quer prestar serviços e vender bens e, por exemplo, a obrigação de uma empresa americana respeitar o direito da UE quando interage com o mercado daquela não é muito diferente do ónus que recai sobre um turista americano de respeitar o direito francês quando visita a Torre Eiffel"[217].

Há ainda quem proponha soluções para mitigar estas falhas, através de mecanismos de cooperação, em especial a abertura dos procedimentos legislativos a interessados estrangeiros, o reforço da transparência e o desenvolvimento de mecanismos de

---

Extraterritoriality, *MJOL*, vol. 28, 2013, p. 208 e ss.. Numa perspetiva mais otimista, v. S. BATTINI, "Globalisation …" cit., p. 75.

[213] M. Prata ROQUE, *A Dimensão* cit., p. 357 e ss.. O autor salienta que, por exemplo, as Constituições nacionais não restringem a noção de "administrado" (enquanto destinatário de normas e deveres jurídicos) aos indivíduos eleitoralmente ativos ou sequer aos que dispõem de capacidade eleitoral. Dele não são excluídos os menores, os incapazes (...) e os estrangeiros residentes".

[214] C. QUEIROZ, *Direito Constitucional* cit., p. 38; D. LOPES, *Eficácia* cit., p. 311 e 312; M. Prata ROQUE, *A Dimensão* cit., p. 924 e 933.

[215] D. LOPES, *Eficácia* cit., p. 113.

[216] Anand MENON e Stephen WEATHERHILL, "Transnational Legitimacy in a Globalizing World: How the European Union Rescues its States", *WEP*, vol. 31, n.º 3, 2008, p. 402; Koen LENAERTS, Marlies DESOMER, "New Models Of Constitution-Making in Europe: The Quest For Legitimicy", *CMLR*, vol. 29, 2002, p. 1223 e ss..

[217] D. SVANTESSON, *Extraterritoriality* cit., p. 171. Em sentido próximo, v. M. Prata ROQUE, *A Dimensão* cit., p. 358.

reconhecimento mútuo que convidem à compatibilização das prescrições com vocação extraterritorial do foro com a ordem jurídica da entidade *ad quem*[218].

2.3.Efeitos

2.3.1. As reações comuns

A tipologia clássica[219] das reações comuns ao exercício de jurisdição extraterritorial toma por referência os sujeitos passivos, em especial os destinatários indiretos da extraterritorialidade ou entidades *ad quem*[220]. São reações *comuns*, pela sua frequência, mas não são uniformes no sentido em que se arrumam apenas numa escala variável, resultante da ponderação casuística entre os interesses estritamente da entidade *ad quem* e os interesses da mesma em cooperar em termos internacionais. Com efeito, as reações das entidades *ad quem* dependerão, em larga medida, da natureza e extensão das externalidades produzidas pela extraterritorialidade e da sensibilidade e motivação daquelas; daí que J. BASEDOW as categorize como "contramedidas factuais" no sentido em que não convocam, necessariamente, a violação de uma obrigação do DIP[221].

Sucintamente, referem-se a comportamentos da entidade *ad quem* que oscilam entre:

(i) Tomadas de posição contestatárias (reações negativas) da pretensão extraterritorial da entidade do foro quando esta é percecionada como ilegal, ofensiva ou simplesmente contrária ao interesse nacional. Estes posicionamentos oscilam entre os protestos diplomáticos e a adoção de medidas de bloqueamento[222] (2.3.1.1); e

[218] D. LOPES, *Eficácia* cit., p. 312 e 313. A autora sublinha que o instituto do reconhecimento confere ao Estado a primeira e a última palavra quanto à eficácia do direito estrangeiro no seu território e, portanto, "os princípios da democracia e do Estado de Direito tanto *fundamentam* como *limitam* a aplicação do direito estrangeiro no foro" e "também o reconhecimento (...) pode funcionar, a uma luz, como mecanismo que *agrava* e, a outra luz, como mecanismo que *atenua* os défices de legitimidade que se verificam nas situações de jurisdição extraterritorial".

[219] Especificamente sobre esta tipologia, v. I. JALLES, *Extraterritorialidade* cit., p. 117 e ss..

[220] Excluí, por agora, as reações dos outros sujeitos passivos para delas cuidar mais adiante.

[221] J. BASEDOW, *The Law of* cit., p. 389. A expressão "contra-medida" ou é usada como sinónimo de represália (com exclusão das represálias armadas), no sentido que lhe é atribuído pela CDI nos trabalhos sobre a responsabilidade internacional dos Estados, como sinónimo de quaisquer medidas reativas ao ilícito (incluindo a legítima defesa), ou, enfim, como expressão que inclui, não só as medidas em princípio ilícitas (as represálias), como, também, as medidas de retorsão, v. J. AZEREDO LOPES, *Entre Solidão* cit., p. 550 e 561.

[222] J. BASEDOW, *The Law of* cit., p. 388.

(ii) Contrastando com as reações anteriores vislumbram-se comportamentos que revelam uma aceitação ou concordância com a intenção, o interesse a tutelar ou com a política subjacente ao exercício de jurisdição extraterritorial (reações positivas, 2.3.1.2)[223].

A esta tipologia clássica acrescento as reações, de igual geometria variável, dos sujeitos passivos *diretos*, isto é, das pessoas singulares ou coletivas a quem se destinam os comandos extraterritoriais da entidade do foro.

2.3.1.1.Reações negativas

Dada a tendencial ausência de processos obrigatórios de resolução pacífica dos diferendos no DIP[224], as reações negativas constituem mecanismos de autotutela, de autoproteção ou de justiça privada, similares à *retorsão*[225] ou à *retaliação pacífica*[226]. Ou seja, são atuações unilaterais que pretendem suprir a falta de mecanismos institucionalizados no DIP para a aplicação de sanções, veiculando, individualmente, uma defesa dos direitos da entidade *ad quem* com base numa apreciação própria das circunstâncias.

Entre este tipo de reações encontram-se, desde logo, os protestos diplomáticos[227]. Os exemplos mais citados são os protestos suscitados por decisões de jurisprudência estrangeira ou pela adoção de legislação com efeitos que se fazem sentir além-fronteiras:

[223] Beth SIMMONS, "The International Politics of Harmonization: The Case of Capital Market Regulation", *IO,* vol. 55, n.º 3, 2001, p. 589 e ss. e Yuko SUDA, "Transatlantic Politics of Data Transfer: Extraterritoriality, Counter-Extraterritoriality and Counter-Terrorism", *JCMS,* vol. 51, n.º 4, 2013, p. 774 e ss. e, do mesmo autor, *The Politics of Data Transfer. Transatlantic conflict and cooperation over data privacy,* Routledge, 2018.

[224] Trata-se de um "ordenamento jurídico predominantemente descentralizado e escassamente organizado, pelo que, em princípio, cabe ao Estado vítima (...) recorrer a medidas de autotutela ou autoproteção", v. Juan SALCEDO, *El Derecho Internacional em un Mundo em cambio,* Tecnos, 1985, p. 159.

[225] Descreve os "atos inamistosos em relação ao seu destinatário ou em seu detrimento, mas que não são ilícitos em si, pois não violam nenhuma obrigação a cargo do seu autor", v. Georges ABI-SAAB, "Cours général de droit international", *RCADI*, vol. 207, 1987, p. 294. Entre nós, Joaquim SILVA CUNHA define contramedidas como "as medidas de auto-tutela dos interesses dos Estado consentidas pelo Direito Internacional comum ou geral (retorsão e represálias)" e continua explicando que "a forma mais moderada de autotutela é a retorsão, que consiste em geral em reagir contra um ato lícito, mas pouco amistoso, como outro também lícito e igualmente pouco amistoso. Na prática internacional, porém, a retorsão pode também revestir a forma de reação estadual, por meio de um ato lícito, contra um ato ilícito de outro Estado, e nesta hipótese, pode incluir-se no número de sanções do Direito Internacional", v. Joaquim SILVA CUNHA, *Direito Internacional Público, Relações Internacionais (Aspetos fundamentais do seu regime),* Instituto Superior de Ciências Sociais e Políticas, 1990, p. 127 e 131 e ss..

[226] A expressão é de C. BRUMMER, "Territoriality as ..." cit., p. 512.

[227] Sobre esta figura, F. FERREIRA DE ALMEIDA, *Direito Internacional* cit., p. 186 e Maria Luísa DUARTE, *Direito Internacional Público e Ordem Jurídica Global do Século XXI,* Coimbra Editora, 2014, p. 151.

por ocasião da aplicação do *Sherman Act*, nos anos 40, pelos tribunais norte-americanos[228] ou, mais recentemente, aquando das sanções extraterritoriais dos EUA contra o Irão, a Rússia e a Coreia do Norte[229].

Mas as reações negativas não se limitam aos protestos diplomáticos. Veja-se o caso das leis de blocagem, medidas de bloqueamento, "leis-antídoto", "leis anti-garras" ou leis bloqueadoras[230]. Tratam-se de atos legislativos especificamente adotados para obstar aos efeitos perniciosos do direito estrangeiro e, sobretudo, sinalizar a discórdia política ou questionar a sua validade jusinternacional, com frequência criando um conflito *direto* ou *positivo* de leis[231].

As primeiras leis de blocagem[232] foram adotadas, em larga medida, como meio de contestação dos métodos usados pelos EUA para assegurar a aplicação eficaz da respetiva legislação, em particular o exercício dos poderes de autoridades públicas fora de portas, ou seja, a respetiva jurisdição de execução[233]. A oposição incidia sobre os esforços de agências administrativas tuteladas pelo Congresso para, na aplicação da legislação *antitrust* e no domínio dos transportes marítimos*,* no âmbito do chamado processo de *discovery,* conduzirem inquéritos fora do respetivo território e emitirem ordens, cujos destinatários eram empresas, para a comunicação de documentos localizados em território estrangeiro, nas respetivas sucursais ou filiais[234]. Além das autoridades administrativas,

---

[228] Por exemplo, como sucedeu em *In re Grand Jury Investigation of the Shipping Industry* quando um *federal grand jury* requereu a produção de documentos localizados num Estado terceiro, produção essa que é contrária ao direito local e, por conseguinte, espoletou protestos dos Governos do Reino Unido, Canadá, Dinamarca, França, Alemanha, Itália, Japão, Holanda. A CDI enuncia outros exemplos, v. "Report on the Work…" cit., Anexo E, n.º 28 e I. JALLES, *Extraterritorialidade* cit., p. 163.

[229] "France says U.S. Sanctions on Iran, Russia look illegal", *Reuters*, 26 de julho de 2017, disponível em https://www.usnews.com/news/world/articles/2017-07-26/france-says-us-sanctions-on-iran-russia-look-illegal, consultado no 30 de setembro de 2018.

[230] B. AUDIT, "Extraterritorialité …" cit., p. 401 e ss.; B. STERN, "Quelques Observations ..." cit, p. 40 e ss.; C. BRUMMER, "Territoriality as ..." cit., p. 509 e ss.; I. JALLES, *Extraterritorialidade* cit., p. 151 e ss.; M. Prata ROQUE, *A Dimensão* cit., p. 725 e ss..

[231] CDI, "Report …" cit., Anexo E, n.º 28, nota de rodapé 48; D. LOPES, *Eficácia* cit., p. 47; I. JALLES, *Extraterritorialidade* cit., p. 151; Nicolas DIACAKIS, *Problèmes Liés Aux Effets extraterritoriaux des normes communautaires,* Bruylant, 2000, p. 179.

[232] Para uma perspetiva histórica, v. Evelyne FRIEDEL-SOUCHU, *Extraterritorialité du droit de la concurrence aux etats-unis et dans la communauté européene,* LGDJ, 1994, p. 241; I. JALLES, *Extraterritorialidade* cit., p. 151 e N. DIACAKIS, *Problèmes* cit., p. 180.

[233] N. DIACAKIS, *Problèmes* cit., p. 181 e 182. Foi também esta a opinião secundada pelo AG do TJ, no caso *Pâte de bois:* "Aliás, é essencialmente contra as medidas tomadas com base na jurisdição de execução que cerca de vinte estados adotaram as chamadas "leis de blocagem"", v. Conclusões do AG no Acórdão do TJ, Ahlstrom c. Comissão Europeia, C-89/85, C-104/85, C-114/85, C-116/85, C-117/85 e C-125/85 a C-129/85, apresentadas em 25 de maio de 1988, n.º 28.

[234] Como a *Security and Exchange Commission*, o *National Labor Relations Board* ou a *Federal Trade Commission*. Cfr. Cedric RYNGAERT, "Conflicts of Jurisdiction over orders to produce documents located abroad: reappraising 'conflict of international jurisdiction: ordering the production of documents in violation of the law of the situs'", *Revue Belge de Droit International,* vol. 1, n.º 2, 2015, p. 423 e ss. e I. JALLES, *Extraterritorialidade* cit., p. 89 e 90.

os tribunais dos EUA podem, no quadro das exigências processuais do *pre-trial discovery,* caraterístico dos sistemas de *common law,* notificar ou intimar uma empresa, com atividade nos dois lados do Atlântico, a apresentar provas, documentos ou informações, mesmo que se encontrem localizadas em território europeu[235]. Os problemas criados inicialmente por estas inquirições, consideradas abusivas[236], decorrem de lacunas na Convenção de Haia de 1970 sobre a obtenção de provas em matéria civil e comercial[237]. Com o advento da era digital estes problemas persistem, com uma nova configuração, como exemplifica o caso *Microsoft* estudado na Parte II.

Na década de 90 a UE adotou o Regulamento 2271/96, de 22 de novembro de 1996, relativo à proteção contra os efeitos da aplicação extraterritorial de legislação adotada por um país terceiro e das medidas nela baseadas ou dela resultantes[238]. Entendeu-se que o "expansionismo jurídico americano" lesava ou podia lesar "a ordem jurídica estabelecida e prejudicar os interesses da Comunidade e das pessoas, singulares e coletivas, que exercem direitos ao abrigo do Tratado que institui a Comunidade Europeia", afirmando-se o imperativo de neutralizar, opor ou, de qualquer forma, contrariar "os efeitos da legislação estrangeira em questão".

Igualmente importante é a recente vaga de legislação bloqueante, que inclui os EUA, em reação a uma medida da UE, de redução das emissões de carbono da indústria da aviação, que antecedeu o já referido acordo CORSIA[239]. Numa Diretiva de 2008, a UE incluiu as atividades daquele setor no regime de comércio de licenças de emissão de gases

---

[235] G29, "Documento de Trabalho 1/2009 sobre a troca preliminar de informação ("*pre-trial discovery")* nos litígios cíveis transfronteiriços", 11 de fevereiro de 2009, p. 6.

[236] É essa a descrição do Relatório Mayoud sobre a lei de bloqueamento francesa de 1980, v. "Rapport Mayoud sur le projet de la loi de 16.7.1980", Assemblé Nationale, n.º 1814, p. 8, disponível em http://archives.assemblee-nationale.fr/7/cri/1983-1984-ordinaire1/086.pdf, consultado no dia 30 de setembro de 2018.

[237] Ora porque as normas desta Convenção não são extensíveis ao domínio fiscal, ao domínio da concorrência e do controlo de exportações, ora por força da invocação frequente do art. 23.º daquele instrumento (onde se pode ler: "Os Estados contratantes podem, no momento da assinatura, ratificação ou adesão, declarar que não cumprirão cartas rogatórias que tenham por objeto um processo conhecido do *Common Law* pela designação de *pre-trial discovery documents*), v. N. DIACAKIS, *Problèmes* cit., p. 184.

[238] A revisão deste diploma está em curso à data em que escrevo, v. Proposta de Regulamento do PE e do Conselho relativo à proteção contra os efeitos da aplicação extraterritorial de legislação adotada por um país terceiro e das medidas nela baseadas ou dela resultantes, disponível em http://eur-lex.europa.eu/legal-content/PT/HIS/?uri=COM:2015:0048:FIN#documentView, consultado no 30 de setembro de 2018.

[239] Lorand BARTELS, "The WTO Legality of the Application of the EU's Emission Trading System to Aviation", *EJIL,* vol. 23, n.º 2, maio de 2012, p. 429 e ss.; Rachel ROSENFELD, "The European Union Aviation Directive and U.S. Resistance: A Deadlock on Aviation Emissions Control", *GIELR,* n.º 25, 2012-2013, p. 589 e ss.; Stefanie HIIESINGER e Petros MAVROIDI, "Planes, Trains, and Automobiles: The EU Legislation on Climate Change and the Question of Consistency with WTO Law", EUI Working Papers, AEL 2013/04, disponível em http://cadmus.eui.eu/bitstream/handle/1814/27457/AEL_2013_04.pdf?sequence=3&isAllowed=y, consultado no dia 30 de setembro de 2018.

com efeito de estufa prevendo que, a partir do dia 1 de Janeiro de 2012, todos os operadores de aeronaves, incluindo companhias aéreas estrangeiras que aterram e descolam de um aeródromo situado na UE, deviam, até 30 de abril de cada ano, devolver licenças de emissão suficientes para cobrir as suas emissões no ano anterior, sob pena de serem obrigadas a pagar uma multa pelas emissões excedentárias[240]. Em reação, em julho de 2011, o Congresso dos EUA adotou o *European Union Emissions Trading Scheme Prohibition Act of 2011*[241] onde, *inter alia,* se proíbem os operadores da aviação civil norte-americana de participar nos esquemas de licença e comércio de emissões unilateralmente estabelecidos pela UE. Esta recente geração de medidas legislativas de bloqueamento contou também com a China[242] e com outros países[243].

Em relação aos seus *efeitos*, genericamente, estas reações constituem uma tentativa de moderar o alcance extraterritorial da legislação estrangeira, interditando a comunicação de certos documentos ou informações às autoridades estrangeiras, proibindo a obediência às respetivas injunções, impedindo o reconhecimento e execução de decisões adotadas por tribunais estrangeiros, entre outros[244]. Em bom rigor, estas medidas constituem uma retorsão ou uma retaliação pacífica a um comportamento de outro sujeito, pelo que o seu principal objetivo é *político*: manifestar à opinião pública mundial uma desaprovação em relação às práticas da entidade do foro. Por um lado, enquanto medidas de retorsão lícitas, atuam como meios de pressão e, por outro, assemelham-se aos protestos diplomáticos, enquanto meios de publicitar a vontade e o desacordo da entidade *ad quem*, com a diferença de instrumentalizarem os agentes económicos transnacionais, gerando um clima de hostilidade interestadual com impacto nas atividades daqueles[245]. Todavia, nos países ocidentais, a confrontação chega, em

---

[240] Art. 3.º, al. r) e 16.º, n.º 3 da Diretiva 2008/101/CE do Parlamento Europeu e do Conselho, de 19 de Novembro de 2008 que altera a Diretiva 2003/87/CE de modo a incluir as atividades da aviação no regime de comércio de licenças de emissão de gases com efeito de estufa na Comunidade. Sobre o tema, v. Jacques HARTMAN, "The European Emissions Trading System and Extraterritorial Jurisdiction", *EIJL Analysis,* 23 de abril de 2012, disponível em https://www.ejiltalk.org/the-european-emissions-trading-system-and-extraterritorial-jurisdiction/, consultado no dia 30 de setembro de 2018.

[241] H.R. 2594 – *European Union Emissions Trading Scheme Prohibition Act of 2011*.

[242] Bridges Weekly Trade News Digest, vol. 16, n.º 5, 8 de fevereiro de 2012; LEWIS, Barbara e VOLCOVICI, Valerie, "Insight: U.S., China turned EU powers against airline pollution law", *Reuters*, 10 de dezembro de 2012, disponível em http://www.reuters.com/article/us-eu-airlines-climate/insight-u-s-china-turned-eu-powers-against-airline-pollution-law-idUSBRE8B801H20121210, consultado no 30 de setembro de 2018.

[243] No caso da Austrália o Governo entendeu que o fórum para discutir estes problemas seria a Organizaçao Internacional da Aviação Civil, v. o debate parlamentar de 28 de Maio de 2012, disponível em http://www.openaustralia.org.au/debates/?id=2012-05-28.178.1#g180.1.

[244] D. SVANTESSON, *Extraterritoriality* cit., p. 161; I. JALLES, *Extraterritorialidade* cit., p. 184; J. BASEDOW, *The Law of* cit., p. 392; N. DIACAKIS, *Problèmes* cit., p. 186.

[245] J. BASEDOW, *The Law of* cit., p. 395.

regra, a bom porto, culminando com acordos de cooperação, como aconteceu no caso do direito da concorrência[246]. Noutros casos os EUA desistiram mesmo da extraterritorialidade[247].

Como se depreende, os efeitos destas reações estendem-se aos outros sujeitos passivos da extraterritorialidade, as pessoas coletivas e singulares ou destinatários diretos dos comandos da entidade do foro. Estes são afetados, por exemplo, na sua mobilidade internacional, e envolvidos num jogo de forças de natureza política e colocados numa difícil situação, sobretudo quando o incumprimento das normas em conflito seja sancionado[248]. Gera-se, nestes casos, um conflito positivo, "verdadeiro" ou "absoluto" de pretensões: por exemplo, a entidade *ad quem* elege como critério para determinar a sua jurisdição a territorialidade objetiva (isto é, a atividade ou uma parte desta desenvolve-se no seu território) ou a doutrina dos efeitos, proibindo determinado comportamento ao agente; já a entidade do foro, caso a sede estatutária do agente económico se situe no seu território, reclamará jurisdição e exigirá o comportamento proibido acolá[249].

Em todo o caso, a invocação de uma disposição bloqueante poderá servir como meio de defesa dos agentes económicos transnacionais em casos de incumprimento. No caso dos EUA, numa tendência originada numa decisão de 1987 do *Supreme Court, Societe Nationale Industrielle Aerospatiale,* aquele tribunal defendeu a necessidade de atender à posição do agente económico e aos interesses estrangeiros nos casos relacionados com o processo de *discovery*[250]. Neste sentido, estas medidas configuram um meio de pressão junto das instâncias com pretensão extraterritorial convocando o argumento da *foreign sovereign compulsion doctrine*[251]*, regulated conduct defense*[252],

---

[246] O acordo mais importante neste domínio foi celebrado entre os EUA e a Comissão Europeia, sobre a aplicação do direito da concorrência, v. J. BASEDOW, *The Law of* cit., p. 395.
[247] Como sucedeu no caso do *Helms-Burton Act,* de 1996, suspenso pelo Presidente dos EUA, v. "Statement of the President of the USA of 3 january 1997", *International Legal Matters,* n.º 36, 1997, p. 216 e ss..
[248] J. BASEDOW, *The Law of* cit., p. 389.
[249] E. FRIEDEL-SOUCHU, *Extraterritorialité du* cit., p. 249; M. HENZELIN, *Le Principe* cit., p. 185; M. Prata ROQUE, *A Dimensão* cit., p. 609 e ss.; P. CAEIRO, *Da Jurisdição Penal* cit., p. 356 e ss..
[250] "Os tribunais Americanos, nos processos de *pretrial*, devem atender aos interesses dos litigantes estrangeiros, em especial aos fardos desnecessários e indevidos e à posição desvantajosa de um pedido de *discovery* (…). As objeções à *discovery* abusiva devem, por isso, merecer cuidadosa atenção. Adicionalmente, há muito que a jurisprudência reconhece a *comity* em processos que envolvem os interesses de outros Estados (...)", v. Acórdão do SCJ*,* Societe Nationale Industrielle Aerospatiale c. U.S. District Court for the Southern District of Iowa*,* 482, U.S. 522, 15 de junho de 1987, p. 546.
[251] CDI, "Report ..." cit., Anexo E, n.º 31.
[252] Esta é a designação da OCDE, *Roundtable of Competition Neutrality,* Directorate for Financial and enterprises affairs competition Committe, 12 de junho de 2015, p. 14 e 15. Sobre esta doutrina v. F. MANN, "Anglo-American Conflict of International Jurisdiction", *ICLQ*, vol. 13, n.º 4, outubro de 1964, p. 1463 e I. JALLES, *Extraterritorialidade* cit., p. 193 e 194.

judicial abstention doctrine[253] ou a doutina do *Act of State*[254]*,* raciocínios que conjugam elementos de cortesia internacional, equidade, proporcionalidade, reconhecimento da legislação bloqueante estrangeira e de proteção das expetativas dos agentes económicos transnacionais. Afinal, nestes casos, os seus comportamentos e práticas não serão adotados de *livre e espontânea vontade,* mas pelo contrário, ditados ou ordenados por uma pessoa coletiva pública[255].

Não obstante, este tipo de argumentário encontra variações no espaço, o que cria alguma indefinição e erraticismo na sua utilidade enquanto meio de defesa e critério de decisão judicial[256].

2.3.1.2.Reações positivas

Estas reações da entidade *ad quem*, por um lado, são mais consentâneas com a gestão necessária do pluralismo jurídico vigente e, por outro, serão o caminho mais adequado se assumirmos que a extraterritorialidade "veio para ficar"[257]. A sua caraterística principal é a abertura à cooperação internacional e a formas de relação internormativa diferenciadas, distanciando-se de atuações ou retaliações na direção contrária à extraterritorialidade, isto é, a entidade *ad quem* atua coordenada com a entidade do foro[258].

Como referi, a extraterritorialidade poderá ser uma antecâmara para a cooperação e para a harmonização normativa, seja através de modos informais ou de meios procedimentais formais que dão azo a processos de aprendizagem entre reguladores, ambos cabendo na cartilha das reações positivas[259]. Entre estas contam-se ainda os

---

[253] I. JALLES, *Extraterritorialidade* cit., p. 369 e "The applicability of the Antitrust Laws to International Cartels Involving Foreign Governments", *YLJ,* vol. 91, n.º 4, 1982, p. 785;

[254] Os atos de Estado são atos adotados por um Estado estrangeiro no âmbito dos seus poderes soberanos e dentro do seu território que, dadas as suas caraterísticas e funções, são subtraídos a qualquer sindicância de licitude por parte de um juiz estrangeiro v., desenvolvidamente, D. LOPES, *Eficácia* cit., p. 208 e ss.. Enunciando exemplos, cfr. CDI, "Report ..." cit., Anexo E, n.º 29 e ss. e M. Prata ROQUE, *A Dimensão* cit., p. 1079.

[255] E. FRIEDEL-SOUCHU, *Extraterritorialité du* cit., p. 280; H. MAIER, "Extraterritorial Jurisdiction ..." cit., p. 299; I. JALLES, *Extraterritorialidade* cit., p. 334 e 368; N. DIACAKIS, *Problèmes* cit., p. 218 e 223.

[256] E. FRIEDEL-SOUCHU, *Extraterritorialité du* cit., p. 250; D. MEAL, "Governmental compulsion as a defence under United States and European Community Antitrust Law", *CJTL,* n.º 20, 1981, p. 51 e ss.; I. JALLES, *Extraterritorialidade* cit., p. 373; J. BASEDOW, *The Law of* cit., p. 394.

[257] P. BERMAN, *Gobal Legal* cit., p. 141 e ss..

[258] M. Prata ROQUE, *A Dimensão* cit., p. 1149.

[259] Gareth DAVIES "Is Mutual Recognition an Alternative to Harmonization? Lessons on Trade and Tolerance of Diversity from the EU", Lorand BARTELS e Frederico ORTINO (eds.), *Regional Trade Agreements and WTO Legal System,* Oxford University Press, 2006, p. 272; Jacques PELKMANS, "Mutual Recognition in Goods and Services: An Economic Perspective", Fiorella SCHIOPP, (ed.), *The Principle of Mutual Recognition in the European Integration Process,* Palgrave Macmillan, 2005, p. 105; P. BERMAN, *Gobal Legal* … cit. p. 141 e ss..

processos de negociação para resolver divergências normativas, mesmo quando não exista um conflito positivo ou absoluto de pretensões. São vários os casos em que as autoridades empreendem esforços na negociação de acordos de cooperação com países terceiros, apostando em mecanismos de harmonização e de acerto, sejam acordos multilaterais ou convenções bilaterais[260]. Outra técnica correntemente utilizada com vista à redução de fricções, sobretudo nas relações com os parceiros comerciais, é a instituição de mecanismos de consulta, partilha de informação e assistência mútua a nível bilateral. Paradigmáticos destas soluções são os domínios da regulação de valores mobiliários[261] e da concorrência[262].

Depois, é possível que a entidade *ad quem* opte por decidir com base em legislação estrangeira, ora através da aplicação de regras de conflitos, ora através do seu reconhecimento e execução. É cada vez mais frequente a aplicação de normas ou a prossecução de pedidos de reconhecimento e execução de pretensões estrangeiras, articulando-se uma transição da mera coexistência para a de efetiva cooperação[263]. Importa sinalizar o instituto do reconhecimento, um relevante instrumento de relacionamento entre ordenamentos jurídicos e, em particular, o seu alargamento a novos domínios, como o direito administrativo[264]. Sem embargo do relevo desta tendência, o reconhecimento pressupõe a existência de uma comunhão jurídica, harmonização

[260] C. RYNGAERT, *Jurisdiction,* cit., p. 198; D. LOPES, "A jurisdição extraterritorial …" cit., p. 1101; I. JALLES, *Extraterritorialidade* cit., p. 119; Russel MARTHA, "Extraterritorial Taxation in International Law", K. MEESSEN, (ed.) *Extraterritorial* cit., p. 29; Spencer WALLER, "The Twilight of Comity", *CJTL,* vol. 38, 2000, p. 573.

[261] C. RYNGAERT, *Jurisdiction* cit., p. 201 e Michael MANN e William BARRY, "Developments in the Internationalization of Securities Enforcement", *Corporate Law and Practice Handbook Series,* PLI Order Number 3011, May 2004, p. 355 e 365 e ss., exemplificando com a atuação da *US Securities Exchange Commission* (SEC) que atua com base em requisitos e *standards* internacionais harmonizados em detrimento do direito interno e abdicando da exigência do "US GAAAP reconciliation".

[262] Acordo entre o Governo dos EUA e a COM sobre a aplicação do direito da concorrência, adotado no dia 23 de setembro de 1991; Acordo entre as Comunidades Europeias e o Governo dos EUA relativo aos princípios da cortesia positiva na aplicação dos respetivos direitos da concorrência, adotado no dia 29 de maio de 1988; Acordo entre o Canadá e a União Europeia relativo à aplicação dos respetivos direitos da concorrência, adotado em 17 de junho de 1999. V. C. RYNGAERT, *Jurisdiction* cit., p. 201 e, especificamente sobre os EUA, Eduardo CADETE, "Acordos de Cooperação entre a Comunidade Europeia e os Estados Unidos da América no âmbito do direito da concorrência", *ROA,* ano 69, vol. I/II, 2009, p. 297 e ss.; Susan BURNETT, "U.S. Judicial Imperialism Post '*Empagran v. f. Hoffmann-Laroche'?* Conflicts of Jurisdiction and International Comity in Extraterritorial Antitrust", *EILR,* n.º 18, 2004, p. 629 e ss..

[263] B. OXMAN, "Jurisdiction…" cit., 547; Campbell MCLACHLAN, "The influence of international law on civil jurisdiction", *HYIL,* vol. 6, 1993, p. 143; D. LOPES, *Eficácia* cit., p. 59.

[264] D. LOPES, *Eficácia* cit., p. 357 e 374; J. SAMPAIO, *O Acto* cit., p. 80 e ss.; M. Prata ROQUE, *A Dimensão* cit., p. 1199. Dando nota do incremento de "regimes de reconhecimento mútuo", v. Kalypso NICOLAIDIS e Gregory SHAFFER, "Transnational Mutual Recognition Regimes: Governance Without Global Government", *LCP,* vol. 68, 2005, p. 263 e ss..

mínima[265] ou de uma "Comunidade de Direito"[266] entre os ordenamentos jurídicos em contacto com determinada situação transnacional[267]. Nestes casos, poucos obstáculos haverá a que cada membro daquela Comunidade aplique a lei estrangeira, na medida em que a referida comunhão impediria a ocorrência de colisões sistémicas entre a solução nacional e a solução externa.

A abertura dos ordenamentos jurídicos ao direito estrangeiro, o seu reconhecimento e absorção[268] serão, por via de regra, voluntários, quando lhes antecede uma *dimensão prudencial*, um controlo da entidade de acolhimento, da entidade *ad quem,* formal e institucionalizado, sobre o mérito das políticas públicas estrangeiras. É esse controlo que garantirá o funcionamento democrático dos respetivos procedimentos de decisão internos. O direito estrangeiro atua apena como "fonte mediata", contribuindo para a formação de novas normas, por via da influência que exerce sobre uma "fonte imediata" (*v.g.* ato legislativo estadual), sem vincular, de modo autónomo, a entidade *ad quem*. A aplicação de direito estrangeiro, realizada deste modo, não beliscará o princípio da não ingerência nos assuntos internos[269].

A harmonização de domínios materiais poderá trazer, além de desvantagens, como o esbatimento de diferenças axiológicas e ideológicas, enormes vantagens, como a certeza e a segurança jurídicas, a integração dos mercados e a eliminação de obstáculos e de distorções à concorrência, a redução dos custos de transação e a facilitação das ações dos agentes económicos transnacionais, a promoção da estabilidade e da unidade na ordem jurídica internacional, e da aceitação no estrangeiro de decisões judiciais nacionais[270].

---

[265] D. LOPES, *Eficácia* cit., p. 321 e M. Prata ROQUE, *A Dimensão* cit., p. 1202.

[266] É esta a ideia subjacente às ideias de SAVIGNY, ao método conflitualista que propõe, ao qual subjaz uma ideia de paridade entre a "lei territorial" e a "lei extraterritorial", v. M. Prata ROQUE, *A Dimensão* cit., p. 116.

[267] Giandomenico MAJONE explica que o reconhecimento não é um fim em si mesmo mas um instrumento regulatório flexível, sofisticado e delicado porquanto carece de ser complementado por outros pressupostos como os da harmonização e da confiança mútua, v. "Mutual Recognition in Federal Type Systems", Anne MULLINS e Cheryl SAUNDERS (eds.), *Economic Union in Federal Systems,* The Federation Press, 1994, p. 69 e ss..

[268] Sobre as várias formas de "interação regulatória", de "difusão" e "exportação" de polítcas, v. A. YOUNG, "The European ..." cit., p.1233 e ss.; E. FAHEY, *The Global* cit., p. 11 e 91; Fabrizio GILARDI, "Transnational diffusion: Norms, ideas, and policies", Walter CARLSNAES *et alii* (eds.), *Handbook of International Relations,* SAGE Publications, 2012, p. 453 e ss.; Y. SUDA, "Transatlantic …" cit., p. 775; Miles KAHLER e David LAKE, "Economic integration and Global Governance: Why so Little Supranationalism?", Walter MATTLI e Ngarie WOODS (eds.), *Politics of Global Regulation,* Princeton University Press, 2009.

[269] M. Prata ROQUE, *A Dimensão* cit., p. 56 e 1218 e ss..

[270] Claus EHLERMANN, "Compétition entre Systèmes Reglementaires", *RMCUE,* n.º 387, abril, 1995, p. 220 e ss.; Dário MOURA VICENTE, "International Harmonization and Unification of Private Law in a Globalized Economy", Anthony D'SOUZA e Carmo D'SOUZA (eds.), *Civil Law Studies: An Indian Perspective,* Cambridge Scholars Publishing, 2009, p. 47 e ss..

Paralelamente, um fator que tem contribuído para o crescimento destas reações positivas é o desenvolvimento de mecanismos internos que criam uma convergência e que promovem a aceitação de pretensões normativas e de autoridade fora de portas, internalizando interesses estrangeiros e fomentando uma cultura de cortesia e de recíproca consideração como, por exemplo: a ponderação dos vários interesses tocados pela extraterritorialidade, procurando o legislador desenhar uma norma o mais talhada possível para suscitar a adesão pelos seus pares; a participação, consulta e cooperação de entidades públicas e privadas, à semelhança do que vem sendo praticado, a nível internacional, nas instituições e OI's; e, por fim, a partilha, desmaterialização e padronização de informação entre Estados, Administrações Públicas e Parlamentos[271].

Em geral, estas reações positivas enquadram-se numa prática emergente adotada por juízes e legisladores, de interação e de diálogo, com o fim de evitar uma utilização imprópria de doutrinas de solipsismo ou exclusivismo jurídico num contexto de pluralismo[272]. O princípio da exclusividade das ordens jurídicas[273] ou *black box theory*[274], ancorado no positivismo jurídico, não serve para acudir às necessidades do "Estado Global" [275], baseadas em constantes inter-relações e dependências entre as ordens jurídicas. Aquele princípio cada vez mais surge como uma *ficção,* útil porventura para conceptualizar noções de soberania, mas sem grande adesão à realidade. Os ordenamentos jurídicos são, nos dias de hoje, interdependentes e permeáveis entre si.

Por último, entre as reações positivas, contam-se também as dos destinatários diretos dos comandos da entidade do foro, sejam pessoas singulares ou coletivas. Com efeito, a hipótese de conformação voluntária destes com o direito estrangeiro funda-se no reconhecimento de géneros de motivação para a aceitação da vinculatividade do direito independentes do aparelho de coação e de garantia da entidade *ad quem.* Isto permite, por exemplo, afirmar que a produção de efeitos do direito com aptidão extraterritorial nem sempre requer um mecanismo formal de atribuição de relevância por parte da entidade *ad quem*[276]. Estes ajustamentos aos comandos estrangeiros, relevantes por exemplo na

[271] D. LOPES, *Eficácia* cit., p. 321 e ss..
[272] Enzo CANNIZARO e Beatrice BONAFÈ, "Beyond the archetypes of modern legal thought. Appraising old and new forms of interaction between legal orders", Miguel POAIRES MADURO *et alii* (eds.), *Transnational Law. Rethinking European Law and Legal Thinking,* 2014, p. 78 e ss..
[273] Christophe GRZEGORCZYK *et alii* (eds.), *Le positivisme juridique,* LGDJ, 1992, p. 34.
[274] Kaarlo TUORI, *Critical Legal Positivism,* Ashgate, 2002.
[275] M. Prata ROQUE, *A Dimensão* cit., p. 200 e ss.. O autor sugere que o mundo jurídico exterior ao Estado impõe-lhe uma globalização das suas funções e, nesse quadro, o princípio da territorialidade torna-se "obsoleto" e as administrações nacionais "passam a assumir-se como "*administrações globais*" (...)".
[276] D. LOPES, *Eficácia* cit., p. 227.

regulação da Internet, estarão ancorados em motivações ligadas ao interesse económico, ao bom-nome ou à confiança[277]. Por outro lado, a origem da vinculação espontânea ao direito estrangeiro poderá ser outra, designadamente certas caraterísticas político-económicas da entidade do foro.

Esta hipótese tem sido estudada sobretudo quando a entidade do foro é a UE. Além da conceção de C. DAMRO sobre o *Market Power Europe* (MPE)[278], uma tese mais recente designa por "efeito de Bruxelas"[279] o *spillover* de padrões regulatórios da UE, em vários domínios do comércio internacional, quando reunidas as seguintes condições:

(i) O poder do mercado, em especial o número de consumidores;
(ii) A intervenção regulatória nas atividades privadas com base no princípio da prevenção de riscos[280];
(iii) A preferência por regras exigentes[281] e
(iv) A não divisibilidade do regime normativo[282].

Os destinatários e, simultaneamente, os motores desta profusão normativa são as empresas transnacionais, cujos incentivos para aderir a um modelo regulatório nem

[277] U. KOHL, *Jurisdiction and* cit., p. 208.
[278] Chad DAMRO, "Market Power Europe", *JEPP,* vol. 19, n.º 5, 2012, p. 682 e ss.: "o mercado único confere existência material à UE enquanto entidade com poder de mercado que externaliza as suas políticas e medidas regulatórias relacionadas com aquele". Desenvolvendo, Abraham NEWMAN e Elliot POSNER, "International Interdependence and Regulatory Power: Authority, Mobility, and Markets", *EJIR,* vol. 17, n.º 4, 2011, p. 589 e ss.; Daniel KELEMEN E David VOGEL, "Trading Places: The Role of the United States and the European union in International Environmental Politics", *CPS,* n.º 43, 2010, p. 427 e ss.; Gregory SHAFFER e Daniel BODANSKY, "Transnationalism, Unilateralism and International Law", *TEL,* n.º 1, 2012, p. 31 e ss.; Zaki LAIDI, "European Preferences and Their Reception", Zaki LAIDI (ed.), *EU Foreign Policy in a Globalized World. Normative Power and Social Preferences,* Routledge, 2008.
[279] Anu BRADFORD, "The Brussels Effect", *NWULR*, vol. 107, n.º 1, p. 3 e ss.. e, da mesma autora, "Exporting Standards: The Externalization of the EU's Regulatory Power via Markets", *IRLE*, vol. 42, 2015, p. 168 e ss..
[280] A. BRADFORD, "The Brussels …", p. 13 e ss..
[281] A autora desenvolve a teoria de David VOGEL segundo a qual requisitos mais exigentes para certos produtos comercializados em grandes mercados podem desencadear uma dinâmica pela qual as empresas exportadoras não só cumprem a regra vigente no mercado estrangeiro (extensão regulatória *de facto*) como exercem pressão sobre os países de origem para aproximarem a respetiva legislação (extensão regulatória *de jure*), v. David VOGEL, "Trading up and governing across: transnational governance and environmental protection", *JEPP,* vol. 4, n.º 4, 1997, p. 556 e ss. e David VOGEL e Robert KAGAN (eds.), *Dynamics of Regulatory Change: How Globaliation Affects National Regulatory Policies,* University of California Press, 2004, p. 2.
[282] A indivisibilidade pode resultar de várias razões, desde uma opção do operador económico por constatar que a adesão ao regime mais exigente é mais eficiente, a razões técnicas (no caso do tratamento de dados pessoais: "quando o operador económico é incapaz de isolar as recolhas de dados pessoais oriundas da UE por razões técnicas, algumas empresas são forçadas a ajustar as suas operações globais ao modelo regulatório mais exigente que é o da UE"), entre outras razões, v. A. BRADFORD, "The Brussels ...", cit., p. 10 a 19.

sempre se resumem a um risco de sancionamento, podendo incluir, por exemplo, questões de reputação e/ou de simplificação da gestão interna[283]. Enfim, a dependência do mercado interno, dada a sua dimensão e o seu âmbito, constituem uma fonte de poder regulatório informal da UE.

Em comum, as duas conceções partem de um ângulo de análise da globalização específico: por um lado, encaram-na como um processo de transformação da engenharia do poder dos Estados terceiros à UE, de prontidão dos mesmos na sua abertura ao exterior e a formas de limitação da própria soberania e, por outro lado, como processo de criação de interdependências entre aqueles. Nesse cenário, as caraterísticas da UE permitem-lhe assumir um papel de promoção da harmonização normativa transnacional, instigando uma *race to the top* na regulação[284]. Esta perspetiva contraria as acusações de que a globalização e o comércio livre conduzem a uma *race to the bottom*, na qual os Estados reduzem as suas exigências regulatórias para atrair investimento estrangeiro e para melhorar a respetiva posição competitiva no mercado global[285].

Não obstante, não são de ignorar os efeitos *internos* desta atuação da UE em termos de concorrência: "a incapacidade de exportar os seus padrões para outros ordenamentos jurídicos coloca as empresas Europeias em desvantagem competitiva. Ao atuar como regulador global, a UE defende as suas preferências sociais sem comprometer a competitividade das suas indústrias (...). Se empresas estrangeiras aderirem a normas da UE, às indústrias europeias é garantido o mesmo nível de concorrência. Se as normas da UE se dispersarem por países terceiros, a UE pode garantir que as suas empresas orientadas para exportações não estão em desvantagem nesses mercados"[286]. Esta lógica vem plasmada em documentos da COM, salientando-se a importância de "agir com rapidez para elaborar uma norma europeia no intuito de a afirmar como norma internacional" o que alegadamente reforça "a vantagem da Europa enquanto pioneira e aumenta a competitividade da indústria europeia"[287].

---

[283] Franz-Stefan GADY, "EU/US Approaches to Data Privacy and the 'Brussels Effect': A Comparative Analysis", *GJIA,* vol. IV, 2014, p. 16.

[284] Ou seja, os padrões regulatórios são orientados por normas rigorosas e exigentes, tal constituindo uma vantagem comercial. Defendendo que a liberalização do comércio instiga esta tendência, v. A. BRADFORD, "The Brussels …" cit., p. 4 e 10; David VOGEL, *Dynamics* cit., p. 3 e ss. e F. GILARDI, "Transnational diffusion ..." cit., p. 453 e ss..

[285] Alan TONELSON, *The Race to the Bottom: Why a Worldwide Worker Surplus and Uncontrolled Free trade are Sinking American Living Standards,* Basic Books, 2ª ed., 2002, p. 14 e ss.; William CARY, "Federalism and Corporate Law: Reflections Upon Delaware", *YLJ,* n.º 83, 1974, p. 663 e ss..

[286] A. BRADFORD, "The Brussels …" cit., p. 36 a 40.

[287] Comissão Europeia, "Uma visão estratégica para a normalização europeia: reforçar e acelerar o crescimento sustentável da economia europeia até 2020", 1 de junho de 2011.

Enfim, tanto o MPE como o "efeito de Bruxelas" descrevem a UE como um "regulador global"[288] unilateral[289], "transnacional"[290] ou "regulador predominante do comércio global"[291] por força da sua dimensão económica e integração nos mercados mundiais, dois importantes fatores na origem da exportação do DUE e das suas políticas internas, para outros mercados e ordenamentos jurídicos, numa panóplia de domínios como a regulação da Internet[292], direito dos refugiados[293], direito do ambiente[294], entre outros[295].

2.3.2. Um sistema de concorrência de jurisdições

Com exclusão da categoria da jurisdição de execução, os imprecisos limites à jurisdição extraterritorial favorecem a vigência de um sistema que potencia o surgimento de conflitos de jurisdição e promove a respetiva concorrência[296]. Será assim, por exemplo, nos casos de choque de várias aplicações do princípio da territorialidade sempre que a atividade tenha lugar em mais do que um território[297]. Os casos em que as reações são positivas não colocam grandes dificuldades e, para alguns autores, essa será a regra[298].

---

[288] Alasdair YOUNG, "The European Union as a global regulator? Context and comparison", *JEPP*, vol. 22, n.º 9, 2015, p. 1233 e ss..

[289] Daniel KELEMEN, "Globalizing European Union Environmental policy", *JEPP,* vol. 17, n.º 3, 2010, p. 335 e ss..

[290] Dominique SINOPOLI e Kai PURNHAGEN, "Reversed Harmonization or Horizontalization of EU Standards? Does WTO Law Facilitate or Constrain the Brussels Effect?", *WILJ,* vol 34, n.º 1, p. 101 e ss..

[291] Elliot POSNER, "Making Rules for Global Finance: Transatlantic Regulatory Cooperation at the Turn of the Millennium", *IO*, vol. 63, n.º 4, 2009, p. 692 e Wade JACOBY e Sophie MEUNIER, "Europe and the Management of Globalization", *JEPP,* vol. 17, n.º 3, 2010, p. 306.

[292] Christopher KUNER, "The Internet and the Global Reach of EU Law", LSE Legal Studies Working Papers, n.º 4, 2017, p. 2 e ss..

[293] Helen LAMBERT *et alii* (eds.), *The Global Reach of European Refugee Law,* Cambridge University Press, 2013.

[294] Elaine FAHEY e Ester HERLIN-KARNELL, "Special Issue: EU law qua global governance law? Deciphering regulatory and constitutional competence between EU environmental law and global governance", *GLJ,* n.º 13, 2012, p. 1147; Geert DE BAERE e Cedric RYNGAERT, "The ECJ's Judgement in Air Transport Association of America and the International Legal Context of the EU's Climate Change Policy", *EFAR,* n.º 18, 2013, p. 389; Joanne SCOTT e Lavanya RAJAMANI, "EU Climate Change Unilateralism", *EJIL,* n.º 23, 2012, p. 469; Katharina HOLZINGER e Thomas SOMMERER, "European Environmental Policy. Greening the world?", Gerda FALKNER e Patrick MULLER (ed.), *EU Policies in a Global Perspective. Shaping or taking international regime?* Routledge, 2014, p. 111 e ss..

[295] Katja BIEDENKOPF, "Hazardous substances in electronics: the effects of European Union risk regulation on China", *EJRR,* n.º 4, 2012, p. 477 e ss..

[296] C. RYNGAERT, *Jurisdiction* cit., p. 7 e autores referidos na nota de rodapé 25.

[297] D. LOPES, *Eficácia* cit., p. 49.

[298] É o caso de M. HENZELIN (*Le Principe* cit., p. 164) e R. JENNINGS e A. WATTS (*Oppenheim's* cit., p. 220: "só num reduzido número de casos é que a sobreposição de jurisdições causa problemas graves, em regra quando os Estados atribuem muita importância às suas pretensões extraterritoriais, e mais frequentemente em casos criminais. Em geral, a coexistência de jurisdições é aceite e a tolerância dos Estados contribui para evitar os conflitos de jurisdição").

Mas e diante de uma reação negativa ou de um conflito positivo de jurisdições? Que critério orienta o decisor?

Na prática, a solução do conflito caberá aos tribunais internacionais, como sucedeu no caso *Lotus*, ou nacionais, aos quais já coube controlar o conceito de jurisdição conforme com o DIP, designadamente nos domínios do direito da concorrência e do ambiente[299]. A doutrina[300] tem proposto metodologias e teorizações para a resolução destes conflitos que, para efeitos de sistematização, divido em dois grupos: as teses *abstencionistas* (não propõem nenhum critério ou procedimento útil para a resolução de conflitos de jurisdição) e as teses *intervencionistas* (que, pelo contrário, propõem). No primeiro grupo, a conceção *unilateralista* recusa qualquer ajuste de interesses entre as pretensões em concurso, advogando uma aplicação extraterritorial *cega* das prescrições nacionais, sem preocupações de coordenação internacional[301]. Noutro sentido, o *territorialismo* tem como expoente máximo uma presunção contra a extraterritorialidade aplicada nas situações nas quais as normas nada dizem a respeito do seu âmbito de aplicação[302]. Estas teorias não são aqui acolhidas pois não são consentâneas com os factos internacionais e com a prática estadual: o unilateralismo é profundamente avesso a considerações de *comity* e não fornece qualquer orientação útil para a solução ou prevenção destes conflitos; já o territorialismo não se coaduna com a evolução, refletida na prática das entidades do foro, dos princípios de jurisdição extraterritorial[303].

No segundo grupo, das teses intervencionistas, inclui-se, desde logo, uma solução de "cortesia", ancorada em larga medida na *comity*, a ser aplicada preventivamente pelo legislador, quando pretende atribuir caráter extraterritorial a uma norma, ou *a posteriori* pelo tribunal nacional, quando se depara com um conflito. A par desta, destacam-se ainda

[299] No caso do TJ, com particular relevo, a propósito do regime de comércio de licenças de emissão de gases com efeitos de estufa no setor da aviação e da interpretação do princípio da territorialidade, v. Acórdão do TJ, Air Transport Association of America *et alii* c. Secretary of State for Energy and Climate Change*,* C-366/10, 21 de dezembro de 2011.

[300] Destaca-se a completíssima sistematização de D. LOPES, *Eficácia* cit., p. 49 e ss..

[301] Jeffrey MEYER, "Dual Illegality and Geoambiguous Law: A New Rule for Extraterritorial Application of U.S. Law", *MLR,* vol. 95, 2010, p. 114 e ss..

[302] Uma presunção que, de resto, nem tem sido aplicada de maneira uniforme nos EUA, v. John KNOX, "The Unpredictable Presumption Against Extraterritoriality", *SLR,* vol. 40, 2011, p. 635 e ss..

[303] Enzo CANIZZARRO, "The EU's Human Rights Obligations in Relation to Policies With Extraterritorial Effects: A Reply to Lorend Bartels", *EJIL,* vol. 25, n.º 4, 2015, p. 1093 e ss..

as hipóteses conflitualista[304], processualista[305], convencional e híbrida. Estas duas últimas teses são as que mais adeptos recolhem.

A primeira, deposita todas as expetativas nos princípios da jurisdição extraterritorial, como critérios de delimitação das esferas de jurisdição, e na sua possível hierarquização firmada numa solução convencional, multilateral, prevendo um acordo sobre os termos precisos da mesma, as finalidades e condições do seu exercício. Esta é a sugestão de certa doutrina[306], que foi também advogada no caso *Lotus:* "É necessário para resolver as dificuldades criadas pela existência de várias regras [de jurisdição] formuladas nos últimos anos, tanto na Europa como na América, preparar convenções para limitar a discricionariedade dos Estados tolerada pelo direito internacional" [307]. Ao longo do tempo, algumas convenções setoriais[308] foram adotadas, mas uma solução convencional geral é, pelo menos por agora, irrealista[309].

A tese híbrida, sufragada por uma parte da doutrina[310] e por algumas instituições internacionais[311], é a que mais se ajusta à atual realidade internacional, propondo um compromisso da entidade do foro repartido em várias frentes:

---

[304] Sugere uma importação do método conflitualista de direito internacional privado. Em sua defesa, v. Donald TRAUTMAN, "The Role of Conflicts Thinking in Defining the International Reach of American Regulatory Legislation", *OSLJ*, vol. 22, n.º 3, 1961, p. 619; Lea BRILMAYER, "Extraterritorial Application of American Law: A Methodological and Constitutional Appraisal", *LCP*, vol. 50, n.º 3, summer, 1987, p. 11 e ss.; P. TORREMANS, "Extraterritorial …" cit., p. 293; William DODGE, "The Public-Private Distinction in the Conflict of Laws", *DJCIL,* vol. 18, 2008, p. 385. Entre nós, L. LIMA PINHEIRO, I. JALLES e D. LOPES são críticos desta hipótese por duas razões: distinguem os princípios de DIP que regulam a jurisdição da entidade do foro das normas de conflito com base no tipo de incidência de cada um; os destinatários dos primeiros são os Estados ou a UE e dos segundo os sujeitos de relações transnacionais. V. D. LOPES, "A jurisdição extraterritorial ..." cit., p. 1096; I. JALLES, *Extraterritorialidade* cit., p. 397 e L. LIMA PINHEIRO, *Direito Internacional,* cit., p. 382.

[305] Esta tese é atribuída a P. PICONE para quem as regras substantivas para delimitar a jurisdição dos Estados não fornecem critérios para prevenir os conflitos de jurisdição, apontando para uma via exclusivamente processual, através da qual os conflitos de jurisdição seriam resolvidos por recurso a meios de resolução de litígios pacíficos, v. Paolo PICONE, "Introduzione – Parte IX Tutela della Concorrenza", P. PICONE *et alii* (eds.), *Diritto internazionale dell'economia: raccolta sistemática dei principal atti normativi internazionali ed interni com testi introduttivi e note,* Franco Angeli, 1982, p. 865 e ss.. Qualquer mecanismo processual não é auto-suficiente e carece, sempre, de uma "dimensão principiológica" que guie o processo e a solução a encontrar na contenda. Este é o principal reparo apontado ao "processualismo", v. D. LOPES, "A jurisdição extraterritorial …" cit., p. 1096 e Vaughan LOWE, "Ends and Means in the Settlement of International Disputes over Jurisdiction", *RIS*, vol. 11, n.º 3, Julho, 1985, p. 183.

[306] G. DAVIES, "International Trade …" cit., p. 1213.

[307] Acórdão do TPJI, França c. Turquia, 7 de setembro de 1927, p. 19.

[308] Como no domínio fiscal, v. Russel MARTHA, *The Jurisdiction to Tax in International Law: Theory and Practice,* cit., p. 3 e C. RYNGAERT, *Jurisdiction* cit., p. 146.

[309] C. RYNGAERT, *Jurisdiction* cit., p. 145.

[310] *Idem*, p. 198; D. LOPES, "A jurisdição extraterritorial …" cit., p. 1096; Herbert KRONKE, "Capital markets and Conflict of Laws", *RCADI,* vol. 286, 2000, p. 245 e 380; P. DEMARET, "L'Extraterritorialité ..." cit., p. 36.

[311] A proposta da CDI prevê alguns elementos desta teoria, bem como a hipótese sugerida pela Câmara do Comércio Internacional, *The Extraterritorial Application of National Laws – The International Chamber of Commerce*, ICC Publishing S. A., 1987, p. 44 e ss., ou pela International Bar Association, v. *Report of*

(i) Ao nível legislativo, desenvolvendo critérios para o reconhecimento de atuações estrangeiras;

(ii) Ao nível diplomático, assumindo uma postura de prevenção de conflitos, seja apostando numa estratégia de cooperação internacional no sentido de harmonizar os domínios materiais em causa[312], seja na aplicação prática e espontânea de deveres processuais internacionais (como o dever de comunicação), seja na procura de consensos no campo dos critérios para a determinação da jurisdição extraterritorial[313];

(iii) Por seu turno, ao nível judicial, sugere-se um dever de assegurar um equilíbrio entre os ordenamentos jurídicos em conflito usando para tal um método de ponderação de interesses[314].

2.3.3. As "duas velocidades" da extraterritorialidade

Mesmo quando inexiste um conflito de jurisdição, perfila-se um outro problema por resolver na perspetiva da entidade do foro: como garantir o cumprimento de prescrições extraterritoriais no estrangeiro? [315]

A execução extraterritorial de prescrições pela entidade do foro, sem o consentimento da entidade *ad quem*, permanece vedada, muito embora o exercício da extraterritorialidade prescritiva continue a aumentar[316]. Portanto, não é de admirar que o problema central da aplicação extraterritorial do direito interno se reporte, quase em exclusivo, ao problema do "défice de capacidade de execução"[317].

---

the Task Force on Extraterritorial Jurisdiction, 2008, disponível em https://www.ibanet.org/Article/NewDetail.aspx?ArticleUid=597D4FCC-2589-499F-9D9B-0E392D045CD1, consultado no 30 de setembro de 2018.

[312] A. MESTRAL, "The Extraterritorial …" cit., p. 49; D. LOPES, *Eficácia* cit., p. 56; Giuliano AMATO, *Antitrust and the Bounds of Power – The Dilemma of Liberal Democracy in the History of the Market,* Hart Publishing, 1997, p. 129 e ss..

[313] G. DAVIES, "International Trade …" cit., p. 1213 e ss..

[314] Esta é sugestão de J. BASEDOW, "Souveraineté ..." cit., p. 153. Veja-se ainda a proposta de P. DEMARET, "L'Extraterritorialité ..." cit., p. 36, situando a extraterritorialidade entre a diplomacia e o direito, apostando na harmonização de leis económicas e na aplicação do direito com diplomacia.

[315] F. MANN, "The Doctrine …" cit., p. 111.

[316] D. LOPES, *Eficácia* cit., p. 57 e M. KAMMINGA, "Extraterritoriality" cit., p. 1076.

[317] A. COLANGELO, "What is ..." cit., p. 1311 e ss.; B. STERN, "L'extra-territorialité ..." cit., p. 247; D. LOPES, *Eficácia* cit., p. 33; Noel COX, "The extraterritorial enforcement of consumer legislation and the challenge of the internet", *EDL,* n.º 8, 2004, p. 60 e ss..

Por exemplo, no caso dos "perigos externos com projeção interna", designadamente na Internet, estamos diante de situações da vida marcadas pela "internacionalidade" e, com frequência, provocadas por agentes que escapam ao controlo da entidade do foro. Dir-se-á que a jurisdição extraterritorial prescritiva não é um instrumento *eficaz*, sobretudo por via da incapacidade da entidade do foro, isoladamente, executar as prescrições sem a cooperação da entidade *ad quem* donde brota a fonte do risco. Se a *execução coerciva* de normas permanece eminentemente territorial, de que vale à entidade do foro regular atuações de agentes estrangeiros cuja presença no seu território é meramente virtual, por exemplo através das suas atividades no ciberespaço dirigidas aos seus nacionais[318]?

Tal sugere a incipiente natureza da extraterritorialidade prescritiva por se esfumar a nota de coercividade dos comandos estatais e se acentuar a suposta (im)possibilidade de concretização da aplicação de sanções no caso de incumprimento. Daí que se diga que nem todas as tentativas de regulação extraterritorial recebem o acolhimento que procuram[319]. Nesse sentido, há quem proponha que as entidades do foro devem domesticar os seus "comportamentos jurisdicionais", que deverão ser idênticos dentro e fora dos respetivos territórios, assim garantindo que apenas prescrevem normas extraterritoriais que podem ser executadas fora de portas[320]. Mas quais são essas normas que podem ser executadas fora de portas? E mesmo que não o possam ser, será legítimo que a entidade do foro não deva acalentar expetativas quanto à efetividade de normas com vocação extraterritorial? E – se é que os há –, quais são os mecanismos que permitem compensar o "défice de capacidade de execução" da entidade do foro?

---

[318] C. REED, *Making Laws* cit., p. 29 e ss.; H. BUXBAUM, "Territory, territoriality ..." cit., p. 673.

[319] Há várias formas de conceber o problema que subjaz a esta afirmação. D. LOPES refere que o "âmbito de aplicação espacial (de definição do facto que espoleta a aplicação da norma) e o âmbito de eficácia espacial das normas e atos estrangeiros (da sua efetiva projeção para o exterior) podem não coincidir. A autora recorda a este propósito os ensinamentos de J. BAPTISTA MACHADO sobre o "âmbito de eficácia das leis" que respeita ao "domínio possível de aplicabilidade da lei (enquanto *regula agendi*), concebe o entrecruzamento de várias leis que também tenham uma conexão relevante com os factos; sendo dentro dessa área de cruzamento que se delineia o *âmbito de competência das leis* ou "âmbito de eficácia ponderada, qualificada ou especializada", decorrente já, na perspetiva jus-privatista, da intervenção de regras de natureza conflitual". A. XAVIER distingue entre "âmbito de incidência" ou *jurisdiction to prescribe* para se reportar ao âmbito de validade ou de competência por oposição ao "âmbito de eficácia" ou *jurisdiction to enforce* para determinar se uma norma é suscetível de ser aplicada coercivamente em território estrangeiro, incluindo neste campo o instituto do reconhecimento. Cfr. Alberto XAVIER, *Direito Tributário Internacional,* 2ª edição, Almedina, 2009, p. 6 e ss. e D. LOPES, *Eficácia* cit., p. 319 e 320.

[320] Mark GIBNEY, "The Extraterritorial Application of US Law: The Perversion of Democratic Governance, the Reversal of Institutional Roles, and the Imperative of Establishing Normative Principles", *BCICLR,* vol. 19, n.º 2, 1996, p. 320 e ss..

No limite, este é um velho problema de qualquer ramo do Direito: as dificuldades de implementação coerciva de uma norma ou princípio que, em regra, não obstam à sua vigência. A maioria da doutrina nota que a ausência de coercibilidade plena não prejudica a validade e imperatividade do Direito, visto que a noção de monopólio coercivo apenas exige a potencialidade de exercício da força[321]. Em todo o caso, as expectativas sobre a efetividade das normas emanadas com vocação extraterritorial deverão ser calibradas, desde logo, pelo princípio da intransitividade, isto é, pela sua ligação com a situação a regular e pela motivação gizada. Por outro lado, como expliquei, o exercício de jurisdição extraterritorial poderá não pretender ser plenamente eficaz, mas apenas influenciar comportamentos e atuações, tanto da comunidade internacional como dos sujeitos passivos, designadamente das entidades *ad quem* e das empresas transnacionais. Em especial, a adesão destas empresas a um determinado padrão regulatório e às decisões de autoridades da entidade do foro nem sempre se pautará pelo risco da sua coercibilidade.

Acresce que, casos haverá nos quais a garantia do cumprimento da norma com vocação extraterritorial depende da reação da entidade *ad quem* e do espírito de colaboração internacional. Equacionando uma reação *positiva* tendo a concordar com quem contesta a ligação absoluta entre territorialidade e coercividade, por ser possível que a entidade *ad quem* consinta ou disponibilize o seu aparelho coercivo ao serviço da entidade do foro[322]. Naturalmente, este tipo de soluções pressupõe um espírito de colaboração internacional, uma proximidade normativa e de políticas públicas, a já referida "Comunidade de Direito". Em alguns casos esta harmonia tem estado presente, sobretudo "num ambiente pluralista"[323], mas nem sempre será esse o caso, designadamente quando a reação da entidade *ad quem* for negativa ou, simplesmente, não exista um espírito colaborativo.

Finalmente, importa enfatizar que cabe no âmbito da jurisdição *territorial* a adoção de medidas internas com impacto *extraterritorial* quando a entidade do foro goza de uma capacidade de controlo, direto ou indireto, sobre o destinatário estrangeiro. Pode acontecer que, independentemente da reação da entidade *ad quem* e sem invadir o domínio territorial alheio, a entidade do foro seja capaz de executar as suas pretensões com vocação extraterritorial, associando ao seu não acatamento certas sanções aos

[321] M. Prata ROQUE, *A Dimensão* cit., p. 447.
[322] J. SAMPAIO, *O Acto* cit., p. 22.
[323] B. OXMAN, "Jurisdiction ..." cit., p. 547; C. MCLACHLAN, "The Influence of …" cit., p. 143; D. LOPES, *Eficácia* cit., p. 59 e 339.

destinatários daquelas, com atividade no seu território e integrados no respetivo mercado e tecido económico. Estas sanções, que têm por finalidade não uma coação material, mas uma *deterrence*, serão territorialmente adotadas e aplicadas[324]. A doutrina apresenta casos em que decisões meramente internas, territorialmente adotadas, podem ser suficientes para surtir efeitos e moldar o comportamento dos atores no ciberespaço que, decididos a gerir o risco nos seus negócios moldam os seus conteúdos, atividades e serviços, às jurisdições "problemáticas"[325].

O que se pretende evidenciar é que a execução de normas extraterritoriais nem sempre pressupõe a adoção de medidas coercivas materialmente praticadas *pela* e *na* entidade *ad quem,* podendo ser promovida mediante a maximização de poderes coercivos territoriais da entidade do foro. Este é o argumento central da chamada "estratégia de execução unilateral", invocada no domínio do ciberespaço, e aprofundada na Parte III.

[324] I. JALLES, *Extraterritorialidade* cit., p. 240.
[325] C. REED, *Making Laws* cit., p. 35 e T. SCHULTZ "Carving Up ..." cit., p. 799. O primeiro apresenta como exemplo as alterações comportamentais de prestadores de conteúdos *online* norte-americanos movidas por legislação de difamação do Reino Unido.

Síntese conclusiva

1. De entre as várias definições enunciadas de extraterritorialidade, aquela que se afigura como uma espécie de síntese das demais, com autoridade e amplitude suficientes para este trabalho, é a definição da CDI. Sem desconsiderar as necessárias atualizações da mesma em consonância com os dados da atualidade internacional, foi aquela definição o meu ponto de partida para responder às três perguntas que orientaram esta primeira Parte:

   1.1. O *que é* a extraterritorialidade? Trata-se de uma tentativa de regular, através de atos legislativos, judiciais ou executivos, a conduta de pessoas, bens ou atos, além das suas fronteiras, que afetam certos interesses na ausência de regulação pelo DIP;

   1.2. *Quem* são os seus titulares? Distingui os sujeitos ativos – que designei de entidades do foro para englobar tanto entes estaduais como não estaduais como a UE – dos sujeitos passivos, por seu turno desdobrados em entidades *ad quem* e destinatários diretos;

   1.3. C*omo* se manifesta? Através de atos legislativos, judiciais ou executivos, correspondentes às diferentes categorias de jurisdição extraterritorial: prescritiva, adjudicativa e de execução.

2. A análise da prática da extraterritorialidade parte da premissa de que esta não é um instrumento neutro[326]. Tal significa que os interesses que a mobilizam podem ser interesses *internos*, proteção de posições individuais (*v.g,* consumidores, titulares de bens jusfundamentais) ou de realidades sociais (*v.g,* concorrência ou economia interna), ou *externos*, ligados à comunidade internacional e à proteção de valores "cosmopolitas". Como refere F. LOUREIRO BASTOS, "as virtualidades da extraterritorialidade enquanto instrumento jurídico decorrem da possibilidade de influenciar ou impor comportamentos a determinados sujeitos jurídicos, qualquer que seja o espaço onde estes se encontrem" [327]. Ora, com o aumento exponencial de

[326] F. Loureiro BASTOS, "Algumas notas ..." cit., p. 442.
[327] *Idem*, p. 453.

situações de relevância internacional que carecem de uma intervenção do poder público, estadual ou supraestadual (no caso da UE), para mitigar falhas normativas que interferem com o desempenho das suas funções[328], diante do marasmo dos foros de discussão internacionais, movidas pelo imperativo de proteger os indivíduos, as entidades do foro projetam a respetiva jurisdição além-fronteiras originando uma redução do "direito interno internacionalmente indiferente"[329]. Tanto não significa que, nas modalidades de atuação externa daquelas, a jurisdição extraterritorial seja a regra[330] – torna-se, isso sim, cada vez mais frequente[331].

3. Não são claros os *limites* do direito internacional público ao exercício de jurisdição extraterritorial, com a exceção da execução de normas e decisões. Com efeito, mesmo quanto ao exercício da jurisdição extraterritorial prescritiva e adjudicativa, a regra de que o mesmo se fundamenta num princípio de jurisdição (territorialidade objetiva, doutrina dos efeitos, personalidade passiva, entre outros) é quebrada quando a entidade do foro invoca a universalidade da sua jurisdição em relação a certos crimes.

4. Os *efeitos* do exercício de jurisdição extraterritorial são os seguintes:

   4.1. As reações mais comuns dos sujeitos passivos, que tanto podem ser negativas ou contestatárias, como positivas e sincronizadas com as pretensões da entidade do foro;

   4.2. As situações de concorrência de jurisdição ou de conflitos, cuja solução será sempre casuística dada a ausência de um consenso global sobre os termos exatos da jurisdição da entidade do foro;

[328] Em sentido próximo, vejam-se as considerações de Joseph STIGLITZ, *Globalisation and its Discontents,* Norton, 2002, p. 214 e ss., considerando que a globalização deve ser acompanhada de opções políticas adequadas, não se cingindo a um fundamentalismo de mercado, tendo os Estados um papel na mitigação das falhas de mercado e na promoção da justiça social, mas devendo, ao mesmo passo, ser promovida uma adequada ação coletiva global.
[329] Heinrich TRIEPEL, "Les Rapports entre le Droit Interne et le Droit International", *RCADI,* Tomo I, 1923, p. 106
[330] Constatando a inexistência de indícios suficientes nesse sentido, v. A. MESTRAL, "The Extraterritorial ..." cit., p. 44.
[331] D. LOPES, *Eficácia* cit., p. 38.

4.3. As duas velocidades da extraterritorialidade que resultam do crescimento exponencial da sua categoria prescritiva sem correspondente na categoria da execução. A execução de normas e decisões será sempre territorial, é verdade, mas o que se poderá discutir é a maximização territorial dos poderes coercivos, como desenvolvo na Parte III.

Parte II – As manifestações de extraterritorialidade do regime geral de proteção de dados pessoais da UE

Nesta segunda Parte da tese identifico, analiso e sistematizo as manifestações de extraterritorialidade do regime geral de proteção de dados pessoais da UE, isto é, como se traduzem as tentativas de regular a conduta de pessoas, bens ou atos, além das fronteiras da UE neste regime? Esta questão circunscreve desde logo a análise a um regime em concreto que, por isso, importa delimitar. As implicações desta opção respeitam, desde logo, as categorias de jurisdição da UE aqui tratadas: é que a suportar este regime estão, sobretudo, atos legislativos, a Diretiva e o RGPD, e decisões judiciais do TJ e das autoridades de controlo, pelo que o estudo que proponho incide, sobretudo, sobre a jurisdição prescritiva e adjudicativa. Não quer isto dizer que, em especial quanto aos limites da extraterritorialidade, a jurisdição de execução não seja relevante – sê-lo-á sobretudo na Parte III.

Isto dito, importa agora explicar os contornos do regime geral de proteção de dados pessoais a que me refiro. É esse o objetivo do Capítulo 1, começando pela sua delimitação e enunciação das respetivas fontes (1.1.), explicando a evolução e as dimensões do processo de "europeização" da proteção de dados pessoais (1.2.), apresentando aa complexa natureza deste regime (1.3) e enunciando as suas caraterísticas distintivas (1.3.)

Sigo, nos Capítulos 2 e 3, para as manifestações de extraterritorialidade propriamente ditas. No primeiro analiso o âmbito de aplicação do regime em apreço traçado pelo art. 4.º da Diretiva e pelo art. 3.º do RGPD, destacando a natureza e estrutura destas disposições (2.1). Interessa-me comparar aqueles artigos e, em especial, os critérios usados para traçar o âmbito de aplicação deste regime (2.2. e 2.3). Com efeito, são esses critérios que lhe conferem vocação extraterritorial e que alargam o seu âmbito de aplicação à conduta de pessoas além das fronteiras da UE. No último ponto deste Capítulo caraterizo esta manifestação de extraterritorialidade, em especial os interesses que prossegue e os princípios em que se fundamenta (2.3.).

Tanto a Diretiva como o RGPD regulam as transferências de dados pessoais para países terceiros, respetivamente, nos Capítulos 4 e 5. Será que as implicações destes

Capítulos se estendem para lá do território da UE? Será que os mesmos visam "regular (...) a conduta de pessoas, bens ou atos além das fronteiras" daquela? Procuro responder a estas questões no Capítulo 3.

Começo, tal como no Capítulo anterior, com a comparação das normas dos dois diplomas e, em especial, dando maior relevo às novidades do RGPD (3.1.). Com base neste exercício, identifico e caraterizo a hipotética vocação extraterritorial das regras aplicáveis às transferencias para países terceiros, sublinhando os interesses prosseguidos pelas mesmas, bem como as particularidades desta manifestação de extraterritorialidade (3.2.).

Capítulo 1 – O regime geral de proteção de dados pessoais da UE

1.1.Delimitação e fontes

O regime geral de proteção de dados pessoais corresponde ao conjunto de normas, aplicáveis aos tratamentos de dados pessoais previsto no RGPD e, anteriormente, na Diretiva. Em extrema síntese, e sem prejuízo de desenvolver mais adiante alguns destes conceitos, uma vez apurado que certo tratamento de dados pessoais cabe no âmbito daqueles diplomas, sobre os "utilizadores de dados pessoais"[332], seja o "responsável pelo tratamento" ("RT") ou "subcontratante" ("ST"), incide um conjunto de obrigações. Como vou explicar, este regime é *geral* por se distinguir do bloco normativo aplicável aos tratamentos de dados pessoais realizados em determinados setores, como é o caso da Diretiva *e-Privacy*[333].

No plano externo, o regime em apreço recolheu influências de instrumentos internacionais que o antecedem, como a Convenção n.º 108 do CdE e as Diretrizes da OCDE[334], ambos adotados na década de 80 e recentemente revistos[335]. Na génese destas

[332] AEDF, CdE, SEPD, *Handbook on European data protection law,* 2018, p. 101.
[333] Diretiva 2002/58/CE do PE 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.
[334] OCDE, *Guidelines on the protection of Privacy and Transborder Flows of Personal Data*, de 29 de setembro de 1080, disponíveis em http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm, consultado no dia 30 de setembro de 2018.
[335] O Protocolo para alterar a Convenção n.º 108 do CdE, para a proteção dos indivíduos em relação ao tratamento de dados pessoais automatizado, de 28 de janeiro de 1981, foi adotado no dia 18 de maio de 2018, tal como o respetivo relatório explicativo, ambos acessíveis em https://www.coe.int/en/web/data-protection/convention108/modernisation, consultado no 30 de setembro de 2018. Por seu turno, a reforma das Diretrizes da OCDE terminou em 2013 e o texto final encontra-se disponível em http://www.oecd.org/sti/ieconomy/privacy.htm, consultado no 30 de setembro de 2018.

fontes externas encontramos uma série de catalisadores, designadamente a necessidade de prevenir os riscos para os direitos fundamentais provocados pelos novos tratamentos de dados pessoais fruto do desenvolvimento tecnológico[336].

Sem prejuízo de, quando oportuno, mencionar estas influências externas, centrar-me-ei na evolução das fontes internas deste regime, resultantes de uma competência atribuída à UE pelos Estados-Membros, com particular incidência sobre o RGPD e as novidades do mesmo. Mas no plano interno, além do direito derivado, designadamente da Diretiva e do RGPD, a proteção de dados pessoais ocupa, desde o TL, uma posição no direito originário, tanto na CDFUE como no TFUE, que se tem manifestado sobretudo na jurisprudência do TJ. A esta evolução corresponde o processo de "europeização" descrito no ponto seguinte.

1.2.A "europeização" da proteção de dados pessoais: evolução e dimensões

O fenómeno da "europeização" de certas matérias corresponde ao papel principal do DUE enquanto fonte do direito aplicável e desdobra-se, essencialmente, em dois vetores: (i) a sua influência na homogeneização dos regimes jurídicos aplicáveis nos Estados-Membros e (ii) a estruturação de um *sistema administrativo europeu* que conjuga degraus ou níveis de administração[337]. O regime em análise reúne estes dois elementos sendo que começarei pelo primeiro[338].

Enquanto "política pública" ou, melhor, competência atribuída à UE, entre 1995 e a atualidade a matéria da proteção de dados pessoais sofreu uma evolução bem patente no direito derivado e no direito originário. É um percurso pontuado pelos avanços genéticos da UE e pela dinâmica própria da sua vivência, destacando-se a harmonização de

---

[336] Alexandre Sousa PINHEIRO, *Privacy e proteção de dados pessoais: a construção dogmática do direito à identidade informacional,* policopiado, 2015; Gloria FUSTER, *The Emergence of Personal Data Protection as a Fundamental Right of the EU,* Springer, 2014, p. 75 e ss.; Hielke HIJMANS, *The European Union as a Constitutional guardian of internet privacy and data protection. The Story of Art. 16.º TFUE,* Springer, 2017, p. 54 e ss.; Lee BYGRAVE, *Data Protection Law. Approaching Its Rationale, Logic and Limits,* Wolters Kluwer, 2003, p. 93 e ss..

[337] Alexandre Dias PEREIRA, *Direitos de Autor e Liberdade de Informação,* Almedina, 2008, p. 344 e ss.; Maria Eduarda GONÇALVES, *Direito da Informação – Novos Direitos e Formas de Regulação na Sociedade da Informação,* 2ª ed., Almedina, 2003, p. 30; Paulo OTERO, *Legalidade e Administração Pública – O sentido da vinculação administrativa à juridicidade,* Almedina, 2003, p. 231 e ss.; Pedro GONÇALVES, "Direito Administrativo da Regulação", *Regulação, Electricidade e Telecomunicações,* Coimbra Editora, 2008, p. 31; Yves POULLET, "Vers la confiance: vues de Bruxelles: um droit européen de l'Internet? Quelques considérations sur la spécificité de l'approche réglementaire européene du cyberspace", Georges CHATILLON, (org.), *Le droit international de l'Internet,* 2002, p. 133 e ss..

[338] O sistema administrativo europeu é tratado no ponto sobre a supervisão onde refiro o "Comité Europeu para a Proteção de dados pessoais" ("CEPD").

divergências nacionais entre Estados-Membros, o florescimento de uma economia de mercado e a consciencialização da necessidade de conferir maior centralidade aos direitos fundamentais no seio da União. É assim que, aos olhos da COM, este regime consagra "duas das mais antigas e igualmente importantes ambições do processo de integração europeia": a proteção dos direitos fundamentais e a realização do mercado interno, em especial a livre circulação de dados pessoais[339]. Desta afirmação retiro as duas *dimensões* deste bloco normativo: uma jusfundamental e outra económica ou "integracionista", correspondentes aos objetivos enunciados no art. 1.º do RGPD e da Diretiva[340]. Aliás, considerou-se que a Diretiva "propõe (...) um modelo de equilíbrio entre a lógica de mercado e as preocupações com a cidadania"[341].

1.2.1. A dimensão económica ou "integracionista"

A década de 70 foi marcada pelo surgimento das primeiras legislações nacionais de proteção de dados pessoais[342]. Tal fez soar o alerta, junto da COM, de que os Estados-Membros estavam na eminência de adotar soluções divergentes[343]. A toada fez eco no PE que, entre 1975 e 1982, apresentou quatro resoluções nas quais antecipava o surgimento de legislação conflituante e os efeitos negativos no desenvolvimento de um mercado comum e apelava à criação de um mercado comum de proteção de dados pessoais de modo a garantir a livre circulação de informação na UE, invocando, para fundamentar a

[339] Comissão Europeia, "Uma abordagem global da proteção de dados pessoais na União Europeia", 4 de novembro de 2010, p. 2.
[340] O art. 1.º, n.º 1, da Diretiva dispunha que "Os Estados-membros assegurarão, em conformidade com a presente directiva, a proteção das liberdades e dos direitos fundamentais das pessoas singulares, nomeadamente do direito à vida privada, no que diz respeito ao tratamento de dados pessoais." (dimensão jusfundamental). Por seu turno, o número 2, referia que "os Estados-membros não podem restringir ou proibir a livre circulação de dados pessoais entre Estados-membros por razões relativas á proteção assegurada por força do n.º 1" (dimensão integracionista). Já o art. 1.º, n.º 2, do RGPD enuncia que "O presente regulamento defende os direitos e as liberdades fundamentais das pessoas singulares, nomeadamente o seu direito à proteção dos dados pessoais" (dimensão jusfundmanental). Por seu turno, o número 3, refere que "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" (dimensão integracionista).
[341] Jean FRAYSSINET, "L'Union Européenne et la protection des données personnelles circulent sur l'Internet", Annie BLANDIN-OBERNESSE, (dir.), *L'Union Européenne et Internet,* Éditions Apogée, 2001, p. 125.
[342] Em 1970 no Estado Alemão de Hesse, em 1973 na Suécia, em 1977 e 78, respetivamente, na Alemanha e em França, v. A. Sousa PINHEIRO, *Privacy e proteção* cit., p. 657 e ss. e G. FUSTER, *The Emergence of* cit., p. 19 e ss..
[343] Comissão Europeia, "Community policy on data processing", novembro de 1973, p. 13.

respetiva competência, o art. 100.º dos Tratados (hoje o art. 114.º do TFUE[344]), e o imperativo de aproximar legislações nacionais [345].

Estes receios ganharam vida quando as autoridades nacionais restringiram os fluxos de dados pessoais entre Estados-Membros, fluxos esses essenciais para empresas estabelecidas em mais do que um. Por exemplo, em 1989 a autoridade de controlo francesa ("CNIL") bloqueou a transmissão dos dados pessoais de um colaborador do escritório da *Fiat*, em Paris, para o escritório de Turim, em Itália, invocando lacunas no direito da proteção de dados pessoais italiano[346]. Tornava-se evidente que a livre circulação de dados pessoais, essencial para um mercado que se pretendia sem fronteiras, requeria um ato legislativo da UE no sentido de harmonizar legislações e remover obstáculos à circulação dos dados pessoais[347]. Por conseguinte, em 1990, a COM apresentou uma proposta de Diretiva[348] ("proposta original"), alterada em 1992[349] ("proposta alterada"), inspirada na Convenção n.º 108, na legislação federal alemã e francesa[350]. As descrições doutrinais da Diretiva 95/46 como uma ferramenta de neutralização da soberania nacional em favor da eficiência económica giram à volta desta dimensão integracionista[351].

O propósito harmonizador do RGPD ou a "dimensão mercado único" são declarados em nas comunicações da COM que antecederam a sua adoção, nos considerandos, e

[344] Cuja epígrafe é "a aproximação de legislações".
[345] Sobre estas resoluções, v. G. FUSTER, *The Emergence of* cit., p. 115 e ss..
[346] CNIL, "Délibération n.º 89/78 du 11 juillet 1989", *Dixième Rapport au Président de la République et au Parlement,* 1989, p. 32 e ss.. Mas há outros exemplos: na década de 70 a autoridade nacional Sueca recusou a transmissão de dados pessoais para o Reino Unido em vários casos; em 1980 a Áustria adotou legislação que exigia a autorização prévia do Comissário Austríaco de Proteção de Dados antes da transmissão de dados sobre pessoas coletivas para certos Estados-Membros uma vez que a legislação de proteção de dados desses países não abrangia aquele tipo de dados, v. Christopher KUNER, *Transborder Data Flows and Data Privacy Law,* Oxford University Press, 2013, p. 40 e Jon BING, *Transnational Data Flows and the Scandinavian Data Protection Legislation*, Stockholm Institute for Scandinavian Law, 1980, p. 73.
[347] G. FUSTER, *The Emergence of* cit., p. 126; Helmut HEIL, "Directive 95/46/EC of the European Parliament and of the Council: Introductory remarks", Alfred BULLESBACH *et alii*, *Consice European IT Law (Second Edition),* Kluwer Law International, 2010, p. 10 e María del Carmen GUERRERO, *El impacto de Internet en el derecho fundamental a la protección de datos de carácter personal,* Thomson Civitas, 2006, p. 61.
[348] Proposta de diretiva do Conselho relativa à proteção das pessoas no que diz respeito ao tratamento dos dados pessoais, 24 de setembro de 1990.
[349] Proposta alterada de diretiva do Conselho relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à sua livre circulação, 18 de outubro de 1992.
[350] G. FUSTER, *The Emergence of* cit., p. 126
[351] Jean-Baptiste THOMAS-SERTILLANGE e Elisabeth QUILLATRE, "Libre circulation des données à caractere personnel au sein du marche intérieur et de l'espace de Liberté Sécurité Justice: Vers une diversification des instruments de régulation", *Petites Affiches,* n.º 400, 2011, p. 3; O. LYNSKEY, *The Foundations* cit., p. 50.

implícitos em várias disposições[352]. Por um lado, no art. 51.º, n.º 2, nos termos do qual as autoridades de controlo devem contribuir para a "aplicação coerente" do RGPD e, por outro lado, em três mecanismos especificamente arquitetados para esse fim: o mecanismo da *one-stop-shop*[353] ou sistema de balcão único, a cooperação entre autoridades de controlo[354] e o procedimento de controlo da coerência[355]. Adicionalmente, o art. 92.º e os considerandos 167 a 169, atribuem poderes executivos à COM para orientar a aplicação de certas normas.

A dimensão integracionista poderá ser prejudicada, por exemplo, pela margem de manobra concedida ao direito nacional em certos domínios[356], pelas divergências interpretativas ainda existentes entre autoridades de controlo ou pela falta de recursos e meios de algumas autoridades por comparação com outras[357]. Por isso compreendo aqueles que invocam F. CARNELUTTI para considerar que o RGPD tem "o corpo de um regulamento, mas a alma de uma diretiva"[358].

1.2.2. A dimensão jusfundamental

Recordando o pendor maioritariamente económico dos primeiros passos da integração europeia, à data de adoção da Diretiva o relevo dos direitos fundamentais no

[352] Comissão Europeia, "Proteção da privacidade num mundo interligado. Um quadro europeu de proteção de dados para o século XXI", 25 de janeiro de 2012, p. 8 e 9 e "Uma abordagem ..." cit., p. 10; considerandos 7, 9 e 10.
[353] Para os casos de "tratamento transfronteiriço", definido nos termos do art. 4.º, n.º 23, quando existe uma "autoridade de controlo principal", de acordo com o art. 56.º. A ideia é que os responsáveis pelo tratamento tenham apenas uma única autoridade de controlo como interlocutor.
[354] Artigos 60.º e ss..
[355] Artigos 63.º e ss.. Este mecanismo visa assegurar que as decisões de uma autoridade de controlo com impacto a nível europeu tenham em conta os pareceres emitidos pelas outras autoridades interessadas e sejam conformes com o DUE.
[356] E SEPD, "Opinion of the European Data Protection Supervisor on the Data Protection Reform Package", 7 de março de 2012, p. 9. Apesar de incidir sobre a primeira proposta do RGPD da Comissão Europeia, muitas dos alertas ali lançados são válidos para a versão final do RGPD: é o caso do art. 6.º, n.º 1, al. c) (a obrigação jurídica podendo resultar do direito nacional), do art. 84.º (sobre as sanções), do art. 23.º (limitações aos direitos do titular dos dados) e a maioria das normas do Capítulo IX. Criticando a margem de manobra conferida aos Estados-Membros e as dificuldades colocadas à harmonização pretendida, v. Christopher KUNER, "The European Commission's Proposed Data Protection Regulation: A Copernican Revolution in European Data Protection Law", *Bloomberg BNA Privacy and Security Law Report,* 6 de fevereiro de 2012, p. 13 e O. LYNSKEY, *The Foundations of* cit., p. 73.
[357] Cfr. Parte III, Capítulo 1, ponto 1.1.1., desta tese.
[358] Pablo MEXÍA, "La singular naturaleza jurídica del reglamento general de protección de datos de la UE. Sus efectos en acervo nacional sobre protección de datos", *Reglamento General De Protección De Datos. Hacia um nuevo modelo europeo de privacidade,* José Piñar MAÑAS (dir.), Reus, 2016, p. 34.

projeto europeu era menor[359]. Em todo o caso, todos os intervenientes do processo legislativo de redação daquele diploma expressaram, desde o início, preocupações com os riscos para os direitos fundamentais oriundos dos novos tratamentos de dados pessoais desencadeados pelo desenvolvimento tecnológico. Em várias resoluções do PE, entre 1975 e 1982[360], a preocupação é manifesta, bem como na Comunicação da COM anexa à primeira proposta de Diretiva, onde se constata que a legislação nacional em vigor nos Estados-Membros é deficiente e "não reflete o compromisso da Comunidade com a proteção dos direitos fundamentais"[361].

No passado, alguns autores enquadraram este bloco normativo numa tendência específica do DUE segundo a qual os direitos fundamentais seriam "trunfos" contra as liberdades do mercado interno[362]. Outros defendiam que este regime seria "consistente com uma conceção de privacidade informacional enquanto direito fundamental"[363]. O TJ declarou, em 2003, no caso *Rundfunk*[364]*,* que a Diretiva devia ser interpretada à luz dos direitos fundamentais. Porém, foi o TL que firmou a dimensão jusfundamental deste regime, em especial o art. 16.º do TFUE e o art. 8.º da CDFUE, no seguimento de recomendações de várias entidades[365]. Redigidos em termos semelhantes, os dois artigos reconhecem que "todas as pessoas têm direito à proteção dos dados de caráter pessoal que lhe digam respeito".

---

[359] G. FUSTER, *The Emergence of* cit., p. 126 e Ludovic COUDRAY, *La Protéction des données personelles dans l'Union européene: Naissance et consecration d'un droit fundamental,* Éditions universitaires européennes, 2010, p. 31.

[360] A própria designação destas resoluções é esclarecedora: "Resolução sobre a proteção dos direitos do indivíduo em face dos desenvolvimentos tecnológicos no domínio da proteção de dados pessoais".

[361] Comissão Europeia, "Comunicação relativa à proteção das pessoas no que diz respeito ao tratamento dos dados pessoais na Comunidade e à segurança dos sistemas de informação, 24 de setembro de 1990, p. 15.

[362] G. FUSTER, *The Emergence of* cit., p. 135 e John MORIJN, "Balancing Fundamental Rights and common market freedoms in Union Law: Schmidberger and Omega in the light of the European Constitution", *ELJ,* vol. 12, n.º 1, 2006, p. 15.

[363] Pamela SAMUELSON, "Privacy as Intellectual Property", *SLR,* n.º 52, 2000, p. 1125 e ss..

[364] "Cabe ainda acrescentar que as disposições da Diretiva 95/46, na medida em que regulam o tratamento de dados pessoais suscetíveis de pôr em causa as liberdades fundamentais e, em especial, o direito à vida privada, devem necessariamente ser interpretadas à luz dos direitos fundamentais (...)", Acórdão do TJ Österreichischer Rundfunk *et alii* c. Christa Neukomm e Joseph Lauermann*,* C-465/00, 20 de maio de 2003, n.º 68.

[365] Como, por exemplo, do G29, "Recommendation 4/99 on the inclusion of the fundamental right to data protection in the European catalogue of fundamental rights", 7 de setembro de 1999, p. 2 ou de um grupo de peritos num relatório para a COM, Expert Group on Fundamental Rights, "Affirming fundamental rights in the European Union: time to act", 1999, disponível online em http://ftp.infoeuropa.eurocid.pt/database/000038001-000039000/000038827.pdf , consultado no 30 de setembro de 2018.

As consequências desta "constitucionalização"[366] da proteção de dados pessoais fazem-se sentir a vários níveis: desde logo, na jurisprudência do TJ – acusado de "ativismo judicial"[367] – bem como na redação do RGPD (1.2.2.1.); adicionalmente, a autonomização do direito à proteção de dados pessoais suscita a questão da sua relação com o direito ao respeito pela vida privada e familiar consagrado no art. 7.º da CDFUE (1.2.2.2.); por fim, a estrutura constitucional daquele direito fundamental integra um dever de proteção constitucionalmente explícito (1.2.2.3).

1.2.2.1.Reflexos na jurisprudência do TJ e no RGPD

No passado alguns autores consideraram que a proteção concedida aos direitos fundamentais pelo TJ era minimalista e instrumentalizada em função dos objetivos da UE[368]. Não é, de todo, o caso do domínio em estudo em relação ao qual aquela instância tem vindo a posicionar-se como líder na solução dos problemas únicos de proteção da pessoa singular no mundo digital[369].

Em várias ocasiões o art. 8.º da CDFUE e o art. 16.º do TFUE constaram do argumentário do TJ para atribuir prioridade ao direito à proteção de dados pessoais quando ponderado em situações de colisão ou conflito com outros direitos, valores e interesses[370]. Por exemplo, no caso *Google Spain*, estudado mais adiante, o TJ declarou que o direito à proteção de dados pessoais prevalece "em princípio, não só sobre o interesse económico do operador do motor de busca mas também sobre o interesse [do] público em encontrar a referida informação durante uma pesquisa sobre o nome dessa pessoa"[371]. O tribunal advogou a "não subordinação dos direitos fundamentais dos

---

[366] O. LYNSKEY, *The Foundations of* cit., p. 87.
[367] O que, em bom rigor e verdade, não se verifica apenas no domínio da proteção de dados pessoais, v. Graça MONIZ, "Compreender o ativismo judicial do Tribunal de Justiça da União Europeia. A "Explicação" de Ronald Dworkin", *Themis,* ano XVIII, n.º 32, 2017, p. 125 e ss..
[368] Catarina Sampaio VENTURA, "Contexto e Justificação da Carta", *Carta dos Direitos Fundamentais da União Europeia,* Coimbra Editora, 2001, p. 46.
[369] Frederico FABBRINI, "The EU Charter of Fundamental Rights and the Rights to Data Privacy: The EU Court of Justice as a Human Rights Court", Sybe de VRIES (ed.), *Five Years of Legally Binding Charter of Fundamental Rights,* Hart Publishing, 2015; Gabriela ZANFIR, "How CJEU's 'Privacy Spring' Construed the Human Rights Shield in the Digital Age", *European judicial systems as a challenge for democracy,* Intersentia, 2015, p. 111; Maja BRKAN, "The Unstoppable Expansion of the EU Fundamental Right to Data Protection. Little Shop of Horrors?", *MJ,* n.º 23, 2016, p. 812 e ss.; Selena CRESPI, "Diritti fondamentali, Corte di giustizia e riforma del Sistema UE di protezione dei dati", *RIDPC,* 2015, p. 819 e ss..
[370] F. FABBRINI, "The EU Charter …" cit., p. 20; M. BRKAN, "The Unstoppable ..." cit., p. 824 e Mistale TAYLOR, "The EU's human rights obligations in relation to its data protection laws with extraterritorial effect", *IDPL,* vol. 5, n.º 4, 2015, p. 247 e 253.
[371] Acórdão do TJ, Google Spain SL e Google Inc. c. Agencia Española de Protección de Datos (AEPD) e Mario Costeja González*,* C-131/12, 13 de maio de 2014, n.º 97.

titulares dos dados pessoais a um entendimento superlativo dos interesses económicos dos prestadores de serviços, da liberdade de expressão e dos direitos dos internautas"[372].

O art. 8.º da CDFUE surge também em juízos de ponderação com interesses de segurança e de aplicação da lei, como evidenciam o caso *Digital Rights Ireland*[373], o caso *Schrems*[374], e a recente opinião do TJ sobre o acordo entre a UE e o Canadá a propósito dos dados de registo de passageiros ou PNR[375].

À luz do relevo crescente da proteção de dados pessoais na jurisprudência do TJ, seja para reforçar a tutela da pessoa singular no contexto digital (*Google Spain*), seja como *wake up call*[376] ou reação ao alarme social surgido com as revelações de Edward Snowden, em 2013, com as tendências de *dataveillance* ou *data surveillance*[377] e as derivas securitárias (*Digital Rights Ireland, Schrems* e PNR), há quem observe a emergência de um "super direito"[378] ou "direito pesado"[379]. Outros autores criticam o *data protection activism*[380] do TJ vaticinando consequências nefastas na promoção e proteção de outros direitos, valores e interesses[381]. Por outro lado, o vanguardismo do TJ

---

[372] Catarina Sarmento e CASTRO, "A jurisprudência do Tribunal de Justiça da União Europeia, o Regulamento Geral sobre a proteção de dados pessoais e as novas perspetivas para o direito ao esquecimento na Europa", *Estudos em Homenagem ao Conselheiro Presidente Rui Moura Ramos*, Vol. 1, 2016, p. 1061.

[373] Acórdão do TJ, Digital Rights Ireland *et alii* c. Minister for Communications, Marine and Natural Resources *et alii,* C-293/12, 8 de abril de 2014. Sobre esta decisão, v. F. FABBRINI, "The EU Charter …" cit., p. 19.

[374] Analisado na Parte III, Capítulo 2, ponto 2.3.1. deste trabalho.

[375] Parecer 1/15 do TJ, ECLI:EU:C:2017:592; Desenvolvendo as implicações deste parecer, v. Christopher KUNER, "Court of Justice International agreements, data protection, and fundamental rights on the international stage: Opinion 1/15, *EU-Canada PNR*", *CMLR*, vol. 55, n.º 3, 2018, p. 857 e ss..

[376] Anna DIMITROVA, "Balancing National Security and Data Protection: The Role of EU and US Policy-Makers and Courts before and after the NSA Affair", *JCMS,* vol. 56, 2018 e Tuomas OJANEN, "Privacy is More than Just a Seven-Letter Word: The Court of Justice of the European Union Sets Constitutional Limits on Mass Surveillance", *ECLR,* n.º 10, 2014, p. 528.

[377] Como refere M. TZANOU as medidas de "vigilância dos dados" partilham o mesmo *modus operandi*: prosseguem a luta contra a criminalidade grave e a prevenção de crimes transnacionais; implicam a cooperação forçada de atores privados e a recolha de um volume significativo de dados pessoais; os dados pessoais são tratados e usados de forma probabilística e algorítmica, v. Maria TZANOU, *The Fundamental Right to Data Protection. Normative Value in the Context of Counter-Terrorism Surveillance,* Hart Publishing, 2017, p. 251.

[378] Christopher KUNER, "A Super-Right to Data Protection? The Irish Facebook Case and the Future of EU Data Transfer Regulation", *LSE Media Policy Project Blog,* Dezembro de 2014, disponível em http://blogs.lse.ac.uk/mediapolicyproject/2014/06/24/a-super-right-to-data-protection-the-irish-facebook-case-the-future-of-eu-data-transfer-regulation/, consultado no 30 de setembro de 2018.

[379] M. TAYLOR, "The EU's human rights …" cit., p. 254.

[380] M. TZANOU, *The Fundamental* cit., p. 63.

[381] M. TAYLOR dá o exemplo da China e a Rússia, países com regimes de privacidade rigorosos e *firewalls* na Internet que conflituam com a liberdade de expressão e com a livre circulação da informação, v. "The EU's human rights …" cit., p. 255, nota de rodapé 86. No mesmo sentido, Bilyana PETKOVA, "Towards na Internal Hierarchy of Values in the EU Legal Order: Balancing the Freedom of Speech and Data Privacy", *MJECL,* vol. 23, n.º 3, 2016 e F. FABBRINI, "The EU Charter …" cit., p. 20, remetendo para bibliografia sobre estes "dilemas constitucionais" e M. BRKAN, "The Unstoppable ..." cit., p. 827, alertando para o surgimento de desequilíbrios na proteção dos direitos fundamentais na UE.

na regulação da era digital não é uma tarefa fácil e, como terei ocasião de demonstrar, decisões disruptivas como *Google Spain* e *Schrems,* geram questões deixadas em aberto pelo poder judicial que, ainda por cima, teima em prosseguir um estilo minimalista[382]. Há mesmo quem note que, em certos casos, o TJ se limitou a abrir uma caixa de pandora[383].

Além da jurisprudência, a valorização crescente da dimensão jusfundamental deste regime salta à vista nas duas comunicações da COM que antecederam a adoção do RGPD. Ambas enunciam, entre os objetivos principais, o reforço dos direitos fundamentais das pessoas singulares, em especial o direito à proteção de dados pessoais, um imperativo em face de um contexto digital que coloca novos desafios e riscos[384]. Acresce que aquele diploma, por contraposição com a Diretiva, autonomizou dos demais o direito fundamental à proteção de dados pessoais[385] e reforçou os direitos do titular dos dados pessoais, criando novos trunfos para este, como, por exemplo, o direito contra decisões individuais e automatizadas[386].

1.2.2.2.A relação entre o direito ao respeito pela vida privada e familiar (art. 7.º da CDFUE) e o direito à proteção de dados pessoais (art. 8.º da CDFUE)

A "emancipação"[387] da proteção de dados pessoais em relação ao direito ao respeito pela vida privada e familiar, além de distinguir este regime do vigente nos EUA – país onde a Lei Fundamental não consagra expressamente qualquer um destes direitos fundamentais[388] – veio causar uma discussão teórica sobre a relação entre ambos. Será o

[382] A. MIGLIO, "Back to … cit., p. 101 e 106; Christopher KUNER, "The Court of Justice of the EU Judgment on Data Protection and Internet Search Engines", Burkhard HESS e Cristina MARIOTTINI, (eds.), *Protecting Privacy in International and Procedural Law and By Data Protection (European and American Developments),* Ashgate-Nomos, 2015, p. 19 e ss.; Gráinne DE BURCA, "After the EU Charter of Fundamental Rights: The Court of Justice as a Human Rights Adjudicator?", *MJECL*, n.º 168, 2013, p. 184; Joseph WEILER, "The Judicial Après Nice", Gráinne DE BURCA e Joseph WEILER (eds), *The European Court of Justice,* 2001, Oxford University Press, p. 215 e 224.
[383] F. FABBRINI, "The EU Charter …" cit., p. 21.
[384] Comissão Europeia, "Uma abordagem ..." cit., p. 5 e Comissão Europeia, "Proteção da ..." cit, p. 2.
[385] Compare-se, por exemplo, o art. 1.º, n.º 1, da Diretiva, realçando o "direito à vida privada", com o art. 1.º. n.º 2, do RGPD, destacando o direito à proteção dos dados pessoais.
[386] Art. 22.º do RGPD.
[387] Na expressão de A. Sousa PINHEIRO, *Privacy e proteção* cit., p. 785.
[388] Acresce que, ao nível constitucional, a 4ª Emenda visa a proteção dos cidadãos das ações do Estado e não do setor privado, v. Daniel SOLOVE, "Digital Dossiers and the Dissipation of Fourth Amendment Privacy", *CalLR*, n.º 75, 2002, p. 1803 e ss.; H. HIJMANS, *The European Union as* cit., p. 402; Paul SCHWARTZ e Daniel SOLOVE, *Information Privacy Law,* 3ª edição, Aspen Publisher, 2009, p. 260 e ss.; Teresa MOREIRA, *A Privacidade dos Trabalhadores e as Novas Tecnologias de Informação e Comunicação: contributo para um estudo dos limites do poder de controlo eletrónico do empregador,* Almedina, 2010, p. 155.

direito à proteção de dados pessoais um *complemento* ou uma *faceta* da tutela da vida privada no atual contexto digital? Será que confere uma proteção alargada a outros direitos fundamentais além da vida privada e familiar? Estas são algumas das questões que ocupam a doutrina[389].

Numa fase inicial o TJ confundiu os termos deste debate ao proclamar, em 2010, um só direito: "o respeito pelo direito à vida privada relativamente ao tratamento de dados pessoais, reconhecido pelos artigos 7.º e 8.º da Carta"[390]. Contudo, decisões mais recentes, como *Digital Rights Ireland* ou *Google Spain* sinalizam uma certa "maturidade" na interpretação deste direito[391]. Em especial, na primeira, aquela instância especificou a existência de uma ingerência ao direito à proteção de dados pessoais sempre que exista um tratamento de dados pessoais independentemente das implicações desse tratamento para o direito à vida privada[392]. Esta evolução mereceu a adesão da doutrina segundo a qual o direito à proteção de dados pessoais, no ordenamento jurídico da UE, ocupa um espaço próprio e único porquanto reflete uma pretensão de reconfigurar a tutela conferida às pessoas singulares (e não apenas à sua vida privada e familiar) num novo contexto de digitalização da vida em sociedade permeado pela utilização crescente de informação pessoal, por sujeitos privados e públicos[393].

---

[389] Antoinette ROUVROY e Yves POULLET, "The Right to Informational Self-Determination and the Value of Self-Development: Reassessing the Importance of Privacy for Democracy", Serge GUTWIRTH et *alii* (eds.), *Reinventing Data Protection?,* Springer, 2009, p. 45; Francesca BIGNAMI, "The Case for Tolerant Constitutional Patriotism: The Right to Privacy before the European Courts", *CILJ,* n.º 41, 2008, p. 211 e ss., referindo que a CDFUE "dedica dois artigos à privacidade"; M. TZANOU, *The Fundamental* cit., p. 21 e ss.; O. LYNSKEY, *The Foundations of EU* cit., p. 89 e ss..

[390] Acórdão do TJ, Volker und Markus Schecke GbR e Hartmut Eifert c. Land Hessen, C-92/09 e C-93/09, 9 de novembro de 2010, n.º 52.

[391] No caso *Digital Rights Ireland* o TJ não só considerou a proteção de dados pessoais lado a lado com a vida privada como analisou separadamente a ingerência a cada um e as possíveis justificações aflorando, pela primeira vez, a "essência" dos dois direitos (Acórdão do TJ, Digital Rights Ireland *et alii* c. Minister for Communications, Marine and Natural Resources *et alii,* C-293/12, 8 de abril de 2014, n.os 29, 30, 31, 36, 40, 47, 48 e 54); em *Google Spain* o tribunal tratou de forma separada os dois direitos (n.º 69) e considerou que o tratamento de dados pessoais realizado por um motor de pesquisa "é suscetível de afetar significativamente os direitos fundamentais ao respeito pela vida privada *e* à proteção de dados pessoais" (Acórdão do TJ, Google Spain SL e Google Inc. c. Agencia Española de Protección de Datos (AEPD) e Mario Costeja González*,* C-131/12, 13 de maio de 2014, n.º 80).

[392] No n.º 36 o TJ afirmou que a "Diretiva 2006/24 é constitutiva de uma ingerência no direito fundamental à proteção dos dados pessoais, garantido pelo artigo 8.º da Carta, visto que prevê um tratamento dos dados pessoais".

[393] Gloria FUSTER e Raphael GELLERT "The Fundamental Right of Data Protection in the European Union: In Search of an Uncharted Right", *IRLCT,* n.º 26, 2012, p. 73; Juliane KOKOTT e Christoph SOBOTTA, "The Distinction between Privacy and Data Protection in the Jurisprudence of the CJEU and the ECtHR", *IDPL,* nº 3, 2013, p. 222; Maria TZANOU, "Data Protection as a Fundamental Right Next to Privacy?" 'Reconstructing' a Not So New Right", *IDPL,* n.º 3, 2013, p. 88 e ss.; Stefano RODOTÀ, "Data Protection as a Fundamental Right", Serge GUTWIRTH *et alii* (eds.), *Reinventing Data* cit., p. 80.

Nessa medida, este direito fundamental é um "direito-garantia" pois desempenha uma função *instrumental* de proteção ou *garantia* de "um conjunto de valores fundamentais individuais de que se destacam a privacidade e a liberdade, em poucas palavras, a autodeterminação individual"[394]. Como explica J. PIÑAR MAÑAS, o tratamento de dados pessoais coloca *riscos* para outros direitos fundamentais o que, aliás, é reconhecido no art. 1.º, n.º 2 do RGPD: "o presente regulamento defende os direitos e liberdades fundamentais das pessoas singulares, nomeadamente o seu direito à proteção dos dados pessoais"[395]. Para o G29 os riscos do tratamento de dados pessoais abrangem vários direitos fundamentais como a liberdade de expressão, de pensamento, de movimento, a proibição de discriminação, a liberdade de religião, entre outros[396]. Por conseguinte há uma "ligação direta" entre este e outros direitos fundamentais[397].

De facto, em termos *materiais*, procurando o bem jurídico – isto é, o *quid* a que o direito concede valor em virtude do seu contributo para a auto-realização do homem enquanto individualidade social – tutelado por este direito vislumbra-se não apenas um mas vários: a dignidade da pessoa humana, liberdade (de ação, de expressão, de pensamento) autonomia, autodeterminação, identidade pessoal, participação social[398]. Não obstante, do direito à proteção de dados pessoais decorre uma intencionalidade própria quanto a pelo menos um dos bens jurídicos que tutela: o controlo sobre os dados

[394] Filipa CALVÃO, "O direito fundamental à proteção dos dados pessoais e a privacidade 40 anos depois", Manuel A. VAZ *et alii, Jornadas nos quarenta anos da constituição da república portuguesa*, Universidade Católica, 2017, p. 89 e, da mesma autora, *Direito da Proteção de Dados Pessoais,* Universidade Católica, 2018, p. 51. Em sentido muito semelhante, defendendo que a proteção de dados pessoais é um direito processual, v. Norberto de ANDRADE, "Oblivion, the right to be diferente from oneself. Reproposin the right to be forgotten", *RIDP,* n.º 13, 2012, p. 125. Sobre os "direitos-garantias" na doutrina portuguesa, v. José Carlos VIEIRA DE ANDRADE, *Os Direitos Fundamentais na Constituição Portuguesa de 1976,* 3ª edição, Almedina, 2007, p. 121.

[395] José Piñar MAÑAS, "Objeto del reglamento", J. Piñar MAÑAS, *Reglamento General,* cit., p. 56 e ss.. Pense-se, por exemplo, na não discriminação no caso de operações de tratamento de certas categorias de dados conforme resulta do art. 9.º do RGPD.

[396] G29, "Statement on the role of a risk-based approach in data protection legal framework", 30 de maio de 2014, p. 4.

[397] F. CALVÃO, *Direito* cit., p. 51.

[398] A. ROUVROY e Yves POULLET, "The Right to .." cit., p. 47 e ss.; F. CALVÃO, "O direito fundamental ..." cit., p. 88.

pessoais[399] ou a "autodeterminação informativa"[400]. Nesse sentido, o considerando 7 do RGPD refere expressamente que "as pessoas singulares deverão poder controlar a utilização que é feita dos seus dados pessoais".

Adicionalmente, em termos *formais*, a autonomização do direito à proteção de dados pessoais retira-se do direito originário e derivado, com destaque para o RGPD que gera a "vida própria" daquele direito. No confronto com a tutela da vida privada e familiar, essa vivência autónoma é um indicador de uma caraterística diferenciadora da proteção de dados pessoais: a sua *estrutura constitucional*. Desta decorre uma exigência "não apenas de abstenção de ingerência na esfera jurídica dos cidadãos, como também uma função ativa para prevenir tal ingerência por parte de terceiros"[401].

1.2.2.3.A estrutura constitucional do artigo 8.º da CDFUE: um dever de proteção constitucionalmente explícito

Portanto, a outra caraterística distintiva do direito à proteção de dados pessoais é a sua estrutura constitucional.

A figura constitucional dos deveres de proteção de direitos fundamentais compreende-se à luz de um paradigma do Estado ativamente envolvido através da sua função legislativa e da sua máquina administrativa, na tarefa de corrigir desigualdades de facto entre sujeitos privados, tutelando a posição materialmente mais fraca por meio de regras imperativas. Com efeito, estes deveres refletem a transformação das funções da proteção jusfundamental, reunindo a função de defesa, prestação e de eficácia nas relações intersubjetivas privadas[402]. Ou, dito de outro modo, os deveres de proteção são uma figura constitucional *a se,* conveniente para casos em que o Estado "é confrontado,

---

[399] Este critério é decisivo para O. LYNSKEY: "o direito à proteção de dados pessoais não é apenas uma atualização do direito à vida privada na era digital. Pelo contrário (...) visa proteger um interesse individual específico de controlar a manipulação da informação pessoal: esta é uma proteção que transcende a tutela da vida privada e se assemelha a um direito pro ativo a gerir os dados pessoais em face das crescentes pressões tecnológicas a um controlo natural". v. J. Piñar MAÑAS, "Objeto ..." cit., p. 57; O. LYNSKEY, *The Foundations of EU* cit., p. 130; Paul DE HERT e Serge GUTWIRTH, "Data Protection in the Case Law of Strasbourg and Luxemburg: Constitutionalisation in Action", Serge GUTWIRTH *et alii* (eds.), *Reinventing Data* cit., p. 8; G29, "Parecer 3/2013 sobre limitação da finalidade", 2 de abril de 2013, p. 17. Esta também é a tese contida no relatório de peritos que antecedeu a CDFUE, v. Expert Group on Fundamental Rights, "Affirming Fundamental Rights in the EU: Time to Act", Bruxelas, Fevereiro de 1998, p. 16.

[400] F. CALVÃO, *Direito* cit., p. 50.

[401] F. CALVÃO, "O direito fundamental ..." cit., p. 90.

[402] Explicando esta transformação, J. Pereira da SILVA, *Deveres* ... cit., p. 63 e ss. e 136: "(...) se bem que não seja reconduzível a nenhuma das três funções jusfundamentais suas predecessoras, a função de proteção também não consome nenhuma delas; mas toma-as a todas (e a um só tempo) como pressuposto seu".

na sua posição de regulador social e de coordenador normativo de liberdades individuais, com uma agressão proveniente de um sujeito privado sobre bens jusfundamentais de outro sujeito privado"[403].

Para aquilo que mais interessa neste trabalho, exemplificando este dever, veja-se o art. 35.º, n.º 1, 2 e 7, da CRP, dispondo um dever legiferante para o Estado Português de modo a garantir proteção legal e ativa dos dados pessoais informatizados, sejam eles detidos por entes públicos ou privados, contra quaisquer formas de acesso ou uso indevido[404].

Ora, analisando o número 2, tanto do art. 16.º do TFUE como do art. 8.º da CDFUE, creio que no TL os Estados-Membros delegaram na UE, no seu legislador, a responsabilidade para prosseguir um dever de proteção com a adoção daquela mesma estrutura constitucional. As duas disposições referidas remetem para o "processo legislativo ordinário" (TFUE) e para a "lei" (CDFUE) o desenvolvimento das normas relativas à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais cuja função é, justamente, a de coordenar os vários interesses e direitos presentes nas relações subjacentes aos tratamentos de dados pessoais[405]. Portanto, cabe à UE, através do poder legislativo, ativamente proteger os dados pessoais prevenindo ingerências na esfera jurídica dos indivíduos por parte de terceiros. Este é um dever legiferante que não se encontra, por exemplo, no art. 7.º da CDFUE, onde apenas se lê: "Todas as pessoas têm direito ao respeito pela sua vida privada e familiar, pelo seu domicílio e pelas suas comunicações".

Além de distinguir o direito à proteção de dados pessoais de outros, há vários aspetos da teoria dos deveres de proteção de direitos fundamentais que fornecem uma chave de leitura do bloco de normas em apreço.

Em primeiro lugar, quanto aos sujeitos da relação jurídica no âmbito do tratamento de dados pessoais, atendendo à estrutura *triangular* [406] que carateriza a relação jusfundamental dos deveres de proteção, noto que:

(i) A fonte de risco, um "agressor, potencial ou efetivo", será o utilizador dos dados pessoais;

[403] *Idem*, p. 125.
[404] *Idem*, 143.
[405] Reconhecendo esta função ao poder legislativo, v. Herbert BURKERT, "Institutions of Data Protection – An Attempt at a Functional Explanation of European National Data", *CLJ,* n.º 3, 1981, p. 167.
[406] F. CALVÃO, *Direito* cit., p. 56 e J. Pereira da SILVA, *Deveres* cit., p.149.

(ii) O titular de um direito fundamental ameaçado por aquele risco – o titular dos dados pessoais – que, não tendo a possibilidade de se defender das ameaças que afetam os seus direitos, encontra-se numa posição passiva de especial vulnerabilidade e, por isso, dependente da proteção que lhe possa ser prestada pelo poder público e

(iii) Um terceiro, a UE, com a tarefa de coordenar os direitos fundamentais em presença através de um ato legislativo.

Para além da relação triangular, há outras formas de relacionamento jusfundamental, designadamente *multipolares*[407], expressas no desdobramento de um dos polos da relação triangular, como quando o RT recorre a um ST ou por via do papel da autoridade de controlo[408].

Em segundo lugar, no que toca à "estratégia"[409] usada pelo legislador para alcançar o seu desiderato de proteção estamos em face de uma proteção *primária* no sentido em que as imposições visam prevenir os riscos do tratamento de dados pessoais, e *secundária* porquanto igualmente sanciona os tratamentos de dados pessoais lesivos[410]; uma proteção *ativa* pois atua na fonte do perigo (sujeitando o utilizador de dados pessoais a condicionamentos de diferente intensidade e a medidas de fiscalização específicas) e, simultaneamente, *passiva,* focada no titular do direito fundamental que vê reforçada a sua capacidade de auto-defesa (através de uma cartilha de direitos específicos); uma proteção *negativa relativa* porquanto, em regra [411], não proíbe o tratamento de dados pessoais mas impõe obrigações a quem gera o risco.

Quanto ao tipo de normas desta proteção legislativa perfilam-se, por exemplo, normas *sancionatórias* de índole contra-ordenacional (art. 58, n.º 2, al. i) e art. 83.º do RGPD)*;* normas de *organização, procedimento e processo* para corrigir o modo de auto-organização dos causadores de risco (*v. g.* art. 24.º e 39.º do RGPD); normas sobre *informação* para promover uma relação de transparência com o titular dos dados e a

[407] F. CALVÃO, *Direito da* cit., p. 56 e J. Pereira da SILVA, *Deveres* cit., p. 159 e ss..
[408] Cfr. Parte III, Capítulo 1, ponto 1.4.1.1. desta tese.
[409] Discutindo as várias modalidades, v. J. Pereira da SILVA, *Deveres* cit., p. 636.
[410] Cfr. Parte III, Capítulo 1, pontos 1.3.2.2 e 1.4.1.1.3 deste trabalho.
[411] Com a exceção das categorias especiais de dados, v. art. 9.º do RGPD. E, mesmo em relação a estas, há exceções.

correção das assimetrias de informação que pautam a relação entre aquele e os causadores de risco[412] e normas de *segurança* que recaem sobre estes (art. 32.º e ss. do RGPD)[413].

Em quarto lugar, a intenção central desta proteção – acautelar riscos para o titular dos dados pessoais – convida o legislador a seguir o caminho da chamada *regulação do risco* – uma opção claramente adotada no RGPD, como demonstrarei no ponto seguinte.

Por fim, o legislador goza de uma ampla margem de liberdade de conformação o que não significa que esteja vinculado a uma obrigação de resultados porquanto "não pode estar obrigado a evitar a lesão dos direitos fundamentais, uma vez que a segurança absoluta é coisa que não existe"; acresce que não controla uma multiplicidade de elementos na origem do perigo[414]. Os limites àquela liberdade decorrem por um lado, das próprias normas onde nascem e crescem os deveres de proteção e, por outro lado, de um conjunto de princípios gerais (igualdade, proporcionalidade, proteção da confiança, reserva de lei) e específicos (primado da prevenção sobre a precaução, subsidiariedade da proteção penal, precaução, vinculação aos melhores conhecimentos científicos e técnicas e a proibição por defeito)[415].

1.3.Complexidade da natureza

Antes de enunciar as caraterísticas distintivas deste bloco de normas (1.4), importa determinar a sua natureza jurídica que, antecipo já, não é de fácil apreensão. Com efeito, é desde logo questionável a sua inserção nos tradicionais ramos do direito (1.3.1). Porventura, uma perspetiva mais útil para compreender a substância desta matéria passa por equacionar a sua índole regulatória (1.3.2), inclusive certas formas específicas de regulação, como a "co-regulação" ou a "auto-regulação publicamente regulada" (1.3.2.1),

[412] E que se verificam noutras relações, como a dos fornecedores e consumidores, v. José J. G. CANOTILHO, e Vital MOREIRA, *Constituição da República Portuguesa,* vol. I., Coimbra Editora, 2014, p. 781. Sobre a relação entre proteção de dados pessoais e proteção do consumidor, v. Natali HELBERGER *et alii*, "The Perfect Match? A Closer Look at the Relationship between EU Consumer Law and Data Protection Law", *CMLR,* vol. 54, n.º 5, 2017; Sobre o desiquilíbrio informacional na proteção de dados pessoais, v. Herbert BURKERT, "Towards a New Generation of Data Protection legislation", Serge GUTWIRTH *et alii, Reinventing Data Protection?* Springer, 2009, p. 339.

[413] A este propósito, J. Pereira da SILVA refere que "o direito mais diretamente atingido pelas normas de segurança é, por regra, a liberdade de iniciativa económica privada. Neste sentido, a conexão jusfundamental da generalidade das normas de segurança (...) constitui um limite que os movimentos de desregulamentação da atividade económica, surgidos nos últimos anos, não poderão nunca ultrapassar", v. J. Pereira da SILVA, *Deveres* cit., p. 651.

[414] *Idem,* p. 567.

[415] J. Pereira da SILVA, *Deveres* cit., p. 569 e ss..

bem como os indícios de uma abordagem baseada no risco já sugeridos pela estrutura constitucional do direito fundamental estudado (1.3.2.2).

1.3.1. Direito Público ou Direito Privado?

As "*situações da vida* são (...) cada vez mais complexas e não se deixam capturar pelas jaulas herméticas nas quais os juristas pretendem aprisioná-las, separando-as entre públicas e privadas. Não raras vezes, as situações jurídicas comungam elementos que carecem de uma aplicação de normas de Direito Privado e de outros que antes exigem a intervenção do Direito Público"[416]. As situações jurídicas no âmbito do tratamento de dados pessoais exemplificam esta observação de M. PRATA ROQUE: por um lado, não "encaixam" na linguagem e nos modelos do Direito Público ou do Direito Privado, cuja distinção, em boa verdade, sempre foi aproximada[417]; por outro, refletem a "equivocidade" trazida pelo DUE que parte de uma "construção própria e original do direito, que não valoriza a distinção privado-público", "utiliza critérios autónomos para definição das *suas* categorias" e "coloca em causa a tradicional divisão entre direito público e privado"[418]. Como sintetiza F. CALVÃO, o objeto da proteção de dados pessoais "reclama uma especialização que as disciplinas tradicionais não são capazes de oferecer"[419].

Se o ponto de partida da matéria da proteção de dados, os seus alicerces, recolhem contributos da disciplina dos Direitos Fundamentais, do Direito Constitucional e do DUE o seu núcleo central será de natureza juspublicista[420]. Em todo o caso, além dos elementos de Direito Administrativo mais evidentes, como as normas que regulam a organização e o funcionamento das autoridades de controlo, conferindo-lhes incumbências de fiscalização e supervisão (art. 51.º e ss.), acham-se também neste regime elementos de Direito Privado, como o direito de indemnização (art. 82.º do RGPD) ou o contrato com

---

[416] M. Prata ROQUE, *A Dimensão* cit., p. 308.
[417] Em todo o caso, há quem refira a "tendencial inesgotabilidade das teses quanto à distinção entre Direito Privado e Direito Público" (M. Prata ROQUE, *A Dimensão* cit., p. 309) e quem procure sumariar os critérios usados para esta distinção: a participação de um órgão de autoridade, as funções desempenhadas, o enquadramento jurídico aplicável, o domínio de uma autoridade pública e o interesse prosseguido (Simon WHITAKER, "Consumer Law and the distinction between public law and private law", *The Public Law/Private Law Divide – Une entente assez cordiale,* Mark FREEDLAND, e Jean-Bernard AUBY (eds.), Hart Publishing, 2006, p. 247). Certo é que o paradigma clássico da distinção taxativa e terminante entre Direito Público e Direito Privado, como dois mundos separados, segundo uma lógica de oposição, encontra-se ultrapassado, v. P. GONÇALVES, *Entidades Privadas* cit., p. 271 e ss..
[418] D. LOPES, *Eficácia* cit., p. 118 e ss..
[419] F. CALVÃO, *Direito* cit., p. 32.
[420] *Idem*, p. 33.

o subcontratante (art. 28.º do RGPD) e, ainda, de Direito Processual Civil e Administrativo, como as regras do acesso dos titulares dos dados aos tribunais (art. 78.º e ss. do RGPD).

Não sendo possível isolar cada um destes elementos e erguer uma separação fictícia para efeitos de classificação rigorosa deste regime, tem-se entendido que o mesmo congrega entrelaçamentos entre os vários ramos do direito, reunindo disposições e institutos dos mesmos cuja identificação dependerá do caso concreto[421]. Este regime é, por isso, um exemplo do "fenómeno da interconexão, sobreposição ou mistura de normas de Direito Público e normas de Direito Privado" [422]. É que mesmo admitindo uma predominância do Direito Público, este não basta para compreender todas as questões jurídicas aqui abordadas[423].

Em suma, este bloco normativo encontra-se, então, numa área de confluência, numa *no man's land*[424], caraterizando-se pela sua *interdisciplinariedade* ao integrar normas de vários ramos do Direito. Donde tão oportunos os apelos à sua "emancipação" científica[425].

1.3.2. A proteção de dados pessoais no espectro da "regulação"

Creio que uma perspetiva mais proveitosa para compreender o regime estudado encontra-se no conceito de "regulação". Para P. GONÇALVES trata-se, genericamente, de "um sistema de *influenciação,* de *orientação* e de *controlo* de processos e de comportamentos ou condutas de pessoas; esse sistema pode revelar-se de uma forma positiva (na feição de *comandos, diretrizes* ou *recomendações*) ou de uma forma negativa (na veste de *proibições, limitações* ou advertências) e utiliza, no seu *instrumentarium,* a edição de normas, bem como a adoção de medidas de implementação e de reação à infração do que aquela normas estabelecem"[426].

---

[421] Christopher KUNER, "Data Protection Law and International Jurisdiction on the Internet (Part 1)", *IJLIT*, vol. 18, n.º 2, 2010, p. 176 e ss.. Em sentido próximo, v. Jon BING, "Data Protection, Jurisdiction and the Choice of Law", *Privacy Law & Policy Reporter,* n.º 92, 1999, disponível em http://www.uio.no/studier/emner/jus/jus/JUR5620/v08/undervisningsmateriale/Data%20Protection,%20jurisdiction%20and%20the%20choice%20of%20law.rtf, consultado no dia 30 de setembro de 2018.

[422] P. GONÇALVES, *Entidades Privadas,* cit., p. 279.

[423] F. CALVÃO, *Direito* cit., p. 33.

[424] Frequente em domínios nos quais há uma prevalência de um dos ramos do direito, em termos de métodos e meios de ação que, todavia, devem ser compaginados com imperativos do outro, v. Pierre OMMESLAGHE, "Le Droit Public Existe-t-il?", *Revue de la faculte de droit et de criminologie de l'ULB,* n.º 33, 2006, p. 62.

[425] F. CALVÃO, *Direito* cit., p. 33.

[426] Pedro GONÇALVES, "Regulação Administrativa e Contrato", *Estudos em Homenagem ao Prof. Doutor Sérvulo Correia,* vol. II, Coimbra Editora, 2010, p. 987 e ss.. Uma análise mais recente do conceito de regulação é da autoria de Raquel CASTRO, *Constituição, Lei e Regulação dos Media,* Almedina, 2016, p. 31 e ss..

Por um lado, o desenvolvimento diferenciado deste tipo de normatividade deve-se a um conjunto de motivos entre os quais destaco "os riscos apresentados por novos produtos e por novas tecnologias"[427]. Por outro lado, compreende-se à luz de um "Estado Regulador" ou "Estado-estratega", hipótese aplicável à UE[428], que prossegue uma *intervenção* externa (heterorregulação) sobre atividades privadas de natureza económica, comercial e financeira tendo em vista "uma proteção ótima do '*interesse público'* através da imposição de limitações ao exercício da iniciativa privada"[429]. Essa intervenção define as condições normativas de funcionamento das atividades reguladas, no cumprimento de uma "função de orientação de sistema" e, além disso, prescreve um controlo da observância de tais condições e uma punição das infrações[430]. Ou seja, a "atuação reguladora" visa conformar, dirigir, orientar, sancionar, disciplinar ou simplesmente controlar a atividade regulada[431].

O *telos* da regulação é a realização de objetivos públicos e finalidades identificadas em sede político-legislativa para promover o bem-estar social. A atuação reguladora prossegue um interesse público relacionado com objetivos sociais como a proteção dos indivíduos, defesa dos interesses ambientais, entre outros[432] – *regulação social* – ou estritamente económicos – *regulação económica*[433]. Para tanto, a iniciativa privada influenciada pela atuação reguladora não é configurada como um direito fundamental

---

[427] Eduardo Paz FERREIRA e Luís MORAIS, "A Regulação sectorial da economia – introdução e perspetiva geral", E. Paz FERREIRA, L. MORAIS e G. ANASTÁCIO, *Regulação em Portugal: Novos Tempos, Novo Modelo?* Almedina, 2009, p. 7 e ss. e Maria C. CARDONA, *Contributo para o conceito e a natureza das entidades administrativas independentes – As Autoridades Reguladoras,* Almedina, 2016, p. 664.

[428] Para alguns o protótipo de um novo Estado Regulador de nível supranacional, v. Giandomenico MAJONE, *La Communauté européenne: un état régulateur,* Montchrestien, 1996; Marisa APOLINÁRIO, *O Estado Regulador: o novo papel do Estado,* Almedina, 2016, p. 242. Em estudos comparativos com os EUA a UE emerge como um "hiper-regulador", tendo mais apetência para aplicar soluções normativas "intervencionistas", v. Jonathan WIENER *et alii* (eds.), *The Reality of Precaution: Comparing Risk Regulation in the United States and Europe,* Routledge, 2010 e David VOGEL, *The Politics of Precaution. Regulating Health, Safety, and Environmental Risks in Europe and the United States,* Princeton University Press, 2010.

[429] M. Prata ROQUE, *A Dimensão* cit., p. 721.

[430] P. GONÇALVES, "Direito Administrativo..." cit., p. 15, considerando o mercado como um "sistema".

[431] *Ibidem*.

[432] Busca determinados equilíbrios entre valores de mercado e outros valores correspondentes a interesses públicos, como a salvaguarda do pluralismo da informação ou outros interesses sociais de "primordial importância que transcendem, de algum modo, as puras condições de economicidade das atividades empresariais" v. E. Paz FERREIRA e L. MORAIS, "A Regulação sectorial..." cit., p. 23. Uma distinção aproximada é a de Vital MOREIRA, v. *Auto-Regulação Profissional e Administração Pública,* Almedina, 1997, p. 39 e ss..

[433] Orientada para a promoção de valores de mercado e de abertura de determinados setores económicos à concorrência, v. E. Paz FERREIRA e L. MORAIS, "A Regulação sectorial..." cit., p. 23. Para P. GONÇALVES, neste caso, a "satisfação do interesse público alcança-se, por forma indireta ou mediata, através do "correto desenvolvimento" das relações económicas e jurídicas (privadas) que se processam entre os vários atores do mercado, designadamente entre as empresas e os consumidores", v. P. GONÇALVES, "Direito Administrativo da ..." cit., p. 66

absoluto: o interesse público na prossecução e garantia de outros direitos fundamentais com aquela conflituantes pode "justificar um mero condicionamento ou até mesmo uma restrição da amplitude máxima do '*direito de iniciativa privada'*, sem que tal implique uma violação do parâmetro normativo constitucional"[434].

As *formas* de regulação desdobram-se, quanto à *origem*, em "regulação de origem ou proveniência privada" e "regulação de origem ou proveniência pública" [435]. Esta é um produto do poder público (estadual ou supranacional), ora provindo de "instâncias integradas na Administração Pública", associadas à execução de uma função administrativa de regulação[436], ora de outros centros de criação de regulação pública como o poder legislativo, correspondendo a atos legislativos[437]. Quanto aos *destinatários*, a regulação *setorial* – "atinge setores determinados da economia, pelo que *regulados* são apenas os operadores económicos que atuam nos setores atingidos (*v. g.* energia, comunicações, banca)"[438] – distancia-se da regulação *transversal*, "aplicável à generalidade dos agentes económicos"[439], cujo caso paradigmático é a regulação da concorrência.

Mais do que caber (ou não) nas "jaulas herméticas" do Direito Público e/ou Direito Privado o regime de que me ocupo compreende-se melhor no quadro de uma atuação reguladora da UE[440]. Carateriza-se, então, enquanto:

(i) Regulação pública, no sentido em que é fruto do poder legislativo daquela e exprime-se enquanto regulação administrativa nos atos praticados pelas autoridades de controlo, sejam ordens, proibições, punições, avisos, recomendações, entre outros[441].

[434] M. Prata ROQUE, *A Dimensão* cit., p. 720 e 721.
[435] Sem prejuízo de outros tipos de regulação de origem privada, que remeto para adiante, o instrumento mais conhecido é o contrato ou, *mutatis mutandis,* o negócio jurídico unilateral, cuja juridicidade nele expressa é desejada e produzida pelos próprios sujeitos da regulação v. P. GONÇALVES, "Regulação Administrativa ...", cit., p. 5.
[436] A "regulação" pode ser entendida enquanto missão da qual, no terreno, se ocupam as "entidades reguladoras" na sua atividade operacional, através do exercício de poderes sancionatórios, de supervisão e de regulamentação, v. P. GONÇALVES, "Direito Administrativo da...", cit., p. 20.
[437] P. GONÇALVES, "Regulação Administrativa..." cit., p. 5.
[438] *Idem*, p. 16.
[439] *Idem*, p. 17.
[440] Luiz COSTA, "Privacy and the precautionary principle", *CLSR,* n.º 28, 2012, p.14 e O. LYNSKEY, *The Foundations of* cit., p. 76.
[441] Art. 58.º, n.º 1 e 2 do RGPD.

(ii) Intervenção externa nas atividades de tratamento de dados pessoais realizadas pelos utilizadores de dados pessoais, definindo as condições das mesmas, e conformando-as com imposições sujeitas a fiscalização e punição por desrespeito. Como explica F. CALVÃO: "no que aos tratamentos de dados pessoais diz respeito, a função do Estado não se pode resumir simplesmente ao acompanhamento sucessivo das atividades privadas (ou públicas), quando das mesmas possa resultar a afetação de direitos, liberdades e garantias dos membros da comunidade estatal. Isto porque, ao contrário de outras atividades, que são livres (porventura só agora desreguladas), por o seu desenvolvimento não implicar risco ou ameaça de direitos e de interesses privados e públicos, as operações que incidam sobre dados pessoais, qualquer que seja a sua natureza, não são, não podem ser livres. Falamos de atividades que são suscetíveis de ter impacto na liberdade, na privacidade, na autodeterminação ou na identidade das pessoas. E um tal impacto e um tal risco de lesão de dimensões fundamentais da dignidade da pessoa humana não podem ser ignorados, muito menos incentivados. É esta a razão por que na União Europeia não se abandona a regulação pública dos tratamentos de dados pessoais, definindo-se no plano normativo condições ou requisitos para a sua realização. E por isso a passagem do foco da função administrativa para o controlo sucessivo não reflete uma conceção de que o tratamento de dados pessoais é livre, quanto ao *se* da sua realização, e que o controlo se limite apenas ao *como* da atividade"[442].

(iii) Acresce que, dado que o tratamento de dados pessoais é uma atividade que perpassa a maioria dos agentes económicos e, como demonstrarei, o próprio setor público, considero tratar-se de regulação *horizontal*[443].

(iv) Por fim, reúne elementos da regulação de natureza económica e social[444].

[442] Filipa CALVÃO, "O modelo de supervisão de tratamento de dados pessoais na União Europeia: da atual Diretiva ao futuro Regulamento", *FDPD,* n.º 1, julho de 2015, p. 40, disponível em https://www.cnpd.pt/bin/revistaforum/forum2015_1/index.html#40, consultado no dia 30 de setembro de 2018.
[443] V. o ponto 1.4.1. desta tese.
[444] O. LYNSKEY, *The Foundations of* cit., p. 9.

Em relação aos primeiros, veja-se, desde logo, o potencial de afirmação e estruturação do mercado interno da UE, uma das dimensões que identifiquei. Adicionalmente, entre os objetivos da reforma que culminou com o RGPD encontra-se a pretensão de estimular a confiança do titular dos dados pessoais enquanto consumidor da economia digital[445], uma premissa para o sucesso do Mercado Único Digital que consta das prioridades da UE para os próximos anos[446]. É este binómio antitético, por um lado, incentivar o desenvolvimento tecnológico e a digitalização da economia europeia e, por outro, precaver os riscos que esse processo coloca para os titulares dos dados pessoais, que orienta este regime[447].

Por fim, depois do que já foi dito, uma componente social é clara: prevenir os riscos para o titular dos dados pessoais provocados pelo tratamento dos seus dados pessoais [448]. A regulação prossegue interesses sociais de "primordial importância que transcendem, de algum modo, as puras condições de economicidade das atividades empresariais" [449]. No âmbito destes interesses sociais caberá a dimensão jusfundamental deste regime.

1.3.2.1.Manifestações de "co-regulação" e de "auto-regulação publicamente regulada"

No contexto da regulação de novas tecnologias e, em especial, do ciberespaço, destaca-se o conceito de "co-regulação" espelhando uma interação entre a lei (*hard law*) e os outros modos de intervenção (*soft law*). Funda-se no reconhecimento da importância de conciliar a dinâmica da regulação pública com diferentes modos de regulação privada, individual, comunitária, económica e técnica[450]. Como observa A. PEREIRA: "uma coisa

---

[445] Atente-se na redação dos considerandos 6 e 7 do RGPD a respeito da "rápida evolução tecnológica" e da "globalização" impondo "um quadro de proteção de dados sólido e mais coerente na União, apoiado por uma aplicação rigorosa das regras, pois é importante gerar a confiança necessária ao desenvolvimento da economia digital no conjunto do mercado interno. As pessoas singulares deverão poder controlar a utilização que é feita dos seus dados pessoais. Deverá ser reforçada a segurança jurídica e a segurança prática para as pessoas singulares, os operadores económicos e as autoridades públicas".

[446] Comissão Europeia, "Mercado Único Digital para a Europa: Comissão Europeia define 16 iniciativas para a sua concretização", 6 de maio de 2015, disponível em http://europa.eu/rapid/press-release_IP-15-4919_pt.htm, consultado no dia 30 de setembro de 2018. A 12.º iniciativa ali enunciada é a revisão da Diretiva 95/46.

[447] Rolf WEBER, "Transnational Data Privacy in the EU Digital Single Market", Dan SVANTESSON e Dariusz KLOZA (eds.), *Trans-atlantic data privacy as a challenge for democracy,* Intersentia, 2017, p. 5 e ss..

[448] O. LYNSKEY, *The Foundations of* cit., p. 77.

[449] E. Paz FERREIRA e L. MORAIS, "A Regulação sectorial ...", cit., p. 23 e O. LYNSKEY, *The Foundations of* cit., p. 78.

[450] A regulação privada, neste sentido, tem origem em *non state actors* e baseia-se em esquemas de *soft law* e não em mecanismos de direito privado, como o contrato. Cfr. Lokke MOEREL, "Export of the Rule of Law: Corporate Self-Regulation of Global Data Transfers", Sam MULLER *et alii, Law of the Future Series,* n.º 1, 2012, p. 353; M. E. GONÇALVES, *Direito* cit., p. 146 e ss.; Thibault VERBIEST e Etienne WÉRY, *Le Droit de L'Internet et de la Société de l'Information,* Larcier, 2001, p. 523.

é deixar tudo à auto-regulação, outra bem diferente é defender a intervenção do direito estadual quando essa auto-regulação não seja possível ou gere resultados contrários aos princípios fundamentais da ordem jurídica"[451].

Paralelamente, tem-se falado de uma postura do poder público, estadual e supraestadual, que, em vez de atuar diretamente, se mostra aberto a instrumentos de ativação do "potencial endógeno da sociedade" e do "património de conhecimentos, criatividade e da capacidade dos atores privados para resolver problemas"[452]. Certos domínios são permeados por uma estratégia de reforço da *responsabilidade* dos privados, no âmbito da sua esfera de atuação, reposicionando o seu papel na realização do bem comum, dando azo a uma nova forma regulatória: a "auto-regulação privada publicamente regulada" ou "provocada, ativada ou induzida" pelo poder público[453]. Este conceito constitui um *tertium genus* da "ação privada desregulada" e da "direção e planificação do Estado", ou seja, a sua essência encontra-se na "associação ou combinação ou mistura entre a mera ação privada e a regulação pública ou estadual, remetendo-nos imediatamente para a ideia de Estado regulador"[454]. Há, por isso, uma continuidade entre a ação privada e a ação pública espelhada na complementaridade entre ambas[455].

Creio que o legislador da UE, no RGPD, terá seguido esta estratégia. Desde logo, entre os seus propósitos encontra-se o incentivo das "iniciativas auto-reguladoras" e dos "regimes de certificação"[456] o que leva alguns autores a registar "uma mudança significativa de regulação tipo comando-e-controlo para a inclusão de ferramentas de co-regulação na legislação de proteção de dados pessoais"[457] ou o surgimento de "um sistema de auto-regulação híbrido com arranjos públicos" [458].

---

[451] A. Dias PEREIRA, *Direitos de* cit., p. 329.
[452] P. GONÇALVES, *Entidades Privadas com* cit., p. 14.
[453] P. GONÇALVES descreve um "novo cenário do Estado ativador" em que os privados assumem ou são convocados para desempenhar um novo papel, que partilham com o Estado, para realizar o interesse público: "Está aqui suposto, sim, o particular no seu estatuto de cidadão comprometido, empenhado e socialmente responsável (o "citoyen" e não o "bourgeois"), que procura e aceita contribuir para a realização do bem comum", podendo ser "induzido" ou obrigado a "assumir as suas responsabilidades próprias, quer na defesa dos seus direitos e interesses próprios, quer na proteção de interesses da coletividade", v. P. GONÇALVES, *Entidades Privadas com* cit., p. 15, 151, 161.
[454] *Idem,* p. 171.
[455] D. LOPES, *Eficácia* cit., p. 124.
[456] Comissão Europeia, "Uma abordagem..." cit., p. 13.
[457] Alberto GÓMEZ, "Los códigos de conducta en el reglamento general de protección de datos", J. Piñar MAÑAS *et alii* (coord.), *Reglamento General* cit., p. 389 e ss.; Carlos SÁNCHEZ e Miguel GAYO, "Certificación en protección de datos personales", J. Piñar MAÑAS *et alii* (coord.), *Reglamento General* cit., p. 413 e ss.; Irene KAMARA, "Co-regulation in EU personal data protection: the case of technical standards and the privacy by design standardisation 'mandate'", *EJLT,* vol. 8, n.º 1, 2017.
[458] L. MOEREL, "Export of the …" cit., p. 329 e ss..

Com efeito, os indícios da "auto-regulação privada publicamente regulada" e de "co-regulação" sobressaem no reconhecimento de efeitos jurídicos aos códigos de conduta destinados a "contribuir para a correta aplicação" da lei[459] e a procedimentos de certificação voluntária, selos e marcas de proteção de dados "para efeitos de comprovação da conformidade das operações de tratamento"[460].

Quanto à função destes instrumentos, visam, na perspetiva do titular dos dados pessoais, "reforçar a transparência" na medida em que lhe permitem avaliar rapidamente o nível de proteção proporcionado pelos produtos e serviços em causa e, na perspetiva dos utilizadores de dados pessoais, facilitam o cumprimento deste regime e adquirem relevo no momento da apreciação da respetiva responsabilidade[461]. Os artigos 24.º, n.º 3, 28.º, n.º 5, e o considerando 81 do RGPD determinam que a adesão àqueles instrumentos poderá indiciar a conformidade dos tratamentos de dados realizados. Do mesmo modo, nos termos do considerando 77, os códigos de conduta e as certificações aprovadas dão *orientações* sobre a execução de medidas e políticas adequadas e para a comprovação de conformidade com o RGPD. Por outro lado, de acordo com o art. 83.º, n.º 2, al. j), o cumprimento destes esquemas constitui um fator de mitigação na aplicação de coimas pela autoridade de controlo como, aliás, sucedeu no passado[462].

Além destas normas, o art. 21.º, n.º 5, dispõe que o direito de objeção por meios automatizados será exercido "utilizando especificações técnicas"; já os artigos 24.º, 25.º e 32.º impõem a adoção de "medidas técnicas e organizativas adequadas" [463]. Anteriormente, em 2015, a COM invocando, *inter alia*, o art. 8.º da CDFUE e a Diretiva, adotou uma Decisão de Implementação sobre a standardização no campo da política de proteção de dados e segurança e endereçou à *European Standardisation Organisation* um pedido de colaboração reconhecendo a importância deste tipo de iniciativas como

[459] Art. 40.º do RGPD.
[460] Art. 42.º do RGPD. O art. 27.º da Diretiva 95/46 remetia para os Estados-Membros e para a Comissão Europeia a "promoção e elaboração de códigos de conduta" para facilitar o cumprimento das normas ali prescritas tendo em atenção as "caraterísticas dos diferentes setores".
[461] Considerando 100 do RGPD e Comissão Europeia, "Uma abordagem ..." cit., p. 14.
[462] Kuan HON, *Data Localization Laws and Policy. The EU Data Protection International Transfers Restriction Through a Cloud Computing Lens*, Edward Elgar Publishing, 2017, p. 211. Algumas decisões das autoridades de controlo tomaram em conta certificações de segurança *standard* da indústria, obtidas pela Azure (Suécia), pela Google Appps (Noruega) e pela Moss (Noruega). Por seu turno, o G29 considerou que a "verificação ou certificação independente por um terceiro reputado pode ser uma forma credível" de demonstração de conformidade, v. G29, "Parecer 05/2012 relativo a computação em nuvem", de 1 de julho de 2012, p. 22 e 27.
[463] Eric LACHAUD, "The General Data Protection Regulation and the rise of certification as a regulatory instrument", *CLSR,* vol. 34, n.º 2, 2018, p. 244 e ss..

complemento da sua ação regulatória[464]. A remissão para "normas técnicas" reflete a constatação de que a proteção de dados pessoais não depende apenas de soluções estritamente jurídicas que exigem ser complementadas por meios tecnológicos e pelas "Ciências das Tecnologias"[465].

Contudo, noto que o RGPD não prevê um esquema de "auto-regulação pura" ou de "regulação privada desregulada" em cujo âmbito são prestados, livremente e numa lógica de mercado, serviços de certificação. O que se pretende criar é um sistema de regulação (ainda) *público* na medida em que é organizado pela UE, pelas autoridades de controlo ou por uma entidade privada investida da gestão do mesmo por um ato de delegação[466]. Esta opção foi motivada pelas lições de outros domínios, como o da certificação de produtos, sugerindo que a ausência de intervenção pública conduz a um nivelamento por baixo porquanto a concorrência entre fornecedores de serviços de certificação pode levar a uma redução dos preços e a uma certa flexibilidade ou relaxamento dos procedimentos[467].

Nesse sentido, o art. 43.º, n.º 9, do RGPD, remete para a COM a adoção de atos de execução "estabelecendo normas técnicas para os procedimentos de certificação e os selos e marcas em matéria de proteção de dados, e regras para promover e reconhecer esses procedimentos de certificação, selos e marcas"[468]. Do mesmo modo, segundo o art. 40.º, n.º 5, a produção de efeitos dos códigos de conduta depende de um processo de apreciação da sua conformidade com o interesse público a cargo da autoridade de controlo. Por outro lado, ainda que a supervisão do seu cumprimento possa ser efetuada por um organismo distinto da autoridade de controlo, tal não prejudica as competências desta que, aliás, o acredita[469]. Em sentido próximo, a competência para emitir a certificação é partilhada entre a autoridade de controlo e os organismos de certificação com base nos critérios aprovados pela primeira ou pelo CEPD[470]. Enfim, o recurso a

---

[464] Disponível em http://ec.europa.eu/growth/tools-databases/mandates/index.cfm?fuseaction=refSearch.search#, consultado no dia 30 de setembro de 2018. Desenvolvendo estes instrumentos, v. I. KAMARA, "Co-regulation in EU ..." cit., p. 14 e ss..

[465] F. CALVÃO, *Direito* cit., p. 31 e Jane WINN, "Technical standards as data protection regulation", S. GUTWIRTH *et alii*, *Reinventing* cit., p. 207.

[466] Sobre estes sistemas v. P. GONÇALVES, *Entidades Privadas* cit., p. 212.

[467] G29, "Parecer 3/2010 sobre o princípio da responsabilidade", 13 de julho de 2010, p. 19.

[468] Nos termos do procedimento previsto no art. 93.º, n.º 2 do RGPD.

[469] Art. 41.º, n.º 1 e 2 do RGPD.

[470] Estes organismos são entidades oficialmente habilitadas, reconhecidas ou acreditadas, que prestam serviços privados de certificação sem exercerem funções ou poderes públicos mas antes atividades privadas que, por terem relevância pública, ficam submetidas a regulação estadual, v. P. GONÇALVES, *Entidades Privadas* cit., p. 213 e artigos 42.º, n.º 5 e 43.º do RGPD. O organismo nacional de acreditação é designado nos termos do Regulamento 765/2008 do PE e do Conselho, em conformidade coma norma EN-ISSO/IEC

novos meios de regulação não aniquila uma intervenção pública que visa enquadrar e definir as condições jurídicas – materiais, formais ou organizativas – de desenvolvimento da auto-regulação privada aplicável aos tratamentos de dados pessoais.

Por conseguinte, a proteção de dados pessoais aproxima-se de um rumo, notado pela doutrina, de transformação das atuações administrativas, em relação a atividades económicas e direitos fundamentais, em intervenções meramente "certificativas ou declarativas e não autorizativas", acompanhadas pela substituição de atos prévios autorizativos que atestará "a menor intervenção pública na economia e a expansão da iniciativa económica" [471].

Esta solução simplifica a atuação administrativa (que deixa de ser prévia e autorizativa) e agiliza as atuações dos privados, mas impõe-lhes a assunção de responsabilidade[472]. Daí a centralidade do *princípio da responsabilidade* (art. 5.º, n.º 2 e 24.º do RGPD), um indicador do novo papel dos utilizadores de dados pessoais que vem descentralizar a proteção dos direitos fundamentais, ativar a quota de responsabilidade daqueles e deslocalizar a decisão sobre os riscos desses tratamentos. É desses riscos que cuido de seguida remetendo para mais adiante a apreciação daquele princípio.

1.3.2.2.Uma abordagem regulatória assente nos riscos dos tratamentos de dados pessoais

Já fui referindo os riscos dos novos tratamentos de dados pessoais surgidos com o desenvolvimento tecnológico. Mas, concretamente, que riscos são esses? A resposta a esta pergunta, lógica e cronologicamente, pode ser antecedida pela resposta a outra: será que as atividades que implicam o tratamento de dados pessoais se enquadram na chamada *regulação preventiva*[473]? Ou seja, os tratamentos de dados pessoais são perspetivados pelo legislador enquanto atividade causadora de "risco" que convoca uma tutela antecipada apesar da incerteza quanto à consumação de danos e à verificação de uma lesão no titular dos dados*?* Parece que sim[474].

17065/2012 e com os requisitos adicionais estabelecidos pela autoridade de controlo competente, v. artigos 43.º, n.º 1, al. b), 42.º, n.º 5 e 63.º do RGPD.

[471] D. LOPES, *Eficácia* cit., p. 268.

[472] *Ibidem*.

[473] Christopher HOOD, Henry ROTHSTEIN e Robert BALDWIN, *The Governance of Risk: Understanding Risk Regulation Regimes,* Oxford University Press, 2004, p. 3; D. VOGEL, *The Politics of Precaution* cit., p. 5 e ss.; J. WIENER *et alii* (eds.), *The Reality of Precaution* cit., p. 10 e ss..

[474] O que gerou críticas oriundas, sobretudo, dos EUA, v. Lucas BERGKAMP, "The Privacy Fallacy: Adverse Effects of Europe's Data Protection in an Information-Driven Economy", *CLSR,* vol. 18, n.º 1, 2002, p. 41: "é notável que os Estados tenham adotado legislação sem qualquer evidência tangível de dano ou ameaça

Em primeiro lugar, nas fontes internacionais deste regime e na legislação dos Estados-Membros que o antecedeu, a doutrina recolheu evidências que suportam esta resposta positiva[475]. Em segundo lugar, recordando a estrutura da relação jusfundamental no âmbito dos tratamentos de dados pessoais, esta compõe-se, *inter alia,* por um "causador de riscos" a um bem jusfundamental. A proteção desse bem é concretizada através de regulação *preventiva* dos riscos gerados pelos tratamentos de dados pessoais, isto é, pela antecipação de danos em detrimento de raciocínios baseados na causalidade. Tipicamente, a *risk regulation*, definida como "uma interferência pública no mercado ou em processos sociais para controlar consequências potencialmente adversas", decompõe-se em três elementos[476]:

(i) Criação de padrões comportamentais (*standard-setting*) traduzida, *in casu,* na estatuição das condições para os tratamentos de dados;

(ii) Monitorização (*monitoring*) pela autoridade de controlo; e

de dano, apenas com base numa vaga noção de direito fundamental e de riscos hipotéticos". Em sentido próximo, v. Neil RICHARDS, "The Dangers of Surveillance", *HLR*, n.º 126, 2013, p. 1935 e ss.

[475] Entre os exemplos de instrumentos regulatórios, nacionais e internacionais, assentes na prevenção de riscos contam-se: (i) o pioneiro diploma do Länder de Hesse, cujo art. 1.º, n.º 2, na sua versão de 1999, como nota L. BYGRAVE, visava "salvaguardar a estrutura constitucional do Estado (...) contra todos os riscos implicados pelo tratamento automatizado de dados", v. L. BYGRAVE, *Data Protection Law* cit., p. 5; (ii) na versão original das Diretrizes da OCDE, de 1980, o art. 2.º determinava a sua aplicação a "dados pessoais que, pela forma como são tratados (...) colocam em perigo a privacidade e as liberdades individuais". Vários autores perspetivam os regimes de proteção de dados como uma resposta aos riscos dos desenvolvimentos tecnológicos em geral, Christopher KUNER *et alii,* "Risk Management in Data Protection", *IDPL,* n.º 5, 2015, p. 95 e ss.; José Piñar MAÑAS, "Introducción. Hacia un nuevo modelo europeo de protección de datos", J. Piñar MAÑAS *et alii* (coord.), *Reglamento General* cit., p. 21; L. COSTA, "Privacy and the precautionary …" cit., p. 14 e ss.; Maria E. GONÇALVES, "The EU data protection reform and the challenges of big data: remaining uncertainties and ways forward", *ICTL,* vol. 26, n.º 2, 2017, p. 90 e ss.; Maximilian von GRAFENSTEIN, *The Principle of Purpose Limitation in Data Protection Law,* Nomos, 2017, p. 79 e ss.; Miguel GAYO, "Aproximación basada en el riesgo, evaluación de impacto relative a la protección de datos personales y consulta previa a la autoridad de control", J. Piñar MAÑAS *et alii* (coord.), *Reglamento General* cit., p. 351 e ss.; Raphael GELLERT, "Data protection: a risk regulation? Between the risk management of everything and the precautionary alternative", *IDPL,* vol. 5, n.º 1, 2015, p. 3 e ss. e, do mesmo autor, "We Have Always Managed Risks in Data Protection Law: Understanding the Similarities and Differences Between the Rights-Based and the Risk-based Approaches to Data Protection", *EDPL,* n.º 4, 2016, p. 481 e ss.; Viktor MAYER-SCHONBERGER, "Generational Development of Data Protection in Europe", Philip AGRE e Marc ROTENBERG (eds.), *Technology and Privacy: The New Landscape,* MIT Press, 1998, p. 225 e ss..

[476] C. HOOD, H. ROTHSTEIN e R. BALDWIN, *The Governance* cit., p. 3.

(iii) Modificação de comportamentos (*behaviour-modification*) visando corrigir e moldar[477] o comportamento dos utilizadores de dados pessoais na economia digital.

Em terceiro lugar, no decurso da reforma de 2012, o G29 pronunciou-se favoravelmente à adoção de uma *risk-based approach* como forma de mitigar as imposições aos utilizadores de dados pessoais e delimitar a conformidade que é exigida com critérios de proporcionalidade: "o Grupo de Trabalho reconhece que algumas das normas do Regulamento podem comportar encargos em alguns responsáveis pelo tratamento que podem ser percebidos como desequilibrados e, por isso, em opiniões anteriores sugeriu que todas as obrigações sejam adaptadas ao responsável pelo tratamento e às operações de tratamento em causa. A conformidade não deve ser um exercício formalístico [*box-ticking exercise*] (…). Por conseguinte, o Grupo de Trabalho entende que os responsáveis pelo tratamento devem atuar em conformidade com a lei, mas isto pode ser feito de maneira gradual"[478]. Note-se que esta não é uma conceção nova porquanto na própria Diretiva já se podiam encontrar (tímidos) reflexos deste tipo de abordagem[479].

O que acabo de referir confirma que este regime é um exemplo de regulação *preventiva*. Contudo, falta identificar quais são, afinal, os riscos decorrentes do tratamento de dados pessoais. Naturalmente que não é fácil calcular o número exato dos perigos pressentidos pelo legislador quando refletiu sobre a massificação e ubiquidade dos tratamentos de dados pessoais, o aprofundamento do Mercado Único Digital e novos tratamentos como, por exemplo, a definição de perfis[480] ou a computação em nuvem[481].

---

[477] Ou *un cambio de actitud* na sugestão de Luis ÁLVAREZ, "La responsabilidade del responsable", J. Piñar MAÑAS *et alii* (coord.), *Reglamento General* cit., p. 293.

[478] G29, "Statement on the …" cit., p. 2.

[479] Em relação ao nível de segurança dos dados pessoais (considerando 46 e art. 17.º, n.º 1), num reconhecimento de que certos tratamentos podem ocasionar riscos particulares e específicos para os direitos e liberdades das pessoas em causa, na exigência de controlo prévio (considerando 53 e 54 e art. 20.º), nas derrogações e restrições aos direitos do titular dos dados (art. 13.º, n.º 2 - a versão portuguesa fala em perigo, enquanto a inglesa refere o termo *risk*).

[480] Definida no art. 4.º, n.º 4, como "qualquer forma de tratamento automatizado de dados pessoais que consista em utilizar esses dados pessoais para avaliar certos aspetos de uma pessoa singular, nomeadamente para analisar ou prever aspetos relacionados com o seu desempenho profissional, a sua situação económica, saúde, preferências pessoais, interesses, fiabilidade, comportamento, localização ou deslocações".

[481] Atilla KISS e Gergely SZOKE, "Evolution or revolution? Steps forward to a new generation of data protection regulation", Serge GUTWIRTH *et alii* (eds.), *Reforming the European Data Protection Law,* Springer, 2015, p. 313 e ss.; C. Sarmento e CASTRO, "A jurisprudência ..." cit., p. 1048. A computação em nuvem é "Um tipo de computação em que são disponibilizadas, sob a forma de um serviço, capacidades escaláveis e elásticas de TI a vários clientes que utilizem tecnologias baseadas na Internet. Tipicamente, os serviços de computação em nuvem disponibilizam aplicações comuns em linha, a que os utilizadores têm

Já a Diretiva não os elencava o que deu espaço para várias críticas, gerou apelos a uma solução regulatória mais focada nos danos efetivamente causados pela utilização de dados pessoais e deu o mote a propostas de consagração expressa do *princípio da precaução* neste domínio[482]. Durante a reforma de 2012, o G29, na senda da OCDE, sugeriu uma conceção alargada de risco compreendendo *qualquer efeito adverso potencial ou efetivo,* incluindo efeitos sociais[483]. Na decisão *Digital Rights Ireland,* o TJ reconheceu os riscos da agregação de certos dados pessoais ("suscetíveis de permitir tirar conclusões muito precisas sobre a vida privada das pessoas cujos dados foram conservados"[484]) e da sua retenção ("gerar no espírito das pessoas em causa (...) a sensação de que a sua vida privada é constantemente vigiada"[485]).

Finalmente, devo ainda sublinhar que no RGPD a palavra "risco" aparece para cima de 70 vezes, pelo que é difícil contestar a opção do legislador por uma abordagem assente na imprevisibilidade ou na incerteza dos efeitos dos tratamentos de dados pessoais sobre o titular dos mesmos. Mas, sobretudo, essa solução decorre diretamente, *inter alia,* das seguintes disposições[486]:

(i) Logo no Preâmbulo o legislador regista a *perceção* social dos riscos, a "insegurança jurídica" e "um sentimento generalizado da opinião pública de que subsistem riscos significativos para a proteção das pessoas singulares, nomeadamente no que diz respeito às atividades por via eletrónica"[487];

---

acesso a partir de um navegador Web, enquanto o software e os dados são armazenados nos servidores. Neste sentido, a nuvem não é uma ilha, mas sim um conetor global das informações e utilizadores de todo o mundo", v. G29, "Parecer 1/2010 sobre os conceitos de "responsável pelo tratamento" e "subcontratante"", 16 de fevereiro de 2010, p. 10.

[482] L. BEGKAMP, "The Privacy Fallacy …" cit., p. 31 e 42; L. COSTA, "Privacy and the …" cit., p. 14 e ss. e O. LYNSKEY, *The Foundations of* ... cit., p. 81 e ss.. Sobre este princípio na legislação de privacidade, v. Adam THIERER, "Privacy Law's Precautionary Principle Problem", *MLR,* vol. 66, n.º 2, 2014, p. 468 e ss..

[483] G29, "Statement on the …" cit., p. 4. Sobre a OCDE, "Recommendation of the Council concerning guidelines governing the protection of privacy and transborder flows of personal data", alterada em 11 de julho de 2013, p. 24: "'Risco' é um conceito amplo, incluindo um número muito alargado de possíveis danos para o indivíduo".

[484] Acórdão do TJ, Digital Rights Ireland *et alii* c. Minister for Communications, Marine and Natural Resources *et alii,* C-293/12, 8 de abril de 2014, n.º 27.

[485] Acórdão do TJ, Digital Rights Ireland *et alii* c. Minister for Communications, Marine and Natural Resources *et alii,* C-293/12, 8 de abril de 2014, n.º 37.

[486] Aflorando medidas de mitigação dos "riscos para os titulares dos dados" como a pseudonimização (considerando 28), a propósito do consentimento de crianças e da falta de consciências dos "riscos inerentes ao tratamento" (considerando 65) e do "risco de erros" e de "potenciais riscos para os interesses e direitos do titular dos dados" como "efeitos discriminatórios" associados à definição de perfis (considerando 71),

[487] Considerando 9 do RGPD. Sobre a ideia de perceção social do risco, v. J. Pereira da SILVA, *Deveres* cit., p. 191.

(ii) O considerando 75 aflora o "risco para os direitos e liberdades das pessoas singulares" que "poderá resultar de operações de tratamento de dados pessoais suscetíveis de causar danos físicos, materiais ou imateriais", seguindo-se um elenco não exaustivo dos mesmos: a discriminação, usurpação ou roubo da identidade, perdas financeiras, prejuízos para a reputação, perdas de confidencialidade de dados pessoais protegidos por sigilo profissional, inversão não autorizada da pseudonimização, ou quaisquer outros prejuízos importantes de natureza económica ou social; uma privação dos direitos e liberdades do titular dos dados ou a impossibilidade de controlar os seus dados pessoais, entre outros riscos[488];

(iii) De harmonia com o considerando 76, a *probabilidade* e a *gravidade* destes riscos, sendo variáveis, devem ser avaliadas, de forma objetiva, tendo em conta os seguintes elementos: a natureza, o âmbito, o contexto e as finalidades do tratamento;

(iv) A obrigação *geral* de responsabilidade, firmada no art. 24.º, n.º 1, é medida em função do risco dos tratamentos de dados para os direitos e liberdades das pessoas singulares, daí que em boa parte se confunda com uma obrigação de "gestão adequada dos riscos" [489];

(v) A obrigação de assegurar um "nível de segurança adequada ao risco" (art. 32.º) e de notificar a autoridade de controlo em caso de violação de dados que "seja suscetível de resultar num risco para os direitos e liberdades das pessoas singulares (art. 33.º); e

(vi) A obrigação de realizar avaliações de impacto (art. 35.º) e de notificar o titular dos dados de uma violação (art. 34.º) quando os tratamentos de dados "impliquem um elevado risco" e, portanto, ultrapassam o "risco residual", isto

[488] Estes danos são reiterados no considerando 85 do RGPD.
[489] G29, "Orientações relativas à Avaliação de Impacto sobre a Proteção de Dados (AIPD) e que determinam se o tratamento é suscetível de resultar num elevado risco para efeitos do Regulamento (EU) 2016/679", 4 de outubro de 2017, p. 7.

> é, aquele que é tolerável e cuja prevenção é sempre contingente e na medida do possível[490].

Três conclusões entrelaçadas se apresentam por agora como incontornáveis: em primeiro lugar, este regime, em sintonia com o direito interno de alguns Estados-Membros[491], a opinião do G29[492] e a doutrina[493], não visa acautelar apenas danos materiais, como propôs alguma doutrina norte-americana[494]. Em segundo lugar, a inspiração preventiva deste regime formula-se do seguinte modo: havendo uma dúvida sobre a lesividade dos efeitos das atividades de tratamento de dados pessoais para o titular dos dados, a incerteza joga a favor deste impondo, aos utilizadores de dados pessoais, uma quota de responsabilidade e um conjunto de obrigações tendo em vista a "domesticação dos riscos"[495]. Em terceiro lugar, a probabilidade e a gravidade do risco que poderá resultar daquelas atividades é mensurável através de uma avaliação ou classificação distinguindo-se, desde logo, o risco residual do "risco elevado"[496]. Para M. GRAFENSTEIN, esta avaliação é o principal desafio deste tipo de abordagem[497].

A doutrina tem sublinhado a vocação universalizante e a difusão do princípio da precaução para domínios que extravasam o dos riscos ambientais, em especial ao nível

---

[490] "O risco residual é o perigo desqualificado, o risco cuja potencialidade lesiva já não obriga à adoção de medidas preventivas, ou simplesmente o risco que, em nome do bom senso, deve ser tolerado pela comunidade", v. Carla Amado GOMES, *Risco e Modificação do Ato Autorizativo Concretizador de Deveres de Proteção do Ambiente,* Coimbra Editora, 2007, p. 234 e 397, disponível em http://www.fd.unl.pt/docentes_docs/ma/cg_ma_17157.pdf, consultado no dia 30 de setembro de 2018; F. CALVÃO, *Direito* cit., p. 61, sugerindo um paralelismo com a avaliação de impacto ambiental.

[491] Em especial no Reino Unido, na decisão *Google Inc. v. Vidal-Hall and others,* apresentada no Court of Appeal, cfr. O. LYNSKEY, *The Foundations of* cit., p. 225. Acrescento que, a proposta inicial não aludia expressamente aos danos imateriais ou morais, tendo sido incluído posteriormente, por sugestão da Alemanha, da Eslováquia e da Suécia, v. Council of the EU, "Note from Presidency to Working Party on Information Exchange and Data Protection", 16 de dezembro de 2013, p. 540 a 544, disponível em http://www.consilium.europa.eu/en/meetings/mpo/2017/7/wp-on-information-exchange-and-data-protection-(258312)/, consultado no dia 30 de setembro de 2018.

[492] Num parecer de 1998 sobre transferências de dados pessoais afirma que "dano", na aceção da Diretiva 95/46, "inclui não apenas danos físicos e perdas financeiras, mas também qualquer prejuízo psicológico ou moral", v. G29, "Documento de Trabalho: Observações preliminares relativas ao uso de cláusulas contratuais no contexto da transferência de dados pessoais para países terceiros", 22 de abril de 1998, p. 14.

[493] O. LYNSKEY, *The Foundations of* cit., p. 196 e ss.: entre os danos intangíveis ou imateriais, a autora refere um sentimento de impotência do titular dos dados *vis-à-vis* o responsável pelo tratamento, a erosão da capacidade de autoapresentação, a inibição e o controlo de comportamentos individuais e a apreensão em relação a danos futuros.

[494] Eric GOLDMAN, "Data Mining and Attention Consumption", Katherine STRANDBURG e Daniela RAICU (eds), *Privacy and Technologies of Identity,* Springer, 2005, p. 225 e ss.; Ryan CALO, "The Boundaries of Privacy Harm", *ILJ,* n.º 86, 2011, p. 1153.

[495] A expressão é de C. Amado GOMES, *Risco e Modificação* cit., p. 174.

[496] Apresentando um conjunto de critérios para o definir, v. G29, "Orientações relativas à ..." cit., p. 9 e ss..

[497] M. GRAFENSTEIN, *The Principle* cit., p. 90.

do DUE[498]. Contudo, não há uma referência expressa a este princípio no regime em estudo contrariamente ao que acontece noutros domínios[499]. Se é verdade que este é um princípio marcado por uma "babilónica desordem conceitual", o legislador é claro quanto à noção de risco abraçada nos considerandos 75 e 76, cuja própria probabilidade é "variável", o que implica um grau de incerteza elevado. Tal poderá indicar uma proximidade deste regime a certas conceções do princípio da precaução[500].

As consequências de uma opção regulatória assente na precaução, em domínios permeados pela incerteza e pela permanente mudança tecnológica, são várias. Desde logo, geram-se as dúvidas comuns nesta sede, como a insegurança jurídica e científica na aplicação da precaução e um indesejável "clima de suspeição crónica" que paira sobre a mesma, e convocam-se os "riscos da precaução" [501]. Para C. AMADO GOMES, este princípio pode ser entendido numa aceção radical, "equívoca e perigosa": "legitimante de uma ação pública univocamente orientada para a preservação da segurança, com sacrifício inquestionado da liberdade"[502]. A autora assume uma "resistência à precaução", afirmando, entre outros aspetos, que "suprimir sistematicamente toda e qualquer possibilidade de risco é uma atitude que privilegia a segurança de forma desproporcionada em detrimento da liberdade, amputando a dignidade humana na sua vertente mais nobre"[503]. Outros autores são menos pessimistas e procuram combater os "mitos" em torno deste princípio[504].

Em segundo lugar, faz-se sentir o decréscimo de *determinabilidade* da legislação por força da sua impregnação por espaços em branco assim deixados para posterior

[498] Dando nota dessa tendência para "outros domínios jusfundamentais", v. Alexandra ARAGÃO, "Aplicação nacional do princípio da precaução", *Colóquios 2011-2012,* Associação dos Magistrados da Jurisdição Administrativa e Fiscal de Portugal, 2013, p. 159 e ss. e J. Pereira da SILVA, *Deveres* cit., p. 184. Equacionando o princípio da precaução no direito da proteção de dados pessoais e sugerindo um paralelismo com o direito do ambiente, v. F. CALVÃO, *Direito* cit., p. 61.

[499] Alexandra ARAGÃO, "Princípio da precaução: manual de instruções", *Revista do Cedoua*, vol. 2, n.º 11, 2008, p. 16 e ss..

[500] Para J. Pereira da SILVA o princípio da prevenção distingue-se do princípio da precaução por força dos pressupostos que acionam a sua aplicação: o primeiro, mobilizado para situações de *perigo* e, o segundo para situações de *risco*. As primeiras correspondem a uma "incerteza *quanto à probabilidade* da lesão do bem jurídico constitucional ou legalmente protegido" e, as situações de risco, a "uma incerteza *quanto à própria existência da probabilidade* dessa lesão", v. J. Pereira da SILVA, *Deveres* cit., p. 170 e 181. Por seu turno, C. Amado GOMES avança que "o risco é um perigo pressentido, mas não comprovado; o perigo é um risco de altíssima probabilidade. A fronteira entre os dois é, teoricamente, a da previsibilidade, que se debate com o ineliminável obstáculo da finitude do conhecimento humano", v. C. Amado GOMES, *Risco e Modificação* cit., p. 226.

[501] A. ARAGÃO, "Aplicação nacional do..." cit., p. 26 e C. Amado GOMES, *Risco e Modificação* cit., p. 244 e ss..

[502] *Ibidem*.

[503] *Ibidem*.

[504] A. ARAGÃO, "Aplicação nacional do..." cit., p. 23 e ss.

preenchimento à luz, por exemplo, de normas técnicas e de auto-regulação[505]. Como admite P. OTERO, "por paradoxal que possa ser (...) só uma intencional imperfeição ou incompletude de muitas das normas pode salvar as leis de uma vigência efémera em matéria de bem-estar e de prevenção de riscos"[506]. Convém ainda ter presente que a regulação dos tratamentos de dados pessoais padece do mesmo "mal" que a regulação da tecnologia em geral, descrito sob várias formas – *challenge of regulatory connection*[507], *pacing problem*[508], *Collingridge dilemma*[509] – para enunciar a rápida desatualização das soluções regulatórias em face da velocidade frenética da evolução tecnológica[510]. Daí a necessidade permanente, vertida no art. 97.º, do RGPD, de repensar e reconstruir as normas à luz dos novos tratamentos de dados pessoais e de reagir à medida dos estímulos das novas tecnologias[511]. Ou, como já foi dito, a proteção de dados pessoais é um "direito fundamental técnico" que requer atualização constante e, porventura, cada vez mais dependente, na sua efetivação, da própria tecnologia[512].

Em terceiro lugar, cabe indagar a *quem* compete avaliar e gerir os riscos associados ao tratamento de dados pessoais? O princípio da responsabilidade, estudado adiante, responderá a esta dúvida.

---

[505] C. Amado GOMES, *Risco e Modificação* p. 465 e ss. e J. Pereira da SILVA, *Deveres,* cit., p. 563 e 573; J. LOUREIRO, "Da sociedade ..." cit., p. 852. Sobre democracia, lei e tecnologia, v. Luís Cabral MONCADA, *Ensaio sobre a lei,* Coimbra Editora, 2002, p. 155 e, especificamente sobre o RGPD, v. Dag SCHARTUM, "Intelligible Data Protection Legislation", *OLR,* vol. 4, n.º 1, 2017, p. 48 e ss..

[506] P. OTERO, *Legalidade* cit., p. 159.

[507] Roger BROWNSWORD, *Rights, Regulation and the Technological Revolution,* Oxford University Press, 2008 e, do mesmo autor, *Law and Technologies of the Twenty-Century: Text and materials,* Cambridge University Press, 2012.

[508] Braden ALLENBY, "Governance and Technology Systems: The Challenge of Emerging Technologies", Gary Marchant *et alii* (eds.), *The Growing Gap between Emerging Technologies and Legal-Ethical Oversight,* vol. 7, Springer, 2011.

[509] David COLLINGRIDGE, *The Social Control Technology,* Pinter, 1980.

[510] Fred CATE *et alii,* "The (Data Privacy) Law Hasn't Even Checked in When Technology Takes Off", *IDPL,* vol. 4, n.º 3, 2014, p. 175.

[511] Aquela disposição prevê que, até ao dia 25 de maio de 2020 e, posteriormente, de quatro em quatro anos, a "Comissão apresenta ao Parlamento Europeu e ao Conselho um relatório sobre a avaliação e revisão do presente regulamento". Em sentido próximo, v. F. CALVÃO, *Direito* cit., p. 50 e C. Sarmento e CASTRO, "A jurisprudência ..." cit., p. 1059. Sobre a necessidade de atualização das soluções adotadas em matérias caraterizadas pela incerteza e mudança permanente, v. J. LOUREIRO, "Da sociedade ..." cit., p. 252; P. OTERO, *Legalidade,* cit., p. 293 e ss., p. 764 e ss. e p. 893 e ss..

[512] Paul DE HERT e Vagelis PAPAKONSTANTINOU, "Google Spain: Addressing Critiques and Misunderstandings One Year Later", *MJ,* vol. 22, n.º 4, 2015, p. 630 e Paul DE HERT, "The Right to Protection of Personal Data. Incapable of Autonomous Standing in the Basic EU Constituting Documents'", *UJIEL*, n.º 31, 2015, p. 1 e ss.. Julgo que essa é uma das premissas de A. Sousa PINHEIRO quando questiona se "a evolução tecnológica, e a consequente transformação das respostas jurídicas, não exige uma resposta distinta da fornecida pelo "direito à proteção de dados" nos moldes em que foi criado", v. A. Sousa PINHEIRO, *Privacy e proteção* cit., p. 63. Exemplo da transformação das respostas do direito é o conceito de *privacy by design* formalizado no art. 25.º do RGPD. Afirmando a dependência da tecnologia para garantir uma tutela efetiva dos dados pessoais, v. Woodrow HARTZOG, *Privacy's Blueprint. The Battle to Control the Design of New Technologies,* Harvard University Press, 2018.

1.4.Caraterísticas distintivas

Um dos traços particulares deste regime é, naturalmente, a sua natureza. Adicionalmente, por comparação com outros, designadamente o dos EUA, o regime estudado revela um conjunto de caraterísticas distintivas que o singularizam e que agrupo em duas categorias:

(i) O âmbito de aplicação alargado (1.4.1.); e
(ii) O conjunto de imposições concretas para os utilizadores de dados pessoais (1.4.2.).

1.4.1. Âmbito de aplicação alargado

Vários autores distinguem dois tipos de regimes aplicáveis aos tratamentos de dados pessoais: um alargado, cujo expoente máximo é o da UE; e outro, setorial, tipificado pelos EUA[513]. A amplitude do bloco normativo em análise decorre de dois elementos peculiares do mesmo: um *subjetivo*, respeitante aos sujeitos das relações jurídicas no âmbito do tratamento de dados pessoais, e outro *objetivo*, relativo ao objeto regulatório. Quem são aqueles *sujeitos*, que venho designando de utilizadores de dados pessoais, (1.4.1.1.) e sobre que realidade incide este regime (1.4.1.2.)?

1.4.1.1.Elemento subjetivo: os sujeitos das relações jurídicas no âmbito do tratamento de dados pessoais

1.4.1.1.1. As relações jurídicas tripolares e a horizontalidade do regime

Recordando a estrutura do direito fundamental à proteção de dados pessoais e retrocedendo um pouco na história da ação regulatória da UE, vislumbra-se a

[513] Abraham NEWMAN, *Protectors of Privacy. Regulating Personal Data in the Global Economy,* Cornell University Press, 2008, p. 23; Marc ROTENBERG, "Fair Information Practices And The Architecture of Privacy (What Larry Doesn't Get)", *STLR,* vol. 34, 2001, p. 13; Olga ESTADELLA-YUSTE, "The Draft Directive of the European Community Regarding the Protection of Personal Data", *ICLQ*, vol. 41, n.º 1, p. 170 e ss.; O. LYNSKEY, *The Foundations of* cit., p. 15. Entre nós, comparando os dois regimes, v. T. MOREIRA, *A Privacidade dos Trabalhadores* cit., p. 133 e ss. e A. Sousa PINHEIRO, *Privacy e proteção* cit., p. 20 e ss..

horizontalidade deste bloco normativo, isto é, a sua aplicação a utilizadores de dados pessoais independentemente da sua natureza pública ou privada.

Em primeiro lugar, de harmonia com aquela estrutura jusfundamental, a relação jurídica tripolar em nada obsta a que um dos sujeitos, o "causador de riscos", seja o próprio Estado ou uma entidade privada[514]. Aliás, como disse, os deveres de proteção de direitos fundamentais refletem uma transformação das funções da proteção jusfundamental que conjuga a função de prestação e de eficácia nas relações intersubjetivas privadas. Ou seja, o direito à proteção de dados pessoais é eficaz também nas relações jurídico privadas e não apenas na relação do titular dos dados pessoais com o Estado[515].

Em segundo lugar, olhando para trás, a discussão que antecedeu a adoção da Diretiva foi marcada pela discórdia quanto ao âmbito de aplicação subjetivo da mesma. Inicialmente, quando a COM apresentou a proposta original[516], público e privado apareciam regulados em capítulos distintos (Capítulo II para o setor público e Capítulo III para o privado). Esta solução não foi acolhida na proposta alterada[517], em conformidade com a Convenção n.º 108 do CdE, que não traça qualquer distinção[518]. Seja como for, as reações do setor privado não tardaram a repudiar a necessidade de uma intervenção regulatória[519].

Em todo o caso, a realidade confirma que cada vez mais os privados tratam dados pessoais e raramente o titular dos mesmos se encontra na melhor posição para se defender (autotutela) ou dispõe de instrumentos céleres para reagir (heterotutela). Estas circunstâncias fundamentam uma proteção ativa e legal que incide sobre a posição jusfundamental do titular dos dados pessoais, ao mesmo tempo que procede à restrição dos direitos contrapostos do agressor ou, por outras palavras, "a proteção faz-se à custa da restrição; a restrição faz-se à medida da proteção" [520]. Com efeito, o dever de proteção

[514] J. Pereira da SILVA, *Deveres* cit., p. 167 e 220.
[515] F. CALVÃO, *Direito* cit., p. 51.
[516] Proposta de diretiva do Conselho relativa à proteção das pessoas no que diz respeito ao tratamento dos dados pessoais, 24 de setembro de 1990.
[517] Proposta alterada de diretiva do Conselho relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à sua livre circulação, 18 de outubro de 1992.
[518] E continua sem a fazer nas definições apresentadas de *controller* e *processor* no art. 2.º.
[519] H. BURKERT, "Towards ..." cit., p. 339; A oposição por parte de associações industriais é manifesta na condenação da *Union of Industrial and Employer's Confederations of Europe* (UNICE), à data a maior organização comercial transetorial, v. "UNICE calls for Changes in Proposal on Personal Data", *European Report*, 1991, p. 3 e de outras, como a *European Direct Marketing Association* ou a *European Banking Federation*, v. "EC Scheme for Data Protection Stuns UK", *Marketing,* 12 de Julho de 1990, p. 3 e "Transnational Data and Communications Report", Novembro-Dezembro de 1992, p. 43 e ss..
[520] J. Pereira da SILVA, *Deveres* cit., p. 596.

tem por objeto, precisamente, a delimitação de esferas de sujeitos jurídicos que se encontram entre si numa relação equiordenada, deste modo estabelecendo relações de compatibilidade entre as esferas de liberdade individual dos vários sujeitos, recorrendo a uma intervenção legislativa de compressão de direito fundamentais[521]. Portanto, o titular dos dados pessoais é protegido através da compressão da liberdade de atuação do utilizador dos seus dados pessoais, também ele titular de uma posição jurídica garantida por um direito fundamental como, por exemplo, o direito de liberdade de empresa (art. 16.º CDFUE)[522].

Para estabelecer a horizontalidade deste regime o legislador muniu-se de conceitos *autónomos* e *funcionais* desdobrando em dois os utilizadores de dados pessoais: "responsável pelo tratamento" (RT) e "subcontratante" (ST). São conceitos *autónomos* no sentido em que devem ser hermeticamente interpretados, em conformidade apenas com as normas que compõem este corpo normativo, e *funcionais* porquanto visam atribuir a responsabilidade àqueles que exercem influência de facto sobre os tratamentos de dados pessoais, *independentemente da sua natureza orgânica pública ou privada*[523].

Em relação ao RT[524] – que corresponde ao "causador do risco" na relação tripolar no âmbito dos tratamentos de dados pessoais – a definição legislativa deste sujeito decompõe-se em três elementos[525]:

(i) Subjetivo: "a pessoa singular ou coletiva, *a autoridade pública, o serviço ou qualquer outro organismo*"[526];

(ii) Objetivo ou relacionado com a possibilidade de controlo coletivo: "que, individualmente ou em conjunto com outrem"; e

(iii) Um fator distintivo do RT em relação a outros intervenientes: "determina as finalidades e os meios de tratamento dos dados pessoais".

[521] *Idem*, p. 30, 149 e 150.
[522] Sobre os vários graus de afetação desvantajosa de um direito fundamental, do mero "limite" à "restrição", v. J. Pereira da SILVA, *Deveres* cit., p. 158; José de Melo ALEXANDRINO, *A Estruturação do Sistema de Direitos, Liberdades e Garantias na Constituição Portuguesa,* Vol. II, Almedina, p. 457 e ss..
[523] G29, "Parecer 1/2010 ..." cit., p. 2 e ss..
[524] O subcontratante será tratado em sede própria e mais à frente.
[525] Art. 4.º, n.º 7 do RGPD.
[526] Sublinhados meus.

Acontece que a apontada horizontalidade não é absoluta. Disso deu nota o G29, segundo o qual o RGPD concedeu "uma posição distinta ao setor público"[527]. É que este diploma alterou o art. 13.º da Diretiva[528] alargando, no art. 23.º, n.º 1, do RGPD, a margem de manobra dos Estados-Membros para limitar, por medida legislativa, o alcance de certas imposições, por razões amparadas em "objetivos importantes do interesse público geral da União ou de um dos Estado-membros"[529]. Esta opção do legislador por um conceito amplo e aberto de "interesse público geral" será um reflexo das divergências que pautaram as negociações do RGPD em torno da questão da sua desadequação para o setor público[530]. Mas outras duas disposições comportam refrações à mencionada horizontalidade: o art. 35.º, n.º 10, exclui da obrigação de realizar uma avaliação de impacto sobre a proteção de dados o tratamento "necessário ao exercício de funções de interesse público ou ao exercício da autoridade pública", e o art. 83.º, n.º 7, dispõe que a aplicação de coimas poderá visar apenas o setor privado.

Em todo o caso, a horizontalidade, ainda que amaciada por estas disposições, é uma das notas distintivas deste bloco de normas por comparação, por exemplo, com os EUA. Um diploma igualmente abrangente foi inicialmente proposto no Congresso norte-americano, mas, durante o debate legislativo, a pressão do setor privado fez valer o argumento da desproporcionalidade dos encargos e da burocracia que aquela proposta comportava[531]. Acabou por ser adotado o *Privacy Act*, em 1974, aplicável apenas ao tratamento de dados pessoais realizado por *agências federais*[532]. Além deste diploma, ao

---

[527] G29, "Parecer 01/2012 sobre as propostas de reforma em matéria de proteção de dados", 23 de março de 2012, p. 13.

[528] Esta norma concedia margem de manobra aos Estados-Membros para restringir o alcance de certas obrigações em benefício da proteção da segurança do Estado, da defesa, da segurança pública, da prevenção, investigação, deteção e repressão de infrações penais e de violações da deontologia das profissões regulamentadas, de um interesse económico ou financeiro importante de um Estado-Membro ou da UE, entre outros fundamentos.

[529] Uma alteração que foi sublinhada pelo SEPD, "Opinion of ..." cit., p. 83.

[530] Conselho da UE, "Working Party on Information Exchange and Data Protection (DAPIX) on 23-24 february 2012: Summary of Discussion", 8 de março de 2012, p. 5, disponível em http://register.consilium.europa.eu/doc/srv?l=EN&f=ST%207221%202012%20INIT, consultado no dia 30 de setembro de 2018. Avançando esta hipótese, O. LYNSKEY, *The Foundations of* cit., p. 22.

[531] Referindo-se à *s.3418 bill* P. REGAN explica que a mesma era "compreensiva no seu âmbito", v. Priscilla REGAN, *Legislating Privacy: Technology, Social Values, and Public Policy,* The University of North Carolina Press, 1995, p. 77. Também sobre este diploma, v. A. NEWMAN, *Protectors of Privacy* cit., p. 57 e ss. e Nadezhda PURTOVA, *Property Rights in Personal Data: A European Perspective,* Kluwer Law International, 2011, p. 109 e ss..

[532] *Privacy Act of 1974, 5 United States Code §552a.* Sobre esta evolução legislativa, v. A. Sousa PINHEIRO, *Privacy e proteção,* cit., p. 482; A. NEWMAN, *Protectors of Privacy* cit., p. 59; Joel REIDENBERG, "E-Commerce and Trans-Atlantic Privacy", *HLR,* n.º 38, 2001, p. 717 e ss.; N. PURTOVA, *Property Rights* cit., p. 109; O. LYNSKEY, *The Foundations of* cit., p. 17; P. SCHWARTZ e D. SOLOVE, *Information* cit., p. 20.

nível de cada Estado vigora legislação aplicável ao setor público e, nas respetivas constituições, há disposições específicas sobre o direito à *privacy*[533].

1.4.1.1.2. As relações jurídicas multipolares: o subcontratante e a autoridade de controlo

A relação jusfundamental em apreço desdobra-se noutros sujeitos, adquirindo uma forma multipolar, se atendermos ao papel do subcontratante e, em especial, da autoridade de controlo.

Em relação ao primeiro, a sua existência num caso concreto depende de uma escolha do RT, entre proceder ao tratamento dos dados pessoais no seio da sua organização ou delegá-lo, total ou parcialmente, numa organização externa. Por conseguinte, são duas as condições básicas para qualificar um ST:

(i) Trata-se de uma entidade jurídica distinta do RT que

(ii) procede ao tratamento dos dados pessoais por conta deste[534].

Em relação ao segundo sujeito, a supervisão deste conjunto de normas cabe a uma "autoridade de controlo"[535]. Este traço particular do regime estudado é hoje uma decorrência do direito primário (art. 16.º do TFUE e art. 8.º da CDFUE) e, segundo o TJ, constitui um "elemento essencial" deste direito fundamental[536]. Este é mais um elemento que nos distancia dos EUA: a proposta legislativa, na década de 70, de estabelecer o *Federal Privacy Board*, não foi aprovada por se ter considerado que tal viria a criar uma camada extra de burocracia e um "super regulador"[537]. Quanto à vocação das autoridades de controlo, de harmonia com os artigos 51.º, n.º 1 e 57.º do RGPD sob aquelas recai a "responsabilidade pela fiscalização" daquele diploma, controlando e executando a sua aplicação "a fim de defender os direitos e liberdades fundamentais das pessoas singulares

[533] P. SCHWARTZ e D. SOLOVE, *Information* cit., p. 36.
[534] G29, "Parecer 1/2010 ..." cit., p. 3.
[535] Capítulo VI do RGPD e art. 28.º da Diretiva.
[536] Acórdão do TJ, Maximillian Schrems c. Data Protection Commissioner, C-363/14, 6 de outubro de 2015, n.º 41 e jurisprudência aí citada.
[537] A. NEWMAN, *Protectors of Privacy,* cit., p. 23 e 57 e N. PURTOVA, *Property Rights,* cit., p. 109.

e facilitar a livre circulação desses dados na União". Em Portugal, cabe à CNPD, uma entidade administrativa independente, desempenhar esta função[538].

No RGPD há várias novidades em relação ao papel destes dois sujeitos. No que respeita ao ST, sobre este recaem agora, *ope legis* e não por via do contrato celebrado com o RT, as seguintes obrigações: registar as atividades de tratamento (art. 30.º, n.º 2); cooperar com a autoridade de controlo (art. 31.º); garantir a segurança do tratamento (art. 32.º); notificar uma violação de dados pessoais ao RT (art 33.º, n.º 2); designar o encarregado da proteção de dados (art. 37.º); e cumprir o regime das Transferências de dados pessoais (Capítulo 5).

Por seu turno, quanto às autoridades de controlo, uma das grandes alterações estruturais do RGPD prende-se com o modelo de supervisão: o controlo *ex ante* é substituído pela fiscalização *ex post*, eliminando-se, como regra, a supervisão prévia dos tratamentos de dados pessoais e transferindo a intervenção administrativa para o plano da orientação das condutas (através de orientações gerais e *soft law*) e, sobretudo, para o plano do controlo *a posteriori* dos tratamentos de dados pessoais[539].

A *ratio* desta opção legislativa vem plasmada no considerando 89, onde se explica que a supervisão prévia, através de uma "obrigação geral de notificação do tratamento de dados pessoais às autoridades de controlo"[540], originava "encargos administrativos e financeiros" e "nem sempre contribuiu para a melhoria da proteção dos dados pessoais", pelo que se suprime este método em prol de "regras e procedimentos eficazes mais centrados nos tipos de operações de tratamento suscetíveis de resultar num elevado risco para os direitos e liberdades das pessoas singulares"[541]. Nesta nova equação o princípio da responsabilidade do RT, adiante estudado, procura *compensar* ou *substituir* esta simplificação administrativa e a consequente ausência de controlo prévio externo,

---

[538] Carlos MORAIS, "As Autoridades Administrativas independentes na Ordem Jurídica Portuguesa", *ROA,* ano 61, n.º 1, 2001, p. 103 e ss; José CARDOSO, Autoridades Administrativas Independentes e Constituição, Coimbra Editora, 2002, p. 39 e ss.; M. C. CARDONA, *Contributo* cit., p. 50 e 527.

[539] F. CALVÃO, "O modelo de supervisão ..." cit., p. 37 e ss..; G29, "Parecer 3/2010 ..." cit., p. 18; L. ÁLVAREZ, "La responsabilidad ..." cit., p. 275 e ss.. A única exceção é a consulta prévia (art. 36.º do RGPD).

[540] Em Portugal os artigos 27.º e 28.º da Lei n.º 67/98, de 26 de outubro, regulavam este controlo.

[541] Sinalizando que esta é uma das vantagens deste novo modelo, v. Catarina Sarmento e CASTRO, "40 anos de 'Utilização da Informática – o artigo 35.º da Constituição da República Portuguesa", *EP,* vol. 3, n.º 3, 2016, p. 54, disponível online em http://e-publica.pt/volumes/v3n3/pdf/Vol.3-Nº3-Art.04.pdf, consultado no dia 30 de setembro de 2018: "O novo modelo tem inegáveis vantagens para aqueles – cidadãos, empresas, instituições públicas – que pretendam iniciar uma atividade, pública ou privada, que requeira o tratamento de dados pessoais, por afastar os entraves administrativos e temporais a que sempre se sujeita uma atividade dependente de autorização, incluindo os que necessitem de, no âmbito da prestação de serviços no mercado interno, fazer circular dados indispensável à circulação de bens e de serviços".

exigindo àquele a aplicação de medidas, determinadas em função do risco do tratamento e do tipo de dados tratados, para reforçar os mecanismos de controlo interno e a boa governação da proteção de dados[542].

No que concerne aos poderes e atribuições, as autoridades de controlo exercem, em conformidade com as garantias processuais, administrativas e penais, previstas no direito interno, poderes de investigação, de correção, poderes consultivos e de autorização, com total independência[543]. Cada deliberação das autoridades de controlo deve respeitar o princípio da proporcionalidade, o direito de todas as pessoas a serem ouvidas antes de tomada qualquer deliberação que as prejudiquem, e evitar custos supérfluos e excessivos para as pessoas em causa[544].

Neste campo o RGPD introduziu outra novidade em relação a estes sujeitos. Com efeito, respondendo a uma vulnerabilidade estrutural da Diretiva[545], o legislador reforçou os instrumentos de garantia ao dispor das autoridades, tendo em vista a eficácia e operatividade da fiscalização empreendida, reconhecendo-lhes, como sucede com uma parcela significativa das entidades administrativas independentes[546] e já sucedia em alguns Estados-Membros[547], poderes sancionatórios típicos da função jurisdicional, pelo que se pode afirmar que exercem poderes de tipo "para-jurisdicional" ou "quase jurisdicional"[548]. Assim, o exercício de poderes sancionatórios passou a estar consagrado no RGPD, segundo uma distinção implícita entre *sanções penais* e *sanções administrativas* (incluindo "coimas"), estas harmonizadas por via do regulamento que

[542] G29, "Parecer 3/2010 ..." cit., p. 2 e 16.
[543] Considerando 129 e artigos 52.º e ss. do RGPD.
[544] Considerando 129.
[545] Relatórios encomendados pela Comissão Europeia e outros estudos atestam a desadequação dos poderes das autoridades de controlo, abrindo a porta a um "défice de controlo" ou de *enforcement* deste regime, v. K. HON, *Data Localization* cit., p. 239.
[546] Paula Costa e SILVA, "As autoridades administrativas independentes", *O Direito,* ano 138.º, tomo III, 2006, p. 558; Vital MOREIRA e Fernanda MAÇAS, *Autoridades Reguladoras Independentes – Estudo e Projecto de Lei-Quadro,* Coimbra Editora, 2003, p. 40; P. COSTA, "Direito Administrativo..." cit., p. 53.
[547] Como é o caso de Portugal, segundo os artigos 35.º e ss. da Lei n.º 67/98, de 26 de outubro, bem como de outros países como o Reino Unido, v. Hazel GRANT e Hannah CROWTHER, "How Effective Are Fines in Enforcing Privacy?", David WRIGHT e Paul DE HERT, *Enforcing Privacy. Regulatory, Legal and Technological Approaches,* Springer, 2016, p. 287 e ss..
[548] Sobre as dúvidas em torno da verdadeira natureza – administrativa ou jurisdicional – da atividade de aplicação de sanções, v. P. COSTA, "Direito Administrativo..." cit., p. 53 e bibliografia aí citada. Há quem critique a atribuição de poderes sancionatórios a entidades administrativas por, tendencialmente, afastar a jurisdição dos tribunais, apesar da possibilidade de impugnação jurisdicional das decisões administrativas sancionatórias. Invoca-se a demora processual destas ações de impugnação que causam sérios prejuízos ao visado por força do decurso do tempo, v. P. COSTA E SILVA, "As autoridades administrativas ..." cit., p. 558. Descrevendo o papel das autoridades de controlo como *quase-judicial authorities* veja-se o estudo de Maria PORCEDDA, "Use of the Charter of Fundamental Rights by national data protection authorities and the EDPS", *RSCAS Research. Project Reports, Center for Judicial Cooperation,* Junho de 2017.

define os termos da violação que lhes subjaz, o montante máximo e o critério de fixação do valor[549].

O poder sancionatório tem a função de reforçar a efetividade da ação do legislador, potencia a sua influência (e das autoridades de controlo), dos seus comandos e proibições legais. Sucintamente, como refere P. GONÇALVES, cria para os "regulados um novo tipo de risco, *o risco regulatório da punição*"[550]. As lições dos Estados que, antes do RGPD, já previam este tipo de poderes confirmam o efeito preventivo que é imputado às normas sancionatórias, a dissuasão de más práticas e a influência dos comportamentos[551]. Como a seu tempo darei nota, 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. Por essa razão o poder sancionatório ficará fragilizado.

Por fim, uma última novidade do RGPD em relação às autoridades de controlo prende-se com a "europeização" da proteção de dados pessoais. Como referi, este processo conduzirá, no longo prazo, a uma estruturação de um *sistema administrativo europeu* para o mercado único da proteção de dados pessoais. O primeiro pilar desse sistema ergue-se com a reformulação do G29, que passa a CEPD, com a finalidade de "melhorar o seu contributo para a aplicação coerente da legislação em matéria de proteção de dados e fornecer uma base sólida de cooperação entre as autoridades de proteção de dados"[552]. O CEPD é um organismo da UE, dotado de personalidade jurídica, sendo representado pelo seu presidente e composto pelo diretor de uma autoridade de controlo de cada Estado-Membro, do SEPD[553] e um representante da CE (art 68.º). O CEPD é independente (art. 69.º) e goza de amplos poderes para-regulamentares (aconselhamento e emissão de diretrizes), de vários instrumentos unilaterais de "orientação" e de sugestão ou indução de comportamentos, de poderes de acreditação de organismos de certificação e de poderes de resolução de litígios entre autoridades de controlo (art. 65.º). A sua criação sugere uma situação de *partilha* ou *concorrência* de poderes com as autoridades

[549] Considerando 149 e 150, artigos 58.º, n.º 2, al. i), 83.º e 84.º do RGPD. Adicionalmente, o G29 publicou orientações sobre o exercício destes poderes, v. G29, "Guidelines on the application and setting of administrative fines for the purposes of the Regulation 2016/679", 3 de outubro de 2017.
[550] P. COSTA, "Direito Administrativo..." cit., p. 54.
[551] H. GRANT e H. CROWTHER, "How Effective Are …" cit., p. 290.
[552] Comissão Europeia, "Proteção da ..." cit, p. 10.
[553] Trata-se da autoridade de controlo responsável pela fiscalização dos tratamentos de dados realizados pelas instituições e órgãos da UE de harmonia com Regulamento 45/2001, do PE e do Conselho, de 18 de dezembro de 2000, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas instituições e pelos órgãos comunitários e à livre circulação desses dados.

de controlo nacionais dada a natureza complexa de algumas situações e procedimentos administrativos que congregam fases nacionais e europeias.

1.4.1.2.Elemento objetivo: objeto regulatório

1.4.1.2.1. Os conceitos de "tratamento" e de "dados pessoais"

A amplitude deste regime decorre também da opção legislativa de delimitação do objeto regulado. Com efeito, tal como a Diretiva[554], o RGPD consagra definições compreensivas de "tratamento de dados pessoais" ou, simplesmente, "tratamento" ("operação ou um conjunto de operações efetuados sobre dados pessoais ou sobre conjuntos de dados pessoais, por meios automatizados ou não automatizados, tais como a recolha, o registo, a organização, a estruturação, a conservação, a adaptação ou alteração, a recuperação, a consulta, a utilização, a divulgação por transmissão, difusão ou qualquer outra forma de disponibilização, a comparação ou interconexão, a limitação, o apagamento ou a destruição")[555] e de "dados 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 de identidade física, fisiológica, genética, mental, económica, cultural ou social dessa pessoa singular")[556].

Como sustentou o TJ no caso *Nowak,* "o emprego da expressão 'qualquer informação' no âmbito da definição do conceito de 'dado pessoal' (...) reflete o objetivo do legislador da União de atribuir um sentido amplo a esse conceito, que não está limitado

---

[554] Art. 2.º, alíneas a) e b): "'Dados pessoais', qualquer informação relativa a uma pessoa singular identificada ou identificável ("pessoa em causa"); é considerado identificável todo aquele que possa ser identificado, direta ou indiretamente, nomeadamente por referência a um número de identificação ou a um ou mais elementos específicos da sua identidade física, fisiológica, psíquica, económica, cultural ou social" e "'tratamento de dados pessoais' ("tratamento"), qualquer operação ou conjunto de operações efetuadas sobre dados pessoais, com ou sem meios automatizados, tais como a recolha, registo, organização, conservação, adaptação ou alteração, recuperação, consulta, utilização, comunicação por transmissão, difusão ou qualquer outra forma de colocação à disposição, com comparação ou conexão, bem como o bloqueio, apagamento ou destruição".

[555] Art. 4.º, n.º 2.

[556] Art. 4.º, n.º 1. Desenvolvendo este conceito, v. G29, "Parecer 4/2007 sobre o conceito de dados pessoais", 20 de junho de 2007 e, entre nós, António Menezes CORDEIRO, "Dados pessoais: conceito, extensão e limites", Centro de Investigação de Direito Privado da FDUL, 2018, disponível em https://blook.pt/publications/publication/e38a9928dbce/, consultado no dia 30 de setembro de 2018.

às informações sensíveis ou de ordem privada, mas engloba potencialmente qualquer tipo de informações, tanto objetivas como subjetivas sob forma de opiniões ou de apreciações, na condição de 'dizerem respeito' à pessoa em causa"[557]. Em sentido semelhante, o Advogado-Geral JAASKINEN observou que o âmbito de aplicação deste regime é "surpreendentemente vasto" e as suas definições "amplas" assim abrangendo um largo leque de situações de facto para acautelar ao máximo as incertezas do desenvolvimento tecnológico[558].

1.4.1.2.2. Transversalidade

Ainda no que respeita ao objeto regulado, sublinho uma outra opção legislativa distintiva: a transversalidade da matéria regulada, ou seja, regulam-se os tratamentos de dados pessoais independentemente da sua especificidade, da tecnologia em causa, do setor económico ou da sensibilidade da área[559]. Contudo, esta transversalidade não é absoluta.

O objeto deste trabalho restringe-se ao regime *geral,* distinto dos regimes *especiais* que com aquele convivem no ordenamento jurídico da UE. Os mais importantes são os seguintes:

(i) As telecomunicações eletrónicas, reguladas pela Diretiva *e-Privacy*, em processo de revisão na data em que escrevo[560];

(ii) A Diretiva sobre tratamento de dados pessoais pelas autoridades competentes para efeitos de prevenção, investigação, deteção ou repressão de infrações penais ou execução de sanções penais que constitui, na descrição do SEPD, um instrumento que "vale por si"[561];

[557] Acórdão do TJ, Peter Nowak c. Data Protection Commissioner*,* C-434/16, 20 de dezembro de 2017, n.º 34.
[558] Conclusões do AG no Acórdão do TJ, Google Spain SL e Google Inc. c. Agencia Española de Protección de Datos (AEPD) e Mario Costeja González*,* C-131/12, apresentadas em 25 de junho de 2013, n.º 29 e 30. Criticando esta amplitude, v. L. BERGKAMP, "The Privacy ..." cit., p. 31 e 42.
[559] A. NEWMAN, *Protectors of Privacy* cit., p. 23; O. ESTADELLA-YUSTE, "The Draft Directive…" cit., p. 22; P. SCHWARTZ e D. SOLOVE, *Information* cit., p. 1.
[560] Diretiva 2002/58/CE do PE 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.
[561] SEPD, "Opinion of the European…" cit., p. 6.

(iii) os tratamentos de dados pessoais realizados pelas instituições europeias[562];

(iv) Outros domínios cuja regulação cabe ao Estado-Membro, como a liberdade de expressão e de informação (art. 85.º do RGPD), o acesso do público a documentos oficiais (art. 86.º do RGPD), o número de identificação nacional (art. 87.º do RGPD), o contexto laboral (art. 88.º do RGPD), fins de arquivo de interesse público, de investigação científica ou histórica, fins estatísticos (art. 89.º do RGPD), obrigações de sigilo (art. 90.º do RGPD) e igrejas e associações religiosas (art. 91.º do RGPD).

Por conseguinte, em bom rigor, dir-se-á que na UE vigora um regime geral e vários regimes setoriais. Mais uma vez o contraponto encontra-se do outro lado do Atlântico onde não existe *qualquer* regime geral, mas vários regimes específicos. Na década de 70, a *Privacy Protection Study Commission*, criada no quadro do *Privacy Act,* concluiu que "ao invés de adotar normas gerais, a regulação do setor privado deve restringir-se a setores sensíveis"[563]. Desde então foram adotados vários diplomas setoriais, como por exemplo o *Video Privacy Protection Act*, de 1988[564].

1.4.2. As imposições para os utilizadores de dados pessoais: princípios, obrigações e direitos do titular dos dados pessoais

A proteção prevista neste corpo de normas materializa-se num conjunto de *imposições,* dirigidas essencialmente ao causador de risco ou RT, que conformam a sua liberdade de reger a respetiva organização e a sua atividade[565]. Ou, dito de outro modo, os tratamentos de dados pessoais são permitidos desde que realizados com respeito por um conjunto de condições[566]. Estas visam prosseguir e concretizar a vocação primordial da ação regulatória deste regime manifestada de forma contundente no RGPD:

[562] Regulamento 45/2001, do PE e do Conselho, de 18 de dezembro de 2000, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas instituições e pelos órgãos comunitários e à livre circulação desses dados.
[563] A. NEWMAN, *Protectors of Privacy* cit., p. 60.
[564] Entre outros, v. A. Sousa PINHEIRO, *Privacy e proteção,* cit., p. 477 e ss..
[565] Como referi só algumas obrigações são dirigidas ao subcontratante.
[566] Daí quem invoca um "efeito legitimador" dos tratamentos de dados pessoais por via do cumprimento destas condições (O. LYNSKEY, *The Foundations of* cit., p. 35) e, por seu turno, quem enfatiza que não há uma proibição de tratar dados pessoais (Winfried VEIL, "DS-GVO: Risikobasierter Ansatz statt rigidez Verbotsprinzip – Eine erste Bestandsaufnahme", *Zeitschrift fur Datenschutz,* vol. 5, n.º 8, 2015, p. 347 e ss.).

"persuadir", "incentivar", "instigar" uma governação responsável dos dados pessoais[567], orientar "uma mudança de atitude" na gestão daqueles dados[568] tendo em vista a tutela do titular dos dados pessoais.

Simultaneamente, findo o controlo prévio dos tratamentos de dados pessoais, pelas razões enunciadas no já mencionado considerando 89, o controlo dos mesmos como que é descentralizado e, em grande medida, delegado nos utilizadores de dados pessoais por via da ativação da respetiva quota de responsabilidade na proteção dos direitos fundamentais o que, na prática, se deve refletir em medidas internas concretas. Uma governação responsável passará pelo respeito por um conjunto de princípios e pelo cumprimento de obrigações (1.4.2.1), das quais saliento a obrigação de facilitar o exercício dos direitos do titular dos dados pessoais (1.4.2.2).

1.4.2.1. Os princípios relativos ao tratamento de dados pessoais, em especial o princípio da responsabilidade

Em larga medida inspirada pela Convenção n.º 108[569], a Diretiva elencava no art. 7.º os "princípios relativos à legitimidade do tratamento de dados" que aparecem agora no art. 5.º do RGPD sob a designação "princípios relativos ao tratamento de dados pessoais". Descritos como a "espinha dorsal" [570] da proteção de dados pessoais, entre eles contam-se: licitude, lealdade e transparência (art. 5.º, n.º 1, al. a) e art. 6.º); limitação das finalidades (art. 5.º, n.º 1, al. b)); minimização dos dados (art. 5.º, n.º 1, al. c)); exatidão (art. 5.º, n.º 1, al. d)); limitação da conservação (art. 5.º, n.º 1, al. e)); integridade e confidencialidade (art. 5.º, n.º 1, al. f)); e responsabilidade (art. 5.º, n.º 2).

Alguns destes princípios são concretizados noutras disposições. Por exemplo, o princípio da licitude significa que todos os tratamentos de dados pessoais se devem ancorar, sob pena de ilicitude (art. 5.º, n.º 1, alínea a) e art. 6.º do RGPD), num conjunto

---

[567] As expressões são do G29, "Parecer 3/2010 ..." cit., p. 5 e 6.
[568] L. ÁLVAREZ, "La responsabilidade ..." cit., p. 293.
[569] Comissão Europeia, "Handbook on Cost Effective Compliance with Directive 95/46/EC", Anexo ao "Annual Report 1998 (XV D/5047/98) of the Working Party Established by Article 29 of the Directive 95/46/EC", 1998, p. 18, disponível em http://ec.europa.eu/justice/data-protection/document/studies/files/19971001_ida_handbook_en.pdf, consultado no dia 30 de setembro de 2018.
[570] ICO, "Information Commissioner's Office: Initial Analysis of the European Commission's Proposals for a Revised Data Protection Legislative Framework", 27 de fevereiro de 2012, p. 8, disponível em https://wiki.laquadrature.net/images/1/12/Ico_initial_analysis_of_revised_eu_dp_legislative_proposals.pdf, consultado no dia 30 de setembro de 2018.

taxativo de "condições de licitude" ou fundamentos do tratamento: o consentimento do titular dos dados, a execução de um contrato ou de diligência pré-contratuais com o titular dos dados, o cumprimento de uma obrigação jurídica, a defesa de interesses vitais, o exercício de funções de interesse público ou exercício de autoridade pública, interesses legítimos prosseguidos pelo responsável pelo tratamento ou por terceiro[571]. Já o princípio da transparência implica que "deverá ser transparente para as pessoas singulares que os dados pessoais que lhes dizem respeito são recolhidos, utilizados, consultados ou sujeitos a qualquer outro tipo de tratamento e a medida em que os dados pessoais são ou virão a ser tratados"[572]. Visa, por conseguinte, implementar uma relação de transparência entre quem trata os dados pessoais e o titular dos mesmos que depende, entre outros aspetos, da prestação de informações nos termos dos artigos 12.º e ss..

Sem prejuízo de não representar uma grande novidade, a arquitetura de um sistema baseado no princípio da responsabilidade foi instigada pelo G29[573] . Como tive ocasião de explicar, o princípio da responsabilidade assume particular importância no seguimento da abolição do controlo prévio dos tratamentos de dados pessoais com o RGPD. Na verdade, a introdução deste princípio corporiza uma descentralização do controlo dos tratamentos de dados, antigamente concentrado na autoridade de controlo e, no fundo, viabiliza uma autorização prévia generalizada à realização de tratamentos de dados pessoais que prosseguirão de acordo com uma boa governação ou uma governação responsável[574]. Este princípio dá corpo a uma obrigação *geral,* plasmada no art. 24.º do RGPD, que reflete a tal ativação da quota de responsabilidade do RT no qual é delegado o dever de proteger os "direitos e liberdades das pessoas singulares relativamente ao tratamento dos seus dados"[575]. Só quando aqueles adaptam as suas práticas internas é que essa proteção pode "passar da teoria à prática" – o que se tornou um imperativo em face

[571] O G29 adotou várias orientações sobre estes fundamentos das quais destaco as seguintes: "Parecer 06/2014 sobre o conceito de interesses legítimos do responsável pelo tratamento de dados na aceção do artigo 7.º da Diretiva 95/46/CE", 9 de abril de 2014 e "Guidelines on consent under Regulation 2016/679", 10 de abril de 2018.
[572] Considerando 39 e G29, "Guidelines on transparency under Regulation 2016/679", 11 de abril de 2018.
[573] Há exemplos da sua presença na Diretiva, em especial no art. 6.º, n.º 2, que refere que "incumbe ao responsável pelo tratamento assegurar a observância do disposto no n.º 1", isto é, dos princípios relativos à qualidade dos dados ali enunciados; bem como no art. 17.º, n.º 1, que exige do RT a aplicação de medidas de natureza técnica e organizacional. Além do mais existe noutros domínios, como dos serviços financeiros, nos quais vigora uma obrigatoriedade de conformidade, v. G29, "Parecer 3/2010 ..." cit., p. 8. A primeira proposta encontra-se em G29, "The Future of Privacy. Joint contribution on the Consultation of the European Commission on the legal Framework for the fundamental right to protection of personal data", 1 de dezembro de 2009, n.^{os} 74 a 79. Remeto para este documento o detalhe sobre os precedentes deste princípio, em especial a OCDE, o Canadá e o quadro jurídico da APEC.
[574] G29, "Parecer 3/2010 ..." cit., p. 16.
[575] Considerando 78; G29, "Orientações relativas à ..." cit., p. 7.

da multiplicação dos riscos dos tipos de tratamentos dos dados pessoais no contexto de novas tecnologias e da globalização da economia[576].

Num parecer de 2010, o G29 enunciava três questões em torno deste princípio[577]: quais as medidas que concretizam a sua aplicação (1.4.2.1.1)? Como proporcionar e adaptar as medidas a circunstâncias específicas (1.4.2.1.2)? Quais as desvantagens desta nova abordagem (1.4.2.1.3)? Nos três pontos que se seguem procuro as respostas a estas questões vertidas no RGPD.

1.4.2.1.1. Quais as medidas de responsabilidade?

No RGPD o legislador não se limitou a proclamar, de forma genérica, o princípio da responsabilidade, mas desdobrou-o num conjunto de medidas concretas e práticas, em certas circunstâncias obrigatórias, de índole técnica e/ou organizativa.

Na prática, criou-se uma "caixa de ferramentas" para o RT implementar aquele princípio[578]. Entre essas ferramentas contam-se as seguintes:

(i) A adoção de políticas de proteção de dados a disponibilizar aos titulares dos dados pessoais[579] e de medidas técnicas, como a pseudonimização ou o controlo de acessos, para assegurar a "proteção de dados desde a conceção" e "por defeito"[580];

(ii) O recurso a subcontratantes que "apresentem garantias suficientes"[581];

(iii) O mapeamento das operações de tratamento, registando-as e gerindo um inventário das mesmas[582];

(iv) A designação de um encarregado de proteção de dados pessoais[583];

[576] G29, "Parecer 3/2010 ..." cit., p. 3, 4 e 20.
[577] *Idem*, p. 12.
[578] G29, "Parecer 3/2010 ..." cit., p. 13.
[579] Art. 24.º, n.º 2 e art. 12.º e ss. do RGPD.
[580] Art. 25.º do RGPD.
[581] Art. 28.º do RGPD.
[582] Art. 30.º do RGPD. Este registo é relevante para efeito de verificação da conformidade com o RGPD, v. F. CALVÃO, *Direito* cit., p. 62.
[583] Art. 37.º do RGPD.

(v) A criação de procedimentos para o exercício dos direitos do titular dos dados[584];

(vi) A elaboração de um plano de resposta que estabeleça as diretrizes de atuação, os procedimentos para a gestão, documentação e comunicação das violações de dados pessoais[585];

(vii) A realização de avaliações de impacto sobre a proteção de dados[586];

(viii) A aplicação e o controlo de procedimentos de verificação destinados a assegurar que as medidas existem não só no papel, mas que foram implementadas e funcionam na prática (auditorias internas ou externas)[587];

(ix) A implementação de medidas técnicas para garantir a segurança dos dados pessoais, como a pseudonimização ou a cifragem[588];

(x) A realização periódica de programas de formação, educação e sensibilização entre os colaboradores, com o intuito de compreender melhor a legislação aplicável assim como os procedimentos estabelecidos pelo RT para esse fim[589];

(xi) A cooperação com a autoridade de controlo em geral e nos termos da consulta prévia[590].

Sem prejuízo de me repetir, sublinho que a quota de responsabilidade que recai sobre o RT é distinta da que recai sobre o ST, excluído do art. 24.º, do RGPD, mas vinculado por um conjunto mais limitado de obrigações.

[584] Art. 12.º, n.º 2 do RGPD. Voltarei a este ponto adiante.
[585] Artigos 33.º e 34.º do RGPD.
[586] Artigos 35.º e 36.º do RGPD.
[587] G29, "Parecer 3/2010 ..." cit., p. 13.
[588] Art. 32.º do RGPD.
[589] G29, "Parecer 3/2010 ..." cit., p. 13.
[590] Artigos 31.º e 36.º do RGPD.

1.4.2.1.2. A adaptabilidade das medidas de responsabilidade

O RGPD não impõe o cumprimento, sem mais, de todas estas medidas, antes criando vários níveis de responsabilidade[591]. Algumas delas são elementos-chave impostos a *todos* os responsáveis pelo tratamento como é o caso, por exemplo, da criação de procedimentos para o exercício dos direitos do titular dos dados[592], da obrigação em relação à escolha de subcontratantes[593], da obrigação de cooperar com a autoridade de controlo[594] e, particularmente relevante, da obrigação geral de fazer uma "gestão adequada dos riscos" decorrentes do tratamento[595]. Como notou o G29, "por forma a gerir os riscos para os direitos e liberdades das pessoas singulares, os riscos têm de ser identificados, analisados, estimados, avaliados, tratados (p. ex. atenuados) e revistos regularmente"[596].

Outras medidas, como a segurança dos tratamentos, a notificação e a comunicação de uma violação de dados, a realização de uma avaliação de impacto e a consulta prévia ou a designação de um encarregado da proteção de dados, são aplicáveis "em função dos factos e das circunstâncias de cada caso"[597] atendendo, por exemplo, às "técnicas mais avançadas" e aos "custos da sua aplicação"[598], à "natureza, âmbito, contexto e finalidades do tratamento dos dados, bem como o risco que possa implicar para os direitos e liberdades das pessoas"[599] ou ao "elevado risco"[600] apurado casuisticamente. Por seu turno, a dimensão da organização poderá, em certas situações, conformar a obrigação de criar um registo das atividades de tratamento como, aliás, esclareceu o G29, invocando o considerando 13 do RGPD[601].

Ou seja, a quota de responsabilidade de cada RT não cabe toda na mesma bitola porquanto a diversidade, a inconstância e o policentrismo do risco dos tratamentos de

[591] L. ÁLVAREZ, "La responsabilidade ..." cit., p. 288 e G29, "Statement on the role …" cit., p. 3.
[592] Art. 12.º, n.º 2 do RGPD. Volto a este ponto adiante.
[593] Art. 28.º do RGPD.
[594] Art. 31.º do RGPD.
[595] G29, "Orientações relativas ..." cit., p. 7.
[596] *Ibidem*.
[597] G29, "Parecer 3/2010 ..." cit., p. 14.
[598] Artigos 25.º e. 32.º do RGPD.
[599] Considerando 74 do RGPD e artigos 24.º, 25.º, 32.º, 33.º, 35.º.
[600] Artigos 34.º, 35.º e 36.º do RFPD. Com efeito, a graduação do risco tem consequências legais, v. M. GRAFENSTEIN, *The Principle* cit., p. 80 e W. VEIL, "DS-GVO ..." cit., p. 351 e 352.
[601] Art. 30.º, n.º 5 do RGPD e G29, "Working Party 29 Position Paper on the derogations from the obligation to maintain records of processing activities pursuant to Article 30 (5) GDPR", 19 de abril de 2018. O considerando 13 *in fine* incentiva os Estados-Membros e as autoridades de controlo a "tomar em consideração as necessidades específicas das micro, pequenas e medias empresas no âmbito de aplicação do presente regulamento".

dados *in casu* inviabilizam a sua redução a um denominador comum, quer quanto aos limites, quer quanto a critérios de imputação de responsabilidade. Já aludi à opinião do G29 sobre o papel do risco na proteção de dados pessoais, descrevendo-o como uma solução para incutir proporcionalidade no cumprimento das medidas obrigatórias[602]. Por conseguinte, estas medidas, em especial a obrigação geral de gerir adequadamente o risco, serão adaptadas à situação e circunstâncias de cada RT[603].

1.4.2.1.3. As desvantagens de um sistema assente no princípio da responsabilidade

O G29 reconheceu que conjugar o princípio da responsabilidade com a lógica do risco incute flexibilidade na aplicação das soluções normativas, promove o "uso de linguagem aberta", gera insegurança jurídica quanto à conformidade exigida (*v.g.* "quando e como nomear um encarregado de proteção de dados, quando devem organizar sessões de formação") e origina "interpretações nacionais arbitrárias e divergentes sobre o âmbito e a natureza das obrigações"[604].

Contudo, o caminho para a conformidade de cada RT não poderia ser hermeticamente fixado pelo legislador numa fórmula mágica: "uma abordagem única obrigaria os responsáveis pelo tratamento a adotar estruturas inadequadas e, por fim, acabaria por falhar"[605]. Grandes organizações ou até pequenas ou médias que efetuem operações de tratamento que gerem mais riscos para os titulares dos dados pessoais devem aplicar medidas mais rigorosas por contraponto com organizações com menor risco[606]. A conformidade será sempre casuística e contextual ou, como sustentou o G29: "a adequação das medidas terá de ser decidida caso a caso. Incumbe aos responsáveis pelo tratamento tomar essas decisões, tendo por base as diretrizes emitidas pelas autoridades nacionais de proteção de dados e pelo Grupo de trabalho do artigo 29.º"[607].

Cabe a estas entidades compensar o clima de insegurança pela adoção de orientações[608]. O G29 sugeriu, inclusive, o desenvolvimento de "*um modelo de programa de conformidade dos dados,* que podia ser utilizado por organizações de média e de grande dimensão como elemento de base para a conceção dos seus programas

[602] G29, "Statement on the …" cit., p. 2 e ss..
[603] G29, "Parecer 3/2010 ..." cit., p. 21.
[604] *Idem*, p. 15.
[605] *Idem*, p. 14.
[606] *Ibidem*.
[607] *Ibidem*.
[608] G29, "Parecer 3/2010 ..." cit., p. 15.

específicos"[609]. No mesmo sentido, mais recentemente, a COM apelou a um esforço concertado entre as autoridades de controlo, Estados-Membros e utilizadores de dados pessoais, na implementação do RGPD[610]. Em especial, compete às primeiras, além de um papel pedagógico de clarificação da aplicação das regras, a promoção do diálogo e de uma cultura de comunicação com os utilizadores de dados pessoais. Este é um ponto reiterado por alguns autores que, à luz do tipo de abordagem regulatória, instigadora de novos comportamentos, defendem que a supervisão deverá assentar na *cooperação* e na *conversação* entre os utilizadores de dados pessoais e as autoridades de controlo: "a discussão contínua entre reguladores e regulados, no sentido da sua orientação para a conformidade, em detrimento do sancionamento agressivo, será o modo mais eficaz para maximizar o cumprimento de sistemas regulatórios complexos e imprecisos como este" [611]. Em muitos Estados, como por exemplo na Áustria, é essa a postura das autoridades de controlo[612].

Igualmente relevantes são as orientações retiradas dos procedimentos de certificação e dos códigos de conduta[613], bem como a obrigação das autoridades de controlo de elaborar e publicar uma lista dos tipos de operações de tratamento sujeitos ao requisito de avaliação de impacto[614] ou, ainda, as recomendações decorrentes de uma consulta prévia[615].

Como o G29 antecipou, as decorrências desta ativação da responsabilidade foram acolhidas com ceticismo pelos responsáveis pelo tratamento, como *custos de contexto* que obrigam a alocar meios financeiros e humanos para garantir a conformidade com o RGPD[616]. Como L. ÁLVAREZ observa, apesar da intenção expressa no considerando 89 no sentido de simplificar o enquadramento normativo dos tratamentos de dados pessoais,

---

[609] *Ibidem*.
[610] Comissão Europeia, "EU Data Protection Reform: a concerted effort to make it work. Fact Sheet", Janeiro 2018, disponível em https://ec.europa.eu/commission/sites/beta-political/files/data-protection-factsheet-who-does-what_en.pdf, consultado no dia 30 de setembro de 2018.
[611] K. HON, *Data Localization* cit., p. 242 e 243.
[612] Dando nota de uma estratégia de conciliação e de correção de desconformidades, v. Douwe KORF, "Existing case-law on compliance with data protection laws and principles in the member states of European Union: annex to the annual report 1998 (XV D-5047-98) of the working party established by article 29 of Directive 95-46-EC", Office for Official Publications of the European Communities, 1998, p. 40 e 55, disponível em https://searchworks.stanford.edu/view/4025981, consultado no dia 30 de setembro de 2018 e, do mesmo autor, "Comparative study on different approaches to new privacy challenges in particular in the light of technological developments: Working paper n.º 2 – Data Protection Laws in the EU: the difficulties in meeting the challenges posed by global social and technical developments", Comissão Europeia, 2010, p. 29, 101.
[613] Considerando 77 e G29, "Parecer 3/2010 ..." cit., p. 18.
[614] Art. 35.º, n.º 4 do RGPD.
[615] Art. 36.º, n.º 2 do RGPD.
[616] G29, "Parecer 3/2010 ..." cit., p. 11.

na prática esta solução impõe mais encargos[617]. Portanto, não será de estranhar que "alguns operadores no mercado europeu sustentam que o serviço fornecido irá encarecer, sendo repercutido no preço ao consumidor"[618]. Em todo o caso, o legislador aposta na tese de que o consumidor tenderá a escolher um operador que lhe oferece garantias de conformidade com as exigências legais pelo que uma boa governança em matéria de dados pessoais será uma vantagem concorrencial por potenciar a confiança do consumidor e contribuir para uma boa reputação[619].

Por seu turno, na perspetiva do titular dos dados pessoais, a doutrina adverte para a margem de manobra que o princípio da responsabilidade confere ao RT na determinação do grau de risco aceitável, por exemplo, do que seja "um nível de segurança adequado ao risco", o que pode gerar níveis de proteção desequilibrados, bem como problemas de concorrência desleal[620].

1.4.2.2.Os direitos do titular dos dados pessoais

Entre as obrigações enunciadas *supra* encontra-se a obrigação de facilitar o exercício dos direitos do titular dos dados pessoais de acordo com o art. 12.º, n.º 2. Na perspetiva deste, a proteção conferida não visa *per se* os dados pessoais, mas sobretudo, o *controlo* dos mesmos, tendo por base um princípio de autonomia deliberativa. Com a adoção do RGPD, o reforço desse controlo tornou-se um dos imperativos da dimensão jusfundamental deste regime[621].

Esta tarefa é concretizada por um conjunto de normas sobre *informação* que, além de corrigir assimetrias informacionais, reconhecem um lugar de relevo à vontade individual: um princípio nodal ali implícito é a *participação* do titular dos dados pessoais nas operações de tratamento dos utilizadores dos dados pessoais, o que lhe garante uma

---

[617] L. ÁLVAREZ, "La responsabilidade ..." cit., p. 283.
[618] C. Sarmento e CASTRO, "A jurisprudência ..." cit., p. 1069.
[619] *Ibidem*. Referindo o respeito pela proteção de dados pessoais como uma vantagem competitiva, v. Comissão Europeia, "Agreement on Commission's EU data protection reform will boost Digital Market", 15 de dezembro de 2015 e G29, "G29, "Parecer 3/2010 ..." cit., p. 5.
[620] M. GRAFENSTEIN, *The Principle of* cit., p. 90; Paul DE HERT e Vagelis PAPAKONSTANTINOU, "The proposed Data Protection Regulation Replacing Directive 95/46/EC: A Sound System for the Protection of Individuals", *CLSR,* n.º 28, 2012, p. 130 e ss.; R. GELLERT, "We Have …" cit., p. 16. Em sentido próximo Sarmento e CASTRO, reconhecendo os benefícios, duvida do novo modelo de supervisão: "não pode deixar de suscitar interrogações sobre o seu reflexo futuro na efetiva proteção dos dados pessoais, em face da reconhecida evolução tecnológica e das limitações da resposta dos titulares dos dados perante as sempre renovadas, e cada vez mais refinadas, ameaças.", v. C. Sarmento e CASTRO, "40 anos de ..." cit., p. 54 e 55.
[621] Comissão Europeia, "Uma abordagem ..." cit., p. 5 e Comissão Europeia, "Proteção da ..." cit., p. 2. Sobre a ideia do "controlo individual dos dados pessoais" v.*, inter alia,* O. LYNSKEY, *The Foundations of EU* cit., p. 177 e ss..

medida de *influência* dessas operações, realizada através de uma cartilha de direitos assegurados até nos casos em que a licitude do tratamento não decorre do seu consentimento[622].

O RGPD herda da Diretiva a cartilha daqueles direitos acrescentando-lhe algumas novidades, como, por exemplo, o direito de resposta, contemplado no art. 12.º, n.º 3 e 4, a portabilidade dos dados pessoais, prevista no art. 20.º, ou o direito contra decisões individuais e automatizadas, consagrado no art. 22.º, além de corrigir as divergências nacionais de implementação da Diretiva[623] e reforçar a relação de transparência tutelada, proporcionando às pessoas singulares meios para controlar os seus dados[624].

As regras gerais aplicáveis ao exercício destes direitos encontram-se no art. 12.º do RGPD, designadamente o prazo de resposta, as condições da recusa, entre outras. O exercício de alguns direitos depende somente destas condições prévias gerais, como é o caso do direito à confirmação do tratamento e ao acesso aos dados pessoais[625] e do direito de retificação[626]. Por seu turno, os demais direitos dependem de certas condições prévias como, por exemplo, de uma alteração das circunstâncias relativas ao tratamento, de uma condição de licitude do mesmo ou do exercício de outro direito: é o caso do direito ao apagamento[627], do direito à limitação do tratamento[628], do direito de portabilidade[629], do direito de oposição[630] e do direito em relação a decisões individuais e automatizadas[631]. Além das exceções previstas ao exercício de alguns destes direitos, plasmadas nos artigos

[622] L. BYGRAVE, *Data Protection Law* cit., p. 63 e ss..
[623] Plasmadas no "Primeiro relatório sobre a implementação da diretiva relativa à proteção de dados 95/46/CE", 15 de maio de 2003, p. 18, disponível em https://www.cnpd.pt/bin/actividade/Pri_rel_implementaDIR.pdf, consultado no dia 30 de setembro de 2018.
[624] Comissão Europeia, "Proteção da ..." cit, p. 7 e C. KUNER, "The European ..." cit., p. 10.
[625] Art. 15.º do RGPD.
[626] Art. 16.º do RGPD
[627] Art. 17.º do RGPD. Apenas reconhecido quando: os dados deixam de ser "necessários para a finalidade que motivou a sua recolha ou tratamento; o titular retira o consentimento e não existe outro fundamento; o titular opõe-se ao tratamento; o tratamento é ilícito; o apagamento por força de uma obrigação jurídca, entre outras circunstâncias.
[628] Art. 18.º do RGPD. Aplica-se apenas numa das seguintes situações: o titular contesta a exatidão dos dados pessoais; o tratamento é ilícitio e o titular opõe-se ao apagamento e solicita a limitação da utilização dos seus dados; o responsável pelo tratamento já não precisa dos dados, mas estes são requeridos pelo titular em sede de processo juidicial; o titular exerceu o direito de oposição.
[629] Art. 20.º do RGPD. Reconhecido apenas quando o tratamento se fundamenta no consentimento ou num contrato e é realizado por meios automatizados.
[630] Art. 21.º do RGPD. Em regra, vale apenas quando o tratamento se fundamenta no exercicio de funções de interesse público ou de autoridade pública ou nos interesses legítimos do responsável pelo tratamento (exceto nos casos de comercialização direta)
[631] Art. 22.º do RGPD. Este direito só é válido se o tratamento se basear numa obrigação jurídica, na defesa dos interesses vitais do titular dos dados, no exercicio de funções de interesse público ou de autoridade pública ou nos interesses legítimos do RT.

12.º, n.º 2, 15.º, n.º 4, 17.º, n.º 3, 20.º, n.º 4, 22.º, n.º 2, de acordo com o art. 23.º todos estes direitos podem se objeto de limitações legislativas.

Para terminar esta breve explicação dos direitos do titular dos dados[632], devo acrescentar que se encontram ao dispor do titular outras vias de recurso: pode apresentar uma reclamação a uma autoridade de controlo no Estado-Membro da sua residência habitual[633] e tem o direito a intentar uma ação judicial, nos termos do art. 47.º da CDFUE e dos artigos 78.º, 79.º e 82.º do RGPD.

Capítulo 2 – O âmbito de aplicação segundo o artigo 4.º da Diretiva e o artigo 3.º do RGPD

2.1. A natureza e estrutura do art. 4.º da Diretiva e do art. 3.º do RGPD

Numa análise da letra da lei salta à vista a distinção entre o art. 4.º da Diretiva e o art. 3.º do RGPD, desde logo nas respetivas epígrafes: "Direito nacional aplicável" e "âmbito de aplicação territorial". Pese embora esta distinção formal, a natureza destas disposições, de regras de conflitos unilaterais que delimitam o campo de aplicação das disposições materiais do ordenamento jurídico em que vigoram, é um fator de aproximação de ambas[634]. Citando o G29, ambas determinam "o âmbito de aplicação externo da legislação da UE em matéria de proteção de dados" e "em que medida ela é aplicável ao tratamento dos dados pessoais efetuado no todo ou em parte fora do espaço UE, mas que mantém uma ligação relevante com o território da UE"[635].

Em todo o caso, há aspetos substantivos que distinguem os dois artigos. O primeiro prende-se com a dupla função do art. 4.º da Diretiva: evitar conflitos e sobreposições entre as legislações nacionais dos Estados-Membros clarificando, no contexto interno, o âmbito de aplicação do direito nacional de cada um[636]. Ou seja, além

---

[632] Desenvolvendo v. Graça CANTO MONIZ, "Direitos do titular dos dados pessoais: o direito à portabilidade", Francisco PEREIRA COUTINHO e Graça CANTO MONIZ, *Anuário da proteção de dados,* CEDIS, 2018, p. 11 e ss..

[633] Art. 77.º do RGPD.

[634] C. KUNER, *Transborder* cit., p. 109; Maria ASINARI, "International Aspects of Personal Data Protection: *Quo Vadis EU?*, Maria ASINARI e Pablo PALAZZI (eds.), *Challenges of Privacy and Data Protection Law,* Buylant 2008, p. 405; M. BRKAN, "Data Protection …" cit., p. 333; P. ASENSIO, "Competencia …" cit., p. 75.

[635] G29, "Parecer 8/2010 sobre a lei aplicável", 16 de dezembro de 2010, p. 6.

[636] *Idem*, p. 9. Aflorando esta dupla função, v. Conclusões do AG no Acórdão do TJ, Weltimmo s. r. o. c. Nemzeti Adatvédelmi és Információszabadság Hatóság*,* C-230/14, apresentadas em 25 de junho de 2015, n.º 23; M. GOMANN, "The new territorial …" cit., p. 572; Santiago Ripol CARULLA, "Aplicación Territorial

da dimensão externa, o art. 4.º desempenhava uma importante função interna ou de distribuição do direito nacional aplicável. Pelo que toca ao RGPD, essa função encontra-se substancialmente atenuada dada a sua natureza uniformizadora do direito nacional dos Estados-Membros[637]. Por conseguinte, *prima facie,* se a Diretiva previa critérios para determinar a lei nacional, num Regulamento esses critérios de distribuição das leis nacionais deixariam de ser necessários[638].

O segundo aspeto diferenciador é a referência no RGPD a ST, com as implicações já identificadas em relação às obrigações que sobre este sujeito recaem por força da própria lei. Por fim, para aquilo que mais interessa neste trabalho, estas disposições distinguir-se-ão quanto aos critérios que conformam o tal "âmbito de aplicação externo" ou a extraterritorialidade deste regime. Para o G29, o art. 4.º alargava "muito o âmbito de aplicação, com implicações jurídicas que se estendem para lá do território da UE"[639]. Explicar como se processa esse alargamento é o objetivo dos próximos pontos.

2.2. Os critérios para determinar o âmbito de aplicação da Diretiva segundo o art. 4.º

Com efeito, segundo o G29, esta norma era aplicável num "contexto internacional mais vasto" e a "situações com ligações a vários países" [640]. Porém, nem sempre foi fácil apurar essas situações. Toda a razão assiste a L. BYGRAVE quando, comentando a Diretiva, sugere que o art. 4.º era o "mais controverso, mal compreendido e o mais misterioso" de todo o seu articulado – o que, aliás, explicará as transposições divergentes desta disposição[641]. De facto, um estudo encomendado pela COM sobre a implementação da Diretiva salientava a existência de "graves problemas com a implementação do art. 4.º" sublinhando que "esta norma não é nem plena nem adequada ou consistentemente

---

del Reglamento", J. Piñar MAÑAS, *Reglamento General de Protección de Datos. Hacia un nuevo modelo europeo de privacidade,* Reus, 2016, p. 77 e ss..

[637] M. BRKAN, "Data Protection …" cit., p. 336 e ss. e M. GOMANN, "The new territorial …" cit., p. 574.

[638] Contudo, é concedida alguma margem de manobra aos Estados para a adoção de legislação específica em certos domínios (*v.g.* artigos 6.º, n.º 2, 8.º, 9.º, n.º 4, 85.º e ss.) o que tem gerados dúvidas sobre os critérios para distribuir essa legislação, v. M. BRKAN, "Data Protection …" cit., p. 336. Por exemplo, o Estado-Membro "A" considera o consentimento válido para crianças apenas aos 14 anos (menos do que os 16 anos do RGPD) e uma criança desse Estado-Membro abre uma conta de e-mail de um prestador de serviços estabelecido no Estado-Membro "B" cuja regra do consentimento são 16 anos. Qual a lei aplicável aos requisitos do consentimento? Alertando para este ponto, v. SEPD, "Opinion of the ..." cit., p. 17.

[639] G29, "Parecer 8/2010 ..." p. 10.

[640] *Idem*, p. 2.

[641] D. SVANTESSON, "Article 4 …" cit., p. 210 e ss. e, do mesmo autor, "Extraterritoriality …" cit., p. 226 e ss.; Lee BYGRAVE, *Data Privacy Law: An International Perspective,* Oxford University Press, 2014, p. 199; L. COLONNA, *Legal* cit., p. 339; M. BRKAN, "Data Protection …" cit., p. 325; Lokke MOEREL, *Binding Corporate Rules: Corporate Self-Regulation of Global Data Transfers,* Oxford University Press, 2012, p. 74.

aplicada pelos Estados-Membros" o que se devia à sua "excessiva complexidade" que convidava a "divergências na transposição" para o direito interno e, consequentemente, a uma aplicação diferente[642].

Na perspetiva dos operadores transnacionais, aquela era a disposição mais importante da Diretiva, uma vez que estipulava a (não) aplicabilidade da mesma às respetivas atividades. Por outro lado, é indiscutível a sua importância do ponto de vista do titular dos dados pessoais, o beneficiário e titular do bem jurídico protegido, uma vez que era o art. 4.º que traçava os termos e limites da proteção que o legislador lhe garantia. Tendo em conta esta importância prática, é paradoxal que os seus elementos centrais tenham permanecido imprecisos durante longo período, em particular até ao G29, em 2010, se pronunciar sobre os mesmos num parecer[643].

O art. 4.º prevê a aplicação da Diretiva ao tratamento de dados pessoais quando este: "a) for efetuado no contexto das atividades de um estabelecimento do responsável pelo tratamento situado no território desse Estado-membro; se o mesmo responsável pelo tratamento estiver estabelecido no território de vários Estados-membros, deverá tomar as medidas necessárias para garantir que cada um desses estabelecimentos cumpra as obrigações estabelecidas no direito nacional que lhe for aplicável"; "b) o responsável pelo tratamento não estiver estabelecido no território do Estado-membro, mas num local onde a sua legislação nacional seja aplicável por força do direito internacional público" e, ainda, "c) o responsável pelo tratamento não estiver estabelecido no território da Comunidade e recorrer, para tratamento de dados pessoais, a meios automatizados ou não, situados no território desse Estado-membro, salvo se esses meios só forem utilizados para trânsito no território da Comunidade". Por fim, o número 2 dispõe que o RT abrangido pela alínea c) deve designar um "representante".

Isto dito há que averiguar o seguinte: qual destas alíneas determina que o regime em apreço aspira a regular a "conduta de pessoas, bens ou atos" além das fronteiras da UE? Para responder a esta pergunta e, portanto, compreender o alargamento deste regime "para lá do território da UE", há que apurar o significado de alguns dos conceitos usados pelo legislador naquelas alíneas.

---

[642] Douwe KORFF, "EC Study on Implementation of Data Protection Directive. Comparative Summary of national laws", setembro de 2002, p. 42 e ss., disponível em http://194.242.234.211/documents/10160/10704/Stato+di+attuazione+della+Direttiva+95-46-CE, consultado no dia 30 de setembro de 2018.

[643] G29, "Parecer 8/2010 sobre a lei aplicável", 16 de dezembro de 2010.

2.2.1. A localização de um estabelecimento do RT

Segundo o art. 4.º, n.º 1, al. a), a Diretiva é aplicável aos "tratamentos de dados pessoais" realizados no "contexto das atividades de um estabelecimento do responsável pelo tratamento situado no território" de um Estado-Membro.

O G29 esclareceu que a "Diretiva associa a aplicabilidade da legislação de proteção de dados de um Estado-Membro ao tratamento de dados pessoais"[644], um conceito definido no art. 2.º, al. b), daquele diploma. Em segundo lugar, a aplicação deste artigo depende da identificação do RT, um conceito também já tratado noutra parte deste trabalho. Por conseguinte, falta apenas explicar o que se entende por "contexto das atividades de um estabelecimento".

2.2.1.1. "Contexto das atividades de um estabelecimento". O caso *Google Spain* e o caso *Weltimmo*

Seguindo pelo enunciado do art. 4.º, o legislador não refere que o tratamento em si mesmo tem de ocorrer no território de um Estado-Membro, ou que o estabelecimento é *o* RT[645]. Do mesmo modo, também não exige que seja o estabelecimento a realizar as operações de tratamento[646]. Para o G29, "o conceito de 'contexto de atividades' não implica que a lei aplicável seja a lei do Estado-Membro em que o *responsável pelo tratamento está estabelecido,* mas sim a do país em que um *estabelecimento* do responsável desenvolve *atividades* ligadas ao tratamento de dados"[647]. Por conseguinte, tal sugere que a Diretiva regula os tratamentos de dados pessoais que ocorrem fora do território do Estado-Membro, se realizados no contexto das atividades de um estabelecimento do RT, *podendo este estar sedeado ou registado no estrangeiro*[648].

Todo o problema está, afinal, em apurar o que é um "estabelecimento", e quando é que o tratamento ocorre no "contexto" das suas atividades. O primeiro conceito não goza de tratamento uniforme no DUE e adquire contornos específicos no regime estudado[649].

---

[644] *Idem*, p. 14.
[645] Como explica o G29 "o conceito de estabelecimento tem ligações flexíveis com o conceito de responsabilidade pelo tratamento", v. G29, "Parecer 8/2010 ..." cit., p. 12.
[646] E. USTARAN, "The Scope…" cit., p. 144; L. MOEREL, "Back to .." cit., p. 97 e, da mesma autora, "The long …" cit., p. 30.
[647] G29, "Parecer 8/2010 ..." cit., p. 14.
[648] *Idem*, p. 9,10 e 14: "mesmo que o responsável pelo tratamento tenha o seu estabelecimento principal num país terceiro, basta ter um dos seus estabelecimentos num Estado-Membro para que seja aplicável a lei deste país, desde que estejam preenchidas as outras condições previstas no artigo 4.º, n.º 1, alínea a)".
[649] B. ALSENOY, "Reconciling …" cit., p. 80 e J. SCOTT, "The new ..." cit., p. 1352.

De harmonia com o considerando 19 um estabelecimento "pressupõe o *exercício efetivo e real* de uma *atividade* mediante uma *instalação estável*; (...) para o efeito, a *forma jurídica* de tal estabelecimento, quer se trate de uma simples sucursal ou de uma filial com personalidade jurídica, *não é determinante*"[650].

Examinando estes conceitos C. KUNER conclui que "o regime de proteção de dados nunca será aplicado consoante a forma corporativa ou jurídica como uma dada empresa está estruturada"[651]. O autor sublinha a facilidade com que algumas autoridades de controlo imputaram à empresa-mãe, situada no estrangeiro, obrigações decorrentes da legislação nacional de transposição da Diretiva do Estado-Membro onde aquela tem uma subsidiária – um estabelecimento, portanto[652]. Este raciocínio, de considerar a empresa-mãe e as subsidiárias como um *operador económico único*, corresponde a uma aplicação da teoria da "unidade económica", recorrente no direito da concorrência, através de um processo de "levantar o véu corporativo" (*lift the corporate veil*), isto é, nega-se ou, pelo menos, relativiza-se, a personalidade jurídica da empresa-mãe, pondo de parte o facto de que ela constitui um sujeito de direito distinto da sua subsidiária[653].

Porém, este processo não deverá ser automático: o tratamento em causa deve ser efetuado no "contexto das atividades" do estabelecimento do utilizador dos dados pessoais. Acontece que esta é uma exigência que não foi levada à letra pelas autoridades de controlo que, por exemplo, em países como a Finlândia e a Suécia, se satisfaziam com a existência de um qualquer tipo de atividade económica da empresa-mãe, nos respetivos territórios, para concluir que esta tem ali um estabelecimento e, só por isso, aplicar a legislação respetiva[654]. Esta prática foi amparada pela transposição errada da Diretiva, em especial do art. 4.º, da qual não constava a expressão "no contexto das atividades de um estabelecimento"[655]. Acompanhando aquelas entidades, os tribunais nacionais prosseguiram raciocínios semelhantes[656].

Com efeito, o problema é que desde a adoção da Diretiva que existe uma enorme opacidade e controvérsia em torno da expressão "contexto das atividades de um

[650] Considerando 19 da Diretiva.
[651] Christopher KUNER, *European Data Protection Law. Corporate Compliance and Regulation,* Oxford University Press, 2007, p. 129.
[652] *Idem*, p. 118, citando o exemplo da Finlândia e da Suécia.
[653] *Ibidem*.
[654] *Ibidem*.
[655] C. KUNER, *European* cit., p. 118.
[656] Kuan HON, Julia HORNLE e Christopher MILLARD, "Data Protection Jurisdiction and Cloud Computing – When are Cloud Users and Providers Subject to EU Data Protection Law? The Cloud of Unknowing, Part 3", *IRLCT*, vol. 26, n.º 3, 2012, p. 129 e ss., apresentando um caso italiano, de 2010, de certo modo antecipando a decisão do TJ *Google Spain,* analisada mais à frente.

estabelecimento"[657]. O G29 sugeriu a aplicação de um teste ao estilo de "quem faz o quê" e uma avaliação casuística[658]. Por seu turno, em alguns países, as autoridades de controlo foram mais longe na concretização desta expressão enunciando algumas situações nas quais a empresa-mãe seria abrangida pela legislação da UE como, por exemplo, se é aquela quem gere um sítio *web* através do qual recolhe dados pessoais de utilizadores situados num Estado-Membro, participa na administração dos dados pessoais dos utilizadores do sítio *web* e assume-se como responsável da parte redigida em língua alemã desse sítio *web* [659].

Admitindo a existência de "zonas cinzentas" que merecem esclarecimentos adicionais, a doutrina sugere alguns exemplos de situações nas quais o tratamento de dados pessoais ocorre no "contexto das atividades de um estabelecimento", mas as operações que lhe subjazem são realizadas pelo estabelecimento principal da empresa fora da UE[660]. L. MOEREL, inspirando-se no exemplo apresentado pelo G29[661], refere o caso das empresas multinacionais que tratam os dados pessoais de forma centralizada: se a empresa-mãe trata os dados dos recursos humanos de forma centralizada, numa base de dados única, das empresas do seu grupo situadas na UE, a autora defende que o regime de proteção de dados pessoais da UE aplicar-se-á a essas partes do tratamento de dados pessoais porque estão relacionados com as atividades dos seus estabelecimentos situados na UE [662]. Outro caso apontado pela mesma autora é semelhante ao sugerido por algumas autoridades de controlo: quando é a empresa-mãe quem opera um sítio *web* que trata os dados pessoais dos visitantes do Estado-Membro onde se encontra o seu estabelecimento, se o estabelecimento é responsável pelas relações com os utilizadores num Estado-Membro (*v. g.* se é ao estabelecimento que cabe a distribuição e o acompanhamento pós-venda)[663].

Além da doutrina e da prática das autoridades de controlo, a jurisprudência sobre este artigo é muito recente e, até à data em que escrevo, resume-se a três decisões. Duas delas,

---

[657] *Ibidem* e M. GOMANN, "The new territorial …" cit., p. 572.
[658] G29, "Parecer 8/2010 ..." p. 5 e ss..
[659] Como foi o caso da autoridade do Estado de Hessen, v. "Report of the Hessen DPA for 2001", Hessischer Landtag Drucksache 15/4659, 26 de novembro de 2002, n.º 7.6.
[660] L. MOEREL, "The long arm …" cit., p. 31.
[661] Refiro-me ao exemplo n.º 4 apresentado no "Parecer 8/2010 ..." p. 17: "Na prática, são cada vez mais as situações em que a mesma base de dados pode estar sujeita a diferentes leis nacionais. Estas situações são frequentes nos domínios dos recursos humanos, em que as filiais/os estabelecimentos em diferentes países centralizam dados relativos aos empregados numa base de dados única (...)".
[662] L. MOEREL, "The long arm …" cit., p. 30. Em sentido próximo v. C. KUNER, *European Data Privacy Law & Online Business,* Oxford University Press, 2003, p. 119 e L. COLONNA, *Legal* cit., p. 378.
[663] L. MOEREL, "The long arm …" cit., p. 31.

Google Spain[664] e *Weltimmo*[665], merecem uma análise detalhada, ao passo que a outra, *Amazon*[666], apenas clarifica um aspeto deixado em aberto no caso *Weltimmo*, remetendo para o tribunal nacional a conclusão final, pelo que não será tratada de forma exaustiva neste trabalho.

2.2.1.1.1. O caso *Google Spain*

A Internet coloca várias questões em matéria de dados pessoais, desde a sua publicação num sítio *web* ("página-fonte"), passando pelas atividades de um motor de busca que fornece resultados que encaminham o utilizador para uma página-fonte, até às situações em que um utilizador efetua uma busca e os seus dados pessoais (como o endereço de IP a partir do qual a pesquisa é feita) são recolhidos e tratados pelo prestador do serviço do motor de busca[667]. O caso *Google Spain,* decidido no dia 13 de maio de 2014, incide sobre a segunda e a terceira hipóteses[668].

A discussão em torno desta decisão centrou-se no "direito a ser esquecido", descurando as implicações da interpretação do TJ para a jurisdição extraterritorial prescritiva e adjudicativa: esta foi a primeira vez que aquela instância se debruçou sobre a aplicação da Diretiva à conduta de uma pessoa coletiva (aos respetivos tratamentos de dados pessoais) cuja sede social se encontra fora do território da UE[669].

a) Enquadramento: os factos e as questões suscitadas

O processo foi impulsionado por uma queixa apresentada pelo Sr. Costeja González ("CG"), junto da autoridade espanhola (Agencia Española de Protección de Datos ou "APD"), a propósito da versão eletrónica de um jornal espanhol que, em 1998, na versão em papel, havia publicado dois anúncios sobre uma venda de imóveis em hasta pública

[664] Acórdão do TJ, Google Spain SL e Google Inc. c. Agencia Española de Protección de Datos (AEPD) e Mario Costeja González*,* C-131/12, 13 de maio de 2014.
[665] Acórdão do TJ, Weltimmo s. r. o. c. Nemzeti Adatvédelmi és Információszabadság Hatóság*,* C-230/14, 1 de outubro de 2015.
[666] Acórdão do TJ, Verein für Konsumenteninformation c. Amazon EU Sàrl*,* C-191/15, 28 de julho de 2016.
[667] Esta é a síntese do AG nas Conclusões do Acórdão do TJ, Google Spain SL e Google Inc. c. Agencia Española de Protección de Datos (AEPD) e Mario Costeja González*,* C-131/12, apresentadas a 25 de junho de 2013, C-131/12, n.º 3.
[668] São vários os textos de análise desta decisão, com destaque para C. KUNER, "The court of …" cit., p. 19 e ss.. Uma listagem, ainda que limitada no tempo, da opinião académica sobre este caso foi compilada por Julia POWLES e Rebekah LARSEN, "Academic Commnetary: Google Spain", *Cambridge Code*, disponível em http://www.cambridge-code.org/googlespain.html, consultado no dia 30 de setembro de 2018.
[669] M. GOMANN, "The new territorial …" cit., p. 570.

relacionada com as dívidas à Segurança Social do senhor CG. Saldadas as dívidas e decorridos vários anos, os anúncios encontravam-se disponíveis na versão eletrónica, no sítio *web* do jornal e, aquando da pesquisa pelo nome de CG através do *Google Search,* ali eram exibidas as respetivas hiperligações.

Em 2009, CG viu recusado um pedido de apagamento daqueles anúncios, dirigido ao editor do jornal, que invocou o cumprimento de uma obrigação de publicação por ordem do Ministério do Empregos e dos Assuntos Sociais. Insatisfeito, CG apresentou uma reclamação à APD requerendo que o jornal suprimisse ou alterasse, do seu sítio *web*, a publicação dos anúncios e que a *Google Spain* ou a *Google Inc.* suprimissem ou ocultassem os seus dados pessoais de modo a que deixassem de ser exibidos nos resultados de pesquisa através das hiperligações para o jornal. Em 30 de julho de 2010, a APD (i) indeferiu a reclamação apresentada contra o editor porque a publicação dos dados pessoais na imprensa tinha, realmente, um fundamento jurídico, e (ii) deferiu a reclamação contra a *Google Spain* e contra a *Google Inc.*, exigindo a ambas a adoção de medidas para retirar os dados do seu índice de resultados.

Inconformadas com esta decisão, a *Google Spain* e a *Google Inc.* interpuserem recurso para a Audiência Nacional que suspendeu a instância e submeteu, por reenvio prejudicial, essencialmente três questões ao TJ:

(i) Sobre a aplicação territorial da Diretiva e da legislação espanhola;

(ii) Duvidando da natureza da atividade do motor de busca; e

(iii) Inquirindo sobre o âmbito do direito de apagamento e de oposição (art. 12.º e 14.º da Diretiva) e sobre o seu cumprimento pelo operador do motor de busca[670].

A primeira dúvida centrou-se no art. 4.º, n.º 1, al. a), em particular no conceito de *estabelecimento*: (i) há um "estabelecimento" quando a empresa-mãe que explora o motor de busca abre, num Estado-Membro, um gabinete ou filial destinado à promoção e venda dos espaços publicitários desse motor de busca, cuja atividade se dirige aos habitantes desse Estado? (ii) E quando a empresa-mãe nomeia uma filial situada nesse Estado-

[670] Acórdão do TJ, Google Spain SL e Google Inc. c. Agencia Española de Protección de Datos (AEPD) e Mario Costeja González*,* C-131/12, 13 de maio de 2014, n.º 20.

Membro como sua representante e RT de dois ficheiros específicos que têm relação com os dados dos clientes que celebraram contratos publicitários com essa empresa? (iii) E quando o gabinete ou filial estabelecido num Estado-Membro transfere para a empresa-mãe, sediada fora da UE, os pedidos e requerimentos que lhe são dirigidos, quer pelos interessados, quer pelas autoridades competentes, relativamente ao respeito do direito à proteção de dados, mesmo que essa colaboração seja de caráter meramente facultativo?[671].

A segunda questão respeita à *atividade do motor de busca*, que "consiste em localizar a informação publicada ou inserida na rede por terceiros, indexá-la automaticamente, armazená-la temporariamente e, finalmente, colocá-la à disposição dos internautas sob determinada ordem de preferência", inquirindo-se o seu cabimento no conceito de "tratamento de dados"[672] . O tribunal espanhol queria ainda saber se a empresa que gere o motor de busca é o RT e, se assim fosse, se pode o titular dos dados pessoais exigir diretamente àquela que retire dos seus índices uma informação publicada por terceiros, sem se dirigir prévia ou simultaneamente ao titular da página web que aloja essa informação[673]?

Por fim, quanto ao *âmbito dos direitos do titular dos dados* em juízo, perguntava-se se deles se exclui "a informação que contém dados pessoais que tenha sido publicada licitamente por terceiros e se mantenha na página[-fonte]". E, além disso, se podem ser "interpretados no sentido de que permitem que a pessoa em causa possa dirigir-se aos motores de [pesquisa] para impedir a indexação da informação referente à sua pessoa, publicada em páginas web de terceiros, com base na sua vontade de […] não [ser] conhecida pelos internautas quando considere que lhe pode ser prejudicial ou deseje [ser] esquecida, mesmo tratando-se de uma informação publicada licitamente por terceiros?"[674].

b) Análise da decisão do TJ

Começando pela segunda questão, o TJ considerou, tal como o AG[675], que as atividades do motor de busca implicam o tratamento de dados pessoais, desde a "recolha",

[671] *Ibidem*.
[672] Art. 2.º, al. b) da Diretiva.
[673] Acórdão do TJ, Google Spain SL e Google Inc. c. Agencia Española de Protección de Datos (AEPD) e Mario Costeja González*,* C-131/12, 13 de maio de 2014, n.º 20.
[674] *Ibidem*.
[675] Conclusões apresentadas a 25 de junho de 2013, C-131/12, n.º 73 a 75.

passando pela "conservação" nos seus servidores até à comunicação ou "colocação à disposição"[676]. Aquela instância considerou irrelevante o argumento da *Google* segundo o qual os dados pessoais por si tratados estão publicamente disponíveis na Internet e não são alterados pelo motor de busca[677].

Em segundo lugar, divergindo neste ponto do AG[678], entendeu que a empresa que gere o motor de busca, a *Google Inc.*, é o RT para efeitos do art. 2.º, al. d), da Diretiva. Para tal invoca, essencialmente, três argumentos:

(i) É a *Google Inc.* quem determina as finalidades e os meios dos seus tratamentos, independentemente da circunstância de os editores de sítios *web* terem a faculdade de excluir a indexação de certa informação por eles publicada. Esta circunstância não isenta o motor de busca das suas responsabilidades antes poderá abrir a porta à responsabilidade conjunta[679];

(ii) Através de uma interpretação teleológica, do *objetivo* da Diretiva, "que consiste em assegurar, através de uma definição ampla do conceito de 'responsável pelo tratamento', uma proteção eficaz e completa das pessoas em causa", o TJ entendeu que o motor de busca é um RT mesmo se não "exercer controlo sobre os dados pessoais publicados nas páginas *web* de terceiros"[680];

(iii) Os tratamentos efetuados por um motor de busca *acrescem* ao tratamento dos editores de sítios *web* pois organizam e agregam informação que se traduz numa "visão global" e "mais estruturada das informações", criando um "perfil mais ou menos detalhado" de uma pessoa[681].

---

[676] Acórdão do TJ, Google Spain SL e Google Inc. c. Agencia Española de Protección de Datos (AEPD) e Mario Costeja González*,* C-131/12, 13 de maio de 2014, n.º 28.
[677] Acórdão do TJ, Google Spain SL e Google Inc. c. Agencia Española de Protección de Datos (AEPD) e Mario Costeja González*,* C-131/12, 13 de maio de 2014, n.º 23.
[678] Que empreendeu uma "interpretação razoável da diretiva" e entendeu que o conceito de RT não incluía o tipo de tratamentos desenvolvidos por um motor de busca, descritos como sendo realizados "de uma forma desorganizada, indiscriminada e aleatória" pelo que não se pode considerar haver uma "determinação das finalidades e meios do tratamento de dados pessoais" (art. 2.º, al. b)), pois o operador do motor de busca "não exerce um controlo sobre os dados pessoais incluídos em páginas *web* de terceiros", v. Conclusões apresentadas a 25 de junho de 2013, C-131/12, n.º 76 a 82.
[679] Acórdão do TJ, Google Spain SL e Google Inc. c. Agencia Española de Protección de Datos (AEPD) e Mario Costeja González*,* C-131/12, 13 de maio de 2014, n.os 33, 39 e 40.
[680] Acórdão do TJ, Google Spain SL e Google Inc. c. Agencia Española de Protección de Datos (AEPD) e Mario Costeja González*,* C-131/12, 13 de maio de 2014, n.º 34.
[681] Acórdão do TJ, Google Spain SL e Google Inc. c. Agencia Española de Protección de Datos (AEPD) e Mario Costeja González*,* C-131/12, 13 de maio de 2014, n.os 35 a 37.

Quanto à aplicação territorial da Diretiva, o problema central foi diagnosticado pelo AG[682]: a letra do art. 4.º, n.º 1 não era muito "útil", uma vez que não era "claro até que ponto e quando o tratamento de dados pessoais de pessoas em causa tem lugar no contexto das filiais da UE" [683]. Com efeito, as filiais da *Google Inc.*, incluindo a *Google Spain,* são meros agentes comerciais, pelo que, *prima facie,* nada têm que ver com os tratamentos de dados pessoais realizados pela *Google Inc.* Será?

Em primeiro lugar, quanto ao conceito de "estabelecimento", o TJ citou o considerando 19 para concluir que a *Google Spain* prossegue o "exercício efetivo e real de uma atividade, através de uma instalação estável em Espanha". Além disso, tem personalidade jurídica própria pelo que, sendo uma filial da *Google Inc.*, é um estabelecimento daquela para efeitos do art. 4.º, n.º 1, al. a). Porém, acrescentou que este critério não basta sendo necessário apurar se o tratamento em causa é "efetuado no contexto das atividades" do estabelecimento do RT.

Ora, para contornar a aplicação deste elemento da alínea a), a *Google Spain* e a *Google Inc.* sustentaram que o tratamento de dados pessoais do motor de busca é realizado "exclusivamente" pela *Google Inc.* "sem qualquer intervenção da Google Spain, cuja atividade se limita a fornecer apoio à atividade publicitária do grupo Google que é distinta do seu serviço de motor de busca"[684]. A *Google Spain* não realiza em Espanha "qualquer atividade diretamente ligada com a indexação ou armazenamento de informações ou de dados contidos nos sítios *web* de terceiros"[685] – apenas a *Google Inc.* o faz. Não obstante, o TJ não considerou estes argumentos e recordou que, por um lado, aquela disposição não exige que seja o próprio estabelecimento a efetuar o tratamento de dados pessoais; por outro lado, escudando-se num elemento teleológico, referiu que o art. 4.º não pode ser interpretado de forma restritiva porquanto o legislador pretendeu "evitar que uma pessoa seja privada da proteção garantida por essa diretiva e que essa proteção seja contornada, estabelecendo um âmbito de aplicação particularmente amplo"[686].

---

[682] G29, "Update of Opinion 8/2010 on applicable law in light of the CJEU judgement in Google Spain", 16 de dezembro de 2015, p. 4.
[683] Conclusões do AG no Acórdão do TJ, Google Spain SL e Google Inc. c. Agencia Española de Protección de Datos (AEPD) e Mario Costeja González*,* C-131/12, apresentadas a 25 de junho de 2013, n.º 63.
[684] Acórdão do TJ, Google Spain SL e Google Inc. c. Agencia Española de Protección de Datos (AEPD) e Mario Costeja González*,* C-131/12, 13 de maio de 2014, n.º 51.
[685] Acórdão do TJ, Google Spain SL e Google Inc. c. Agencia Española de Protección de Datos (AEPD) e Mario Costeja González*,* C-131/12, 13 de maio de 2014, n.º 46.
[686] Acórdão do TJ, Google Spain SL e Google Inc. c. Agencia Española de Protección de Datos (AEPD) e Mario Costeja González*,* C-131/12, 13 de maio de 2014, n.º 52 a 54.

É com base nestas premissas que o tribunal explica que a aplicação do art. 4.º, n.º 1, al. a), pressupõe que exista uma "conexão indissociável" entre o tratamento de dados pessoais realizados pelo RT (a *Google Inc.*) e as atividades do seu estabelecimento (a *Google Spain)*, mesmo que este não participe diretamente no tratamento dos dados pessoais do primeiro[687].

A indissociabilidade da conexão resultou, *in casu,* do próprio modelo de negócios da *Google*, ou seja, um modelo assente na prestação de serviços em linha gratuitos dependentes do tratamento de dados pessoais e financiados por publicidade. Com efeito, este modelo baseia-se na publicidade na Internet a partir de palavras-chave, que é a fonte de receitas da *Google Inc.* e, enquanto tal, a razão de ser económica da disponibilização de uma ferramenta de localização de informação gratuita sob a forma de um motor de pesquisa. A entidade que se ocupa da publicidade na Internet, neste caso, é a *Google Spain.* Por isso, o TJ entende que as atividades desta servem para "rentabilizar o serviço prestado" pela *Google Inc.* que, por seu turno, é a razão de ser da *Google Spain:* estão "indissociavelmente ligadas uma vez que as atividades relativas aos espaços publicitários constituem um meio para tornar o motor de busca em causa economicamente rentável e que esse motor é, ao mesmo tempo, o meio que permite realizar essas atividades[688]. Ou seja, as atividades da *Google Spain* integram o *core* do modelo de negócio da *Google Inc.*: sem publicidade a *Google Inc.* não prestaria os seus serviços de forma rentável nem trataria dados pessoais[689]. Esta "conexão indissociável" de natureza económica é evidenciada por uma conexão *digital*: a divulgação dos resultados de pesquisa, em si mesma um tratamento, é acompanhada, "na mesma página, pela exibição de publicidade relacionada com os termos de pesquisa", portanto esse tratamento, de mera divulgação, é efetuado no "contexto da atividade publicitária e comercial do estabelecimento", ou seja, da *Google Spain*[690].

No raciocínio do TJ está implícita a sugestão do AG, na apreciação da "aplicabilidade territorial" da Diretiva, de recorrer a teoria da unidade económica segundo a qual, apesar de juridicamente distintas, a *Google Inc.* e a *Google Spain* são um "operador económico"

[687] Acórdão do TJ, Google Spain SL e Google Inc. c. Agencia Española de Protección de Datos (AEPD) e Mario Costeja González*,* C-131/12, 13 de maio de 2014, n.º 60.
[688] Acórdão do TJ, Google Spain SL e Google Inc. c. Agencia Española de Protección de Datos (AEPD) e Mario Costeja González*,* C-131/12, 13 de maio de 2014, n.º 55 e 56.
[689] S. CARULLA, "Aplicación ..." cit., p. 89 e G29, "Update …" cit., p. 3 e 4: "as vendas do estabelecimento local da Google em Espanha encontravam-se 'indissociavelmente ligadas' aos lucros gerados pelos tratamentos de dados pessoais [da *Google Inc.*]".
[690] Acórdão do TJ, Google Spain SL e Google Inc. c. Agencia Española de Protección de Datos (AEPD) e Mario Costeja González*,* C-131/12, 13 de maio de 2014, n.º 57.

que "deve ser considerado uma unidade singular e não deve (...) ser decomposto com base nas suas atividades individuais relativas ao tratamento de dados pessoais ou nos diferentes grupos e pessoas em causa relacionadas com as suas atividades"[691]. "Em conclusão", rematou o AG, "o tratamento de dados pessoais tem lugar no contexto do estabelecimento de um responsável pelo tratamento se esse estabelecimento fizer a ponte entre o serviço de referenciamento e o mercado publicitário desse Estado-Membro, mesmo que as operações técnicas de tratamento sejam efetuadas noutros países terceiros"[692].

Por fim, resumidamente, quanto ao *âmbito* de aplicação dos direitos ao apagamento e de oposição, o TJ declarou que "o operador de um motor de busca é obrigado a suprimir da lista de resultados, exibida na sequência de uma pesquisa efetuada a partir do nome de uma pessoa, as ligações a outras páginas web publicadas por terceiros e que contenham informações sobre essa pessoa, também na hipótese de esse nome ou de essas informações não serem prévia ou simultaneamente apagadas dessas páginas web, isto, se for caso disso, mesmo quando a sua publicação nas referidas páginas seja, em si mesma, lícita"[693].

Julgo que, do que foi dito, posso extrair duas ilações e enunciar outras tantas dúvidas surgidas após esta decisão. Em primeiro lugar, em termos metodológicos, o tribunal recorreu à interpretação teleológica invocando o "efeito útil" da Diretiva num contexto permeado por "tecnologias que surgiram depois da sua publicação", o imperativo de "assegurar uma proteção eficaz e completa" e de acautelar lacunas nessa proteção[694]. Deste modo, avança uma "proibição de interpretação restritiva"[695] do art. 4.º, n.º 1, al. a), que viabiliza um "âmbito de aplicação particularmente amplo"[696]. Esta tese havia sido expressa, em 2010, pelo G29, referindo que a expressão "contexto das atividades de um estabelecimento" devia ser interpretada num sentido amplo de modo a assegurar a

[691] Conclusões do AG no Acórdão do TJ, Google Spain SL e Google Inc. c. Agencia Española de Protección de Datos (AEPD) e Mario Costeja González*,* C-131/12, apresentadas a 25 de junho de 2013, n.º 66.
[692] Conclusões do AG no Acórdão do TJ, Google Spain SL e Google Inc. c. Agencia Española de Protección de Datos (AEPD) e Mario Costeja González*,* C-131/12, apresentadas a 25 de junho de 2013, n.º 67.
[693] Acórdão do TJ, Google Spain SL e Google Inc. c. Agencia Española de Protección de Datos (AEPD) e Mario Costeja González*,* C-131/12, 13 de maio de 2014, n.º 99.
[694] Acórdão do TJ, Google Spain SL e Google Inc. c. Agencia Española de Protección de Datos (AEPD) e Mario Costeja González*,* C-131/12, 13 de maio de 2014, n.º 19. No mesmo sentido, v. A. MIGLIO, "Back to … cit., p. 112; M. GOMMAN, "The new …", cit., p. 577; Paul DE HERT e Vagelis PAPAKONSTANTINOU, "Google Spain. Adressing Critiques and Misunderstandings One Year Later", *MJ,* n.º 22, 2015, p. 624 e ss.; S. CARULLA, "Aplicación ..." cit., p. 87.
[695] Filipa CALVÃO, "A proteção de dados pessoais na internet: desenvolvimentos recentes", *RDI*, n.º 2, 2015, p. 6791.
[696] Acórdão do TJ, Google Spain SL e Google Inc. c. Agencia Española de Protección de Datos (AEPD) e Mario Costeja González*,* C-131/12, 13 de maio de 2014, n.º 54 e 53.

plenitude da proteção dos direitos fundamentais[697]. Considerou-se que este exercício interpretativo do TJ assenta num "raciocínio consequencialista" (*consequence-focused thinking* ou *result oriented*) segundo o qual a não aplicação da Diretiva implicaria uma desproteção do senhor CG e a isenção de qualquer tipo de responsabilidade dos motores de busca quanto aos tratamentos por si realizados[698]. Aliás, o tribunal é claro: "não se pode aceitar que o tratamento de dados pessoais efetuado com vista às necessidades do funcionamento do referido motor de busca fique isento das obrigações e garantias previstas na Diretiva 95/46, o que lesaria o efeito útil desta e a proteção eficaz e completa das liberdades e dos direitos fundamentais das pessoas singulares que ela visa assegurar"[699].

A segunda conclusão, e dado que nenhuma das partes contestou que a *Google Spain* era um "estabelecimento"[700] da *Google Inc.*, prende-se com o papel do mesmo enquanto "elo" territorial de conexão com a entidade do foro, no caso a UE[701]. De facto, a interpretação do "contexto das atividades de tratamento" é entendida, por alguns autores, como uma suavização da territorialidade aparentemente implicada na exigência de um "estabelecimento" do RT. A consequência deste amaciamento da territorialidade é o aumento do número de situações de aplicação desta alínea tendo em vista a maximização da proteção dos direitos fundamentais[702].

O papel do estabelecimento é secundário na medida em que este não participa, efetivamente, no tratamento, mas, ainda assim, não deixa de desempenhar uma função: "mesmo que o estabelecimento local não esteja diretamente envolvido no tratamento dos dados (…) as suas atividades podem trazer o tratamento para o âmbito do direito de proteção de dados da UE, desde que exista uma 'conexão indissociável' entre as atividades do estabelecimento local e o tratamento"[703]. Essa conexão pode ser *direta* (*v.g.*

---

[697] G29, "Parecer 8/2010 ..." cit., p. 16: "o objetivo geral da Diretiva deve igualmente ser tomado em consideração, na medida em que visa garantir uma *proteção efetiva* das pessoas singulares, de forma simples, eficaz e previsível" (itálicos meus).

[698] D. SVANTESSON, "Extraterritoriality …" cit., p. 229 e, do mesmo autor, "Article 4 ..." cit., p. 210 e ss.; M. GOMANN, "The new territorial …" cit., p. 572.

[699] Acórdão do TJ, Google Spain SL e Google Inc. c. Agencia Española de Protección de Datos (AEPD) e Mario Costeja González*,* C-131/12, 13 de maio de 2014, n.º 58.

[700] Acórdão do TJ, Google Spain SL e Google Inc. c. Agencia Española de Protección de Datos (AEPD) e Mario Costeja González*,* C-131/12, 13 de maio de 2014, n.º 49.

[701] M. GOMANN, "The new territorial …" cit., p. 571. VAN ALSENOY e KOEKKOEK notam que "a conexão territorial do "estabelecimento" da Google não é tão forte como inicialmente pensado", v. B. ALSENOY e M. KOEKKOEK, "Internet …" cit., p. 5. Já antes desta decisão, L. MOEREL havia alertado para a natureza *virtual* da territorialidade no art. 4.º, v. L. MOEREL, "The long ..." cit., p. 29.

[702] C. RYNGAERT, *Unilateral Jurisdiction* cit., p. 78; M. GOMANN, "The new territorial …" cit., p. 574 e 577.

[703] G29, "Update …" cit., p. 4.

se o estabelecimento presta serviços de apoio ao cliente) ou *indireta* (*v.g.* o desenvolvimento de atividades pelo estabelecimento que permitem, causam ou sustentam o tratamento de dados pessoais)[704].

Porém, acontece que esta decisão, aclamada como um passo fundamental para a tutela da personalidade digital, foi acolhida com algum ceticismo, em especial no que respeita ao seu âmbito geográfico e subjetivo[705]. Começando por este, o G29 esclareceu que, apesar de esta decisão visar questões relativas ao modelo de negócio de um motor de busca, tal não impede que as lições do *Google Spain* sejam aplicáveis a, pelo menos, duas situações:

(i) "[E]mpresas não europeias cujo modelo de negócio assenta na oferta de "serviços gratuitos" dentro da UE, que são financiados pela utilização de dados pessoais recolhidos dos utilizadores (por exemplo para publicidade)";

(ii) "[A]tividades de empresas que operam com outros modelos de negócios (...) oferecendo os seus serviços na UE em troca de taxas de filiação ou subscrições" acrescentando que ali se podem incluir "organizações que angariam doações" [706]. Nos exemplos apresentados, o G29 esclareceu que a pertença ao mesmo grupo não basta para ampliar o DUE ao utilizador de dados pessoais estrangeiro exigindo, sem os densificar, "fatores indicativos" da conexão entre o tratamento de dados realizado por aquele e a atividade do seu estabelecimento[707].

Além disto, colocam-se dificuldades ao nível da implementação desta decisão e, em especial, quanto ao âmbito geográfico do direito ao "esquecimento" ou, melhor dizendo, do "dever de desassociar o nome de uma pessoa singular dos resultados de pesquisa" que

[704] B. ALSENOY, "Reconciling …" cit., p. 84.
[705] Sem prejuízo de suscitar outras dúvidas, menos relevantes para este trabalho, enunciadas na doutrina, v. A. MIGLIO, "Back to …" cit., p. 102; C. KUNER, "The court of …" cit., p. 19; D. SVANTESSON, "Extraterritoriality and …" cit., p. 230 e, do mesmo autor, "Article 4..." cit., p. 210 e ss.; F. CALVÃO, "A proteção ..." cit., p. 6796; M. BRKAN, "Data Protection …" cit., p. 327 e, da mesma autora, "The Unstoppable ..." cit., p. 812 e ss..
[706] G29, "Guidelines on the implementation of the court of justice of the European Union Judgement on 'Google Spain and Inc V. Agencia Española de Protección de Datos (AEPD) And Mario Costeja González" C-131/12", 26 de novembro de 2014, p. 8 e G29, "Update …" cit., p. 5, nota de rodapé 12.
[707] G29, "Update …" cit., Anexo 2, p. 1.

recai sobre os motores de busca[708]. O acórdão não oferece qualquer orientação sobre esse aspeto: deve a *Google*, na sequência de um pedido de "esquecimento", modificar os resultados de pesquisas *globais* ou restringir o "esquecimento" ao *território* da UE?

Em teoria existem três modelos de implementação:

(i) Segundo o critério do domínio, os resultados de pesquisa são modificados com base no ccTLD (*country code top level domain*) usado para aceder ao motor de busca (*Google.pt, Google.es, Google.com*). Deste modo, o efeito da desassociação é limitado à versão de um país do serviço do motor de busca[709];

(ii) De acordo com o critério do filtro geográfico, os resultados de pesquisa são apresentados com base na origem geográfica da mesma e independentemente do domínio usado[710]. Tanto pressupõe a utilização de *software* para identificar a geolocalização do utilizador do motor de busca, independentemente do ccTLD usado para aceder àquele[711];

(iii) Pelo critério da implementação global, todos os resultados de pesquisa são modificados, independentemente da origem geográfica da pesquisa ou do domínio usado para aceder ao motor de pesquisa[712].

---

[708] B. ALSENOY e M. KOEKKOEK, "Internet and Jurisdiction …" cit., p. 105 e ss.; C. KUNER, "The court of …" cit., p. 16 e ss.; Dan SVANTESSON, "The Google Spain case: part of a harmful trend of jurisdictional overreach", *EUI Working Papers*, 2015, disponível em http://cadmus.eui.eu/bitstream/handle/1814/36317/RSCAS_2015_45.pdf?sequence=1&isAllowed=y, consultado no dia 30 de setembro de 2018; Emmanouil BOUGIAKIOTIS, "The enforcement of the Google Spain Ruling", *IJLIT,* n.º 24, 2016, p. 331 e ss.; F. CALVÃO, "A proteção ..." cit., p. 6784 e ss.; Ira RUBINSTEIN e Bilyana PETKOVA, "The international impact of the General Data Protection Regulation", Marc COLE & Franziska BOEHM (eds.), *Commentary on the General Data Protection Regulation,* Edward Elgar Publishing, 2018; Mistale TAYLOR, "*Google Spain* Revisited: The Misunderstood Implementation of a Landmark Decision and How Public International Law Could Offer Guidance", *EDPL,* n.º 2, 2017, p. 195 e ss..

[709] B. ALSENOY e M. KOEKKOEK, "Internet …" cit., p. 120 e ss.; D. SVANTESSON, "Delineating the Reach of Internet Intermediaries's Content Blocking – "ccTLD Blocking", "Strict Geolocation Blocking" or a "Country Lens Approach", *SCRIPTed,* vol. 11, n.º 2, 2014, p. 153 e ss.; M. TAYLOR, "*Google Spain* …" cit., p. 201 e ss..

[710] Este modelo é usado pela Youtube para selecionar os vídeos apresentados em certos países e disponíveis em www.youtube.com, v. B. ALSENOY e M. KOEKKOEK, "Internet …" cit., p. 139 e ss. e D. SVANTESSON, "Delineating ..." cit., p. 162 e ss., adotando a designação de "geofiltração rigorosa".

[711] Sobre a geolocalização, v. D. SVANTESSON, "Data Privacy …" cit., p. 173 e, do mesmo autor, D. SVANTESSON, "Delineating …" cit., p. 161 e ss.; Marketa TRIMBLE, "The Future of Cybertravel: Legal Implications of the Evasion of Geo-Location", *FIPMELJ,* vol. 22, n.º 2, 2012, p. 567 e ss. e Niloufer SELVADURAI, "The Proper Basis for Exercising Jurisdiction in Internet Disputes: Strengthening State Boundaries or Moving Towards Unification?", *JTLP,* vol. 13, n.º 2, 2012, p. 17 e ss..

[712] B. ALSENOY e M. KOEKKOEK, "Internet …" cit., p. 141 e ss..

Em novembro de 2014, o G29 publicou as linhas de orientação sobre a implementação da decisão dando nota da escolha do terceiro critério[713]. Sucede que, nessa data, a implementação da Google não respeitava aquele critério sendo, antes, uma conjugação dos dois primeiros: os visitantes situados na UE, ao aceder ao sítio *web* "google.com", eram automaticamente redirecionados para a versão do respetivo país do motor pesquisa (em Portugal seria *Google.pt*). Todavia, o utilizador poderia optar por mudar para o sítio *web* "universal" (*Google.com*). Isto significa que certos resultados da pesquisa poderiam ser removidos do *Google.pt* mas permaneciam disponíveis se o utilizador da UE mudar para o *Google.com* ou *Google.ca,* assim afastando o efeito do "esquecimento". Daí que, em Março de 2016, a CNIL tenha multado a *Google* no valor de € 100,000 e ordenado a implementação global do "esquecimento"[714].

[713] G29, "Guidelines …" cit., p. 9: "A implementação adequada desta decisão deve ser feita de modo a que os titulares dos dados sejam efetivamente protegidos contra o impacto da disseminação e acessibilidade universal da informação pessoal disponibilizada pelos motores de busca (...)".

[714] CNIL, "Délibération nº 2016-054 du 10 mars 2016", disponível em https://www.legifrance.gouv.fr/affichCnil.do?id=CNILTEXT000032291946, consultada no dia 30 de setembro de 2018 e "Right to be delisted: the CNIL Restricted Committee imposes a €100,000 fine on Google", de 24 de março de 2016, disponível em https://www.cnil.fr/en/right-be-delisted-cnil-restricted-committee-imposes-eu100000-fine-google, consultado no dia 30 de setembro de 2018.

Sem prejuízo das várias propostas da doutrina[715] e dos argumentos das autoridades de controlo[716], o âmbito geográfico do "esquecimento" está, no momento em que escrevo, nas mãos do TJ que responderá às seguintes perguntas:

(i) O direito à desindexação significa que os motores de pesquisa devem desindexar os links de *todos* os domínios ou o seu âmbito é limitado à União Europeia?

(ii) Se o âmbito é limitado à UE, deverá a desindexação limitar-se apenas ao domínio nacional do titular dos dados ou a todos os domínios da União?

---

[715] B. ALSENOY e M. KOEKKOEK, "Internet …" cit., p. 120 e ss.. Para os autores o ideal será uma determinação casuística do método mais adequado através de um exercício de ponderação interesses, enquadrado na lógica da *comity* incluindo, por exemplo, a existência de um interesse público de outros Estados – e dos seus cidadãos – em aceder à informação que se sobrepunha ao interesse do titular dos dados, a existência de outros fatores de conexão em relação ao território da entidade do foro (a localização dos servidores do sítio *web* indexado, a nacionalidade do titular dos dados e do editor da publicação) ou em relação a Estados terceiros, o grau de harmonização internacional e os riscos para o titular dos dados do confinamento da desindexação ao Estado do foro. Por seu turno, M. TAYLOR sugere que a Google implemente o critério do filtro geográfico para toda a UE, criando uma "muralha digital" no seu território. Em defesa desta posição, a autora invoca o respeito pelos interesses de outros Estados e recorre ao argumento segundo o qual, na prática, apenas um número limitado de utilizadores da Internet iria aceder aos resultados não modificados: quando situado fora da UE e se recorresse a tecnologia como uma VPN para esconder a respetiva localização. Para M. TAYLOR o dever da UE de proteger o direito fundamental à proteção de dados não é absoluto e critica a pretensão demasiado "vigilante" da CNIL cuja aplicação limita, de forma inaceitável, o acesso à informação de utilizadores da Google sem qualquer ligação ao território da UE, v. M. TAYLOR, "*Google Spain* ..." cit., p. 206 e ss.. Uma sugestão semelhante, também propondo o filtro geográfico, é de Álvaro RIVERO, "Right to Be Forgotten in the European Court of Justice Google Spain Case: The Right Balance of Privacy Right, Procedure, and Extraterritoriality", *European Union Law Working Paper,* n.º 19, 2017, disponível em https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2916608, consultado no dia 30 de setembro de 2018. Outra proposta, de D. SVANTESSON, assenta num modelo para determinar o âmbito geográfico da desindexação com base num esquema de "conexões substanciais" e "interesses legítimos". O autor sugere, por princípio, a implementação do esquecimento apenas nos domínios da UE. A sua extensão a outros domínios dependerá da invocação, por parte do titular dos dados quando realiza o pedido de desindexação de um (ou vários) dos seguintes elementos: (i) a extensão poderia ser reconhecida pelo ordenamento jurídico de um Estado estrangeiro em relação ao respetivo domínio (critério da harmonização); (ii) o conteúdo da informação é particularmente sério o que seria apurado caso a caso atendendo ao tipo de dados e às circunstâncias especificas do titular dos dados (critério do tipo de dados, da sua gravidade e sensibilidade); (iii) nesta categoria cabem várias situações: a) invocação de uma conexão substancial com pelo menos um Estado-Membro; b) o impacto da desindexação além dos domínios da UE nos interesses de outros utilizadores da Internet seria reduzido; c) a existência de riscos para o titular dos dados no caso da restrição da desindexação apenas ao domínio da UE; d) as tentativas de remoção do conteúdo original na página indexada pela Google foram frustradas por falta de cooperação com o editor original, v. D. SVANTESSON, "The Google Spain case ..." cit., p. 17.

[716] Para quem o método da implementação global não colide com a liberdade de expressão uma vez que a página-fonte, a origem da informação associada pelo motor de pesquisa, não é apagada. Cfr. CNIL, "Délibération nº 2016-054 ..." cit., p.1; João MARQUES, "Direito ao Esquecimento. A Aplicação Do Acórdão Google Pela CNPD", *FDPD*, 2016, p. 54. Também por esta razão não se poderá falar rigorosamente de um "direito ao esquecimento", v. C. KUNER, "The court of …" cit., p. 26 e ss. e F. CALVÃO, "A proteção ..." cit., p. 6795.

(iii) Deverá ser utilizado o *geoblocking* para garantir que os utilizadores do mesmo país do titular dos dados não recebem os resultados desindexados?[717].

Ainda quanto ao âmbito geográfico do direito à desindexação, alguns autores sustentaram que esta decisão viabilizou pedidos de titulares dos dados pessoais sem qualquer conexão com a UE[718]. Com efeito, a Diretiva, de acordo com o considerando 2, era aplicável independentemente da nacionalidade ou da residência da pessoa. Bastaria que o tratamento de dados pessoais a sustentar o pedido de desindexação fosse abrangido pelo art. 4.º, n.º 1, al. a), da Diretiva. Por conseguinte, ali caberia um pedido de um cidadão chinês, situado na China, que utiliza um motor de busca operado por uma empresa dos EUA com uma subsidiária na UE. Esta situação gera, na expressão de C. KUNER, um *right to suppression tourism*[719] exercido por pessoas sem qualquer ligação com a UE, além do facto de utilizarem serviços prestados também ali.

Aflorando este problema, o G29 atribuiu prioridade aos pedidos que evidenciam "uma conexão clara entre o titular dos dados e a UE, por exemplo a sua nacionalidade ou residência num Estado-Membro" [720]. Recentemente, a APD indeferiu um pedido de um cidadão do Paraguai pois, enquanto titular dos dados pessoais, não era cidadão ou residente na UE, e não tinha nenhuma "vinculação clara com nenhum Estado-Membro da União Europeia"[721]. Em sentido próximo, o ICO limitou a sua atuação a pedidos "relacionados com uma evidência clara de dano ou perturbação para o indivíduo"[722].

2.2.1.1.2. O caso *Weltimmo*

O caso *Weltimmo* criou "uma nova oportunidade ao Tribunal de Justiça de se pronunciar sobre a determinação do direito aplicável ao tratamento de dados nos termos

[717] Conseil d'Etat, 19 de juillet 2017, Google Inc, n.º 399922, disponível em http://www.conseil-etat.fr/Decisions-Avis-Publications/Decisions/Selection-des-decisions-faisant-l-objet-d-une-communication-particuliere/CE-19-juillet-2017-GOOGLE-INC, consultado no dia 30 de setembro de 2018.
[718] C. KUNER, "The court of justice …" cit., p. 28 a 31 e P. ASENSIO, "Competencia …" cit., p. 87.
[719] C. KUNER, "The court of …" cit., p. 23 e ss..
[720] G29, "Guidelines on …", cit., p. 8 e 9.
[721] AEPD, "Resolución n.º R/01976/2015", p. 7, disponível em http://www.agpd.es/portalwebAGPD/resoluciones/tutela_derechos/tutela_derechos_2015/common/pdfs/TD-01176-2015_Resolucion-de-fecha-11-12-2015_Art-ii-culo-16-LOPD_Recurrida.pdf, consultado no dia 30 de setembro de 2018.
[722] Como explicou o Deputy Commissioner and Director of Data Protection, David SMITH, "Four things we've learned from the Google judgment", 20 de maio de 2014, disponível em https://iconewsblog.wordpress.com/2014/05/20/four-things-weve-learned-from-the-eu-google-judgment/, consultado no dia 30 de setembro de 2018.

do art. 4.º, n.º 1, alínea a)"[723]. Sublinho que, apesar de incidir sobre o problema do direito nacional aplicável, sem qualquer elemento internacional que suscite a aplicação do DUE fora de portas, as conclusões desta decisão servem para firmar a maleabilidade do conceito de "estabelecimento" que, bem vistas as coisas, é invariável em questões internas e internacionais. Ou seja, o TJ utiliza o mesmo método de interpretação desta norma em situações intra-UE e extra-UE[724].

a) Enquadramento: os factos e as questões prejudiciais

As questões prejudiciais submetidas pela *Kúria* (Tribunal Supremo da Hungria) emergem de um litígio entre a autoridade de controlo húngara e uma empresa, registada e com sede social na Eslováquia, designada *Weltimmo s. r. o.*. Esta empresa geria um sítio *web* de mediação imobiliária com anúncios de imóveis sitos na Hungria. Um elevado número de anunciantes solicitou o apagamento dos respetivos anúncios, bem como dos seus dados pessoais, mas a *Weltimmo* não deu seguimento a estes pedidos.

Em resposta às reclamações apresentadas pelos anunciantes, a autoridade de controlo húngara, com base na legislação nacional de transposição da Diretiva, aplicou uma sanção à *Weltimmo*. A decisão foi impugnada por esta com base no argumento de que, de acordo com o art. 4.º, n.º 1, alínea a), da Diretiva, a autoridade húngara não podia aplicar o direito húngaro a uma empresa registada e com sede social noutro Estado-Membro. A contenda chegou à *Kúria* que, em 22 de abril de 2014, submeteu oito questões prejudiciais entre as quais o problema da lei aplicável formulado no argumento da *Weltimmo*: será que o art. 4.º, n.º 1, alínea a), podia ser interpretado no sentido de que permite a aplicação da lei húngara a uma empresa que gere um sítio *web* e está estabelecida exclusivamente noutro Estado-Membro (Eslováquia)[725]?

[723] Conclusões apresentadas em 25 de junho de 2015, n.º 2.
[724] M. GOMANN, "The new territorial …" cit., p. 573.
[725] "(...) Deve o artigo 4.º, n.º 1, alínea a) (...) ser interpretado no sentido de que a [Autoridade húngara para a proteção de dados] não pode aplicar a lei húngara para a proteção de dados, enquanto direito nacional, a um gestor de uma página Internet de mediação imobiliária estabelecido exclusivamente noutro Estado-Membro, mesmo que este divulgue, entre outros, imóveis húngaros cujos proprietários forneceram, provavelmente a partir do território da Hungria, os dados relativos aos seus imóveis a um meio (servidor) de armazenamento e processamento de dados pertencente ao gestor da página Internet e que está situado noutro Estado-Membro? 3) É relevante, para efeitos de interpretação, que o serviço prestado pelo responsável pelo tratamento de dados que gere a página Internet se destine ao território de outro Estado-Membro? 4) É relevante, para efeitos de interpretação, que os dados relativos aos imóveis situados no território do outro Estado-Membro e os dados pessoais dos proprietários tenham sido efetivamente carregados a partir do território desse outro Estado-Membro? 5) É relevante, para efeitos de interpretação, que os dados pessoais relacionados com os referidos imóveis sejam dados pessoais de cidadãos de outro Estado-Membro? 6) É relevante, para efeitos de interpretação, que os proprietários da empresa estabelecida

b) Análise da decisão

Citando o acórdão *Google Spain*, o TJ desde logo reiterou a "proibição de interpretação restritiva"[726] da expressão "no contexto das atividades de um estabelecimento"[727]. Ainda com base naquela decisão, tal como o AG[728], o tribunal adotou uma "análise em duas etapas":

(i) Apurar se a *Weltimmo* dispunha de um "estabelecimento" na Hungria; e

(ii) Verificar se o tratamento efetuado pela *Weltimmo* se inseria "no contexto das atividades do referido estabelecimento".

Quanto à primeira etapa, citando o considerando 19, a instância da União advoga uma "conceção flexível" de estabelecimento para apreciar se "uma sociedade, responsável por um tratamento de dados, dispõe de um estabelecimento (...) num Estado-Membro diferente do Estado-Membro ou do país terceiro em que está registada", o que requer avaliar "tanto o grau de estabilidade da instalação como a realidade do exercício das atividades nesse outro Estado-Membro, tendo em conta a natureza específica das atividades económicas e das prestações de serviços em causa. Este entendimento vale especialmente para as empresas que se dedicam a oferecer serviços exclusivamente na Internet"[729]. Noto que a alusão ao "país terceiro" me permite transpor este raciocínio ao caso de um RT registado nesse país e não num Estado-Membro.

Depois, invocando o objetivo da Diretiva, o TJ acrescenta que "a presença de um único representante pode, em certas circunstâncias, ser suficiente para constituir uma instalação estável se este atuar com um grau de estabilidade suficiente através dos meios necessários para a prestação dos serviços específicos em causa no Estado-Membro em questão" pelo que "o conceito de 'estabelecimento' (...) abrange qualquer atividade real

na Eslováquia tenham domicílio na Hungria?", cfr. Acórdão do TJ, Weltimmo s. r. o. c. Nemzeti Adatvédelmi és Információszabadság Hatóság, C-230/14, 1 de outubro de 2015, n.º 14.

[726] F. CALVÃO, "A proteção de ..." cit., p. 6791.

[727] Acórdão do TJ, Weltimmo s. r. o. c. Nemzeti Adatvédelmi és Információszabadság Hatóság, C-230/14, 1 de outubro de 2015, n.º 25.

[728] Conclusões apresentadas pelo AG em 25 de junho de 2015, n.º 23 e ss..

[729] Acórdão do TJ, Weltimmo s. r. o. c. Nemzeti Adatvédelmi és Információszabadság Hatóság, C-230/14, 1 de outubro de 2015, n.º 29.

e efetiva, ainda que mínima, exercida através de uma instalação estável"[730]. O tribunal deu por preenchido este requisito com base em dois elementos do caso concreto: "a atividade exercida pela *Weltimmo* consiste, pelo menos, na exploração de um ou de vários sítios *web* de anúncios de imóveis situados na Hungria, que são redigidos em língua húngara e que deixam de ser gratuitos depois de decorrido um período de um mês"[731] e, acresce ainda que, "a *Weltimmo* dispõe de um representante na Hungria (...) que tentou negociar com os anunciantes o pagamento de créditos em dívida (...) serviu de intermediário entre a [*Weltimmo*] e os queixosos e representou aquela nos procedimentos administrativos e judiciais. Além disso [a *Weltimmo*] (...) abriu uma conta bancária na Hungria, destinada à cobrança dos seus créditos e utiliza uma caixa de correio" na Hungria "para gerir os seus assuntos correntes"[732].

Em relação à segunda etapa, o TJ repete, tal como em *Google Spain,* que o tratamento não tem de ser operado pelo "próprio estabelecimento (...) mas apenas 'no contexto das atividades' deste"[733]. De seguida identifica os tratamentos no caso: a publicação, pela *Weltimmo*, no seu sítio *web,* de dados pessoais dos proprietários dos imóveis e a sua utilização para as necessidades de faturação dos anúncios. Ora, para aquelas instâncias, estes tratamentos ocorrem no contexto das atividades do seu estabelecimento, encarregue, por exemplo, de cobrar os créditos resultantes dos anúncios e de representar a *Weltimmo* em procedimentos administrativos e judiciais[734]. Por fim, o tribunal afirmou que a questão da nacionalidade dos titulares dos dados pessoais é "desprovida de pertinência" para efeitos do art. 4.º[735].

Que conclusões retirar desta decisão? Desde logo, em sintonia com o caso *Google Spain,* o tribunal repete a importância da interpretação teleológica a respeito do art. 4.º, n.º 1, al. a)[736]. A aplicação deste método afasta o elemento literal e privilegia um *entendimento* daquela alínea à luz da respetiva finalidade ou, o mesmo é dizer, atribui

[730] Acórdão do TJ, Weltimmo s. r. o. c. Nemzeti Adatvédelmi és Információszabadság Hatóság, C-230/14, 1 de outubro de 2015, n.º 30 e 31.
[731] Acórdão do TJ, Weltimmo s. r. o. c. Nemzeti Adatvédelmi és Információszabadság Hatóság, C-230/14, 1 de outubro de 2015, n.º 32.
[732] Acórdão do TJ, Weltimmo s. r. o. c. Nemzeti Adatvédelmi és Információszabadság Hatóság, C-230/14, 1 de outubro de 2015, n.º 33.
[733] Acórdão do TJ, Weltimmo s. r. o. c. Nemzeti Adatvédelmi és Információszabadság Hatóság, C-230/14, 1 de outubro de 2015, n.º 35.
[734] Acórdão do TJ, Weltimmo s. r. o. c. Nemzeti Adatvédelmi és Információszabadság Hatóság, C-230/14, 1 de outubro de 2015, n.º 29 a 41.
[735] *Ibidem*.
[736] M. GOMANN, "The new territorial …" cit., p. 572 e ss. e P. HERT e M. CZERNIAWSKI, "Expanding …" cit., p. 234.

primazia ao *espírito* em detrimento da *letra da lei.* Nos dois casos analisados, o TJ recordou, em primeiro lugar, a proteção "completa" e "eficaz" dos direitos fundamentais dos titulares dos dados pessoais enquanto objetivo da Diretiva, só posteriormente delineando o campo de aplicação do art. 4.º de acordo com aquele postulado.

Por outro lado, esta decisão confirma que a aplicação prática do art. 4.º assenta em duas etapas: a primeira, em torno do conceito de "estabelecimento", incide sobre a verificação de que o RT desenvolve atividades, mesmo que "mínimas", num Estado-Membro[737]. Inequivocamente, no caso *Weltimmo*, firma-se "uma conceção flexível (...) que afasta qualquer abordagem formalista segundo a qual uma empresa só se pode considerar estabelecida no lugar em que estiver registada"[738]. Assim tem entendido a maioria da doutrina para a qual poderá ser suficiente para preencher esta condição, por exemplo, a presença permanente de um agente ou de um funcionário equipado com um computador[739].

Na segunda etapa, a metodologia usada pelo TJ nos dois casos assemelha-se à proposta "funcional" do G29: "mais do que uma indicação teórica acerca da lei a aplicar pelas partes, é o seu comportamento prático e as suas interações que são decisivas" e, sobretudo, a conexão entre o tratamento de dados pessoais do RT e as atividades do seu estabelecimento[740].

Certo é que, da aplicação desta metodologia, pode resultar que o tratamento de dados pessoais do RT não seja regido pelo direito da sua nacionalidade, da sua sede ou registo: no caso *Google Spain* seria a legislação dos EUA e, no caso *Weltimmo*, o direito da Eslováquia. A doutrina enquadra estas decisões do TJ numa tendência crescente na regulação da Internet de rejeitar um "princípio do país de origem", isto é, que apenas o país da nacionalidade, origem ou de incorporação formal do ator em linha pode legislar sobre a sua atividade e, portanto, exercer jurisdição prescritiva sobre o mesmo[741].

---

[737] Acórdão do TJ, Weltimmo s. r. o. c. Nemzeti Adatvédelmi és Információszabadság Hatóság*,* C-230/14, 1 de outubro de 2015, n.º 31 e 41.

[738] Acórdão do TJ, Weltimmo s. r. o. c. Nemzeti Adatvédelmi és Információszabadság Hatóság*,* C-230/14, 1 de outubro de 2015, n.º 29.

[739] B. ALSENOY, "Reconciling …" cit., p. 80 e ss.; M. BRKAN, "Data Protection …" cit., p. 329; P. de HERT e M. CZERNIAWSKI, "Expanding the …", cit., p. 234. Foi esta a posição do AG nas suas conclusões em *Weltimmo*, n.º 34.

[740] G29, "Parecer 8/2010 ..." cit., p. 32.

[741] A rejeição do "princípio do país de origem" dá corpo a uma tendência crescente na regulação da Internet como observa U. KOHL uma vez que os Estados não estão dispostos a deixar apenas para o Estado de origem a regulação dos atores *online* cuja atividade tem impacto interno, v. Utah KOHL, "Jurisdiction in Cyberspace", Nicholas TSAGOURIAS e Russell BUCHAN, (eds.), *Research Handbook on International Law and Cyberspace,* Edward Elgar Publishing, 2015, p. 50. Em sintonia com esta posição, v. L. MOEREL,

Merece ainda uma breve referência o contributo do caso *Amazon* que veio confirmar a interpretação ampla do conceito de "estabelecimento", clarificando apenas que o mesmo "não pode existir pelo simples facto de o sítio *web* da empresa em questão ser acessível nesse Estado-Membro"[742].

2.2.2. O direito internacional público

De harmonia com o art. 4.º, n.º 1, al. b), a Diretiva aplicava-se quando o RT não estivesse estabelecido num Estado-Membro, mas num "local onde a sua legislação nacional seja aplicável por força do direito internacional público". O G29 pronunciou-se no sentido de afirmar a existência de "critérios externos", decorrentes do DIP, que podem determinar em certos casos a "extensão da aplicação da legislação nacional de proteção de dados para lá das fronteiras nacionais", como quando um acordo internacional estipula a lei aplicável numa embaixada ou consulado[743]. Assim, uma embaixada de um Estado-Membro, situada no Canadá, poderá estar sujeita à legislação daquele Estado-Membro e não à legislação Canadiana.

Para alguns autores não havia aqui um verdadeiro exercício de jurisdição extraterritorial porquanto a aplicação do direito da entidade do foro resultaria do próprio DIP[744]. Com efeito, não houve aqui nenhuma intervenção supletiva da entidade do foro na ausência de regulação do DIP, como pressupõe a definição avançada na Parte I, mas, pelo contrário, esta norma seria uma remissão para uma decisão previamente consensualizada entre os Estados.

2.2.3. O recurso a "meios" no território da Comunidade

O terceiro critério para delimitar o campo de aplicação da Diretiva, segundo o art. 4.º, n.º 1, al. c), é aquele em que, de forma mais óbvia, se manifestava a extraterritorialidade em relação a responsáveis pelo tratamento *sem* estabelecimento na UE. A letra da lei, a opinião do G29 e a doutrina[745] são as únicas fontes interpretativas

---

Binding ... cit., p. 56 e, da mesma autora, "The long ..." cit., p. 28 e ss.; P. HERT e M. CZERNIAWSKI, "Expanding …" cit., p. 235; P. HERT e M. CZERNIAWSKI, "Expanding …" cit., p. 235.

[742] Acórdão do TJ, Verein für Konsumenteninformation c. Amazon EU Sàrl, C-191/15, 28 de julho de 2016, n.º 76.

[743] G29, "Parecer 8/2010 ..." cit., p. 30.

[744] A. GONÇALVES, "The extraterritorial ..." cit., p. 202.

[745] C. KUNER, *European* cit., p. 120 e 121; L. MOEREL, *Binding* ... cit., p. 111; U. DAMMANN e S. SIMITIS, *EG-Datenschutzrichtlinie* cit., p. 130.

deste preceito pois não existe jurisprudência do TJ. A única decisão que poderia acrescentar especificações às outras fontes, o caso *Rease*[746]*,* não prosseguiu.

O G29 esclareceu que esta disposição "procura salvaguardar o direito à proteção dos dados pessoais (...) mesmo que o responsável pelo tratamento não esteja estabelecido no território da UE/EEE, nos casos em que haja uma ligação inequívoca entre o tratamento de dados pessoais e esse território"[747]. Acrescentou ainda que este critério foi pensado tendo em consideração as novas tecnologias, em especial a Internet, "que facilitam a recolha e o tratamento de dados pessoais à distância, independentemente de qualquer presença física do responsável pelo tratamento no território" de um Estado-Membro[748].

Procurou incluir-se nesta alínea todo o tipo de *software* de monitorização que instrumentaliza os "meios" usados pelos internautas (computador, *i-pad*, disco rígido, *browser*, etc.) para recolher dados pessoais e enviá-los para outro local, porquanto "estas tecnologias são, por definição, usadas sem que o utilizador disso seja informado (...), constituem uma forma de tratamento invisível e não legítimo"[749]. Em 2010, o G29 avançou uma "interpretação extensiva do critério" dos meios de modo a incluir[750]: (i) intermediários humanos e/ou técnicos, nomeadamente estudos ou inquéritos e questionários, como sucede nalguns ensaios farmacêuticos; (ii) "atividades externalizadas que se realizem por subcontratantes no território" da UE, em nome de um RT estabelecido fora dali; (ii) computadores pessoais dos utilizadores (no caso dos testemunhos de conexão ou *cookies* e de faixas publicitárias em *JavaScript*)[751].

Sem prejuízo do travão ao campo de aplicação disposto na parte final desta alínea[752], desde cedo a doutrina enfatizou que esta norma seria fonte de incertezas e

[746] Acórdão do TJ, T. D. Rease e P. Wullems c. College bescherming persoonsgegevens, C-192/15, 9 de dezembro de 2015. O despacho do presidente do TJ encontra-se disponível em http://curia.europa.eu/juris/document/document.jsf?text=&docid=173506&pageIndex=0&doclang=FR&mode=lst&dir=&occ=first&part=1&cid=730134, consultado no dia 30 de setembro de 2018.
[747] G29, "Parecer 8/2010 ..." cit., p. 20.
[748] *Idem*, p. 21.
[749] G29, "Documento ..." cit., p. 13.
[750] G29, "Parecer 8/2010 ..." cit., p. 23.
[751] Enfatizando a necessidade de "avaliar, caso a caso, o modo de utilização dos meios para recolher e efetuar o tratamento de dados pessoais" o G29 considerou que, a recolha de dados pessoais através de uma *cookie*, com recurso a um computador pessoal, por um RT situado fora do território da UE, cabe no âmbito desta alínea c). De facto, não é decisiva a propriedade sobre os meios usados para a recolha da informação; o que é determinante é a realização de um conjunto de operações técnicas que têm lugar *sem o controlo e participação do titular dos dados*. Cfr. G29, "Privacidade na Internet – uma abordagem integrada da UE no domínio da proteção de dados em linha", 21 de novembro de 2000, p. 30; G29, "Documento ..." cit., p. 11; G29, "Parecer 8/2010 ..." cit., p. 23.
[752] Sempre que os "meios" fossem usados apenas para "trânsito" dos dados no território da Comunidade a Diretiva não será aplicável. É o caso, por exemplo, dos cabos das redes de telecomunicações ou dos serviços

insegurança jurídica, podendo conduzir à interpretação de um âmbito de aplicação excessivo[753]. Estas preocupações encontraram eco numa posição do G29[754] e do SEPD[755]: a aplicação daquela disposição suscitava "consequências indesejáveis em termos de impacto económico e de aplicabilidade", uma "aplicação universal do direito da UE", em "casos em que a ligação com a UE é limitada (por exemplo, um responsável pelo tratamento estabelecido fora da UE, que trata dados de não residentes na UE, utilizando um subcontratante ali estabelecido)" [756].

Por este motivo o G29 sugeriu "um fator de conexão mais específico, tendo em conta a eventual 'seleção' de destinatários" ou uma "abordagem orientada para os serviços" que "poderia ser útil em termos de segurança jurídica". Esta proposta foi inspirada noutros domínios do DUE[757], jurisprudência do TJ[758], em legislação dos EUA

---

postais, "que apenas asseguram o trânsito das comunicações pela União, para depois chegarem a países terceiros". Todavia, o G29 notou que "são cada vez mais os serviços de telecomunicações que fundem o mero trânsito e os serviços de valor acrescentado, incluindo, por exemplo, filtragem *spam* ou outras manipulações de dados durante a transmissão", v. G29, "Parecer 8/2010 ..." cit., p. 25.

[753] Andrea MATWYSHYN, "Of Nodes and Power Laws: A Network Theory Approach to Internet Jurisdiction Through Data Privacy", *NWULR,* n.º 98, 2003-2004, p. 540; C. KUNER, *European* cit., p. 125; Diana SANCHO VILLA, *Negocios internacionales de tratamiento de datos personales,* Civitas, 2010, p. 43; Dov SCHERZER, "EU Regulation of Processing of Personal Data by Wholly Non-Europe-Based Websites", *EIPLR,* vol. 25, n.º 7, 2003, p. 292 e ss.; Lee BYGRAVE, "Determining applicable law pursuant to European Data Protection Legislation", *CLSR,* n.º 16, 2000, p. 252 e 255; L. MOEREL, *Binding* cit., p. 116; P. ASENSIO, "Competencia …" cit., p. 79 e, do mesmo autor, *Derecho privado de Internet,* Civitas, 2015, p. 359; Peter SWIRE, "Of Elephants, Mice, and Privacy: International Choice of Law and the Internet", *UPLR,* vol. 153, 2005, p. 1977 e ss.; Stephen KOBRIN, "The Trans-Atlantic Data Privacy Dispute. Territorial Jurisdiction and Global Governance", Working Paper Series, The Wharton School, novembro de 2003.

[754] G29, "Parecer 8/2010 ..." cit., p. 23 e 35.

[755] SEPD, "Parecer do SEPD sobre a Comunicação da Comissão – 'Uma abordagem global da proteção de dados pessoais na União Europeia'", 14 de janeiro de 2011, n.º 122 e SEPD, "Opinion of the …" cit., p. 17.

[756] G29, "Parecer 8/2010 ..." cit., p. 23 e 35.

[757] Alude-se expressamente ao art. 15.º, n.º 1, alínea c) do Regulamento 44/2001 relativo à competência judiciária, ao reconhecimento e à execução de decisões em matéria civil e comercial, onde se lê: "1. Em matéria de contrato celebrado por uma pessoa para finalidade que possa ser considerada estranha à sua actividade comercial ou profissional, a seguir denominada «o consumidor», a competência será determinada pela presente secção, sem prejuízo do disposto no artigo 4.º e no ponto 5 do artigo 5.º: a) Quando se trate de venda, a prestações, de bens móveis corpóreos; ou b) Quando se trate de empréstimo a prestações ou de outra operação de crédito relacionados com o financiamento da venda de tais bens; ou c) *Em todos os outros casos, quando o contrato tenha sido concluído com uma pessoa que tem actividade comercial ou profissional no Estado-Membro do domicílio do consumidor ou dirige essa actividade, por quaisquer meios, a esse Estado-Membro ou a vários Estados incluindo esse Estado-Membro, e o dito contrato seja abrangido por essa actividade"* (itálicos meus).

[758] O G29 invoca as conclusões do AG, apresentadas a 18 de maio de 2010, no Acórdão do TJ, Peter Pammer c. Reederei Karl Schluter GmbH & Co KG*,* C-585/08 e C-144/09, sobre a interpretação a dar ao art. 15.º, n.º 1, alínea c), do Regulamento 44/2001: "(...) para a 'direção' da atividade no sentido do artigo 15, parágrafo 1, alínea c), do Regulamento 44/2001 não basta que o sítio da Internet da pessoa que exerce uma atividade comercial ou profissional seja acessível a partir do Estado-Membro do domicilio do consumidor. O juiz nacional deve atender ao conjunto das circunstâncias do caso para apreciar se uma pessoa que exerce uma atividade comercial ou profissional dirige a sua atividade para o Estado-Membro do domicílio do consumidor. Os fatores importantes para a apreciação são, sobretudo, o conteúdo do sítio

sobre proteção de crianças na Internet[759] e no direito nacional que transpôs a Diretiva 2000/31 relativa ao comércio eletrónico. Em especial, este diploma dispõe que os prestadores de serviços que não se encontrem estabelecidos na UE são por ele abrangidos sempre que ofereçam serviços especificamente destinados ao território dos Estados-Membros[760].

2.3. A reforma de 2012 e o art. 3.º do RGPD

Entre os objetivos da reforma de 2012 que deu origem ao RGPD, enunciados em duas Comunicações da COM[761], encontra-se a revisão das "disposições em vigor sobre a lei aplicável, incluindo a atual determinação dos critérios, no intuito de aumentar a segurança jurídica, clarificar a responsabilidade dos Estados-Membros na aplicação das normas de proteção de dados e, por último, proporcionar o mesmo nível de proteção de todas as pessoas da UE a que os dados dizem respeito, independentemente da localização geográfica do responsável pelo tratamento"[762].

Invocando o relatório de 2003 sobre a implementação da Diretiva, a COM apontava as dificuldades com que os agentes económicos e as autoridades de controlo se deparavam na determinação da lei aplicável quando um RT "está sujeito a exigências diferentes de diversos Estados-Membros, quando uma empresa multinacional está estabelecida em mais de um Estado-Membro ou quando o responsável pelo tratamento não está estabelecido na UE, mas presta serviços a clientes da UE"[763]. Daí que, de modo a reforçar

---

da Internet, a atividade anterior da pessoa que exerce a atividade comercial ou profissional, o tipo de domínio utilizado pelo sítio e o recurso às possibilidades oferecidas pela publicidade na Internet (…)".

[759] "A aplicação desta legislação pode ser determinada quer pela localização de um editor nos Estados Unidos, quer pelo facto de as crianças americanas constituírem um dos destinatários do sítio *web*: os sítios e serviços em linha estrangeiros devem cumprir o disposto nesta legislação se se destinarem a crianças residentes nos EUA ou intencionalmente recolherem ou divulgarem informações pessoais sobre elas", v. G29, "Parecer 8/2010 ..." cit., p. 27, nota de rodapé 31.

[760] G29, "Parecer 8/2010 ..." cit., p. 27.

[761] "Uma abordagem global da proteção de dados pessoais na União Europeia", novembro de 2010 e "Proteção da privacidade num mundo interligado. Um quadro europeu de proteção de dados para o século XXI", janeiro de 2012.

[762] Comissão Europeia, "Uma abordagem ..." cit., p. 2 e ss..

[763] *Idem*, p. 12. Um exemplo apresentado é o seguinte: "uma empresa multinacional com vários estabelecimentos no território da UE desenvolveu um sistema de cartografia em linha na Europa que recolhe imagens de todos os edifícios públicos e privados, e que também pode fotografar pessoas na via pública. Num Estado-Membro, a inclusão de fotografias não desfocadas de pessoas que ignoravam estar a ser fotografadas foi considerada ilícita", mas noutros países não, v. Comissão Europeia, "Proteção da ..." cit., p. 8.

o "mercado único" da proteção de dados pessoais, a COM tenha optado por um regulamento[764].

Por outro lado, a "globalização e os avanços tecnológicos"[765] facilitam a prestação de serviços à distância por responsáveis pelo tratamento estabelecidos fora da UE que recolhem e tratam dados pessoais em linha. Em todo o caso, a COM reiterou que "o facto de o tratamento de dados pessoais ser feito por um responsável estabelecido num país terceiro não deve privar as pessoas da proteção a que têm direito por força da Carta dos Direitos Fundamentais e da legislação de proteção de dados da UE"[766] daí que, por um lado, não seja relevante a localização geográfica do RT[767] e, por outro lado, a proteção conferida pelo RGPD deverá abranger os tratamentos de dados pessoais "de pessoas que se encontrem nos Estados-membros" e que sejam "utilizados ou analisados por prestadores de serviços estabelecidos em países terceiros"[768].

Como procurarei demonstrar, em geral, as alterações desta reforma vertidas no art. 3.º do RGPD não se afastaram das recomendações de 2010, do G29[769], e de 2011 do SEPD[770].

2.3.1. Os critérios para determinar o âmbito de aplicação do RGPD segundo o art. 3.º: o que há de novo?

O art. 3.º do RGPD dispõe o seguinte: "1. O presente regulamento aplica-se ao tratamento de dados pessoais efetuado no contexto das atividades de um estabelecimento de um responsável pelo tratamento ou de um subcontratante situado no território da União, independentemente de o tratamento ocorrer dentro ou fora da União. 2. "O presente regulamento aplica-se ao tratamento de dados pessoais de titulares residentes no território da União, efetuado por um responsável pelo tratamento ou subcontratante não estabelecido na União, quando as atividades de tratamento estejam relacionadas com: a) a oferta de bens ou serviços a esses titulares dos dados na União, independentemente da exigência de os titulares dos dados procederem a um pagamento; b) o controlo do seu

[764] De acordo com as estimativas da Comissão Europeia, em 2012, "tal representará uma poupança líquida para as empresas de cerca de 2,3 mil milhões de EUR por ano só em termos de encargos administrativos". Cfr. Comissão Europeia, "Proteção da ..." cit., p. 9.
[765] Comissão Europeia, "Uma abordagem ..." cit., p. 12.
[766] *Ibidem*.
[767] *Ibidem* e Comissão Europeia, "Proteção da ..." cit., p. 11 e 12.
[768] Comissão Europeia, "Proteção da ..." cit., p. 11.
[769] G29, "Parecer 1/2010 ..." cit., p. 33 e ss..
[770] SEPD, "Parecer do SEPD ..." cit., n.º 122 e ss..

comportamento, desde que esse comportamento tenha lugar na União. 3. O presente regulamento aplica-se ao tratamento de dados pessoais por um responsável pelo tratamento estabelecido não na União, mas num lugar em que se aplique o direito de um Estado-Membro por força do direito internacional público".

Do que foi dito sobre os objetivos da reforma iniciada pela COM na origem do RGPD, e comparando com o art 4.º da Diretiva, destacam-se alguns ajustes no que respeita à terminologia empregue, assinala-se a introdução de novos termos e a substituição do critério do "recurso a meios". São essas alterações que pretendo elencar nos pontos seguintes.

Antes, porém, importa clarificar o equívoco que poderá gerar a epígrafe do art. 3.º, quando esta se refere ao "âmbito territorial". A referência textual à territorialidade no elemento textual não deve ser lida literalmente, porquanto o âmbito do RGPD, tal como o âmbito da Diretiva, não é rigorosamente territorial[771].

2.3.1.1. A localização de um estabelecimento do RT ou do ST

Neste particular, destacam-se duas notas. Desde logo, não há alterações aos elementos da noção de "estabelecimento", agora descritos no considerando 22: "exercício efetivo e real de uma atividade com base numa instalação estável" sem ser determinante a "forma jurídica" do estabelecimento, que inclui "uma sucursal" ou "uma filial com personalidade jurídica".

Passando para o que há de novo, além da já assinalada aplicação direta do RGPD a *subcontratantes*, a parte final do art. 3.º, n.º 1, por sugestão introduzida pelo PE[772], formaliza a extensão do âmbito de aplicação do RGPD ao tratamento de dados pessoais que ocorra no exterior da UE, enfatizando a irrelevância do lugar onde efetivamente decorre o tratamento. A doutrina explica que esta norma incorpora o *Google Spain acquis* porquanto, nesse caso, a *Google Inc.* argumentou que o tratamento de dados pessoais era

[771] Em sentido semelhante, v. Dan SVANTESSON, "Article 3", Lee BYGRAVE *et alii* (eds.), *Commentary on the EU General Data Protection Regulation,* Oxford University Press, p. 1, disponível em https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3179907, consultado no dia 30 de setembro de 2018.

[772] Resolução legislativa do Parlamento Europeu, de 12 de março de 2014, sobre a proposta de regulamento do Parlamento Europeu e do Conselho relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados (regulamento geral de proteção de dados), alteração 97, disponível em http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+TA+P7-TA-2014-0212+0+DOC+PDF+V0//PT, consultado no dia 30 de setembro de 2018, doravante designada "Resolução legislativa do PE".

realizado, pela própria, fora da UE e sem a intervenção do seu estabelecimento espanhol[773].

2.3.1.2. O critério da localização do titular dos dados pessoais

O legislador prescindiu do critério do "recurso a meios", do art. 4.º, n.º 1, alínea c), da Diretiva, substituindo-o, no art. 3.º, n.º 2, do RGPD, por um critério centrado na localização dos titulares dos dados pessoais "no território da União".

A origem desta disposição, enaltecida como sendo um dos grandes desenvolvimentos da "revolução copérnica" imputada ao RGPD[774], encontra-se nas preocupações enunciadas pelo G29[775] e pelo SEPD[776], a propósito das imprecisões e do expansionismo do art. 4.º, n.º 1, al. c), da Diretiva[777]. Em particular o primeiro, sugeriu a adoção de um critério visando tratamentos de dados pessoais que mantenham uma "ligação suficiente com o território da UE"[778]. Esse critério seria o da "seleção de destinatários" de uma atividade segundo o qual o DUE só abrange o tratamento de dados pessoais de responsáveis pelo tratamento e subcontratantes sem estabelecimento na UE cujas atividades visam os titulares dos dados pessoais que ali se encontram.

Este critério apresenta a seu favor o facto de já ser utilizado no domínio da defesa do consumidor: "a sua aplicação no contexto da proteção de dados representaria segurança jurídica adicional para os responsáveis pelo tratamento, na medida em que teriam de aplicar os mesmos critérios a atividades que determinam, com frequência, a aplicação de normas de defesa do consumidor e de proteção de dados"[779]. Por isso se compreende que este esforço legislativo haja sido saudado do outro lado do Atlântico[780]. Acresce que se afigura razoável a premissa que lhe subjaz, também designada *moderate destination*

[773] Christian KOHLER, "Conflict of law issues in the 2016 Data Protection Regulation of the European Union", *RDIPP,* vol. 52, n.º 3, 2016, p. 653 e ss.; M. GOMANN, "The new territorial …" cit., p. 575; P. de HERT e M. CZERNIAWSKI, "Expanding the …", cit., p. 242.
[774] M. GOMANN, "The new territorial …" cit., p. 567 e ss. e P. de HERT e M. CZERNIAWSKI, "Expanding the …", cit., p. 238.
[775] G29, "Parecer 8/2010 ..." cit., p. 26.
[776] SEPD, "Parecer do SEPD sobre ..." cit., n.º 122 e SEPD, "Opinion of the …" cit., p. 17.
[777] Mistale TAYLOR, "Permissions and prohibitions in data protection jurisprudence", Brussels privacy Hub Working Paper 3, 2016, p. 18 e M. CZERNIAWSKI, "Do We …" cit., p. 221.
[778] G29, "Parecer 8/2010 ..." cit., p. 34.
[779] *Idem*, p. 35.
[780]Alexander DIX, "The Commission's Data Protection Reform After Snowden's Summer", *Intereconomics,* n.º 5, 2013, p. 269 e Omar TENE e Christopher WOLF, "Overextended: Jurisdiction and Applicable Law under the EU General Data Protection Regulation", White Paper, *The Future of Privacy Forum*, 2013, p. 6.

approach[781] ou apenas *destination approach*[782]: se um operador estrangeiro dirige a sua atividade para o mercado da UE, para os seus consumidores e titulares dos dados pessoais, tal implica uma ligação com o mesmo e uma aceitação pelo menos tácita quanto ao direito ali vigente podendo invocar-se uma submissão voluntária ao direito estrangeiro[783]. O recurso a este teste suaviza o exercício de jurisdição e minimiza o potencial impacto nos interesses da entidade *ad quem,* uma vez que a extraterritorialidade atinge uma atividade dirigida aos titulares dos dados pessoais situados na entidade do foro e ao respetivo mercado interno[784]. Como sublinham P. DE HERT e M. CZERNIAWSKI, os operadores estrangeiros só estarão vinculados pelo DUE se dirigem a sua atividade para o mercado da UE: *you might be target by EU law only if you target*[785].

A redação do art. 3.º, n.º 2, gerou várias dúvidas, algumas ainda por esclarecer, tratadas na Parte III, e uma questão entretanto clarificada, fruto de uma divergência da redação daquela norma na versão oficial portuguesa e inglesa. Na primeira versão, portuguesa, aquele artigo sugere que a proteção conferida pelo RGPD se limita a pessoas singulares *residentes* no território da UE[786] ao passo que na versão inglesa – e noutras – a categoria de titulares dos dados pessoais protegidos é indiferente ao seu local de residência (*data subjects who are in the Union*) [787].

Na doutrina, há quem não tenha dado conta desta divergência[788]. Tal dever-se-á ao facto de este conjunto de autores ter consultado apenas a versão oficial em inglês do RGPD para as suas inquirições. Outros, pelo contrário, como M. BRKAN[789] e P. ASENSIO[790], conhecedores de várias versões daquele diploma, sustentam que a vontade do

[781] P. de HERT e M. CZERNIAWSKI, "Expanding the …" cit., p. 238 e U. KOHL, "Jurisdiction…" cit., p. 35.
[782] P. de HERT e M. CZERNIAWSKI, "Expanding the …" cit., p. 231.
[783] C. REED, *Making Laws* cit., p. 225: "(...) um vendedor online que tenha como alvos os consumidores localizados num determinado Estado aderiu, ainda que temporariamente, à comunidade comercial desse Estado. Por esta razão, o vendedor provavelmente reconhecerá a autoridade desse Estado sobre as suas transações, aderindo aos seus comandos voluntariamente". Defendendo a mesma ideia, v. B. ALSENOY, "Reconciling …" cit., p. 95.
[784] M. GOMANN, "The new territorial …" cit., p. 586 usando a expressão "trading community of the EU".
[785] P. de HERT e M. CZERNIAWSKI, "Expanding the …", cit., p. 231.
[786] "O presente regulamento aplica-se ao tratamento de dados pessoais de *titulares residentes* no território da União (...)" (itálicos meus). Assim também nas versões Bulgara, Dinamarquesa, Espanhola, Polaca e Finlandesa.
[787] No caso francês, *personnes concernées qui se trouvent dans l' Union* (art. 3.º, n.º 2 e respetivos considerandos); no alemão *personenbezogener Daten von betroffenen Personen, die sich in der Union befinden* (art. 3.º, n.º 2 e respetivos considerandos); na versão italiana *dei dati personali degli interessati che si trovano nell'Unione* (art. 3.º, n.º 2 e respetivos considerandos); na versão inglesa lê-se *data subjects who are in the Union* (art. 3.º, n.º 2 e respetivos considerandos).
[788] A. MIGLIO, "Back to …" cit., p. 114 e 115; B. ALSENOY, "Reconciling …" cit., p. 85 e ss.; E. KINDT, "Why research …" cit., p. 17 e ss.; P. de HERT e M. CZERNIAWSKI, "Expanding the …", cit., p. 238 e ss..
[789] M. BRKAN, "Data Protection …" cit., p. 339.
[790] P. ASENSIO, "Competencia …" cit., p. 89.

legislador foi a de adotar o critério da localização do titular dos dados no território da UE, independentemente da sua residência. Uma interpretação sistemática do RGPD, invocando o considerando 2 e 14, suporta esta segunda posição[791]: o considerando 2 refere que "[o]s princípios e as regras em matéria de proteção das pessoas singulares relativamente ao tratamento dos seus dados pessoais deverão respeitar, independentemente da nacionalidade ou do local de residência dessas pessoas, os seus direitos e liberdades fundamentais, nomeadamente o direito à proteção dos dados pessoais"; o considerando 14 dispõe que "[a] proteção conferida pelo presente regulamento deverá aplicar-se às pessoas singulares, independentemente da sua nacionalidade ou do seu local de residência, relativamente ao tratamento dos seus dados pessoais".

De igual modo, atendendo ao procedimento legislativo do RGPD, um argumento histórico poderia também amparar a tese de M. BRKAN e P. ASENSIO: a proposta inicial da COM, contendo o critério da residência, foi alterada pelo PE[792] e mantida pelo Conselho[793]. Por fim, o direito à proteção de dados pessoais, tanto no art. 8.º da CDFUE como no art. 16.º do TFUE, é reconhecido a "[t]odas as pessoas singulares" sem quaisquer distinções. Afastando a incidência na matéria da proteção de dados pessoais, numa apreciação geral do DUE, a evolução do direito originário parece acentuar a ideia base de que "o ser humano se deve posicionar no centro das preocupações da União Europeia (não apenas o ser humano enquanto agente económico, não apenas o cidadão da União, mas sim todo e qualquer ser humano que tem contacto com a União"[794].

---

[791] Nesse sentido, entre outros argumentos, invocando o considerando 14, v. CNPD, "Parecer n.º 20/2018", p. 6, CNPD, "Parecer n.º 20/2018", 2018, disponível em http://app.parlamento.pt/webutils/docs/doc.pdf?path=6148523063446f764c324679626d56304c334e706447567a4c31684a53556c4d5a5763765130394e4c7a464451554e4554456376524739 6a6457316c626e527663306c7561574e7059585270646d46446232317063334e686279396a5a57593359544d794f4330325a44526c4c54526c4e546b74596a41304e4331694e54426d4f5449314d6a64684d7a45756347526d&fich=cef7a328-6d4e-4e59-b044-b50f92527a31.pdf&Inline=true, consultado no dia 30 de setembro de 2018.

[792] A Resolução legislativa do PE, alteração 97, retirou a expressão "residentes" e a disposição passou a referir apenas os "titulares dos dados no território da União". Na exposição de motivos da mesma, o relator é bastante claro: "(...) o relator gostaria de clarificar que o regulamento deve também ser aplicável a um responsável pelo tratamento não estabelecido na União sempre que as atividades de tratamento visem a oferta de bens ou serviços a titulares dos dados na União, independentemente da necessidade ou não de pagamento desses bens ou serviços ou do controlo desses titulares dos dados".

[793] "Position of the Council at first Reading with a view to the adoption of a Regulation of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data", 8 de abril de 2016, p. 110, disponível em https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=consil%3AST_5419_2016_REV_1_ADD_1, consultado no dia 30 de setembro de 2018.

[794] Ana Maria Guerra MARTINS, "Algumas Notas sobre o Espaço de Liberdade, Segurança e Justiça no Tratado de Lisboa", *Cadernos O Direito,* n.º 5, 2010, p. 28. Sobre o princípio da universalidade na CDFUE, v. Ana RITA GIL, *Imigração e Direitos Humanos,* Petrony, 2017, p. 228.

Finalmente, em abril de 2018, o Conselho da UE veio esclarecer as dúvidas existentes ao corrigir o erro da versão portuguesa alinhando-a com a inglesa e alargando a proteção a todos os titulares "que se encontrem no território da União"[795]. Deste modo, mesmo um cidadão chinês, temporariamente no território da União, pode beneficiar da proteção do RGPD. Em todo o caso, excluídos dessa proteção estão os titulares dos dados que se encontrem numa das situações apresentadas por P. DE HERT e M. CZERNIAWSKI: um turista português compra um cachecol na quinta avenida de Nova Iorque ou, ainda, um cidadão chinês, situado na China, adquire um boné vendido por um RT estabelecido nos EUA [796].

Adicionalmente, nem todos os tratamentos de dados pessoais de titulares dos dados situados no território da UE e realizados por um utilizador de dados pessoais não estabelecido no território da UE serão abrangidos pelo RGPD: só cabem no RGPD os tratamentos relacionados com a "oferta de bens e serviços" (art. 3.º, n.º 2, al. a)) ou os tratamentos que impliquem o "controlo do comportamento" daqueles titulares (art. 3.º, n.º 2, al. b)).

2.3.1.2.1. A oferta de bens e serviços

O considerando 23 enuncia o critério do acesso ao mercado ou da intenção de um utilizador de dados pessoais desenvolver uma atividade à distância mas dirigida a titulares dos dados pessoais que se encontram no território da UE, elencando alguns fatores que, sem grande novidade no ordenamento jurídico da União, o preenchem: "a utilização de uma língua ou de uma moeda de uso corrente num ou mais Estados-Membros, com a possibilidade de encomendar bens ou serviços nessa outra língua, ou a referência a clientes ou utilizadores que se encontrem na União, que podem ser reveladores de que o responsável pelo tratamento tem a intenção de oferecer bens ou serviços a titulares dos dados na União" [797]. Por seu turno, o mesmo considerando refere que "o mero facto de estar disponível na União um sítio *web* do responsável pelo tratamento ou subcontratante

[795] Conselho da UE, n.º 8088/18, 19 de abril de 2018, p. 278.
[796] P. de HERT e M. CZERNIAWSKI, "Expanding the …", cit., p. 85.
[797] Analisando estes fatores, v. B. ALSENOY, "Reconciling …" cit., p. 89; D. SVANTESSON, "Extraterritoriality and …" cit., p. 231 e 232; G29, "Parecer 8/2010 …" cit., p. 35; Michael CZERNIAWSKI, "Do We Need the 'Use of Equipment' as a factor for the territorial applicability of the EU Data Protection Regime?", D. SVANTESSON e D. KLOZA (eds.), *Trans-atlantic data* cit., p. 230; P. ASENSIO, "Competencia …" cit., p. 85. Como explica J. SCOTT estes critérios refletem uma "conduta que consiste num passo em direção ao Mercado da UE", v. J. SCOTT, "The New …" cit., p. 1348.

ou de um intermediário, um endereço eletrónico ou outro tipo de contactos, ou de ser utilizada uma língua de uso corrente no país terceiro em que o referido responsável está estabelecido, não é suficiente para determinar a intenção acima referida".

Nesta disposição o legislador importou para o campo da proteção de dados pessoais os indicadores desenvolvidos pelo TJ em *Hotel Alpenhof*[798]*, Muhlleitner*[799] e *Emrek*[800]*,* sobre a proteção do consumidor quando a atividade em linha do vendedor se "dirige" ao país do domicílio do consumidor, em conformidade com o art. 17.º, n.º 1, al. c), do Regulamento 1215/2012[801] e com o art. 6.º, n.º 1, al. b), do Regulamento 593/2008 (Roma I)[802].

Em termos práticos, esta alínea do art. 3.º, n.º 2, implica que, por exemplo, muitas lojas *online*, de empresas de nacionalidade estrangeira, sem subsidiária, filial ou representante no território da UE, fiquem abrangidas pelo RGPD quando oferecem bens ou serviços a titulares dos dados que se encontrem na UE devendo, por isso, ajustar os respetivos sítios *web*, por exemplo, ao exercício dos direitos do titular dos dados[803]. Veja-se o seguinte caso: a empresa "H" tem sede social no Brasil e vende fatos de banho numa loja *online*. Não tem subsidiárias ou representantes na UE e o seu sítio *web* está redigido apenas em português. "H" trata os dados pessoais das encomendas que recebe no seu sítio *web*. O pagamento é aceite em reais e em euros e os produtos podem ser entregues na Alemanha, França e Itália. Sempre que clientes situados na UE acedem ao sítio *web* são identificados através de técnicas de geolocalização e redirecionados do domínio ".br" para os domínios dos respetivos países. Neste exemplo, este redireccionamento, a possibilidade de pagamento em euros e de entrega na UE determinam que a empresa "H" tem a intenção de vender bens destinados ao mercado interno da União[804].

---

[798] Acórdão do TJ, Peter Pammer c. Reederei Karl Schluter GmbH & Co KG*,* C-585/08 e C-144/09, 7 de dezembro de 2010.
[799] Acórdão do TJ, Daniela Muhlleitner c. Ahmad Yusufi e Wadat Yusufi*,* C-190/11, 6 de setembro de 2012.
[800] Acórdão do TJ, Lokman Emrek c. Vlado Sabranovic*,* C-218/12, 17 de outubro de 2013.
[801] Relativo à competência judiciária, ao reconhecimento e à execução de decisões em matéria civil e comercial, de 12 de dezembro de 2012.
[802] Sobre a lei aplicável às obrigações contratuais (Roma I), de 17 de junho de 2008.
[803] M. BRKAN, "Data Protection …" cit., p. 338.
[804] Outros exemplos em Paul VOIGT e Axel BUSSCHE, *The EU General Data Protection Regulation (GDPR). A Practical Guide*, Springer, 2017, p. 27. Um exemplo semelhante a este é apresentado pelo G29, "EU general data protection regulation. General Information Document", 12 de fevereiro de 2018.

2.3.1.2.1. O controlo do comportamento na UE

O RGPD aplica-se também ao tratamento de dados pessoais de um titular situado no território da UE, efetuado por um utilizador de dados pessoais estabelecido fora da UE, mas cujas atividades implicam o "controlo do comportamento" daqueles titulares dos dados, "desde que esse comportamento tenha lugar na União".

A doutrina tem entendido que a alínea b) do número 2 do artigo 3 terá sido gizada para as atividades de definição de perfis[805], *online tracking* e publicidade comportamental, associadas a situações de controlo invisível do comportamento do titular dos dados através de soluções tecnológicas que permitem o acesso à informação no equipamento do utilizador[806]. Este controlo, por natureza, implica a monitorização permanente dos internautas e a criação de perfis que, por exemplo, são mais tarde utilizados para lhes apresentar anúncios baseados nos seus interesses[807]. A tecnologia mais usada no quadro da "publicidade comportamental" para monitorizar os utilizadores na Internet baseia-se nos chamados "testemunhos persistentes" ou "testemunhos de terceiros", pequenos textos alfanuméricos, instalados no equipamento terminal do utilizador que permite a terceiros criar um perfil comportamental do utilizador, das suas preferências, consumos e atitudes, para apresentar lhe publicidade personalizada[808].

Com efeito, de harmonia com o considerando 24, o tratamento de dados pessoais comporta o "controlo do comportamento" de titulares dos dados pessoais se estes são "seguidos na Internet" e houver uma "potencial utilização subsequente de técnicas de tratamento de dados pessoais que consistem em definir o perfil de uma pessoa singular, especialmente para tomar decisões relativas a essa pessoa ou analisar ou prever as suas preferências, o seu comportamento e as suas atitudes". Será o caso, por exemplo[809]: a

[805] A noção de "definição perfil" está no art. 4.º, n.º 2, do RGPD: "qualquer forma de tratamento automatizado de dados pessoais que consista em utilizar esses dados pessoais para avaliar certos aspetos pessoais de uma pessoa singular, nomeadamente para analisar ou prever aspetos relacionados com o seu desempenho profissional, a sua situação económica, saúde, preferências pessoais, interesses, fiabilidade, comportamento, localização ou deslocações". Há dois tipos de perfis: (i) implícitos, criados por inferência, com base na observação do comportamento individual e coletivo dos utilizadores ao longo do tempo, especialmente através da monitorização das páginas que estes visitaram e dos anúncios que visualizaram ou em que clicaram; (ii) explícitos, criados com base nos dados pessoais que os próprios fornecem a um serviço Web, nomeadamente na fase de registo. No caso da publicidade comportamental, tipicamente são usados os primeiros. Cfr. G29, "Parecer 2/2010 sobre publicidade comportamental em linha", 22 de junho de 2010, p. 7 e 8.

[806] B. ALSENOY, "Reconciling …" cit., p. 87; M. BRKAN, "Data Protection …" cit., p. 340; M. GOMANN, "The new territorial …" cit., p. 238.

[807] P. ASENSIO, "Competencia …" cit., p. 86 e ss.; Susana NAVAS NAVARRO, *La personalidade virtual del usuário de Internet,* Tirant lo Blanch, 2015, p. 149 a 193.

[808] Desenvolvendo, G29, "Parecer 2/2010 ...", p. 7 e ss..

[809] Em sentido semelhante, v. P. VOIGT e A. BUSSCHE, *The EU General* cit., p. 27.

empresa "A", com a sede social em Singapura, vende imobiliário oriental *online*. Os produtos só podem ser pagos em dólares e a entrega na UE não é possível. Contudo, "A" quer analisar o mercado interno da UE pois está a pensar expandir-se para aí. Qualquer pessoa que entre no sítio *web* tem de aceitar a utilização de "cookies" que, por seu turno, permitem a "A" descobrir se há pessoas que tenham acedido ao seu sítio *web* a partir da UE, e quais os produtos que procuram. Neste caso, a empresa "A" está a analisar as preferências de consumidores situados na UE pelo que o RGPD será aplicável.

2.3.1.3. O direito internacional público

O art. 3.º, n.º 3, do RGPD, dispõe que este regime será aplicado ao tratamento de dados pessoais efetuado por um RT não estabelecido na UE "mas num lugar em que se aplique o direito de um Estado-Membro por força do direito internacional público".

Quanto a esta norma, não havendo nenhuma novidade em relação ao art. 4.º, n.º 1, al. b), da Diretiva, as observações avançadas anteriormente a propósito do art. 4.º são válidas para a disposição do RGPD.

2.4. Caraterização da extraterritorialidade segundo o art. 4.º da Diretiva e o art. 3.º do RGPD

A pergunta que antecedeu os pontos 2.2. (a propósito do art. 4.º da Diretiva) e 2.3. (sobre o art. 3.º do RGPD) prendia-se com a forma como ambos alargam o âmbito de aplicação daqueles diplomas, "com implicações jurídicas que se estendem para lá do território da UE"[810]. Essas implicações indiciavam já uma dose de aplicação extraterritorial daqueles diplomas, ou seja, uma tentativa de regular, através de um ato legislativo (Diretiva e RGPD) a conduta de pessoas, bens ou atos" além-fronteiras[811].

Com efeito, do exposto decorre que tanto a Diretiva como o RGPD visam regular os tratamentos de dados pessoais efetuados por um utilizador de dados situado fora do território da UE em três situações:

(i) Quando aquele tratamento é indissociável das atividades de um estabelecimento situado no território da UE;

[810] G29, "Parecer 8/2010 ..." p. 10.
[811] CDI, "Report …" cit., nº 2.

(ii) Quando não exista um estabelecimento, mas o tratamento tem outra conexão com o território da UE: ou porque ali se situam os "meios" usados para a sua recolha, ou porque os tratamentos visam titulares dos dados que ali se encontram;

(iii) Por força do DIP.

Sendo estas, por agora, as três manifestações de extraterritorialidade do regime geral de proteção de dados pessoais, cabe indagar quais os *interesses* que prosseguem (2.4.1.) e quais os *princípios de jurisdição extraterritorial* subjacentes aos critérios estudados e que poderão fundamentar essa mesma jurisdição (2.4.2.).

2.4.1. Os interesses prosseguidos

Pelo menos em duas ocasiões o G29 mencionou o objetivo da "dimensão externa" do art. 4.º da Diretiva. Num primeiro momento, em 2002, esclareceu que a opção pelos "efeitos internacionais" do art. 4.º exprime a "preocupação de um determinado Estado de proteger os direitos e interesses dos seus cidadãos, residentes, indústria e outros agentes"[812]. Mais recentemente, em 2010, o G29 referiu que o objetivo do "vasto âmbito de aplicação" é duplo: garantir que "os particulares não se vejam privados da proteção a que têm direito nos termos da Diretiva e, em simultâneo, evitar que a lei seja contornada"[813].

Mas como podem os titulares dos dados ser "privados" da proteção a que têm direito sendo a lei contornada em simultâneo? É que este regime ergue um "elevado nível de proteção" [814] que contrasta com o direito vigente nos países terceiros, em particular nos chamados *data heaven*: "[A]s leis desses países terceiros não estão harmonizadas (...) e a proteção dos indivíduos no que diz respeito ao tratamento dos seus dados pessoais poderá, por isso, ser pouca ou nenhuma" [815]. Por isso, o legislador procurou proteger o titular dos

[812] G29, "Documento de trabalho sobre a determinação da aplicação internacional da legislação da UE em matéria de proteção de dados ao tratamento de dados pessoais na Internet efetuado por sites não europeus", 30 de maio de 2002, p. 3.
[813] G29, "Parecer 8/2010 ..." cit., p. 10.
[814] Art. 1.º e considerando 10 da Diretiva e art. 1.º e considerando 10 do RGPD.
[815] G29, "Documento de trabalho ..." cit., p. 7 e 8; C. KUNER, *European* p. 111; D. SVANTESSON, *Extraterritoriality* cit., p. 96; M. BRKAN, "Data Protection …" cit., p. 326. Em sentido próximo, Viviane

dados pessoais e garantir a integridade do nível de proteção criado, minimizando possíveis fraudes à lei, o *forum shopping* e retirando aos agentes económicos a possibilidade de escaparem às exigências da "elevada proteção" pela deslocalização dos tratamentos para um *data heaven* ou pela escolha da nacionalidade de um daqueles paraísos[816]. Por conseguinte, há uma certa proximidade entre este regime e as "leis-garra" estudadas na Parte I: aquele como que se "agarra" aos tratamentos de dados pessoais conexos com as atividades dos agentes económicos que formalmente são de nacionalidade estrangeira, mas cujos *efeitos* se fazem sentir no território da UE.

O mesmo entendimento decorre da jurisprudência do TJ, em especial quando esta instância sujeita a interpretação do art. 4.º ao "objetivo da Diretiva 95/46 de assegurar uma proteção eficaz e *completa* das liberdades e dos direitos fundamentais das pessoas singulares"[817]. Então, a extraterritorialidade propõe-se colmatar lacunas do direito estrangeiro cuja existência o legislador presumiu uma vez que não existe uma uniformização normativa global desta matéria. Recordando a definição de extraterritorialidade, um dos seus elementos é, justamente, a ausência de regulação pelo DIP pelo que a mesma, aos olhos da entidade do foro, é percecionada como um instrumento para suprir essa falha[818]. *Prima facie* a entidade do foro só pode exercer jurisdição extraterritorial na ausência de um consenso interestadual sobre a matéria em causa.

Ora, sempre se poderá invocar, no domínio da proteção de dados pessoais, que esse consenso existe e foi firmado na Convenção n.º 108 do CdE. Contudo, apesar de aberta a Estados que não são membros do CdE, o número de Estados nessa condição continua a ser bastante reduzido: o Uruguai e Marrocos foram os primeiros países a ser aceites [819].

REDING, "The European data protection Framework for the twenty-first century", *IDPL,* n.º 2, 2012, p. 127, justificando a expansão do RGPD a sujeitos situados em países terceiros, que atuam sobre indivíduos na UE, como uma forma de preencher lacunas na proteção destes.

[816] C. KUNER refere que um dos objetivos do art. 4.º foi "prevenir a possibilidade de evasão às regras da UE pela relocalização do tratamento de dados pessoais para países terceiros" e D. SVANTESSON explica que "na Diretiva da UE encontro um instrumento primeiramente vocacionada para regular os fluxos de dados internos àquela e para prevenir a chamada *fraude à la loi* (evasão fraudulenta)", v. C. KUNER, *European* p. 111; D. SVANTESSON, *Extraterritoriality* cit., p. 96; M. BRKAN, "Data Protection …" cit., p. 326. Em sentido próximo, v. Jan ALBRECHT, "Das Neue EU-Datenschutzrecht – von der Richtlinie zur Verordnung"*, Computer und recht*, n.º 2, 2016, p. 88 e ss.; L. MOEREL, *Binding* ... cit., p. 54; P. de HERT e M. CZERNIAWSKI, "Expanding the …", cit., p. 235.

[817] Acórdão do TJ, Google Spain SL e Google Inc. c. Agencia Española de Protección de Datos (AEPD) e Mario Costeja González*,* C-131/12, 13 de maio de 2014, n.º 53. Uma ideia repetida no Acórdão do TJ, Weltimmo s. r. o. c. Nemzeti Adatvédelmi és Információszabadság Hatóság*,* C-230/14, 1 de outubro de 2015, n.º 25.

[818] CDI, "Report …" cit., n.º 2.

[819] Graham GREENLEAF, "Morocco and Uruguay start Convention 108's journey to global privacy treaty", *PLBIR*, n.º 122, Abril de 2013.

A adesão depende de convite e de um processo de apreciação da adequação da proteção conferida pelo ordenamento jurídico do candidato[820]. Quer isto dizer que em relação a todos os Estados que não foram (ainda) considerados adequados, as razões que levam a UE a recorrer à extraterritorialidade são válidas. Todavia, tendo em conta o cada vez maior número de Estados convidados[821], julgo que o futuro da extraterritorialidade neste domínio não deverá ser indiferente a esta evolução. Ou, o mesmo é dizer, quanto menores as divergências entre o regime da UE e o direito estrangeiro, atenuadas pela ação do DIP, menos necessária será a intervenção da UE para colmatar lacunas regulatórias e mais reduzidos os números de *data heaven's*[822].

Recorrendo à classificação da Parte I, os interesses prosseguidos pela extraterritorialidade são, desde logo, interesses *internos*, da UE, no sentido em que tem o dever de garantir "o direito fundamental das pessoas singulares à proteção dos dados pessoais" na "UE e fora dela"[823]. Entre nós, F. CALVÃO, a propósito do art. 3.º do RGPD, sublinha a intenção do legislador garantir a tutela efetiva dos direitos dos titulares dos dados contra ingerências, independentemente do Estado onde se situa a sede da empresa que trata os dados[824]. Por conseguinte, creio que a extensão do DUE fora de portas aparece como um meio de realizar o *dever de proteção* que, como disse, vigora mesmo em relação a "perigos com conexões internacionais" e, dentro destes, "perigos externos com projeção interna"[825].

Tanto significa, por um lado, que esse dever atinge o utilizador de dados pessoais situado num país terceiro e, por outro lado, que a aplicação do direito derivado arrasta consigo a aplicação do direito originário, em especial da CDFUE. Quanto a esta segunda conclusão, a doutrina entende que, não existindo uma "cláusula de jurisdição" na CDFUE, os direitos fundamentais ali consagrados acompanham as "viagens" do direito derivado[826]. Além do domínio da proteção de dados pessoais, o mesmo fenómeno tem

[820] Graham GREENLEAF, "Modernising Data Protection Convention 108: A Safe Basis for a Global Privacy Treaty?", *CLSR*, vol. 29, n.º 4, 2013, p. 403 e ss. e Griet VERHENNEMAN e Fanny COUDERT, "Widening and strengthening the appeal of Convention 108", *DPLP,* Março de 2015, p. 8 e ss.
[821] Segundo o sítio do CdE, em processo de apreciação estão os seguintes países: Argentina, Burkina Faso, Maurícias, Senegal e Tunísia, v. https://www.coe.int/en/web/data-protection/convention108/parties, consultado no dia 30 de setembro de 2018.
[822] Em sentido próximo, v. C. KUNER, *Transborder* cit., p. 108.
[823] Comissão Europeia, "Uma abordagem ..." cit., p. 4.
[824] F. CALVÃO, "A proteção ..." cit., p. 6790.
[825] D. SVANTESSON, "Article 3 ..." cit., p. 5.
[826] V. M. BRKAN, "The Unstoppable …" cit., p. 831 e V. MORENO-LAX e C. COSTELO, "The extraterritorial application of the EU Charter …" cit., p. 1679.

sido constatado na proteção do consumidor (art. 38.º da CDFUE)[827] e do ambiente (art. 37.º da CDFUE)[828].

Esta relação entre os deveres de proteção de direitos fundamentais e a utilização da extraterritorialidade tem sido aflorada pela doutrina estrangeira[829]. M. TAYLOR sustenta que, por força do art. 8.º da CDFUE, a UE tem uma obrigação positiva de ativamente proteger os direitos fundamentais prevenindo violações de terceiros, mesmo dos que se acham fora do seu território. Para a autora o caso *Google Spain* exemplifica essa obrigação: "por força do estabelecimento de uma subsidiária em Espanha, a Google Inc., incorporada num país terceiro (os EUA), foi considerada responsável por interferir nos direitos fundamentais de um cidadão da UE"[830]. P. DE HERT e M. CZERNIAWSKI concordam com este entendimento[831], tal como C. KUNER que sugere o seguinte: "[o]s Estados podem ter uma obrigação de proteger os indivíduos de atividades de sujeitos privados extensível a situações que envolvem fluxos de dados transfronteiriços" [832]; mais recentemente aquele autor invoca "a obrigação positiva de um Estado garantir o respeito pelos direitos fundamentais das pessoas sujeitas à sua jurisdição de violações de quaisquer sujeitos privados"[833]. É também essa a ideia defendida por V. ALSENOY[834] e D. SVANTESSON[835]. Por fim, também na doutrina alemã a extraterritorialidade é descrita como meio de reforçar a proteção dos direitos fundamentais[836].

Além deste interesse *interno*, intimamente relacionado com a dimensão jusfundamental do regime estudado, vislumbra-se um outro interesse, de índole económica ou de estruturação do mercado interno: a proteção de responsáveis pelo tratamento e subcontratantes com atividade apenas na UE, através da correção de uma alegada vantagem concorrencial dos seus equivalentes estrangeiros, localizados em *data heaven's* mas com atividade económica no mercado interno, que estão libertos dos "custos de contexto" criados na área da proteção de dados pessoais pela União. Esta

[827] N. COX, "The extraterritorial …" cit., p. 60 e ss..
[828] Tetsuya MORIMOTO, "Growing industrialization and our damaged planet: The extraterritorial application of developed countries' domestic environmental laws to transnational corporations abroad", *ULR,* n.º 1, 2005, p. 134 e ss..
[829] M. TAYLOR, "The EU's human rights …" cit., p. 246 e ss..
[830] *Idem*, p. 254.
[831] P. de HERT e M. CZERNIAWSKI, "Expanding the …", cit., p. 235.
[832] C. KUNER, *Transborder* cit., p.130.
[833] C. KUNER, "The Court of Justice …" cit., p. 12 e M. MILANOVIC, *Extraterritorial* cit., p. 210.
[834] B. ALSENOY, "Reconciling …" cit., p. 93.
[835] D. SVANTESSON, *Extraterritoriality* cit., p. 131.
[836] M. GOMANN, "The new territorial…" cit., p. 568; Peter SCHANTZ, "Die Datenschutzgrundverordnung. Beginn einer neuen Zeitrechnung im Datenschutzrecht", *NJW,* n.º 26, 2016, p. 1842; Ulrich DAMMANN, "Erfolge und Defizite der EU-Datenschutzgrundverordnung", *Zeitschrift fur Datenschutz,* 2016, p. 309.

intenção de criar igualdade de circunstâncias é avançada por alguns autores [837], pelo próprio relator do PE[838], e foi aflorada pela vice-presidente da COM, em 2014, quando afirmou que o RGPD "pretende criar igualdade de condições entre empresas europeias e não europeias. [O RGPD] é sobre concorrência justa num mundo globalizado"[839]. Sugestivamente, o G29 havia já defendido que a extraterritorialidade exprime a preocupação da UE de proteger os interesses da sua "indústria e de outros agentes" [840].

2.4.2. Os princípios da jurisdição extraterritorial

Existindo um consenso quanto à desadequação de uma visão estritamente territorial para regular a relação jurídica no âmbito do tratamento de dados pessoais, a questão verdadeiramente controvertida prende-se com o princípio mais adequado para fundamentar a extraterritorialidade[841]. Por exemplo, o princípio da territorialidade pode ser usado, pelo menos, com base no local: (i) do armazenamento (em servidores ou outra infraestrutura informática) dos dados pessoais; (ii) onde se encontra o titular dos dados e onde se produzem os *efeitos* do tratamento ou (iii) onde se encontra o utilizador dos dados pessoais (sedeado ou estabelecido). Por seu turno, o princípio da nacionalidade poderá dar origem à jurisdição sobre um utilizador de dados pessoais nacional de um dado Estado ou sobre um titular dos dados nacional de outro Estado[842]. Qual terá sido a opção do legislador da UE? Será a mesma na Diretiva e no RGPD? E trata-se de extraterritorialidade pura ou impura*?*

---

[837] B. ALSENOY e M. KOEKKOEK, "Internet and …" cit., p. 110; B. ALSENOY, "Reconciling …" cit., p. 94; D. SVANTESSON, "Article 4 …" cit., p. 210 e, do mesmo autor, "Article …" cit., p. 9; M. GOMANN, "The new territorial …" cit., p. 568; P. de HERT e M. CZERNIAWSKI, "Expanding the …", cit., p. 235; Radim POLCÁK e Dan SVANTESSON, *Information Sovereignty. Data Privacy, Sovereign Powers and the Rule of Law,* Edward Elgar Publishing, 2017, p. 218 e ss..

[838] J. ALBRECHT, "Das neue …" cit., p. 4.

[839] Viviane REDING, "The EU data protection Regulation: Promoting technological innovation and safeguarding citizen's rights – Intervention at the Justice Council", 4 de março de 2014, disponível em http://europa.eu/rapid/press-release_SPEECH-14-175_en.htm, consultado no dia 30 de setembro de 2018.Esta tese seria reiterada pela mesma no debate no PE, do dia 11 de março de 2014, disponível em http://www.europarl.europa.eu/sides/getDoc.do?type=CRE&reference=20140311&secondRef=ITEM-013&language=PT&ring=A7-2013-0402, consultado no dia 30 de setembro de 2018.

[840] G29, "Documento de trabalho ..." cit., p. 3.

[841] François RIGAUX, "La loi applicable à la protection des individus à l'égard du traitement automatisé des données à caractere personnel", *RCDIP,* 1980, p. 443 e ss..

[842] Sintetizando os termos do debate, v. a posição do Relator Especial da ONU para a privacidade na sua intervenção enquanto *Amicus Curiae* no caso Microsoft, estudado adiante, *United States of America* v. *Microsoft Corporation,* "Brief of Amicus Curiae of U.N. Special Rapporteur on the Right to Privacy Joseph Cannatazi In Support of Neither Party", 13 de dezembro de 2017, p. 23, disponível em https://www.supremecourt.gov/search.aspx?filename=/docket/docketfiles/html/public/17-2.html , consultado no dia 30 de setembro de 2018.

A principal preocupação da opção legislativa na delimitação do âmbito de aplicação deste regime foi, conforme explicou o G29, verificar a existência de "um elo suficientemente estreito e genuíno" entre a UE e "o objeto ou a situação que pretende regular" ou a "ligação relevante" entre o tratamento de dados e a UE[843]. Isto dito, o que se pergunta é: quais são os elos inscritos no art. 4.º da Diretiva e no art. 3.º do RGPD e quais os princípios de jurisdição extraterritorial que refletem?

A formulação textual do art. 4.º parece excluir, pelo menos, o princípio da nacionalidade, tanto do RT como do titular dos dados, bem como o princípio da territorialidade, entendido no sentido da localização física dos dados pessoais[844]. Porém, o princípio da territorialidade, mesmo que não absoluto ou rigoroso, é o epicentro daquela norma[845]. É assim em relação ao art. 4.º, n.º 1, al. a), espoletado por força da localização no território de um Estado-Membro de um "estabelecimento" do RT, indicador de um certo nível da sua presença física ali e do exercício de atividade económica: "se uma empresa está estabelecida e opera no território de um Estado, então tem de jogar segundo as suas regras"[846]. Quanto ao art. 4.º, n.º 1, al. b), não se vislumbra nenhum princípio específico já que a aplicação do DUE resulta, por exemplo, de um acordo internacional. Por seu turno, o art. 4.º, n.º 1, al. c), expressa o princípio da territorialidade objetiva uma vez que pelo menos uma parte da conduta – o recurso a "meios" para o tratamento de dados pessoais – ocorre dentro da UE. Nestes casos a recolha de dados pessoais, por exemplo, decorreria ali.

Acresce que, bem vistas as coisas, tanto em relação à alínea a) como à alínea c) é possível, e porventura mais rigoroso, invocar a doutrina dos efeitos: os *efeitos* dos tratamentos de dados pessoais que ocorrem total (art. 4.º, n.º 1, al. a) e no caso *Google Spain*) ou parcialmente (art. 4.º, n.º 1, al. c)) no estrangeiro fazem-se sentir no território da UE por duas vias: seja porque estão relacionados com a atividade de um estabelecimento do utilizador dos dados pessoais situado no território da UE ou porque pressupõem o recurso a "meios" que envolvem o controlo de um titular dos dados que ali se encontra[847]. A adequação desta doutrina é mais evidente no caso da al. a) porquanto,

[843] G29, "Parecer 8/2010 ..." cit., p. 6.
[844] *Idem*, p. 9.
[845] É esse o entendimento maioritário da doutrina, v. B. ALSENOY, "Reconciling …" cit., p. 81 e 91; C. KUNER, *European* cit., p. 117 e ss.; K. HON *et alii,* "Data Protection Jurisdiction ..." cit., p. 129; L. COLONNA, *Legal* cit., p. 340 e 345; M. GOMANN, "The new territorial …" cit., p. 579; U. DAMMANN e S. SIMITIS, *EG-Datenschutzrichtlinie* cit., p. 127 e ss..
[846] B. ALSENOY, "Reconciling …" cit., p. 91 e 92.
[847] C. KUNER, "Data Protection Law …" cit., p. 176 e ss. e L. COLONNA, *Legal* cit., p. 345.

ao invés de incidir sobre o tratamento realizado pelo próprio estabelecimento, visa regular o tratamento operado pelo RT que, como no caso *Google Spain*, ocorreu no estrangeiro, mas tem impacto nas atividades da *Google Spain* – no limite esta deixaria de existir sem aqueles tratamentos[848].

Também o elemento textual do art. 3.º, afasta considerações sobre a nacionalidade, tanto do utilizador dos dados pessoais como do titular dos mesmos. O art. 3.º, n.º 1, do RGPD permanece, grosso modo, semelhante ao art. 4.º, n.º 1, al. a), da Diretiva, pelo que vale também aqui o que foi dito. Já o número 2 elege como ligação relevante o lugar onde se situa territorialmente o (potencialmente) afetado pelo tratamento de dados pessoais, o titular dos dados, numa manifestação da doutrina dos efeitos. Esta interpretação é corroborada pela doutrina[849] e pelo G29 ao afirmar que o âmbito de aplicação deste regime, alargado pelo caso *Google Spain*, "será ampliado ainda mais no futuro" pelo RGPD "que, mais diretamente, assenta no 'princípio dos efeitos' para completar o 'princípio da territorialidade' no que respeita às atividades na UE de responsáveis pelo tratamento estrangeiros"[850].

Capítulo 3 – O regime das transferências de dados pessoais

3.1. Da Diretiva ao RGPD

3.1.1. A Diretiva

Do art. 25.º, n.º 1, conjugado com o considerando 57, resulta uma "restrição"[851] ou uma "proibição"[852] à transferência de dados pessoais para um país terceiro. Melhor dizendo, do elemento textual, resulta um *princípio* segundo o qual uma transferência "só pode realizar-se se (...) o país terceiro em questão assegurar um nível de proteção adequado". O artigo seguinte consagra duas derrogações a este princípio: o n.º 1 dispõe que as transferências possam ocorrer, independentemente da adequação do país terceiro,

[848] B. ALSENOY, "Reconciling …" cit., p. 92 e L. MOEREL, "The long …" cit., p. 28 e ss..
[849] B. ALSENOY, "Reconciling the …" cit., p. 95; D. SVANTESSON, *Extraterritoriality* cit., p. 140 e P. ASENSIO, "Competencia …" cit., p. 89 e ss... Em defesa desta solução invoca-se um documento da Convenção de Haia de Direito Internacional Privado, entitulado "Les échanges de données informatisés, Internet et le commerce electronique", Doc. Prel. N.º 7, abril de 2000, p. 25.
[850] G29, "Update of …" cit., p. 5 e 6.
[851] K. HON, *Data Localization* cit., p. 3 e ss..
[852] C. KUNER, "Extraterritoriality and …" cit., p. 235 e ss.; G29, "Working Document on surveillance of electronic communications for intelligence and national security purposes", 5 de dezembro de 2014, p. 38.

num conjunto de situações elencadas, e o n.º 2 sujeita-as à apresentação de "garantias suficientes" pelo RT.

O elemento comum a estas três hipóteses é a exigência de que o RT realize as transferências para países terceiros com base numa condição de licitude ou num fundamento *autónomo* em relação ao plasmado no art. 6.º[853]. É dessa específica condição de licitude que trato nos pontos que se seguem.

3.1.1.1. Os fundamentos das transferências

3.1.1.1.1. A decisão de adequação

O primeiro fundamento decorre do seguinte princípio: a adequação do nível de proteção do país terceiro ou de destino. Este é um *país terceiro* em relação à UE, excluído do efeito uniformizador da Diretiva, pelo que se tem considerado que esta solução regulatória assenta numa *geographical approach*, isto é, na localização ou "destino" geográfico dos dados pessoais transferidos e, em especial, no grau de proteção aí vigente[854].

Ora, se os dados pessoais só podem ser transferidos para países com um certo nível de proteção, tal pressupõe uma apreciação *ex ante* da mesma. A quem compete essa tarefa, quais os seus trâmites e como se mede essa adequação?

a) Competência

A *competência* para apreciar a adequação do nível de proteção do país terceiro estava repartida entre os Estados-Membros e a COM[855]. Os primeiros poderiam escolher os meios para dar cumprimento ao art. 25.º: fosse a instituição de sistemas de autorização prévia das transferências ou de fiscalização *ex post facto* pela autoridade de controlo conferindo, neste caso, ao utilizador dos dados pessoais a faculdade de autoavaliar a adequação do país terceiro [856]. Atendendo ao elevado número diário de fluxos de dados

[853] Consentimento, execução de um contrato, obrigação jurídica, entre outros.
[854] C. KUNER, *Transborder* cit., p. 64; K. HON, *Data Localization* cit., p. 57.
[855] Art. 25.º, n.º 3, 4, 5 e 6.
[856] G29, "Primeiras orientações sobre as transferências de dados para países terceiros – eventual metodologia a adotar para avaliar a adequação do grau de proteção", 26 de junho de 1997, p. 6. A autoavaliação da adequação era permitida, por exemplo, no Reino Unido, v. ICO, "The Eight Data Protection Principle in International Data Transfers v4", 2010, p. 9, disponível em https://ico.org.uk/media/for-organisations/documents/1566/international_transfers_legal_guidance.pdf,

pessoais e à multiplicidade dos atores envolvidos nesses processos, o G29 reconheceu que "nenhum Estado-membro (...) poderá garantir um exame pormenorizado de todos os casos" sugerindo a "criação de mecanismos suscetíveis de racionalizar o processo de tomada de decisões" e, em especial, de um sistema de gestão das prioridades dos trabalhos a empreender pela autoridade de controlo em face do risco especial de uma certa transferência ou categoria de transferências[857].

Quanto às incumbências atribuídas à COM nos termos do art. 25.º, n.º 6, cabia-lhe verificar o "nível de proteção adequado" através do procedimento de comitologia consagrado no art. 31.º. Sem prejuízo de voltar a este aspeto, nomeadamente na Parte III, por agora basta sublinhar que a comitologia é apenas um dos momentos de um procedimento complexo, demorado e faseado noutros momentos: (i) um pedido formal pelo país terceiro que pretende ser declarado adequado; (ii) um estudo jurídico preparado por uma instituição académica a pedido da COM; (iii) um parecer do G29; (iv) um parecer do Comité do art. 31.º, composto por representantes dos Estados-Membros e presidido pelo representante da COM; (iv) um período de 30 dias de escrutínio pelo PE que pode sugerir recomendações (não vinculativas) e, por fim, (v) um parecer do colégio de comissários [858].

O culminar deste procedimento era, segundo o art. 31.º, uma "medida de execução", correntemente designada "decisão de adequação", com efeitos *internos* e *externos*[859]. Internamente, esta decisão visava (e, como veremos, ainda visa) uniformizar e flexibilizar as condições das transferências de dados pessoais lícitas gerando uma presunção sobre a adequação do nível de proteção do país terceiro cujo efeito era autorizar, por defeito, as transferências para o mesmo. Como sintetizou o G29, existindo uma decisão de adequação as transferências para o país terceiros seriam tratadas como as exportações dos dados pessoais para os Estados-Membros[860]. Externamente, a decisão de adequação

consultado no no dia 30 de setembro de 2018. Na prática isto significava que o RT adotava as medidas que bem entendesse, jurídicas ou técnicas (por exemplo de encriptação) para acautelar os riscos da transferência, v. K. HON, *Data Localization* cit., p. 153.

[857] G29, "Primeiras orientações ..." cit., p. 3, 5 e 6.

[858] Comissão Europeia, "Commission decisions on adequacy of the protection of personal data in third countries", disponível em http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/index_en.htm, consultado no dia 30 de setembro de 2018.

[859] Até à data contam-se 13 decisões de adequação: Andorra, Argentina, Canadá, as Ilhas Faroé, Israel, a Ilha do Homem, Nova Zelândia, Suíça, Uruguai, entre outros enumerados em www.ec.europa.eu/justice/data-protection/document/international-transfers/adequacy/index_en.htm, consultado no dia 30 de setembro de 2018. No mesmo sítio é possível consultar o projeto de decisão de adequação do Japão.

[860] G29, "Working Document on surveillance ..." cit., p. 38.

corporizava um juízo de apreciação sobre o nível de proteção do ordenamento jurídico de um país estrangeiro. Esse juízo poderia ser *negativo* e, nesse caso, desencadeava, nos termos do art. 25.º, n.os 4 e 5, um procedimento de negociações com o país terceiro para corrigir a constatação resultante do procedimento de comitologia.

b) Os critérios da apreciação

Quanto aos critérios de determinação do nível de proteção adequado, o art. 25.º, n.º 2, indicava que deveriam ser atendidas "todas as circunstâncias que rodeiem a transferência ou o conjunto de transferências de dados" e enumerava, de modo não exaustivo, aquelas que deveriam ser tidas em conta: a natureza dos dados, a finalidade e a duração do tratamento, os países de origem e de destino final, as regras de direito, gerais e setoriais, as regras profissionais e as medidas de segurança. Estas indicações deveriam conformar os processos de autoavaliação permitidos em certos Estados (*v.g.* Reino Unido) aos utilizadores de dados pessoais. O n.º 6, especialmente dirigido à COM, dispunha que a mesma apreciava a "legislação interna" ou os "compromissos internacionais" do país terceiro tendo em vista a "proteção do direito à vida privada e das liberdades e direitos fundamentais das pessoas". A Convenção n.º 108 do CdE desempenhava uma função importante na medida em que o legislador presumia a adequação do nível de proteção dos países que a ratificaram[861].

Nas suas orientações sobre transferências para países terceiros, o G29 sugeriu que a adequação fosse avaliada tendo por base o modelo de proteção instituído pela Diretiva e dividido em dois níveis: (i) regras "materiais" ou "princípios respeitantes ao conteúdo" e (ii) "meios destinados a assegurar uma aplicação eficaz" ou "mecanismos processuais ou de aplicação" [862]. O primeiro nível congregava os *princípios básicos* (limitação do tratamento, proporcionalidade, qualidade, transparência, segurança, respeito pelos direitos do titular dos dados, e a vigência de restrições relativas a transferências subsequentes para outros países terceiros) e os princípios adicionais aplicáveis a tipos específicos de tratamento (dados sensíveis, no *marketing* direto, e em relação a decisões individuais e automatizadas).

O segundo nível conferia eficácia ao primeiro, distinguindo-se os mecanismos processuais gerais, como sanções pelo não cumprimento da Diretiva e o direito de recurso

[861] G29, "Primeiras orientações ..." cit., p. 10 e 11.
[862] *Idem*, p. 7.

judicial, dos mecanismos processuais complementares, como a criação de autoridades de controlo. Quanto a estes, era essencial apurar se o sistema de proteção do país terceiro prosseguia três objetivos: garantir um nível satisfatório de observância das regras materiais[863], conceder apoio e assistência aos titulares dos dados[864] e assegurar meios de recurso adequados[865].

Como se vê, a metodologia e os critérios para apreciar o nível de proteção do país terceiro parte das normas da Diretiva. Pretendia-se garantir que os tratamentos posteriores, realizados fora da UE na sequência de uma transferência, continuassem a ser regidos por um conjunto de normas respeitantes ao "teor" do DUE no domínio da proteção de dados pessoais que, por seu turno, eram garantidas por mecanismos processuais de aplicação das mesmas[866]. Ou seja, esta metodologia tem em vista *garantir a continuidade* da aplicação do modelo de proteção instituído pela Diretiva aos dados pessoais transferidos para países terceiros.

3.1.1.1.2. As garantias suficientes

Como dispõe o considerando 56, o legislador atendeu às exigências de flexibilidade que o desenvolvimento do comércio internacional pressupõe em termos de transferências internacionais de dados pessoais[867]. Uma concretização desta preocupação é a possibilidade de derrogação do art. 26.º, n.º 2, viabilizando transferências para países terceiros que não assegurassem uma proteção adequada e remetendo o ónus dessa tarefa para os próprios agentes económicos. Como sublinhou o G29, "sempre que esteja previsto transferir dados pessoais para um país terceiro [não adequado], *os responsáveis pelo tratamento estabelecidos na União Europeia devem preconizar soluções que facultem às pessoas em causa a garantia de que, mesmo depois de transferidos os seus dados,*

[863] Segundo o G29 um "bom sistema" carateriza-se com base nos seguintes elementos: tanto os responsáveis pelo tratamento de dados como os titulares dos mesmos deverão ter um "conhecimento profundo" sobre as suas obrigações e sobre os seus direitos e meios de exercício e tutela, respetivamente. Por outro lado, a existência de sanções eficazes e dissuasoras e de sistemas de controlo direto pelas autoridades, auditores e funcionários independentes responsáveis pela proteção de dados são outros dos elementos, v. G29, "Primeiras orientações ..." cit., p. 9 e 10.

[864] Os titulares dos dados devem poder exercer os seus direitos de forma rápida e efetiva, sem custos excessivos. Para tal deverá existir um mecanismo para investigar, de forma independente, as queixas apresentadas pelos titulares dos dados, v. G29, "Primeiras orientações ..." cit., p. 10.

[865] O sistema deve garantir meios de reparação adequados no caso de infração às normas vigentes, que permitam um julgamento imparcial da infração, que poderá dar origem, quando necessário, ao pagamento de uma indemnização adequada e à imposição de sanções, v. G29, "Primeiras orientações ..." cit., p. 10.

[866] G29, "Primeiras orientações ..." cit., p. 7.

[867] Reiterando esta ideia, v. G29, "Documento de Trabalho sobre uma interpretação comum do n.º 1 do artigo 26.º da Diretiva 95/46", 24 de outubro de 1995, p. 8.

continuarão a beneficiar dos direitos fundamentais e das garantias a que têm direito na UE" (itálicos meus) [868]. Estas "soluções" traduziam-se na apresentação, pelo RT que pretendesse exportar os dados pessoais, de "garantias suficientes de proteção da vida privada e dos direitos e liberdades fundamentais das pessoas, assim como do exercício dos respetivos direitos"[869]. Em poucas palavras, aquele devia certificar-se de que o "destinatário providencia proteção adequada"[870].

Portanto, as garantias suficientes distinguiam-se da decisão de adequação e do procedimento que a antecedia dada a lógica organizacional (*organizationally-based approach*) a que obedeciam, centrada menos no destino geográfico dos dados pessoais, no país de destino, e mais nas medidas adotadas pelo exportador e pelo importador para garantir a proteção dos dados pessoais[871].

3.1.1.1.2.1. A solução contratual

Entre as garantias suficientes o legislador destacou as "cláusulas contratuais adequadas" acrescentando, no art. 26.º, n.º 4, que a COM tinha poder para determinar, nos termos do procedimento de comitologia, que certas cláusulas contratuais-tipo garantiam a proteção depois de realizada a transferência. Desde 1995, a COM desenvolveu dois modelos de cláusulas contratuais-tipo consoante a natureza do exportador e do importador dos dados pessoais: (i) quando ambos são responsáveis pelo tratamento[872] e (ii) quando o primeiro é RT e o segundo ST[873].

[868] G29, "Documento de Trabalho sobre uma ..." cit., p. 10.
[869] Art. 26.º, n.º 2.
[870] G29, "Documento de Trabalho sobre uma ..." cit., p. 8.
[871] C. KUNER, *Transborder* cit., p. 71 e K. HON, *Data Localization* cit., p. 190.
[872] Para as transferências entre responsáveis pelo tratamento existem dois conjuntos de cláusulas ao abrigo da Decisão da Comissão de 15 de junho de 2001 relativa às cláusulas contratuais-tipo aplicáveis à transferência de dados pessoais para países terceiros, nos termos da Diretiva 95/46/CE (Decisão 2001/497/EC) e ao abrigo da Decisão da COM de 27 de Dezembro de 2004 que altera a Decisão 2001/497/EC no que se refere à introdução de um conjunto alternativo de cláusulas contratuais típicas aplicáveis à transferência de dados pessoais para países terceiros (Decisão 2004/915/EC). Qualquer um destes modelos pode ser usado apesar de se registar uma preferência pelos segundos por incorporarem alterações sugeridas pelos agentes económicos, v. Kuan HON e Christopher MILLARD, "Data Export in Cloud Computing – How Can Personal Data Be Transferred Outside the Eea? The Cloud of Unknowing, Part 4", *SCRPIT-ed,* vol. 9, n.º 25, 2011, p. 20 e Samson ESAYAS, "A walk in to the Cloud and Cloudy it Remaisn: The Challenges and Prospects of 'Processing' and 'Transferring' Personal Data", *CLSR,* n.º 28, 2012, p. 672.
[873] Decisão da Comissão de 5 de fevereiro de 2010 relativa a cláusulas contratuais-tipo aplicáveis à transferência de dados pessoais para subcontratantes estabelecidos em países terceiros nos termos da Diretiva 95/46/CE do Parlamento Europeu e do Conselho (Decisão 2010/87/EU).

No passado, os agentes económicos manifestaram um grande interesse nesta solução "pronta a usar" dada a não exigência de uma autorização administrativa prévia o que, para transferências pouco complexas, era fonte de libertação de encargos administrativos e burocráticos[874]. Por exemplo, o art. 20.º da Lei n.º 67/98[875], dispunha que a CNPD autorizava as transferências de dados pessoais efetuadas ao abrigo de tais cláusulas. Pelo contrário, um contrato *ad hoc* só seria considerado uma garantia suficiente depois de submetido ao controlo da autoridade de controlo[876].

A solução contratual, como meio de regular transferências de dados pessoais, é anterior à adoção da Diretiva. Em 1992, o CdE, a Câmara de Comércio Internacional e a COM elaboraram um estudo propondo um contrato modelo com os seguintes objetivos: (i) apresentar um exemplo para a solução dos problemas dos fluxos de dados pessoais sujeitos a vários regimes de proteção de dados; (ii) facilitar as transferências internacionais de dados em benefício do comércio internacional e (iii) promover a segurança e a certeza das transações internacionais[877].

Em suma, esta garantia especificada pelo legislador era – e, como se verá, ainda é – um meio de compensar a ausência de um certo nível de proteção no país terceiro, através da inclusão nas cláusulas contratuais de disposições que assegurem as regras materiais de proteção de dados e os mecanismos processuais para o titular dos dados pessoais, designadamente apoio e assistência no que se refere ao exercício dos seus direitos e de meios de reparação adequados quando sofra danos por via do não cumprimento daquelas regras[878]. Assim se procura assegurar a continuidade da proteção do titular dos dados, o beneficiário neste contrato, mesmo depois de transferidos os seus dados pessoais para um país terceiro.

---

[874] Abraham NEWMAN, "Building Transnational Civil Liberties: Transgovernmental Entrepreneurs and the European Data Privacy Directive", *IO,* vol. 62, n.º 1, 2008, p. 103 e ss.; Alexander ZINSER, "The European Commission Decision on Standard Contractual Clauses for the Transfer of Personal Data to Third Countries: an Effective Solution?", *CKJIP*, n.º 3, 2003, p. 24; Joel REIDENBERG, "Rules of the Road for Global Electronic Highways: Merging the Trade and Technical Paradigms", *HJLT,* n.º 6, 1992-1993, p. 287 e ss.; Lingjie KONG, "Data Protection and Transborder Data Flow in the European and Global Context", *TEJIL,* vol. 21, n.º 2, 2010, p. 441 e ss.; Rolf WEBER, "Transborder data transfers: concepts, regulatory approach and new legislative initiatives", *IDPL,* vol. 3, n.º 2, 2013, p. 128.

[875] Este diploma de 26 de outubro, designada "Lei da Proteção de dados pessoais", transpunha para a ordem jurídica portuguesa a Diretiva 95/46.

[876] Art. 26.º, n.º 2.

[877] "Model Contract to Ensure Equivalent Data Protection in the Context of Transborder Data Flows with Explanatory Memorandum", 2 de novembro de 1992, disponível em https://www.edoeb.admin.ch/datenschutz/00626/00753/index.html?lang=en&download=NHzLpZeg7t,lnp6I0NTU042l2Z6ln1ad1IZn4Z2qZpnO2Yuq2Z6gpJCDdYB6fGym162epYbg2c_JjKbNoKSn6A--, consultado no dia 30 de setembro de 2018; Yves POULLET *et alii* "Data Protection and Privacy in Global Networks: a European Approach", *EDILR,* vol. 8, n.º 2 e 3, 2001, p. 172.

[878] G29, "Documento de Trabalho: observações preliminares ..." cit., p. 4 e 11.

3.1.1.1.2.2. As regras vinculativas aplicáveis às empresas ("RVAE")

Não sendo expressamente mencionadas na Diretiva, as RVAE configuram uma nova manifestação da flexibilidade que o comércio internacional impõe tal como refere o considerando 56 da Diretiva. Estas regras nasceram de uma interpretação extensiva do conceito de garantias suficientes impulsionada pela constatação das autoridades de controlo de que, no atual cenário internacional, a dimensão e a natureza das atividades de muitos operadores económicos exige uma estratégia *global* de proteção de dados pessoais.

Por conseguinte, entre 2003 e 2015, o G29, em diálogo com aqueles operadores, desenvolveu um modelo de regras internas para as transferências de dados pessoais realizadas por multinacionais dispersas por vários pontos do mundo[879]. Nestes casos, fosse a transferência fundamentada num contrato, tal exigia um complexo e oneroso processo de conclusão de múltiplos contratos com as várias entidades do mesmo grupo. As RVAE vieram a ser expressamente consagradas no RGPD, na cartilha das "garantias adequadas" do art. 46.º, n.º 2, pelo que remeto a sua apreciação para esse novo enquadramento normativo.

3.1.1.1.3. Derrogações em sentido estrito

Optei por esta designação ("derrogações em sentido estrito") para distinguir este fundamento das situações que acabei de analisar, do art. 26.º, n.º 2, sob a epígrafe genérica "derrogações". O número 1 desta norma consagrava estas "derrogações em sentido

[879] G29, "Explanatory Document on the Processor Binding Corporate Rules", 19 de abril de 2013 e revisto a 22 de maio de 2015, p. 4; "Working Document on Transfers of personal data to third countries: Applying Article 26 (2) of the EU Data Protection Directive to Binding Corporate Rules for International Data Transfers", 3 de junho de 2003; "Model Checklist Application for approval of Binding Corporate Rules", 25 de novembro de 2004; "Working Document Setting Forth a Co-Operation procedure for issuing Common Opinions on Adequate Safeguards Resulting From 'Binding Corporate Rules'", 14 de abril de 2005; "Working Document Establishing a Model Checklist Application for Approval of Binding Corporate Rules", 14 de abril de 2005; "Recommendation 1/2007 on the Standard Application for Approval of Binding Corporate Rules for the Transfer of Personal Data", 10 de janeiro de 2007; "Working Document setting up a table with the elements and principles to be found in Binding Corporate Rules", 24 de junho de 2008; "Working Document setting up a framework for the structure of Binding Corporate Rules", 24 de junho de 2008; "Working Document on Frequently Asked Questions (FAQs) related to Binding Corporate Rules", 24 de junho de 2008; "Recommendation 1/2012 on the Standard Application form for Approval of Binding Corporate Rules for the Transfer of Personal Data for Processing Activities", 17 de setembro de 2012; "Working Document 02/2012 setting up a table with the elements and principles to be found in Processor Binding Corporate Rules", 6 de junho de 2012; "Opinion 02/2014 on 'Referential for requirements for Binding Corporate Rules submitted to national data protection authorities in the EU and Cross Border Privacy Rules submitted to APEC CBPR Accountability Agents", 27 de fevereiro de 2014.

estrito" num elenco taxativo de situações que excluíam a exigência de uma decisão de adequação ou da apresentação de garantias suficientes. Por outras palavras, nestas situações, o RT não precisava de se certificar de que o destinatário providenciava a proteção adequada ou que vigorava uma decisão de adequação, pelo que não havia qualquer mecanismo para assegurar a continuidade da proteção do titular dos dados pessoais[880].

O recurso a estas derrogações pautava-se pela "necessária rigidez de interpretação" e pelo respeito do "princípio inerente à legislação europeia de que as cláusulas relativas a exceções sejam interpretadas com rigidez" de forma a que não se transformem na regra[881]. Como explicou o G29, "esta regra de interpretação estrita deriva claramente também da jurisprudência do Tribunal Europeu dos Direitos do Homem que interpreta os direitos fundamentais de maneira bastante ampla, de acordo com o *princípio do efeito útil* (*principe d'effet utile*) da proteção garantida, para limitar o âmbito das derrogações ao mesmo"[882]. Tanto sugere que as "derrogações em sentido estrito" deveriam ser o último recurso para a fundamentação das transferências.

3.1.2. O RGPD

3.1.2.1. A reforma de 2012: o que há de novo?

Em 2003, o diagnóstico da COM sobre a implementação da Diretiva quanto ao Capítulo 4 não era positivo e as divergências na respetiva transposição, consideradas "excessivas", variavam entre: uma abordagem que remitia a avaliação do nível de proteção do país terceiro para o RT com o controlo *ex post* da autoridade de controlo; e uma outra, exigindo a submissão de todas as transferências para países terceiros a uma autorização administrativa prévia[883]. Reconheciam-se as crescentes necessidades "do comércio internacional" e o impacto "das redes globais de telecomunicações" e lançava-se um alerta: um regime demasiado rigoroso poderia "criar uma lacuna entre a lei e a prática que seria prejudicial para a credibilidade da diretiva e para o direito comunitário

[880] G29, "Documento de Trabalho. Transferência de dados pessoais para países terceiros: aplicação dos artigos 25.º e 26.º da Diretiva comunitária relativa à proteção dos dados", 24 de julho de 1998, p. 26 e G29, "Documento de Trabalho sobre uma ..." cit., p. 8.
[881] G29, "Documento de Trabalho sobre uma ..." cit., p. 9.
[882] *Ibidem*.
[883] Comissão Europeia, "Primeiro relatório ..." cit., p. 18.

em geral"[884]. Esta *décalage* seria confirmada pela COM ao admitir que muitas transferências, que na prática se realizavam sem controlo, seriam ilícitas, sugerindo-se a "simplificação das condições aplicáveis às transferências internacionais"[885].

O G29 havia sinalizado as dificuldades práticas associadas, por exemplo, à solução contratual[886]; mais recentemente, o G29 identificou a incapacidade de se garantir um nível coerente de proteção das pessoas singulares, especialmente à luz do aumento do número e da complexidade das transferências decorrentes, da computação em nuvem, da globalização, dos novos modelos de gestão do tratamento internacional de dados pessoais, entre outros elementos[887]. A isto acrescia, como darei devida nota na Parte III, um problema da falta de recursos humanos e financeiros das autoridades de controlo. Neste quadro, não é de estranhar que o debate travado no Conselho, durante o procedimento legislativo do RGPD, tenha avaliado a preservação ou não do modelo da Diretiva para as transferências de dados pessoais[888].

Com efeito, renovar e simplificar o regime das transferências constituíram objetivos declarados pela COM nas Comunicações que antecederam o RGPD. Em 2010, referiu que "muitas organizações consideram que os mecanismos atuais não são totalmente satisfatórios, pelo que devem ser revistos e racionalizados, de forma a tornar as transferências mais simples e menos pesadas"[889]. Além disto, os requisitos da adequação não estavam suficientemente circunscritos naquele diploma e nenhum instrumento estava previsto na Diretiva para as transferências entre administrações públicas. A COM aflorou, ainda, o desenvolvimento de outros modos de regulação, como "forma de auto-regulação", nomeadamente as RVAE, que não gozavam de previsão legal expressa apesar da sua manifesta utilidade.

Adicionalmente, a COM descrevia o tratamento de dados pessoais como um "fenómeno mundial" que "carece do desenvolvimento de princípios universais", devendo

---

[884] *Idem*, p. 19.
[885] *Ibidem* e Comissão Europeia, "Analysis and Impact Study on the Implementation of Directive EC 95/46 in Member States. Technical Annex to First Report", 2003, p. 51: "(…) muitas transferências não autorizadas e ilegais são realizadas para destinos ou destinatários que não garantem a proteção adequada. Contudo, não existem sinais de ações de fiscalização ou sancionatórias das autoridades de controlo".
[886] G29, "Documento de Trabalho: Observações preliminares ..., cit., p. 7 e ss..
[887] G29, "Documento explicativo sobre as regras vinculativas para empresas destinadas aos subcontratantes", 19 de abril de 2013, p. 5.
[888] Conselho da UE, "Proposal for a Regulation on the proposal for a regulation of the European Parliament and of the Council on the protection of individual with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation). Preparation of a general approach", 11 de junho de 2015, n.º 448, disponível em http://data.consilium.europa.eu/doc/document/ST-9788-2015-INIT/en/pdf, consultado no dia 30 de setembro de 2018.
[889] Comissão Europeia, "Uma abordagem ..." cit., p. 4.

a UE ocupar o lugar de "força motriz" do "desenvolvimento e da promoção de normas jurídicas e técnicas internacionais em matéria de proteção de dados"[890]. Nesta estratégia, assumem um papel de destaque as "normas técnicas internacionais elaboradas por organismos de normalização" buscando-se a coerência entre o quadro normativo que se avizinhava e aquelas normas, para facilitar a sua aplicação, de forma uniforme e fácil. Para tal a COM propunha-se: promover a elaboração de normas jurídicas e técnicas para uma proteção de dados de elevado nível em países terceiros e a nível internacional; defender o princípio da reciprocidade da proteção nas atividades internacionais da UE, acima de tudo relativamente a pessoas cujos dados pessoais sejam exportados da UE para países terceiros; reforçar, para esse efeito, a cooperação com países terceiros e OI, como a OCDE, o CdE, a ONU e outras organizações regionais; seguir de perto a elaboração de normas técnicas internacionais pelos organismos de normalização como o *European Committee for Standardisation* e a *International Organization for Standardisation*, para que estas sejam um complemento das normas jurídicas e para garantir a aplicação funcional e eficaz dos requisitos da proteção de dados[891].

Em 2012, descrevendo o contexto de "globalização atual" no qual os dados são transferidos sem atenção às fronteiras, virtuais e geográficas, são conservados em servidores instalados em vários países, em que cada vez mais empresas oferecem serviços de computação em nuvem que permitem a consulta e a conservação remota, a COM repetiu o imperativo de flexibilizar os "mecanismos de transferência de dados para países terceiros"[892].

Este intuito reformista não prejudicou a estrutura essencial das normas aplicáveis às transferências que continua, no RGPD, idêntica à da Diretiva, designadamente: (i) a combinação entre uma estratégia geográfica e organizacional[893]; e (ii) o teste com dois momentos, isto é, "primeiro, um fundamento legal tem de ser aplicado ao tratamento de dados, tal como as demais regras do RGPD; em segundo lugar, as normas do Capítulo V devem ser respeitadas"[894]. Assim dispõe o art. 44.º: "qualquer transferência de dados pessoais que sejam ou venham a ser objeto de tratamento após transferência para um país terceiro ou uma organização internacional só é realizada se, *sem prejuízo das outras*

[890] *Idem*, p. 18.
[891] *Ibidem*.
[892] Comissão Europeia, "Proteção da ..." cit., p. 12.
[893] C. KUNER, "Extraterritoriality and …" cit., p. 245 e, do mesmo autor, *Transborder* cit., p. 121.
[894] G29, "Guidelines on Article 49 of Regulation 2016/679", 6 de fevereiro de 2018, p. 3.

disposições do presente regulamento, as condições estabelecidas no presente capítulo forem respeitadas" (itálicos meus).

Sem prejuízo de existir uma continuidade na estrutura essencial do modelo regulatório, importa ainda assim assinalar uma série de alterações, das quais sublinho as seguintes:

(i) Quanto ao procedimento de adequação, a reformulação do papel da COM, o alargamento e especificação dos critérios que orientam a avaliação do "nível de proteção adequado", a faculdade de apreciar não apenas um país terceiro, mas também OI's, um território ou um ou mais setores específicos desse país terceiro, a natureza temporária e provisória das decisões de adequação;

(ii) As garantias suficientes passam a ser designadas "garantias adequadas" e, além disso, o seu leque é alargado;

(iii) Introduzem-se alterações ao nível das derrogações em sentido estrito e, por fim,

(iv) Introduz-se uma disposição específica para as transferências ou divulgações não autorizadas pelo DUE que merece uma análise autónoma no ponto 3.1.2.4.

De seguida trato cada um destes aspetos de forma mais detalhada.

3.1.2.2.Os fundamentos das transferências

3.1.2.2.1. A decisão de adequação

a) O novo papel da Comissão Europeia

Procurando garantir "efeitos no conjunto da União"[895], o legislador atribui competência exclusiva à COM para decidir sobre a adequação do país terceiro. Havendo uma decisão da COM as transferências podem realizar-se sem supervisão prévia da

[895] Considerando 103.

autoridade de controlo[896]. Esta alteração parece excluir *in limine* a possibilidade de autoavaliação da adequação como existia, por exemplo, no Reino Unido retirando alguma flexibilidade ao regime das transferências[897].

O procedimento que antecede as decisões de adequação corre os termos do "procedimento de comité", de harmonia com a leitura conjugada do art. 45.º, n.º 5 e do art. 93.º, desenvolvido no Regulamento 182/2011[898]. O art. 45.º, n.º 5 clarifica a *natureza* da decisão de adequação: sendo o RGPD um "ato de base" ou "primário", atribuindo à COM competências de execução, tal decisão, de entre as categorias de atos de execução consagradas no direito originário, assume a forma de ato de *implementação* (art. 291.º do TFUE) distinto do ato de *delegação* (art. 290.º do TFUE)[899].

Verdadeiramente inovador, no RGPD, é o dever de supervisionar a eficácia e a validade das decisões de adequação, prevendo-se um procedimento de avaliação periódica, em consulta com o país terceiro ou com a OI[900]. Sempre que a informação disponível revelar que o país, o setor, o território ou a OI, deixaram de assegurar a proteção adequada, a COM pode revogar, alterar ou suspender, a decisão de adequação, devendo iniciar consultas com a outra parte com vista a corrigir a situação que deu origem à alteração das circunstâncias[901].

b) O alargamento do "objeto" da adequação e a especificação dos critérios de avaliação

O art. 45.º, nº 1 alarga o "objeto" da adequação, além dos países terceiros, a territórios, setores específicos de um país terceiro ou a organizações internacionais; o n.º 2 do mesmo artigo especifica os critérios que orientam a avaliação da COM. Exige-se um exame exaustivo que inclui, *inter alia,* além das regras materiais de proteção de dados pessoais vigentes no país terceiro, "o primado do Estado de direito, o respeito pelos direitos humanos e liberdades fundamentais", legislação "pertinente", "geral e setorial", "nomeadamente em matéria de segurança pública, defesa, segurança nacional e direito penal, e respeitante ao acesso das autoridades públicas a dados pessoais",

[896] *Ibidem*.
[897] K. HON, *Data Localization* cit., p. 153.
[898] Trata-se do Regulamento que estabelece as regras e os princípios gerais relativos aos mecanismos de controlo pelos Estados-Membros do exercício das competências de execução pela Comissão, de 16 de fevereiro de 2011.
[899] G29, "Adequacy Referential", 6 de fevereiro de 2018 e considerandos 1 e 2 do Regulamento 182/2011.
[900] Art. 45.º, n.º 3 e 4 e considerando 106.
[901] Art. 45.º, n.º 5 e 6.

"jurisprudência", "os direitos do titular dos dados", "vias de recurso administrativo e judicial", a existência de autoridades de controlo independentes e os "compromissos internacionais assumidos pelo país terceiro ou pela organização internacional em causa". Destaco a importância da Convenção n.º 108 do CdE cuja adesão, pelo país terceiro, terá um impacto favorável à adoção de uma decisão de adequação da COM[902].

3.1.2.2.2. As novas "garantias adequadas": os códigos de conduta, os mecanismos de certificação, as RVAE e instrumentos para autoridades ou organismos públicos

Na ausência de uma decisão de adequação o utilizador de dados pessoais deve adotar as medidas necessárias para colmatar a insuficiência do nível de proteção de dados pessoais no país terceiro ou na OI[903]. Estas medidas estão enunciadas no art. 46.º, sob a epígrafe "garantias adequadas", dispondo o RGPD um leque mais alargado quando comparado com a Diretiva. Tal reflete, claramente, um esforço legislativo no sentido de flexibilizar as imposições relativas às transferências[904].

As garantias previstas no n.º 2 distinguem-se das do n.º 3 pela referência ao papel da autoridade de controlo: as primeiras não requerem "nenhuma autorização específica" e compõem um elenco taxativo ("por meio de"); as segundas exigem uma "autorização da autoridade de controlo competente" e podem ser de outra natureza que não aquelas enumeradas pelo legislador ("nomeadamente por meio de"). Contudo, a redação é equívoca uma vez que, mesmo em relação às garantias do n.º 2, haverá uma intervenção prévia da autoridade de controlo, pelo menos no caso das RVAE, bem como ao nível dos códigos de conduta e dos procedimentos de certificação.

Segundo o considerando 108, o escopo daquela disposição é "assegurar o cumprimento dos requisitos relativos à proteção de dados e o respeito pelos direitos dos titulares dos dados adequados ao tratamento no território da UE, incluindo a existência de *direitos do titular dos dados* e de *medidas jurídicas corretivas eficazes*, como o direito de recurso administrativo e judicial e de exigir uma indemnização, *quer no território da União, quer num país terceiro*" (itálicos meus).

[902] Considerando 105.
[903] Considerando 108.
[904] R. WEBER, "Transborder data ..." cit., p. 128.

Em relação à solução contratual não se vislumbram alterações a registar, com uma exceção: o RGPD atribui competência, além da COM, às autoridades de controlo para a adoção de cláusulas contratuais-tipo, posteriormente aprovadas pela COM ao abrigo do procedimento de exame previsto no art. 93.º, n.º 2 do RGPD. A grande novidade deste diploma é a absorção da "auto-regulação publicamente regulada" no campo das transferências. Este foi, como sublinhei, um desiderato da reforma de 2012 vertido em três garantias adequadas novas: os códigos de conduta, os procedimentos de certificação e as RVAE. Recorde-se, a respeito da *natureza* destas soluções, que as mesmas não correspondem a uma forma "pura" de auto-regulação mas, pelo contrário, a uma "auto-regulação publicamente regulada", exigindo uma intervenção pública a atestar a sua conformidade[905]. Outra novidade do RGPD são as garantias adequadas gizadas para o setor público.

a) Os códigos de conduta e os procedimentos de certificação

Estes fundamentos para as transferências decorrem do art. 46.º, n.º 2, al. e) ("[u]m código de conduta, aprovado nos termos do artigo 40.º, acompanhado de compromissos vinculativos e com força executiva assumidos pelos responsáveis pelo tratamento ou pelos subcontratantes no país terceiro no sentido de aplicarem as garantias adequadas, nomeadamente no que respeita aos direitos dos titulares dos dados") e f) ("um procedimento de certificação, aprovado nos termos do artigo 42.º, acompanhado de compromissos vinculativos e com força executiva assumidos pelos responsáveis pelo tratamento ou pelos subcontratantes no país terceiro no sentido de aplicarem as garantias adequadas, nomeadamente no que respeita aos direitos dos titulares dos dados").

Os artigos 40.º, n.º 3 e 42.º, n.º 2 explicam o *modus operandi* destes instrumentos. Para os códigos de conduta, a primeira norma dispõe que, além de responsáveis pelo tratamento ou subcontratantes sujeitos ao RGPD, "também os responsáveis pelo tratamento ou subcontratantes que não estão sujeitos ao presente regulamento por força do artigo 3.º podem cumprir códigos de conduta (...) de modo a fornecer garantias apropriadas no quadro das transferências dos dados pessoais (...). Os responsáveis pelo tratamento ou os subcontratantes assumem compromissos vinculativos e com força executiva, por meio de instrumentos contratuais ou de outros instrumentos juridicamente

[905] K. HON, *Data Localization* cit., p. 212.

vinculativos, no sentido de aplicar as garantias apropriadas, inclusivamente em relação aos direitos do titular dos dados". Em sentido semelhante, o art. 42.º, n.º 2, dispõe que "os procedimentos de certificação em matéria de proteção de dados, bem como selos ou marcas (...) também podem ser estabelecidos para efeitos de comprovação da existência de garantias adequadas fornecidas por responsáveis pelo tratamento ou por subcontratantes que não estão sujeitos ao presente regulamento por força do artigo 3.º no quadro das transferências de dados pessoais (...). Os responsáveis pelo tratamento ou os subcontratantes assumem compromissos vinculativos e com força executiva, por meio de instrumentos contratuais ou de outros instrumentos juridicamente vinculativos, no sentido de aplicar as garantias adequadas, inclusivamente em relação aos direitos dos titulares dos dados".

O que importa salientar por agora é que em ambos os casos não basta por exemplo que um RT respeite um código de conduta: o legislador exige ainda a adoção de "compromissos vinculativos e com força executiva, por meio de instrumentos contratuais ou de outros instrumentos juridicamente vinculativos".

b) As RVAE

Segundo o G29, as virtudes da "abordagem pragmática" veiculada nas RVAE são enaltecidas pelos próprios agentes económicos[906]. Por isso se tem afirmado que a consagração expressa destas regras, nos artigos 46.º, n.º 2, alínea b) e 47.º, é um dos grandes avanços do RGPD[907].

Quanto à sua *natureza,* são códigos de boas práticas internos, decantados das "regras materiais" e dos "mecanismos processuais" de proteção de dados contidos no RGPD e sujeitos a um controlo *ex ante* pela autoridade de controlo[908]. Tal como sucede com os códigos de conduta e com os procedimentos de certificação há uma intervenção da autoridade de controlo. Este controlo não deve ser confundido com uma autorização prévia de cada transferência pois é, sobretudo, um controlo de conformidade das RVAE, em si mesmas, com as exigências da lei.

Os *pressupostos* e o *conteúdo* das RVAE são enunciados no art. 47.º, n.º 1 e 2 e o seu procedimento de aprovação corre termos de acordo com o procedimento de controlo

[906] G29, "Documento explicativo …" cit., p. 5.
[907] R. WEBER, "Transborder …" cit., p. 128 e C. KUNER, "The European Commission's …" cit., p. 10.
[908] Art. 47.º do RGPD e G29, "Documento explicativo …" cit., p. 21.

de coerência previsto no art. 63.º do RGPD. Em larga medida, estas disposições refletem o trabalho desenvolvido pelo G29 com as distinções clarificadas num parecer de novembro de 2017[909]. Tendo em consideração a importância da cooperação com as autoridades de controlo, o número 3 do artigo 47.º prevê a competência da COM para especificar o formato e os procedimentos de intercâmbio de informações com aquelas no que respeita às RVAE.

O G29 sublinhou no passado as vantagens das RVAE e, em especial, a sua adaptabilidade às especificidades e atividades de tratamento *in casu*[910]. Este é um fator de aproximação com os códigos de conduta e os procedimentos de certificação, no sentido em que ambos procuram superar o nível de abstração da lei adaptando-a às especificidades de um determinado setor e à dimensão do utilizador dos dados pessoais[911]. De todo o modo, o seu nível de detalhe deve ser suficiente para permitir às autoridades de controlo avaliar se as garantias nelas previstas são ou não adequadas[912].

As RVAE distinguem-se das demais garantias adequadas pela especificidade dos seus *destinatários*: entidades que compõem um "grupo empresarial" ou um "grupo de empresas envolvidas numa atividade económica conjunta" (art. 47.º, nº 1, a) e art. 4.º, n.º 19[913]). Estas regras devem prever que uma das entidades que compõe o grupo – a sede na UE ou um dos membros do grupo ali situado com responsabilidades de proteção de dados delegadas – aceite as consequências da violação das RVAE, incluindo a possibilidade de ressarcir o titular dos dados[914].

O efeito útil deste fundamento para as transferências de dados pessoais é transformar a entidade transnacional num *safe heaven* organizacional no seio do qual os dados pessoais circulam internamente, livre e independentemente do nível de proteção conferido pelos países onde se encontram as várias entidades do grupo. Por conseguinte,

[909] G29, "Working Document setting up a table with the elements and principles to be found in Binding Corporate Rules", 27 de novembro de 2017.
[910] G29, "Documento explicativo …" cit., p. 13.
[911] Art. 40.º, n.º 1 e art. 42.º, n.º 1 do RGPD.
[912] Devem, por exemplo, incluir uma descrição detalhada das atividades económicas desenvolvidas por cada uma das entidades do grupo, v. G29, "Working Document. Transfers of personal data to third countries: Applying Article 26 (2) of the EU Data Protection Directive to Binding …" cit., p. 14.
[913] Este artigo define "grupo empresarial" como "um grupo composto pela empresa que exerce o control e pelas empresas controladas".
[914] Como decorre da interpretação do G29 do art. 47.º, n.º 2, al. f), v. G29, "Working Document setting up …" cit., p. 8 e "Working Document Setting Forth a Co-Operation Procedure for the apporcal of 'Binding Corporate Rules' for controllers and processors under the GDPR", 11 de abril de 2018. Um aspeto importante para a responsabilização da entidade situada na UE é a parte final da alínea f) delimitando a exoneração da responsabilidade "mediante prova de que o facto que causou o dano não é imputável à referida entidade".

qualquer transferência de uma entidade pertencente ao grupo para um destinatário fora do mesmo é possível com base, por exemplo, na adoção de cláusulas contratuais-tipo ou de uma solução contratual *ad hoc* celebrada com o importador dos dados pessoais[915]. A lista de grupos que recorrem às RVAE é extensa, incluindo as seguintes: Airbus, American Express, AXA, BMW, BP, Citigroup, eBay, HP Enterprise, Intel Corporation, Mastercard, Motorola, Siemens, Société Générale, Total, entre outras[916].

c) Instrumentos para autoridades ou organismos públicos

O art. 46.º, n.º 2, al. a), prevê "um instrumento juridicamente vinculativo e com força executiva entre autoridades ou organismos públicos" e o art. 46.º, n.º 3, al. b), sob reserva de autorização da autoridade de controlo, refere-se a "disposições a inserir nos acordos administrativos entre as autoridades ou organismos públicos que contemplem os direitos efetivos e oponíveis dos titulares dos dados".

3.1.2.2.3. Derrogações em sentido estrito

Durante as negociações do RGPD alguns Estados sugeriram o reconhecimento de que, na realidade, as "derrogações" sempre foram o principal fundamento das transferências[917]. Contudo, esta sugestão não singrou.

Elencadas no art. 49.º estas derrogações valem apenas para "situações específicas". O G29 destacou que esta norma deve ser lida à luz do art. 44.º: "todas as disposições do presente capítulo são aplicadas de forma a assegurar que não é comprometido o nível de proteção das pessoas singulares garantido pelo presente regulamento"[918]. Adicionalmente, persiste o entendimento segundo o qual estas derrogações devem ser interpretadas de forma "bastante restritiva" e sujeitas a um teste de necessidade da própria transferência[919]. No mesmo sentido apontaram as orientações

[915] G29, "Working Document. Transfers of personal data to third countries: Applying Article 26 (2) of the EU Data Protection Directive to Binding …" cit., p. 9. O G29 alerta para o facto de que, no caso da Decisão de 2001 e de 2010, tratando-se de categorias especiais de dados pessoais, a transferência ulterior exige o consentimento inequívoco do titular dos dados.
[916] A lista completa está disponível em https://ec.europa.eu/info/strategy/justice-and-fundamental-rights/data-protection/data-transfers-outside-eu/binding-corporate-rules_en#listofcompanies, consultada no dia 30 de setembro de 2018.
[917] Conselho da UE, "Preparation ..." cit., nota de rodapé 480.
[918] G29, "Primeiras orientações..." cit., p. 2 e ss. e G29, "Guidelines on article 49 ..." cit., p. 3 e ss..
[919] *Ibidem.*

do G29[920] e do SEPD[921] defendendo que a utilização de derrogações em sentido estrito fosse válida apenas para transferências ocasionais, de natureza não massiva ou estrutural.

A alteração mais relevante em sede de derrogações prende-se com a introdução de restrições ao uso do consentimento que, além de "explícito", é acompanhado de um direito a ser informado dos possíveis riscos da transferência por falta de decisão de adequação e de garantias adequadas[922]. Igual relevo assume a alínea d) que viabiliza transferências por "importantes razões de interesse público" exemplificadas no considerando 112: "intercâmbio internacional de dados entre autoridades de concorrência, administrações fiscais ou aduaneiras, entre autoridades de supervisão financeira, entre serviços competentes em matéria de segurança social ou de saúde pública". Esta disposição foi criticada pelo SEPD por ser excessivamente ampla e permitir transferências, em vários domínios, sem quaisquer garantias de proteção dos titulares dos dados pessoais[923].

Por fim, o número 1 *in fine* prevê uma derrogação, com respeito de algumas condições, quando a transferência "for necessária para efeitos dos interesses legítimos visados pelo responsável pelo seu tratamento". Vislumbram-se algumas semelhanças com o sistema de autoavaliação vigente no Reino Unido como mecanismo para flexibilizar as transferências[924]. Contudo, considera-se que, dadas as exigentes condições impostas pelo G29, a sua aplicação prática será residual[925].

3.1.2.3.As particularidades do art. 48.º do RGPD

3.1.2.3.1. Evolução legislativa

Esta norma, sob a epígrafe "Transferências ou divulgações não autorizadas pelo direito da União", dispõe que o legislador não *reconhece* ou *executa* "decisões judiciais"

[920] G29, "Parecer 01/2012" cit., p. 24 e ss..
[921] SEPD, "Opinion of the …" cit., p. 37
[922] Art. 49.º, n.º 1, al. a). As condições gerais aplicáveis ao consentimento decorrem dos arts. 4.º, n.º 11 e 7.º do RGPD e em G29, "Guidelines on Consent under Regulation 2016/679", 28 de novembro de 2017 e G29, "Guidelines on article 49 ..." cit., p. 6.
[923] SEPD, "Opinion of the European …" cit., p. 37.
[924] Comissão Europeia, "Proposta de regulamento do Parlamento Europeu e do Conselho relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados", 25 de janeiro de 2012, anexo 5, p. 102; K. HON, *Data Localization* cit., p. 215; R. WEBER, "Transborder …" cit., p. 129.
[925] K. HON, *Data Localization* cit., p. 215. Desenvolvendo estas condições, v. G29, "Guidelines on article 49 ..." cit., p. 15.

ou "decisões administrativas de um país terceiro", enquanto fundamento ou condição de licitude da transferência, exceto "se [aquelas decisões] tiverem com base um acordo internacional, como um acordo de assistência judiciária mútua, em vigor entre o país terceiro em causa e a União ou um dos Estados-Membros, sem prejuízo de outros motivos de transferência nos termos do presente capítulo".

O considerando 115 acrescenta os seguintes esclarecimentos: "Alguns países terceiros aprovam leis, regulamentos e outros atos normativos destinados a regular diretamente as atividades de tratamento pelas pessoas singulares e coletivas sob a jurisdição dos Estados-Membros. Pode ser o caso de sentenças de órgãos jurisdicionais ou de decisões de autoridades administrativas de países terceiros que exijam que o responsável pelo tratamento ou subcontratante transfira ou divulgue dados pessoais sem fundamento em nenhum acordo internacional, como seja um acordo de assistência judiciária mútua, em vigor entre o país terceiro em causa e a União ou um dos Estados-Membros. Em virtude da sua aplicabilidade extraterritorial, essas leis, regulamentos e outros atos normativos podem violar o direito internacional e obstar à realização do objetivo de proteção das pessoas singulares, assegurado pela União Europeia pelo presente regulamento. As transferências só deverão ser autorizadas quando estejam preenchidas as condições estabelecidas pelo presente regulamento para as transferências para países terceiros. Pode ser esse o caso, nomeadamente, sempre que a divulgação for necessária por um motivo importante de interesse público, reconhecido pelo direito da União ou dos Estados-Membros ao qual o responsável pelo tratamento está sujeito".

Esta disposição não constava da Diretiva. Foi introduzida na proposta original da COM, em sede de considerando, redigido em termos semelhantes ao considerando 115: "[a]lguns países terceiros aprovam leis, regulamentos e outros instrumentos legislativos destinados a regular diretamente as atividades de tratamento de dados pelas pessoas singulares e coletivas sob a jurisdição dos Estados-Membros. Em virtude da sua aplicabilidade extraterritorial, essas leis, regulamentos e outros instrumentos legislativos podem violar o direito internacional e obstar à realização do objetivo de proteção das pessoas singulares, assegurado na União Europeia pelo presente regulamento. As transferências só devem ser autorizadas quando as condições estabelecidas pelo presente regulamento para as transferências para os países terceiros estejam preenchidas. Pode ser o caso, nomeadamente, sempre que a divulgação for necessária por um motivo importante de interesse público, reconhecido pelo direito da União, ou pelo direito do Estado-Membro ao qual o responsável pelos dados está sujeito. As condições para a existência

de um motivo importante de interesse público devem ser precisadas pela Comissão mediante um ato delegado"[926].

Posteriormente, o PE acrescentou o art. 43.º-A, especificando quatro elementos do considerando proposto pela COM:

(i) Reiterando, no n.º 1, o não reconhecimento ou execução do direito estrangeiro "sem prejuízo de um acordo de assistência judiciária mútua ou de um acordo internacional";

(ii) Prevendo o dever de notificar a autoridade de controlo nas situações em que um utilizador de dados pessoais se depare com um acórdão de um tribunal ou uma decisão de uma autoridade administrativa de um país terceiro exigindo a divulgação ou a transferência de dados pessoais, sujeitando as mesmas a uma autorização prévia daquela autoridade;

(iii) Determinando que a autoridade de controlo avalie a conformidade do pedido estrangeiro, de acordo com o art. 44.º, n.º 1, alíneas d) e e)[927];

(iv) Acrescentando o dever de informar o titular dos dados do pedido e da decisão da autoridade de controlo[928].

---

[926] Comissão Europeia, "Proposta de regulamento ..." cit., considerando 90.

[927] Tratam-se das derrogações aplicáveis às transferências quando estas são necessárias "por motivos importantes de interesse público" ou à "declaração, ao exercício ou à defesa de um direito num processo judicial".

[928] "1. As sentenças de órgãos judiciais e as decisões de autoridades administrativas de um país terceiro, que solicitem a um responsável pelo tratamento ou subcontratante que divulgue dados pessoais, não serão reconhecidas ou executadas de nenhuma forma. 2. Sempre que os acórdãos de tribunais e as decisões de autoridades administrativas de um país terceiro solicitem a um responsável pelo tratamento ou subcontratante que divulgue dados pessoais, o responsável pelo tratamento ou o subcontratante e, caso exista, o representante do responsável pelo tratamento, deve notificar a autoridade de controlo do pedido, sem demora injustificada, e deve obter autorização prévia da autoridade de controlo para a transferência ou divulgação. 3. A autoridade de controlo avalia a conformidade da divulgação pedida com o regulamento e, em particular, se a divulgação é necessária e exigida legalmente de acordo com o artigo 44.º, n.º 1, alíneas d) e e), e com o n.º 5 do mesmo artigo. Sempre que sejam prejudicados titulares dos dados de outros Estados-Membros, a autoridade de controlo competente aplica o mecanismo de controlo da coerência referido no artigo 57.º. 4. A autoridade de controlo informa do pedido a autoridade nacional competente. Sem prejuízo do disposto no artigo 21.º, o responsável pelo tratamento ou o subcontratante deve ainda informar os titulares dos dados do pedido e da autorização pela autoridade de controlo e, se necessário, informar o titular dos dados sobre se foram fornecidos dados pessoais às autoridades públicas durante o último período consecutivo de 12 meses, nos termos do artigo 14.º, n.º1, alínea h-A).", v. "Projeto de resolução legislativa do PE sobre a proposta de regulamento do Parlamento Europeu e do Conselho relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados", Alteração 140, disponível em http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-

Em sede de considerando, o PE acrescentou que "[n]os casos em que os responsáveis pelo tratamento ou os subcontratantes se vejam confrontados com exigências de conformidade contraditórias entre a jurisdição da UE, por um lado, e as de um país terceiro, por outro, a Comissão deve velar por que a legislação da UE prevaleça em todas as circunstâncias. A Comissão deve fornecer orientações e assistência ao responsável pelo tratamento e ao subcontratante, bem como procurar resolver os conflitos de jurisdição com o país terceiro em questão"[929].

Contudo, não terá sido possível chegar a um acordo político sobre os contornos deste procedimento de controlo e de comunicação ao titular dos dados dos pedidos estrangeiros o que conduziu a uma simplificação do art. 48.º diminuindo, em parte, o impacto do mesmo no dia-a-dia de muitos operadores transnacionais que lidam com pedidos estrangeiros e com as exigências do RGPD[930].

3.1.2.3.2. Origem e campo de aplicação

A *origem* desta norma encontrar-se-á numa sugestão do G29 para que o RGPD conferisse maior relevo aos "tratados de auxílio judiciário mútuo (MLAT)" e a outros acordos internacionais "comparáveis" na matéria dos pedidos estrangeiros que solicitam ao utilizador de dados pessoais a divulgação ou a transferência de dados pessoais da UE para o país terceiro[931]. Na exposição de motivos do PE lê-se que o art. 43.º-A visa regular os pedidos de acesso a dados pessoais armazenados e tratados na UE, apresentados por autoridades públicas ou tribunais de países terceiros – uma questão que ganhará "*mais importância com o crescimento da computação em nuvem* (itálicos meus)"[932].

A doutrina tem apontado as imprecisões do art. 48.º como, por exemplo, a distinção textual e sem critério orientador entre "divulgação" e "transferência"[933]. Sem prejuízo dos esclarecimentos que a prática e o tempo venham a acrescentar, o seu campo de aplicação

---

//EP//TEXT+REPORT+A7-2013-0402+0+DOC+XML+V0//PT#title2, consultado no dia 30 de setembro de 2018.

[929] *Idem*, alteração 63.

[930] David J. KESSLER, Jamie NOVAK e Sumera KHAN, "The potential impact of article 48 of the General Data Protection Regulation on Cross Border Discovery From the United States", *TSCJ,* vol. 17, n.º 2, 2016, p. 584.

[931] G29, "Parecer 1/2012 sobre as propostas de reforma em matéria de proteção de dados", 23 de março de 2012, p. 23, "Guidelines on Article 49 ..." cit., p. 5 e "Parecer 05/2012 …" cit., p. 28.

[932] PE, "Exposição de Motivos", 22 de novembro de 2013, p. 211 e ss., disponível em http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+REPORT+A7-2013-0402+0+DOC+PDF+V0//PT, consultado no dia 30 de setembro de 2018.

[933] D. J. KESSLER, J. NOVAK e S. KHAN, "The potential impact …" cit., p. 586; K. HON, *Data Localization*, cit., p. 314.

respeita, pelo menos, a duas hipóteses: os programas de vigilância dos países terceiros e a situação na origem do caso *Microsoft.*

a) As revelações de Edward Snowden

Com efeito, o art. 48.º merece ser lido à luz de um acontecimento melindroso que marcou o curso do procedimento legislativo do RGPD: as revelações de Edward Snowden (ES), em 2013, sobre os programas de vigilância geridos pelos EUA[934].

Na sequência de uma reunião do Comité dos Representantes Permanentes (Coreper[935]), foi instituído um grupo de trabalho para apurar a veracidade daquelas revelações, grupo esse que contou com a colaboração dos EUA[936]. As conclusões desta investigação não revelaram ser absolutamente esclarecedoras já que, de forma sistemática, os EUA se escusaram a responder a certas dúvidas invocando os riscos para a segurança nacional[937]. Em todo o caso, estas conclusões serviram de suporte a várias reações das instituições da UE[938], designadamente da COM[939], do PE[940] e do G29[941], que resumo nos pontos seguintes: em primeiro lugar, o grupo de trabalho conclui que nos EUA vigora legislação que implementa programas de "recolha de informação em grande escala" que afetam os direitos fundamentais e suportam "a vigilância generalizada das

[934] Barton GELLMAN e Laura POITRAS, "U.S., British intelligence mining data from nine U.S. Internet companies in broad secret programs", *Washington Post,* 7 de junho de 2013; D. J. KESSLER, J. NOVAK e S. KHAN, "The potential impact …" cit., p. 584; E. MACASKILL, G. GREENWALD, "NSA PRISM Program taps in to user data of Apple, Google and others", *The Guardian,* 7 de junho de 2013; Glenn GREENWALD, Ewen MACASKILL, Laura e POITRAS, "Edward Snowden: the whistleblower behind the NSA surveillance revelations", *The Guardian,* 9 de junho de 2013; H. HIJMANS, *The European Union* cit., p. 499 e ss..

[935] O Coreper constitui, simultaneamente, uma instância de diálogo e de controlo político sendo o responsável pelo exame prévio dos processos que figuram na ordem de trabalhos do Conselho. Mais informações sobre este Comité, v. http://eur-lex.europa.eu/summary/glossary/coreper.html?locale=pt, consultado no dia 30 de setembro de 2018.

[936] "Report on the Findings by the EU Co-chairs of the ad hoc EU-US Working Group on Data Protection", 27 november 2013, disponível em http://ec.europa.eu/justice/data-protection/files/report-findings-of-the-ad-hoc-eu-us-working-group-on-data-protection.pdf, consultado no dia 30 de setembro de 2018.

[937] "Report on the Findings …" cit., ponto 2.1.3 e ponto 2.3.

[938] David WRIGHT e Reinhard KREISSL, "European responses to the Snowden revelations: A discussion paper", *Increasing Resilience in Surveillance Societies (IRISS),* Dezembro de 2013, disponível em http://irissproject.eu/wp-content/uploads/2013/12/IRISS_European-responses-to-the-Snowden-revelations_18-Dec-2013_Final.pdf , consultado no dia 30 de setembro de 2018.

[939] Comissão Europeia, "Restabelecer a confiança nos fluxos de dados entre a UE e os EUA", 27 de novembro de 2013 e "Sobre o funcionamento do sistema 'porto seguro' na perspetiva dos cidadãos da UE e das empresas estabelecidas na UE", 27 de novembro de 2013.

[940] Resolução do PE, de 12 de março de 2014, sobre o programa de vigilância da Agência Nacional de Segurança dos EUA (NSA), os organismos de vigilância em diversos Estados-Membros e o seu impacto nos direitos fundamentais dos cidadãos da UE e na cooperação transatlântica no domínio da justiça e dos assuntos internos.

[941] "Parecer 04/2014 sobre a vigilância de comunicações eletrónicas para efeitos de informações e segurança nacional", 10 de abril de 2014 e "G29, "Working Document on surveillance ..." cit., p. 2 e ss..

comunicações privadas dos cidadãos, das empresas ou dos dirigentes políticos [estrangeiros]"[942]. Entre esses diplomas contam-se: a secção 702 do *Foreign Intelligence Surveillance Act of 1978* (FISA), a Seção 215 do *USA Patriot Act of 2001* e a *Executive Order 1233*[943]. Daqui emerge o problema do *alcance* daqueles programas, geridos por um país terceiro, visando pessoas singulares e coletivas estrangeiras, descritos como tendo uma "grande escala" e como "maciços", "indiscriminados" e "para além do que é "estritamente necessário e proporcionado numa sociedade democrática", em especial à luz da CEDH[944].

A doutrina tem salientado que as implicações das revelações de ES transcendem o mero problema das ingerências de um Estado terceiro a direitos fundamentais de estrangeiros alargando-se, por exemplo, à espionagem internacional[945]. É que o conteúdo dos programas de vigilância inclui, além de dados pessoais, a recolha de informação conexa com os assuntos externos dos EUA[946]. De entre os vários diplomas identificados o principal foco das críticas europeias é a secção 702 do FISA, exclusivamente orientada para cidadãos estrangeiros, "que razoavelmente se acredita estarem localizados no estrangeiro" visando a aquisição de "informação externa" (*foreign intelligence information*) [947].

Em segundo lugar, ficou também clara a posição de vulnerabilidade dos cidadãos estrangeiros vigiados que não beneficiam dos mesmos direitos e garantias, administrativas e judiciais, que os cidadãos norte-americanos, sendo os primeiros mais afetados por aqueles programas do que os segundos[948]. Por exemplo, a *Executive Order 12333* viabiliza a adoção de ordens de vigilância, pelos serviços de informações dos EUA, sem qualquer controlo judicial[949]. Já no quadro da seção 702 do FISA, cabe ao FISC

[942] Comissão Europeia, "Restabelecer a confiança ..." cit., p. 3.
[943] "Report on the Findings …" cit., ponto 5.
[944] "Parecer 04/2014 ..." cit., p. 2 e "Working Document on surveillance ..." cit., p. 45.
[945] Casper BOWDEN, "The US surveillance programs and their impact on EU citizens' fundamental rights: note for the European Parliament's Committee on Civil Liberties, Justice and Home Affairs", 2013, disponível em http://www.europarl.europa.eu/meetdocs/2009_2014/documents/libe/dv/briefingnote_/briefingnote_en.pdf, consultado no dia 30 de setembro de 2018, p. 6 e Silja VOENEKY, "Espionage, Security Interests, and Human Rights in the Second Machine Age: NSA Mass Surveillance and the Framework of Public International Law", Russell MILLER (ed.), *Privacy and Power. A Transatlantic Dialogue in the Shadow of the NSA-Affair,* Cambridge University Press, 2017, p. 492.
[946] G29, "Working Document on surveillance ..." cit., p. 25.
[947] Desenvolvendo os dois tipos de vigilância que este diploma viabiliza - "PRISM collection" e "Upstream collection" - Francesca BIGNAMI e Giorgio RESTA, "Transatlantic Privacy Regulation: Conflict and Cooperation", *Law and Contemporary Problems*, vol. 78, n.º 4, 2015, p. 248 e ss..
[948] Comissão Europeia, "Restabelecer a confiança ..." cit., p. 4; "Report on the Findings ..." cit., ponto 2 e ponto 5, n.º 2; G29, "Parecer 04/2014 ..." cit., p. 8 e 9; C. BOWDEN, "The US Surveillance..." cit., p. 10.
[949] "Report on the Findings …" cit., ponto 5, número 6.

(*Foreign Intelligence Surveillance Court*), que atua *ex parte* e *in camera,* aprovar as decisões que executam aqueles programas tendo, nesse exercício, poderes bastante limitados e a obrigação de acautelar apenas a posição de cidadãos dos EUA[950]. Adicionalmente, constatou-se não existirem mecanismos administrativos ou judiciais para contestar as decisões do FISC, para aceder, retificar ou apagar os dados pessoais recolhidos[951]. No campo do direito constitucional, a vigilância de estrangeiros não está acautelada pelas garantias da Quarta Emenda uma vez que o *Supreme Court* decidiu que a mesma não se aplica a estrangeiros[952].

Esta negação de garantias a estrangeiros desencadeou um debate doutrinal sobre a vigilância sem restrições de *estrangeiros*, localizados no *estrangeiro*, e a possível violação de obrigações de DIP, designadamente do Pacto Internacional de Direitos Civis e Políticos[953]. É assim que tem origem a discussão em curso sobre os limites à vigilância *extraterritorial*[954] ou *transnacional*[955] e a hipótese de violação extraterritorial de direitos fundamentais: "existe uma grande preocupação com as violações extraterritoriais de direitos fundamentais e com a incapacidade de os indivíduos saberem que estão a ser objeto de vigilância estrangeira e de contestarem as decisões que a viabilizam ou procurar recursos"[956].

---

[950] Comparando com a supervisão judicial dos sistemas de vigilância europeus, v. F. BIGNAMI e G. RESTA, "Transatlantic ..." cit., p. 250.
[951] "Report on the Findings ..." cit., ponto 5, n.º 5.
[952] "Report on the Findings ..." cit., ponto 4.3.
[953] F. BIGNAMI e G. RESTA, "Transatlantic ..." cit., p. 254 e bibliografia ali enunciada.
[954] Por oposição à vigilância doméstica, distinção que consta da Resolução da ONU 68/167 de janeiro de 2014 citada pelo G29, "Working Document on ..." cit., p. 12. Defendendo que os programas de vigilância "extraterritorial" dos EUA são ilegais ao abrigo do DIP, em especial invocando os Direitos Humanos, o art. 12.º da Declaração Universal dos Direitos do Homem e o art. 17.º, n.º 2 do Protocolo Internacional dos Direitos Civis e Políticos, v. Anne PETERS, "Privacy, *Rechtsstaatlichkeit,* and legal limits on extraterritorial surveillance", R. MILLER, *Privacy* cit., p. 145 e ss.; Alan WALEN, "Fourth Amendment Rights for Nonresident Aliens", R. MILLER, *Privacy* cit., p. 282 e ss.; Ian BROWN *et alii*, "Toward Multilateral Standards for Foreign Surveillance Reform", Russell MILLER, *Privacy* citp. 462; K. HON, *Data Localization* cit., p. 313; Stephen SCHULHOFER, "A Transatlantic Privacy Pact?: A Sceptical View", David D. Cole *et alii*, *Surveillance, Privacy and Trans-Atlantic Relations,* Hart Publishing, 2017, p. 193. Como sintetiza David LINDSAY: "a controvérsia em torno dos fluxos de dados transatlânticos deve ser compreendida no contexto mais amplo das obrigações do Estado em relação aos direitos dos indivíduos situados fora do seu território", v. "The Role of Proportionality in Assessing Trans-Atlantic Personal Data Flows", Dan SVANTESSON e Dariusz KLOZA (eds.), *Trans-Atlantic Data Privacy Relations As a Challenge for Democracy,* Intersentia, 2017, p. 51.
[955] Ira RUBINSTEIN *et alii,* "Systematic government access to personal data: a comparative analysis", *IDPL,* vol. 4, n.º 2, 2014, p. 118.
[956] Frank LA RUE, "Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Expression", 17 de abril de 2013, p. 64, disponível em https://www.ohchr.org/EN/Issues/FreedomOpinion/Pages/Annual.aspx, consultado no dia 30 de setembro de 2018.

Em terceiro lugar, concluiu-se que os destinatários das decisões do FISC e dos serviços de informações são empresas privadas, nomeadamente que prestam serviços na Internet e de telecomunicações, com estabelecimentos nos EUA e na UE. Como resumiu a COM os programas norte-americanos sugeriam uma ligação entre a vigilância do Estado e o tratamento de dados pessoais pelo setor privado, o que pode prejudicar a confiança na economia digital e ter efeitos negativos no respetivo crescimento[957]. Nessa medida, a vulnerabilidade dos operadores transnacionais e os seus dilemas, quando confrontados com os pedidos de autoridades de países terceiros, foi outro aspeto salientado[958].

O art. 48.º tem sido lido neste contexto o que lhe valeu a designação de "cláusula Anti-FISA"[959]. Um dos casos de aplicação desta norma será, por exemplo, se uma decisão do FISC ou dos serviços de informações dos EUA compelir um RT com estabelecimento nos dois lados do Atlântico a facultar o *acesso direto* a dados pessoais armazenados no território da UE[960]. Outra possibilidade é se essas decisões impuserem uma transferência daqueles dados para os EUA, como comprovam relatos da *Microsoft* e da *Google*[961]. I. BROWN e D. KORFF designam estas práticas de "recolhas transnacionais de dados pessoais", enquadrando-as no quadro da jurisdição de execução extraterritorial por constituírem atos materiais (de "extração" dos dados pessoais) levados a cabo no território de um país terceiro e que, enquanto tal, exigem o consentimento daquele[962].

---

[957] Comissão Europeia, "Restabelecer a confiança ..." cit., p. 3 e 4.
[958] G29, "Parecer 04/2014 ..." cit., p. 8.
[959] Cristina CASAGRAN, *Global Data Protection in the Field of Law Enforcement. An EU Perspective,* Routledge, 2017, p. 183; C. BOWDEN, "The US Surveillance ..." cit., p. 29; K. HON, *Data Localization* cit., p. 313 e ss..
[960] Este sistema, de acesso direto, é designado sistema de "extração" (*push*) por permitir que os dados pessoais são selecionados e transferidos pelas empresas privadas para as autoridades dos EUA, por contraponto a um sistema de "exportação" (*pull*) por meio do qual os dados são selecionados e transferidos pelas prórpias autoridades dos EUA, sem qualquer intermediação e filtro, v. F. BIGNAMI e G. RESTA, "Transatlantic ..." cit., p. 251.
[961] K. HON, *Data Localization* cit., p. 117. Entre outros exemplos citados pelo ICC, "Cross-Border Law Enforcement Access ..." cit., p. 1.
[962] "Os dados pessoais são ativamente exportados de um servidor num país terceiro para – ou a pedido de – uma agência de outro país" e, mais adiante defendem que "um Estado que recorre aos seus poderes legislativos e de execução para capturar ou exercer qualquer tipo de controlo sobre dados pessoais que não estão no seu território físico mas no território de outro Estado, por exemplo, utilizando a infraestrutura física da Internet e um sistema de comunicações global para retirar esses dados daqueles servidores, de computadores pessoais ou aparelhos móveis localizados noutro Estado, ou exigindo a entidades privadas localizadas neste e com acesso a esses dados para os transferir para outro país, tal constitui uma importação desses dados e, com eles, do titular dos dados, para a respetiva 'jurisdição' (...)". Os autores concluem que é um princípio de DIP, "confirmado pelo costume internacional, que a recolha transnacional de dados de um país sem o seu consentimento, seja para a aplicação da lei ou para a preservação da segurança nacional, é ilícita", v. Ian BROWN e Douwe KORFF, "Foreign Surveillance: law and practice in a global digital environment", *EHRLR,* n.º 3, 2014, p. 243 e 245.

Naturalmente que esta disposição não trava, sem mais, o alcance dos programas de vigilância. Contudo, a mesma é um *sinal político* de contestação à aliança entre a vigilância estadual estrangeira e o setor privado com uma conexão com a UE (*v.g* que dirige a sua atividade económica ou armazena os dados pessoais ali), materializada nos pedidos do FISC e em decisões dos serviços de informações dos EUA. Esta aliança tem sido designada *dataveillance* ou *data surveillance*[963]. Não são ignorados os interesses de segurança dos EUA nem a relevância dos fluxos de dados para a cooperação em matéria de aplicação da lei, incluindo prevenção e luta contra o terrorismo[964]. O problema é o *método*[965] unilateral implementado pelos EUA em detrimento daquele que, para o legislador, é o apropriado: a cooperação internacional por "acordo internacional, como um acordo de assistência judiciária mútua"[966]. O unilateralismo contraria os compromissos assumidos pelos EUA nesses acordos e, sugerem alguns, constitui uma violação do princípio da boa fé vigente no DIP[967].

O Relator Especial da ONU para a liberdade de opinião e de expressão, recomenda que, por um lado, os Estados limitem os pedidos de acesso a dados pessoais tratados pelo setor privado apenas a situações de último recurso, depois de exauridas técnicas menos intrusivas, respeitando o princípio da proporcionalidade e, por outro lado, devem privilegiar os canais formais de cooperação com os outros Estados, tais como os MLAT's (*Mutual Legal Assistance Treaties*) ou outros acordos setoriais[968]. O que se pode questionar é a adequação desses canais de cooperação para responder às necessidades que os Estados enfrentam, nos dias de hoje, em matéria de segurança. Esta é uma questão sinalizada pela doutrina[969] , que voltou à ribalta com o caso *Microsoft* e que tem estado no radar das recomendações mais recentes do Relator Especial da ONU para a privacidade[970].

---

[963] G29, "Working Document on …" cit., p. 45, "Parecer 04/2014 …" cit., p. 16 e Capítulo 2, a propósito da reação do TJ a esta tendência.
[964] Este ponto é frisado pela Comissão Europeia, elencado os vários acordos celebrados entre a UE ou os Estados-Membros e os EUA para esse fim, v. Comissão Europeia, "Restabelecer a confiança ..." cit., p. 2.
[965] F. BIGNAMI e G. RESTA, "Transatlantic ..." cit., p. 256.
[966] Comissão Europeia, "Restabelecer a confiança ..." cit., p. 9.
[967] F. BIGNAMI e G. RESTA, "Transatlantic ..." cit., p. 256. Nesse sentido, "Letter from EU Vice-President Viviane Reding to U.S. Attorney General Eric Holder", 10 de junho de 2013, p. 2.
[968] F. LA RUE, "Report of the Special Rapporteur …" cit., p. 21.
[969] Anna-Maria OSULA, "Mutual Legal Assistance & Other Mechanisms for Accessing Extraterritorially Located Data", *MUJLT,* n.º 9, 2015, p. 43 e Gail KENT, "Sharing Investigation Specific Data with law Enforcement – An International Approach", *Stanford Public Law Working Paper,* 14 de fevereiro de 2014, disponível em https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2472413, consultado no dia 30 de setembro de 2018.
[970] Joseph CANNATACI, "Report of the Special Rapporteur on the right to privacy", 24 de fevereiro de 2017, p. 12, disponível em https://www.ohchr.org/EN/Issues/Privacy/SR/Pages/SRPrivacyIndex.aspx,

b) O caso *Microsoft*

Este caso alargou o campo de aplicação desta norma para além do problema específico dos programas de vigilância dos EUA e reacendeu o debate, agora travado num contexto digital, sobre os pedidos de documentos localizados no estrangeiro por autoridades da entidade do foro[971]. A disputa girou em torno de um mandado (*warrant*), decidido por um juiz, a pedido do *Departement of Justice* (DoJ), em dezembro de 2013, com base no *Stored Communications Act*, 18 U.S.C. § 2703 ("SCA"), no contexto de uma investigação de tráfico de droga e lavagem de dinheiro. Este mandado obrigava a *Microsoft USA* a transferir, para o DoJ, os dados pessoais de uma conta de email armazenados nos centros de dados localizados na Irlanda e operados pela *Microsoft Ireland.*

Tendo perdido junto do *District Court*[972]*,* a *Microsoft* recorreu para o *US Court of Appeals for the Second Circuit* recusando-se a cumprir a ordem do DoJ por entender que o SCA não era aplicado fora do território dos EUA. Aquele tribunal deu razão à *Microsoft* com base em duas decisões do *Supreme Court*[973] nas quais se firmou uma presunção contra a extraterritorialidade segundo a qual a jurisdição dos EUA é territorial "exceto quando exista uma intenção clara, em sentido contrário, do legislador"[974]. Com efeito, por um lado, o *Court of Appeals* descurou a possibilidade, confirmada inclusive pela *Microsoft*[975], de acesso remoto aos dados pessoais a partir dos EUA e, por outro, entendeu que o Congresso, na redação do SCA, não teve uma intenção clara de abranger dados localizados no estrangeiro e, assim, estender a jurisdição dos EUA para fora do respetivo

consultado no dia no dia 30 de setembro de 2018 e "Draft Legal Instrument on Government-led Surveillance and Privacy", 10 de janeiro de 2018, p. 17 e ss., disponível em https://www.ohchr.org/Documents/Issues/Privacy/DraftLegalInstrumentGovernmentLed.pdf, consultado no dia 30 de setembro de 2018.

[971] Cfr. Parte I, Capítulo 2 desta tese.

[972] A história deste processo encontra-se relatada no Acórdão do USCASC, Microsoft Corporation c. United States of America, 14-2985, 14 de julho de 2016, disponível em http://www.chamberlitigation.com/sites/default/files/cases/files/16161616/Opinion%20--%20Microsoft%20v.%20U.S.%20%28Second%20Circuit%29.pdf , consultado no no dia 30 de setembro de 2018.

[973] Acórdão do USCASC, Microsoft Corporation c. United States of America, 14-2985, 14 de julho de 2016, p. 6 citando, entre outros, o Acórdão do SCJ, Robert Morrisson *et alii* c. National Australia Bank Ltd. *et alii*, 561 U.S. 247, 23 de junho de 2010.

[974] Acórdão do USCASC, Microsoft Corporation c. United States of America, 14-2985, 14 de julho de 2016, p. 21.

[975] Acórdão do USCASC, Microsoft Corporation c. United States of America, 14-2985, 14 de julho de 2016, p. 9.

território [976]. Aquela instância entendeu que o ato de aceder e "exportar" os dados pessoais da Irlanda constitui uma conduta que ocorre *fora* do território dos EUA e, além disso, que a *Microsoft USA* estaria a atuar como uma *longa manus* dos EUA[977]. Esta tese parte de várias premissas como, por exemplo, a de que o armazenamento persistente dos dados pessoais na Irlanda confere jurisdição a este país sobre os mesmos[978], que as incursões eletrónicas da *Microsoft USA* constituem ofensas à soberania da Irlanda[979], que a "exportação" dos dados pessoais da Irlanda comporta a realização de ações físicas naquele país pelo que, de acordo com o princípio da cortesia internacional, os interesses daquele país devem ser atendidos[980].

O caso não ficou por aqui. Um recurso para o *Supreme Court,* instaurado pelo DoJ, foi aceite em 16 de outubro de 2017. Na sua argumentação, o DoJ rejeita a interpretação do *Court of Appeals* por vários motivos:

(i) O SCA e o mandado em causa são aplicados à *Microsoft USA,* situada no território dos EUA e, além do mais, a divulgação dos dados pessoais ao DoJ ocorreria nos EUA, dada a possibilidade de acesso remoto[981].

[976] Acórdão do USCASC, Microsoft Corporation c. United States of America, 14-2985, 14 de julho de 2016, p. 22 e ss.. Sublinhando que o DIP proíbe a execução unilateral de uma decisão judicial no interior do território de um país terceiro, v. "Brief of International and Extraterritorial Law Scholars as Amici Curiae in Support of Respondent", p. 6, disponível em https://www.supremecourt.gov/DocketPDF/17/17-2/28256/20180118132126676_17-2%20bsac%20International%20and%20Extraterritorial%20Law%20Scholars--PDFA.pdf, consultado no no dia 30 de setembro de 2018.

[977] Acórdão do USCASC, Microsoft Corporation c. United States of America, 14-2985, 14 de julho de 2016, p. 39.

[978] Acórdão do USCASC, Microsoft Corporation c. United States of America, 14-2985, 14 de julho de 2016, p. 40: "os dados encontram-se sujeitos à jurisdição de um Estado soberano estrangeiro".

[979] Sobre este ponto, "Brief of International …" cit., p. 3 e ss..

[980] Acórdão do USCASC, Microsoft Corporation c. United States of America, 14-2985, 14 de julho de 2016, p. 42 e, suportando esta tese, veja-se o contributo de 51 informáticos v. "Brief of 51 Computer Scientists As *Amici Curiae* in Support of The Respondent", disponível em https://www.supremecourt.gov/DocketPDF/17/17-2/28101/20180117133756823_FILE-Amicus%20Brief-US%20v%20Microsoft%20No.%2017-2.pdf, consultado no dia 30 de setembro de 2018.

[981] Acórdão do SCJ, United States of America c. Microsoft Corporation, 584 U.S., 17 de abril de 2018, disponível em https://www.supremecourt.gov/DocketPDF/17/17-2/22902/20171206191900398_17-2tsUnitedStates.pdf, consultado no no dia 30 de setembro de 2018, p. 17. Contudo, o DoJ acaba por admitir, adiante, que há uma transferência dos servidores na Irlanda para os servidores nos EUA operada pela Microsoft USA, v. Acórdão do USCASC, Microsoft Corporation c. United States of America, 14-2985, 14 de julho de 2016, p. 25 e 27.

(ii) O Congresso adotou aquele diploma partindo da premissa de que os destinatários dos mandados nele fundamentados devem transmitir todas as provas e registos sob o seu *controlo técnico*[982].

(iii) Adicionalmente, o DoJ repete o argumento da desadequação dos MLAT's em vigor entre os EUA e a Irlanda sublinhando o processo moroso e burocrático ali consagrado[983].

Por seu turno, a *Microsoft* reiterou os argumentos relativos à extraterritorialidade do SCA com base no critério da localização dos dados pessoais fora dos EUA e invocou, novamente[984], o surgimento de obrigações conflituantes, de conflitos de jurisdição, e a posição frágil de empresas transnacionais à luz do RGPD, designadamente do art. 48.º. Em particular, a *Microsoft* sujeitava-se a coimas no valor de 3.6 biliões de dólares[985].

A argumentação da *Microsoft* amparou-se num conjunto de intervenientes de peso, enquanto *Amicus Curiae,* como outras empresas tecnológicas[986], doutrina[987],

[982] Acórdão do USCASC, Microsoft Corporation c. United States of America, 14-2985, 14 de julho de 2016, p. 18.
[983] Acórdão do USCASC, Microsoft Corporation c. United States of America, 14-2985, 14 de julho de 2016, p. 32.
[984] Acórdão do USCASC, Microsoft Corporation c. United States of America, 14-2985, 14 de julho de 2016, p. 5.
[985] Acórdão do SCJ, United States of America c. Microsoft Corporation, caso 584 U.S., 17 de abril de 2018, disponível em https://www.supremecourt.gov/DocketPDF/17/17-2/27619/20180111205746909_Brief%20for%20Respondent%202018.01.11.pdf , consultado no dia 30 de setembro de 2018, p. 41. Um ponto que é suportado por Anthony COLANGELO, v. "Brief of *Amicus Curiae* Anthony J. Colangelo, International Law Scholar, in support of Appellant", 15 de dezembro de 2015, disponível em https://blogs.microsoft.com/datalaw/wp-content/uploads/sites/149/2014/12/International-Law-Scholar.pdf, consultado no dia 30 de setembro de 2018. O autor invoca a proibição de jurisdição de execução em território alheio, a presunção contra a extraterritorialidade em caso de inexistência de uma intenção clara e, por fim, a existência de tratados que instituem um método adequado e consistente com o DIP para as pretensões do DoJ.
[986] Incluindo as seguintes: Amazon, Google, Cisco, Dropbox, eBay, Facebook, HP, Mozilla, Verizon, entre outras. Cfr. "Brief for Technology Companies as *Amici Curiae* in Support of Respondent", disponível em https://www.supremecourt.gov/DocketPDF/17/17-2/28322/20180118154539559_17-2%20USA%20v.%20Microsoft%20Corporation.pdf, consultado no dia 30 de setembro de 2018.
[987] "Brief of EU Data Protection and Privacy Scholars as *Amici Curiae* in Support of Respondent", 18 de janeiro de 2018, disponível em https://www.supremecourt.gov/DocketPDF/17/17-2/28272/20180118141249281_17-2%20BSAC%20Brief.pdf, consultado no dia 30 de setembro de 2018; "Brief of *Amici Curiae* Electronic Privacy Information Center (EPIC) and Thirty-Seven Technical Experts and Legal Scholars in Support of Respondent", 18 de janeiro de 2018, disponível em https://www.supremecourt.gov/DocketPDF/17/17-2/28360/20180118172113162_17-2%20bsac%20Electronic%20Privacy%20Information%20Center.pdf, consultado no dia 30 de setembro de 2018; "Brief of International and Extraterritorial Law Scholars as *Amici Curiae* in Support of Respondent", disponível em https://www.supremecourt.gov/DocketPDF/17/17-2/28256/20180118132126676_17-2%20bsac%20International%20and%20Extraterritorial%20Law%20Scholars--PDFA.pdf, consultado no no dia 30 de setembro de 2018.

membros do PE[988], a Irlanda[989], entre outros[990]. Vale a pena destacar um argumento transversal a muitas destas posições: a existência de MLTA's, tanto com a Irlanda como com a UE, sendo que a primeira se manifestou disponível para acionar essa via para resolver o problema de base neste caso, isto é, de acesso a dados pessoais armazenados na Irlanda.

No contexto do DIP, a vigência destes acordos à data do pedido do DoJ não deve ser ignorada porquanto sinaliza, por parte dos EUA, a aceitação de um conjunto específico de procedimentos gizados justamente para resolver os problemas de jurisdição e os conflitos aqui em causa com a devida ponderação dos vários interesses em jogo[991]. Tal como em relação aos programas de vigilância, a postura *unilateralista* dos EUA e o desprezo pelo equilíbrio previamente negociado convocam a violação do princípio da boa fé, da proteção da confiança (v. g. *res judicata*) e do *non venire contra factum proprium* (ou *estoppel)*[992].

Fosse o caso relativo a um documento em papel, trancado num armário na Irlanda, e os EUA ver-se-iam na circunstância de ter de recorrer às vias tradicionais de cooperação estadual. Ora, será que a mera *digitalização da prova* sustenta uma alteração das circunstâncias tal, que fundamente a postura unilateral daquele país em detrimento dos interesses dos países terceiros previamente reconhecidos e considerados pelo primeiro? Ou, como explicou o Relator Especial da ONU, "o facto de um diário estar armazenado numa coleção de ficheiros na nuvem e não numa prateleira física não deve dar ao Estado

---

[988] "Brief of *Amici Curiae* Jan Philipp Albrecht, Sophie In'T Veld, Viviane Reding, Birgit Sippel, and Axel Voss, members of the European Parliament in Support of Respondent Microsoft Corporation", disponível em https://www.supremecourt.gov/DocketPDF/17/17-2/28328/20180118155453076_17-2%20bsac%20Jan%20Philipp%20Albrecht.pdf, consultado no dia 30 de setembro de 2018.

[989] Mostrando-se disponível para colaborar com os EUA através dos acordos de assistência mútua, v. "Brief of Amicus Curiae Ireland, *Microsoft* v. *United States of America",* disponível em https://www.eff.org/files/2015/01/12/ireland_microsoft_second_circuit_amicus_brief.pdf, consultado no dia 30 de setembro de 2018.

[990] Uma lista completa encontra-se em https://www.supremecourt.gov/search.aspx?filename=/docket/docketfiles/html/public/17-2.html , consultado no dia 30 de setembro de 2018.

[991] "Ao participar nos processos de negociação dos MLAT's, os EUA aderiram a um conjunto de procedimentos para resolver as complexas questões de jurisdição e de conflitos de leis apresentadas por pedidos de acesso a dados pessoais armazenados no estrangeiro. Esses acordos são o meio pelo qual um país pode obter a assistência de outro para ter acesso aos dados armazenados no segundo. Tal resulta de um equilíbrio ponderado entre as necessidades de uma nação e a autonomia da outra, entre outras coisas, de promover os seus interesses no domínio da proteção dos dados pessoais", v. "Brief for Technology Companies ..." cit., p. 23. Em sentido próximo, v. "Brief of *Amici Curiae* Jan Philipp Albrecht, Sophie …" cit., p. 18 e ss.; "Brief of *Amici Curiae* Electronic Privacy Information Center (EPIC) …" cit., p. 11 e 14; C. RYNGAERT, "Conflicts of …" cit., p. 430.

[992] Sobre este princípio, v. M. DUARTE, *Direitos Internacional Público* cit., p. 153.

o acesso aos primeiros de formas que são materialmente diferentes em relação ao acesso ao segundo" [993].

Mas será que a digitalização da informação, das provas, não exige uma revisão dos MLAT's, desenhados para as transferências de provas tangíveis, ou mesmo a sua substituição por mecanismos mais céleres[994]? Procurando responder a estas questões o Relator Especial da ONU para a privacidade abriu uma discussão sobre um instrumento internacional aplicável aos serviços de informações e às autoridades de aplicação da lei em geral, que incluirá, *inter alia,* um "Mandado Internacional de Acesso aos Dados" para quando "múltiplos Estados têm pretensões *bona fide* sobre os mesmos dados" [995]. No mesmo sentido evoluiu a legislação dos EUA através do CLOUD Act (*Clarifying Lawful Overseas Use of Data Act*), assinado em 23 de abril de 2018, pelo Presidente Trump, e que, entre outros aspetos, veio confirmar a necessidade de os EUA celebrarem novos acordos de assistência mútua com países terceiros. Em face deste desenvolvimento legislativo o DoJ requereu que o caso fosse julgado improcedente, ao que o *Supreme Court* aquiesceu[996].

3.1.2.3.3. Fundamento

Segundo o G29 o fundamento do art. 48.º do RGPD é o Regulamento (CE) n.º 2271/96 do Conselho, de 22 de Novembro de 1996, relativo à proteção contra os efeitos da aplicação extraterritorial de legislação adotada por um país terceiro e das medidas nela baseadas ou dela resultantes[997]. Em face deste entendimento, o art. 48.º aproxima-se de

---

[993] "Brief *Amicus Curiae* of U.N. Special Rapporteur on the Right to Privacy Joseph Cannataci in Support of Neither party", 18 de janeiro de 2018, disponível em https://www.supremecourt.gov/DocketPDF/17/17-2/28272/20180118141249281_17-2%20BSAC%20Brief.pdf, consultado no dia 30 de setembro de 2018.

[994] Sobre as ineficiências dos mecanismos de assistência mútua, v. A. OSULA, "Mutual Legal …" cit., p. 43; Sergio CARRERA *et alii, Access to Electronic Data by Third-Country Law Enforcement Authorities. Challenges to EU Rule of Law and Fundamental Rights,* Centre for European Policy Studies, 2015, disponível em https://www.ceps.eu/system/files/Access%20to%20Electronic%20Data%20%2B%20covers_0.pdf, consultado no dia 30 de setembro de 2018; "Brief of *Amici Curiae* Electronic Privacy Information Cnter (EPIC) …" cit., p. 11 e ss.; "Brief *Amicus Curiae* of U.N. Special …" cit., p. 25; "Brief of Internet Lab Law and Technology Center as *Amicus Curiae* in Support of Respondent", p. 31, disponível em https://www.supremecourt.gov/DocketPDF/17/17-2/28382/20180118203851162_17-2%20bsac%20Internetlab%20Law%20and%20Technology%20Center.pdf, consultado no no dia 30 de setembro de 2018.

[995] "Draft Legal Instrument on …" cit., p. 3.

[996] Acórdão do SCJ, United States of America c. Microsoft Corporation, caso 584 U.S., 17 de abril de 2018, disponível em https://www.supremecourt.gov/opinions/17pdf/17-2_1824.pdf, consultado no dia 30 de setembro de 2018.

[997] G29, "Parecer 05/2012 …" cit., p. 28.

uma disposição bloqueante ao não reconhecer ou executar decisões judiciais ou decisões de autoridades administrativas de países terceiros.

Há duas conclusões que retiro da natureza bloqueante desta norma. Em primeiro lugar, como referi, mesmo na versão proposta pela PE, o art. 48.º nunca seria uma espécie de *deus ex machina* de resolução dos problemas suscitados *pós Snowden*[998]. Ainda assim, não o esvazio de sentido. Coincidindo a autonomização desta norma com as divulgações de ES, o seu significado *político*, próximo de uma espécie de *protesto* da UE em relação à "aplicabilidade extraterritorial" das "leis, regulamentos e atos normativos" que implementam programas de vigilância, não deve ser ignorado. Este é um caminho para a UE dar nota da sua posição à opinião pública mundial e contrariar uma postura de inação ou silêncio que poderia ser interpretada como aquiescência. Num domínio como este, conexo com os direitos fundamentais, não seria espectável que a UE, à luz da missão que atribuiu a si própria no direito originário[999], abdicasse de uma posição contestatária à consolidação de uma situação de vigilância (e espionagem) estrangeira. Como sintetizam F. BIGNAMI e G. RESTA, "a existência de um coro de vozes sonantes na Europa poderá manter a atenção para um problema político por resolver, preservando as violações de direitos fundamentais na agenda pública global"[1000].

Acresce que, como disse, esta norma reflete o entendimento de que o direito estrangeiro atentatório dos direitos fundamentais, sejam decisões administrativas ou sentenças judiciais, para produzir efeitos na UE requer um reconhecimento oficial e uma integração formal na ordem jurídica da mesma, por exemplo, através de um acordo internacional ou, como propunha o PE no art. 43.º-A, de um controlo pelas autoridades competentes[1001]. Nesse sentido, as imposições de países terceiros para transferir dados pessoais para as autoridades desses países devem ser formalmente enquadradas, por exemplo, nos MLAT's[1002]. Daí haver quem entenda que esta disposição irá encorajar

[998] G29, "Working Document on …" cit. p. 51; K. HON, *Data Localization* cit., p. 314.
[999] Art. 3.º, n.º 5 do TUE: "Nas suas relações com o resto do mundo, a União afirma e promove os seus valores e interesses e contribui para a proteção dos seus cidadãos. Contribui para a paz, a segurança, o desenvolvimento sustentável do planeta, a solidariedade e o respeito mútuo entre os povos, o comércio livre e equitativo, a erradicação da pobreza e a proteção dos direitos do Homem, em especial os da criança, bem como para a rigorosa observância e o desenvolvimento do direito internacional, incluindo o respeito dos princípios da Carta das Nações Unidas".
[1000] F. BIGNAMI e G. RESTA, "Transatlantic ..." cit., p. 266.
[1001] G29, "Parecer 06/2014 ..." cit., p. 30.
[1002] Reforçando esta tese, v. "Brief of the European Commission on Behalf of the European Union as *Amicus Curiae* in support of Neither Party", p. 14, disponível em https://www.supremecourt.gov/DocketPDF/17/17-2/23655/20171213123137791_17-2%20ac%20European%20Commission%20for%20filing.pdf, consultado no dia 30 de setembro de 2018.

países terceiros a entrar em negociações com a UE para a celebração de acordos de assistência judiciária[1003].

Em segundo lugar, apesar da simplificação deste artigo na redação final, o mesmo vem colocar os operadores económicos transnacionais, como no caso *Microsoft*, diante de um conflito: ou violam o RGPD ou o direito do país terceiro[1004]. De todo o modo, como demonstra a argumentação daquela empresa no *Supreme Court,* a invocação desta disposição pode ser útil numa estratégia de defesa, de modo a persuadir o decisor estrangeiro da validade da recusa de cumprir o mandado do DoJ. Como referi, ainda que com algum erraticismo, esta poderá ser uma das funções das normas de bloqueamento[1005].

3.2. Caraterização da extraterritorialidade segundo o regime das transferências

3.2.1. Os interesses prosseguidos

Nem os considerandos da Diretiva nem os artigos 25.º e ss. esclarecem os interesses prosseguidos pela restrição às transferências de dados pessoais[1006]. Recorrendo ao elemento histórico encontro um primeiro esclarecimento na exposição de motivos da proposta de 1992: "a regra que visa prevenir que o regime da Comunidade seja contornado na sequência de transferências para países terceiros assume a forma de uma proibição de transferir dados para países que não garantem um nível de proteção adequado (...). Sem esta regra os esforços da Comunidade para garantir um elevado nível de proteção aos indivíduos poderiam ser anulados pelas transferências para outros países nos quais a proteção dos dados pessoais é inadequada"[1007].

O G29 veio a confirmar que o que se pretende é criar "condições que garantem que as pessoas em causa continuam a ser protegidas no que toca ao tratamento dos seus dados depois de efetuada a transferência", acrescentando que "o princípio da proteção adequada,

---

[1003] H. HIJMANS, *The European Union* cit., p. 500.
[1004] D. J. KESSLER, J. NOVAK e S. KHAN, "The potential impact …" cit., p. 595 e K. HON, *Data Localization*, cit., p. 314.
[1005] Para alguns autores, o art. 48.º é uma afirmação clara de quanto a UE valoriza a proteção de dados pessoais dando-lhe prioridade sobre outras preocupações comerciais e nacionais, pelo que os tribunais americanos não poderão descurar este seu interesse, v. D. J. KESSLER, J. NOVAK e S. KHAN, "The potential impact …" cit., p. 608.
[1006] Constatando o mesmo, v. C. REED, *Making Laws* cit., p. 175; K. HON, *Data Localization* cit., p. 46.
[1007] Comissão Europeia, "Amended proposal for a Council Directive on the protection of individuals with regard to the processing of personal data and on the free movement of such data. Explanatory Memorandum", 15 de outubro de 1992, p. 34, disponível em http://aei.pitt.edu/10375/1/10375.pdf, consultado no dia 30 de setembro de 2018.

consagrado no artigo 25.º, justifica-se para garantir que as pessoas continuem a beneficiar dos direitos e liberdades fundamentais que lhes assistem no tratamento dos seus dados pessoais na União Europeia mesmo quando esses dados tenham sido transferidos para um país terceiro. Visa ainda impedir que seja possível contornar a proteção garantida pela legislação europeia de proteção de dados pessoais pelo facto de os dados serem transferidos para países terceiros"[1008].

Com efeito, recordando o que disse, exige-se ao exportador que "sempre que esteja previsto transferir dados pessoais para um país terceiro (...) *preconizar soluções que facultem às pessoas em causa a garantia de que, mesmo depois de transferidos os seus dados, continuarão a beneficiar dos direitos fundamentais e das garantias a que têm direito na UE*"[1009] (itálicos meus).

A mesma leitura é feita pela doutrina segundo a qual esta espécie de *controlo de fronteira* dos dados pessoais visa garantir a continuidade da proteção dos titulares dos dados[1010]. Como sublinhou o SEPD, "as garantias de proteção dos dados pessoais são diferentes consoante o país onde se encontram localizados"[1011]. Portanto, o controlo das transferências acautela o impacto de eventuais lacunas no direito estrangeiro do país de destino dos dados pessoais já que "quando os dados pessoais são transferidos para um país terceiro (…) esse país pode, através da sua legislação, regulação e/ou outras ações, afetar o nível de proteção dos dados oriundos da UE" [1012].

[1008] G29, "Documento de Trabalho sobre uma ..." cit., p. 7 e 8.
[1009] *Idem*, p. 10.
[1010] Allan GOTLIEB *et alii*, "The Transborder Transfer of Information by Communications and Computer Systems: Issues and Approaches to Guiding Principles", *AJIL,* vol. 68, n.º 2, p. 247; C. KUNER, *Transborder* cit., p. 107 e 116; Dan SVANTESSON, "The regulation of cross-border data flows", *IDPL,* vol. 1, n.º 3, 2011, p. 191 e, do mesmo autor, "Privacy, The Internet and Transborder Data Flows. An Australian Perspective", *MUJLT,* vol. 4, n.º 1, 2010, p. 2 e ss.; Frits HONDIUS, *Emerging Data Protection in Europe,* Elsevier, 1975, p. 247; Gehan GUNASEKARA, "The 'Final' Privacy Frontier? Regulating Trans-Border Data Flows" *IJLIT,* vol. 17, n.º 2, 2009, p. 155; K. HON, *Data Localization* cit., p. 25, 46 e 136.
[1011] SEPD, "Opinion on the Commission's Communication on 'Unleashing the Potential of Cloud Computing in Europe'", 2012, n.º 104, disponível em https://edps.europa.eu/sites/edp/files/publication/12-11-16_cloud_computing_en.pdf, consultado no no dia 30 de setembro de 2018 e, em sentido próximo, AEPD, "Guía para clientes que contraten servicios de Cloud Computing", 2013, p. 15, disponível em https://future.inese.es/aepd-guia-para-clientes-que-contraten-servicios-de-cloud-computing/, consultado no dia 30 de setembro de 2018.
[1012] Um relatório para o PE confirma que o regime das transferências "implicitamente reconhece que as transferências para países terceiros com uma proteção que não é equivalente pode conduzir a uma redução da proteção" v. Jonathan CAVE *et alii*, "Data protection review: impact on EU innovation and competitiveness – study for the European Parliament's Committee on Industry, Research and Energy", 2012, p. 18, disponível em http://www.europarl.europa.eu/RegData/etudes/etudes/join/2012/492463/IPOL-ITRE_ET(2012)492463_EN.pdf, consultado no dia 30 de setembro de 2018 e K. HON, *Data Localization* cit., p. 125.

Também ao nível internacional singrou a tese de controlar as transferências de dados pessoais para *data heavens*, tanto na OCDE[1013] como no CdE[1014]. Noutros países, como no Canadá, a preocupação é a mesma: "algumas transferências são perigosas por causa da natureza incerta do direito estrangeiro"[1015].

No caso *Schrems,* o TJ confirmou que este regime visa "assegurar (...) a continuidade do nível elevado da proteção em caso de transferência de dados pessoais para um país terceiro" e que "o elevado nível de proteção garantido pela Diretiva 95/46, lida à luz da Carta, poderia ser facilmente contornado através de transferências de dados pessoais na União para países terceiros com vista ao seu tratamento nesses países"[1016]. O RGPD determina, no considerando 101 e na parte final do art. 44.º, n.º 1 que "[t]odas as disposições do presente capítulo são aplicadas de forma a assegurar que não é comprometido o nível de proteção das pessoas singulares garantido pelo presente regulamento". É que, como dispõe o considerando 116, "sempre que os dados pessoais atravessarem fronteiras fora do território da União, aumenta o *risco* de que as pessoas singulares não possam exercer os seus direitos à proteção de dados, nomeadamente para se protegerem da *utilização ilegal ou da divulgação dessas informações*" (itálicos meus).

O risco de desproteção das pessoas singulares foi confirmado nas revelações de ES, mas havia já sido antecedido por um alerta do G29[1017] e apontado noutras latitudes[1018]. A verdade é que, nas relações entre a UE e os EUA, este é um risco que se materializou, em 2006, no caso *SWIFT,* e atingiu o ponto máximo com a decisão *Schrems* decidida a 5 de outubro de 2015 pelo TJ[1019]. O segundo caso será tratado adiante, mas o primeiro merece agora uma breve explicação. A *SWIFT* é uma cooperativa com sede na Bélgica que presta um serviço mundial de mensagens financeiras que facilita as transferências internacionais

---

[1013] "Supplementary Explanatory Memorandum to the revised OECD Privacy Guidelines", 2013, p. 29.
[1014] CdE, "New Technologies: A Challenge to Privacy Protection? (1989) Study prepared by the Committee of Experts on Data Protection (CJ-PD) under the Authority of the European Committee on Legal Co-operation (CDCJ)", 1989, p. 25, disponível em https://rm.coe.int/1680684607, consultado no dia 30 de setembro de 2018.
[1015] OPC, "Guidelines for Processing Personal Data across Borders", 2009, disponível em https://www.priv.gc.ca/en/privacy-topics/personal-information-transferred-across-borders/gl_dab_090127/, consultado no dia 30 de setembro de 2018.
[1016] Acórdão do TJ, Maximillian Schrems c. Data Protection Commissioner, C-363/14, 6 de outubro de 2015, n.º 72 e 73.
[1017] G29, "Documento de trabalho. Transferência ..." cit., p. 22 e 23 e K. HON, *Data Localization* cit., p. 55.
[1018] Information & Privacy Commissioner for British Columbia, "Privacy and the USA Patriot Act: Implications for British Columbia Public Sector Outsourcing", Outubro de 2004, disponível em https://www.oipc.bc.ca/special-reports/1271, consultado no no dia 30 de setembro de 2018.
[1019] Acórdão do TJ, Maximillian Schrems c. Data Protection Commissioner, C-363/14, 6 de outubro de 2015.

de dinheiro. Sucede que armazenava todas as mensagens, contendo dados pessoais como os nomes do pagador e do beneficiário, em dois centros operacionais, um na UE e outro nos EUA, através de uma forma de tratamento designada por "cópia integral". Em finais de junho de 2006 a comunicação social divulgou que, desde os atentados do 11 de setembro, as autoridades dos EUA, designadamente o Departamento de Tesouro, acediam de forma pouco transparente aos dados pessoais conservados nos EUA[1020].

O interesse prosseguido pelo regime das transferências, de garantir a continuidade da proteção do titular dos dados pessoais, é um corolário do dever de proteção de direitos fundamentais que será o fundamento último da restrição às transferências para fora da UE[1021]. Foi esse o entendimento do TJ, no caso *Schrems,* ao afirmar que "o artigo 25.º, n.º 6, da Diretiva 95/46 dá execução à *obrigação explícita* de proteção dos dados pessoais, prevista no artigo 8.º, n.º 1, da Carta, e visa assegurar, como o AG salientou no n.º 139 das suas conclusões, a continuidade do nível elevado dessa proteção em caso de transferência de dados pessoais para um país terceiro" (itálicos meus)[1022]. Já era assim quanto às restrições a transferências nas primeiras legislações de proteção de dados pessoais, que encontravam fundamento na ideia de que o Estado tem o dever de proteger os direitos e a dignidade dos indivíduos dentro das suas fronteiras e a permissão indiscriminada e irrestrita de transferências para fora dali, poderia colocá-los em perigo[1023].

Por fim, a doutrina é hoje consensual quanto à rejeição de um hipotético interesse prosseguido pela restrição de transferências de dados pessoais: o protecionismo comercial[1024]. É verdade que o controlo de fronteira dos dados pessoais poderá ter impacto nas trocas comerciais internacionais, mas, em boa verdade, o mesmo é coerente com a criação de um "nível elevado de proteção" na UE porquanto, como explica L.

[1020] G29, "Parecer 10/2006 sobre o tratamento de dados pessoais pela Sociedade das Telecomunicações Financeiras Interbancárias no Mundo (Worldwide Interbank Financial Telecommunication – SWIFT)", 22 de novembro de 2006.

[1021] C. KUNER, *Transborder* cit., p. 114; D. LINDSAY, "The Role …" cit., p. 73; Y. POULLET, "Transborder Data …" cit., p. 143 e ss. e, referindo uma necessidade de coerência na proteção, K. HON, *Data Localization*, cit., p. 46.

[1022] Acórdão do TJ, Maximillian Schrems c. Data Protection Commissioner, C-363/14, 6 de outubro de 2015, n.º 72.

[1023] C. KUNER, *Transborder* cit., p. 115 citando Lucius WOCHNER, *Der Personlichkeitsschutz im grenzuberschreitenden Datenverkehr,* Schulthess Polygraphischer Verlag, 1981, p. 24.

[1024] Fred CATE, "Privacy and telecommunication", *WFLR,* n.º 33, vol. 1, 1998, p. 35; J. C. O'QUINN, "None of your business: world data flows, electronic commerce, and the European privacy directive", *HJLT,* vol. 12, n.º 3, 1998, p. 692; K. HON, *Data Localization* cit., p. 55; Lee BYGRAVE, "Privacy and data protection in an international perspective", *SSL*, n.º 56, 2010, p. 187; Office of the United States Trade Representative, "Section 1377 Review on Compliance with Telecommunications Trade Agreement", 2014, p. 5.

BYGRAVE, visa uma proteção *efetiva* e *integra* dos dados pessoais[1025]. Por outro lado, as regras internacionais aplicáveis ao comércio internacional favorecem uma abordagem deste tipo[1026]. Acresce que, a meu ver, um dos interesses subjacentes à progressiva flexibilização e alargamento das "garantias adequadas" é, justamente, o comércio internacional, tal como dispõe o considerando 101. O desafio será, então, conciliar esta necessária flexibilidade com a continuidade do nível de proteção.

Adicionalmente, o regime das transferências prossegue um outro interesse, externo ou da comunidade internacional, se atentarmos nas particularidades da sua vocação extraterritorial, explicada de seguida.

3.2.2. Natureza específica: o regime das transferências enquanto "extensão territorial" do DUE

A dimensão extraterritorial da regulação das transferências não é óbvia[1027]. Por outras palavras, a "tentativa de regular (...) a conduta de pessoas, bens ou atos, além-fronteiras" que trato neste trabalho adquire contornos específicos por força do *modus operandi* da continuidade da proteção do titular dos dados que o legislador pretende assegurar através da exigência de um fundamento para as transferências. Com efeito, esta opção legislativa tem duas consequências:

(i) Está na origem da tentativa de regular os tratamentos de dados pessoais realizados pelo importador dos dados pessoais situado num país terceiro;

[1025] L. BYGRAVE, "Privacy and …" cit., p. 187.

[1026] G29, "Documento de trabalho ..." cit., p. 8. Analisando a aplicação da exceção do art. XIV, al. c), ii), do GATS ao regime das transferências da UE, v. Maria ASINARI, "Is there any Room for Privacy and Protection within WTO Rules?", *ECLR*, n.º 9, 2002, p. 249 e ss. e, da mesma autora, "The WTO and the Protection of Personal Data. Do EU Measures Fall within Gats Exception? Which Future for Data Protection within the WTO e-commerce Context?", 18th BILETA Conference: Controlling Information in the Online Environment, abril de 2013, disponível em http://www.bileta.ac.uk/content/files/conference%20papers/2003/The%20WTO%20and%20the%20Protection%20of%20Personal%20Data.%20Do%20EU%20Measures%20Fall%20within%20GATS%20Exception.pdf, consultado no dia 30 de setembro de 2018.Uma análise semelhante v. UNCTAD, "Data protection regulations and international flows: Implications for trade and development", 2016, p. 3, UNCTAD, "Data protection regulations and international flows: Implications for trade and development", 2016, disponível em http://unctad.org/en/PublicationsLibrary/dtlstict2016d1_en.pdf, consultado no dia 30 de setembro de 2018 e Y. POULLET, "Transborder Data …" cit., p. 141 e ss..

[1027] C. KUNER, *Transborder* cit., p. 121 e, do mesmo autor, "Extraterritoriality and regulation …" cit., p. 235 e ss.; Y. POULLET, "Transborder Data …" cit., p. 141 e ss..

(ii) É o meio para garantir a proteção do titular dos dados "fora do perímetro assegurado pela diretiva", delimitado pelo seu art. 4.º e, agora, pelo art. 3.º do RGPD[1028].

No que respeita às garantias adequadas, a tentativa de regular os tratamentos de dados realizados pelo importador localizado num país terceiro não adequado, é clara. Se, nesse país, vigora uma "insuficiência da proteção de dados pessoais" o importador deverá compensar essa lacuna comprometendo-se com as "medidas necessárias" ou garantias adequadas para o efeito propostas pelo exportador[1029]. Com efeito, o destinatário primário destas garantias é o exportador dos dados que só pode prosseguir as suas operações de transferências fundamentando as mesmas numa garantia. Porém, o que estas verdadeiramente visam regular são os tratamentos de dados pessoais do importador já que é este que se encontra num país terceiro com proteção insuficiente e que se vincula ao cumprimento daquelas garantias.

De facto, a celebração de um contrato-tipo ou a adoção de RVAE impõem um conjunto de princípios e de regras ao importador dos dados pessoais. Com efeito, a propósito das cláusulas contratuais, o G29 sustentou que as garantias adequadas "terão de compensar de forma satisfatória a ausência de um nível de proteção adequado, através da inclusão de elementos essenciais de proteção omissos numa determinada situação"[1030]. Veja-se, a título de exemplo, a cláusula 5 da decisão da COM, de 15 de junho de 2001, vinculando o importador a um conjunto de princípios, os "elementos essenciais" do regime da UE, enumerados no apêndice 2 ou 3[1031]. O mesmo acontece nas cláusulas aprovadas pela COM, em 2010, para transferências de dados pessoais para subcontratantes[1032]. Também, no que respeita à adoção das RVAE, os membros do grupo empresarial, situados em países terceiros, devem observar exigências decorrentes do DUE[1033].

Como se vê, a extensão do DUE operada deste modo distingue-se dos casos do art. 4.º da Diretiva e 3.º do RGPD pois não decorre diretamente de uma prescrição legislativa

[1028] G29, "Documento de trabalho. Transferência ..." cit., p. 17.
[1029] Considerando 108.
[1030] *Ibidem*.
[1031] Decisão da Comissão de 15 de junho de 2001 relativa às cláusulas contratuais-tipo aplicáveis à transferência de dados pessoais para países terceiros, nos termos da Diretiva 95/46/CE (Decisão 2001/497/EC).
[1032] Decisão da Comissão de 5 de fevereiro de 2010 relativa a cláusulas contratuais-tipo aplicáveis à transferência de dados pessoais para subcontratantes estabelecidos em países terceiros nos termos da Diretiva 95/46/CE do Parlamento Europeu e do Conselho. O G29 sublinha o mesmo ponto, v. "Working Document on surveillance ..." cit., p. 42.
[1033] G29, "Working Document Establishing a Model Checklist …" cit., p. 8.

mas, ao invés, é intermediada por uma garantia adequada. Em todo o caso, as normas que delimitam o âmbito de aplicação da Diretiva e do RGPD desempenham uma função equivalente: garantir que a proteção criada ao nível da UE é aplicada a tratamentos de dados pessoais de utilizadores de dados pessoais situados fora das fronteiras da UE[1034].

Mas as especificidades da extraterritorialidade do regime das transferências não se quedam por aqui, sobretudo se atentarmos a outro fundamento das transferências de dados pessoais: a decisão de adequação do país terceiro. A configuração deste fundamento e do procedimento que o antecede gira em torno de uma "cláusula de equivalência" prevista no art. 25.º da Diretiva e no art. 45.º do RGPD. Por outras palavras, o país terceiro só é adequado se o respetivo ordenamento jurídico garantir uma proteção do titular dos dados pessoais "essencialmente equivalente" à da UE[1035].

Este é o primeiro indicador de que o legislador recorreu à técnica da "extensão territorial" apresentada na Parte I. A segunda evidência é o elo territorial com a UE nas situações jurídicas no âmbito das transferências na medida em que a origem daquelas é o seu território: seja porque os dados pessoais "partem" dali, porque o titular dos dados pessoais se encontra ali ou o utilizador dos dados pessoais está ali estabelecido[1036]. Por fim, o terceiro indicador de que o legislador recorreu àquela técnica é a efetiva intervenção regulatória da UE, sobretudo a um nível intermédio (do conteúdo do direito estrangeiro) e macro (da evolução do DIP).

Quanto ao primeiro, resulta de uma estratégia de regulação transnacional tipo *carrot and stick:* ao consagrar uma decisão de adequação como fundamento para as transferências de dados pessoais, a UE cria um incentivo para os países terceiros adotarem legislação equivalente de modo a que os operadores económicos ali situados sejam, por força da vigência de uma decisão de adequação, importadores privilegiados dos dados pessoais oriundos do mercado da UE. Se, como observa C. KUNER, os benefícios oriundos de uma decisão de adequação (*v.g.* em termos de competitividade da economia do país visado) não foram ainda empiricamente verificados, pelo menos constam das perceções dos países terceiros[1037].

[1034] C. KUNER, *Transborder* cit., p. 125.
[1035] Considerando 104.
[1036] C. RYNGAERT, "Whither Territoriality? …" cit., p. 434.
[1037] C. KUNER, "The Internet and …" cit., p. 18 e, do mesmo autor, *Transborder* ... cit., p. 66. No caso da Índia, v. Amiti SEN e Harsimran JULKA, "India seeks 'Data Secure Nation' status, move Hi-end business from European Union", *The Economic Times*, 16 de Abril de 2012, disponível em http://economictimes.indiatimes.com/news/economy/foreign-trade/india-seeks-data-secure-nation-status-more-hi-end-business-from-european-union/articleshow/12681901.cms consultado no dia 30 de setembro de 2018, onde se explica o *lobby* do governo indiano para a Comissão Europeia adotar uma decisão de

A doutrina e a própria COM confirmam o sucesso daquela estratégia[1038]. De facto, nos últimos anos, cada vez mais países em todo o mundo, de África à Ásia, adotaram, ou estão em vias de o fazer, legislação em matéria de proteção de dados pessoais influenciada pelo padrão da UE[1039]. Os casos mais recentes são a Índia, o Japão e a Coreia do Sul que adotaram ou modernizaram recentemente legislação à luz do modelo da UE[1040]. No

adequação. No caso da Nova Zelândia a ideia enunciada no corpo do texto é bem visível nas palavras do New Zealand Privacy Commissioner, "Privacy amendment important for trade and consumer protection", 26 de Agosto de 2010: "Uma decisão de adequação da UE satisfaz os requisitos de exportação de dados para outros países. Eu acredito que as empresas da Nova Zelândia já estão a perder algumas oportunidades económicas por força das lacunas nas nossas regras de proteção de dados. Esta mudança permitirá à Nova Zelândia competir numa base segura a nível internacional", disponível em https://privacy.org.nz/news-and-publications/statements-media-releases/updated-media-release-30-8-10-privacy-amendment-important-for-trade-and-consumer-protection/, consultado no dia 30 de setembro de 2018. No caso do Uruguai, o sítio *web* da presidência, aquando da adoção da decisão daquele país, explicava que "(…) a decisão de adequação irá favorecer o fluxo de dados e a transferência de informação em termos comerciais e financeiros" v. David HASKEL, "Uruguay's Data Protection Act Wins Key EC Support; Seen Generating New Business", *Privacy Law Watch, Bloomberg*, disponível em http://en.ferrere.com/latest-posts/news/uruguays-data-protection-act-wins-key-ec-support/documentos/uruguay-data-protection.pdf, consultado no dia 30 de setembro de 2018. No caso do Canadá sucedeu o mesmo, v. Steve COUGHAN, "Global reach, Local grasp: Constructing extraterritorial jurisdiction in the Age of Globalization", *Report addressed to the Law Commission of Canada*, 23 de junho de 2006, disponível em https://dalspace.library.dal.ca/bitstream/handle/10222/10268/Coughlan_Currie%20et%20al.%20Extraterritoriality%20EN.pdf?sequence=1&isAllowed=y, consultado no dia 30 de setembro de 2018.

[1038] Alex MAKULILO, "Privacy and Data protection in Africa: a state of the art", *IDPL,* vol. 2, n.º 3, 2012, p. 172; Comissão Europeia, "Intercâmbio ..." cit., p. 2; Corin PRINS, "Should ICT regulation be undertaken at an international level?", Bert-Jaap KOOPS *et alii* (eds.), *Starting Points for ICT Regulation: Deconstructing Prevalent Policy One-Liners,* TMC Asser Press, 2006, p. 162 e 172; C. KUNER, *European* cit., capítulo 4.5.1. e, do mesmo autor, "The European Union and the Search for an International Data Protection Framework", *GJIL*, vol. 2, n.º 2, 2014, p. 60; D. SVANTESSON, "The regulation of …" cit., p. 184 e 196; Graham GREENLEAF, "The influence of European Privacy Standards Outside Europe: Implications for Globalisation of Convention 108", *IDPL,* vol. 2, n.º 2, 2012, p. 68 e do mesmo autor, "Do not dismiss 'adequacy': European data privacy standards are entrenched", *PLB,* n.º 114, dezembro de 2011, p. 17, "Global data privacy laws 2015: 109 countries, with European laws now in a minority", *PLB,* n.º 133, 2015, p. 14 e *Asian Data Privacy Laws. Trade and Human Rights Perspectives,* Oxford University Press, 2014, p. 3 e ss.; K. HON, *Data Localization* cit., p. 25, 149 e 334; L. BYGRAVE, "Privacy and …" cit., p. 163; L. MOEREL, *Binding Corporate* cit., p. 19; Paul DE HERT e Vagelis PAPAKONSTANTINOU, "Three scenarios for international governance of data privacy: towards an international data privacy organization, preferably a UN agency?", *I/S: A Journal of Law and Policy for the Information Society,* vol. 9, 2013, p. 275; P. SCHWARTZ, "The EU-U.S. …" cit., p. 1966 e ss.; Y. POULLET, "Transborder Data …" cit., p. 141 e ss..

[1039] A. BRADFORD, "The Brussels ..." cit., p. 3; A. NEWMAN, *Protectors of* cit., p. 3; Antonio REIGADA, "El desarrollo de la protección de datos personales en iberoamérica desde una perspectiva comparada y el reequilibro en los modelos de protección de datos a nivel internacional", *Revista Internacional de Protección de Datos Personales,* n.º 1, Julho-Dezembro de 2012, p. 4 e ss.; Colin BENNETT e Charles RAAB, *The Governance of Privacy: Policy Instruments in Global Perspective,* MIT Press, 2003, p. 93; C. KUNER, "The Internet and …" cit., p. 18; G. GREENLEAF, *Asian Data* cit., p. 3; P. SCHWARTZ, "The EU-U.S. …" cit., p. 1979; UNCTAD, "Data protection regulations …" cit., p. 8 e 42.

[1040] Comissão Europeia, "Intercâmbio ..." cit., p. 9.

passado, contam-se, por exemplo, a Argentina[1041], o Canadá[1042], o Uruguai[1043] e a Nova Zelândia[1044]. Por seu turno, a adoção do RGPD levou alguns países a repensar os respetivos ordenamentos jurídicos, sobretudo países que foram no passado considerados adequados, como o Canadá[1045], a Argentina[1046] e a Nova Zelândia[1047].

[1041] Este país adotou a Lei sobre a proteção dos dados pessoais a 4 de Outubro de 2001 e o Decreto Regulamentar 1558/2001, antes de solicitar que a Comissão Europeia verificasse que a Argentina assegura um nível de proteção adequado, um pedido que foi efetuado por Carta do Embaixador junto da UE em 23 de janeiro de 2002, v. Decisão da Comissão Europeia de 30 de junho de 2003, nos termos da Diretiva 95/46/CE do Parlamento Europeu e do Conselho relativa à adequação do nível de proteção de dados pessoais na Argentina (Decisão 2003/490/EC); G29, "Parecer sobre o nível de proteção dos dados pessoais na Argentina", 3 de outubro de 2002; J. REIDENBERG, "E-Commerce and ..." cit., p. 717 e ss.; Maxim GAKH, "Argentina's Protection of Personal Data: Initiation and Response", *I/S: A Journal of Law and Policy*, vol. 2, n.º 3, 2006, p. 781 e ss..

[1042] A adoção do PIPEDA (*Personal Information Protection and Electronic Documents Act*) antecedeu a declaração da Comissão Europeia sobre a adequação do Canadá. Cfr. Decisão da Comissão Europeia de 20 de Dezembro de 2001, nos termos da Diretiva 95/46/CE do Parlamento Europeu e do Conselho relativa à adequação do nível de proteção proporcionado pela lei canadiana sobre dados pessoais e documentos eletrónicos (Personal Information and Electronic Documents Act); C. BENNETT, C. RAAB, *The Governance* of, cit., p. 117; G29, "Parecer 2/2001 relativo ao nível de adequação proporcionado pela lei canadiana sobre dados pessoais e documentos eletrónicos (*Personal Information and Electronic Documents Act*), 26 de janeiro de 2001; Jennifer MCCLENNA e Vadim SCHICK, "'O, Privacy'. Canada's Importance in the Development of the International Data Privacy Regime", *GJIL,* vol. 38, 2007, p. 669 e ss.; J. REIDENBERG, "E-Commerce …" cit., p. 737. Em particular, justificando a proposta Canadiana para a criação de uma proteção de dados pessoais compreensiva por força das exigências da legislação europeia, v. Industry Canada, "The International Evolution of Data Protection", dezembro de 2000, disponível em www.e-com.ic.gc.ca/english/fastfacts/43d10.htm, consultado no dia 30 de setembro de 2018.

[1043] O Uruguai apresentou um pedido de decisão de adequação em outubro de 2008 depois da aprovação da Lei n.º 18331, de 11 de Agosto de 2008, relativa à proteção dos dados pessoais. Posteriormente adotou também o Decreto Regulamentar de 31 de agosto de 2009 que procede à sua aplicação, v. G29, "Parecer 6/2010 sobre o nível de proteção dos dados pessoais na República Oriental do Uruguai", 12 de outubro de 2010 e Decisão de execução da Comissão Europeia, de 21 de agosto de 2012, nos termos da diretiva 95/46/CE do Parlamento Europeu e do Conselho relativa à adequação do nível de proteção de dados pessoais pela República Oriental do Uruguai no que se refere ao tratamento automatizado de dados (Decisão 2102/484/EU).

[1044] Privacy Commissioner, "Privacy Bill hels trade in global economic climate", disponível em https://privacy.org.nz/news-and-publications/statements-media-releases/media-release-privacy-cross-border-amendment-bill/, consultado no dia 30 de setembro de 2018; G29, "Parecer 1/2011 sobre o nível de proteção de dados pessoais na Nova Zelândia", 4 de abril de 2011, p. 2 e Nigel WATERS, "The European influence on privacy law and practice", *PLPR,* n.º 2, 2003, disponível em http://www.austlii.edu.au/au/journals/PLPR/2003/2.html, consultado no dia 30 de setembro de 2018.

[1045] Office of the Privacy Commissioner of Canada, "The Case for Reforming the Personal Information Protection and Electronic Documents Act", maio de 2013, disponível em https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/pipeda_r/pipeda_r_201305/, consultado no no dia 30 de setembro de 2018; Gabe MALDOFF e Omer TENE, "'Essential Equivalence' and European Adequacy after Schrems: The Canadian Example", *WILJ,* n.º 34, 2016, p. 211 e ss..

[1046] Diego FERNANDEZ, "La Dirección Nacional de Protección de Datos Personales em Argentina invita a debatir sobre la posible reforma a Ley de Protección de Datos Personales", disponível em https://iapp.org/news/a/la-direccion-nacional-de-proteccion-de-datos-personales-en-argentina-invita-a-debatir-sobre-la-posible-reforma-a-ley-de-proteccion-de-datos-personales/, consultado no dia 30 de setembro de 2018. A documentação desta reforma está disponível no sítio do Ministério da Justicia y Derechos Humanos em https://www.justicia2020.gob.ar/justicia-2020-reabre-debate-reforma-ley-proteccion-datos-personales/, consultado no dia 30 de setembro de 2018.

[1047] John HANNAN e Brittany MOORE, "Proposed Amendments to New Zealand Privacy Law. New powers to audit and compel compliance – Million dólar penalties", disponível em

Contudo, é verdade que quase se contam pelos dedos das mãos os países "adequados"[1048]. Esta passividade da COM, sem grande impacto na capacidade de persuasão dos benefícios de um alinhamento normativo com a UE, parece ter chegado ao fim com o anúncio recente de uma "colaboração ativa" com países como o Japão, a Coreia do Sul e a India, bem como países do Mercosul e países abrangidos pela Política Europeia de Vizinhança[1049]. Recentemente, a Coreia do Sul formalizou junto da COM um pedido de decisão de adequação[1050], e há quem defenda que também a Colômbia, o México e o Peru passariam no teste de adequação em virtude de alterações recentes nos respetivos ordenamentos jurídicos[1051].

Além da incidência regulatória num nível intermédio, a intervenção da UE espraia-se a um nível global. Como expliquei, ao procedimento de avaliação da adequação não é indiferente a adesão do país terceiro à Convenção n.º 108 do CdE conforme dispõe o considerando 105 do RGPD. Assim se cria um estímulo à adesão a este instrumento, aprofundando-se o desenvolvimento do DIP neste domínio o que, na prática, se tem traduzido em vários pedidos de adesão por parte de Estados sem assento no CdE como a Argentina (já considerada adequada), Burkina Faso, Maurícias, Marrocos, Senegal, Tunísia, Cabo Verde, México e Uruguai (estes três já considerados adequados)[1052]. Daí que tenha referido que o regime das transferências de dados pessoais também prossegue interesses ligados à comunidade internacional.

A intenção de atuar a estes dois níveis, intermédio e global, foi confirmada em 2010 e 2012 quando a COM expressamente assumiu o objetivo de promover níveis elevados de proteção de dados pessoais a nível mundial e autoproclamou o seu "papel motor" ou "força motriz" na promoção de "princípios universais" e no desenvolvimento de normas jurídicas internacionais em matéria de proteção de dados pessoais, executando

---

https://www.dlapiper.com/en/us/insights/publications/2017/03/proposed-amendments-nz-privacy-law/, consultado no dia 30 de setembro de 2018.

[1048] O que contrasta com o que sucedeu noutros domínios caraterizados pela utilização da "extensão territorial", como no domínio bancário e financeiro, a proprósito, por exemplo, das ANR's, v. Chistopher KUNER, "Reality and Illusion in EU Data Transfer Regulation Post Schrems", *GLJ,* n.º 18, 2017, p. 911.

[1049] Em Janeiro de 2017, v. Comissão Europeia, "Intercâmbio ..." cit., p. 2 e ss..

[1050] Whon-il PARK, "South Korea's GDPR preparation: Hurdles ahead", *PLBIR,* n.º 149, outubro de 2017, p. 23 e ss..

[1051] G. GREENLEAF, "The influence of European …" cit., p. 14.

[1052] G. GREENLEAF, "Do not dismiss …" cit., p. 16 e ss. e, do mesmo autor, "Data protection Convention 108 accession eligibility: 80 parties now possible", *PLBIR,* n.º 148, 2017, p. 12 e ss.. Para consultar os países que são parte deste diploma e os demais candidatos, v. https://www.coe.int/en/web/data-protection/convention108/parties, consultado no dia 30 de setembro de 2018.

os princípios contidos nos artigos 3.º, n.º 5 e 21.º, n.º 3, do TUE[1053]. Além da COM[1054], numa longa entrevista depois do caso *Schrems,* o Presidente do TJ, K. LENAERTS, dissipou qualquer dúvida ainda existente sobre o papel da UE na regulação desta matéria: "[a] Europa não se deve envergonhar dos seus princípios básicos e (...) se esses princípios têm efeitos internacionais, porque razão haveria a Europa de se envergonhar do seu contributo para o respeito pelos direitos fundamentais no mundo?"[1055]. No mesmo sentido se havia pronunciado o G29, em 2009[1056], bem como a AEPD[1057].

Por último, falta-me aferir a vocação extraterritorial de outro fundamento das transferências: as derrogações para situações específicas. Porém, quanto a estas, uma vez que não exigem decisão de adequação nem qualquer garantia adequada, não encontro qualquer vocação daquele teor nas situações elencadas no art. 49.º do RGPD. Como referi, não há, nestes casos, qualquer tipo de extensão da proteção do titular dos dados pessoais que resulte numa imposição no estrangeiro.

[1053] Comissão Europeia, "Uma abordagem global ..." cit., p. 5 e 18 e Comissão Europeia, "Proteção da..." cit., p. 13.
[1054] Veja-se a afirmação da Vice-Presidente da Comissão Europeia, Viviane Reding: "A atuação da Europa é decisiva para a criação de um enquadramento de proteção de dados pessoais robusto que poderá ser um modelo para o Mundo", v. "A data protection compact for Europe", 28 de janeiro de 2014, disponível em http://europa.eu/rapid/press-release_SPEECH-14-62_en.htm, consultado no dia 30 de setembro de 2018.
[1055] Valentina POPP, "ECJ President on EU Integration, Public Opinion, Safe Harbor, Antitrust", *The Wall Street Journal,* 14 de outubro de 2015, disponível em https://blogs.wsj.com/brussels/2015/10/14/ecj-president-on-eu-integration-public-opinion-safe-harbor-antitrust/, consultado no dia 30 de setembro de 2018.
[1056] G29, "The Future of Privacy Joint contribution to the Consultation of the European Commission on the legal framework for the fundamental right to protection of personal data", 1 de dezembro de 2009, disponível em https://www.garanteprivacy.it/documents/10160/10704/WP168++The+Future+of+PrivacY, consultado no dia 30 de setembro de 2018.
[1057] O presidente desta entidade referiu que "a minha esperança é que (…) seja alcançado um padrão comum, uma espécie de padrão de ouro digital, que acompanhará a globalização, todos os benefícios e desafios que a mesma coloca aos indivíduos e à sociedade", v. Giovanni BUTTARELLI, "The EU GDPR as a clarion call for a new global digital gold standard", *IDPL,* vol. 6, n.º 2, p. 77.

Síntese conclusiva

1. As *fontes* do regime geral de proteção de dados pessoais encontram-se, sobretudo, no direito derivado e no direito originário: quanto ao primeiro, a evolução é evidente com a adoção de um novo ato legislativo, o RGPD, e a revogação da Diretiva 95/46; quanto ao segundo, a consagração no TFUE e na CDFUE de um direito fundamental sedimentou uma dimensão jusfundamental deste regime que acresce a outra, de natureza económica ou integracionista, e que tem em vista a criação do mercado único digital dentro da UE. Examinei estas fontes, por um lado, para estudar a *natureza* deste regime (1.1.) e, por outro, para mapear as suas *caraterísticas* distintivas (1.2.).

   1.1. Em relação ao primeiro aspeto, verifiquei que este regime não cabe na divisão clássica entre Direito Público/Direito Privado e sugeri um ângulo de estudo segundo o conceito de "regulação". Com efeito, de forma inequívoca, o RGPD reflete uma intervenção legislativa sobre as atividades de tratamento de dados pessoais, do setor público e privado, tendo em vista uma proteção ótima do titular dos dados pessoais, através da imposição de condições àquelas atividades. Adicionalmente, como referi, esse tipo de intervenção prossegue com o recurso à chamada "co-regulação" ou "auto-regulação publicamente regulada" e segundo uma estratégia de prevenção de riscos.

   1.2. No que respeita às *caraterísticas* distintivas deste bloco de normas, conclui que o seu âmbito de aplicação é alargado por força de dois elementos: um elemento subjetivo, isto é, dos sujeitos das relações jurídicas no âmbito do tratamento de dados pessoais, determinado com recurso a conceitos autónomos e funcionais e, por isso, indiferente à natureza (pública ou privada) do sujeito; um elemento objetivo, conexo com o objeto regulatório, assente em conceitos também eles amplos por opção legislativa, sancionada em decisões do TJ (como o caso *Google Spain*). A outra caraterística distintiva deste regime é a imposição para os utilizadores de dados pessoais de um conjunto de princípios e obrigações e o reconhecimento de uma cartilha de direitos do titular dos dados pessoais.

2. Tendo em conta a linguagem e os critérios específicos usados para delimitar o âmbito de aplicação deste regime no art. 4.º da Diretiva poderia não ser evidente, logo em 1995, a pretensão de o legislador regular os tratamentos de dados pessoais de um utilizador de dados pessoais situado fora do território da UE. Contudo, a jurisprudência do TJ tornou inequívoca essa intenção, munindo-se de uma interpretação teleológica, centrada na maximização da proteção do titular dos dados pessoais, e numa "proibição de interpretação restritiva" do âmbito de aplicação da Diretiva. Por conseguinte, essa opção legislativa pela extraterritorialidade persiste no RGPD apesar das novidades inscritas no art. 3.º.

3. O critério central, tanto na Diretiva como no RGPD, para determinar o respetivo âmbito de aplicação é a existência (ou não) de um estabelecimento do utilizador de dados pessoais no território da UE. De facto, o que importa apurar não é a sua nacionalidade, o local da sede social estatutária ou a sua residência fiscal mas, isso sim, verificar se tem um estabelecimento, seja principal ou secundário, no território de um Estado-Membro[1058.] Este é o primeiro passo de um teste complexo e com várias etapas. Com efeito, existindo um estabelecimento, haverá que avaliar se os tratamentos de dados pessoais ocorrem no "contexto das atividades" daquele estabelecimento. Não existindo estabelecimento, o RGPD prevê um novo critério: a localização geográfica dos titulares dos dados pessoais no território da União. Assim, não é rigoroso afirmar que o regime estudado se aplica apenas a empresas nacionais de Estados-Membros ou, como sugerem alguns autores[1059,] que protege apenas residentes ou nacionais em/de Estados-Membros da UE.

4. Da aplicação deste teste podem resultar "implicações jurídicas que se estendem para lá do território da UE"[1060] ou, melhor, a tentativa de regular os tratamentos de dados pessoais realizados por utilizadores de dados pessoais situados além das fronteiras da UE em duas situações:

[1058] Ulrich DAMMANN e Spiros SIMITIS, *EG-Datenschutzrichtlinie Kommentar,* Nomos, 1997, p. 127. Entre nós, A. GONÇALVES, "A privacidade ..." cit., p. 16.
[1059] M. BRKAN, "The Unstoppable …" cit., p. 834.
[1060] G29, "Parecer 8/2010 ..." p. 10.

4.1. Quando o tratamento é indissociável das atividades de um estabelecimento situado no território da UE;

4.2. Quando não exista um estabelecimento, mas o tratamento tem outra conexão com o território da UE: ou porque ali se situam os "meios" usados para a sua recolha, ou porque os tratamentos visam titulares dos dados que ali se encontram;

5. Os *interesses* prosseguidos pelo legislador com a jurisdição extraterritorial são duplos: o cumprimento do dever de proteger o titular dos dados pessoais de ingerências estrangeiras aos seus direitos fundamentais e a criação de condições de igualdade de concorrência entre as empresas europeias e estrangeiras.

6. Quanto aos *princípios* que fundamentam a assunção de jurisdição extraterritorial da UE julgo, em primeiro lugar, que o legislador se preocupou em encontrar uma ligação relevante entre o tratamento de dados pessoais regulado e o território da UE, em coerência com a regra da intransitividade. Por outro lado, os "elos" que firmam as prescrições da UE são ainda *territoriais*, rejeitando-se o princípio da nacionalidade tanto do titular dos dados como do utilizador dos dados pessoais, bem como uma manifestação de territorialidade alternativa que seria a localização física dos dados pessoais[1061]. Não obstante, nota-se uma tendência de desapego à territorialidade, visível na interpretação flexível do conceito de "estabelecimento", vertida na jurisprudência do TJ e descrita na ideia de "territorialidade limitada" ou "virtual"[1062]. O mesmo vale para a aplicação da doutrina dos efeitos, subjacente ao art. 3.º, n.º 2, já que os efeitos ou, melhor, os *riscos* do tratamento afetam um titular dos dados pessoais que se encontra no território da UE.

7. Em relação a este novo critério, que adota o lema *if you target data subjects who are in the EU then the Regulation reaches out to you*[1063], creio que o mesmo reflete uma boa dose de razoabilidade e de moderação na assunção de jurisdição pela UE. Por outro lado, uma vez que esta solução tem em vista, sobretudo, os tratamentos de

[1061] *Idem*, p. 9.
[1062] L. MOEREL, "The long …" cit., p. 29; M. GOMANN, "The new territorial …" cit., p. 571 e P. de HERT e M. CZERNIAWSKI, "Expanding the …" cit., p. 234 e 236.
[1063] P. de HERT e M. CZERNIAWSKI, "Expanding the …" cit., p. 242.

dados pessoais à distância permitidos pela Internet, deve ser enquadrada numa tendência de regulação daquele espaço sem fronteiras que, como referi na Parte I, rejeita territorialismos para firmar a assunção jurisdição e se vai abrindo a outros princípios, como a doutrina dos efeitos. No mesmo sentido segue a redação dada ao art. 3.º, n.º 1, da Convenção n.º 108 do CdE, que abdica do critério do território, presente na redação original, passando a dispor que "[c]ada Parte se compromete a aplicar a Convenção *aos tratamentos de dados pessoais sujeitos à sua jurisdição*, realizados no setor público ou privado, assim garantindo a cada indivíduo o direito à proteção dos dados pessoais"[1064]. A Convenção não especifica o conceito de "jurisdição", nem delimita o seu âmbito, deixando em aberto os termos da jurisdição extraterritorial de cada Parte.

8. A vocação extraterritorial do regime das transferências de dados pessoais para países terceiros não é evidente pois não decorre imediatamente da letra da lei ou de um princípio de jurisdição extraterritorial. Defendo que a vocação extraterritorial deste regime resulta das condições impostas à realização de transferências, isto é, dos fundamentos das mesmas. De uma banda, as garantias suficientes ou adequadas são o veículo de uma tentativa de regular os tratamentos de dados efetuados pelo importador dos dados pessoais. De outra banda, o procedimento de apreciação da adequação do país terceiro é uma concretização da técnica da extensão territorial no domínio da proteção de dados pessoais com implicações demonstradas nos países terceiros.

9. Através da mesma, muito mais do que regular este ou aquele tratamento de dados pessoais, a UE assumiu um papel significativo no curso da evolução mundial da regulação desta matéria, promovendo o direito fundamental à proteção de dados pessoais ao mesmo tempo que procura facilitar a sua circulação internacional, incentivar a interoperabilidade entre ordenamentos jurídicos e o desenvolvimento do DIP com mais adesões à Convenção n.º 108 do CdE. Há quem veja este posicionamento da UE como reflexo de uma pretensão mais ampla de moldar e regular o ciberespaço e os direitos fundamentais no ambiente digital, colocando em segundo plano a influência dos EUA e isolando os países que não adotam o "modelo

[1064] *Idem*, p. 231 e ss..

europeu" como é o caso daquele e da China[1065]. Seja como for, de saída da presidência do G29, Isabelle FALQUE-PIERROTIN alertou que um dos grandes desafios do RGPD é "influenciar potências estrangeiras a atualizar os seus padrões de proteção de dados através da ferramenta conhecida como "decisão de adequação". [1066] Com efeito, se o tratamento de dados pessoais é, cada vez mais, um fenómeno mundial, a sua proteção também o deverá ser[1067].

10. Os interesses prosseguidos por este *controlo de fronteira* dos dados pessoais são:

    10.1. Interesses internos, de proteção do titular dos dados pessoais das ingerências aos seus direitos fundamentais quando os seus dados são transferidos; e

    10.2. Interesses externos, da comunidade internacional e do desenvolvimento do DIP, em especial da Convenção n.º 108 do CdE.

11. Em último lugar, as normas que delimitam o âmbito de aplicação deste regime e as normas aplicaveis às transferências de dados pessoais, estrutural e formalmente distintas, arrumadas em capítulos diferentes, ao ampliarem a aplicação deste bloco de normas para fora do território da UE, prosseguem pelo menos um interesse em comum: a proteção do titular dos dados pessoais das ingerências dos utilizadores de dados pessoais que tenham estabelecimento na UE (art. 3.º, n.º 1), dos que não o têm (art. 3.º, n.º 2) ou, então, dos que tratam os dados pessoais na condição de importadores dos mesmos[1068].

[1065] C. KUNER, "The Internet and ..." cit., p. 15; G. GREENLEAF, *Asian Data Privacy,* cit., p. 8 e Nicola LUGARESI, "Internet Law Trends in Europe: A Case Law Perspective", *Revista da Faculdade de Direito da UFMG*, n.º especial – 2nd Conference Brazil-Italy, 2017, p. 305 e ss.; P. SCHWARTZ, "The EU-U.S. …" cit., p. 1966.

[1066] "Europe's data protection chief signs off, with a warning", *Politico*, 7 de feveiro de 2017, disponível em https://www-politico-eu.cdn.ampproject.org/c/s/www.politico.eu/article/isabelle-falque-pierrotin-europe-data-protection-chief-signs-off-with-a-warning/amp/, consultado no dia 30 de setembro de 2018.

[1067] Comissão Europeia, "Uma abordagem ..." cit., p. 18.

[1068] Em sentido próximo, v. Cécile de TERWAGNE e Sophie LOUVEAUX, "Data Protection and Online Networks", *CLSR,* n.º 13, 1997, p. 234; C. KUNER, *Transborder* cit., p. 121, 126 e 128; K. HON, *Data Localization* cit., p. 54; P. de HERT e M. CZERNIAWSKI, "Expanding the …" cit., p. 235.

Parte III – Limites à extraterritorialidade do regime geral de proteção de dados pessoais da UE

Nesta última Parte proponho-me identificar os limites à ampliação deste conjunto de normas aos tratamentos de dados pessoais realizados fora do território da UE e discutir mecanismos para contornar esses limites.

Este exercício é relevante à luz de afirmações do G29, como a de que "as regras relativas à proteção dos dados só podem contribuir para a proteção das pessoas se forem respeitadas na prática"[1069]. Também no caso *Google Spain,* o TJ repetiu a necessidade de enfatizar uma proteção "completa e efetiva" das pessoas singulares[1070]. A doutrina alerta para uma "crise de credibilidade"[1071] ou, dito de outro modo, "o direito da proteção de dados tem sido atormentado por desenvolvimentos que colocam em questão a capacidade do mesmo para garantir uma proteção eficaz dos direitos fundamentais"[1072]. De igual modo, o problema do "cumprimento da legislação de proteção de dados" e a questão do "controlo da sua execução" há muito que foram diagnosticados pela COM[1073]. Serão, por exemplo, as regras das transferências de dados pessoais "respeitadas na prática"? E o âmbito de aplicação deste regime é suficientemente claro para assegurar uma proteção "completa e eficaz" do titular dos dados?

Respostas negativas a estas inquirições poderão resultar num diagnóstico pessimista sobre o fosso entre a lei no papel e a realidade da sua (não) execução que, levado ao limite, coloca em causa a utilidade da extraterritorialidade enquanto instrumento normativo que verdadeiramente adere à realidade, segundo critérios que medem a sua capacidade real para atingir um resultado, bem como a sua adequação enquanto instrumento de proteção de bens jusfundamentais. Ou, como já se escreveu, a

[1069] G29, "Documento de trabalho. Transferência ..." cit., p. 5.
[1070] Acórdão do TJ, Google Spain SL e Google Inc. c. Agencia Española de Protección de Datos (AEPD) e Mario Costeja González*,* C-131/12, 13 de maio de 2014, n.º 58.
[1071] C. KUNER *et alii*, "The Data Protection Credibility Crisis", *IDPL,* vol. 5, n.º 3, 2015, p. 161 e ss..
[1072] C. KUNER, "Extraterritoriality …" cit., p. 242.
[1073] Comissão Europeia, "Primeiro relatório ..." cit., p. 12 e 13 e Comissão Europeia, "Impact Assessment Accompanying the document Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) and Directive of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data", 25 de janeiro de 2012, p. 17.

extraterritorialidade "ladra" sem "morder" e não será mais do que um híper garantismo ingénuo ou utópico[1074].

O efeito pernicioso deste diagnóstico é uma incongruência entre as promessas constitucionais da UE, de tutela de "todas as pessoas singulares" (art. 8.º da CDFUE e art. 16.º do TFUE), e as suas concretizações na realidade, acompanhada da frustração de expectativas dos indivíduos. Como salientou o ICO, a proclamação do legislador em relação a um utilizador de dados pessoais não estabelecido na UE poderá pecar por falta de realismo e induzir os consumidores europeus em erro ao prometer um grau de proteção que não é capaz de garantir[1075]. Em causa está também, como bem observa D. SVANTESSON, a credibilidade deste regime[1076].

Assim, começarei por explicar os limites à aplicação deste bloco de normas segundo o art. 4.º da Diretiva e o art. 3.º do RGPD (Capítulo 1). Tratarei, sobretudo, a fiscalização dos tratamentos de dados pessoais abrangidos pelo art. 3.º, n.º 2 do RGPD (1.1). Além disto, recordando as conclusões da Parte I, o risco de adoção de reações negativas pela entidade *ad quem*, em especial medidas de bloqueamento (1.2), não deve ser excluído nem mesmo o surgimento de conflitos de jurisdição (1.3). Em quarto lugar, tanto o art. 4.º da Diretiva como o art. 3.º do RGPD recorrem a conceitos indeterminados e autónomos cuja concretização é complexa e dificulta a previsibilidade do direito a aplicar (1.4).

Seguindo para o regime das transferências no Capítulo 2 trato, em primeiro lugar, do problema da definição do conceito de "transferência", fonte de divergências interpretativas e de insegurança para os agentes económicos (2.1). Igualmente imprecisa é a relação entre a regulação das transferências de dados pessoais e o âmbito de aplicação segundo o art. 4.º da Diretiva e o art. 3.º do RGPD (2.2). Os últimos pontos incidem sobre a (in) eficácia do regime das transferências de dados pessoais, um tema incontornável no contexto da decisão *Schrems* (2.3), as insuficiências dos fundamentos das transferências (2.4) e, finalmente, o anacronismo de uma "restrição" à circulação dos dados pessoais na atualidade tecnológica (2.5).

À medida que vou enunciando todos estes limites equaciono soluções para os abreviar, explorando a viabilidade daquelas que se encontram no RGPD e de outras a ponderar a longo prazo e que, a meu ver, merecem ser equacionadas tanto pela COM

[1074] D. SVANTESSON, *Extraterritoriality* cit., p. 68 e ss..
[1075] ICO, "Initial Analysis of …" cit., p. 5.
[1076] D. SVANTESSON e R. POLCAK, *Information Sovereignty…* cit., p. 222.

quando, nos termos do art. 97.º do RGPD, levar a cabo uma revisão do mesmo, como pelo CEPD no seu trabalho de orientação pedagógica.

Capítulo 1- Os limites ao âmbito de aplicação segundo o art. 4.º da Diretiva e o art. 3.º do RGPD

1.1.A fiscalização dos tratamentos de dados pessoais abrangidos pelo art. 3.º, n.º 2 do RGPD

A natureza meramente simbólica da extraterritorialidade deste regime é apontada pela doutrina, pelas autoridades de controlo e percecionada pelos operadores económicos[1077]. Acontece que este problema não é exclusivo do bloco normativo em apreço: suscita-se a propósito de toda a regulação com vocação extraterritorial atenta a incapacidade da entidade do foro executar os seus comandos em território estrangeiro. A esta conclusão chegam, por exemplo, as autoridades de outros países a propósito da proteção de dados pessoais[1078] bem como a doutrina a propósito da jurisdição extraterritorial na Internet[1079].

Identificar as especificidades de que se reveste este problema no regime em apreço (1.1.1) e equacionar soluções para o mesmo (1.1.2) são as metas dos pontos seguintes.

[1077] Bernhard MAIER, "How Has the Law Attempted to Tackle the Borderless Nature of the Internet?", *IJLIT*, vol. 18, n.º 2, 2010, p. 161; Christopher KUNER, "Data Protection Law and International Jurisdiction on the Internet (Part 2)", *IJLIT,* vol. 18, n.º 3, p. 235; C. REED, *Making Laws* p. 49 e 366; D. SVANTESSON, "Enforcing Privacy across different jurisdictions", David WRIGHT e Paul de HERT (eds.), *Enforcing privacy: regulatory, legal and technological approaches,* Springer, 2016, p. 201 e, do mesmo autor, *Extraterritoriality* cit., p. 68; ICO, "Initial Analysis …" cit., p. 5; J. GOLDSMITH e T. WU, *Who controls* cit., p. 156 e ss.; L. BYGRAVE, "Determining …" cit., p. 252; M. LOKKE, "The long arm …" cit., p. 28 e ss.; M. GOMANN, "The new territorial …" cit., p. 569; P. de HERT e M. CZERNIAWSKI, "Expanding the …" cit., p. 240.

[1078] Ao apresentar a extraterritorialidade do *Personal Data Protection Act 2012*, o Ministro da Informação, das Comunicações e das Artes de Singapura afirmava estar "consciente dos desafios da sua implementação. Em particular, quando as organizações em causa não tenham qualquer presença em Singapura, será difícil realizar investigações na sequência de reclamações em relação às atividades dessas organizações ou proceder a uma ação de execução contra as mesmas (...)", v. "Public Consultation Issued by Ministry of Information, Communications and the Arts – Proposed Personal Data Protection Bill", 19 de março de 2012, disponível em https://www.imda.gov.sg/regulations-licensing-and-consultations/consultations/consultation%20papers/2012/public-consultation-by-mica-on-proposed-personal-data-protection-bill-for-singapore, consultado no dia 30 de setembro de 2018.

[1079] D. SVANTESSON, *Solving* cit., p. 132 e F. MEDEIROS e L. BYGRAVE, "Brazil's Marco …" cit., p. 127 e ss..

1.1.1. A falta de meios e as duas "velocidades" da jurisdição extraterritorial

O G29 reconheceu que a opção pela ampliação extraterritorial deste conjunto de normas foi prosseguida com consciência "das dificuldades intrínsecas de aplicação ligadas à situação transfronteiriça em questão"[1080], sublinhou que a "aplicação de regras num contexto internacional não é tão fácil como dentro de um país"[1081] e que a "localização física dos dados pessoais em países terceiros dificulta a aplicação do DUE e o cumprimento das funções das autoridades nacionais de controlo"[1082]. Estas observações foram acompanhadas por alertas da doutrina sobre a divergência entre o âmbito de aplicação extraterritorial deste regime e as possibilidades da sua garantia[1083]. Até o TJ, no caso *Digital Rights Ireland,* afirmou, quanto aos tratamentos de dados pessoais fora do território da UE, que "não se pode considerar que esteja plenamente garantida a fiscalização, por parte de uma entidade independente"[1084].

O culminar destas constatações encontra-se na avaliação de impacto que acompanha o RGPD: "mesmo quando parte do equipamento usado para o tratamento está situada dentro da UE, as autoridades dali, em regra, não têm meios para executar as suas decisões ou sanções em relação a entidades cujo estabelecimento principal se encontra fora da sua jurisdição territorial"[1085]. Se, como se reconhece neste trecho, há um esvaziamento dos poderes das autoridades de controlo quando o estabelecimento principal está no território de um país terceiro, o que dizer quando não há sequer um estabelecimento secundário no território da UE, como sucede nas situações do art. 3.º, n.º 2, do RGPD?

São essencialmente dois os fatores na origem deste esvaziamento. Em primeiro lugar, o desempenho dos poderes das autoridades de controlo *dentro* e *fora* da UE é prejudicado

[1080] G29, "Documento de trabalho ..." cit., p. 3.
[1081] *Idem*, p.15.
[1082] G29, "Parecer 7/2001 sobre o projeto de decisão da Comissão (versão de 31 de Agosto de 2001) relativa às cláusulas contratuais-tipo aplicáveis à transferência de dados pessoais para subcontratantes estabelecidos em países terceiros, em conformidade com o n.º 4 do artigo 26.º da Diretiva 95/46/CE", 13 de setembro de 2001, p. 3.
[1083] B. MAIER, "How Has …" cit., p. 161 e ss.; C. KUNER, "Data Protection Law and (Part 2) …" cit., p. 234 e ss.; C. REED, *Making Laws* cit., p. 49; D. SVANTESSON, *Solving* cit., p. 132 e ss.; Lee BYGRAVE, "Data Privacy Law and the Internet: Policy Challenges", Norman WITZLEB *et alii, Emerging Challenges in Privacy Law: Comparative Perspective,* Cambridge University Press, 2014, p. 277; L. MOEREL, "The Long …" cit., p. 23 e ss.; Market TRIMBLE, "Advancing National Intellectual Property Policies in a Transnational Context", *MLR*, n.º 74, 2014, p. 203 e ss.; R. POLCAK e D. SVANTESSON, *Information Sovereignty,* cit., p. 218.
[1084] Acórdão do TJ, Digital Rights Ireland *et alii* c. Minister for Communications, Marine and Natural Resources *et alii,* C-293/12, 8 de abril de 2014, n.º 68.
[1085] Comissão Europeia, "Impact Assessment …" cit., p. 24 e 25.

pela escassez de recursos, financeiros e humanos[1086]. No relatório da COM, de 2003, sobre a implementação da Diretiva, constatou-se, *inter alia,* (i) que os recursos alocados ao controlo da execução das normas são insuficientes e as ações coercitivas têm uma prioridade baixa entre as muitas tarefas destas autoridades; e (ii) o cumprimento fragmentário das regras por parte dos responsáveis pelo tratamento e dos subcontratantes quando o risco de penalização pelo incumprimento é reduzido[1087]. Mais recentemente a situação foi confirmada pela Agência Europeia de Direitos Fundamentais, em 2010, concluindo que 11 das 27 autoridades não são capazes de desempenhar a totalidade das suas tarefas ou exercer todos os seus poderes[1088]. Portugal não é exceção[1089]. Alguns autores alertam que esta situação fomenta uma fiscalização seletiva e discricionária, em prejuízo da legitimidade da mesma e, adicionalmente, estimula o *forum shopping*[1090].

Em segundo lugar, recorde-se o problema das duas "velocidades" que perpassa a prática da extraterritorialidade: o alargamento dos domínios em que os Estados exercem jurisdição *prescritiva* fora de portas não foi acompanhado por uma tendência equivalente ao nível da jurisdição de *execução*. Ora, o expoente máximo desta discrepância vislumbra-se no RGPD, designadamente atendendo à vocação *extraterritorial* do art. 3.º, n.º 2, por contraste com a *territorialidade* dos poderes das autoridades de controlo plasmada no art. 55.º[1091]. O paradoxo confirma-se no considerando 122 do RGPD: "as autoridades de controlo deverão ser competentes no *território* do respetivo Estado-Membro", mas essas competências incluem o tratamento de dados que "afete os titulares dos dados no seu território" e "o tratamento de dados efetuado por um responsável pelo

---

[1086] C. KUNER, *Transborder* cit., p. 145; David WRIGHT, "Enforcing Privacy", D. WRIGHT e P. DE HERT, (eds.), *Enforcing Privacy* cit., p. 13 e ss.; D. SVANTESSON, "Enforcing Privacy …" cit., p. 201; K. HON, *Data Localization* cit., p. 239 e ss.; L. BYGRAVE, *Data Privacy* cit., p. 189; Omar TENE, "For Privacy, European Commission must be innovative", *Center for Democracy & Technology,* 2011, disponível em https://cdt.org/blog/for-privacy-european-commission-must-be-innovative/, consultado no dia 30 de setembro de 2018; Philip SCHUTZ, "The Set Up of Data Protection Authorities as a New Regulatory Approach", Serge GUTWIRTH *et alii* (eds.), *European Data Protection: In Good Health?,* Springer, p. 29.

[1087] Comissão Europeia, "Primeiro relatório ..." cit., p. 12 e 13.

[1088] AEDF, "Data Protection in the European Union: The Role of National Data Protection Authorities", 2010, disponível em http://fra.europa.eu/sites/default/files/fra_uploads/815-Data-protection_en.pdf, consultado no dia 30 de setembro de 2018.

[1089] "Proteção de dados sem meios para cumprir regulamento europeu a partir de maio", *TSF,* de 12 de janeiro de 2018, disponível em https://www.tsf.pt/lusa/interior/protecao-de-dados-sem-meios-para-cumprir-regulamento-europeu-a-partir-de-maio-9043625.html, consultado no dia 30 de setembro de 2018.

[1090] D. SVANTESSON e R. POLCAK, *Information Sovereignty* cit., p. 221. Destaco o alerta sobre o fenómeno do *fórum shopping* do presidente da autoridade de proteção de dados de Berlim, v. Alexander DIX, "The International Working Group on Data Protection in Telecommunications: Contributions to Transnational Privacy Enforcement", D. WRIGHT e P. DE HERT, (eds.), *Enforcing Privacy* cit., p. 190.

[1091] Onde se pode ler, no n.º 1, "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".

tratamento ou subcontratante não estabelecido na União". Por conseguinte, estas autoridades deverão, a partir do próprio território, fiscalizar tratamentos de dados pessoais ocorridos fora dali e realizados por agentes económicos sem conexão territorial expressiva (isto é, sem estabelecimento). O mesmo entendimento territorial quanto aos poderes destas autoridades vigora noutras latitudes, como no Canadá[1092].

A territorialidade dos poderes das autoridades de controlo coloca-lhes um travão, em particular em relação a deslocações daquelas ao território estrangeiro como é suposto, por exemplo, para a realização de auditorias, o acesso aos dados pessoais e às instalações do utilizador de dados pessoais sem estabelecimento no Estado-Membro [1093]. Esta será uma limitação consentânea com o entendimento tradicional na doutrina sobre a realização de "atos reais transnacionais" ou "atos reais informativos", isto é, diligências procedimentais e preparatórias levadas a cabo pelas autoridades administrativas de um país com vista à obtenção de prova em território estrangeiro, designadamente a recolha de documentos ou de informações[1094].

Não obstante, estas atuações extraterritoriais podem ser enquadradas normativamente numa convenção internacional ou com a obtenção de consentimento prévio da entidade *ad quem* [1095]. Como refere M. PRATA ROQUE, os "limites da atuação extraterritorial de órgãos administrativos encontram-se diretamente dependentes do grau de integração internacional a que cada Estado se comprometeu. Como tal, quanto maior for essa integração num "*sistema administrativo global em rede"* – seja por via da pertença a uma "*organização internacional"* ou a qualquer outro mecanismo de atuação transnacional, seja por via da vinculação a deveres jurídicos decorrentes de uma convenção internacional –, maior será a disponibilidade de cada Estado para aceitar o exercício de "*competência transnacional"* por órgãos administrativos estrangeiros"[1096].

[1092] O *Privacy Commissioner* viu-se na obrigação de rejeitar a investigação de uma queixa contra uma empresa norte-americana por entender não ter jurisdição para exercer os seus poderes em relação àquela empresa o que, posteriormente, foi confirmado por uma decisão do Tribunal Federal (*Lawson v Accusearch Inc.)* determinando que a autoridade canadiana não poderia entrar nas instalações de uma empresa norte-americana, no *Wyoming* (EUA), durante a investigação realizada na sequência de uma queixa de um cidadão Canadiano. Não obstante, o tribunal canadiano entendeu que o *Privacy Commissioner* devia exercer os seus poderes de investigação se o pudesse fazer sem aceder às instalações daquela empresa situada nos EUA, v. Office of the Privacy Commissioner of Canada, "Reaching for the Cloud(s): Privacy Issues related to Cloud Computing", março de 2010, disponível em https://www.priv.gc.ca/en/opc-actions-and-decisions/research/explore-privacy-research/2010/cc_201003/#fn23-rf, consultado no dia 30 de setembro de 2018.

[1093] Art. 58.º, n.º 1, al. b), e) e f), do RGPD.

[1094] D. LOPES, *Eficácia* cit., p. 241 e M. Prata ROQUE, *A Dimensão* cit., p. 1147.

[1095] D. LOPES, *Eficácia* cit., p. 241.

[1096] M. Prata ROQUE, *A Dimensão* cit., p. 1133.

Nesse sentido, adquire particular relevo o art. 50.º, al. b), do RGPD, e a aposta na cooperação internacional desde o momento da investigação.

Por outro lado, será que o exercício de todos os poderes é territorialmente limitado? É que a cartilha de poderes aqui em causa não se resume aos "atos reais transnacionais": incluem-se ali poderes de correção, autorização e consulta. O que se pergunta, então, é o seguinte: pode uma autoridade de controlo notificar uma loja *online*, estabelecida no estrangeiro e não na UE, das alegadas violações do RGPD[1097]? Poderá dirigir-lhe uma advertência ou impor uma coima?[1098] O legislador entendeu que sim. Com efeito, segundo o art. 83.º, n.º 4, al. a), do RGPD, as autoridades de controlo gozam de poderes sancionatórios alargados a utilizadores de dados pessoais sem estabelecimento na UE[1099]. No passado, o G29 havia já sugerido que, quando um titular dos dados da UE "tenha problemas com um site não europeu" e apresentar uma reclamação à autoridade de controlo, esta "poderá estabelecer contacto com o site estrangeiro a fim de resolver o problema"[1100].

A meu ver, as atuações e decisões que não caibam no conceito de "atos reais transnacionais" consubstanciam um "exercício de poderes no território do Estado-Membro", conforme com o critério do art. 55.º do RGPD, aproximando-se substancialmente da categoria da jurisdição prescritiva ou adjudicativa e afastando-se dos contornos da jurisdição de execução[1101]. As mesmas correspondem a decisões adotadas a partir do território onde se situa a autoridade de controlo, pelo que não há um exercício, efetivo e corpóreo de poderes coercivos, tal como não há um automatismo da coercividade das mesmas, nem da sua produção de efeitos extraterritoriais, que se concretizam com a execução das mesmas no território da entidade do foro ou, em alternativa, com a colaboração da entidade *ad quem,* através de instrumentos de reconhecimento e de execução do direito estrangeiro e da disponibilização dos seus meios coercivos ao serviço dos interesses do foro. Como refere M. PRATA ROQUE, "a mera tomada de decisões administrativas que visem produzir efeitos extraterritoriais (sem que o tenha, ainda, logrado fazer), mesmo que desfavoráveis ao administrado (...) não pode ser interpretada como uma interferência ilegítima em território estrangeiro" por duas

[1097] Art. 58, n.º 1, al. d), do RGPD.
[1098] Art 58.º, n.º 2, alíneas a) e i), do RGPD.
[1099] Quando, por exemplo, não respeitam a obrigação de designar um representante para a UE segundo o art. 27.º do RGPD.
[1100] G29, "Documento de trabalho ..." cit., p. 16.
[1101] Em sentido próximo, sobre os poderes das autoridades administrativas, v. Brigitte STERN, "Quelques Observations ..." cit., p. 14 e ss..

razões: primeiro, o destinatário pode voluntariamente conformar-se com o cumprimento da decisão e, segundo, porque a entidade *ad quem* pode colocar os seus meios coercivos ao serviço da execução da decisão estrangeira[1102]. Acresce que, como defendem alguns autores, é duvidosa a existência de uma "ingerência nos assuntos internos" da entidade *ad quem* se a decisão for comunicada à distância, por exemplo, por correio eletrónico[1103].

Por conseguinte, a territorialidade dos poderes das autoridades de controlo não significa, necessariamente, uma incapacidade paralisante para fiscalizar os tratamentos do art. 3.º, n.º 2, do RGPD. Nesse sentido veja-se, por exemplo, a recente notificação do ICO a uma empresa do Canadá[1104]. Porém, como referi, poderá ser necessária a colaboração dos países terceiros. Mas como se processa essa colaboração? E será possível (e como) potenciar as promessas da extraterritorialidade prescritiva *além* dessa colaboração?

Responder a estas questões exige, antes de mais, a cautela do jurista que não está em posição para solucionar os constrangimentos de origem financeira que afetam a efetividade deste bloco de normas e que se refletem no dia-a-dia das autoridades de controlo. Disso depende não só extraterritorialidade como, de resto, a efetividade da proteção de dados pessoais em geral que, enquanto direito fundamental, se encontra sujeito à "reserva do financeiramente possível"[1105]. Esta circunstância vem refletida na confissão do G29 de que a fiscalização dos tratamentos total ou parcialmente ocorridos fora da UE apenas se verifique nos casos em que "é necessário, em que faz sentido e em que existe um nível razoável de capacidade de aplicação, tendo em conta a situação transfronteiriça envolvida"[1106]. Do mesmo modo, há que ter presente que nenhuma pretensão de tutela preventiva de riscos *transnacionais* assegura uma garantia de

[1102] M. Prata ROQUE, *A Dimensão* cit., p. 1148.
[1103] Esta é a posição de M. Prata ROQUE, *A Dimensão* cit., p. 1142 e ss.. Em sentido próximo, Pieter KUYPER admite, por exemplo, a realização de notificações a destinatários situados em território estrangeiro, com base na prática dos Estados, de permitir o envio através de correio normal, sem prejuízo do direito de objeção a essa prática do Estado *ad quem,* v. "European Community Law and Extraterritoriality: some Trends and New Developments", *ICLQ*, vol. 33, parte 4, outubro de 1984, p. 1018 e ss.. Outros autores consideram que as notificações do Estado do foro destinadas a um sujeito situado no território do Estado *ad quem* são proibidas por violarem o princípio da soberania do Estado, v. D. LOPES, *Eficácia* cit., p. 242.
[1104] ICO, "Enforcement Notice", 6 de julho de 2018, disponível online em https://ico.org.uk/media/action-weve-taken/enforcement-notices/2260123/aggregate-iq-en-20181024.pdf , consultado no dia 30 de setembro de 2018.
[1105] J. Pereira da SILVA, *Deveres,* cit., p. 578.
[1106] G29, "Documento de trabalho sobre a determinação da aplicação internacional da legislação da UE em matéria de proteção de dados ao tratamento de dados pessoais na Internet efetuado por sites não-europeus", adotado no dia 20 de maio de 2002, p. 10 e 15.

resultados de proteção plena ou um risco-zero[1107]. Por conseguinte, a fiscalização daqueles tratamentos encontra-se sujeita a uma genérica reserva de garantia do possível.

A esta conclusão não se deve seguir, imediatamente, um desvalor sobre a extraterritorialidade e, em especial, sobre a sua utilidade para prosseguir os interesses do titular dos dados pessoais. Uma apreciação sobre a mesma tendo por base um critério de *garantia* do direito associado à coercibilidade, ao uso legítimo da coação, da força (exclusivo e monopolizado pelo Estado) ou do aparelho estadual excluiria certos efeitos daquela, de influenciar comportamentos de países terceiros e de empresas transnacionais. Quanto a estas, a motivação para a aceitação da vinculatividade do direito estrangeiro não se confunde, necessariamente, com o risco de sancionamento pela entidade do foro[1108]. Paralelamente, não são de descurar certos efeitos da extensão além-fronteiras de normas, como de *deterrence*[1109]*,* nem mesmo a intenção de sinalizar à comunidade internacional a posição da UE numa matéria em que o DIP se mostra (ainda) insuficiente[1110]. Como expliquei, certas caraterísticas específicas da UE, políticas e económicas, potenciam a efetividade da extraterritorialidade enquanto processo motivacional e instrumento para influenciar comportamentos[1111].

Em todo o caso, como demonstro nos pontos que se seguem, há mecanismos que incrementam a possibilidade de garantir a conformidade dos tratamentos de dados pessoais abrangidos pelo art. 3.º, n.º 2.

[1107] J. Pereira da SILVA, *Deveres,* cit., p. 292: "num mundo de ameaças transnacionais e crescentemente globalizadas, seria contraditório confinar dogmaticamente a figura dos deveres de proteção ao plano interno estadual, a pretexto de uma pretensa plenitude de proteção que só aí poderia ser alcançada.

[1108] A. Santos CAMPOS, *Glosas* cit., p. 318. Um exemplo do que se diz verifica-se em relação a um conjunto de sítios em linha norte-americanos que, enquanto se encontram a adaptar ao RGPD, bloqueram o respetivo acesso a utilizadores situados no território da União, v. BBC, "US news sites unavailable to EU users under new rules", 25 de maio de 2018, disponível em https://www.bbc.com/news/world-europe-44248448, consultado no dia 30 de setembro de 2018.

[1109] Foi este o argumento invocado, em Singapura, aquando da discussão da amplitude do *Personal Data Protection Act* 2012 (PDPA) em relação a empresas estrangeiras: "a extraterritorialidade atua como instrumento de dissuasão para empresas situadas fora do nosso território atuarem em violação do PDPA". Em sentido próximo, U. KOHL refere o "receio de sanções" (U. KOHL, *Jurisdiction and the* cit., p. 205) e D. SVANTESSON sublinha que, num enquadramento pós-positivista, que uma pretensão regulatória pode ter valor mesmo sem ser executada na prática, sobretudo quando é moralmente justificada v. D. SVANTESSON, *Extraterritoriality* cit., p. 71.

[1110] C. KUNER, *Transborder* cit., p. 164; D. SVANTESSON, *Solving the Internet* cit., p. 135 e Gregory SHAFFER, "Globalization and Social Protection: the Impact of EU and International Rules in Ratcheting Up Privacy Standards", *YJIL,* n.º 25, 2000, p. 80.

[1111] F. Loureiro BASTOS, "Algumas notas ..." cit., p. 443.

1.1.2. Os mecanismos promotores da aplicação do art. 3.º, n.º 2

Estes mecanismos dividem-se em duas categorias com base num critério assente na colaboração da entidade *ad quem*: mecanismos internos (1.1.2.1) e mecanismos externos (1.1.2.2). Antes de avançar devo esclarecer duas premissas das quais parto: em primeiro lugar, recordando a natureza *supletiva* da extraterritorialidade, julgo que a hipótese de a coordenar com o DIP deve ser explorada de modo a circunscrever o seu exercício a utilizadores de dados pessoais não estabelecidos nem na UE nem, por exemplo, num Estado parte da Convenção n.º 108 do CdE[1112]. Nestes casos haverá menos razões para suprir lacunas ou "duvidar" do direito estrangeiro que, em princípio, estará minimamente harmonizado com o DUE. O mesmo valerá nas situações em que o país onde se encontra estabelecido o utilizador dos dados pessoais foi visado por uma decisão de adequação. Por outras palavras, dificilmente estes países serão *data heaven's*.

Em segundo lugar, não posso ignorar que o RGPD lança, no art. 50.º, um forte apelo à cooperação internacional e à assistência mútua entre autoridades de controlo. Por isso, deverão ser estes os canais a privilegiar[1113].

1.1.2.1.Mecanismos internos

Nem sempre será necessário recorrer à colaboração da entidade *ad quem* para garantir a conformidade dos tratamentos nas situações do art. 3.º, n.º 2, do RGPD. Esta constatação parte da distinção entre execução *estrangeira* e execução *doméstica* da jurisdição extraterritorial prescritiva ou adjudicativa (*foreign enforcement of a jurisdictional claim* e *domestic enforcement of a jurisdictional claim*)[1114]. Na segunda hipótese incluem-se três situações:

(i) A responsabilização do representante do utilizador dos dados pessoais (1.1.2.1.1.);

[1112] Em sentido próximo, sugerindo que a extraterritorialidade pode ser mitigada "quando os países terceiros desenvolveram garantir normativas que correspondem às expetativas da UE", v. P. de HERT e M. CZERNIAWSKI, "Expanding the …" cit., p. 241.
[1113] Propondo que a jurisdição de execução seja mobilizada por critérios de cortesia internacional e de razoabilidade, C. KUNER, "Data Protection Law and (Part 2) ..." cit., p. 242 e ss..
[1114] D. SVANTESSON, *Solving the Internet* cit., p. 142.

(ii) A "teoria das medidas de destruição do mercado" desenvolvida no contexto da regulação da Internet (1.1.2.1.2.); e

(iii) O cumprimento voluntário das decisões das autoridades de controlo (1.1.2.1.3.).

1.1.2.1.1. A responsabilização do representante

Segundo o art 27.º do RGPD a obrigação de designar um representante recai sobre os utilizadores de dados pessoais visados pelo art. 3.º, n.º 2. Esta norma prossegue o mesmo fim da sua antecessora, o art. 4.º, n.º 2, da Diretiva, com modificações em três aspetos: (i) estende o alcance a subcontratantes; (ii) exige apenas *um* representante para todo o espaço da UE[1115]; e (iii) sanciona o incumprimento com uma coima[1116]. Mas quem é, afinal, o representante?

O representante é, de acordo com o art.º 4.º, n.º 17, do RGPD, uma pessoa singular ou coletiva estabelecida na UE que deve ser mandatado, por escrito, para esta função pelo utilizador dos dados pessoais. As exceções a esta obrigação encontram-se densificadas no art. 27.º do RGPD. Da leitura conjugada do considerando 80 e do art. 27.º, n.º 4, conclui-se que o representante deverá agir em nome do utilizador dos dados pessoais, no que diz respeito às obrigações que lhe são impostas pelo RGPD, e será o ponto de contacto das autoridades de controlo e do titular dos dados[1117]. Nos termos dos artigos 13.º, n.º 1, al. a) e 14.º, n.º 1, al. a), do RGPD, sempre que há uma recolha de dados pessoais, devem ser fornecidos elementos sobre a identidade do representante. Esta informação é particularmente relevante porquanto o titular dos dados poderá contactar o representante em "substituição" ou em "complemento"[1118] do representado, sempre que pretenda exercitar os seus direitos.

Independentemente dos termos do acordo celebrado entre o utilizador de dados e o seu representante, sobre o segundo recaem, *ope legis,* alguns deveres. Cabe-lhe, desde logo, o dever de cooperar com as autoridades de controlo e, por conseguinte, de fornecer informações de que aquelas necessitem[1119]. Acresce que deverá conservar um registo das

[1115] Art. 27.º, n.º 1 e 3, do RGPD.
[1116] Art. 83.º, n.º 4, al. a), do RGPD.
[1117] Art. 13.º, n.º 1, al. a) e art. 14.º, n.º 1, al. a), do RGPD.
[1118] Art. 27.º, n.º 4, do RGPD.
[1119] Art. 31.º e art. 58.º, n.º 1, al. c), do RGPD.

atividades de tratamento, do qual consta o conjunto de informações elencadas no art. 30.º, que deve disponibilizar, em caso de pedido, à autoridade de controlo.

Esta figura não deve ser confundida com o encarregado de proteção de dados pessoais (EPD), previsto no art. 37.º do RGPD. Ambos lidam com pedidos de titulares dos dados e de autoridades de controlo, mas a sua designação corresponde a obrigações diferentes. Um utilizador de dados pessoais obrigado a designar um representante poderá ser obrigado a nomear um EPD. Se, por exemplo, realiza operações de tratamento em grande escala de categorias especiais de dados pessoais, tais operações não são "ocasionais" pelo que terá de nomear ambos[1120]. Por seu turno, empresas não estabelecidas na UE que, por um lado, realizam operações de tratamento relacionadas com a oferta de bens e serviços mas que não preenchem os requisitos do art. 37.º, n.º 1, devem nomear um representante e não um encarregado. Há quem critique a imposição de designar um EDP a empresas estrangeiras por tanto constituir um encargo administrativo e organizacional pouco razoável e demasiado oneroso[1121]. A solução passaria por estabelecer uma graduação das exigências impostas aos utilizadores de dados pessoais sem estabelecimento na UE com base na intensidade da sua presença no mercado interno[1122]. Contudo, parece-me que os critérios usados para delimitar a obrigatoriedade de designar um EPD ("o controlo regular e sistemático dos titulares dos dados em grande escala" e a realização de "operações de tratamento em grande escala de categorias especiais de dados") já traduzem, em si mesmos, a força da presença da empresa estrangeira no mercado interno. Por seu turno, estabelecer uma graduação das exigências mitigava a pretensão de criar iguais condições para operadores da UE e operadores estrangeiros com atividade no mercado interno da União.

Os heterónimos do representante encontram-se noutros domínios do DUE: a Diretiva 2011/61/UE, sobre gestores de fundos de investimento alternativos (FIA), prevê um "representante legal", uma pessoa singular com domicílio na UE ou uma pessoa coletiva com sede social na UE e que, tendo sido expressamente designada por um gestor de um FIA extra-UE, age em nome e por conta deste[1123]; assim também na regulação de veículos, o Regulamento 168/2013 prescreve uma obrigação, para fabricantes

[1120] Art. 37.º, n.º 1, al. b) e art. 27.º, n.º 2, al. b), do RGPD.
[1121] D. SVANTESSON, *Extraterritoriality* cit., p. 195 e D. SVANTESSON e R. POLCAK, *Information Sovereignty* cit., p. 221 e 222.
[1122] D. SVANTESSON e R. POLCAK, *Information Sovereignty* cit., p. 222.
[1123] Art. 4.º, n.º 1, alínea u) e art. 37.º, n.º 3 da Diretiva 2011/61.

estabelecidos fora da UE, de nomearem um "representante"[1124] e, ainda, em relação a dispositivos médicos fabricados no exterior da UE, a Diretiva 2007/47/CE dispõe, para fabricantes com sede social fora dali, a obrigação de designar um "mandatário"[1125].

A designação de um representante tem duas funções: facilitar as interações do titular dos dados pessoais com um utilizador dos mesmos que esteja ausente e as interações com as autoridades de controlo de modo a potenciar a fiscalização dos tratamentos de dados pessoais realizados ao abrigo do art. 3.º, n.º 2, de harmonia com lógica da territorialidade dos poderes das autoridades de controlo. A designação de um representante visa, em última análise, organizar a capacidade de aplicar as disposições do RGPD "chamando" para o domínio de jurisdição territorial do Estado-Membro, se não o causador do risco (o utilizador dos dados pessoais), o seu substituto. Todo o problema reside, então, nos termos da responsabilidade do representante no lugar do utilizador de dados pessoais: segundo o memorando explicativo da proposta inicial da COM o representante sub-roga aquele nas suas obrigações e direitos[1126].

Em todo o caso, o art. 58.º, n.º 1, al. a), do RGPD, parece restringir as interações com as autoridades de controlo às "ordens" para o "fornecimento de informações", nomeadamente do registo das atividades de tratamento. Por conseguinte, parece que o RGPD não ficciona que o representante é o utilizador dos dados pessoais, imputando àquele as obrigações deste. Mas em que medida poderá o titular dos dados pessoais exercer os seus direitos contra o representante?[1127]

O art. 27.º, n.º 5, do RGPD, prevê que a designação de um representante não prejudica ações judiciais que possam ser intentadas contra o representado[1128]. Especificamente, em relação aos termos da sua responsabilidade, o considerando 80 *in fine* determina que este "deverá estar sujeito a procedimentos de execução em caso de incumprimento pelo

[1124] Que será "qualquer pessoa singular ou coletiva estabelecida na União, devidamente nomeada pelo fabricante para o representar junto da entidade homologadora ou da autoridade de fiscalização do mercado para agir em seu nome relativamente a questões abrangidas pelo âmbito de aplicação" do regulamento, v. artigos 3.º, n.º 48, 9.º, n.º 4 e 5 do Regulamento 168/2013 do Parlamento Europeu e do Conselho, de 15 de janeiro de 2013, relativo à homologação e fiscalização do mercado dos veículos de duas ou três rodas e dos quadriciclos.

[1125] Considerando 14 e art. 1.º, n.º 1, iii, al. j), da Diretiva 2007/47/CE do Parlamento Europeu e do Conselho, de 5 de setembro de 2007, que altera a Diretiva 90/385/CEE do Conselho relativa à aproximação das legislações dos Estados-Membros respeitantes aos dispositivos medicinais implantáveis ativos, a Diretiva 93/42/CEE do Conselho relativa aos dispositivos médicos e a Diretiva 98/8/CE relativa à colocação de produtos biocidas no mercado.

[1126] Este memorando não se encontra disponível no sítio da Comissão Europeia, podendo ser consultado no Archive of European Integration of the University of Pittsburgh, http://aei.pt.edu/10375, consultado no dia 30 de setembro de 2018.

[1127] Apelando à necessidade de clarificar este ponto, v. G29, "Parecer 8/2010 ..." cit., p. 35.

[1128] Art. 79.º do RGPD.

responsável pelo tratamento ou pelo subcontratante". Recuando à história legislativa do RGPD constato que a proposta inicial da COM era mais ambiciosa: o art. 78.º, n.º 2, previa a aplicação de sanções ao representante[1129]. O recuo do legislador terá sido motivado pela circunstância de eventuais medidas de execução contra o representante suscitarem questões práticas ao nível do direito interno dos Estados-Membros, designadamente dada a ausência de uniformidade em relação às mesmas e à possibilidade de responsabilizar o representante, aplicar-lhe sanções, nos termos do direito penal ou civil, em nome do representado[1130]. Os ordenamentos jurídicos internos divergem sobre a natureza da relação entre o representado e o representante: nuns casos o representante substitui o representado no que diz respeito à execução e às sanções e, noutros, dispõe de mero mandato[1131]. Ou seja, os termos da responsabilidade do representante dependem do direito nacional e não do DUE o que a torna variável[1132]. Conjugando esta geometria variável da responsabilidade do representante com a possibilidade de ser designado apenas *um* para todo o espaço da UE[1133], o legislador facilitou o *forum shopping* quanto à escolha de um Estado-Membro com a legislação que for mais favorável à (não) responsabilização daquele.

Como se não bastasse, a utilidade desta figura para efeitos de reforçar a exequibilidade das prescrições do art. 3.º, n.º 2, será reduzida quando a obrigação que lhe subjaz, a própria designação do representante, não for cumprida, o que sucedeu recentemente[1134].

[1129] "Sempre que o responsável pelo tratamento tiver designado um representante, as sanções são aplicadas ao representante, sem prejuízo de quaisquer sanções que possam vir a ser aplicadas contra o responsável pelo tratamento", v. Proposta de regulamento relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados (regulamento geral de proteção de dados), apresentada no dia 25 de janeiro de 2012, disponível em http://eur-lex.europa.eu/legal-content/en/ALL/?uri=CELEX%3A52012PC0011, consultado no dia 30 de setembro de 2018.

[1130] Esta dificuldade foi identificada pelo G29, "Parecer 8/2010 ..." cit., p. 25.

[1131] Tal refletia-se, aliás, na legislação de transposição da Diretiva. Em alguns Estados o direito interno previa explicitamente as sanções pecuniárias aplicáveis aos representantes (o caso da legislação de proteção de dados belga, de 8 de dezembro de 1992, da lei de 6 de julho de 2000 dos Países Baixos e da legislação grega. A legislação portuguesa, nos termos do art. 4.º, n.º 5, da Lei n.º 97/98, consagrava uma substituição plena do RT, "em todos os seus direitos e obrigações, sem prejuízo da sua própria responsabilidade"), noutros, como a Lei 78/17 francesa, de 6 de janeiro de 1978, não se prevêem sanções pecuniárias para os representantes, v. G29, "Parecer 8/2010 ..." cit., p. 26.

[1132] C. KUNER, *European* cit., p. 133; Rosemary JAY e Angus HAMILTON, *Data Protection law and Practice,* 2ª ed., Sweet and Maxwell, 2003, p. 96; U. DAMMANN e S. SIMITIS, *EG-Datenschutzrichtlinie* cit., p. 76.

[1133] Art. 27.º, n.º 3 do RGPD.

[1134] Correu termos num tribunal administrativo holandês um processo no qual o *WhatsApp* recorreu de uma coima da autoridade de controlo daquele país por incumprimento de designação de um representante na Holanda. Numa decisão de 22 de novembro de 2016, o tribunal deu razão à autoridade de controlo, numa decisão disponível em https://uitspraken.rechtspraak.nl/inziendocument?id=ECLI:NL:RBDHA:2016:14088& , consultada no dia 30 de setembro de 2018; Cobun KEEGAN e Jeroen TERSTEGGE, "The WhatsApp wake-up call for companies doing business in the EU", 14 de dezembro de 2016, disponível em https://iapp.org/news/a/the-whatsapp-

Se o passado não permite conclusões otimistas[1135], o futuro dirá se a estatuição de uma coima, até 10 000 000 EUR ou até 2% do volume de negócios anual da empresa, para o incumprimento desta obrigação exercerá um efeito *in terrorem*[1136].

Seja como for, na avaliação de impacto do RGPD, identificam-se outros obstáculos à imputação de responsabilidades ao representante, "em particular nos casos em que os serviços do responsável pelo tratamento sem estabelecimento na UE são claramente customizados para os titulares dos dados de certo Estado-Membro, pela utilização da língua daquele, pelas adaptações às suas preferências culturais e pela obtenção de receitas de publicidade de marcas, produtos e serviços locais, quando nem sempre é fácil ao titular dos dados reconhecer que ao usar aqueles serviços está a confiar os seus dados pessoais a um responsável pelo tratamento que pode não estar sujeito a legislação de proteção de dados pessoais eficaz"[1137]. Bem vistas as coisas, o principal óbice à garantia da proteção conferida pelo art. 3.º, n.º 2, do RGPD, é a existência de biliões de sítios *web* que cabem naquela descrição da avaliação de impacto, pelo que os recursos necessários para fiscalizar o cumprimento desta obrigação transcendem as capacidades do titular dos dados e das próprias autoridades de controlo[1138].

1.1.2.1.2. A teoria das "medidas de destruição do mercado" na regulação da Internet

Esta hipótese popularizou-se no contexto dos problemas colocados pela extraterritorialidade prescritiva no ciberespaço pelo que é particularmente apropriada para as atividades *online* reguladas pelo art. 3.º, n.º 2 do RGPD. Sucintamente, advoga-se o exercício de poderes coercivos *dentro das fronteiras* da entidade do foro, não diretamente sobre o autor ou a fonte da comunicação, atividade ou conteúdo *online,* mas indiretamente, em relação a intermediários, entidades locais e ao eventual património daquele[1139]. Como sintetiza D. SVANTESSON, "o poder dos Estados dentro das fronteiras

---

wake-up-call-for-companies-doing-business-in-the-eu/, consultado no dia 30 de setembro de 2018 e G29, "Letter of the Chair of Article 29 data protection working party", 16 de dezembro de 2016.

[1135] A propósito do incumprimento desta obrigação durante a vigência da Diretiva, v. C. KUNER, *European* cit., p. 133.

[1136] Art. 83.º, n.º 4, al. a), do RGPD.

[1137] Comissão Europeia, "Impact Assessment …" cit., p. 24 e 25.

[1138] D. SVANTESSON e R. POLCAK, *Information Sovereignty* cit., p. 221.

[1139] C. REED, *Making Laws* cit., p. 30; D. SVANTESSON, *Extraterritoriality* cit., p. 168 e do mesmo autor, *Solving the* cit., p.141; Marketa TRIMBLE, "Extraterritorial Enforcement of National Laws in Connection with Online Commercial Activity", John ROTHCHILD (ed.), *Research Handbook of Electronic Commerce Law,* Edward Elgar Publishing, 2015, p. 261 e ss.; Uta KOHL, *Jurisdiction and the Internet. Regulatory Competence over Online Activity,* Cambridge University Press, 2007, p. 225 e ss..

territoriais pode ser colocado ao serviço de atuações contra atividades e comunicações *offshore online*"[1140]. Esta via só é possível existindo controlo *interno* e *indireto* sobre o operador estrangeiro e sobre o mercado (de consumidores, serviços de publicidade, etc.) relevante para aquele. É esse controlo que permite maximizar os poderes coercivos (territoriais) da entidade do foro, que exerce jurisdição prescritiva fora de portas, segundo uma estratégia de execução unilateral, composta por medidas para penalizar o operador, o causador de um perigo externo com projeção interna, cuja atividade é prejudicial ou ilícita à luz da normatividade ali vigente.

Do catálogo destas medidas U. KOHL destaca a proibição de prestação, por parte de sujeitos locais, de serviços acessórios (como publicidade) à atividade principal do agente económico estrangeiro[1141], ou o bloqueamento do conteúdo ilegal através dos prestadores de serviços de Internet (ISP's) locais[1142]. D. SVANTESSON[1143] sugere a adoção de medidas legislativas e alterações no direito substantivo que permitam às autoridades da entidade do foro, no caso de recusa persistente de incumprimento, decretar, por exemplo, que o infrator estrangeiro não pode desenvolver atividades económicas no mercado nacional, as suas dívidas não podem ser executadas no território da entidade do foro, ou que os comerciantes e os operadores económicos locais não podem negociar com aquele. M. TRIMBLE[1144] propõe medidas que visam os ISP's, porquanto são estes quem se encontra em melhor posição para pôr termo às atividades ilícitas, no sentido de bloquearem ou não indexarem certos sítios *web*, e sublinha a utilidade de ordens judiciais sobre os processadores de pagamentos para recusarem transações aos infratores estrangeiros.

Um exemplo recente de aplicação destas medidas vem de um litígio no Brasil, com o *Facebook*. Em extrema síntese, o caso envolveu alegações de difamação, em publicações naquela rede social, visando uma celebridade brasileira que peticionava a sua remoção. Perante a rejeição da empresa norte-americana, um tribunal brasileiro ordenou a remoção do conteúdo no prazo de 48 horas acrescentando que, no caso de incumprimento, o *Facebook* seria bloqueado naquele país[1145]. Por outro lado, um domínio que parece ter

[1140] D. SVANTESSON, *Solving the Internet* cit., p. 142.
[1141] Como, por exemplo, na Nova Zelândia é proibida a publicitação de serviços de jogo ilegais. Nos EUA, vigora legislação para que os intermediários financeiros sejam pressionados, pela ameaça de coimas, a negar transações de cartões de crédito para empresas estrangeiras de jogo ilegal, v. U. KOHL, *Jurisdiction and the* cit., p. 228.
[1142] *Idem* p. 229.
[1143] D. SVANTESSON, *Extraterritoriality* cit., p. 169.
[1144] M. TRIMBLE, "Extraterritorial Enforcement …" cit., p. 266.
[1145] D. SVANTESSON, *Solving the Internet* cit., p. 147. Os tribunais brasileiros, sob críticas de violação da liberdade de expressão e de comunicação, têm sido particularmente ativos na adoção deste tipo de medidas, sobretudo em situações em que o *Facebook* e o *WhatsApp* se recusam a colaborar com as autoridades em

abraçado estas medidas é o dos direitos de autor. O art. 8.º da Diretiva 2001/29/CE prevê a faculdade de os titulares destes direitos solicitarem uma injunção contra intermediários que veiculem atos de violação de terceiros contra obras ou outros materiais protegidos[1146].

A utilização destas medidas nos esquemas de regulação da Internet denota que o princípio da territorialidade não é absolutamente irrelevante e, como aponta D. SVANTESSON, "a execução da jurisdição extraterritorial prescritiva pode não estar tão limitada como *prima facie* parece (…). Este ponto é essencial porquanto destrói o argumento de que aquela nunca pode ser executada" e, portanto, que apenas "ladra sem morder"[1147].

Entre as virtualidades desta solução sobressai o facto de apenas interferir com a atividade económica dirigida para o mercado em causa e não com as operações mundiais do operador estrangeiro. Com efeito, no caso de discordar da medida, aquele poderá abandonar o mercado em questão e desenvolver as suas atividades noutro[1148]. Tenha-se presente que, no contexto *online*, um operador que pretenda evitar o contacto com um determinado mercado, para assim contornar os riscos destas medidas, tem ao seu dispor soluções tecnológicas como o chamado *dis-targeting* e, em geral, as tecnologias de geo-localização, que permitem identificar a localização geográfica do internauta[1149]. Estas soluções existem há vários anos e, apesar de o direito manifestar alguma lentidão na sua acomodação, operadores em certos setores, como no *marketing*, há muito que as adotaram nas suas práticas[1150].

---

investigações criminais. A frequência deste instrumento é tal que estão a ser discutidas propostas para legislar estas medidas, v. Artigo 19, "Bloqueios de sites e aplicativos no Brasil – Subsídios ao debate legislativo", 10 de dezembro de 2017, disponível em https://www.article19.org/resources/brazil-proposed-bills-regulate-blocking-websites-applications-threaten-freedom-expression/, consultado no dia 30 de setembro de 2018.

[1146] Acórdão do TJ, UPC Telekabel Wien GmbH c. Constantin Film Verleih GmbH e Wega Filmproduktionsgesellschaft mbH, C-314/12, 27 de março de 2014. O caso versa sobre um sítio *web* que colocava obras cinematográficas à disposição do público, sem o consentimento dos titulares de um direito conexo com o direito de autor, e desenvolve o conceito de "intermediários" cujos serviços são utilizados por terceiros para violar um direito daquele tipo tal como expresso no art. 8.º da Diretiva 2001/29/CE do PE e do Conselho, de 22 de maior de 2001, relativa à harmonização de certos aspetos do direito de autor e dos direitos conexos na sociedade da informação. Este artigo dispõe que "Os Estados-Membros deverão garantir que os titulares dos direitos possam solicitar uma injunção contra intermediários cujos serviços sejam utilizados por terceiros para violar um direito de autor ou direitos conexos".

[1147] D. SVANTESSON, *Solving the Internet* cit., p. 143 e 144 e, do mesmo autor, *Extraterritoriality* cit., p. 173.

[1148] D. SVANTESSON, *Solving the Internet* cit., p. 145.

[1149] Dan SVANTESSON, "Pammer and Hotel Alpenhof – ECJ Decision Creates Further Uncertainty about When E-Business 'Direct Activities' to a Consumer's State under the Brussels I Regulation", *CLSR,* vol. 27, n.º 3, 2011, p. 298 e ss..

[1150] D. SVANTESSON, *Extraterritoriality* cit., p. 175 e, do mesmo autor, "Time for the Law to Take Internet Geo-Location Technologies Seriously", *JPIL,* vol. 8, n.º 3, 2012, p. 473 e ss.; Kevin KING, "Personal

Isto dito, julgo que estas medidas haviam de ser equacionadas no modelo de garantia das prescrições do art. 3.º, n.º 2, do RGPD. Com isto não quero fazer das mesmas o rochedo de bronze dos poderes de correção das autoridades de controlo ou dos tribunais nacionais. Atendendo ao impacto que podem ter numa sociedade cada vez mais digitalizada, a sua consagração legislativa e a sua adoção prática devem ser balizadas por critérios de proporcionalidade[1151]. No domínio da proteção de dados pessoais, esses critérios devem incluir, pelo menos, o grau de risco do tratamento de dados pessoais, o tipo de dados e o tipo de incumprimento, bem como outros indicadores da situação em concreto, como a existência de um representante e a faculdade de o responsabilizar, o grau de colaboração do infrator estrangeiro e, em especial, o recurso a mecanismos externos e colaborativos que apresento adiante.

1.1.2.1.3. A adesão voluntária ao direito estrangeiro

Conforme referi, uma autoridade de controlo pode adotar decisões desfavoráveis (e, *a fortiori*, favoráveis) com vocação extraterritorial, isto é, em relação a um utilizador de dados pessoais sem estabelecimento. Creio que o legislador se terá estribado em duas possibilidades para viabilizar a produção de efeitos dessas decisões:

(i) O utilizador de dados pessoais conforma-se, voluntariamente, com as cominações legais estrangeiras ou

(ii) O reconhecimento e execução daquelas decisões pela entidade *ad quem,* onde se situa o infrator.

Trato agora do primeiro aspeto e remeto o segundo para diante. A conformação voluntária de um utilizador de dados pessoais com comandos e decisões estrangeiras funda-se, como referi na Parte I, no reconhecimento de géneros de motivação para a aceitação da vinculatividade das normas independentes do aparelho de coação e de garantia da entidade do foro. Por conseguinte, certos efeitos das decisões das autoridades de controlo com aptidão extraterritorial não requerem um mecanismo formal de

Jurisdiction, Internet Commerce, and Privacy: The Pervasive Legal Consequences of Modern Geolocation Technologies", *AJST,* n.º 21, 2011, p. 61 e ss.; M. TRIMBLE, "The Future …" cit., p. 567.

[1151] D. SVANTESSON, *Extraterritoriality* cit., p. 170 e, do mesmo autor, *Solving the Internet* cit., p. 145.

atribuição de relevância ao ato estrangeiro por parte da entidade *ad quem*[1152]. Ou seja, a simples existência de uma decisão de uma autoridade estrangeira, visando um utilizador de dados pessoais situado fora do seu território, pode produzir efeitos mesmo na ausência de controlo ou reconhecimento pela entidade *ad quem*.

O G29 parece apostar nesta tese quando, a propósito das sentenças dos tribunais do Estados-Membros, explica que o tribunal "poderá considerar que o site estrangeiro estava a fazer um tratamento ilegal e desleal dos dados pessoais do indivíduo. Muitos países terceiros já preveem o reconhecimento e a aplicação da sentença, mas, mesmo que o não façam, há exemplos nos quais o sítio *web* estrangeiro pode, mesmo assim, seguir a sentença e adaptar o seu tratamento de dados, com vista a desenvolver uma boa prática comercial e a manter uma boa imagem comercial"[1153]. Assim também, a propósito do acórdão *Google Spain,* F. CALVÃO sublinha que "não obstante estas limitações na execução do acórdão, a verdade é que o tempo vai demonstrando que há algum efeito útil em decisões judiciais deste teor, porque os responsáveis pelos tratamentos tendem a ajustar as condições dos mesmos ao naquelas definido"[1154].

Também na Parte I referi que a adesão aos comandos estrangeiros estará ancorada em motivações ligadas ao interesse económico, ao bom-nome ou à confiança. Com efeito, segundo U. KOHL, "ser percecionado como um infrator não é positivo para as empresas"[1155]. Nestas situações, o poder da publicidade, a eficácia do chamado *naming and shaming*, foram reconhecidos por várias autoridades de controlo[1156]. Mas mais. O domínio estudado tem sido apontado como mais um exemplo do MPE e do "efeito de Bruxelas". Como notou a COM numa Comunicação de 2017, são muitas as empresas, especialmente as de dimensão transnacional, que estão voluntariamente a alinhar as suas práticas com o RGPD[1157]. O mesmo havia concluído a doutrina a propósito da Diretiva[1158]. Assim, também no domínio da proteção de dados pessoais, a UE tem vindo

[1152] D. LOPES refere que nem todos os atos administrativos estrangeiros estão dependentes de uma intervenção do Estado *ad quem* ou "receptor", isto é, de um processo específico de reconhecimento, v. D. LOPES, *Eficácia* cit., p. 227.
[1153] G29, "Documento de trabalho ..." cit., p. 16. Foi, aliás, o que sucedeu na litigância entre a LICRA e o Yahoo, quando este operador acabou por se conformar com a legislação francesa v. J. GOLDSMITH e T. WU, *Who controls the* cit., p. 10 e ss; L. COLONNA, *Legal* cit., p. 364; Winston ANDERSON, "Foreign Orders and Local Land and the Caribbean Gets its Own Version of Duke v Andler", *ICLQ,* n.º 48, 1999, p. 167 e 172.
[1154] F. CALVÃO, "A proteção ..." cit., p. 6799.
[1155] U. KOHL, *Jurisdiction and* cit., p. 208. Aflorando esta hipótese, v. Kuan HON, "GDPR's extra-territoriality means trouble for cloud computing", *Privacy Law & Business,* Abril 2016, p. 26.
[1156] Nomeadamente a CNIL e o ICO, v. D. WRIGHT, "Enforcing ..." cit., p. 17.
[1157] Comissão Europeia, "Intercâmbio ..." cit., p. 2.
[1158] C. KUNER, *Transborder* cit., p. 180; G. SHAFFER, "Globalization and …" cit., p. 78.

a posicionar-se como regulador transnacional, não apenas por via do procedimento de adequação, mas também por força das suas caraterísticas políticas e económicas, em especial a dimensão do seu mercado interno e as dependências que este cria[1159].

1.1.2.2.Mecanismos externos

A reação da entidade *ad quem* não será necessariamente negativa podendo colaborar na execução da pretensão da entidade do foro. Fala-se, nestes casos, de execução estrangeira da jurisdição extraterritorial da entidade do foro.

Será esse o pressuposto do legislador ao introduzir o art.º 50.º no RGPD sobre cooperação internacional, designadamente para "facilitar a aplicação efetiva da legislação em matéria de proteção de dados pessoais" (al. a)) e para "a assistência mútua a nível internacional, nomeadamente através da notificação, comunicação de reclamações, e assistência na investigação e intercâmbio de informações, sob reserva das garantias adequadas de proteção de dados pessoais e de outros direitos e liberdades fundamentais" (art. 50, al. b)). Assim, formalmente, o legislador da UE adere a uma tendência internacional[1160] ou bilateral[1161] em estado avançado. Com efeito, a importância da

[1159] Anu BRADFORD, "The Brussels …" cit., p. 2 e ss.; C. KUNER, "The Internet …" cit., p. 23; F. GADY, "EU/US …" cit., p. 12 e ss.; H. HIJMANS, *The European* cit., p. 10 e ss..; M. GOMANN, "The new territorial …" cit., p. 568; Paul SCHWARTZ, "The EU-U.S. Privacy Collision: A Turn to Institutions and Procedures", *HLR*, n.º 126, 2013, p. 1986; P. de HERT e M. CZERNIAWSKI, "Expanding the …", cit., p. 568.

[1160] Além de a Convenção n.º 108 do CdE consagrar regras de cooperação mútua entre as partes e as autoridade de supervisão, nos últimos tempos multiplicam-se os casos de resoluções e declarações mútuas com a mesma intenção, sublinhe-se a iniciativa das próprias autoridades de controlo de criação de uma rede informal conhecida como GPEN (*Global Privacy Enforcement Network*) com a missão de promover e estimular a cooperação na execução transnacional de leis de proteção de dados e a troca de informações entre autoridades de controlo (GPEN, "Action Plan for the Global Privacy Enforcement Network", 15 de junho de 2012, disponível em https://www.privacyenforcement.net/public/activities, consultado no dia 30 de setembro de 2018. Outra importante rede é a *International Conference of Data Protection and Privacy Commissioners* (ICDPPC), um encontro anual para promover a troca de boas práticas e moldar políticas.

[1161] A este nível, em 2005, um memorando de entendimento foi assinado entre a autoridade de controlo espanhola e a *US Federal Trade Commission* sobre a prestação de assistência mútua em assuntos comerciais relativos aos emails (v. Federal Trade Commission, "Memorandum of understanding on mutual enforcement assistance in commercial email matters between the Federal Trade Commission of the United States of America and the Agencia Espanola de Proteccion de Datos", 2005, disponível em https://www.ftc.gov/sites/default/files/attachments/international-antitrust-and-consumer-protection-cooperation-agreements/050224memounderstanding.pdf, consultado no dia 30 de setembro de 2018). Arranjos semelhantes foram celebrados entre a Austrália e a Nova Zelândia (v. Office of the Privacy Commissioner of New Zealand , "Memorandum of Understanding between the Office of the Australian Privacy Commissioner and the Office of the New Zealand Privacy Commissioner", 28 de agosto de 2008, disponível em https://www.privacy.org.nz/further-resources/events-and-networks/memorandum-of-understanding/ , consultado no dia 30 de setembro de 2018), e a Alemanha e o Canadá (v. Office of the Privacy Commissioner of Canada, "Memorandum of Understanding (Germany)", 2012, disponível em https://www.priv.gc.ca/en/about-the-opc/what-we-do/international-collaboration/international-memorandums-of-understanding/mou-germany/, consultado no dia 30 de setembro de 2018).

cooperação internacional foi reconhecida numa recomendação da OCDE, de 12 de junho de 2007 e por outras instituições internacionais[1162]. Uma comunicação da COM, de janeiro de 2017, confirmou o relevo da cooperação na estratégia de implementação e garantia deste regime com a dupla função de "assegurar uma proteção mais eficaz dos direitos individuais e uma maior segurança jurídica para as empresas"[1163].

O espírito da cooperação internacional deverá passar do papel à prática em dois momentos distintos da fiscalização dos tratamentos abrangidos pelo art. 3.º, n.º 2, do RGPD: um momento *prévio* e outro *posterior*. No primeiro, firmado num *princípio de efetividade* cuja adoção proponho para este domínio. Adicionalmente, há instrumentos ao dispor das autoridades de controlo que "facilitam a previsão e concretização de vias que conferem eficácia" às suas decisões com vocação extraterritorial[1164]. No segundo momento, posterior, a cooperação internacional materializa-se em mecanismos de reconhecimento e execução de sentenças judiciais e de decisões das autoridades de controlo.

1.1.2.2.1. O princípio da efetividade

Este princípio tem sido tratado pela doutrina internacional-administrativista[1165]. Em síntese, significa que a fixação do órgão administrativo competente para agir, relativamente a situações com elementos de estraneidade, deve resultar da verificação de uma capacidade efetiva de implementação coerciva, que pode ser aferida, entre outros fatores, pela proximidade física em relação a cada um dos elementos de estraneidade.

Creio que este princípio deverá figurar entre as "regras internacionais de cooperação" anunciadas no art. 50.º, al. a), do RGPD, pelas seguintes razões:

(i) Reflete uma manifestação concreta de *comity,* uma preocupação que tem estado presente em posições, por exemplo, da COM[1166];

[1162] OCDE, "Recommendation on Cross-border Co-operation in the Enforcement of Laws Protecting Privacy", 12 de junho de 2007 e Hague Conference on Private International Law, "Cross-Border Data Flows and Protection of Privacy", 2010, n.º 3.
[1163] Comissão Europeia, "Intercâmbio ..." cit., p. 6.
[1164] D. LOPES, *Eficácia* cit., p. 321 e ss..
[1165] M. Prata ROQUE, *A Dimensão* cit., p. 1168 e nota de rodapé 2969.
[1166] D. SVANTESSON sublinha este ponto citando a posição da Comissão Europeia enquanto *Amicus Curiae* no caso *Microsoft:* "qualquer lei nacional que cria obrigações transnacionais – adotada pelos EUA, pela UE ou por outro Estado – deve ser aplicada e interpretada tendo em atenção o respeito pela *comity* (...)", cfr. "Article 3 ..." cit., p. 3.

(ii) É um critério que busca eficiência e razoabilidade na implementação deste bloco de normas, que garante o "maior efeito útil possível da atuação administrativa"[1167] e materializa as afirmações do G29 segundo as quais a fiscalização dos tratamentos total ou parcialmente ocorridos fora da UE apenas se verificará nos casos em que "é necessário, em que faz sentido e em que existe um nível razoável de capacidade de aplicação, tendo em conta a situação transfronteiriça envolvida"[1168].

Na prática, este critério já permeia o dia-a-dia das autoridades de controlo como sugere, por exemplo, o parecer do G29 sobre a implementação do caso *Google Spain*[1169]*,* e outros critérios de *self-restraint* das atuações destas autoridades[1170], como o avançado pelo ICO[1171] e o aplicado pela AEPD[1172]. Sem prejuízo da legitimidade desta "triagem" pragmática das autoridades de controlo quanto aos pedidos de desindexação, sem adesão em sede jurisprudencial ou legislativa e que se aproxima de uma restrição aos direitos fundamentais dos titulares dos dados que peticionam a desindexação[1173], o que ela reflete é o imperativo de introduzir nas atuações administrativas critérios de eficiência e de razoabilidade.

A consagração legislativa do princípio da efetividade implicará que os poderes das autoridades de controlo sejam "travados" por um momento prévio de verificação da possibilidade de outra autoridade de controlo estrangeira se encontrar mais apta a garantir

[1167] M. Prata ROQUE, *A Dimensão* cit., p. 1166.
[1168] G29, "Documento de trabalho sobre a determinação da aplicação internacional da legislação da UE em matéria de proteção de dados ao tratamento de dados pessoais na Internet efetuado por sites não-europeus", 20 de maio de 2002, p. 10 e 15.
[1169] G29, "Guidelines on …" cit., p. 8 e 9.
[1170] Seja porque lhes faltam recursos, financeiros e humanos, ou porque dão prioridade à proteção dos titulares dos dados com uma conexão razoável com o respetivo Estado-Membro, v. Christopher KUNER, "Foreign Nationals and Privacy protection: A Comparative Transatlantic Analysis", Hielke HIJMANS *et alii* (eds.), *Data Protection 2014: How to Restore Trust,* Intersentia, 2014, p. 213 e ss..
[1171] D. SMITH, "Four things we've learned …" cit., p. 1. Como expliquei, a autoridade do Reino Unido dá prioridade a pedidos "relacionados com uma evidência clara de dano ou perturbação para o indivíduo".
[1172] AEPD, "Resolución ..." cit., p. 8. A autoridade espanhola invoca o art. 4.º, n.º 1, al. a), da Diretiva, tal como o TJ no caso *Google Spain,* restringindo-o ao tratamento de dados pessoais de titulares dos dados com uma "vinculação clara" com um Estado-Membro da UE.
[1173] A restrição dos pedidos de "esquecimento" a uma categoria específica de titulares dos dados não decorre do caso *Google Spain,* nem da Diretiva, do RGPD, da CDFUE (art. 8.º) ou do TFUE (art. 16.º), ambos alargando a proteção a "titulares dos dados", independentemente da nacionalidade, residência, ou a qualquer outro critério. Suscitando estas dúvidas, v. C. KUNER, "The Court of Justice …" cit., p. 13.

o efeito útil da decisão para prevenir dificuldades futuras na sua execução[1174]. Confirmando-se essa hipótese, a reclamação deverá ser remetida para essa autoridade.

Esta solução encontra-se, por exemplo, no *Privacy Act* da Nova Zelândia na secção 72C: "(1) Quando, ao receber uma reclamação ao abrigo desta Parte, o Comissário considere que a reclamação se relaciona, no todo ou em parte, com uma situação que será mais bem resolvida por uma autoridade de controlo estrangeira, o Comissário pode consultar com aquela de modo a determinar os meios adequados para tratar da reclamação; (2) Assim que possível, depois de consultar a autoridade de controlo estrangeira, o Comissário deve decidir se a reclamação deve ser resolvida, no todo ou em parte, ao abrigo deste Ato; (3) Se o Comissário decidir que a reclamação pode ser decidida, no todo ou em parte, pela autoridade de controlo estrangeira, e esta e o reclamante concordarem nesse sentido, o Comissário pode reencaminhar a queixa para aquela autoridade; (4) Por autoridade de controlo estrangeira entende-se qualquer órgão público responsável por fiscalizar a aplicação da legislação de proteção de dados pessoais e com poder de conduzir investigações e adotar medidas de execução"[1175].

Por outro lado, o princípio da efetividade vigora noutros domínios com vocação extraterritorial, em especial no direito da concorrência, sempre que uma das autoridades não se considere competente ou a mais competente para agir, em especial quando as atividades em causa não têm efeitos diretos, substanciais e previsíveis nos consumidores da entidade do foro ou tendo-os, quando as atividades anti-concorrenciais ocorreram principalmente no, ou se dirigem principalmente, ao território da outra parte[1176].

No art. 50.º, al. a) e b), do RGPD, ilumina-se um indício deste princípio cuja sede própria podem ser, por exemplo, acordos de assistência mútua celebrados entre a UE e países terceiros. Numa Comunicação de 2017, a COM adiantou a "possibilidade de explorar um acordo-quadro de cooperação entre as autoridades responsáveis pela proteção de dados na UE e as autoridades responsáveis pela aplicação da legislação em

[1174] Sugerindo um esquema semelhante, v. C. KUNER, *Transborder* cit., p. 182 e, do mesmo autor, "Extraterritoriality and …" cit., p. 242, 244 e 245.
[1175] Disponível em http://www.legislation.govt.nz/act/public/1993/0028/latest/DLM3242805.html, consultado no dia 30 de setembro de 2018.
[1176] É a solução prevista no Acordo entre as Comunidades Europeias e o Governo dos EUA relativo aos princípios de cortesia positiva na aplicação dos respetivos direitos de concorrência, de 1998, complementado pelo Acordo Administrativo de 1999 relativo à participação mútua em fases de tramitação.

determinados países terceiros", à luz do que sucede noutros domínios como a concorrência[1177] e a defesa dos consumidores[1178].

Contudo, há uma limitação ao alargamento deste princípio a novas matérias: o seu campo de aplicação. A efetividade dever-se-á restringir aos casos em que vigore entre a entidade do foro e os países terceiros uma "Comunidade de Direito", um processo de harmonização pragmático quanto aos padrões normativos aplicáveis, ou um indicador do comprometimento da entidade *ad quem* com a prossecução da jurisdição prescritiva ou adjudicativa da entidade do foro [1179]. No campo da proteção de dados pessoais há, pelo menos, duas situações em que este compromisso existirá:

(i) Os Estados que são parte da Convenção n.º 108, do CdE, vincularam-se a um mesmo bloco de normas;

(ii) Os Estados visados numa decisão de adequação, cujo ordenamento jurídico foi, previamente, verificado pela COM e considerado adequado.

Por conseguinte, nestas situações, o princípio da efetividade abre um caminho para a execução estrangeira de um comando ou pretensão com vocação extraterritorial de um Estado-Membro da UE. A longo prazo, prosseguindo o processo de convergência substantiva dos regimes de proteção de dados pessoais em termos globais, este princípio poderá ganhar mais relevância.

[1177] Veja-se a informação da Comissão Europeia, MEMO/03/33 de 13 de fevereiro de 2013: "A cooperação internacional é uma grande prioridade da Comissão Europeia no campo das políticas anti-cartel. O tema da concorrência cada vez mais se torna global e as empresas, junto com as respetivas estratégias empresariais, há muito que transcendem o Estado individual e o território da União Europeia. A grande maioria dos cartéis, hoje em dia, são internacionais. Portanto, torna-se critico apostar numa política de concorrência que permita à União Europeia aplicar as suas normas de forma eficaz no mundo", cfr. E. FRIEDEL-SOUCHU, *Extraterritorialité du* cit., p. 194 e Richard WISH e David BAILEY, *Competition law,* 7ª ed., *Oxford University Press,* 2012, p. 273.

[1178] Comissão Europeia, "Intercâmbio ..." cit., p. 14.

[1179] Jurgen BASEDOW, "International Antitrust: From Extraterritorial Application to Harmonization", *LLR*, vol. 60, n.º 4, 2000, p. 1042 e ss. e M. Prata ROQUE, *A Dimensão* cit., p. 1168.

1.1.2.2.2. A ponderação de interesses, a participação, cooperação e difusão de informação

Uma atuação administrativa aberta é uma via que potencia a eficácia de atos administrativos com vocação extraterritorial[1180]. Assim, sempre que uma autoridade de controlo antecipar possíveis efeitos extraterritoriais deverá:

(i) Tomar em consideração os vários interesses em jogo, como o do utilizador dos dados pessoais, do respetivo titular, o tipo de tratamento e o risco conexo, aliados ao comércio internacional e aos interesses estrangeiros;

(ii) Convocar a participação de autoridades estrangeiras, no sentido da "internalização dos interesses públicos estrangeiros e da criação de uma cultura de *recíproca consideração*"[1181];

(iii) Divulgar e partilhar informação entre as várias autoridades interessadas, tal como sugere o art. 50.º, al. d), do RGPD, o que inclui a troca de informação a pedido da autoridade de controlo local, mecanismos de informação mútua, bem como modos de assistência mais integrados como o pedido de atuação administrativa na entidade *ad quem* em benefício da entidade do foro, a possibilidade de a autoridade de controlo da entidade do foro exercer atividades operacionais na entidade *ad quem* ou até a realização de operações e investigações conjuntas[1182].

Um exemplo deste tipo de medidas é o documento informativo do G29, sobre o RGPD, vocacionado para as *Asia Pacific Privacy Authorities* (APPA)[1183]. Ainda que, de um modo geral, os mecanismos de troca de informações de assistência administrativa não sejam desconhecidos, a possibilidade de celebração de acordos de assistência mútua é o palco privilegiado para este tipo de interações.

[1180] D. LOPES, *Eficácia* cit., p. 321.
[1181] *Idem* p. 329.
[1182] *Idem* p. 330.
[1183] G29, "EU general data protection regulation. General Information Document", 12 de fevereiro de 2018.

1.1.2.2.3. O reconhecimento e execução das sentenças judiciais e das decisões de autoridades de controlo

Mas a colaboração da entidade *ad quem*, agora num momento *posterior* à apreciação de desconformidade de um tratamento, é viável através da "ampliação consentida da extraterritorialidade" [1184], isto é, do reconhecimento e execução das sentenças dos Estados-Membros e das decisões das autoridades de controlo. Abre-se assim outro caminho para a execução estrangeira de uma prescrição com vocação extraterritorial da entidade do foro, um caminho que, aliás, é recomendado pela OCDE[1185].

Em relação à primeira hipótese, relativa às sentenças judiciais, de harmonia com o art. 79.º, n.º 2, são dois os critérios que determinam o foro competente para uma ação judicial contra um utilizador de dados pessoais[1186]: (i) o Estado-Membro onde esse utilizador tem estabelecimento; e (ii) o Estado-Membro da residência habitual do titular dos dados pessoais. Por conseguinte, nos casos dos utilizadores de dados pessoais abrangidos pelo art. 3.º, n.º 2, sem estabelecimento num Estado-Membro, apenas os titulares dos dados pessoais residentes na UE podem propor uma ação judicial. O G29 recomendou esta via, para os casos envolvendo *sites* estrangeiros, sublinhando que em muitos países se prevê o reconhecimento e a execução da sentença nestas situações[1187]. Esta sugestão é corroborada pela doutrina que defende o recurso direto aos tribunais, sem a intermediação de uma autoridade de controlo, pelas mesmas razões[1188]. Será esse o caso em relação a muitos problemas potenciados pelo uso de redes sociais, tratados pelos tribunais, em sede de direito penal ou civil como, por exemplo, o uso abusivo de imagem[1189]. Devo destacar que a Conferência de Haia de Direito Internacional Privado se tem debruçado sobre este tema e, em maio de 2018, divulgou um projeto de Convenção

[1184] M. Prata ROQUE, *A Dimensão* cit., p. 219 e ss..
[1185] OCDE, "Recommendation on Cross-Border Co-Operation in International Enforcement of Laws Protecting Privacy", 2007, p. 9, n.º 10
[1186] Onde se lê: "Os recursos contra os responsáveis pelo tratamento ou os subcontratantes são propostos nos tribunais do Estado-Membro em que tenham estabelecimento. Em alternativa, os recursos podem ser interpostos nos tribunais do Estado-Membro em que o titular dos dados tenha residência habitual, salvo se o responsável pelo tratamento ou o subcontratante for uma autoridade de um Estado-Membro no exercício dos seus poderes públicos".
[1187] G29, "Documento de trabalho ..." cit., p. 16.
[1188] D. SVANTESSON, "Enforcing Privacy ..." cit., p. 211.
[1189] A. Sousa PINHEIRO, *Privacy* cit., p. 815 e C. Sarmento e CASTRO, "A jurisprudência ..." cit., p. 1056.

com regras sobre o reconhecimento e execução de decisões judiciais[1190]. Nesse projeto o art. 2.º, n.º 1, al. l), exclui do seu âmbito as questões da privacidade, com exceção daquelas baseadas num contrato entre as partes. Poderá caber nesta exceção o tratamento de dados pessoais do art. 3.º, n.º 2, do RGPD, sempre que exista um contrato entre um titular e o utilizador dos seus dados pessoais.

Em relação às decisões das autoridades de controlo, a sua vocação extraterritorial é "eventual" pois, *ab initio,* no momento da sua edição, não é inequívoco que vão produzir efeitos no território estrangeiro onde se situa o utilizador de dados pessoais. Essa aptidão concretiza-se pelo reconhecimento e execução pela entidade *ad quem,* "dadas as regras aplicáveis à jurisdição executiva e segundo as quais é ao Estado de destino que compete definir os termos e condições de reconhecimento e execução de atos administrativos estrangeiros"[1191]. Ou seja, compete-lhe definir *se* e *como* acolhe as decisões das autoridades de controlo. Daí que a doutrina venha colocando bastante ênfase na necessidade de criação de mecanismos de reconhecimento mútuo[1192]. Como reconheceu o ICO, sem estas vias o respeito pelo regime de proteção de dados, por RT/ST estrangeiros sem presença física na UE, seria voluntário [1193].

Em todo o caso, nas duas hipóteses, há que distinguir o *reconhecimento* da *execução* do direito estrangeiro, seja das sentenças judiciais de tribunais de Estados-Membros seja das decisões das autoridades de controlo. O reconhecimento é essencialmente tolerante ou recetivo, ao passo que a execução implica uma atuação positiva e uma "intensa colaboração internacional"[1194]. Entre os vários fatores determinantes para a implementação destes mecanismos vislumbra-se a vigência de uma "Comunidade de Direito" ao jeito da velha ideia de SAVIGNY, para que aqueles que dela fazem parte consintam na ampliação do âmbito de eficácia de atos administrativos e leis

[1190] Special Commission on the Recognition and Enforcement of Foreign Judgements, "2018 Draft Convention", document de trabalho n.º 262 REV, disponível em https://assets.hcch.net/docs/23b6dac3-7900-49f3-9a94-aa0ffbe0d0dd.pdf, consultado no dia 30 de setembro de 2018.

[1191] D. LOPES, *Eficácia* cit., p. 301. A autora inclui estas decisões na categoria dos atos administrativos estrangeiros em sentido estrito por oposição, por exemplo, aos atos administrativos transnacionais, verificados em relações horizontais e bilaterais e não em relações unidirecionais entre Estados, como nos nossos casos, mediante as quais "a eficácia extraterritorial é função da intervenção do Estado de reconhecimento".

[1192] C. KUNER, *Transborder* cit., p. 179 e ss.. A criação destes mecanismos já vem acontecendo. Disso é exemplo a colaboração entre o G29 e a APEC para facilitar que as empresas asiáticas abrangidas pelo RGPD e pela legislação local respeitam a legislação dos dois lados do mundo, v. G29, "Opinion 02/2014 on a referential for requirements for Binding Corporate Rules submitted to national Data Protection Authorities in the EU and Cross Border Privacy Rules submitted to APEC CBPR Accountability Agents", 27 de fevereiro de 2014.

[1193] ICO, "Initial Analysis …" cit., 2012, p. 5.

[1194] D. LOPES, *Eficácia* cit., p. 352.

estrangeiras ou na atribuição de força executiva em virtude da confiança recíproca existente[1195]. É esse o entendimento do G29 ao enunciar que, nos países terceiros com normas de proteção de dados pessoais e autoridades de controlo, a aplicação do art. 4.º, n.º 1, al. c), da Diretiva, seria menos problemática[1196]. Indicando a vigência deste grau de confiança em matéria de proteção de dados pessoais vejam-se, por exemplo, os países visados por uma decisão de adequação[1197], bem como os Estados parte da Convenção n.º 108 do CdE[1198].

Porém, não é rigoroso falar-se de um *dever* de reconhecer e executar o direito estrangeiro pelo que, em último caso, a mais-valia destes mecanismos dependerá de um enquadramento de elevada cooperação e de uma ponderação da entidade *ad quem,* amparada por critérios de cortesia internacional e mobilizada por interesses próprios como, por exemplo, colocar fim ao litígio ou à litigância, não despender recursos com situações que já foram razoavelmente adjudicadas ou outro tipo de razões inerentes aos interesses daquela[1199].

1.2.Reações negativas

Ainda que desconhecidas até ao momento em que escrevo, as reações negativas de países terceiros à UE, à extraterritorialidade deste regime não são de descartar em absoluto, em particular a adoção de medidas de bloqueamento[1200].

Não obstante, julgo que este é um risco residual por duas razões:

(i) A tendência generalizada, desde os países asiáticos aos africanos, pelo alinhamento com o regime da UE, num processo de regulação transnacional e de convergência de soluções[1201];

[1195] J. SAMPAIO, *O Acto* cit., p. 82; M. Prata ROQUE, *A Dimensão* cit., p. 1199.
[1196] G29, "Documento de trabalho ..." cit., p. 16.
[1197] No Canadá, por exemplo, existe uma autoridade de controlo (*Privacy Commissioner of Canada*), tal como na Nova Zelândia (*Privacy Commissioner*) e na Argentina (*Dirección Nacional de Protección de Datos Personales*), entre outras.
[1198] Tanto a versão original, no Protocolo Adicional adotado em 2001 (art. 1.º), como a versão revista recentemente (capítulo 3) preveem uma autoridade de controlo e supervisão neste domínio.
[1199] Em sentido próximo v. D. LOPES, *Eficácia* cit., p. 429 e 439.
[1200] D. SVANTESSON, *Extraterritoriality* cit., p. 161 e ss. e, do mesmo autor, "The Extraterritoriality …" cit., p. 94 e L. COLONNA, *Legal* cit., p. 367.
[1201] Cfr. Parte II, Capítulo 3, ponto 3.2.2 desta tese.

(ii) A razoabilidade da jurisdição da UE, porquanto esta se encontra fundamentada em elos significativos com a mesma e prossegue interesses jusfundamentais e económicos legítimos. Daí que, como referi, o critério adotado no art. 3.º, n.º 2, do RGPD, tenha sido bem acolhido noutros países, nomeadamente nos EUA.

1.3. O surgimento de conflitos de jurisdição

Como observa C. KUNER, os conflitos de jurisdição são inevitáveis no atual paradigma do *pluralismo jurídico*[1202]. Porém, esta circunstância não impede que, gradualmente, se procure a harmonização e se gerem consensos: "[o pluralismo jurídico] (...) não se coaduna com o estabelecimento de uma ordem institucional claramente estruturada e pressupõe disputas entre diferentes regimes e níveis de governança global regulatória. As relações entre as partes da ordem geral são 'heterárquicas', não hierárquicas e, muitas vezes, de natureza estritamente política. A estabilidade é criada não por decisões finais, baseadas numa autoridade unívoca e última, mas através de processos de negociação e de compromissos, desafios e concessões constantes entre os diferentes membros da comunidade global"[1203].

Os conflitos de jurisdição surgem quando, para o mesmo utilizador de dados pessoais, há um *duplo fardo,* uma sobreposição de normas, da entidade do foro e da entidade *ad quem*, sujeitando aquele a um conflito *positivo* de imposições de difícil solução uma vez que não existe uma "regra de reconhecimento" ou de conflitos que confira prioridade a uma das normas em concurso[1204]. O resultado é pernicioso em termos de segurança jurídica; além disto, e como P. DE HERT e M. CZERNIAWSKI advertem, vislumbra-se um possível desrespeito pelo *due process* e pelo princípio do *ne bis in idem* em prejuízo dos operadores económicos[1205].

Iluminam-se, pelo menos, dois tipos de conflitos positivos:

(i) O primeiro entre regimes de proteção de dados pessoais de diferentes países. Por exemplo, um utilizador de dados pessoais vinculado pelo RGPD, por força

[1202] C. KUNER, *Transborder* cit., p. 135.
[1203] Nico KRISCH, "The pluralism of global administrative law", *EJIL,* n.º 17, 2006, p. 269 e ss..
[1204] Ralf MICHAELS e Joost PAUWELYN, "Conflict of Norms or Conflict of Laws? Different Techniques in the Fragmentation of International Law", *Duke Scholarship Repository,* 4/2012, disponível em https://scholarship.law.duke.edu/djcil/vol22/iss3/3/, consultado no dia 30 de setembro de 2018.
[1205] P. de HERT e M. CZERNIAWSKI, "Expanding the …" cit., p. 240 e 241.

do art. 3.º, n.º 2, e pela legislação do seu país de origem que prevê disposições divergentes do RGPD em matéria de consentimento, de apagamento e conservação dos dados. Há quem proponha, como solução, a atribuição de uma etiqueta (*tag*) aos dados pessoais de modo a indicar qual a legislação anexa aos mesmos[1206]. Este tipo de conflitos poderá nunca desaparecer se a convergência substantiva entre regimes de proteção de dados pessoais excluir certas questões jurídicas, traduzindo-se apenas num esbatimento de divergências orientado pelo princípio do "mínimo denominador comum".

(ii) O segundo tipo de conflitos reporta-se às situações de incompatibilidade entre o RGPD e obrigações decorrentes de outros domínios do direito estrangeiro. Entre outros, o caso *Microsoft,* já tratado neste trabalho, é um exemplo deste tipo de conflitos. Além dos EUA, as autoridades de países como a China, a India e outros na região do Golfo, podem obrigar responsáveis pelo tratamento ou subcontratantes, abrangidos pelo art. 3.º, n.º 2, a divulgar e comunicar dados pessoais em violação do disposto no art. 48.º do RGPD[1207]. O alerta foi recentemente dado pela ICC, em 2012: "as empresas que tratam dados pessoais em vários países enfrentam cada vez mais pressão dos Estados para cumprir normas e atender a pedidos das respetivas autoridades que entram em conflito com a legislação de proteção de dados pessoais dos países onde operam. O número crescente destes casos é causado, em parte, pelo crescimento explosivo de fenómenos como o uso de servidores para a computação em nuvem localizados em vários territórios, que fornecem serviços eficientes e a baixo custo (...)", e continua "em muitos casos, os pedidos das autoridades de aplicação da lei podem entrar em conflito com aquela legislação (...) e violar os requisitos relativos às transferências de dados pessoais para países terceiros"[1208].

[1206] C. KUNER, *Transborder* cit., p. 136 e Paula BRUENING e Krasnow WATERMAN, "Data tagging for new models of information governance", *EEE Security & Privacy,* n.º 8, setembro-outubro, 2010, p. 64 e ss..
[1207] C. KUNER, *Transborder* cit., p. 137 e 138.
[1208] ICC, "Cross-border law enforcement access to company data – current issues under data protection and privacy law", 7 de fevereiro de 2012, disponível em https://iccwbo.org/publication/icc-policy-statement-on-cross-border-law-enforcement-access-to-company-data-current-issues-under-data-protection-and-privacy-law/, consultado no dia 30 de setembro de 2018.

No RGPD, o art. 50.º, al. d), dispõe que a COM e as autoridades de controlo devem tomar as "medidas necessárias" para a promoção do "intercâmbio e a documentação da legislação e das práticas em matéria de proteção de dados pessoais, nomeadamente no que diz respeito a conflitos jurisdicionais com países terceiros" (50.º al. d)). Para alguns autores, qualquer abordagem *unilateral* regulatória deve ser completada por uma estratégia *multilateral* para encontrar pontos de convergência e resolver conflitos de jurisdição[1209]. No limite, verdadeiramente decisiva é uma harmonização substancial neste domínio[1210].

Enquanto tal não suceder, em grande medida porque não há um tratado global sobre proteção de dados pessoais[1211], estes conflitos, alimentados por um sistema de concorrência de jurisdições e pela ausência de regras claras sobre a jurisdição extraterritorial em geral e, em especial, em relação aos tratamentos de dados pessoais, não são de fácil resolução. Tanto mais é assim porquanto não existe uma entidade internacional encarregue de os dirimir pelo que, como referi na Parte 1, a sua solução partirá de consensos pontuais e de uma estratégia híbrida dos Estados, composta por várias dimensões e frentes, visando um alinhamento dos vários interesses e pretensões concorrentes[1212].

Alguns autores debruçaram-se já sobre critérios para resolver estes conflitos no domínio específico dos tratamentos de dados pessoais e eleger a entidade com jurisdição efetiva num determinado caso. Merece destaque a proposta de D. SVANTESSON e R. POLCAK sugerindo um método assente num exercício de ponderação com os seguintes eixos:

(i) Na *conexão substancial*: seja a localização física dos dados, a localização da sede do RT/ST, a nacionalidade do titular dos dados, entre outros;

[1209] C. REED, *Making Laws* cit., p. 362 e P. de HERT e M. CZERNIAWSKI, "Expanding the …", cit., p. 241.
[1210] C. KUNER, "Data Protection Law and (Part 2) …" cit., p. 242.
[1211] Muitas expetativas são depositadas na Convenção n.º 108 do CdE, v. G. GREENLEAF, "Modernising Data ..." cit., p. 430 e ss. e, no discurso do Secretário Geral do CdE, "Convention 108: from a European reality to a global treaty", 17 de junho de 2016, disponível em https://www.coe.int/en/web/secretary-general/-/-convention-108-from-a-european-reality-to-a-global-treaty-, consultado no dia 30 de setembro de 2018.
[1212] K. HON, *Data Localization* cit., p. 314.

(ii) Nos *interesses legítimos* das jurisdições em confronto: a proteção dos dados pessoais e os direitos fundamentais, a cibersegurança, a investigação criminal, entre outros; e

(iii) Na *ponderação* entre estes interesses e outros: o interesse dos utilizadores de dados pessoais, do comércio internacional e da comunidade internacional em geral[1213].

1.4.A determinabilidade da extraterritorialidade

Aplicar o art. 4.º da Diretiva nunca foi uma tarefa fácil[1214]. A utilização de uma linguagem jurídica específica, com conceitos autónomos, como o de RT e de ST, levou o seu tempo a sedimentar[1215]. Além disso, a estatuição de conceitos abertos, como o de "estabelecimento" ou de "contexto das atividades", o acentuar das diferenças de implementação entre os Estados-Membros e das divergências de interpretação entre as autoridades de controlo não ajudaram. A COM identificou estes problemas no relatório sobre a implementação da Diretiva[1216] e num estudo que recomendava, com urgência, "normas mais claras e menos ambíguas em matéria de lei aplicável"[1217]. A complexidade e a falta de clareza das obrigações e, sobretudo, dos seus destinatários, dificultam o cumprimento, alimentam insegurança jurídica e geram uma desconfiança quanto à validade e credibilidade das soluções normativas que podem ser confundidas com declarações de interesse político[1218]. Na perspetiva dos operadores estrangeiros trata-se de saber, afinal, se o DUE se lhes aplica ou não[1219].

Nos capítulos 1 e 2 desta parte da tese aflorei o problema da falta de determinabilidade do regime em apreço[1220]. Decisões do TJ como *Google Spain* e

[1213] D. SVANTESSON e R. POLCAK*, Information Sovereignty* cit., p. 140.
[1214] D. KORFF, "EC Study on …" cit., p. 42 e ss.; D. SVANTESSON, "Article 4 …" cit., p. 210 e ss. e, do mesmo autor, "Extraterritoriality …" cit., p. 226 e ss.; L. BYGRAVE, *Data Privacy Law* cit., p. 199; L. COLONNA, *Legal* cit., p. 339; L. MOEREL, *Binding corporate* cit., p. 74; M. BRKAN, "Data Protection …" cit., p. 325.
[1215] G29, "Parecer 1/2010 ..." cit., p. 10.
[1216] Comissão Europeia, "Primeiro relatório ..." cit., p. 17.
[1217] "Estudo comparativo sobre as abordagens diferentes relativamente aos novos desafios à privacidade, em especial à luz dos desenvolvimentos tecnológicos", Janeiro de 2010.
[1218] M. GOMANN, "The new territorial …" cit., p. 580 e 588 e P. de HERT e M. CZERNIAWSKI, "Expanding the …", cit., p. 240.
[1219] M. BRKAN, "Data Protection …" cit., p. 324 e ss.; P. ASENSIO, "Competencia …" cit., p. 77; P. de HERT e M. CZERNIAWSKI, "Expanding the …", cit., p. 239 e S. CARULLA, "Aplicación Territorial ..." cit., p. 82.
[1220] V. ponto 1.4.2.1.3. sobre as "desvantagens de um sistema assente no princípio da responsabilidade" e na análise dos casos *Google Spain* e *Weltimmo* no ponto 2.2.1.1.

Weltimmo resultam disso mesmo, em especial da linguagem aberta da Diretiva e da interpretação de conceitos indeterminados como "estabelecimento" ou "contexto das atividades"[1221]. Por conseguinte, com base no caso *Google Spain*, há quem defenda que alguma insegurança jurídica é o preço a pagar para garantir a tutela dos direitos fundamentais em face dos constantes desenvolvimentos tecnológicos[1222]. Se, com o tempo, alguns conceitos se vão sedimentando, o RGPD, no art. 3.º, introduz novidades que originaram várias dúvidas e ambiguidades quanto ao seu real âmbito de aplicação[1223]. Aliás, como já referi, considera-se que um dos aspetos mais controversos da reforma de 2012 é a delimitação geográfica do âmbito de aplicação do RGPD[1224].

A abertura e adaptabilidade do direito investe o legislador, e as autoridades de controlo neste caso, a nível nacional ou europeu, de uma responsabilidade acrescida de esclarecer o âmbito de aplicação do art. 3.º, bem como de acautelar as potenciais divergências interpretativas entre as autoridades de controlo. Por este motivo, é surpreendente que desde a adoção do RGPD, em 2016, e Setembro de 2018, o G29 não haja adotado linhas de orientação sobre este artigo, ao contrário do que vem fazendo em relação a outros. Espera-se que, em breve, esta lacuna seja colmatada.

No que concerne ao número 1 há vários aspetos que suscitam dúvidas:

(i) Desde logo, os tratamentos realizados por um RT que recorre a uma *server farm,* situada no território de um Estado-Membro, gerida por um prestador de serviços de computação de nuvem estabelecido ali (um ST), ficam abrangidos por este regime[1225]? Ou seja, será possível considerar o ST como um "estabelecimento" do RT[1226]?

[1221] M. GOMANN, "The new territorial …" cit., p. 581, invocando o considerando 4 da Diretiva para demonstrar que o legislador antecipava a instabilidade da matéria que se propunha regular.

[1222] M. GOMANN, "The new territorial …" cit., p. 581 e Spiecker DOHMAN, "A new framework for information markets: Google Spain", *CMLR,* n.º 52, 2015, p. 1042.

[1223] D. SVANTESSON, "Extraterritoriality and …" cit., p. 232 e, do mesmo autor, "Article 3 ..." cit., p. 8; M. GOMANN, "The new territorial …" cit., p. 570 e 582; P. HERT e M. CZERNIAWSKI, "Expanding …" cit., p. 239 e 242; P. ASENSIO, "Competencia …" cit., p. 85 e ss..

[1224] D. SVANTESSON, "Extraterritoriality and …" cit., p. 230; O. TENE e C. WOLF, "Overextended …" cit., p. 10.

[1225] Uma nota que vale a pena salientar: em geral, o cliente do serviço de computação em nuvem determina a finalidade última do tratamento, decide sobre a externalização desse tratamento e a delegação da totalidade ou de parte das atividades de tratamento numa organização externa. Por esse motivo atua como RT. Contudo, pode haver situações em que o prestador de serviços é considerado o RT, como quando procede ao tratamento dos dados para as suas próprias finalidades, v. G29, "Parecer 5/2012 relativo a computação em nuvem", 1 de julho de 2012, p. 9 e ss..

[1226] Discutindo esta hipótese, K. HON *et alii*, "Data Protection Jurisdiction ..." cit., p. 18 e ss. e, da mesma autora, "GDPR's extra-territoriality ..." cit., p. 26.

(ii) Depois, se, como defendeu o G29, a mera pertença a um grupo de empresas não basta para desencadear a aplicação do art. 3.º, n.º 1, quais são os "fatores indicativos"[1227] que determinam a aplicação daquela disposição à empresa-mãe? Permanece válida a posição de algumas autoridades de controlo, no passado, propondo como critérios a existência de clientes na UE da empresa-mãe estrangeira ou sua participação na administração e gestão dos dados pessoais dos clientes da subsidiária[1228]?

(iii) Por fim, interpretações com algum peso institucional – como a do relator do PE do RGPD – deste artigo geram ainda mais dificuldades e equívocos ao avançar como critério decisivo da aplicação do RGPD a localização dos dados pessoais no território de um Estado-Membro[1229]. Contudo, a meu ver, neste ponto pelo menos, o G29 foi claro: "O G29 sublinha que a localização dos dados pessoais não é o critério usado pelo RGPD para definir o seu âmbito territorial"[1230].

Em relação ao número 2 do artigo 3.º outras tantas questões se podem enunciar:

(i) Recordo que conclui que o critério determinante é a localização do titular dos dados no território da UE. Mas, pergunta-se: em que momento e durante quanto tempo?[1231]. Uma das hipóteses, alinhada com a pretensão de maximizar a proteção dos dados pessoais, é que bastaria que o titular dos dados se encontrasse na UE no momento em que os dados são recolhidos[1232]. Outra alternativa exige que o titular se encontre no território da UE *enquanto* os dados pessoais são tratados pelo utilizador sem estabelecimento na UE[1233];

[1227] Deixados em aberto em G29, "Update …" cit., Anexo 2, p. 1.
[1228] Como foi o caso da autoridade do Estado de Hessen, v. "Report of the Hessen DPA for 2001", Hessischer Landtag Drucksache 15/4659, 26 de novembro de 2002, n.º 7.6.
[1229] V. "Brief of *Amici Curiae* Jan Philipp Albrecht …" cit., p. 5 e 14 (afirmando que "os dados pessoais localizados no território da UE estão sujeitos a regras rigorosas desenhadas para manter a autonomia do indivíduo afetado" e que o regime de proteção de dados tem a "intenção específica de abranger os dados pessoais armazenados num Estado-Membro da UE").
[1230] G29, "Statement on electronic evidence", Bruxelas, p. 5.
[1231] Jan ALBRECHT, "Das Neue …" cit., p. 88 e ss. e P. VOIGT e A. BUSSCHE, *The EU General* cit., p. 28.
[1232] P. VOIGT e A. BUSSCHE, *The EU General* cit., p. 29.
[1233] J. ALBRECHT, "Das Neue …" cit., p. 90.

(ii) A alínea a) desta norma suscita várias dúvidas, designadamente a falta de sofisticação e rigor do critério da *intenção* do utilizador de dados pessoais em dirigir as suas atividades para a União[1234]:

a) Em primeiro lugar, estranha-se o desprezo, no considerando 23, pelas tecnologias de geo-localização, manifestamente úteis para apurar se uma atividade é "dirigida" ou não para um determinado território[1235].

b) Depois, imagine-se que não é possível reconstruir a *intenção* do RT porque, por exemplo, o *site* está em inglês e os pagamentos são em *bitcoin*?[1236]

c) Em terceiro lugar, sugere-se que o critério da *intenção* seja densificado por contributos do direito internacional privado como, por exemplo, o critério do "centro de gravidade" da relação jurídica entre o utilizador dos dados pessoais e o respetivo titular[1237].

d) Por fim, e se o titular dos dados pessoais situado na UE deliberadamente escolhe um prestador de serviços que não dirige a sua atividade para ali[1238]? Será o caso, por exemplo, de um estudante chinês que frequenta um programa de Erasmus em Portugal e que encomenda o seu chá favorito de uma loja *online* Chinesa[1239]. Não parece haver aqui qualquer tipo de intenção da loja chinesa em direcionar as suas ofertas para o mercado da União.

[1234] D. SVANTESSON, "Extraterritoriality and…" cit., p. 232; M. BRKAN, "Data Protection …" cit., p. 338 e, da mesma autora, "The Unstoppable …" cit., p. 836; P. de HERT e M. CZERNIAWSKI, "Expanding the …" cit., p. 239 e P. ASENSIO, "Competencia …" cit., p. 85.
[1235] Em sentido próximo, v. M. BRKAN, "The Unstoppable …" cit., p. 836.
[1236] Referindo que é esse o caso de alguns jogos em linha, M. GOMANN, "The new territorial …" cit., p. 586.
[1237] P. de HERT e M. CZERNIAWSKI, "Expanding the …" cit., p. 241.
[1238] M. GOMMAN adianta o exemplo do *video streaming* e a hipótese de o titular dos dados utilizar ferramentas técnicas (como a rede *Tor*) para despistar o *geo-blocking* do RT/ST sem estabelecimento na UE, v. M. GOMANN, "The new territorial …" cit., p. 586.
[1239] M. BRKAN, "The Unstoppable …" cit., p. 836.

(iii) Por seu turno, quanto à aplicação do art. 3.º, n.º 2, al. b), uma vez que este critério não conhece precedentes, as dúvidas centram-se na delimitação das atividades de tratamento qualificáveis como implicando um "controlo do comportamento dos titulares dos dados" como, por exemplo, as realizadas pelos chamados *wearables* e *smart devices* equivalentes, como os relógios e as pulseiras *fitness*[1240]. Segundo o considerando 24, essa delimitação passa por determinar se o titular dos dados "é seguido na Internet" e por apurar a "potencial utilização subsequente" de certas técnicas de tratamento de dados para a definição de perfis. Este segundo critério é particularmente problemático uma vez que pressupõe um juízo de prognose sobre a vontade "potencial" do utilizador dos dados pessoais[1241].

(iv) Por fim, pergunta-se se o RGPD se aplica ao tratamento de dados pessoais realizado por autoridades públicas de países terceiros que controlam comportamentos para efeitos de vigilância?[1242] Na verdade, o art. 27.º, n.º 2, al. b), ao excecionar da obrigação de designar um representante as "autoridades ou organismos públicos" pressupõe que o art. 3.º, n.º 2, se aplica a estas autoridades.

Chamo ainda a atenção para um ponto paradoxal: o balizamento do direito à ação judicial segundo o art. 79.º, n.º 2, do RGPD. Esta disposição prevê, como referi, dois critérios para determinar a competência dos tribunais dos Estados-Membros: o local do estabelecimento do utilizador dos dados pessoais ou em alternativa o recurso pode ser interposto no tribunal do Estado-Membro da residência habitual do titular dos dados pessoais. Quer isto dizer que, em relação aos tratamentos de dados pessoais realizados por um utilizador de dados pessoais sem estabelecimento na União, abrangido pelo art. 3.º, n.º 2, um titular dos dados não residente na UE poderia reclamar para a autoridade de controlo, mas não teria direito a uma ação judicial por via do art. 79.º. Com efeito, o

[1240] B. ALSENOY, "Reconciling …" cit., p. 88; Els KINDT, "Why research may no longer be the same: about the territorial scope of the new data protection regulation", *CMLR,* n.º 32, 2016, p. 738 e ss.; L. COLONNA, "Article 4 …" cit., p. 215; M. GOMANN, "The new territorial …" cit., p. 588.
[1241] M. GOMANN, "The new territorial …" cit., p. 587.
[1242] M. GOMANN, "The new territorial …" cit., p. 588 e M. BRKAN, "The Unstoppable …" cit., p. 836: "nada no texto do artigo 3(2)(b) sugere que as autoridades públicas estrangeiras que vigiam empresas e pessoas da UE estão excluídas do mesmo".

utilizador dos dados não tem estabelecimento na União e, por seu turno, o titular dos dados não preenche a condição imposta pelo critério alternativo do Estado-Membro da residência. Portanto, parece que a tutela conferida aos titulares dos dados não residentes será, nestes casos, *parcial*.

Nestas situações do art. 3.º, n.º 2, o titular dos dados pessoais não residente no território da União poderá utilizar a via judicial apenas na sequência de um recurso da decisão da autoridade de controlo, nos termos do art. 78.º. Esta norma, por um lado, reconhece, no número 1, legitimidade ativa a "todas as pessoas singulares ou coletivas" e, por outro lado, no número 3, estipula que o critério para atribuir competência aos tribunais é o do Estado-Membro onde se encontra estabelecida a autoridade de controlo.

Capítulo 2 - Os limites ao regime das transferências

2.1. Em busca de uma definição de "transferência"

O legislador, tanto no RGPD como na Diretiva, eximiu-se de adotar uma definição expressa deste termo. Adicionalmente, na prática, determinar quando ocorre uma transferência de dados pessoais tornou-se mais difícil com os desenvolvimentos tecnológicos como a Internet e, mais recentemente, a computação em nuvem[1243]. Acontece que, por um lado, estas circunstâncias podem enfraquecer a intenção garantística deste regime, colocando em causa a tutela efetiva dos direitos fundamentais e vedando aos titulares dos dados uma antevisão precisa da respetiva situação jurídica[1244]. Por outro lado, a existência ou não de uma transferência desencadeia a aplicação de imposições específicas, nomeadamente a adoção de garantias adequadas, cujo incumprimento é sancionado ao abrigo do art. 83.º, n.º 5, al. c), do RGPD.

O RGPD, no art. 4.º, n.º 23, apenas esclarece o que é um "tratamento transfronteiriço": "a) O tratamento de dados pessoais que ocorre no contexto das atividades de 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) O

[1243] SEPD, "Opinion of the European …" cit., ponto 108; G29, "Working Document on surveillance ..." cit., p. 51. No mesmo sentido, v. Gloria FUSTER, "Un-mapping Personal Data Transfers", *EDPL,* n.º 2, 2016, p. 160 e ss. e José Piñar MAÑAS, "Transferencias de datos personales a terceros países u organizaciones internacionales", J. Piñar MAÑAS *et alii*, *Reglamento General* cit., p. 427 e ss..
[1244] C. KUNER, *Transborder* cit., p. 174 e K. HON, *Data Localization* cit., p. 69 e ss..

tratamento de dados pessoais que ocorre no contexto das atividades de um único estabelecimento de um responsável pelo tratamento ou de um subcontratante, mas que afeta substancialmente, ou é suscetível de afetar substancialmente, titulares dos dados em mais do que um Estado-Membro". Por seu turno, o art. 48.º distingue "divulgação" de dados pessoais de "transferência" dos mesmos, sem esclarecer o critério distintivo.

No passado, o G29 identificou três situações-tipo de transferência: i) a comunicação de dados pessoais por um RT estabelecido na UE para outro RT estabelecido num país terceiro; ii) a comunicação por um RT estabelecido na UE para um ST estabelecido num país terceiro; iii) a comunicação por uma pessoa estabelecida na UE a um RT estabelecido num país terceiro[1245]. Por conseguinte, uma transferência é uma "comunicação" de dados pessoais, com origem na UE, realizada por RT ou por pessoas (singulares e coletivas?) ali estabelecidas. Porém, julgo que esta tipologia se encontra desatualizada ao excluir, por exemplo, as comunicações realizadas por um ST estabelecido na UE para o RT fora dali. Imagine-se que uma empresa chinesa decide armazenar os seus dados pessoais numa *server farm* de um ST estabelecido em Espanha. Terá o ST espanhol de adotar uma garantia adequada para enquadrar as transmissões de dados e os acessos remotos da empresa chinesa à sua *server farm?* Ou será que o ST espanhol pode ser considerado um estabelecimento do RT chinês, estando este abrangido pelo art. 3.º, n.º 1, do RGPD[1246]? Neste caso não terá de celebrar um contrato de subcontratação, nos termos do artigo 28.º do RGPD?

Adicionalmente, na prática, a tipologia do G29 não serviu de modelo nem para as próprias instituições europeias.

Com efeito, mais de uma década volvida desde a adoção da Diretiva, a COM perguntava, num documento enunciado "perguntas mais frequentes", "[o] que é uma transferência de dados pessoais?" [1247]. Ao invés de recorrer à tipologia do G29, a COM respondeu que "o termo é com frequência associado a um ato de enviar ou transmitir dados pessoais de um país para outro, por exemplo pelo envio de papel ou de documentos eletrónicos, contendo dados pessoais, pelo correio ou por e-mail. Outras situações que

[1245] G29, "Primeiras orientações ..." cit., p. 12.
[1246] Há quem defenda esta segunda hipótese, amparando-se na interpretação "mínima" que o TJ vem fazendo sobre o conceito de estabelecimento. Porém, tal teria para a competitividade dos subcontrantes europeus, v. K. HON *et alii*, "Data Protection Jurisdiction ..." cit., p. 18 e ss. e, da mesma autora, "GDPR's extra-territoriality ..." cit., p. 26.
[1247] Comissão Europeia, "Frequently Asked Questions Relating To Transfers of Personal Data From the EU/EEA to Third Countries", 2009, , disponível em http://ec.europa.eu/justice_home/fsj/privacy/docs/international_transfers_faq/international_transfers_faq.pdf, consultado no dia 30 de setembro de 2018.

também cabem nesta definição são todos os casos em que há uma ação do responsável pelo tratamento de disponibilização dos dados pessoais a um terceiro localizado num país terceiro"[1248]. Esta explicação da COM evidencia as ambiguidades que rodeiam este conceito que, "com frequência", é o ato de transmitir dados pessoais para outro país por exemplo por correio, mas, por outro lado, também inclui "todos os casos" em que há um comportamento imputável ao RT de dar o acesso aos dados pessoais a terceiros, situados num país terceiro[1249].

Estes dois exemplos, do G29 e da COM, exemplificam a falta de consenso em torno da definição de transferência. Esta tese é confirmada pela evolução da jurisprudência do TJ (2.1.1) e pelas decisões e posições das autoridades de controlo e do SEPD (2.1.2) que me proponho apresentar, de forma sistematizada e com o intuito de, no final, fornecer um guião interpretativo minimamente coeso deste termo (2.1.3).

2.1.1. Na jurisprudência do TJ

2.1.1.1.O caso *Lindqvist*

Nesta decisão, entre outros aspetos[1250], o TJ entendeu *não* haver uma transferência "quando uma pessoa que se encontra num Estado-membro insere numa página Internet, armazenada num fornecedor de serviços de anfitrião que está estabelecido nesse mesmo Estado, dados de caráter pessoal, tornando-os deste modo acessíveis a qualquer pessoa que se ligue à Internet"[1251]. Para chegar a esta conclusão aquela instância analisou dois elementos:

(i) A "natureza técnica das operações" efetuadas pela pessoa em causa, a senhora B. LINDQVIST*;* e

(ii) o "objetivo e a economia do capítulo IV" da Diretiva[1252].

[1248] Comissão Europeia, "Frequently …" cit., p. 18.
[1249] Criticando, v. G. FUSTER, "Un-mapping …" cit., p. 161.
[1250] Acórdão do TJ, Bodil Lindqvist c. Göta hovrätt, 6 de novembro de 2003. As outras questões em juízo prendem-se com o tipo de tratamento de dados pessoais em causa como, por exemplo, saber se a referência, feita num sítio *web,* a várias pessoas e a sua identificação pelo nome ou por outros meios (n.º de telefone, informações sobre o trabalho ou passatempos) constitui um tratamento de dados pessoais (n.º 19 e ss.); averiguar a aplicação da exceção do art. 3.º, n.º 2 da Diretiva (n.º 29 e ss.); apurar se a expressão "dados relativos à saúde", usada no art. 8.º, n.º 1 da Diretiva, inclui informações relativas a todos os aspetos, quer físicos quer psíquicos, da saúde de uma pessoa (n.º 49 e ss.).
[1251] Acórdão do TJ, Bodil Lindqvist c. Göta hovrätt, 6 de novembro de 2003, n.os 69 a 71.
[1252] Acórdão do TJ, Bodil Lindqvist c. Göta hovrätt, 6 de novembro de 2003, n.º 57.

Quanto ao primeiro aspeto, o TJ considerou que "para obter as informações que constam das páginas Internet nas quais B. LINDQVIST inserira dados relativos aos seus colegas, um utilizador da Internet devia não apenas ligar-se a esta como também efetuar, a título pessoal, as ações necessárias para consultar as referidas páginas. Por outras palavras, as páginas da Internet criadas por B. LINDQVIST não incluíam os mecanismos técnicos que permitiriam o envio automático dessas informações a pessoas que não tinham deliberadamente tentado aceder a essas páginas"[1253]. Acrescentou ainda, ao que me parece tratando a transferência como uma *transmissão direta,* que "nas circunstâncias como as do caso em análise (...) os dados de caráter pessoal que chegam ao computador de uma pessoa situada num país terceiro, provenientes de uma pessoa que os carregou num sítio *web*, não foram transferidos diretamente entre essas duas pessoas, mas através da infraestrutura informática do fornecedor de serviços de anfitrião onde a página está armazenada"[1254]. Daí que "as operações como as que foram efetuadas por B. LINDQVIST não constituem em si mesmas uma 'transferência para um país terceiro de dados'"[1255].

A este propósito, o TJ esclareceu que o âmbito da sua análise e as suas conclusões se limitam às operações de B. LINDQVIST, isto é, ao *upload*, "com exclusão das [operações] efetuadas pelos fornecedores de serviços de anfitrião", designadamente o armazenamento dos dados pessoais descarregados por B. LINDQVIST e a disponibilização dos mesmos a partir do respetivo servidor[1256]. Ou seja: o tribunal não apreciou a "natureza técnica" daquelas operações deixando em aberto o papel do fornecedor de serviços de anfitrião nos casos de transferências.

No que toca ao segundo aspeto, o TJ aplicou um teste de razoabilidade[1257]*,* de índole pragmática, para afirmar que a existência de uma transferência *in casu* implicaria a aplicação do art. 25.º sempre que são carregados dados pessoais num sítio *web*, tornando essa norma um "regime de aplicação geral" a todos os países terceiros onde é possível aceder à Internet[1258]. Ora, para o tribunal, o Capítulo IV da Diretiva é um "regime especial", com "regras complementares", pelo que não deve ser de aplicação geral ao universo da Internet[1259].

[1253] Acórdão do TJ, Bodil Lindqvist c. Göta hovrätt, 6 de novembro de 2003, n.º 60.
[1254] Acórdão do TJ, Bodil Lindqvist c. Göta hovrätt, 6 de novembro de 2003, n.º 61.
[1255] Acórdão do TJ, Bodil Lindqvist c. Göta hovrätt, 6 de novembro de 2003, n.º 70.
[1256] Acórdão do TJ, Bodil Lindqvist c. Göta hovrätt, 6 de novembro de 2003, n.º 68.
[1257] D. SVANTESSON, "Privacy, the Internet and …" cit., p. 15.
[1258] Acórdão do TJ, Bodil Lindqvist c. Göta hovrätt, 6 de novembro de 2003, n.º 69.
[1259] *Ibidem*.

As análises doutrinais deste caso são bastante críticas[1260]. O apontamento que aqui destaco, tendo em conta o objeto do meu estudo, é a conclusão minimalista do TJ[1261]. Com efeito, além de não apresentar uma definição de transferência, a análise dos factos é bastante limitada. É que, em regra, quando se utiliza um terceiro, um fornecedor de serviços de anfitrião, equacionam-se operações de tratamento de dados pessoais, pelo menos, em três diferentes níveis:

(i) O *upload* para os servidores daquele;

(ii) O armazenamento dos dados pessoais;

(iii) O acesso e o possível *download* sempre que alguém visita o sítio *web*.

As conclusões da instância da UE limitam-se ao *upload* dos dados pessoais, apesar de reconhecer que o recurso a uma terceira entidade poderá significar uma dispersão dos dados pessoais por vários locais se a respetiva infraestrutura, os seus servidores e centros de armazenamento, se encontram na UE e/ou fora dela: "[o]s computadores que constituem esta infraestrutura informática podem estar situados, estando mesmo frequentemente situados, num ou em vários países que não o lugar de estabelecimento do fornecedor de serviços de anfitrião, sem que a clientela deste último tenha ou possa razoavelmente ter conhecimento da sua existência"[1262].

Ao contrário daquele que, como demonstrarei, vem sendo o entendimento de algumas autoridades de controlo, o TJ descurou os potenciais riscos do armazenamento dos dados pessoais num país terceiro. Porquê? Julgo que há duas circunstâncias do caso concreto

[1260] C. KUNER, *European Data Protection* cit., capítulo 4.08; D. SVANTESSON, "The regulation of …" cit., p. 185; K. HON, *Data Localization* cit., p. 78 e ss.; Y. POULLET, "Transborder Data …" cit., p. 141e ss..

[1261] A doutrina não poupou as considerações do TJ sobre a natureza automática e direta da transmissão e a irrelevância conferida ao acesso aos dados pessoais por pessoas situadas em países terceiros. Para existir uma transferência, defendem alguns, o critério essencial deveria ser a mera *possibilidade* do acesso, um aspeto que passou ao lado das considerações do TJ. D. SVANTESSON critíca o raciocínio do TJ expondo uma situação caricata: sendo verdade que B. LINDQVIST não transmitiu diretamente o conteúdo daquela página para um utilizador da Internet que não estivesse em linha naquele momento ou que não desenvolveu os passos necessários para visitar aquela página, o mesmo raciocínio levará à conclusão de que uma determinada estação de televisão não fornece programas a quem não liga a sua televisão ou que não escolhe um determinado canal. Depois, aplicando o mesmo raciocínio a outras realidades tecnológicas, há quem entenda que, nos casos de serviços de computação em nuvem será difícil apurar a ocorrência de uma transferência direta e automática. Cfr. C. KUNER, *Transborder* cit., p. 13; D. SVANTESSON, "Privacy, the Internet …" cit., p. 15; S. ESAYAS, "A walk in to the …" cit., p. 669.

[1262] Acórdão do TJ, Bodil Lindqvist c. Göta hovrätt, 6 de novembro de 2003, n.º 59. Enfatizando este ponto, v. K. HON, *Data Localization* cit., p. 77.

que respondem a esta dúvida e explicam a opção do tribunal: por um lado, o prestador de serviços de anfitrião encontrava-se estabelecido na Suécia[1263] e, por outro lado, o servidor que armazenava os dados pessoais descarregados por B. LINDQVIST também[1264]. Ou seja, o tribunal terá partido da premissa de que os dados pessoais não foram efetivamente transferidos para um país terceiro, restringindo-se à Suécia.

As conclusões minimalistas do TJ neste caso, bem como estas duas circunstâncias, fundamentam as interpretações restritivas do mesmo, por exemplo do SEPD[1265] e da doutrina[1266], restringindo-o apenas ao *upload* de dados pessoais para um sítio *web* público, de acesso universal, gerido por um prestador de serviços de anfitrião estabelecido na UE e com servidores ali. Ora, esta apreciação circunscrita não fornece uma resposta final para o meu propósito, de delimitar o conceito em apreço e, aliás, abriu espaço para novas interpretações.

2.1.1.2.O caso *Schrems*

A hipótese tratada nesta decisão será aprofundada adiante. Por agora, saliento que o TJ não seguiu o mesmo caminho interpretativo que em *Lindqvist* e preencheu a definição de transferência de dados pessoais com base na letra do art. 2.º da Diretiva: "a transferência de dados pessoais de um Estado-Membro para um país terceiro constitui (...) um tratamento de dados pessoais na aceção do artigo 2.º, alínea b), da Diretiva 95/46 (...) efetuado no território de um Estado-Membro. Com efeito, esta disposição define o «tratamento de dados pessoais» como «qualquer operação ou conjunto de operações efetuadas sobre dados pessoais, com ou sem meios automatizados» e indica, a título de

[1263] Acórdão do TJ, Bodil Lindqvist c. Göta hovrätt, 6 de novembro de 2003, n.º 52.
[1264] Acórdão do TJ, Bodil Lindqvist c. Göta hovrätt, 6 de novembro de 2003, n.º 18, pergunta 5.
[1265] SEPD, "The Transfer of Personal Data to Third Countries and International Organisations by EU Institutions and Bodies", 14 de julho de 2014, p. 6, disponível em https://edps.europa.eu/sites/edp/files/publication/14-07-14_transfer_third_countries_en.pdf, consultado no dia 30 de setembro de 2018: "As conclusões do Tribunal devem ser contextualizadas" sendo que a avaliação do caso deve ter em conta as "circunstâncias tais como as do caso em concreto". O Supervisor prossegue referindo que "[o] Tribunal não tratou de outros tipos de tratamento – diferentes, por exemplo, em termos de escala, intenção, riscos, etc. – a não ser do *upload* de dados pessoais para uma página da Internet nas circunstâncias concretas do caso (o que a Senhora Lindqvist queria era somente informar a sua comunidade). A conclusão do tribunal sobre a noção de "transferência" não deve, por isso, ser automaticamente aplicada aos casos com caraterísticas diferentes deste".
[1266] C. KUNER, *Transborder* cit., p. 13 e, do mesmo autor, *European Data Protection* cit., capítulo 4.08; J. Piñar MAÑAS, "Transferencias ..." cit., p. 433; D. SVANTESSON, "Privacy, the Internet …" cit., p. 15; K. HON, *Data Localization* cit., p. 69 e 86; Roger BAKER, "Offshore IT outsourcing and the 8th Data Protection Principle: legal and regulatory requirements – with reference to financial services", *IJLIT,* vol. 14, n.º 1, 2006, p. 7

exemplo, a «*comunicação por transmissão, difusão ou qualquer outra forma de colocação à disposição*»"[1267].

O afastamento do teste formulado em *Lindqvist,* incidente sobre a "natureza técnica das operações" e sobre "o objetivo e a economia do capítulo IV da Diretiva", dever-se-á ao facto de não ter sido levantada a hipótese de existir (ou não) uma operação de transferência no caso concreto, a saber do *Facebook Ireland* para o *Facebook USA*. Porém, a verdade é que o entendimento agora avançado é suficientemente amplo para abranger o *upload* de dados pessoais para uma página na Internet como "forma de colocação à disposição". Ou seja, a aplicação rigorosa deste entendimento implicaria que B. LINDQVIST, ao descarregar os dados pessoais num sítio *web,* os colocou à "disposição" de outras pessoas situadas em países terceiros.

Acontece que, como se não bastasse, a prática das autoridades de controlo, desapegada da letra do art. 2.º da Diretiva, foi acrescentando novas dimensões a este termo.

2.1.2. Na prática das autoridades de controlo

A prática destas autoridades neste campo constitui um exemplo claro da fragmentação interpretativa e da falta de consenso que se pretenderam acautelar com a reforma de 2012 e com a opção legislativa e política de um regulamento. Este é, recordo, um dos principais obstáculos à dimensão integracionista deste regime identificada na Parte II desta tese.

O ICO, por exemplo, defende que o *upload* de dados pessoais num sítio *web* pode, em certas situações, constituir uma transferência: "colocar dados pessoais num sítio *web* resulta com frequência numa transferência para países fora da UE. A transferência ocorrerá quando alguém fora dali acede ao sítio *web*. Se descarregar informação num servidor localizado no Reino Unido para que possa ser acedida num sítio *web*, deverá considerar a probabilidade de ocorrer uma transferência e antecipar se tal é razoável para o titular dos dados. Se quem descarrega a informação no sítio *web* tem a intenção de que a mesma seja acedida fora da UE, então haverá uma transferência[1268]". Noutra ocasião defendeu que "só ocorre uma transferência quando a Internet foi efetivamente acedida

[1267] Acórdão do TJ, Maximillian Schrems c. Data Protection Commissioner, C-363/14, 6 de outubro de 2015, n.º 45.
[1268] ICO, "The Guide to Data Protection", p. 87, disponível em https://ico.org.uk/for-organisations/guide-to-data-protection/principle-8-international/, consultado no dia 30 de setembro de 2018.

por uma pessoa localizada num país terceiro"[1269]. Ainda, fora do contexto específico da Internet, o ICO subscreveu um conceito amplo de transferência, enquanto "transmissão de dados pessoais de um lugar, pessoa, etc. para outro", alargando-o ao caso do funcionário de uma empresa que viaja para fora da UE e leva o computador da empresa consigo[1270].

Já a autoridade de controlo da Holanda recorre ao critério da *intenção* de conferir o acesso aos dados pessoais a terceiros situados em países terceiros. Foi esta a tese sustentada por aquele país no caso *Lindqvist:* uma transferência implica um ato que visa deliberadamente transmitir dados pessoais do território de um Estado-Membro para um país terceiro[1271]; e, em 2007, a mesma posição foi reiterada[1272]. Por seu turno, a autoridade eslovena, nas linhas de orientação sobre computação em nuvem, avança um critério semelhante ao da intenção: ocorre uma "transferência" sempre que o acesso remoto a dados pessoais armazenados na UE é autorizado (a expressão usada é *enabling*) a terceiros que se acham fora do território daquela[1273].

Por seu turno, o SEPD define "transferência" como a "comunicação, revelação ou outra forma de disponibilização de dados pessoais, realizada com o conhecimento e a intenção de um sujeito, abrangido pelo DUE, de que o destinatário terá acesso aos dados"[1274]. Esta foi também a definição citada, recentemente, pelo G29 para colmatar a lacuna da Diretiva[1275] bem como a proposta, que não singrou, do relator do RGPD, J. ALBRECHT, para o art. 4.º, n.º 3, al. a): "qualquer comunicação de dados pessoais, ativamente disponibilizada a um número limitado de partes identificadas, com o conhecimento ou intenção do remetente de dar ao destinatário acesso aos dados

---

[1269] ICO, "The eigth data protection principle and international data transfers", versão 4.1., n.º 21, disponível em https://ico.org.uk/media/for-organisations/documents/1566/international_transfers_legal_guidance.pdf, consultado no dia 30 de setembro de 2018.

[1270] ICO, "The eigth ..." cit., n.º 18 e "The Guide ..." cit., p. 91.

[1271] "(…) o conceito de 'transferência' (…) deve ser entendido como tendo por objeto um ato que visa deliberadamente transferir dados de caráter pessoal do território de um Estado-Membro para um país terceiro", Acórdão do TJ, Bodil Lindqvist c. Göta hovrätt, 6 de novembro de 2003, n.º 54.

[1272] College bescherming persoonsgegevens (autoridade de controlo holandesa), "Publication of Personal Data on the Internet", dezembro de 2007, p. 50, disponível em https://autoriteitpersoonsgegevens.nl/sites/default/files/downloads/mijn_privacy/en_20071108_richtsnoeren_internet.pdf, consultado no dia 30 de setembro de 2018.

[1273] Information Commissioner, "Personal Data Protection & Could Computing", 2012, secção 3.4., disponível em https://www.ip-rs.si/fileadmin/user_upload/Pdf/smernice/Cloud_computing_and_data_protection_-_ENG_final.pdf, consultado no dia 30 de setembro de 2018.

[1274] SEPD, "The Transfer of Personal Data to Third Countries and International Organisations by EU Institutions and Bodies", 14 de julho de 2014, p. 7. Esta posição encontrava-se já na opinião do SEPD de 2012, sobre a reforma de proteção de dados, v. ""Opinion of the ..." cit., p. 109.

[1275] G29, "Working Document on surveillance ..." cit., p. 37.

pessoais"[1276]. Na doutrina K. HON defende que "sempre que há o acesso aos dados pessoais por uma pessoa localizada num país terceiro ocorre uma 'transferência', mas só se o remetente teve a intenção (ou é razoavelmente possível presumir essa intenção) de permitir o acesso"[1277].

Mas esta viagem pela prática das autoridades de controlo ficaria incompleta sem uma explicação de outro critério: a localização geográfica dos dados pessoais. Decisivas serão as "movimentações físicas" dos dados pessoais pelo que, por exemplo, se um utilizador de dados pessoais estabelecido na UE utiliza centros de armazenamento ou servidores fora dali realizará "transferências", como sucedeu no caso *SWIFT*. O G29 considerou aquela entidade, estabelecida na Bélgica, um RT, porquanto havia tomado decisões como a escolha do *mirror* (cópia automática) dos dados pessoais, armazenados em servidores na Bélgica, para os EUA[1278]. Entendeu, por isso, que essa operação era uma transferência para os servidores, localizados nos EUA, da própria *SWIFT*[1279]. Por conseguinte, mesmo um utilizador de dados pessoais estabelecido na UE, que trata os dados pessoais *in-house,* sem recorrer aos serviços de terceiros, realiza transferências para um país terceiro onde armazena os dados numa infraestrutura própria[1280]. Por outras palavras: segundo este critério ocorre uma transferência sempre que os dados pessoais são "movidos" para uma infraestrutura localizada num país terceiro (servidores, centros de dados ou outro tipo de *hardware*).

Numa opinião mais recente, sobre publicidade comportamental *online*, uma transferência verifica-se quando os dados são transmitidos para "servidores localizados em países terceiros"[1281]. Em 2012, a propósito da computação em nuvem, reconhecendo alguns aspetos fundamentais desta tecnologia ("os dados pessoais podem ser mantidos de forma redundante em diferentes servidores e em diferentes locais"[1282] ou "frequentemente, intervêm prestadores de serviços de grandes dimensões com

[1276] Alteração 86, "I Draft Report on the proposal for a regulation of the European Parliament and of the Council on the protection of individual with regard to the processing of personal data and on the free movement of individual with regard to the processing of personal data and on the free movement of such data", de 16 de janeiro de 2013, disponível em http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-%2F%2FEP%2F%2FNONSGML%2BCOMPARL%2BPE-501.927%2B04%2BDOC%2BPDF%2BV0%2F%2FEN, consultado no dia 30 de setembro de 2018.
[1277] J. Piñar MAÑAS, "Transferencias ..." cit., p. 433 e K. HON, *Data Localization* cit., p. 90.
[1278] G29, "Parecer 10/2006 ..." cit., p. 11.
[1279] Importa sublinhar a inexistência de um terceiro destinatário dos dados pessoais distinto da *SWIFT* já que é esta a proprietária dos centros de dados nos EUA, v. G29, "Parecer 10/2006 ..." cit., p. 21 e ss..
[1280] K. HON, *Data Localization* cit., p. 88.
[1281] G29, "Parecer 2/2010 ..." cit., p. 24.
[1282] G29, "Parecer 05/2012 ..." cit., p. 14

infraestruturas complexas. É por essa razão, por a computação em nuvem se poder distribuir por vários locais e os utilizadores poderem não saber exatamente onde estão a ser armazenados os seus dados"[1283]), que o G29 alude em diversos momentos à localização dos servidores/centros de dados e ao local do armazenamento/tratamento[1284], o que sugere o entendimento segundo o qual uma "transferência" inclui os movimentos de dados pessoais para uma infraestrutura situada no estrangeiro[1285].

Com efeito, como referi, o critério da localização dos dados pessoais foi rejeitado para efeitos de delimitar o âmbito de aplicação do regime geral de proteção de dados pessoais, tanto segundo o art. 4.º da Diretiva como segundo o art. 3.º do RGPD[1286], mas tem servido para desencadear a aplicação do regime das transferências de dados pessoais. Por exemplo, na Suécia, tal como no Reino Unido, uma transferência inclui a "viagem" de um computador portátil armazenando dados pessoais[1287]. Em 2011, a autoridade de controlo da Dinamarca, numa opinião sobre o projeto de uma autarquia para utilizar a *Google Apps SaaS*[1288] para o tratamento de dados pessoais na aérea da educação, entendeu que o RT seria o município e o ST a *Google Ireland Ltd.* [1289]. Os dados pessoais seriam armazenados nos servidores da *Google Inc.* "nos EUA e na Europa", apesar de os clientes Europeus "primariamente armazenarem os seus dados pessoais na Europa". O *Datalisynet* entendeu que as comunicações de dados pessoais da *Google Ireland Ltd.* para os centros de dados da *Google Inc.*, nos EUA, configuravam uma transferência, estando abrangidos pelo (ainda vigente) esquema do "porto seguro". Entendimento semelhante tem defendido a autoridade sueca também em casos envolvendo a *Google Apps*[1290].

[1283] *Idem*, p. 30

[1284] *Idem,* p. 5 ("localização dos servidores onde os dados são tratados"), p. 13 ("localização de todos os centros de dados"), p. 28 ("centros de dados espalhados por todo o mundo"), entre outros exemplos.

[1285] K. HON, *Data Localization* cit., p. 96.

[1286] G29, "Statement on electronic evidence", Bruxelas, p. 5.

[1287] K. HON, *Data Localization* cit., p. 245.

[1288] O acrónimo significa *Cloud Software as a Service* correspondendo a um dos modelos de prestação de serviços de nuvem, distinto do IaaS (*Cloud Infrastructure as a Service)* e do PaaS (*Cloud Platform as a Service*). Desenvolvendo as diferenças, v. G29, "Parecer 5/2012 ..." cit., p. 31.

[1289] Datatilsynet, *Processing of sensitive personal data in a cloud situation,* 2011, ponto 3.3., disponível em https://www.datatilsynet.dk/english/processing-of-sensitive-personal-data-in-a-cloud-solution/, consultado no dia 30 de setembro de 2018.

[1290] Datainspektionen, *Salems*, de 28 de setembro de 2011, p. 17, disponível em https://www.datainspektionen.se/Documents/beslut/2011-09-30-salems-kommun.pdf, consultado no dia 30 de setembro de 2018 e Datainspektionen, *Salems*, 31 de maio de 2013, p. 11, disponível em https://www.datainspektionen.se/Documents/beslut/2013-05-31-salems-kommun.pdf, consultado no dia 30 de setembro de 2018. Além dos exemplos apontados veja-se na Alemanha: Konferenz der Datenschutzbeauftragten des Bundes und der Länder & Düsseldorfer Kreises, "Orientierungshilfe: Cloud Computing Version 2.0", outubro de 2014, disponível em https://www.bfdi.bund.de/DE/Infothek/Orientierungshilfen/orientierungshilfen-node.html, consultado no dia 30 de setembro de 2018.

2.1.3. A determinação de uma transferência na prática

Como se vê, uma "transferência" é uma noção de conteúdo variável, determinada com base num conjunto de critérios não articulados entre si. O ideal seria que o CEPD, no âmbito das suas competências, arrumasse todos estes critérios e, eventualmente, avançasse uma noção uniforme. Contudo, nesta matéria vale a pena recordar que *omnis definitio periculosa est,* pelo que se admite que poderá ser uma imprudência firmar este termo num conceito fechado que rapidamente se veja desatualizado face à evolução tecnológica[1291]. Ainda assim, sem tal noção, a dado momento restritiva face ao contexto tecnológico, o que aí porventura se perdesse, ganhar-se-ia em sede de segurança e certeza na aplicação do Direito. Talvez por essa razão o CdE não se tenha escusado de propor, no relatório explicativo da revisão da Convenção n.º 108, a seguinte definição: "uma transferência ocorre quando os dados pessoais são revelados ou disponibilizados a um destinatário sujeito à jurisdição de outro Estado ou organização internacional"[1292]. Esta proposta é composta, essencialmente, por dois elementos que destaco: (i) o tipo de operação de tratamento, de revelação ou disponibilização e (ii) a exigência de que o importador dos dados, o destinatário, está sujeito à jurisdição estrangeira.

O que, pelo menos, caberá ao CEPD, de modo a orientar as atuações dos responsáveis pelo tratamento e subcontratantes, é a publicação de uma grelha de critérios ou de um guião para apurar a existência de uma transferência assente, pelo menos, nos seguintes elementos retirados da análise anterior:

(i) A indefinição diagnosticada não deve ser aproveitada como uma válvula de escape para que o utilizador dos dados pessoais se furte à obrigação de garantir a "continuidade do nível de proteção" do titular dos dados pessoais.

(ii) Uma transferência será uma operação de "divulgação por transmissão, difusão ou qualquer outra forma de disponibilização" dos dados pessoais

[1291] C. KUNER, *Transborder* cit., p. 174.
[1292] CdE, "Draft Explanatory Report: Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data", n.º 99, acordado em maio de 2018 e disponível em https://rm.coe.int/16806b6ec2, consultado no dia 30 de setembro de 2018.

a um utilizador de dados pessoais sujeito à jurisdição de um país terceiro[1293].

(iii) Essa operação deverá ser imputada a um comportamento de um utilizador de dados pessoais que indique a intenção ou o conhecimento de divulgar, difundir ou disponibilizar o acesso aos dados àquele utilizador.

(iv) A localização dos dados pessoais numa infraestrutura informática, num centro de dados ou servidor num país terceiro configura uma transferência de dados pessoais independentemente da relação do importador da mesma com o exportador.

Porém, noto que as orientações do CEDP nesta matéria não se encontram entre as atribuições elencadas no art. 70.º ("Atribuições do Comité") pelo legislador e, além disto, correm o risco de ser desprezadas pelas autoridades de controlo tal como sucedeu, no passado, em relação às situações-tipo identificadas pelo G29[1294].

2.2. A relação entre o regime das transferências de dados pessoais e o âmbito de aplicação da Diretiva e do RGPD

Alguma doutrina suscita dúvidas sobre a relação entre o art. 4.º da Diretiva e o art. 3.º do RGPD e o regime das transferências de dados para países terceiros, apontando uma sobreposição desnecessária entre ambos em certas situações[1295]. A mesma questão foi levantada durante as negociações do RGPD[1296] sendo exponenciada pelas imprecisões, anteriormente tratadas, do conceito de transferência.

[1293] É a expressão referida no art. 4.º, n.º 2 do RGPD, equivalente à expressão da Diretiva, citada pelo TJ no caso *Schrems,* e muito próxima da noção do CdE de "divulgar" ou "disponibilizar". A expressão "outra forma de disponibilização" é de tal modo ampla que não exige o acesso efetivo aos dados pessoais e incluirá o armazenamento de dados pessoais na infraestrutura ou centro de dados, situados em países terceiros, do próprio RT/ST (tal como em *SWIFT*) e, no limite, o *upload* de dados pessoais para um sítio *web* (como em *Lindqvist*).

[1294] G29, "Primeiras orientações ..." cit., p. 12.

[1295] Aleksandra KUCZERAWY, "Facebook and Its EU Users – Applicability of the EU Data Protection Law to US Based SNS in Advances", *Information and Communication Technology,* n.º 320, 2010, p. 75 e ss.; B. MAIER, "How has the law …" cit., p. 162; C. KUNER, *European Data Privacy Law* … cit., p. 119 e, do mesmo autor, *European Data Protection* cit., p. 166 e ss. e "Extraterritoriality and …" cit., p. 244; K. HON, *Data Localization* cit., p. 53, 54 e 87; L. COLONNA, "Article 4 …" cit., p. 215 e, da mesma autora, *Legal Implications* cit., p. 376; R. POLCAK e D. SVANTESSON, *Information Sovereignty* cit., p. 211.

[1296] Conselho da UE, "Preparation of a general approach", doc. n.º 9788/15, 11 de junho de 2015, nota de rodapé 450.

Como assinalam C. KUNER e K. HON aquela sobreposição verificava-se, por exemplo, sempre que os utilizadores de dados pessoais estabelecidos em países terceiros aderiam ao esquema do porto seguro ou adotavam cláusulas contratuais para importar dados pessoais encontrando-se, simultaneamente, abrangidos pelo art. 4.º, n.º 1, al. c), da Diretiva. Aplicando-se esta norma, aqueles utilizadores tornar-se-iam, pelo menos formalmente, utilizadores de dados pessoais equiparados aos utilizadores de dados pessoais situados exclusivamente na UE e, por conseguinte, sujeitos às mesmas imposições em matéria de proteção de dados pessoais – pelo menos em relação aos tratamentos de dados que cabiam na alínea c) da Diretiva[1297]. Num sentido próximo, L. COLONNA apresenta exemplos de situações nas quais o exportador, situado na UE, deverá exigir de um importador abrangido pelo art. 4.º da Diretiva ou pelo art. 3.º do RGPD uma garantia adequada[1298].

Esta doutrina nota que esta é a posição subscrita pelo G29[1299]. Significa isto que, na prática, nestes casos, não há uma verdadeira equiparação entre os utilizadores de dados pessoais *exclusivamente* estabelecidos na UE e os utilizadores *sem* estabelecimento na UE – mas abrangidos pelo DUE – uma vez que, antes de transmitir os dados pessoais, o exportador exige do importador garantias adequadas. O mesmo não se verifica se a transmissão dos dados pessoais tiver como destinatário um utilizador situado exclusivamente na UE. Com efeito, o bizarro desta hipótese de aplicação simultânea daquelas normas prende-se com o facto de ambos os utilizadores de dados pessoais, importador e exportador, estarem abrangidos pela jurisdição prescritiva da UE, mas, apesar disto, os fluxos de dados entre si carecem de enquadramento ao abrigo do regime específico das transferências.

Esta aplicação simultânea do âmbito de aplicação do regime em apreço e das normas das transferências é, segundo C. KUNER, uma solução de "cinto e suspensórios"

[1297] C. KUNER, "Extraterritoriality …" cit., p. 16 e K. HON, *Data Localization* cit., p. 54. Em sentido próximo L. COLONNA, *Legal Implications ...* cit., p. 375 e ss..

[1298] C. KUNER, *European Data Privacy ...* cit., p. 119 e L. COLONNA, *Legal Implications ...,* cit., p. 379.

[1299] KUNER invoca o seguinte trecho do parecer do G29, "Parecer 4/2000 sobre o nível de proteção assegurado pelo conjunto de princípios de 'Porto Seguro'", 16 de maio de 2000, p. 3: "O Grupo lembra que, nos termos do n.º 1 do artigo 4.º da directiva, os Estados-Membros são obrigados a aplicar as suas disposições nacionais não só às operações de tratamento efectuadas pelos responsáveis pelo tratamento dos dados estabelecidos no seu território, mas igualmente aos outros responsáveis que, não estando estabelecidos nesse território, utilizem equipamento aí situado, nomeadamente para a recolha de dados pessoais. O Grupo de Trabalho convida a Comissão a esclarecer no seu projecto de decisão ou na sua carta para o *Department of Commerce* dos EUA que *o "porto seguro" não irá afectar a aplicação do artigo 4.º da directiva*". Cfr. C. KUNER, *European Data Privacy Law* … cit., p. 119. Este entendimento confirma a aplicação simultânea do art. 4.º e do regime das transferências que, neste exemplo, se manifesta na vigência de uma decisão de adequação.

para os tratamentos de dados pessoais realizados no estrangeiro tendo em vista uma proteção reforçada do titular dos dados pessoais[1300]. Não obstante, este autor, acompanhado por outros, apelam, por um lado, a uma maior coordenação entre o regime das transferências e as normas que delimitam o âmbito de aplicação e, por outro lado, sugerem que não devia ser necessário cumprir os requisitos autónomos do regime das transferências quando o DUE *já* se aplica a todos os tratamentos de dados pessoais realizados pelo importador por via das normas que delimitam o âmbito de aplicação do mesmo: "é injusto permitir a livre circulação dos dados pessoais entre responsáveis pelo tratamento localizados no território da União (com base na ideia de que todos esses responsáveis pelo tratamento respeitam o regime de proteção de dados pessoais criando um elevado nível de proteção dos fluxos internos) mas exigir um fundamento específico para as transferências dirigidas a responsáveis pelo tratamento estabelecidos em países terceiros (que também estão vinculados pelo RGPD por força do art. 3.º) simplesmente porque não se encontram localizados exclusivamente no território da União"[1301]. No fundo, esta corrente da doutrina contesta o *duplo fardo* que onera o importador dos dados pessoais nas situações descritas.

Há bons argumentos para concluir que esta tese não foi acolhida, pelo menos expressamente, no RGPD. Em primeiro lugar, não há nenhum indicador nos artigos 44.º e ss. que suporte esta espécie de supletividade do regime das transferências em relação ao âmbito de aplicação. De facto, a estrutura deste regime permanece, no essencial, inalterada no RGPD.

Em segundo lugar, atendendo, por exemplo, aos artigos 40.º, n.º 3 e 42.º, n.º 2, do RGPD, aí se dispõe que *mesmo* os utilizadores de dados pessoais sujeitos àquele diploma, delimitados pelo art. 3.º ("[a]lém dos responsáveis pelo tratamento ou dos subcontratantes sujeitos ao presente regulamento"), podem recorrer aos "códigos de conduta aprovados" e aos "procedimentos de certificação" de modo a "fornecer as garantias apropriadas" no quadro das transferências. Tal significará que mesmo os importadores de dados pessoais abrangidos pelo RGPD, sujeitos à jurisdição da UE e dos seus Estados-Membros e, simultaneamente, à jurisdição do país terceiro onde se encontram, devem apresentar garantias adequadas *e*, adicionalmente, como dispõem aquelas normas na parte final, "assumir compromissos vinculativos e com força executiva, por meio de instrumentos

[1300] C. KUNER, "Extraterritoriality …" cit., p. 16.
[1301] L. COLONNA, *Legal Implications* cit., p. 376.

contratuais ou de outros instrumentos juridicamente vinculativos, no sentido de aplicar as garantias apropriadas, inclusivamente em relação aos direitos dos titulares dos dados".

Em terceiro lugar, objetivamente, tratam-se de operações de tratamento distintas: por um lado, a operação de transferir dados pessoais, imputável a quem os exporta e, por outro lado, os tratamentos de dados pessoais realizados pelo importador, noutra qualidade que não essa, que o colocam sob a jurisdição da UE. Nesse sentido, e em quarto lugar, a razão de ser do excesso de zelo legislativo encontrar-se-á no facto de o importador estar fisicamente num país terceiro, sujeito à jurisdição deste país o que dificulta, como expliquei, a fiscalização dos tratamentos realizados pelo importador[1302]. Ora, a aplicação do regime das transferências neste caso promove uma dose de controlo adicional dos tratamentos de dados realizados pelo importador na sequência da transferência. De facto, esse controlo cabe às autoridades dos vários Estados-Membros que, aliás, o viram ser reforçado depois do caso *Schrems*[1303] através da faculdade de bloquear as operações de transferência[1304].

Em quinto lugar, a inexistência de um compromisso, de uma garantia adequada, por parte do importador, colocaria o exportador numa posição vulnerável: perderia o controlo sobre os tratamentos realizados pelo importador sem qualquer garantia ou compromisso deste a respeito das práticas usadas para os tratamentos dos dados transferidos. A necessidade deste compromisso e a importância que o legislador lhe atribui são evidentes, por exemplo, na exigência adicional de "compromissos vinculativos e com força executiva assumidos pelos responsáveis pelo tratamento ou pelos subcontratantes no país terceiro no sentido de aplicarem as garantias adequadas, nomeadamente no que respeita aos direitos dos titulares dos dados". Estes compromissos devem, nos termos dos artigos 46.º, n.º 2, al. e) e f), acompanhar os códigos de conduta e as certificações.

Em todo o caso, esta hipótese de aplicação simultânea das normas em apreço poderá colidir com certos conceitos de transferência como, por exemplo, o do CdE. De facto, recordando a definição de transferência sugerida pelo CdE, a mesma faz depender a sua verificação da sujeição do importador à jurisdição de outro país: aquela operação apenas ocorrerá "quando os dados pessoais são revelados ou disponibilizados a um destinatário

[1302] K. HON, *Data Localization* cit., p. 54.
[1303] C. KUNER, *Transborder* cit., p.128 e 129; K. HON, *Data Localization* cit., p. 54; L. COLONNA, *Legal Implications* cit., p. 378.
[1304] Conforme prevê o art. 58.º, n.º 2, alínea j), do RGPD.

sujeito à jurisdição de outro Estado ou organização internacional" (itálicos meus)[1305]. Reconhecendo a falta de clareza em relação à categoria de jurisdição pressuposta nesta definição, a mesma é suficientemente ampla para sugerir que nos casos em que o importador se encontrar sujeito à jurisdição *prescritiva* de outro Estado *e* da UE não existirá uma transferência.

Como bem se vê este aspeto carece de esclarecimentos, por parte do CEPD, que se esperam para breve[1306]. Com efeito, é essencial perceber, na prática, se antes de transferir os dados pessoais para um importador abrangido pelo art. 3.º do RGPD o exportador dos dados pessoais deverá *sempre* respeitar duas condições: (i) apresentar um fundamento para o tratamento em causa (art. 6.º) e (ii) um fundamento específico para as transferências para aquele importador (art. 44.º)[1307].

2.3. A insuficiência do regime das transferências depois do caso *Schrems*: a ilusão de uma proteção?

Reagindo às revelações de ES em 2014 o G29 lançou a seguinte pergunta: "em que medida é que o amplamente reconhecido direito fundamental à proteção de dados pessoais se continua a aplicar (efetivamente) nos dias de hoje, quando os dados pessoais são tão facilmente acessíveis pelo Estado?"[1308]. A resposta, negativa, a esta questão, viria um ano mais tarde com a decisão do TJ que ficou conhecida como o caso *Schrems* e com os desenvolvimentos que se lhe seguiram. Começo por aí, analisando essa decisão (2.3.1) para, de seguida, compreender os contornos daquela resposta e as implicações quanto à eficácia da continuidade da proteção do titular dos dados que a restrição às transferências prossegue (2.3.2).

[1305] CdE, "Draft Explanatory Report: Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data", n.º 99, acordado em maio de 2018 e disponível em https://rm.coe.int/16806b6ec2, consultado no dia 30 de setembro de 2018.
[1306] Embora já tenha sido anunciada a aprovação de linhas de orientação do CEPD sobre o artigo 3.º, as mesmas não foram, até à data, publicadas, conforme resulta do sítio daquela entidade, https://edpb.europa.eu/news/news_pt, consultado no dia 30 de setembro de 2018.
[1307] No mesmo sentido, P. VOIGT e A. BUSSCHE, *The EU General* cit., p. 25.
[1308] G29, "Working Document on surveillance ..." cit., p. 10.

2.3.1. O caso *Schrems*

2.3.1.1.Enquadramento

a) O contexto pré-Schrems

A saga *Schrems* tem início com uma "quebra de confiança"[1309] nas relações transatlânticas, espoletada pelas revelações de ES e fatal para a "adequação" dos EUA que a COM havia constatado numa decisão[1310]. Esta decisão de adequação implementava um mecanismo de auto-certificação para os importadores de dados pessoais estabelecidos nos EUA, designado "porto seguro" (*safe harbour*, na designação inglesa), objeto de críticas desde a sua origem[1311].

Como disse, as várias instituições da UE reagiram, destacando-se as comunicações da COM que haviam de ser citadas pelo TJ: "os programas norte-americanos de recolha de informações em grande escala (...) afetam os direitos fundamentais" acrescentando que "a vigilância generalizada das comunicações privadas dos cidadãos, das empresas ou dos dirigentes políticos é inaceitável" [1312]. Além disto, particularmente relevante, a COM reconheceu que o mecanismo do "porto seguro" funcionava como "um canal para transferir dados pessoais dos cidadãos da UE para os EUA pelas empresas que estão obrigadas a fornecer dados aos serviços de informações norte-americanos no âmbito dos programas de recolha de informações dos EUA", o que pode "comprometer o direito fundamental à proteção dos dados pessoais"[1313]. Numa outra Comunicação a COM reforçou esta ideia de que o "porto seguro", na prática, alimentava programas de "grande envergadura" das autoridades americanas que implicavam o tratamento de dados pessoais oriundos da UE, para além do estritamente necessário e proporcional em relação aos imperativos de proteção da segurança nacional[1314].

Igualmente relevante foi o já apresentado grupo de trabalho criado para apurar os factos mediatizados por ES, a resolução do PE, o parecer e o documento de trabalho do

[1309] Comissão Europeia, "Restabelecer a confiança ..." cit., p. 2.
[1310] Decisão da Comissão Europeia, de 26 de julho de 2000, nos termos da Diretiva 95/46, relativa ao nível de proteção assegurado pelos princípios de "porto seguro" e pelas respetivas questões mais frequentes (FAQ) emitidos pelo Department of Commerce dos Estados Unidos da América (Decisão 2000/520/CE)
[1311] Enunciando as várias críticas, v. Domingos FARINHO, "(Un)Safe Harbour: Comentário à decisão do TJUE C-362/14 e suas consequências legais", *FDPD,* n.º 2, 2016, p. 109 e ss..
[1312] Comissão Europeia, "Restabelecer a confiança ..." cit., p. 3.
[1313] *Idem* p. 8.
[1314] Comissão Europeia, "sobre o funcionamento ..." cit., p. 19.

G29. Mas as reações vieram também da sociedade civil, em particular de um jovem austríaco chamado MAX SCHREMS ("MS").

b) Os factos e as questões suscitadas

Em junho de 2013 MS apresentou uma queixa junto da autoridade de controlo Irlandesa (Data Protection Commissioner, doravante "DPC"), contra a *Facebook Ireland* ("FI"), arguindo a ilicitude das transferências realizadas para os servidores da *Facebook EUA* ("FEUA"), situados nos EUA, fundamentadas no "porto seguro" e, portanto, na Decisão 2000/520.

Invocando as revelações de ES sobre os programas de vigilância dos EUA, MS argumentou que o direito e a prática em vigor naquele país, em particular as atividades de vigilância dos serviços de informações, não preenchiam o requisito do nível de proteção adequada. Diante da recusa do DPC de instruir a queixa, MS recorreu para o Supremo Tribunal Irlandês que, a 18 de junho de 2014, suspendeu a instância para inquirir o TJ sobre a validade dos fundamentos da recusa do DPC: "no âmbito da análise de uma queixa segundo a qual o direito e as práticas de um país terceiro (neste caso, os EUA) para o qual são enviados dados pessoais não oferecem proteção adequada" será que a autoridade de controlo está vinculada, em termos absolutos, pela constatação de "adequação" da COM, consagrada na Decisão 2000/520, ou será que pode proceder à investigação sobre a matéria[1315]?

Como se constata, a dúvida suscitada àquela instância circunscreveu-se ao âmbito dos poderes do DPC *vis-à-vis* os poderes da COM. Contudo, o TJ foi além deste aspeto o que, a meu ver, tem consequências para todo o regime das transferências.

2.3.1.2.Análise da decisão

A argumentação que está na base deste caso acolhe, em grande parte, as conclusões do AG alicerçadas numa "questão central": a "transferência de dados pessoais da Facebook Ireland para a Facebook USA à luz do acesso generalizado da NSA e de outras

[1315] Acórdão do TJ, Maximillian Schrems c. Data Protection Commissioner, C-363/14, 6 de outubro de 2015, n.º 36.

agências de segurança dos Estados Unidos aos dados armazenados na Facebook USA ao abrigo das competências que lhes confere a legislação americana"[1316].

Em primeiro lugar, o TJ sustentou que, dada a sua independência e a vinculação à CDFUE, as autoridades de controlo devem examinar queixas relacionadas com a adequação da proteção de um país terceiro reconhecida numa decisão de adequação. Em relação a este ponto, os poderes daquelas autoridades são reforçados porquanto passam a dispor dos mesmos, em especial do poder de bloquear transferências, *apesar* da vigência de uma decisão da COM[1317]. Já se questionou se à atribuição desta missão, de verificar a adequação de um país terceiro, terá sido indiferente a falta de recursos, humanos e financeiros, que carateriza a ação destas entidades[1318]. Por outro lado, realizada essa verificação, a mesma poderá criar uma desarmonização de posições e interpretações entre autoridades de controlo em detrimento da natureza uniformizadora de uma decisão da COM[1319]. Para corrigir esta situação, a utilização dos mecanismos de cooperação será fundamental[1320].

Mas aquela instância não se quedou pela apreciação dos poderes das autoridades de controlo, pois invalidou a Decisão 2000/520 e, de uma forma diplomática e indireta, determinou a inadequação dos EUA para efeitos do art. 25.º da Diretiva. *Diplomática* porque o TJ nunca o afirma expressamente; e *indireta,* porque o objeto da sua apreciação é, por um lado, a compatibilidade do direito primário da UE com a Decisão 2000/520 (e não a ordem jurídica dos EUA) e, por outro, "operações de tratamento de dados" (as transferências) que ocorrem no território da UE[1321]. Mas porque razão os EUA não foram considerados como sendo um país adequado?

Antes de tudo, o tribunal apurou que a expressão "nível de proteção adequado" não significa um nível "idêntico ao garantido na ordem jurídica da União"[1322]. Porém, considerou o modelo dos EUA desadequado por duas ordens de razões:

[1316] Conclusões do AG no Acórdão do TJ, Maximillian Schrems c. Data Protection Commissioner, C-363/14, apresentadas em 23 de setembro de 2015, n.º 53.
[1317] Acórdão do TJ, Maximillian Schrems c. Data Protection Commissioner, C-363/14, 6 de outubro de 2015, n.os 38 a 66.
[1318] Sugerindo que falta às autoridades de controlo capacidade para, de forma eficaz, dar conta daquela tarefa, v. C. KUNER, "Reality and …" cit., p. 894.
[1319] J. Piñar MAÑAS, "Transferencias ..." cit., p. 443.
[1320] Artigos 60.º a 76.º do RGPD.
[1321] C. KUNER, "Reality and …" cit., p. 892; Martin SCHEININ, "Towards evidence-based discussion on surveillance: A Rejoinder to Richard A. Epstein", *ECLR,* n.º 12, 2016, p. 344; Acórdão do TJ, Maximillian Schrems c. Data Protection Commissioner, C-363/14, 6 de outubro de 2015, n.os 44 e 45.
[1322] Acórdão do TJ, Maximillian Schrems c. Data Protection Commissioner, C-363/14, 6 de outubro de 2015, n.º 81.

(i) Como sublinha D. FARINHO, o TJ "não nega a possibilidade de 'autorregulação regulada' no que diz respeito à proteção de dados pessoais, mas coloca a ênfase na (publicamente) 'regulada' e não na 'autorregulação'"[1323]. Por outras palavras, a desadequação do modelo dos EUA advém da natureza *pura* da autorregulação, sem qualquer intervenção *ex ante* ou *ex post* de uma autoridade pública.

(ii) A expressão "nível de proteção adequado" deve ser interpretada no sentido de que exige que o país terceiro assegure efetivamente um nível de proteção das liberdades e direitos fundamentais "substancialmente equivalente" ao conferido dentro da UE, nos termos da Diretiva lida à luz da CDFUE[1324]. Ora, será que esse nível de proteção se coaduna com a situação diagnosticada por ES? É sustentável, depois desse diagnóstico, constatar que o direito e a prática dos EUA respeitam os direitos fundamentais dos vigiados?

[1323] D. FARINHO, "(Un)Safe ..." cit., p. 118. Como explica o autor, para o TJ, a "autorregulação" só é válida quando for acompanhada pela "implementação de mecanismos eficazes de deteção e de fiscalização que permitam identificar e punir, na prática, eventuais violações das regras que asseguram a proteção dos direitos fundamentais (...)", v. Acórdão do TJ, Maximillian Schrems c. Data Protection Commissioner, C-363/14, 6 de outubro de 2015, n.º 81.

[1324] Acórdão do TJ, Maximillian Schrems c. Data Protection Commissioner, C-363/14, 6 de outubro de 2015, n.os 73 e 74.

Dificilmente. Até porque, analisando a Decisão 2000/520, em especial os artigos 1.º[1325] e 3.º[1326], o TJ, tal como o AG[1327], considerou que este instrumento jurídico não remediava a desadequação *estrutural* do ordenamento jurídico dos EUA. Pelo contrário, aquela decisão abria uma "via verde" às pretensões daquele país de vigiar estrangeiros por três ordens de razões:

[1325] "1. Nos termos do n.º 2 do artigo 25.° da Diretiva 95/46/CE, para efeitos de todas as atividades abrangidas pelo âmbito da diretiva, considera-se que os 'princípios da privacidade em porto seguro' (a seguir denominados 'os princípios') que figuram no anexo I da presente decisão (...) asseguram um nível adequado de proteção dos dados pessoais transferidos a partir da Comunidade Europeia para organizações estabelecidas nos Estados Unidos da América (...) 2. No que respeita a cada transferência de dados:
a) A organização destinatária dos dados comprometer-se-á clara e publicamente a cumprir os princípios aplicados em conformidade com as FAQ; e b) A referida organização fica sujeita aos poderes legais dos entes públicos administrativos norte-americanos referidos no anexo VII da presente decisão, com competência para investigar denúncias, tomar medidas contra práticas desleais e enganosas, assim como proceder à reparação de [danos sofridos por] pessoas singulares, independentemente do seu país de residência ou da sua nacionalidade, sempre que se verificar incumprimento dos princípios segundo as orientações das FAQ. 3. Considera-se que a organização que declarar a sua adesão aos princípios aplicados em conformidade com as FAQ cumpre o disposto no n.° 2, a partir da data em que comunicar ao Department of Commerce dos EUA ou ao seu representante, a divulgação do compromisso referido na alínea a) do n.° 2, bem como a identidade da entidade pública a que se refere a alínea b) do n.° 2."

[1326] "1.Sem prejuízo da competência para tomar medidas que garantam o cumprimento das disposições nacionais adotadas por força de outras disposições além das previstas no artigo 25.° da Diretiva 95/46/CE, as autoridades competentes dos Estados-Membros podem exercer as suas competências para suspender a transferência de dados para uma organização que tenha declarado a sua adesão aos princípios aplicados em conformidade com as FAQ, se isso se verificar necessário à proteção das pessoas no que diz respeito ao tratamento dos seus dados pessoais, nos casos seguintes: a) A entidade pública administrativa norte-americana referida no anexo VII da presente decisão, ou um mecanismo de recurso independente, nos termos da alínea a) do princípio de aplicação que figura no anexo I da presente decisão, determinou que a organização violou os princípios em conformidade com as FAQ; ou b) Existem fortes probabilidades para supor que os princípios não estão a ser respeitados. Há indícios de que o mecanismo de aplicação em causa não toma ou não tomará as medidas adequadas na altura necessária para resolver o caso em questão, que a continuação da transferência dos dados pode causar graves prejuízos às pessoas em causa e que as entidades competentes nos Estados-Membros envidaram esforços razoáveis, dadas as circunstâncias, para facultar à organização em causa a informação e oportunidade necessárias para responder. A suspensão cessará assim que o respeito dos princípios aplicados em conformidade com as FAQ estiver assegurado e a autoridade competente em questão na Comunidade Europeia seja disso informada. 2. Os Estados-Membros devem informar imediatamente a Comissão da adoção de medidas nos termos do n.º 1. 3. Os Estados-Membros e a Comissão devem ainda manter-se mutuamente informados relativamente aos casos em que os organismos responsáveis pelo cumprimento dos princípios aplicados em conformidade com as FAQ nos Estados Unidos da América não garantam esse mesmo cumprimento. 4. Se a informação recolhida nos termos dos n.ºs 1 a 3 demonstrar que os organismos responsáveis pelo cumprimento dos princípios em conformidade com as FAQ nos Estados Unidos da América não desempenham eficazmente as suas funções, a Comissão deve informar o Department of Commerce norte-americano e, se necessário, apresentar um projeto de medidas, de acordo com o procedimento estabelecido no artigo 31.º da diretiva, para revogar ou suspender a presente decisão ou limitar o seu âmbito."

[1327] Conclusões do AG no Acórdão do TJ, Maximillian Schrems c. Data Protection Commissioner, C-363/14, apresentadas em 23 de setembro de 2015, n.º 159.

(i) Do seu âmbito de aplicação estavam excluídas as autoridades públicas americanas[1328] ou seja, o "porto seguro" não providencia um nível de proteção adequado em relação aos tratamentos realizados por aquelas autoridades[1329];

(ii) Consagrava, de forma imprecisa, o primado dos "requisitos de segurança nacional, interesse público ou [cumprimento da lei] sobre os princípios do porto seguro" e um conjunto de derrogações enunciadas no anexo I daquela Decisão. Tal significava que os importadores de dados pessoais certificados estavam obrigados a afastar, sem limites ou salvaguardas, os princípios e garantias do "porto seguro" por via da aplicação de uma daquelas derrogações de "caráter geral". Ora, estas derrogações viabilizam ingerências injustificadas e ilimitadas aos direitos fundamentais dos titulares dos dados pessoais que foram ou podiam ser transferidos ao abrigo do "porto seguro", designadamente aos artigos 7.º e 8.º da CDFUE[1330]; e, por fim,

(iii) A Decisão 2000/520 não salvaguarda a exposição dos titulares dos dados a estas ingerências[1331].

O tribunal sustentou-se nas Comunicações da COM, de 2013, sobre os programas de vigilância dos EUA para caraterizar aquelas ingerências: (1) não se limitam ao estritamente necessário na medida em que autorizam, de forma generalizada, "a conservação da totalidade dos dados pessoais de todas as pessoas cujos dados foram transferidos da União para os Estados Unidos, sem qualquer diferenciação, limitação ou exceção em função do objetivo prosseguido e sem que esteja previsto um critério objetivo que permita delimitar o acesso das autoridades públicas aos dados e a utilização posterior, para fins precisos, estritamente limitados e suscetíveis de justificar a ingerência"; (2) permitem o acesso generalizado ao conteúdo das comunicações eletrónicas o que afeta o "conteúdo essencial do direito fundamental ao respeito da vida privada"; (3) não respeitam o "conteúdo essencial do direito fundamental a uma proteção jurisdicional

[1328] Acórdão do TJ, Maximillian Schrems c. Data Protection Commissioner, C-363/14, 6 de outubro de 2015, n.º 82.
[1329] G29, "Working Document on surveillance ..." cit., p. 38.
[1330] Acórdão do TJ, Maximillian Schrems c. Data Protection Commissioner, C-363/14, 6 de outubro de 2015, n.os 87 e 88.
[1331] Acórdão do TJ, Maximillian Schrems c. Data Protection Commissioner, C-363/14, 6 de outubro de 2015, n.os 84 a 89.

efetiva, tal como é consagrado no artigo 47.º da Carta" uma vez que os estrangeiros vigiados não podem apresentar um recurso administrativo ou judicial caso, no âmbito dos programas de vigilância, os seus dados pessoais sejam recolhidos nem obter o acesso, solicitar a retificação ou apagamento dos mesmos[1332].

Toda a análise em torno da adequação dos EUA se parece estribar numa comparação entre o direito e as práticas da UE e o direito e as práticas daquele país: uma vez que é impossível àquela, como atesta o caso *Digital Rights Ireland*[1333]*,* adotar disposições legislativas que, em violação da CDFUE e da CEDH[1334], prevejam uma vigilância em larga escala e não dirigida, sem garantias para os vigiados, *a fortiori,* não se pode considerar que um país terceiro assegura um "nível de proteção adequado" quando legislação interna autoriza esse tipo de vigilância. Por outro lado, este caso não respeita apenas e só ao problema das transferências, antes deve ser enquadrado numa narrativa do TJ de combater derivas securitárias de *dataveillance,* centrada no princípio da proporcionalidade de restrições aos direitos fundamentais em matéria de vigilância do Estado[1335]. Nesta narrativa as especificidades da decisão *Schrems* situam-se a dois níveis:

(i) A vigilância não é conduzida por um Estado-Membro, mas por um país terceiro e com alcance extraterritorial;

(ii) Os termos dessa vigilância caraterizam-se não só pelo seu alcance, em massa e indiscriminado, mas também por uma desproteção do vigiado e pela afetação do núcleo essencial do direito à vida privada por via do acesso ao conteúdo das comunicações[1336].

[1332] Acórdão do TJ, Maximillian Schrems c. Data Protection Commissioner, C-363/14, 6 de outubro de 2015, n.º 93 a 95.

[1333] Acórdão do TJ, Digital Rights Ireland *et alii* c. Minister for Communications, Marine and Natural Resources *et alii,* C-293/12, 8 de abril de 2014.

[1334] Citada no Acórdão do TJ, Digital Rights Ireland *et alii* c. Minister for Communications, Marine and Natural Resources *et alii,* C-293/12, 8 de abril de 2014, n.º 35, 47, 54, entre outros.

[1335] A decisão pioneira neste campo foi o já referido caso *Digital Rights Ireland.* Nesta decisão, o TJ aplicou rigorosamente aquele princípio, em especial a dimensão de necessidade, retirando substancial margem de manobra às instituições da UE para a adoção de legislação sobre retenção de dados pessoais e gerando dúvidas sobre a validade da recolha indiscriminada e em massa de dados pessoais para fins securitários, v. D. LINDSAY, "The Role …" cit., p. 49, 69 e 73; M. SCHEININ, "Towards evidence ..." cit., p. 342. Estas dúvidas vêm sendo clarificadas em decisões posteriores como o Acórdão do TJ, Tele2 Sverige AB c. Post- och telestyrelsen e Secretary of State for the Home Department *et alii*, C-203/15 e C-698/15, 21 de dezembro de 2016 e o Parecer 1/15 sobre o PNR Canada, 26 de julho de 2017.

[1336] D. LINDSAY, "The Role …" cit., p. 49; M. SCHEININ, "Towards evidence ..." cit., p. 342 e 344.

O que esta instância veio clarificar nesta decisão é que um país terceiro só será adequado se respeitar um determinado esquema de proteção das pessoas singulares em matéria de ingerências aos direitos fundamentais para efeitos de vigilância do Estado. De modo a clarificar esse quadro jurídico o G29 elencou quatro "garantias essenciais" que preenchem esse esquema, decantando-as da jurisprudência do TJ e do TEDH sobre vigilância do Estado"[1337]: "1) o tratamento deve-se basear em regras claras, precisas e acessíveis (fundamento legal); 2) requer-se a demonstração da necessidade e da proporcionalidade em relação aos objetivos prosseguidos; 3) requer-se a sujeição do tratamento a supervisão independente; 4) exigem-se meios de recurso efetivos ao dispor dos indivíduos" [1338]. É este o modelo para testar a adequação das práticas de vigilância extraterritorial, de países terceiros, e territorial, de um Estado-Membro[1339]. Também assim se compreende que o art. 45.º, n.º 2, al. a), do RGPD, inclua, expressamente, entre a avaliação da legislação vigente no país terceiro, a "matéria de segurança pública, segurança nacional e direito penal, e respeitante ao acesso das autoridades públicas a dados pessoais".

O paradoxo que rodeia o caso *Schrems,* minando a sua legitimidade e impacto, resulta da desadequação da proteção contra aquelas ingerências em vários Estados-Membros[1340]. É que as revelações de ES incluíram os programas de vigilância de países como o Reino Unido e a Alemanha, o que valeu acusações de hipocrisia à UE[1341]. O TJ estará, neste ponto, de "mãos atadas" na medida em que, como sintetizou o G29, "os programas de vigilância geridos pelos Estados-Membros da UE não são, regra geral, sujeitos ao direito da UE"[1342]. No campo da segurança nacional, segundo o art. 4.º, n.º 2, do TUE, vigora uma separação de competências[1343]. Em todo o caso, se por um lado, o

[1337] G29, "Working Document 01/2016 on the justification of interferences with the fundamental rights to privacy and data protection through surveillance measures when transferring personal data (European Essential Guarantees)", 13 de abril de 2016.
[1338] G29, "Adequacy ..." cit., p. 3 e ss., capítulo 1.
[1339] D. LINDSAY, "The Role …" cit., p. 79.
[1340] Como refere M. TZANOU: "A pretensão da UE enquanto líder moral no respeito dos direitos fundamentais nem sempre é óbvia", v. "The war against terror and transatlantic information sharing: spillovers of privacy or spillovers of security", *UJIEL,* n.º 31, vol. 80, 2015, p. 87 e ss..
[1341] Benjamin WITTES, "Privacy, Hypocrisy, and a Defense of Surveillance", Russel MILLER, *Privacy and* cit., p. 180; K. HON, *Data Localization* cit., p. 310; Stepahn HEUMANN, "German Exceptionalism? The Debate About the German Foreign Intelligence Service (BND)", Russel MILLER, *Privacy and* cit., p. 349 e ss..
[1342] G29, "Parecer 04/2014 …" cit., p. 6.
[1343] G29, "Working Document on surveillance ..." cit., p. 22 e ss..

alcance dos programas de vigilância dos Estados-Membros é menor, por outro lado, poderão ser sindicados pelo TEDH[1344].

2.3.2. A ilusão da proteção do regime das transferências depois de *Schrems*

Os efeitos do caso *Schrems* transcendem a adequação dos EUA enquanto "país terceiro" e atingem o *core* do regime das transferências, designadamente a intenção de garantir a "continuidade da proteção", isto é, que mesmo depois de transferidos os dados pessoais o titular continuará a beneficiar dos direitos fundamentais e das garantias a que tem direito na UE[1345]. Com efeito, o que se seguiu a esta decisão exemplifica isso mesmo.

Dado o seu impacto no comércio transatlântico[1346] e fazendo fé nas promessas dos EUA de reformar o direito e as práticas em vigor[1347], a COM adotou uma nova decisão, conhecida como "Escudo de Proteção" (*Privacy Shield*)[1348]. Tem-se entendido que este "escudo" é um mero paliativo, uma solução temporária, uma ficção política de adequação para sustentar o comércio transatlântico[1349]. Vários elementos suportam esta hipótese:

[1344] B. WITTES, "Privacy, Hypocrisy ..." cit., p. 191 e ss.; F. BIGNAMI e G. RESTA, "Transatlantic ..." cit., p. 256; G29, "Parecer 04/2014 …" cit., p. 6 e "Working Document on surveillance ..." cit., p. 14 e ss..

[1345] G29, "Documento de Trabalho sobre uma ..." cit., p. 10.

[1346] Numa estimativa, sem um instrumento a regular estes fluxos de dados, o Produto Interno Bruto da Europa cairia 1,3% e a exportação de serviços para os EUA cerca de 6,7%, v. AmCham EU, "Adoption of the EU-US Privacy Shield Restores Trust to Transatlantic Data Flows", 2016, disponível em https://www.amchameu.eu/sites/default/files/press_releases/press_-_adoption_of_the_eu-us_privacy_shield_restores_trust_to_transatlantic_data_flows.pdf, consultado no dia 30 de setembro de 2018.

[1347] Comissão Europeia, "Transferência transatlântica de dados: restaurar a confiança através de garantias sólidas", 29 de fevereiro de 2016, p. 17.

[1348] Decisão de execução da Comissão Europeia de 12 de julho de 2016, relativa ao nível de proteção assegurado pelo Escudo de Proteção da Privacidade UE-EUA, com fundamento na Diretiva 95/46/CE do Parlamento Europeu e do Conselho (Decisão 2016/1250/EU).

[1349] João MARQUES, "And [they] built a crooked h[arbour] – the Schrems ruling and what it means for the future of data transfers between the EU and US", *EU Law Journal,* vol. 2, n.º 2, junho de 2016, p. 54 e ss.. As análises doutrinais desta decisão são várias, *inter alia,* v. C. KUNER, "Reality and …" cit., p. 902; D. LINDSAY, "The Role of …" cit., p. 74; Gert VERMEULEN, "The Paper Shield. On the degree of Protection of the EU-US Privacy Shield against Unnecessary or Disproportionate Data Collection by the US Intelligence and Law Enforcement Services", D. J. SVANTESSON e D. KLOZA (eds.), *Trans-Atlantic* … cit., p. 127 e ss.. Elencando os problemas do *Privacy Shield* v. PE, "From Safe Harbour to Privacy Shield. Advances and shortcomings of the new EU-US data transfer rules", janeiro de 2017, p. 14, disponível em http://www.europarl.europa.eu/RegData/etudes/IDAN/2017/595892/EPRS_IDA(2017)595892_EN.pdf, consultado no dia 30 de setembro de 2018. A natureza temporária do *Privacy Shield* foi reconhecida pelo presidente do SEPD, v. "EU privacy watchdog: Privacy Shield should be temporary", 3 de agosto de 2017, https://www.euractiv.com/section/data-protection/interview/eu-privacy-watchdog-privacy-shield-should-be-temporary/, consultado no dia 30 de setembro de 2018.

(i) A posição reprovadora do SEPD[1350] e do G29[1351] ao conteúdo da nova decisão;

(ii) A "chantagem" do G29 na sequência da primeira revisão do *Privacy Shield*, alertando que, caso os EUA e a COM não procurem uma alternativa, irá acionar vias de recurso para suscitar a validade da nova decisão junto do TJ[1352];

(iii) O reenvio prejudicial pendente naquela instância para invalidar a nova decisão[1353];

(iv) O "escudo" não passa no teste das quatro "garantias essenciais europeias", designadamente porque no mesmo é notória a falta de clareza sobre certos programas de vigilância norte-americanos, o teste da proporcionalidade dificilmente é compatível com o alcance dos programas de vigilância de cidadãos estrangeiros ("massivos e indiscriminados"), a fiscalização ao abrigo, por exemplo, da *Executive Order 12333* é inexistente, o FISC não acautela a posição dos estrangeiros e o recurso para o *Privacy Shield Ombudsperson* não está disponível sendo questionável a sua independência[1354].

Ainda longe de terminar, a saga *Schrems* lembra o caso *Kadi*, quando as instituições políticas da UE renovaram a lista de terroristas da qual constava o sr. KADI,

---

[1350] SEPD, "Opinion on the EU-U.S. Privacy Shield Draft Adequacy Decision. Opinion 4/2016", 30 de maio de 2016.
[1351] G29, "EU-U.S. Privacy Shield – First annual Joint Review", 28 de novembro de 2017.
[1352] G29, "EU-U.S. Privacy …" cit., p. 4: "Se as preocupações do G29 não forem atendendidas, os membros do G29 adotaram as ações apropriadas, incluindo colocar a decisão de adequação do escudo de proteção nos tribunais nacionais para suscitar um reenvio prejudicial para o TJ".
[1353] Continua pendente no TJ o caso que opõe *La Quadrature du Net e o.* à *Comissão,* T-738/16, recurso interposto em 25 de outubro de 2016. Os fundamentos e principais argumentos encontram-se em http://curia.europa.eu/juris/document/document.jsf?text=&docid=185146&pageIndex=0&doclang=PT&mode=lst&dir=&occ=first&part=1&cid=1495879, consultado no dia 30 de setembro de 2018.Por seu turno, o Processo T-670/16, Digital Rights Ireland v. Comissão, recurso interposto em 16 de setembro de 2016, foi considerado inadmissível por falta de legitimidade processual, numa decisão do TJ de 22 de novembro de 2017, disponível em http://curia.europa.eu/juris/document/document.jsf?text=&docid=197141&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=215880, consultado no dia 30 de setembro de 2018.
[1354] D. LINDSAY, "The Role of …" cit., p. 81; E. SCHEIGHOFER, "Principles …" cit., p. 47; G. VERMEULEN, "The Paper Shield …" cit., p. 127 e ss.; J. MARQUES, "And [they] built ..." cit., p. 70.

conhecendo de antemão o risco de uma ronda de litígios no Tribunal de Primeira Instância e no TJ[1355]. Por conseguinte, se formalmente existe uma decisão de adequação dos EUA a sua eficácia "garantística", a sua validade material, são bastante duvidosas.

Adicionalmente, a inadequação estrutural dos EUA causa um problema em cascata contagiando os demais fundamentos para as transferências, incluindo as cláusulas contratuais-tipo, o expediente mais usado pelos operadores económicos no pós-*Schrems*[1356]. É esse o objeto do caso *Schrems 2*, iniciado em 2015, centrado na validade daquelas cláusulas para as transferências realizadas pelo FI para o FEUA[1357]. Na sua argumentação, MS defende que a "questão central" em relação à adequação dos EUA persiste: a vigência, *inter alia,* da *Executive Order 1233,* a inexistência de garantias para os cidadãos da UE e de controlo e fiscalização das atividades de vigilância[1358]. Referindo-se ao FISC, MS defende que este "tribunal" se resume a uma operação de "carimbo", excluindo todos os elementos de um verdadeiro tribunal na aceção corrente nas sociedades democráticas, em particular à luz do art. 6.º da CEDH (direito a um processo equitativo) e do art. 47.º da CDFUE (direito à ação e a um tribunal imparcial). A questão encontra-se pendente no TJ, desde abril de 2018[1359], pelo que caberá àquela instância colocar um ponto final nas dúvidas ainda existentes em certos países, em especial onde as autoridades de controlo proibiram as transferências para os EUA com base naquele fundamento[1360].

Atendendo a esta sequência de eventos, creio que o caso *Schrems* expõe a fragilidade de *todos* os fundamentos das transferências para garantir a "continuidade da proteção" assegurada pela UE, sobretudo quando os poderes das autoridades dos países

---

[1355] M. SCHEININ, "Towards evidence …" cit., p. 341.

[1356] C. KUNER, "Reality and …" cit., p. 881 e ss.; D. FARINHO, "(Un)Safe ..." cit., p. 121; E. SCHWEIGHOFER, "Principles for ..." cit., p. 27 e ss.; G29, "Working Document 01/2016 …" cit., p. 3 e "Parecer 04/2014 …" cit., p. 3; G. MALDOFF e O. TENE, "'Essential Equivalence' …" cit., p. 2 e ss.; K. HON, *Data Localization* cit., p. 166; R. POLCAK e D. SVANTESSON, *Information Sovereignty* cit., p. 216.

[1357] DPD, "Update on Litigation involving Facebook and Maximilian Schrems", disponível em https://www.dataprotection.ie/docs/01-02-2017-Update-on-Litigation-involving-Facebook-and-Maximilian-Schrems/1598.htm, consultado no dia 30 de setembro de 2018.

[1358] A queixa apresentada por MS pode ser lida em http://www.europe-v-facebook.org/EN/Complaints/Model_Contracts/model_contracts.html, consultado no dia 30 de setembro de 2018.

[1359] Europe-v-facebook, "Irish High Court sends Facebook's EU-US data transfers before CJEU 'Standard Contractual clauses' and 'Privacy Shield' on the table", 12 de abril de 2018, disponível em http://www.europe-v-facebook.org/sh2/pa-ref.pdf, consultado no dia 30 de setembro de 2018.

[1360] Como sucedeu, por exemplo, na Alemanha, v. "ULD Position Paper on the Judgement of the Court of Justice of the European Union of 6 October 2015, C-362/14", adota a 14 de outubro de 2015, disponível em https://www.datenschutzzentrum.de/uploads/internationales/20151014_ULD-PositionPapier-on-CJEU_EN.pdf, consultado no dia 30 de setembro de 2018. Neste documento, na página 4, a autoridade do Estado alemão de *Schleswig-Holstein* declara: "(…) aplicando de forma consistente os requisitos do TJ, uma transferência com base em cláusulas contratuais-tipo para os EUA é proibida".

terceiros em matéria de acesso aos dados pessoais não respeitam as quatro "garantias essenciais europeias". E há boas razões para acreditar que não são só os EUA a preencher esta quota[1361]. Por conseguinte, o regime das transferências, tanto através do procedimento de adequação como das "garantias adequadas", apenas cria uma *ilusão* de proteção do titular dos dados pessoais. Apesar da sua validade num sentido *formal,* as garantias adequadas são tão inaptas para proteger os indivíduos da vigilância de países terceiros como as decisões de adequação: nem aquelas nem as estas obstam à vigência e aplicação do direito dos EUA[1362].

Ainda assim, esta incapacidade de colocar travão à vigilância estrangeira não me leva a recusar totalmente o sentido e a utilidade do regime das transferências, em especial o procedimento de apreciação de adequação. É que este não deixa de servir os interesses do titular dos dados pessoais e de contribuir para a atuação externa da UE enquanto "regulador transnacional"[1363]. De facto, sempre se pode dizer que o procedimento de adequação adquire relevo, pelo menos no curto prazo, ao criar um canal de *negociações* e de *pressão* aos EUA (e a outros países terceiros). Esta hipótese parece preferível à abolição deste procedimento viabilizando, sem mais, uma "via verde" às pretensões das autoridades estrangeiras e uma espécie de "bênção" aos respetivos programas de vigilância.

Enquanto canal de *negociações*, o procedimento de adequação já deu provas de mérito. Mesmo admitindo que o *Privacy Shield* é um mero paliativo, a verdade é que, como o próprio G29 admitiu, trata-se de um avanço em relação ao esquema do "porto seguro" [1364]. Na feliz expressão de A. FISCHER-LESCANO e G. TEUBENER, este procedimento funciona como *gentle civilizer of social systems*[1365], instigando o diálogo entre a UE e os países terceiros[1366]. Enquanto instrumento de *pressão*, a sua utilidade é a capacitação da sociedade civil para reagir à vigilância estrangeira, como atestam os

[1361] Referindo o Canadá e Israel, v. G. MALDOFF e O. TENE, "'Essential Equivalence …" cit., p. 211 e ss.; I. S. RUBINSTEIN, "Systematic government access …" cit., p. 118 e ss..
[1362] C. KUNER, "Reality and …" cit., p. 907; C. BOWDEN, "The US Surveillance ..." cit., p. 27; Joanna KULESZA, "Transboundary data protection and international business compliance", *IDPL,* vol. 4, n.º 4, 2014, p. 298; K. HON, *Data Localization*, cit., p. 97; e ss.; P. de HERT e M. CZERNIAWSKI, "Expanding the …", cit., p. 235.
[1363] K. HON, *Data Localization*, cit., p. 25 e 149.
[1364] G29, "Working Document on surveillance ..." cit., p. 8 e "EU-U.S. Privacy Shield …" cit., p. 3, 14 e ss..
[1365] Andreas FISCHER-LESCANO e Gunther TEUBNER, "Regime-Collisions: The Vain Search for Legal Unity in the Fragmentation of Global Law", *MIJIL,* vol. 25, 2003, p. 999.
[1366] Em sentido próximo, v. Bilyana PETKOVA, "Domesticating the 'foreign' in making transatlantic data privacy law", *IJCL,* vol. 15, n.º 4, 2017, p. 1135 e ss. e C. KUNER, "Reality and ..." cit., p. 893.

desenvolvimentos do caso *Schrems 2,* o "ativismo" do G29 e a decisão de anulação do *Privacy Shield* pendente no TJ. Como reconheceu a COM, numa demonstração de otimismo moderado, o *Privacy Shield* marca um "novo capítulo nas relações bilaterais" caraterizado por um "momento de vigilância que ainda não terminou"[1367]. Este será um capítulo atribulado por denúncias à comunidade internacional, com valor ético-político, pondo em marcha um processo de divulgação de um problema que carece de uma solução e que merece ser exposto à censura da opinião pública mundial.

A longo prazo, iluminam-se duas alternativas pelas quais a UE se deve bater ao longo deste novo capítulo: um tratado bilateral, com os EUA, como alternativa a uma decisão de adequação[1368]; ou um audacioso tratado global sobre os métodos e os limites da vigilância extraterritorial incluindo, porventura, um direito à encriptação[1369]. Esta segunda hipótese tem estado na mira das recomendações da ONU em matéria de promoção e proteção dos direitos humanos e liberdades fundamentais nas políticas de contra terrorismo[1370] e, recentemente, do Relator Especial da ONU para a privacidade[1371].

Entretanto, apanhados nos meandros de uma estratégia de curto prazo, estão os utilizadores de dados pessoais cuja atividade depende de transferências para os EUA. A sua posição é particularmente sensível por duas razões:

(i) Não sabem a que fundamento recorrer para, de forma segura e estável, realizar as suas operações transnacionais; e

(ii) Continuam sujeitos a pedidos estrangeiros considerados abusivos e proibidos ao abrigo do art. 48.º do RGPD.

Acresce que o G29 não excluiu *in limine* a adoção de "medidas repressivas (...) em especial quando os responsáveis pelo tratamento dos dados cooperam voluntária e conscientemente" com as autoridades estrangeiras, por exemplo transferindo dados

[1367] Comissão Europeia, "Transferências transatlânticas ..." cit., p. 16. Em sentido semelhante, v. Franziska BOEHM, "Assessing the new instruments in EU-US surveillance and data protection law – US legislation, Privacy Shield and Umbrella Agreement", *EDPLR,* n.º 3, 2016, p. 1 e ss. e M. TZANOU, *The Fundamental Right* cit. p. 147.

[1368] Volto a este aspecto no ponto 2.4.1. deste Capítulo.

[1369] G29, "Parecer 04/2014 …" cit., p. 17. Na doutrina, C. KUNER, "Reality and …" cit., p. 918; D J. SVANTESSON e D. KLOZA, "Landscape …" cit., p. 566; I. BROWN *et alii*, "Toward …" cit., p. 461 e ss.; K. HON, *Data Localization*, cit., p. 170 e 315; M. SCHEININ, "Towards …" cit., p. 346 e 437.

[1370] Os relatórios dos vários Relatores Especiais encontram-se disponíveis em http://www.ohchr.org/EN/Issues/Terrorism/Pages/Annual.aspx, consultado no dia 30 de setembro de 2018.

[1371] "Draft Legal Instrument on …" cit., p. 3.

pessoais a pedido daquelas[1372]. Julgo que, como tem sucedido noutros países, dois fatores determinantes para estas "medidas repressivas" serão o grau de cooperação com as autoridades estrangeiras e a transparência para com os titulares dos dados[1373]. Por exemplo, um banco canadiano que subcontratou uma empresa americana notificou os seus clientes de que a respetiva informação poderia ser acedida pelas autoridades dos EUA ao abrigo do *US Patriot Act*, tendo a autoridade canadiana entendido que tal não violava o PIPEDA[1374]. Adicionalmente, os utilizadores de dados pessoais dispõem de três alternativas para rebater a insegurança jurídica quanto à validade dos fundamentos das transferências, para mitigar o risco de "medidas repressivas" e dificultar as pretensões das autoridades estrangeiras.

Em primeiro lugar, o armazenamento de dados pessoais no território da UE vem sendo defendido pela doutrina[1375], sugerido por várias instituições[1376] e mereceu destaque do TJ[1377]. Na prática, tem sido o caminho de alguns agentes económicos e foi a solução encontrada no caso *SWIFT*[1378]. Em geral, o chamado *data nationalism*, que passa pela não realização de transferências para países terceiros, tem servido como "escudo de proteção" de muitos Estados para contornar as práticas de vigilância denunciadas por ES. Porém, citando a anterior presidente do G29 quando confrontada com esta solução, "talvez seja uma vantagem a curto prazo, mas a Europa não pode ser uma fortaleza. Não

[1372] G29, "Parecer 04/2014 ..." cit., p. 8.
[1373] *Ibidem*. No mesmo sentido, v. E. SCHEIGHOFER, "Principles ..." cit., p. 47.
[1374] K. HON, *Data Localization* cit., p. 99.
[1375] Anupam CHANDER e Lê UYÊ, "Data Nationalism", *EmLR,* 2015, n.º 64, p. 677 e ss.; C. BOWDEN, "The US Surveillance ..." cit., p. 33; Christopher KUNER, "Data Nationalism and its Discontents", *EmLR,* 2015, n.º 64, p. 2089 e ss. e, do mesmo autor, "Reality and …" cit., p. 913.
[1376] A autoridade de controlo austríaca recomendou que as organizações dependentes do "porto seguro" armazenassem os dados pessoais em servidos na UE, v. K. HON, *Data Localization* cit., p. 166. A Comissão Europeia sugeriu que "A localização é também utilizada como indicador de garantias em termos de privacidade (...)", v. Comissão Europeia, "Construir uma economia europeia dos dados", 10 de janeiro de 2017, p. 6.
[1377] No caso *Digital Rights Ireland,* ao apreciar a validade da Diretiva 2006/26, o TJ afirmou: "deve acrescentar-se que a referida diretiva não impõe que os dados em causa sejam conservados no território da União, pelo que não se pode considerar que esteja plenamente garantida a fiscalização, por uma entidade independente, expressamente exigida pelo artigo 8.°, n.° 3, da Carta, do respeito das exigências de proteção e de segurança, tal como referidas nos dois números anteriores", Acórdão do TJ, Digital Rights Ireland *et alii* c. Minister for Communications, Marine and Natural Resources *et alii,* C-293/12, 8 de abril de 2014, n.º 68.
[1378] Comissão Europeia, "Sobre a transferências de dados pessoais da UE para os Estados Unidos da América ao abrigo da Diretiva 95/46/CE na sequência do acórdão proferido pelo Tribunal de Justiça no processo C-362/14 (Schrems), 6 de novembro de 2015. O caso da Fujitsu é paradigmático, v. Martin JUNG, "Wir sind NSA-Frei", *Frankfurter Allgemeine Zeitung*, 16 de novembro de 2016, p. 26, onde o Diretor da empresa para a Europa afirma que a localização da infraestrutura na Alemanha garante a ausência de intrusões da NSA. Dando outros exemplos, v. K. HON, *Data Localization*, cit., p. 108. Sobre *SWIFT*, v. G29, "Parecer 10/2006 ..." cit., p. 2 e ss..

creio verdadeiramente que seja possível manter os dados na Europa"[1379]. Erguer uma espécie de *linha Maginot* cibernética não parece ser uma solução satisfatória, tanto na perspetiva do prestador do serviço como do consumidor, sendo aliás uma solução que a própria COM não vê com bons olhos: "[i]nfelizmente, a tendência, tanto a nível mundial como europeu, é no sentido de uma maior localização dos dados, uma abordagem frequentemente baseada na falsa ideia de que os serviços localizados são automaticamente mais seguros do que os serviços transfronteiriços" [1380].

Outra alternativa, enaltecida por alguma doutrina[1381], por MS[1382] e recentemente aflorada pelo G29[1383], é a adoção de medidas de segurança como a encriptação e outras soluções técnicas que dificultam o acesso inteligível, por terceiros, aos dados pessoais transferidos da UE para os EUA. Entre as recomendações do Relator Especial da ONU para a promoção e proteção do direito à liberdade de opinião e de expressão, encontra-se a encriptação e anonimização[1384]. A própria indústria, com a *Google* a destacar-se[1385], tem sido uma defensora desta via, assegurando que a encriptação dificulta e torna mais onerosa a tarefa do acesso direto do Estado e, sobretudo, obriga-o a recorrer às vias judiciais adequadas. Desde as revelações de ES, muitos operadores transatlânticos reforçaram a encriptação da sua informação, recorrendo a algoritmos mais fortes, chaves

[1379] Cécile Barbière, "Le mieux légiférer menace l'Europe numérique", *EurActiv.com*, 20 de junho de 2016, disponível em https://www.euractiv.fr/section/innovation-entreprises/news/le-mieux-legiferer-menace-leurope-numerique/, consultado no dia 30 de setembro de 2018.

[1380] Comissão Europeia, "Construir ..." cit., p. 7. Elencando as várias desvantagens de uma estratégia de limitação da localização dos dados, entre as quais destaco os custos, a resiliência e a continuidade do negócio, o comércio global, entre outros, v. K. HON, *Data Localization* cit., p. 112.

[1381] Jonathan HAFETZ, "The Possibilities and Limits of Corporations as Privacy Protectors in the Digital Age", David D. COLE *et alii*, *Surveillance* cit., p. 91 e ss. e K. HON, *Data Localization* cit., p. 117, 139, 274.

[1382] Apesar de reconhecer que, no curto prazo, a localização dos dados pessoais na UE é a solução mais evidente, ainda que não totalmente eficaz, v. Jennifer BAKER, "Catching up with Max Schrems", *IAPP*, 2016.

[1383] Depois do caso *Schrems,* o G29 lançou um apelo para que as discussões com os EUA fossem centradas em soluções "políticas, jurídica e *técnicas*", v. G29, "Statement on Schrems Judgement", 3 de fevereiro de 2016.

[1384] David KAYE, "Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression", 22 de maio de 2015, p. 4 e ss., disponível em https://www.ohchr.org/EN/Issues/FreedomOpinion/Pages/OpinionIndex.aspx, consultado no dia 30 de setembro de 2018.

[1385] Segundo o CEO da Google, Eric SCHMIDT, a solução para a vigilância estadual é a encriptação, v. Paul Rubens, "The year of encryption", *BBC*, 10 de janeiro de 2014, disponível em http://www.bbc.com/news/business-25670315, consultado no dia 30 de setembro de 2018. Num discurso diante do parlamento da Baviera, Vice-Presidente de Public Policy da Google, Rachel WHETSTONE, defendeu o mesmo, v. "Privacy, security, surveillance: getting right is importante", 13 de feveiro de 2015, disponível em https://europe.googleblog.com/2015/02/privacy-security-surveillance-getting.html, consultado no dia 30 de setembro de 2018.

mais longas e não reutilizáveis[1386]. Há casos de "resistência" bem-sucedida mesmo em relação a pedidos das autoridades norte-americanas[1387].

Em terceiro lugar, sugere-se que a dispersão da infraestrutura informática e corporativa das operações de um utilizador de dados pessoais despista as autoridades[1388]. O caso de estudo neste domínio é o serviço de partilha de ficheiros *The Pirate Bay* ("TPB"), sob constante ameaça por várias autoridades que procuram evitar que os utilizadores do TPB acedam a conteúdos ilegais. A solução adotada está disponível *online* num diagrama desenvolvido por K. HON. Em extrema síntese, a solução avançada propõe uma distribuição geográfica dos serviços informáticos da TPB por diferentes meios, servidores e prestadores de serviços de computação em nuvem, criando uma complexidade na cadeia de fornecimento de serviços informáticos (*supply chain*) e na multi-intermediação: "[o] exemplo do TPB demonstra que os sistemas e procedimentos configurados de determinada forma, usando muitos prestadores de serviços de nuvem, servidores e backups, com extensa aplicação de encriptação, podem ser resilientes e muito protetores (…). Se o país A reclama jurisdição sobre o TPB com base na sua utilização do servidor X localizado no país A, o TPB pode desligar esses servidores, que contém informação encriptada, terminar a relação com X e trocar para outro servidor noutro país. O facto de a informação no servidor X se encontrar encriptada torna mais difícil e quase impossível a A descobrir TPB e identificar os seus utilizadores finais, assim protegendo a confidencialidade. Mesmo que A obtenha a cooperação de X, X não tem acesso inteligível à informação que armazena porque os dados estão encriptados" [1389].

2.4.O desajustamento dos fundamentos das transferências

Outro limite ao regime das transferências, que mina a legitimidade da solução normativa e a sua credibilidade perante a sociedade, é o fosso existente entre a lei no papel e a realidade da sua eventual (ir) relevância. Um dos fatores na origem desta

[1386] K. HON, *Data Localization* cit., p. 278.
[1387] *Idem*, p. 288; John LEYDEN, "Brazilian banker's crypto baffles FBI", *The Register*, 28 de junho de 2010, disponível em https://www.theregister.co.uk/2010/06/28/brazil_banker_crypto_lock_out/ 2010, consultado no dia 30 de setembro de 2018; Spiegel Staff, "Inside the NSA's war on Internet Security", 28 de dezembro de 2014, disponível em http://www.spiegel.de/international/germany/inside-the-nsa-s-war-on-internet-security-a-1010361.html, consultado no dia 30 de setembro de 2018.
[1388] K. HON, *Data Localization* cit., p. 307.
[1389] K. HON, "Cloud computing: geography or technology – virtualisation and control", 2014, disponível em https://www.scl.org/articles/3000-cloud-computing-geography-or-technology-virtualisation-and-control, consultado no dia 30 de setembro de 2018 e, da mesma autora, K. HON, *Data Localization* cit., p. 307.

discrepância é o recorte dos fundamentos das transferências, entendidos como "custos de contexto" desproporcionais para o utilizador dos dados pessoais e desligados do novo contexto tecnológico. Aliás, para alguns autores, esse mesmo contexto proporciona o caminho que deve ser seguido numa próxima reforma do regime das transferências e que passe por absorver soluções mistas, mais flexíveis, ora estritamente jurídicas ora estritamente técnicas ou ambas (2.4.1).

Antes de me debruçar sobre este aspeto, explico os pontos críticos do procedimento de adequação e sugiro algumas melhorias para o mesmo tendo presente que, como referiu o TJ no caso *Schrems,* aquele procedimento deverá dar execução à *obrigação explícita* de proteção dos dados pessoais, prevista no art. 8.º, n.º 1, da Carta, e assegurar a continuidade do nível elevado dessa proteção quando os dados pessoais são transferidos para um país terceiro[1390] (2.4. 2).

Sublinho que o intuito das linhas que se seguem não é questionar a oportunidade de uma restrição das transferências ou da imposição, ao utilizador de dados pessoais, de uma obrigação de "controlo de fronteira" dos dados pessoais. O que discuto é o *modo* de implementar esse controlo.

2.4.1. O procedimento de adequação da Comissão Europeia

O primeiro apontamento a este procedimento prende-se com a amplitude e a complexidade do seu objeto: o ordenamento jurídico de um país terceiro[1391]. Questionando a viabilidade e o rigor de uma análise tão compreensiva, a doutrina desconfia da eficácia do sistema de avaliação e aponta as dificuldades da apreciação de domínios como a proteção de dados pessoais e a privacidade que, por natureza, são *context-bound and linked to culture*[1392].

Em segundo lugar, a realidade demonstra que uma apreciação do ordenamento jurídico alheio, centrada exclusivamente nos critérios de adequação delineados no art. 45.º do RGPD e imune a considerações (e pressões) políticas e diplomáticas, nem sempre é viável. Com efeito, a sua natureza discricionária tem sido apontada como uma

[1390] Acórdão do TJ, Maximillian Schrems c. Data Protection Commissioner, C-363/14, 6 de outubro de 2015, n.º 72.
[1391] Este aspeto foi tido em consideração durante as negociações do RGPD, v. Conselho da UE, "Preparation of ..." cit., nota de rodapé 448. A Alemanha, França e Reino Unido sublinharam "muitas dificuldades práticas e políticas" do "princípio da adequação".
[1392] C. KUNER, "Reality and …" cit., p. 900; G29, "The Future of Privacy", 1 de dezembro de 2009, p. 10 e 11; K. HON, *Data Localization* cit., p. 158.

fragilidade[1393]. Um exemplo da politização deste procedimento ocorreu em 2010 quando o governo da Irlanda congelou uma decisão de adequação sobre Israel com base no alegado envolvimento daquele país na falsificação de passaportes Irlandeses[1394]. C. KUNER refere também os exemplos da Argentina e da Austrália para demonstrar a captura deste procedimento por motivações estritamente políticas[1395].

Em terceiro lugar, a falta de transparência das conclusões e dos estudos que acompanham o procedimento de adequação é outro dos pontos criticados, abrindo a porta ao erro e ao uso indevido do mesmo[1396].

Estes pontos críticos do procedimento de adequação compreendem-se à luz de dois aspetos relacionados entre si: a natureza jurídica da decisão de adequação e o procedimento que a antecede. Quanto ao primeiro, as decisões de adequação são atos secundários, ou melhor, atos de implementação de um ato primário, a Diretiva ou, na atualidade, o RGPD. Os atos de implementação distinguem-se dos atos de delegação por força de um critério que tem sido contestado na doutrina: os atos de implementação, previstos no art. 291.º, do TFUE, são adotados "quando são necessárias condições uniformes de execução dos atos juridicamente vinculativos da União"; por seu turno, os atos de delegação, segundo o art. 290.º, n.º 1, do TFUE, são adotados quando "um ato legislativo" delega na "Comissão o poder de adotar atos não legislativos de alcance geral que completem ou alterem certos elementos não essenciais do ato legislativo". Para P. CRAIG "o critério para a divisão entre estes dois tipos de atos é frágil e difícil de aplicar, colocando em causa a adequação dessa distinção", acrescentando aquele autor que "seguramente existirão muitos casos em que é contestável a verdadeira natureza da medida secundária" [1397]. Não cabe no âmbito deste trabalho entrar nas minudências deste debate, mas para se compreender o *iter* procedimental que antecede a decisão de adequação interessa sublinhar que a opção por uma daquelas categorias de atos jurídicos da UE se reflete ao nível do procedimento de adequação, em especial no que diz respeito ao controlo do exercício dos poderes da COM.

[1393] C. KUNER, "Reality and …" cit., p. 911; G29, "Documento de Trabalho. Transferência de dados ..." cit., p. 30; R. WEBER, "Transborder data ..." cit., p. 124.
[1394] John OATES, "Ireland to block EU-Israel data hoover", *The Register*, 12 de julho de 2010, disponível em https://www.theregister.co.uk/2010/07/12/ireland_israel_passport/, consultado no dia 30 de setembro de 2018.
[1395] C. KUNER, *Transborder* cit., p. 66.
[1396] C. KUNER, "The Internet and ..." cit., p. 25.
[1397] Paul CRAIG, "Delegated Acts, Implementing Acts and the New Comitology Regulation", *ELR*, vol. 36, 2011, p. 671 e 668.

De facto, conforme dispõe o art. 290.º, n.º 2, do TFUE, os atos de delegação são objeto de controlo *ex ante* e *ex post* pelo Conselho e pelo PE[1398]; pelo contrário, os atos de implementação correm termos pelo procedimento de comitologia, já referido anteriormente, plasmado no Regulamento 182/2011 e adotado ao abrigo do art. 291.º, n.º 3, do TFUE. A comitologia, controversa desde a sua origem, parte da premissa de que a implementação de um ato legislativo respeita apenas à COM e aos Estados-Membros, colocando de parte o eventual interesse institucional do PE e do Conselho[1399]. Daí que a história da comitologia se paute por uma constante luta do PE para "conquistar" poderes de controlo de modo a salvaguardar os seus crescentes poderes legislativos[1400]. O art. 11.º do Regulamento 182/2011 atribui ao PE e ao Conselho "direitos de controlo" sobre atos de implementação *ultra vires* que, não obstante, conhecem limites: a COM deve apenas rever o projeto de ato em questão, "tendo em conta as posições expressas" do PE e do Conselho e comunicar-lhes se tenciona "manter, alterar ou retirar o projeto de ato". Portanto, não há um poder de veto sobre o projeto de ato da COM[1401].

Ora, importa agora recordar que, no caso *Schrems,* o TJ determinou que "tendo em conta, por um lado, o importante papel desempenhado pela proteção de dados pessoais (...) e, por outro, o elevado número de pessoas cujos direitos fundamentais podem ser violados em caso de transferência de dados pessoais para um país terceiro que não assegure um nível de proteção adequado, o poder de apreciação da Comissão quanto à adequação do nível de proteção assegurado por um país terceiro é reduzido, pelo que se deve proceder a uma fiscalização estrita das exigências que decorrem do artigo 25.º da Diretiva"[1402]. Creio que este entendimento do tribunal, sugerindo um poder de apreciação da COM "reduzido" e uma "fiscalização estrita" da aplicação do art. 25.º, é difícil de compatibilizar com o tipo e o grau dos "direitos de controlo" atribuídos ao PE e ao Conselho no procedimento de adequação.

[1398] "Os atos legislativos estabelecem explicitamente as condições a que a delegação fica sujeita, que podem ser as seguintes: a) O Parlamento Europeu ou o Conselho podem decidir revogar a delegação"; b) O ato delegado só pode entrar em vigor se, no prazo fixado pelo ato legislativo, não forem formuladas objeções pelo Parlamento Europeu ou pelo Conselho".

[1399] P. CRAIG, "Delegated Acts …" cit., p. 683. Sobre as críticas à comitologia, Steeve PEERS e Marios COSTA, "Accountability for delegated and implementing acts after the Treaty of Lisbon", *ELJ,* vol. 18, n.º 3, 2012, p. 427 e ss..

[1400] S. PEERS e M. COSTA, "Accountability for …" cit., p. 457 e ss..

[1401] P. CRAIG, "Delegated Acts …" cit., p. 683.

[1402] Acórdão do TJ, Maximillian Schrems c. Data Protection Commissioner, C-363/14, 6 de outubro de 2015, n.º 78.

Por outro lado, a falta de transparência do procedimento de adequação é também uma decorrência do método da comitologia[1403]. Por exemplo, segundo o art. 10.º, n.º 5, do Regulamento 182/2011, a informação disponibilizada ao público encontra-se minuciosamente delimitada[1404].

À luz do exposto, em face da indignação da UE após as revelações de ES, por um lado, e atendendo à fundamentação do TJ em *Schrems* em torno das ingerências inaceitáveis aos direitos fundamentais por outro lado, muitos autores perguntam se um ato unilateral, secundário, de implementação, aprovado nos termos descritos, será o instrumento jurídico mais adequado a uma narrativa centrada na proteção efetiva do titular dos dados pessoais[1405]. Advogam que um acordo bilateral seria uma base jurídica mais sólida pois implicaria um processo de negociação mais transparente, obrigaria os EUA (e os países terceiros) a compromissos mais sólidos e, sobretudo, viabilizaria a participação do PE e até do TJ. Veja-se, por exemplo, o caminho seguido no quadro do projeto de acordo entre o Canadá e a UE sobre a transferência e o tratamento dos dados dos registos de identificação dos passageiros, objeto de um escrutínio que incluiu um parecer do TJ[1406]. A intervenção do tribunal neste processo, exemplifica, segundo C. KUNER, uma caraterística do sistema de direitos fundamentais da UE: a autocorreção[1407]. Quer isto dizer que as falhas imputadas a algumas instituições (como a COM e o Conselho) foram posteriormente corrigidas por outras (o TJ). É justamente esta dose de equilíbrio que falta no procedimento de aprovação das decisões de adequação.

Noto que, naquele parecer, a instância da UE assinalou que as transferências de dados para um país terceiro carecem de "um acordo entre a União e o país terceiro em causa, equivalente ao referido acordo, ou de uma decisão da Comissão, para efeitos do artigo 25.º, n.º 6 da Diretiva"[1408]. Aliás, logo no início o tribunal entendeu que aquele acordo

[1403] S. PEERS e M. COSTA, "Accountability for …" cit., p. 427 e 460. Os autores referem que "é lamentável que os novos procedimentos não sejam suficientemente transparentes para assegurar a prestação de contas junto do público".
[1404] P. CRAIG, "Delegated Acts …" cit., p. 683.
[1405] Dan SVANTESSON e Dariusz KLOZA, "Landscape with the rise of data privacy protections", D. SVANTESSON e D. KLOZA (eds.), *Trans-atlantic* cit., p. 564 e ss.; Erich SCHWEIGHOFER, "Principles for US-EU Data Flow Attangements", D. SVANTESSON e D. KLOZA (eds.), *Trans-atlantic* cit., p. 27 e ss.; Richard EPSTEIN, "The ECJ's Fatal Imbalance: Its cavalier treatment of national security issues poses serious risk to public safety and sound commercial practices", *ECLR,* n.º 12, 2016, p. 339.
[1406] Conforme prevê o art. 218.º do TFUE.
[1407] Chistopher KUNER, "International Agreements, Data Protection, and EU Fundamental Rights on the International Stage: Opinion 1/15 (EU-Canada PNR) of the Court of Justice of the EU", *CMLR,* vol. 55, n.º 3, 2018 e Mark DAWSON, *The Governance of EU Fundamental Rights,* Oxford University Press, 2017, p. 113 (edição Kindle).
[1408] Parecer 1/15, 26 de julho de 2017, n.º 214.

visava "criar uma forma de 'decisão de adequação', na aceção do artigo 25.º, n.º 6 da Diretiva 95/46, com vista a oferecer uma base jurídica para a transferência legal dos dados PNR da União para o Canadá"[1409]. Apesar desta leitura do TJ, o RGPD não prevê expressamente esta hipótese como alternativa à decisão de adequação o que, para alguns, é uma oportunidade perdida[1410].

Os problemas aqui enunciados a respeito do procedimento de apreciação da adequação verificam-se noutros domínios nos quais são tomadas decisões políticas através de atos de implementação sem garantir a função institucional do PE e do Conselho[1411]. Veja-se, a este propósito, a recomendação da AG SHARPSTON, nas conclusões do Acórdão *Sophie in't Veld*: "os atos executivos abrangem um amplo leque de diferentes atividades (...) quando essas atividades respeitam a matérias com impacto nos cidadãos da União – em particular, quando incidem sobre os direitos fundamentais desses cidadãos –, a abertura constitui um elemento importante no processo decisório. A transparência fortalece a democracia, permitindo aos cidadãos estar informados e participar na tomada de decisões"[1412].

Dir-se-á que a opção por um ato de implementação é, por um lado, uma resposta à necessidade de garantir "condições uniformes de execução dos atos juridicamente vinculativos" para garantir os efeitos de uma decisão de adequação; e, por outro, cria um expediente procedimental, sem obstáculos e intervenções bloqueantes do PE ou linhas vermelhas do TJ, que flexibiliza a adoção de decisões de adequação imperiosas para sustentar o comércio internacional. Contudo, a expedita adoção do *Privacy Shield* ilustra as consequências desta escolha: uma segurança jurídica aparente e dependente do desfecho das ações junto do TJ cuja intervenção, bem vistas as coisas, tem sido a mais inequívoca via para assegurar a continuidade da proteção do titular dos dados pessoais que o regime das transferências pretende assegurar.

[1409] Parecer 1/15, 26 de julho de 2017, n.º 31.
[1410] Chistopher KUNER, "Data Protection, Data Transfers, and International Agreements: the CJEU's Opinion 1/15", 26 de julho de 2017, disponível em https://verfassungsblog.de/data-protection-data-transfers-and-international-agreements-the-cjeus-opinion-115/, consultado no dia 30 de setembro de 2018.
[1411] P. CRAIG, "Delegated Acts …" cit., p. 686.
[1412] Conclusões do AG no Acórdão do TJ, Sophie In't Veld c. Comissão Europeia, T-310/10, apresentadas em 13 de fevereiro de 2014, n.º 73.

2.4.2. O anacronismo das garantias adequadas

O anacronismo das garantias adequadas funda-se, desde logo, na constatação pós-*Schrems* de que a restrição às transferências, no seu recorte atual, é incapaz de garantir a continuidade da proteção do titular dos dados diante da envergadura dos programas de vigilância estrangeiros. Mas o anacronismo daquelas garantias também é mencionado a propósito da desadequação estrutural das mesmas, da solução normativa que lhes subjaz à luz da realidade empresarial e tecnológica dos nossos tempos. É que essa realidade, caraterizada pela ubiquidade geográfica dos dados pessoais, pela utilização da Internet, dos serviços de computação em nuvem e tantos outros desafios que o futuro reserva à proteção de dados pessoais, é profundamente divergente da situação existente na década de 80, altura em que foi bolado o regime das transferências.

Este desajustamento, já aflorado pela COM em 2003[1413], foi suscitado por alguns Estados-Membros durante as negociações do RGPD[1414] bem como na avaliação de impacto do mesmo: "as normas sobre transferências para países terceiros (...) são desafiadas pela crescente natureza globalizada dos fluxos de dados (isto é, o facto de os dados pessoais cruzarem um grande número de fronteiras virtuais e geográficas, como no quadro da 'computação em nuvem'" [1415].

Autores como K. HON[1416] e C. KUNER[1417], entre outros[1418], opõem-se à atual solução para as transferências, herdada de um passado tecnológico caraterizado por um modelo hoje caduco, designado *mainframe,* numa alusão aos primeiros computadores[1419].

[1413] Cfr. Parte II, Capítulo 3, ponto 3.1.2.

[1414] Questionaram a eficácia deste regime de transferências num quadro de "fluxos massivos de dados pessoais no contexto da computação em nuvem", v. Conselho da UE, "Preparation of ..." cit., nota de rodapé 448.

[1415] Comissão Europeia, "Impact Assessment …" cit., p. 16.

[1416] K. HON, *Data Localization* cit., p. 130.

[1417] C. KUNER, *Transborder* cit., p. 148 e ss..

[1418] François LE SIEUR, "Regulating cross-border data flows and privacy in the networked digital environment and global knowledge economy", *IDPL*, vol. 2, n.º 2, 2012, p. 104; G. GUNASEKARA, "The 'Final' …" cit., p. 149; G. FUSTER, "Un-mapping …" cit., p. 160 e ss.; Jonathan CAVE *et alii*, "Data protection review …" cit., p. secção 3.3.4; Omar TENE, "Reforming Data Protection in Europe and beyond: A Critical Assessment of the Second Wave of Global Privacy Laws", Artemi LOMBARTE *et alii*, *Hacia Un Nuevo Derecho Europeo de Protección de Datos,* Tirant Lo Blanch, 2015, p. 197; Peter BLUME, "EU adequacy decisions: the proposed new possibilities", *IDPL,* vol. 5, n.º 1, 2015, p. 38.

[1419] Desenvolvidamente, sobre o modelo *mainframe*, v. Chris REED, "The law of unintended consequences: embedded business models IT regulation", *JILT*, n.º 2, 2007, p. 1 e ss.; K. HON, *Data Localization* cit., p. 131, 227. Sobre as alterações sociais, empresarias e tecnológicas com impacto nas transferências de dados pessoais, v. Omar TENE, "Privacy: the new generations", *IDPL,* vol. 1, n.º 1, 2011, p. 15 e ss. e OCDE, "Report on the Implementation of the OECD Recommendation on Cross-Border Co-operation in the Enforcement of Laws Protecting Privacy", 2011, p. 15, disponível em http://www.oecd.org/sti/ieconomy/oecdrecommendationoncross-borderco-operationintheenforcementoflawsprotectingprivacy.htm, consultado no dia 30 de setembro de 2018.

Nesse modelo, a um certo conjunto de dados pessoais era possível atribuir uma localização física ou geográfica. Adicionalmente, os movimentos de dados ocorriam, em regra, entre dois pontos, duas entidades apenas e, efetivamente, de um país para um país terceiro. Hoje não será já assim. A própria COM, já em 1992, quando discutia o melhor critério para delimitar o âmbito de aplicação da Diretiva, reconheceu a dificuldade prática de determinar a localização dos dados pessoais no país *x* ou *y*, bem como a crescente dispersão geográfica dos mesmos: "ao abrigo da proposta original o lugar onde se localiza o ficheiro servia para determinar a jurisdição territorial, mas este critério não foi adotado uma vez que a localização do ficheiro ou da operação de tratamento serão com frequência impossíveis de determinar: as operações de tratamento podem ter mais do que um local e ocorrer em vários sítios ao mesmo tempo, em especial no caso de bases de dados ligadas a redes, que são cada vez mais frequentes"[1420].

Esta transformação a que me refiro é bem sintetizada por K. HON na descrição que traça dos desenvolvimentos tecnológicos, sociais e organizacionais na origem da complexidade dos atuais fluxos de dados pessoais e de um novo paradigma: "com a natureza contínua e multiponto dos modernos fluxos de dados internacionais as transmissões deixaram de ser ponto-a-ponto e passam a ser parte de uma série de processos em rede para alcançar um resultado económico (...). Observam-se, em particular, os aumentos do tratamento de dados distribuído e a automação do mesmo em diferentes hardwares situados em diferentes locais"[1421]. Por outras palavras, nos dias de hoje uma transferência de dados pessoais não se realiza *apenas* para *um* país terceiro pelo que um regime assente nessa premissa afasta-se da realidade[1422]. Mas a discrepância entre as conotações semânticas de "fluxos" e "transferências" e a realidade das práticas de tratamento de dados pessoais nos dias de hoje manifestar-se-á ainda da seguinte forma: os primeiros são percecionados e regulados como uma mudança, um movimento, de um lugar (A) para outro (B) quando, na realidade, as operações em causam tipicamente consistem numa duplicação dos dados, que estão acessíveis em A e em B, podendo o exportador controlar o acesso que o importador tem aos dados pessoais[1423].

[1420] Comissão Europeia, "Amended proposal …" cit., p. 13.
[1421] K. HON, *Data Localization* cit., p. 133 e ss.; Paul SCHWARTZ, "Managing global data privacy: cross-border information flows in a networked environment", *The Privacy Projects*, 2009, p. 4, disponível em http://theprivacyprojects.org/wp-content/uploads/2009/08/The-Privacy-Projects-Paul-Schwartz-Global-Data-Flows-20093.pdf, consultado no dia 30 de setembro de 2018.
[1422] McKay CUNNINGHAM, "Complying with International Data Protection Law", *UCLR,* vol. 84, n.º 2, 2016, p. 421.
[1423] G. FUSTER, "Un-mapping …" cit., p. 162.

O automatismo da dispersão e duplicação dos dados digitais e a arbitrariedade desses processos criam obstáculos à regulação das transferências, sobretudo se o aplicador insiste num critério *geográfico* e numa abordagem sobre os dados pessoais "contidos" numa infraestrutura (um servidor ou um centro de dados) situada numa localização específica[1424].

O exemplo paradigmático desta disrupção já não é apenas a Internet[1425] mas, também, a computação em nuvem. Além da doutrina[1426], o G29, em 2012, confirmou a dificuldade de saber, "em tempo real, onde os dados estão localizados, armazenados ou em trânsito" pelo que se verificam "limitações nos instrumentos jurídicos tradicionais que proporcionam um quadro regulamentar aplicável às transferências"[1427]. Algumas autoridades confessaram que "as regras das transferências de dados pessoais da Diretiva são irrealistas em face do enorme volume de fluxos de dados em termos globais"[1428]. No terreno, os utilizadores de dados pessoais confessam dificuldades em adaptar os fundamentos disponíveis aos processos organizacionais e às transações modernas de *outsourcing*[1429]. Além da computação em nuvem, recentemente a autoridade de controlo

---

[1424] Jennifer DASKAL, "The Un-territoriality of Data", *YLJ,* n.º 125, 2015, p. 365 e Xawery KONARSKI *et alii*, "Reforming the Data Protection Package: Study for the European Parliament's Committee on Internal Market and Consumer Protection", 2012, p. 12, disponível em http://www.europarl.europa.eu/document/activities/cont/201209/20120928ATT52488/20120928ATT52488EN.pdf, consultado no dia 30 de setembro de 2018.

[1425] Como sublinha C. KUNER: "(…) talvez o principal problema seja a relação desproporcional entre o aumento dos dados transferidos online e as possibilidades limitadas de garantir o cumprimento da regulação aplicável às mesmas (…)", v. C. KUNER, *Transborder* cit., p. 154 e 155.

[1426] Cecilia RIGAUDIAS, "Condiciones para las transferências internacionales de datos personales em servicioes de cloud", Ricardo MARTINEZ, *Derecho Y Cloud Computing,* Thomson Reuter, 2012, p. 109 e ss.; Dominic N. STAIGER, "Cross-border data flow in the cloud between the EU and the US", Anne CHEUNG e Rolf WEBER, *Privacy and Legal Issues in Cloud Computing,* Edward Elgar Publishing, 2015, p. 96; Javier Puyol MONTERO, *Algunas consideraciones sobre Cloud Computing,* AEPD, 2013, p. 154; K. HON, *Data Localization* cit., p. 2 e ss.; S. ESAYAS, "A walk in to the …" cit., p. 665.

[1427] G29, "Parecer 5/2012 ..." cit., p. 21.

[1428] Citando o anterior presidente do ICO, Richard Thomas, v. Neil ROBINSON *et alii,* "Review of the European Data Protection Diretive", *RAND Cambridge,* 2009, p. 2, disponível em https://www.rand.org/pubs/technical_reports/TR710.html, consultado no dia 30 de setembro de 2018.

[1429] Comissão Europeia, "Summary of Replies to the Public Consultation about the Future Legal Framework for Protecting Personal Data", 2010, disponível em http://ec.europa.eu/justice/news/consulting_public/0003/summary_replies_en.pdf , consultado no dia 30 de setembro de 2018; Kommerskollegium, "No Transfer, No Trade: The Importance of Cross-Border Data Transfers for Companies Based in Sweden", 2014, p. 19, disponível em https://www.kommers.se/Documents/dokumentarkiv/publikationer/2014/No_Transfer_No_Trade_webb.pdf, consultado no dia 30 de setembro de 2018; ECIPE, "The Economic Importance of Getting Data Protection Right: Protecting Privacy, Transmiting Data, Moving Commerce", 2013, p. 9 e 13, disponível em https://www.uschamber.com/sites/default/files/documents/files/020508_EconomicImportance_Final_Revised_lr.pdf, consultado no dia 30 de setembro de 2018; K. HON, *Data Localization* cit., p. 194; Boris WOJTAN, "The new EU Model Clauses: one step forward, two steps back?", *IDPL,* n.º 1, vol. 1, 2011, p. 80; Emmanuelle BARTOLI, "Data transfers in the could: discussion paper for the Commission's Expert Group on Cloud Computing Contracts", 2014, p. 8, disponível em

francesa reconheceu que a *blockchain* coloca desafios ao regime das transferências dada a dificuldade de identificar a localização exata dos chamados "mineiros"[1430].

Sucede que estas dificuldades demovem, em especial PME's e *startups*, do esforço de conformidade, sobretudo quando são conjugadas com a perceção da falta de recursos das autoridades de controlo e da complexidade do regime[1431]. Tanto gera um enfraquecimento do efeito normativo da regulação das transferências diagnosticado pela doutrina e pelos Estados durante a negociação do RGPD[1432]. Na preparação da reforma de 2012, um grupo de trabalho patrocinado pela COM sublinhou que "a principal conclusão é que o respeito pelas regras das transferências de dados é, em geral, muito reduzido (...) e o art. 26 é raramente respeitado"[1433].

Quanto à efetividade da tutela providenciada pelas garantias adequadas, o G29, logo em 1998, admitiu o "enorme desafio" de "encontrar meios que possam compensar a ausência de mecanismos de controlo e de aplicação [no país terceiro] e que possam proporcionar apoio, assistência e, em último caso, reparação, a uma pessoa cujos dados tenham sido objeto de tratamento", sinalizando igualmente as dificuldades em encorajar o destinatário a respeitar as garantias adequadas e, em especial, a prestar o apoio e assistência aos titulares dos dados[1434]. Ou seja, o papel que o legislador julga atribuir às garantias adequadas, como forma de "compensar de forma satisfatória a ausência de um

---

http://collections.internetmemory.org/haeu/20171122154227/http://ec.europa.eu/justice/contract/files/expert_groups/discussion_paper_data_transfers_in_cloud.pdf, consultado no dia 30 de setembro de 2018.

[1430] "Premiers éléments d'analyse de la CNIL. Blockchain", setembro de 2018, p. 6, disponível em https://www.cnil.fr/sites/default/files/atoms/files/la_blockchain.pdf, consultado no dia 30 de setembro de 2018.

[1431] O próprio G29, logo em 1997, teve em atenção estes aspectos, bem como "o elevado número de transferências de dados pessoais efetuadas diariamente a partir da Comunidade e à multiplicidade das pessoas envolvidas nessas transferências, nenhum Estado-membro (...)", sugerindo que as autoridades de supervisão canalizassem recursos e esforços em relação a transferências que colocam maiores riscos, v. G29, "Primeiras orientações ..." p. 5. Em sentido próximo, v. Comissão Europeia, "Impact Assessment …" cit., p. 10; C. REED, *Making Laws for* cit., capítulo 8; Dimitra KAMARINOU, "International transfers of personal data and corporate compliance under Directive 95/46/EC, the draft Regulation and the international community: part 1", *CL*, n.º 18, vol. 2, 2013, p. 49 e ss.; Jonathan CAVE *et alii*, "Data protection review …" cit., p. 61; K. HON, *Data Localization* cit., p. 152, 189, 194, 206, 222; N. ROBINSON *et alii,* "Review of the …" cit., p. 229; Richard JONES, "Extra territoriality and international transfers under the draft Regulation", *PDP,* vol. 12, n.º 2, 2013, p. 6 e ss..

[1432] C. KUNER, *Transborder* cit., p. 146, 154; C. REED, *Making Laws for* cit., cap. 8; Conselho da UE, "Preparation of ..." cit., nota de rodapé 448; D. KORF, "Existing case-law …" cit., p. 62; K. HON, *Data Localization* cit., p. 153, 223 e 226 e ss..

[1433] Douwe KORFF, "Data protection laws in the EU: the difficulties in meeting the challenges posed by global social and technical developments", 2010, n.os 76 a 79, disponível em https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1638949, consultado no dia 30 de setembro de 2018.

[1434] G29, "Documento de Trabalho. Transferência ..." cit., p. 19 e ss. e 22.

nível de proteção adequada no país terceiro"[1435] não supre as insuficiências da tutela daquele país terceiro nem a falta de controlo das autoridades da UE sobre o importador.

Ao arrepio disto, qual o contributo do RGPD para este diagnóstico tão pessimista? Desde logo, é evidente o esforço do legislador em alargar o leque de garantias adequadas ao dispor dos utilizadores de dados pessoais, em especial as RVAE, os procedimentos de certificação e os códigos de conduta.

Com efeito, as RVAE serão um instrumento mais flexível e, por exemplo, a sua adequação para as cadeias de subcontratação típicas da computação em nuvem poderá caber no campo do "grupo de empresas envolvidas numa atividade económica conjunta" conforme se lê no art. 47.º do RGPD. Porém, a doutrina permanece cética quanto a esta hipótese: "mesmo se um "grupo de empresas" abrange prestadores de serviços de computação em nuvem com sub-prestadores juridicamente distintos daqueles, a relação entre ambos teria de ser próxima e de longo prazo para que ambos estivessem dispostos a prosseguir os termos de adoção das RVAE no âmbito das quais o membro da UE assumirá responsabilidade"[1436]. A duração do controlo de conformidade realizado pela autoridade de controlo (meses e até anos[1437]) e, agora, o procedimento de controlo de coerência[1438] poderão desincentivar os subcontratantes[1439].

Os códigos de conduta e as certificações são uma das grandes novidades do RGPD. Todavia, devo recordar que são acompanhados de "compromissos voluntários e com força executiva" assumidos pelos "importadores" que colocarão os mesmos desafios enunciados pelo G29 a propósito da solução contratual. Em termos de praticabilidade, os ínvios caminhos para a sua validação, a burocracia, o tempo e os custos associados a estas garantias adequadas podem torná-las pouco atrativas para PME's. Por exemplo, uma *startup* portuguesa, a Movvo, demorou dois anos a obter um selo de privacidade de uma entidade certificadora alemã, a EuroPriSe[1440].

[1435] *Idem*, p. 17.
[1436] K. HON, *Data Localization* cit., p. 209
[1437] Segundo o IAPP, em 2013, a aprovação das RVAE na CNIL demorava cerca de 5 meses, no ICO 18 meses, v. "International Data Transfers: Reviewing the Options", 2013, Londres, disponível em https://iapp.org/resources/article/international-data-transfers-considering-your-options/ , consultado no dia 30 de setembro de 2018.
[1438] Artigos 47.º, n.º 1, 63.º e 64.º e, desenvolvendo, cfr. G29, "Working Document …" cit., p. 1 e ss..
[1439] Adicionalmente os custos de manutenção podem ser elevados, variando entre os €20.000 e €1 milhão, consoante o número de subsidiárias, v. Comissão Europeia, "Comission Staff Working ..." cit., Anexo 4, p. 177.
[1440] Amir MIZROCH, "For location-tracking startup, a data-privacy odyssey", *Digits,* 2014, disponível em https://blogs.wsj.com/digits/2014/11/04/for-location-tracking-startup-a-data-privacy-odyssey/, consultado no dia 30 de setembro de 2018.

Ao manter inalterada a estrutura essencial da Diretiva, o RGPD não abraçou as teses de certa doutrina, cujos expoentes máximos são C. KUNER e K. HON, sugerindo um modelo assente no *princípio da responsabilidade* do exportador[1441]. Caberia a este avaliar a adequação da transferência em face do risco que coloca, em função de todas as circunstâncias que a rodeiem, em especial o tipo de dados, o potencial dano decorrente de uma utilização ou divulgação indevida, o local de destino dos dados, entre outros elementos[1442]. Uma transferência que coloque um "elevado risco" não mereceria ser tratada da mesma forma que uma transferência com "risco residual". De seguida, o utilizador dos dados deveria adotar e documentar medidas de mitigação razoáveis (*reasonable steps*[1443]) para acautelar os riscos encontrados, medidas essas não taxativas ou pré-determinadas pelo legislador, e que podem variar consoante o risco. A título ilustrativo refere-se a adoção de medidas de segurança (como a encriptação ou a *tokenização* e outras ferramentas para controlar o acesso inteligível aos dados pessoais[1444], ou a dispersão automatizada dos dados pessoais por vários pontos geográficos[1445]), a mera exigência de uma auditoria imparcial ao importador dos dados ou a consulta prévia à autoridade de controlo[1446]. O que esta proposta pretende é romper com uma visão formalista do regime das transferências segundo a qual apenas um instrumento jurídico pré-determinado é capaz de garantir a continuidade da proteção do titular dos dados: "[a] prioridade conferida no RGPD a medidas jurídicas/contratuais sobre medidas técnicas não se compreende. Ignorar o valor da tecnologia para proteger dados pessoais e confiar apenas em soluções jurídicas é retrógrado e contraproducente" [1447].

Adicionalmente, como sustenta C. KUNER[1448], a opção legislativa pelo princípio da responsabilidade do exportador exige, naturalmente, uma fiscalização rigorosa e capaz das autoridades de controlo, que gozam da prerrogativa de bloquear as transferências de dados pessoais, como reconheceu o TJ no caso *Schrems.*

São, grosso modo, duas as vantagens desta nova estratégia de política legislativa:

[1441] C. KUNER, *Transborder* cit., p. 173 e K. HON, *Data Localization* cit., p. 333.
[1442] Sugerindo a realização de uma avaliação de impacto, J. KULESZA, "Transboundary data ..." cit., p. 304.
[1443] K. HON, *Data Localization* cit., p. 289.
[1444] *Idem*, p. 66, 145, 161, 189, 261, 318 e ss.. Um pouco adiante explico este conceito.
[1445] *Idem*, p. 276.
[1446] C. KUNER, *Transborder* cit., p. 173 e 175.
[1447] K. HON, *Data Localization* cit., p. 155 e 189. Em sentido semelhante, v. C. KUNER, *Transborder* cit., p. 96 e ss; Joel REIDENBERG, "Workshop 4: International issues: international data transfers, applicable law and jurisdiction", Comissão Europeia, 2002, p. 2.
[1448] C. KUNER, *Transborder* cit., p. 174.

(i) Em primeiro lugar, facilitaria um esquema de regulação mais flexível, menos burocrático, mais realista e respeitável: os "fundamentos" seriam substituídos por uma espécie de autoavaliação da adequação à semelhança do sucedido durante a vigência da Diretiva em alguns Estado-Membros, como no Reino Unido. Tal não irá bulir com o *dever de proteger* o titular dos dados pessoais quando transferidos: dele não decorre (leia-se, do art. 8.º da CDFUE ou do art. 16.º do TFUE) um determinismo quanto ao *como* da sua concretização, cabendo essa opção no espectro da liberdade de conformação do legislador[1449]. A proteção do titular dos dados pessoais não implicará, necessariamente, a apresentação de um fundamento *jurídico,* previamente especificado pelo legislador, para as transferências de dados pessoais. Como sublinha C. KUNER, "os direitos fundamentais exigem que os Estados adotem medidas para que o titular dos dados não seja privado da proteção quando os dados atravessam as fronteiras nacionais, mas não obriga à adoção de um determinado método para prosseguir esse objetivo"[1450]. Portanto, não creio que exista nesta proposta qualquer défice de proteção censurável até porque não desvirtua a ideia de que o utilizador dos dados pessoais deve "preconizar soluções que facultem às pessoas em causa a garantia de que, mesmo depois de transferidos os seus dados, continuarão a beneficiar dos direitos fundamentais e das garantias a que têm direito na UE"[1451];

(ii) A segunda vantagem é a abertura deste caminho a soluções estritamente tecnológicas cujo mérito vem sendo reconhecido para a tutela efetiva dos titulares dos dados pessoais[1452] e, inclusive, em sede de transferências. Por exemplo, o grupo que reúne as autoridades de controlo alemãs (*Dusseldorfer Kreis*) considerou que a legislação alemã de proteção de dados pessoais não seria aplicável, em certas circunstâncias, a

[1449] J. Pereira da SILVA, *Deveres,* cit., p. 578.
[1450] C. KUNER, *Transborder* cit., p. 172
[1451] G29, "Documento de trabalho sobre uma interpretação comum ..." cit., p. 10.
[1452] A melhor ilustração esta adesão do legislador aos contributos da tecnologia para proteção dos dados pessoais é o conceito de proteção de dados desde a conceção e por defeito consagrado no art. 25.º do RGPD.

> transferências de dados pessoais encriptados[1453]. Em Portugal, a CNPD tem exigido, no domínio da investigação clínica, que as transmissões de dados pessoais "codificados", ou seja, "no destino não é conhecida a chave da codificação e, nessa medida, quem é o titular dos dados", não requerem o cumprimento dos requisitos do regime das transferências[1454]. De resto, a COM reconheceu o valor da encriptação, em especial para a computação em nuvem[1455]. K. HON sustenta que o controlo do acesso a dados pessoais inteligíveis é fulcral porquanto "para os dados digitais isto significa a capacidade de entender o (s) padrão (s) de bits que representam o conteúdo informacional, bem como restringir e alterar o acesso a esse padrão (...). Dados ininteligíveis podem ser transmitidos ou compartilhados mas os destinatários não conseguem retirar conhecimento das informações contidas em tais dados; dados ininteligíveis são, por definição, desprovidos de conteúdo informativo" [1456]. Por seu turno, a ideia de controlo de acesso pressupõe um acesso lógico (remoto, através de um de software que permita uma pessoa autorizada, depois de fazer o log in no sistema, utilizar os dados pessoais, independentemente da sua localização geográfica) e não necessariamente físico, a capacidade de ler e modificar (acrescentar, apagar ou alterar) os dados pessoais, de ceder e bloquear essas mesmas ações a terceiros.

Apesar destas vantagens o RGPD não abraçou o princípio da responsabilidade do exportador. Na origem desta postura cautelosa estarão vários fatores. Em primeiro lugar,

---

[1453] Numa situação descrita nos seguintes termos: "O prestador de serviços de tratamento de dados 1, residente na UE, é instruído por uma empresa sua cliente, residente num país terceiro, para tratar dados pessoais e subsequentemente transferi-los para a sua cliente. Os dados são oriundos da UE. Foram recolhidos ou pela própria cliente ou, segundo instruções da mesma, pelo prestador de serviços de tratamento de dados 2 (…) O prestador de serviços de tratamento de dados 1 recebe os dados de forma encriptada e não tem conhecimento do conteúdo dos mesmos". Concluiu-se que neste caso, "a legislação de proteção de dados alemã não é aplicável a nenhum dos intervenientes (nem a 1, 2 ou à empresa cliente de ambos" uma vez que os dados circulam num circuito fechado ou encriptado", v. Dusseldorf Kreis, "Fallgruppen zur Internationalen Auftragsdatenverarbeitung, Handreichung des Dusseldorf Kreises zur rechtlichen Bewertung", 28 de março de 2007, disponível em https://datenschutz-berlin.de/pdf/publikationen/duesseldorfer-kreis/2007/HandreichungApril2007.pdf, consultado no dia 30 de setembro de 2018.

[1454] CNPD, "Deliberação n.º 1704/2015 aplicável aos tratamentos de dados pessoais efetuados no âmbito de Investigação Clínica", p. 18.

[1455] Comissão Europeia, "What does the Commission Mean by Secure Cloud Computing Services in Europe?", MEMO/13/898, 2013, disponível em http://europa.eu/rapid/press-release_MEMO-13-898_en.htm, consultado no dia 30 de setembro de 2018.

[1456] K. HON, *Data Localization* cit., p. 66, 145, 161, 189, 261, 318 e ss.

o legislador não reconheceu a equivalência, em termos de proteção do titular dos dados, entre o princípio da responsabilidade do exportador e as garantias adequadas ou, melhor, as fórmulas normativas que lhes subjazem. Acresce que não parece existir um consenso científico quanto à "força" das medidas tecnológicas[1457]. Como nota C. KUNER a propósito da encriptação, esta não é uma fórmula mágica que previne todo o tipo de riscos em relação aos dados pessoais transferidos: "protege os dados de acessos não autorizados enquanto os mesmos estão a ser transferidos ou armazenados, mas não os protege, por exemplo, do uso ilegal por destinatários autorizados que os podem desencriptar"[1458]. Todavia, o relevo que pode ser conferido a um tipo de proteção tecnológica é bem visível num exemplo simples: se armazenar dados pessoais numa *pen* que viaja comigo para fora da UE, para ser guardada por um terceiro, a encriptação dos dados antes da minha deslocação, da qual apenas eu tenho a chave, não será mais protetora de acessos indevidos do que a celebração de um contrato com o terceiro no qual este garante que irá, ele próprio, proceder à encriptação dos dados pessoais?

Em segundo lugar, a adesão estrita ao princípio da responsabilidade do exportador implicaria a abolição do procedimento de adequação e forçava a UE a abdicar do *soft power* de "regulador transnacional" [1459]. Há quem diga que, a longo prazo, o comércio internacional beneficiará do resultado do processo de harmonização que lhe subjaz por potenciar a livre circulação de dados pessoais[1460].

Em todo o caso, aos poucos, há indicadores de que o legislador se vai deixando seduzir por um esquema mais flexível e centrado na componente organizacional em detrimento da componente geográfica, numa valorização do papel do exportador para acautelar a continuidade da proteção do titular dos dados pessoais, sendo também visível um caminho de prudente flexibilização da regulação das transferências[1461]. De facto, aos poucos, o legislador vai introduzindo concretizações do princípio da responsabilidade em certos fundamentos, como é caso das cláusulas contratuais-tipo de 2004[1462] ou das

[1457] *Idem*, p. 224 e 287; C. BOWDEN, "The US Surveillance ..." cit., p. 14; I. BROWN e D. KORFF, "Foreign surveillance ..." cit., p. 244.
[1458] C. KUNER, *Transborder* cit., p. 97.
[1459] K. HON, *Data Localization* cit., p. 25 e 149.
[1460] Danilo DONEDA, "International Data Transfers in Brazil", D. J. SVANTESSON e D. KLOZA (eds.), *Trans-Atlantic* cit., p. 150. Para o autor, quanto mais harmonizadas estiverem as regras de proteção de dados menos obstáculos haverá para a sua circulação.
[1461] K. HON, *Data Localization* cit., p. 56; K. HON e C. MILLARD, "Data Export …" cit., p. 8; P. BLUME, "EU adequacy …" cit., p. 38.
[1462] Entre as obrigações do exportador encontra-se a garantia de que "são envidados esforços razoáveis no intuito de assegurar que o importador de dados possa cumprir as obrigações legais" (cláusula I. (b)) e, além disto, a pedido do exportador, o importador tem de dar provas de que tem recursos financeiros suficientes

RVAE[1463]. Deve ainda referir-se que a introdução daquele princípio na regulação das transferências foi aflorada pelo G29, em 2009[1464], indo ao encontro das sugestões da indústria[1465] e vigorando noutras ordens jurídicas. O exemplo mais citado é o Canadá: "o ponto crítico para as organizações que 'externalizam' tratamentos de dados pessoais além do território do Canadá é saber se implementam medidas razoáveis para proteger a privacidade e a segurança dos dados na sua custódia e controlo" [1466].

Acresce ainda que, incrementar a utilização de "medidas técnicas" para a proteção dos dados pessoais é um desígnio do RGPD, além da abertura já referida a soluções tecnológicas, como exponencia a "proteção de dados desde a conceção e por defeito"[1467]. Em todo o caso, no que respeita especificamente às transferências, estas só não encontram "barreiras" quando os dados pessoais foram anonimizados, de forma irreversível, desprezando-se as outras formas de os camuflar[1468]. Não obstante, sempre se pode argumentar que, sob reserva de autorização prévia, o art. 46.º, n.º 3, *in fine*, do RGPD, abre a porta à adoção de garantias adequadas técnicas ou tecnológicas.

---

para preencher as suas obrigações (cláusula II.(f)), v. o anexo da Decisão da Comissão Europeia de 27 de Dezembro de 2004 que altera a Decisão 2001/497/CE no que se refere à introdução de um conjunto alternativo de cláusula contratuais típicas aplicáveis à transferência de dados pessoais para países terceiros.

[1463] Segundo o G29, "as regras empresariais obrigatórias são um exemplo da forma de aplicar princípios de proteção de dados com base no princípio da responsabilidade", v. "Parecer 3/2010 ..." cit., p. 16. Para uma análise exaustiva da relação entre as RVAE e o princípio da responsabilidade, v. L. MOEREL, *Binding Corporate* cit., p. 175 e ss..

[1464] "(…) os responsáveis pelo tratamento permanecem responsáveis pela proteção dos dados pessoais mesmo que esses dados sejam transferidos para terceiros", v. G29, "Contribution on ..." cit., p. 3 e ss..

[1465] As respostas dos vários interessados à consulta realizada pela Comissão Europeia em 2010 apontam neste sentido, v. Comissão Europeia, "Proposta ..." cit., anexo 2, p. 86. Veja-se igualmente a sugestão da Vodafone, dando nota da necessidade de garantir a proteção dos dados pessoais "para onde quer que estes viagem" mas suportando a tese de que a responsabilidade recai no exportador e peticionando a abolição dos atuais fundamentos das transferências com base na sua ineficácia para um "incremento real da proteção" das pessoas singulares, v. Vodafone, "A Comprehensive Approach on Personal Data Protection in the European Union: Vodafone Response", 2011, p. 19, disponível em http://ec.europa.%20eu/justice/news/%20consulting_public/0006/contributions/o, consultado no dia 30 de setembro de 2018.

[1466] Information and Privacy Commissioner of Ontario, "Reviewing the Licensing Automation System of the Ministry of National Resources", 2012, p. 6.

[1467] Art. 24.º e 25.º do RGPD.

[1468] Considerando 26; C. KUNER, *Transborder* cit., p. 99; K. HON, *Data Localization* cit., p. 333.

Síntese conclusiva

1. Os interesses prosseguidos pelas duas manifestações de extraterritorialidade identificadas na Parte II conhecem vários limites. No que respeita à proteção do titular dos dados pessoais por força do alargamento do âmbito de aplicação segundo os artigos 4.º da Diretiva e 3.º do RGPD, ergue-se o obstáculo das "duas velocidades" da jurisdição extraterritorial, identificado na Parte I desta tese.

2. Para contornar esta dificuldade e potenciar a proteção do titular dos dados pessoais, o legislador dispõe de um conjunto de mecanismos internos e externos:

   2.1. Ao nível *interno*, a responsabilização do representante depende de vários fatores: (i) da disposição do utilizador de dados pessoais para nomear um representante (ii) das soluções do direito interno onde este se encontrar. Adicionalmente, a adoção de medidas de destruição do mercado desejado pelo infrator estrangeiro, balizadas por critérios de proporcionalidade, podem constituir uma ferramenta ao dispor da entidade do foro para exercer uma dose de controlo sobre utilizadores de dados pessoais cuja presença no respetivo território é meramente digital. Por último, não são de excluir géneros de adesão voluntária ao direito estrangeiro motivados por fatores como a reputação, o bom nome e a confiança do consumidor;

   2.2. Ao nível *externo*, os mecanismos ao dispor da UE dependem da colaboração dos outros países e, em especial, do crescimento de uma "Comunidade de direito" no domínio da proteção de dados pessoais.

3. No Capítulo 1, identifiquei outros limites à aplicação do art. 3.º do RGPD além das "duas velocidades" da jurisdição extraterritorial. O primeiro, manifestado, por exemplo, na adoção de legislação bloqueante, não se fez sentir durante a vigência da Diretiva pelo que tendo a excluí-lo no longo prazo, sobretudo em face da aceitação e razoabilidade das novas regras do número 2 daquele artigo. O segundo limite, os conflitos de jurisdição, são inevitáveis num contexto de pluralismo jurídico. A sua solução há-de ser sempre casuística e negociada, pelo menos enquanto não existir um acordo global quanto à jurisdição sobre os tratamentos de dados pessoais. Por último,

a indeterminabilidade da extraterritorialidade limita a capacidade dos utilizadores de dados pessoais identificarem, afinal, se o RGPD se lhes aplica ou não. As imprecisões enunciadas, que merecem ser esclarecidas, podem minar a credibilidade e legitimidade do DUE, à semelhança do que vem sucedendo noutras áreas[1469].

4. Em relação aos limites à manifestação de extraterritorialidade identificada no regime das transferências, recordo que o aprofundamento da dimensão económica ou "integracionista" do regime geral de proteção de dados pessoais depara-se, desde 1995, com divergências ao nível do direito interno dos Estados-Membros. Ou seja, não é exagerada a descrição de uma UE a várias velocidades no domínio da proteção de dados pessoais. Daí, em 2012, a opção por um regulamento, ainda que com "alma de Diretiva". Essas assimetrias internas refletem-se no capítulo das transferências marcado por uma esquizofrenia de definições e entendimentos sobre as mesmas. Acresce que o RGPD foi uma oportunidade perdida para moderar esta patologia que, agora, poderá ser medicada pelo CEPD ou pelo TJ.

5. O segundo limite identificado no Capítulo 2 prende-se com a relação entre o âmbito de aplicação da Diretiva e do RGPD e o regime das transferências. Servindo os mesmos interesses e, portanto, sendo "armas do mesmo arsenal", há quem sugira uma coordenação entre ambos de modo a evitar a sua sobreposição em situações de tratamentos de dados pessoais realizados por um utilizador de dados pessoais situado fora do território da UE mas abrangido pelo DUE. No passado, o G29 manifestou-se favorável à aplicação cumulativa de ambas as normas em relação àqueles sujeitos mas, no quadro do RGPD, este é um ponto que carece de esclarecimento pelo CEPD e que deverá ter em conta o que se entende por transferência.

6. Por fim, outros dois limites se ergueram nos últimos anos ao regime das transferências:

   6.1. A vigilância de países terceiros e a evolução tecnológica e organizacional. Em relação ao primeiro, o caso *Schrems* veio demonstrar que a UE não tem sido bem-sucedida na garantia efetiva do direito fundamental à proteção de dados pessoais.

[1469] Analisando o "âmbito global" do DUE e os problemas de legitimidade associados, v. E. FAHEY, *The Global* cit., p. 5 e ss..

Nem o procedimento de adequação, cujas limitações enunciei, nem as garantias adequadas, servem o propósito de garantir a continuidade da proteção do titular dos dados pessoais quando os mesmos são transferidos para países terceiros nos quais vigoram programas de vigilância com reduzidas garantias para os vigiados. Alimenta-se, assim, uma expetativa perniciosa aos titulares dos dados ou, melhor, uma *ilusão* de que estão a ser protegidos;

6.2. Em relação à evolução tecnológica e organizacional, o anacronismo das garantias adequadas parece persistir no RGPD no sentido em que serão insuficientes para abarcar certo tipo de fluxos de dados pessoais, como os da computação em nuvem. Apesar do esforço do legislador em alargar a cartilha de garantias adequadas, a introdução de um princípio da responsabilidade do exportador, a solução proposta por alguns autores, mereceu uma adesão conservadora e cirúrgica.

Teses

1. Enquanto instrumento jurídico ao dispor da UE, sem constrangimentos absolutos ao seu exercício, a extraterritorialidade encontra terreno fértil na atualidade internacional caraterizada por fatores como a vulnerabilidade e exposição daquela à globalização, os imperativos de proteção dos direitos fundamentais em relação a "perigos com conexões internacionais" ou ingerências oriundas do estrangeiro, a necessidade de acautelar interesses económicos e a incapacidade da comunidade internacional alcançar consensos em certos domínios que requerem soluções para desafios de âmbito transnacional e com impacto interno.

2. A matéria da proteção de dados pessoais é uma espécie de *pot pourri* de todos esses fatores em virtude, sobretudo, da dimensão global dos tratamentos de dados pessoais e da inexistência de um tratado global prescrevendo regras sobre os mesmos, incluindo no que ao exercício de jurisdição prescritiva diz respeito.

3. Neste quadro, a regulação dos tratamentos de dados pessoais segundo uma lógica estrita de territorialidade estaria condenada ao fracasso. Desta premissa parte o regime geral de proteção de dados pessoais da UE onde se encontram manifestações de extraterritorialidade com o intuito de impor e de influenciar comportamentos, tanto de utilizadores de dados pessoais, independentemente da sua localização geográfica, como de outros países e dos respetivos ordenamentos jurídicos.

4. As manifestações de extraterritorialidade identificadas justificam-se, por um lado, na dimensão jusfundamental do regime geral de proteção de dados pessoais da UE, na medida em que aquela assumiu o dever de proteger o titular dos dados pessoais independentemente do local onde se realiza o tratamento dos seus dados e do local onde se encontra o utilizador dos mesmos; por outro lado, a integridade e eficácia da dimensão económica deste regime, de criação de um mercado único digital, depende da existência de condições de igualdade para todos os operadores que ali atuam, mesmo para os estrangeiros.

5. Com efeito, o alargamento do âmbito de aplicação, prosseguido tanto pelo art. 4.º da Diretiva como pelo art. 3.º do RGPD, visa *impor* determinar condições aos tratamentos de dados pessoais de qualquer utilizador de dados pessoais com uma conexão com o mercado da UE, seja porque existe um estabelecimento daquele ali ou porque os tratamentos respeitam a um titular dos dados que ali se encontra.

6. Já no que respeita à *influência* de outros países e ordenamentos jurídicos, a mesma é prosseguida pelo regime das transferências de dados pessoais pela estatuição de uma "cláusula de equivalência" que viabiliza a exportação do padrão subjacente ao regime geral de proteção de dados pessoais. Deste modo a UE cria um estímulo à adoção de legislação interna "adequada" à luz daquele padrão e, além disto, promove o desenvolvimento do DIP, em especial da Convenção n.º 108 do CdE.

7. Julgo que esta estratégia de influência deve ser enquadrada nas descrições doutrinais da UE enquanto regulador transnacional ou global, enquanto empreendedor normativo, um papel que tem assumido noutros domínios regulatórios. Com efeito, na matéria da proteção de dados pessoais, a União tem cumprido as orientações do *princípio da responsabilidade*, dispostas no art. 3.º, n.º 5, do TUE, em especial de promoção dos seus valores e interesses nas relações com o resto do mundo.

8. Porém, a eficácia das duas manifestações de extraterritorialidade tratadas conhece vários limites cuja solução não depende exclusivamente da União mas, sobretudo, da cooperação internacional. Ainda assim, proponho algumas soluções ao seu alcance, e dos seus Estados-Membros, como a incorporação da teoria das "medidas de destruição de mercado", o princípio da efetividade, o esclarecimento de alguns conceitos e da articulação entre as duas manifestações de extraterritorialidade identificadas.

9. Os limites que, a meu ver, se afiguram como os mais difíceis de solucionar respeitam ao surgimento de conflitos de jurisdição, e à incapacidade de a UE de, por um lado, garantir efetivamente o direito fundamental à proteção de dados pessoais em relação à vigilância de países terceiros e, por outro lado, de responder,

de forma realista, aos desafios que o desenvolvimento tecnológico lhe vai apresentando.

Bibliografia

ABI-SAAB, Georges, "Cours général de droit international", *RCADI*, vol. 207, 1987, p. 294 e ss.

AKEHURST, Michael, "Jurisdiction in International Law", *BYIL*, n.º 46, 1972-1973, p. 145 e ss.

ALBRECHT, Jan, "Das Neue EU-Datenschutzrecht – von der Richtlinie zur Verordnung"*, Computer und recht*, n.º 2, 2016, p. 88 e ss.

ALEXANDRINO, José de Melo, *A Estruturação do Sistema de Direitos, Liberdades e Garantias na Constituição Portuguesa,* Vol. II, Almedina, Coimbra, 2006

ALLENBY, Braden, "Governance and Technology Systems: The Challenge of Emerging Technologies", Gary Marchant *et alii* (eds.), *The Growing Gap between Emerging Technologies and Legal-Ethical Oversight,* vol. 7, Springer, Dordrecht, 2011, p. 3 e ss.

ALMEIDA, Francisco Ferreira de, *Os Crimes Contra a Humanidade no Actual Direito Internacional Penal,* Almedina, Coimbra, 2009

- *Direito Internacional Público,* Coimbra Editora, Coimbra, 2003

ALSENOY, Brendan e KOEKKOEK, Marieke, "Internet and Jurisdiction after Google Spain: the extraterritorial reach of the 'right to be delisted'", *IDPL,* vol. 5, n.º 2, 2015, p. 105 e ss.

ÁLVAREZ, Luis, "La responsabilidade del responsable", José Piñar MAÑAS *et alii* (dir.), *Reglamento General De Protección De Datos. Hacia um nuevo modelo europeo de privacidade,* Reus, Madrid, 2016, p. 275 e ss.

AMATO, Giuliano, *Antitrust and the Bounds of Power – The Dilemma of Liberal Democracy in the History of the Market,* Hart Publishing, Oxford/Portland, 1997

AMTENBRINK, Fabian, "What Role for the European Union in Shaping Global Financial Governance", Bart VAN VOOREN, Steven BLOCKMANS e Jan WOUTERS, (eds.)*, The EU's Role in Global Governance. The Legal Dimension*, Oxford University Press, Oxford, p. 243 e ss.

ANDERSON, Winston, "Foreign Orders and Local Land and the Caribbean Gets its Own Version of Duke v Andler", *ICLQ,* n.º 48, 1999, p. 167 e ss.

ANDRADE, José Vieira de, *Os Direitos Fundamentais na Constituição Portuguesa de 1976,* 3ª edição, Almedina, Coimbra, 2007

ANDRADE, Norberto, "Oblivion, the right to be diferente from oneself. Reproposin the right to be forgotten", *RIDP,* n.º 13, 2012, p. 125 e ss.

ANKERSMIT, Laurens e LAWRENCE, Jessis e DAVIES, Garreth, "Diverging EU and WTO Perspectives on Extraterritorial Process Regulation", *MJIL,* n.º 21, 2012, p. 23 e ss.

APOLINÁRIO, Marisa, *O Estado Regulador: o novo papel do Estado,* Almedina, Coimbra, 2016

ARAGÃO, Alexandra, "Aplicação nacional do princípio da precaução", *Colóquios 2011-2012,* Associação dos Magistrados da Jurisdição Administrativa e Fiscal de Portugal, 2013, p. 159 e ss..

- "Princípio da precaução: manual de instruções", *Revista do Cedoua*, vol. 2, n.º 11, 2008, p. 16 e ss.

ASENSIO, Pedro, "Competencia y Derecho aplicable en el Reglamento General sobre Proteccion de Datos de la Unión Europea", *Revista española de Derecho Internacional,* 69, n.º 1, 2017, p. 75 e ss.

- *Derecho privado de Internet,* Civitas, Pamplona, 2015

ASINARI, Maria, "International Aspects of Personal Data Protection: *Quo Vadis EU?* Maria ASINARI e Pablo PALAZZI (eds.), *Challenges of Privacy and Data Protection Law,* Buylant, Bruxelas, 2008, p. 405 e ss.

- "Is there any Room for Privacy and Protection within WTO Rules?", *ECLR*, n.º 9, 2002, p. 249 e ss.

- "The WTO and the Protection of Personal Data. Do EU Measures Fall within Gats Exception? Which Future for Data Protection within the WTO e-commerce Context?", 18th BILETA Conference: Controlling Information in the Online Environment, Abril de 2013, disponível em http://www.bileta.ac.uk/content/files/conference%20papers/2003/The%20WTO%20and%20the%20Protection%20of%20Personal%20Data.%20Do%20EU%20Measures%20Fall%20within%20GATS%20Exception.pdf

AUBY, Jean-Bérnard, "L'internationalisation du Droit des contrats publics", *DA,* n.º 8-9, 2003, p. 5 e ss.

AUDIT, Bernard, "Extraterritorialité et commerce international – L'affaire du gazoduc sibérien", *RCDI,* n.º 72, 1983, p. 101 e ss.

BAKER, Roger, "Offshore IT outsourcing and the 8th Data Protection Principle: legal and regulatory requirements – with reference to financial services", *IJLIT,* vol. 14, n.º 1, 2006, p. 1 e ss.

BARTELS, Lorand, "The WTO Legality of the Application of the EU's Emission Trading System to Aviation", *EJIL,* vol. 23, n.º 2, Maio de 2012, p. 429 e ss.

BARTOLI, Emmanuelle, "Data transfers in the could: discussion paper for the Commission's Expert Group on Cloud Computing Contracts", 2014, disponível em

http://collections.internetmemory.org/haeu/20171122154227/http://ec.europa.eu/justice/contract/files/expert_groups/discussion_paper_data_transfers_in_cloud.pdf

BASEDOW, Jurgen, *The Law of Open Societies. Private Ordering and Public Regulation in the Conflict of Laws,* Brill, Leiden, 2012

- "International Antitrust: From Extraterritorial Application to Harmonization", *LLR*, vol. 60, n.º 4, 2000, p. 1042 e ss.

- "Souveraineté Territoriale et Globalisation des Marchés: Le Domaine d'Application des Lois Contre Les Restrictions de La Concurrence", *RCADI,* vol. 264, 1999, p. 9 e ss.

BASTOS, Fernando Loureiro, "Algumas notas sobre globalização e extraterritorialidade", *Liber Amicorum Fausto de Quadros*, vol. I, 2016, p. 437 e ss.

BATIFFOL, Henri, "La règle de droit international prive", Chaim PERELMAN, (org.), *La règle de droit,* Bruylant, Bruxelas, 1971, p. 214 e ss..

BATTINI, Stefano, "Globalisation and Extraterritoriality: an Unexceptional Exception", Gordon ANTHONY, JEAN-BERNARD AUBY, JOHN MORISON, TOM ZWART (eds.), *Values in Global Administrative Law,* Hart Publishing, Oxford/Portland, 2011, p. 61 e ss.

- "Extraterritoriality: an Unexceptional Exception", *Séminaire de droit administrative, européen et global – Extraterritoriality and Administrative Law,* Charie M.A.D.P./SciencesPo, 2008, p. 61 e ss., disponível em https://www.irpa.eu/wp-content/uploads/2011/09/Extraterritoriality-an-Unexceptional-Exception2.pdf

BECK, Ulrich, *La sociedade del riesgo global*, Siglo XXI, Madrid, 2006

- *La sociedade del riesgo: Hacia una nueva modernidade*, Paidos Iberica, Barcelona, 2006

BENNETT, Colin e RAAB, Charles, *The Governance of Privacy: Policy Instruments in Global Perspective,* MIT Press, Cambridge, 2006

BERGKAMP, Lucas, "The Privacy Fallacy: Adverse Effects of Europe's Data Protection in an Information-Driven Economy", *CLSR,* vol. 18, n.º 1, 2002, p. 31 e ss.

BERMAN, Paul, "The Globalization of Jurisdiction", *PLR,* n.º 151, 2002, p. 311 e ss.

- *Global Legal Pluralism,* Cambridge University Press, Cambridge, 2012

BERNAUER, Thomas, GAMPFER, Robert e KACHI, Aya, "European unilateralism and involuntary burden-sharing in global climate politics: A public opinion perspective from the other side", *EUP,* vol. 15, n.º 1, 2014, p. 132 e ss..

BIANCHI, Andreas, "Extraterritoriality and Export Controls: Some Remarks on the Alleged Antinomy Between European and U.S. Approaches", *GYIL,* vol. 35, 1992, p. 366 e ss.

BIGNAMI, Francesca, "The Case for Tolerant Constitutional Patriotism: The Right to Privacy before the European Courts", *CILJ,* n.º 41, 2008, p. 211 e ss.

BIGNAMI, Francesca e RESTA, Giorgio, "Transatlantic Privacy Regulation: Conflict and Cooperation", *LCP*, vol. 78, n.º 4, 2015, p. 248 e ss.

BING, Jon, "Data Protection, Jurisdiction and the Choice of Law", *Privacy Law & Policy Reporter,* n.º 92, 1999, disponível em http://www.uio.no/studier/emner/jus/jus/JUR5620/v08/undervisningsmateriale/Data%20Protection,%20jurisdiction%20and%20the%20choice%20of%20law.rtf

BIRCHFIELD, Vicky, "Coercion with Kid Gloves: The European Union's Role in Shaping a Global Regulatory Framework for Aircraft Emissions", *JEPP,* vol. 22, n.º 9, 2015, p. 1276 e ss.

BLUME, Peter, "EU adequacy decisions: the proposed new possibilities", *IDPL,* vol. 5, n.º 1, 2015, p. 34 e ss.

BODANSKY, Daniel, "What's So Bad About Unilateral Action to Protect the Environment?", *EJIL,* n.º 11, 2000, p. 339 e ss.

BOEHM, Franziska, "Assessing the new instruments in EU-US surveillance and data protection law – US legislation, Privacy Shield and Umbrella Agreement", *EDPLR,* n.º 3, 2016, p. 1 e ss..

BOTELHO, Catarina Santos, "Novo ou velho direito? – O Direito ao esquecimento e o princípio da proporcionalidade no constitucionalismo global", *AB Instantia,* vol. V, n.º 7, 2017, p. 49 e ss..

BOUGIAKIOTIS, Emmanouil, "The enforcement of the Google Spain Ruling", *IJLIT,* n.º 24, 2016, p. 331 e ss.

BOYLE, Alan, "EU Unilateralism and the Law of the Sea", *TIJMCL,* vol. 21, n.º 1, p. 15 e ss.

BOWETT, Derek, "Jurisdiction: Changing Patterns of Authority over Activities and Resources", *BYIL*, vol. 53, 1982, p. 1 e ss..

BRITO, Wladimir, *Responsabilidade de Proteger no Direito Internacional,* Almedina, Coimbra, 2016

BRILMAYER, Lea, "Extraterritorial Application of American Law: A Methodological and Constitutional Appraisal", *LCP*, vol. 50, n.º 3, summer, 1987, p. 11 e ss.

BRKAN, Maja, "The Unstoppable Expansion of the EU Fundamental Right to Data Protection. Little Shop of Horrors?", *MJ,* n.º 23, 2016, p. 812 e ss.

BROWNLIE, Ian, *Principles of International Law,* Clarendon Press, Londres, 4ª ed., 1990

BRUMMER, Chris, "Territoriality as a regulatory technique: notes from the finantial crisis", *UCLR,* vol. 79, n.º 2, 2011, p. 504 e ss..

BOWDEN, Casper, "The US surveillance programs and their impact on EU citizens' fundamental rights: note for the European Parliament's Committee on Civil Liberties, Justice and Home Affairs", 2013, disponível em http://www.europarl.europa.eu/meetdocs/2009_2014/documents/libe/dv/briefingnote_/briefingnote_en.pdf

BROWN, Ian *et alii*, "Toward Multilateral Standards for Foreign Surveillance Reform", Russell MILLER (ed.), *Privacy and Power. A Transatlantic Dialogue in the Shadow of the NSA-Affair,* Cambridge University Press, Cambridge, 2017, p. 462 e ss.

BROWN, Ian e KORFF, Douwe, "Foreign Surveillance: law and practice in a global digital environment", *EHRLR,* n.º 3, 2014, p. 243 e ss.

BROWNSWORD, Roger, *Law and Technologies of the Twenty-Century: Text and materials,* Cambridge University Press, Cambridge, 2012

- *Rights, Regulation and the Technological Revolution,* Oxford University Press, Oxford, 2008

BRUENING, Paula e WATERMAN, Krasnow, "Data tagging for new models of information governance", *EEE Security & Privacy,* n.º 8, setembro-outubro, 2010, p. 64 e ss.

BURCA, Gráinne de, "After the EU Charter of Fundamental Rights: The Court of Justice as a Human Rights Adjudicator?", *MJECL*, n.º 168, 2013, p. 168 e ss.

BURKERT, Herbert, "Towards a New Generation of Data Protection legislation", Serge GUTWIRTH, Yves POULLET, Paul de HERT e Cécile de TERWANGNE, *Reinventing Data Protection?* Springer, Dordrecht, 2009, p. 335 e ss.

- "Institutions of Data Protection – An Attempt at a Functional Explanation of European National Data", *CLJ,* n.º 3, 1981, p. 167 e ss.

BURNETT, Susan, "U.S. Judicial Imperialism Post '*Empagran v. f. Hoffmann-Laroche'?:* Conflicts of Jurisdiction and International Comity in Extraterritorial Antitrust", *EILR,* n.º 18, 2004, p. 629 e ss.

BUXBAUM, Hannah, "Territory, territoriality and the resolution of jurisdictional conflict", *AJCL*, n.º 3, 2009, p. 631 e ss.

BYGRAVE, Lee, "Data Privacy Law and the Internet: Policy Challenges", Norman WITZLEB, David LINDSAY, Moira PATERSON e Sharon RODRICK, *Emerging Challenges in Privacy Law: Comparative Perspective,* Cambridge University Press, Cambridge, 2014, p. 277 e ss..

- "Privacy and data protection in an international perspective", *SSL*, n.º 56, 2010, p. 166 e ss.

- *Data Protection Law. Approaching Its Rationale, Logic and Limits,* Wolters Kluwer, Haia, 2003

- "Determining applicable law pursuant to European Data Protection Legislation", *CLSR,* n.º 16, 2000, p. 252 e ss.;

CAEIRO, Pedro, *Da Jurisdição Penal do Estado,* Coimbra Editora, Coimbra, 2010

CALO, Ryan, "The Boundaries of Privacy Harm", *ILJ,* n.º 86, 2011, p. 1132 e ss.

CALVÃO, Filipa, *Direito da Proteção de Dados Pessoais,* Universidade Católica, Lisboa, 2018

- "O direito fundamental à proteção dos dados pessoais e a privacidade 40 anos depois", Manuel VAZ, Catarina BOTELHO, Luís TERRINHA e Pedro COUTINHO, Jornadas nos quarenta anos da constituição da república portuguesa, Universidade Católica, Lisboa, 2017, p. 87 e ss.

- "A proteção de dados pessoais na internet: desenvolvimentos recentes", *RDI*, n.º 2, 2015, p. 6791 e ss.

- "O modelo de supervisão de tratamento de dados pessoais na União Europeia: da atual Diretiva ao futuro Regulamento", *FDPD,* n.º 1, julho de 2015, p. 37 e ss.., disponível em https://www.cnpd.pt/bin/revistaforum/forum2015_1/index.html#40

CAMPOS, André Santos, *Glosas Abertas de Filosofia do Direito. Um tronco comum para juristas e filósofos,* Quid Juris, Lisboa, 2013

CANANEA, Giacint, "I pubblici poteri nello spazio giuridico globale", *RTDP,* n.º 1, 2003, p. 1 e ss.

CANIZZARRO, Enzo, "The EU's Human Rights Obligations in Relation to Policies With Extraterritorial Effects: A Reply to Lorend Bartels", *EJIL,* vol. 25, n.º 4, 2015, p. 1093 e ss.

CANNIZARO, Enzo e BONAFÈ, Beatrice,"Beyond the archetypes of modern legal thought. Appraising old and new forms of interaction between legal orders", Miguel POAIRES MADURO, Kaarlo TUORI e Suvi SANKARI, (eds.), *Transnational Law. Rethinking European Law and Legal Thinking*, Cambridge University Press, Cambridge, 2014, p. 78 e ss.

CANNATACI, Joseph, "Report of the Special Rapporteur on the right to privacy", 24 de fevereiro de 2017, disponível em https://www.ohchr.org/EN/Issues/Privacy/SR/Pages/SRPrivacyIndex.aspx

- "Draft Legal Instrument on Government-led Surveillance and Privacy", 10 de janeiro de 2018, disponível em https://www.ohchr.org/Documents/Issues/Privacy/DraftLegalInstrumentGovernmentLed.pdf

CANOTILHO, José J. J. e MOREIRA, Vital, *Constituição da República Portuguesa,* vol. I., Coimbra Editora, Coimbra, 2014

CARDOSO, José, Autoridades Administrativas Independentes e Constituição, Coimbra Editora, Coimbra, 2002

CARDONA, Maria Celeste, *Contributo para o conceito e a natureza das entidades administrativas independentes – As Autoridades Reguladoras,* Almedina, Coimbra, 2016

CARRERA, Sergio, FUSTER, Gloria, GUILD, Elspeth e MITSILEGAS, Valsamis, *Access to Electronic Data by Third-Country Law Enforcement Authorities. Challenges to EU Rule of Law and Fundamental Rights,* Centre for European Policy Studies, 2015, disponível em https://www.ceps.eu/system/files/Access%20to%20Electronic%20Data%20%2B%20covers_0.pdf

CARULLA, Santiago, "Aplicación Territorial del Reglamento", José Piñar MAÑAS, *Reglamento General de Protección de Datos. Hacia un nuevo modelo europeo de privacidade,* Reus, Madrid, 2016, p. 77 e ss.

CASAGRAN, Cristina, *Global Data Protection in the Field of Law Enforcement. An EU Perspective,* Londres, Routledge, 2017

CASTRO, Catarina Sarmento e, "40 anos de 'Utilização da Informática – o artigo 35.º da Constituição da República Portuguesa", *EP,* vol. 3, n.º 3, 2016, p. 42 e ss., disponível online em http://e-publica.pt/volumes/v3n3/pdf/Vol.3-Nº3-Art.04.pdf

- "A jurisprudência do Tribunal de Justiça da União Europeia, o Regulamento Geral sobre a proteção de dados pessoais e as novas perspetivas para o direito ao esquecimento na Europa", *Estudos em Homenagem ao Conselheiro Presidente Rui Moura Ramos*, vol. 1, Almedina, Lisboa, 2016, p. 1047 e ss.

CASTRO, Raquel, *Constituição, Lei e Regulação dos Media,* Almedina, Coimbra, 2016

CATE, Fred, KUNER, Christopher, MILLARD, Christopher, SVANTESSON, Dan, "The (Data Privacy) Law Hasn't Even Checked in When Technology Takes Off", *IDPL,* vol. 4, n.º 3, 2014, p. 175 e ss.

CAVE, Jonathan, SCHINDLER, Rebecca, ROBINSON, Neil, HORVATH, Veronika, CASTLE-CLARKE, Sophie, ROOSENDAAL, Arnold, KOTTERINK, Bas, "Data protection review: impact on EU innovation and competitiveness – study for the European Parliament's Committee on Industry, Research and Energy", 2012, disponível em http://www.europarl.europa.eu/RegData/etudes/etudes/join/2012/492463/IPOL-ITRE_ET(2012)492463_EN.pdf

CHANDER, Anupam e UYÊ, Lê, "Data Nationalism", *EmLR,* 2015, n.º 64, p. 677 e ss.

COHAN, John, "Sovereignty in a Postsovereign World", *FJIL,* n.º 18, 2006, p. 907 e ss..

COLANGELO, Anthony, "Constitutional Limits on extraterritorial jurisdiction: Terrorism and the intersection of national and international law*", HILJ*, n.º 48, 2007, p. 126 e ss.

- "What is Extraterritorial Jurisdiction?", *CLR*, vol. 99, 2014, p. 1303 e ss.

COLLINGRIDGE, David, *The Social Control Technology,* St. Martin's Press, Nova Iorque, 1980

CONFORTI, Benedetto, *International Law and the Role of Domestic Legal Systems,* Martinus Nijhoff, Leiden/Boston, 1995

- "The Theory of Competence in Verdross", *EJIL*, vol. 5, 1994, p. 70 e ss.

CORDEIRO, António Menezes, "Dados pessoais: conceito, extensão e limites", Centro de Investigação de Direito Privado da FDUL, 2018, disponível online em https://blook.pt/publications/publication/e38a9928dbce/

CORREIA, António, *Lições de Direito Internacional Privado,* vol. I, Almedina, Coimbra, 2000

COSTA, Luiz, "Privacy and the precautionary principle", *CLSR,* n.º 28, 2012, p.14 e ss.

COUDRAY, Ludovic, *La Protéction des données personelles dans l'Union européene: Naissance et consecration d'un droit fundamental,* Éditions universitaires européennes, Paris, 2010

COUGHAN, Steve, "Global reach, Local grasp: Constructing extraterritorial jurisdiction in the Age of Globalization", *Report addressed to the Law Commission of Canada*, 23 de junho de 2006, disponível em https://dalspace.library.dal.ca/bitstream/handle/10222/10268/Coughlan_Currie%20et%20al.%20Extraterritoriality%20EN.pdf?sequence=1&isAllowed=y

CRAIG, Paul, "Delegated Acts, Implementing Acts and the New Comitology Regulation", *ELR*, vol. 36, 2011, p. 671 e ss.

CRESPI, Selena, "Diritti fondamentali, Corte di giustizia e riforma del Sistema UE di protezione dei dati", *RIDPC,* 2015, p. 819 e ss.

CUNHA, Joaquim Silva, *Direito Internacional Público, Relações Internacionais (Aspetos fundamentais do seu regime),* Lisboa, Instituto Superior de Ciências Sociais e Políticas, 1990, policopiado

CZERNIAWSKI, Michael, "Do We Need the 'Use of Equipment' as a factor for the territorial applicability of the EU Data Protection Regime?", Dan SVANTESSON e Dariusz KLOZA (eds.), *Trans-atlantic data privacy as a challenge for democracy,* Intersentia, Cambridge, 2017, p. 221 e ss.

D'AMATO, Anthony, "Domestic Jurisdiction", *Encyclopedia of Public International Law,* vol. I, 1992, p. 1090 e ss.

DAMMANN, Ulrich e SIMITIS, Spiros, *EG-Datenschutzrichtlinie Kommentar,* Nomos, Baden-Baden, 1997

DASKAL, Jennifer, "The Un-territoriality of Data", *YLJ,* n.º 125, 2015, p. 326 e ss.

DAVIES, Gareth, "International Trade, Extraterritorial Power, and Global Constitutionalism: A Perspective from Constitutional Pluralism", *GLJ,* vol. 13, n.º 11, 2012, p. 1203 e ss.

- "Is Mutual Recognition an Alternative to Harmonization? Lessons on Trade and Tolerance of Diversity from the EU", Lorand BARTELS e Frederico ORTINO (eds.), *Regional Trade Agreements and WTO Legal System,* Oxford University Press, Oxford, 2006

DEMARET, Paul, "L'extraterritorialité des lois et les relations transatlantiques: une question de droit ou de diplomatie?", *RTDE*, vol. 21, n.º 1, 1985, p. 1 e ss.

DIACAKIS, Nicolas, *Problèmes Liés Aux Effets extraterritoriaux des normes communautaires,* Bruylant, Bruxelas, 2000

DIMITROVA, Anna, "Balancing National Security and Data Protection: The Role of EU and US Policy-Makers and Courts before and after the NSA Affair", *JCMS,* vol. 56, 2018, p. 751 e ss.

DIX, Alexander, "The International Working Group on Data Protection in Telecommunications: Contributions to Transnational Privacy Enforcement", D. WRIGHT e P. DE HERT, (eds.), *Enforcing Privacy. Regulatory, Legal and Technology,* Springer, Dordrecht, 2016, p. 183 e ss.

- "The Commission's Data Protection Reform After Snowden's Summer", *Intereconomics,* n.º 5, 2013, p. 268 e ss.

DOBSON, Natalie e RYNGAERT, Cedric, EU 'Extraterritorial' Regulation of Maritime Emissions", *ICLQ,* vol. 66, n.º 2, 2017, p. 295 e ss..

DODGE, William, "The Public-Private Distinction in the Conflict of Laws", *DJCIL,* vol. 18, 2008, p. 371 e ss.

DOHMAN, Spiecker, "A new framework for information markets: Google Spain", *CMLR,* n.º 52, 2015, p. 1033 e ss.

DONEDA, Danilo, "International Data Transfers in Brazil", D. J. SVANTESSON e D. KLOZA (eds.), Dan SVANTESSON e Dariusz KLOZA (eds.), *Trans-atlantic data privacy as a challenge for democracy,* Intersentia, Cambridge, 2017, p. 149 e ss.

DOUZINAS, Costas, "The Metaphysics of Jurisdiction", Shaun MCVEIGH (ED.), *Jurisprudence of Jurisdiction,* Routledge, Londres, 2007, p. 7 e ss.

DUARTE, Maria Luísa, *Direitos Internacional Público e Ordem Jurídica Global do Século XXI*, Coimbra Editora, Coimbra, 2014

Editorial Note, "The applicability of the Antitrust Laws to International Cartels Involving Foreign Governments", *YLJ,* vol. 91, n.º 4, 1982, p. 785 e ss.

Editorial Note, "Predictability and Comity: Toward Commons Principles of Extraterritorial Jurisdiction", *HLR,* n.º 98, 1985, p. 1310 e ss.

Editorial Comment, "Extraterritorial Application of United States Law: The Case of Export Controls", *UPLR,* vol. 132, 1984, p. 355 e ss.

Editorial Note, "Developments in the Law-Extra-territoriality", *HLR,* n.º 124, 2011, p. 1226 e ss.

EHLERMANN, Claus, "Compétition entre Systèmes Reglementaires", *RMCUE,* n.º 387, avril, 1995, p. 220 e ss..

EPSTEIN, Richard, "The ECJ's Fatal Imbalance: Its cavalier treatment of national security issues poses serious risk to public safety and sound commercial practices", *ECLR,* n.º 12, 2016, p. 330 e ss.

ESAYAS, Samson, "A walk in to the Cloud and Cloudy it Remains: The Challenges and Prospects of 'Processing' and 'Transferring' Personal Data", *CLSR,* n.º 28, 2012, p. 662 e ss.

ESTADELLA-YUSTE, Olga, "The Draft Directive of the European Community Regarding the Protection of Personal Data", *ICLQ*, vol. 41, n.º 1, p. 170 e ss.

FABBRINI, Frederico, "The EU Charter of Fundamental Rights and the Rights to Data Privacy: The EU Court of Justice as a Human Rights Court", Sybe de VRIES (ed.), *Five Years of Legally Binding Charter of Fundamental Rights,* Hart Publishing, Oxford/Portland, 2015

FAHEY, Elaine, *The Global Reach of EU Law,* Routledge, Londres, 2017

FARINHO, Domingos Soares, "(Un)Safe Harbour: Comentário à decisão do TJUE C-362/14 e suas consequências legais", *FDPD,* n.º 2, 2016, p. 109 e ss.

FERREIRA, Eduardo Paz e MORAIS, Luís, "A Regulação sectorial da economia – introdução e perspetiva geral", E. Paz FERREIRA, L. MORAIS e G. ANASTÁCIO, *Regulação em Portugal: Novos Tempos, Novo Modelo?* Almedina, Coimbra, 2009, p. 7 e ss.

FISCHER-LESCANO, Andreas e TEUBNER, Gunther, "Regime-Collisions: The Vain Search for Legal Unity in the Fragmentation of Global Law", *MIJIL,* vol. 25, 2003, p. 999 e ss.

FRAYSSINET, Jean, "L'Union Européenne et la protection des données personnelles circulent sur l'Internet", Annie BLANDIN-OBERNESSE, (dir.), *L'Union Européenne et Internet,* Éditions Apogée, Paris, 2001

FRIEDEL-SOUCHU, Evelyne, *Extraterritorialité du droit de la concurrence aux etats-unis et dans la communauté européene,* LGDJ, Bruxelas, 1994

FUSTER, Gloria, "Un-mapping Personal Data Transfers", *EDPL,* n.º 2, 2016, p. 160 e ss.

- *The Emergence of Personal Data Protection as a Fundamental Right of the EU,* Springer, Dordrecht, 2014

FUSTER, Gloria e GELLERT, Raphael, "The Fundamental Right of Data Protection in the European Union: In Search of an Uncharted Right", *IRLCT,* n.º 26, 2012, p. 73 e ss.

GAKH, Maxim, "Argentina's Protection of Personal Data: Initiation and Response", *I/S: A Journal of Law and Policy*, vol. 2, n.º 3, 2006, p. 781 e ss.

GAYO, Miguel, "Aproximación basada en el riesgo, evaluación de impacto relative a la protección de datos personales y consulta previa a la autoridad de control", José Piñar MAÑAS (dir.), *Reglamento General De Protección De Datos. Hacia um nuevo modelo europeo de privacidade,* Reus, Madrid, 2016, p. 351 e ss.

GEHRING, Markus e GENEST, Alexandre, "Disputes on sustainable development in the WTO regime", Marie-Claire SEGGER e Christopher WEERAMANTRY, *Sustainable Development Principles in the Decisions of International Courts and Tribunals. 1992-2012,* Routledge, Londres*,* 2017, p. 365 e ss..

GELLERT, Raphael, "We Have Always Managed Risks in Data Protection Law: Understanding the Similarities and Differences Between the Rights-Based and the Risk-based Approaches to Data Protection", *EDPL,* n.º 4, 2016, p. 481 e ss.

- "Data protection: a risk regulation? Between the risk management of everything and the precautionary alternative", *IDPL,* vol. 5, n.º 1, 2015, p. 3 e ss.

GIBNEY, Mark, "The Extraterritorial Application of US Law: The Perversion of Democratic Governance, the Reversal of Institutional Roles, and the Imperative of Establishing Normative Principles", *BCICLR,* vol. 19, n.º 2, 1996, p. 320 e ss..

GIL, Ana Rita *Imigração e Direitos Humanos,* Petrony, 2017

GILARDI, Fabrizio, "Transnational diffusion: Norms, ideas, and policies", Walter CARLSNAES, Thomas RISSE-KAPPEN, Beth SIMMONS, (eds.), *Handbook of International Relations,* SAGE Publications, Washington D.C., 2012, p. 453 e ss.

GOLDMAN, Eric, "Data Mining and Attention Consumption", Katherine STRANDBURG e Daniela RAICU (eds.), *Privacy and Technologies of Identity,* Springer, Dordrecht, 2005, p. 225 e ss.

GOLDSMITH, Jack, "The Internet and the abiding significance of territorial sovereignty", *IJGLS,* n.º 5, 1998, p. 475 e ss..

GOLDSMITH, Jack e WU, Tim, *Who controls the Internet? Illusions of a Borderless World,* Oxford University Press, Oxford, 2008

GOMES, Carla Amado, *Risco e Modificação do Ato Autorizativo Concretizador de Deveres de Proteção do Ambiente,* 2007, disponível em http://www.fd.unl.pt/docentes_docs/ma/cg_ma_17157.pdf

- "A Evolução do Conceito de Soberania – Tendências Recentes", *Scientia Iuridica*, Julho-Dezembro de 1998, Tomo XLVII, n.os 274/276, p. 185 e ss.

GÓMEZ, Alberto, "Los códigos de conducta en el reglamento general de protección de datos", José Piñar MAÑAS (dir.), *Reglamento General De Protección De Datos. Hacia um nuevo modelo europeo de privacidade,* Reus, Madrid, 2016, p. 389 e ss.

GONÇALVES, Anabela, *Da Responsabilidade Extracontratual em Direito Internacional Privado. A Mudança de Paradigma,* Almedina, Coimbra, 2013

GONÇALVES, Maria Eduarda, "The EU data protection reform and the challenges of big data: remaining uncertainties and ways forward", *ICTL,* vol. 26, n.º 2, 2017, p. 90 e ss.

- *Direito da Informação – Novos Direitos e Formas de Regulação na Sociedade da Informação,* 2ª ed., Almedina, Coimbra, 2003

GONÇALVES, Pedro, "Regulação Administrativa e Contrato", *Estudos em Homenagem ao Prof. Doutor Sérvulo Correia,* vol. II, Coimbra Editora, Coimbra, 2010, p. 987 e ss.

- "Direito Administrativo da Regulação", *Regulação, Electricidade e Telecomunicações,* Coimbra Editora, 2008

- *Entidades Privadas com Poderes Públicos,* Almedina, Coimbra, 2005

GOTLIEB, Allan, DALFEN, Charles, KATZ, Kenneth, "The Transborder Transfer of Information by Communications and Computer Systems: Issues and Approaches to Guiding Principles", *AJIL,* vol. 68, n.º 2, p. 227 e ss.

GRAFENSTEIN, Maximilian, *The Principle of Purpose Limitation in Data Protection Law,* Nomos, Baden-Baden, 2017

GRANT, Hazel e CROWTHER, Hannah, "How Effective Are Fines in Enforcing Privacy?", David WRIGHT e Paul DE HERT, *Enforcing Privacy. Regulatory, Legal and Technological Approaches,* Springer, Dordrecht, 2016, p. 287 e ss.

GREENLEAF, Graham, "Data protection Convention 108 accession eligibility: 80 parties now possible", *PLBIR,* n.º 148, 2017, p. 12 e ss.

- *Asian Data Privacy Laws. Trade and Human Rights Perspectives,* Oxford University Press, Oxford, 2014

- "Global data privacy laws 2015: 109 countries, with European laws now in a minority", *PLB,* n.º 133, 2015, disponível em https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2603529

- "Morocco and Uruguay start Convention 108's journey to global privacy treaty", *PLBIR*, n.º 122, Abril de 2013

- "'Modernising Data Protection Convention 108: A Safe Basis for a Global Privacy Treaty?", *CLSR*, vol. 29, n.º 4, 2013, p. 430 e ss.

- "The influence of European Privacy Standards Outside Europe: Implications for Globalisation of Convention 108", *IDPL,* vol. 2, n.º 2, 2012, p. 68 e ss.

- "Do not dismiss 'adequacy': European data privacy standards are entrenched", *PLB,* n.º 114, dezembro de 2011, p. 16 e ss.

GRZEGORCZYK, Christophe, MICHAUT, Françoise e TROPER, Michel (eds.), *Le positivisme juridique,* LGDJ, Bruxelas, 1993

GUERRERO, María del Carmen, *El impacto de Internet en el derecho fundamental a la protección de datos de carácter personal,* Civitas, Pamplona, 2006

GUNASEKARA, Gehan, "The 'Final' Privacy Frontier? Regulating Trans-Border Data Flows" *IJLIT,* vol. 17, n.º 2, 2009, p. 147 e ss.

HAFETZ, Jonathan, "The Possibilities and Limits of Corporations as Privacy Protectors in the Digital Age", David COLE, Frederico FABBRINI e Stephen SCHULHOFER (eds.), *Surveillance, Privacy and Trans-Atlantic Relations,* Hart Publishing, Oxford/Portland, 2017, p. 91 e ss.

HARTMAN, Jacques, "The European Emissions Trading System and Extraterritorial Jurisdiction", *EIJL Analysis*, 23 de abril de 2012, disponível online em https://www.ejiltalk.org/the-european-emissions-trading-system-and-extraterritorial-jurisdiction/

HARTZOG, Woodrow, *Privacy's Blueprint. The Battle to Control the Design of New Technologies,* Harvard University Press, Cambridge, 2018

HAYASHI, Mika, "Objective Territorial Principle or Effects Doctrine? Jurisdiction and Cyberspace", *In Law*, n.º 6, 2006, p. 284 e ss.

HEIL, Helmut, "Directive 95/46/EC of the European Parliament and of the Council: Introductory remarks", Alfred BULLESBACH, Yves POULLET, Corien PRINS e Serge GIJRATH, *Consice European IT Law,* 2ª ed., Kluwer Law International, Haia, 2010

HELBERGER, Natali, BORGESIUS, Frederik, REYNA, Agustin, "The Perfect Match? A Closer Look at the Relationship between EU Consumer Law and Data Protection Law", *CMLR,* vol. 54, n.º 5, 2017, p. 1427 e ss.

HELD, David, "Law of States, Law of Peoples: Three Models of Sovereignty", *Legal Theory,* vol. 8, n.º 2, 2002, p. 1 e ss..

HENZELIN, Michael*, Le Principe de l'Universalité em droit penal international: droit et obligation pour les États de poursuivre et juger selon le principe de l'universalité,* Helbing & Lichtenhahn*,* Basileia, 2001

HEIJER, Maarten LAWSON, Rick, "Extraterritorial Human Rights and the Concept of 'Jurisdiction', Malcolm LANGFORD, Wouter VANDENHOLE, Martin SCHEININ e Willem van GENUGTEN, (eds.), *Global Justice, State Duties – The Extraterritorial Scope of Economic, Social and Cultural Rights in International Law,* Cambridge University Press, Oxford, 2013, p. 153 e ss.

HERT, Paul de e PAPAKONSTANTINOU, Vagelis, "Google Spain: Addressing Critiques and Misunderstandings One Year Later", *MJ,* vol. 22, n.º 4, 2015, p. 324 e ss.

- "Three scenarios for international governance of data privacy: towards an international data privacy organization, preferably a UN agency?", *I/S: A Journal of Law and Policy for the Information Society,* vol. 9, 2013, p. 271 e ss.

- "The proposed Data Protection Regulation Replacing Directive 95/46/EC: A Sound System for the Protection of Individuals", *CLSR,* n.º 28, 2012, p. 130 e ss.

HERT, Paul de, "The Right to Protection of Personal Data. Incapable of Autonomous Standing in the Basic EU Constituting Documents'", *UJIEL*, n.º 31, 2015, p. 1 e ss.

HERT, Paul de e GUTWIRTH, Serge, "Data Protection in the Case Law of Strasbourg and Luxemburg: Constitutionalisation in Action", Serge GUTWIRTH*,* Yves POULLET, Paul de HERT e Cécile de TERWANGNE, (eds.), *Reinventing Data Protection?* Springer, Dordrecht, 2009, p. 3 e ss.

HERT, Paul de e CZERNIAWSKI, Michael, "Expanding the European data protection scope beyond territory: Article 3 of the General Data Protection Regulation in its wider context", *IDPL,* vol. 6, n.º 3, 2016, p. 230 e ss.

HEUMANN, Stepahn, "German Exceptionalism? The Debate About the German Foreign Intelligence Service (BND)", Russell MILLER (ed.), *Privacy and Power. A Transatlantic Dialogue in the Shadow of the NSA-Affair,* Cambridge University Press, Cambridge, 2017, p. 349 e ss.

HIGGINS, Rosalyn, "The Legal Basis of Jurisdiction", Cecil OLMSTEAD (ed.), *Extra-Territorial Application of Laws and Responses Thereto,* ESC Publishing, Oxford, 1984, p. 3 e ss.

HIIESINGER, Stefanie e MAVROIDI, Petros, "Planes, Trains, and Automobiles: The EU Legislation on Climate Change and the Question of Consistency with WTO Law", EUI

Working Papers, AEL 2013/04, disponível online em http://cadmus.eui.eu/bitstream/handle/1814/27457/AEL_2013_04.pdf?sequence=3&isAllowed=y

HIJMANS, Hielke, *The European Union as a Constitutional guardian of internet privacy and data protection. The Story of Art. 16.º TFUE,* Springer, Dordrecht, 2017

HON, Kuan, *Data Localization Laws and Policy. The EU Data Protection International Transfers Restriction Through a Cloud Computing Lens*, Edward Elgar Publishing, Cheltenham/Northampton, 2017

- "GDPR's extra-territoriality means trouble for cloud computing", *Privacy Law & Business,* Abril 2016, p. 26 e ss.

HON, Kuan, HORNLE, Julia e MILLARD, Christopher, "Data Protection Jurisdiction and Cloud Computing – When are Cloud Users and Providers Subject to EU Data Protection Law? The Cloud of Unknowing, Part 3", *IRLCT*, vol. 26, n.º 3, 2012, p. 129 e ss.

HON, Kuan e MILLARD, Christopher, "Data Export in Cloud Computing – How Can Personal Data Be Transferred Outside the EU? The Cloud of Unknowing, Part 4", *SCRPIT-ed,* vol. 9, n.º 25, 2011, p. 25 e ss.

HONDIUS, Frits, *Emerging Data Protection in Europe,* North-Holand, Amesterdão, 1975

HOOD, Christopher, ROTHSTEIN, Henry e BALDWIN, Robert, *The Governance of Risk: Understanding Risk Regulation Regimes,* Oxford University Press, Oxford, 2004

JALLES, Isabel, *Extraterritorialidade e Comércio Internacional. Um Exercício de Direito Americano,* Universidade Católica, Lisboa, 1986

JENNINGS, Robert e WATTS, Arthur, *Oppenheim's International Law,* 9ª edição, vol. I, Peace, Oxford University Press, Oxford, 1992

- "Extraterritorial Jurisdiction and the United States Antitrust Laws", *BYIL*, n.º 33, 1957, p. 146 e ss.

JANSEN, Bernhard, "The Limits of Unilateralism from a European Perspective", *EJIL,* vol. 11, n.º 2, 2000, p. 309 e ss.

JAY, Rosemary e HAMILTON, Angus, *Data Protection law and Practice,* 2ª ed., Sweet and Maxwell, Londres, 2003

JESSUP, Phillip, *Transnational Law,* Yale University Press, New Heaven, 1956

JONES, Richard, "Extra territoriality and international transfers under the draft Regulation", *PDP,* vol. 12, n.º 2, 2013, p. 6 e ss.

KAHLER, Miles e LAKE, David, "Economic integration and Global Governance: Why so Little Supranationalism?", Walter MATTLI e Ngarie WOODS (eds.), *Politics of Global Regulation,* Princeton University Press, New Jersey, 2009

KAMARA, Irene, "Co-regulation in EU personal data protection: the case of technical standards and the privacy by design standardisation 'mandate'", *EJLT,* vol. 8, n.º 1, 2017

KAMARINOU, Dimitra, "International transfers of personal data and corporate compliance under Directive 95/46/EC, the draft Regulation and the international community: part 1", *CL*, n.º 18, vol. 2, 2013, p. 49 e ss.

KAMMINGA, Menno, "Extraterritoriality", *The Max Planck Encyclopedia of Public International Law,* Vol. III, Rudiger WOLFRUM (dir.), Oxford University Press, Oxford, 2012, p. 1070 e ss.

KAYE, David, "Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression", 22 de maio de 2015, disponível em https://www.ohchr.org/EN/Issues/FreedomOpinion/Pages/OpinionIndex.aspx

KELSEN, Hans, *Teoria Pura do Direito,* vol. I, 2ª ed., tradução de João Baptista Machado, Arménio Amado Editor, Coimbra, 1962

- *General Theory of Law and State,* Edição Kindle, The Law Book Exchange Ltd., Nova Jérsia,1945

KELEMEN, Daniel, "Globalizing European Union Environmental policy, *JEPP*, vol. 17, n.º 3, 2010, p. 342 e ss.

KENT, Gail, "Sharing Investigation Specific Data with law Enforcement – An International Approach", *Stanford Public Law Working Paper,* 14 de fevereiro de 2014, disponível em https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2472413

KESSLER, David, NOVAK, Jamie e KHAN, Sumera, "The potential impact of article 48 of the General Data Protection Regulation on Cross Border Discovery From the United States", *TSCJ,* vol. 17, n.º 2, 2016, p. 576 e ss.

KINDT, Els, "Why research may no longer be the same: about the territorial scope of the new data protection regulation", *CMLR,* n.º 32, 2016, p. 738 e ss.

KING, Kevin, "Personal Jurisdiction, Internet Commerce, and Privacy: The Pervasive Legal Consequences of Modern Geolocation Technologies", *AJST,* n.º 21, 2011, p. 61 e ss.

KISS, Atilla e SZOKE, Gergely, "Evolution or revolution? Steps forward to a new generation of data protection regulation", Serge GUTWIRTH, Ronald LEENES e Paul DE HERT (eds.), *Reforming the European Data Protection Law,* Springer, Dordrecht, 2015, p. 313 e ss.

KNOX, John, "The Unpredictable Presumption Against Extraterritoriality", *SLR,* vol. 40, 2011, p. 635 e ss..

KOBRIN, Stephen, "The Trans-Atlantic Data Privacy Dispute, Territorial Jurisdiction and Global Governance", Working Paper Series, The Wharton School, novembro de 2003, disponível em https://papers.ssrn.com/sol3/papers.cfm?abstract_id=349561

KOENING, Carsten, "An Economic Analysis of the single economic entity doctrine in EU competition law", *JCLE,* vol. 13, n.º 2, junho de 2017, p. 281 e ss..

KOHL, Utah, "Jurisdiction in Cyberspace", Nicholas TSAGOURIAS e Russell BUCHAN, (eds.), *Research Handbook on International Law and Cyberspace,* Edward Elgar Publishing, Cheltenham/Northampton, 2015, p. 50 e ss.

- *Jurisdiction and the Internet – Regulatory Competence of Online Activity,* Cambridge University Press, Oxford, 2007

- "Eggs, Jurisdiction, and the Internet", *ICLQ*, vol. 51, n.º 3, 2002, p. 579 e ss.

KOKOTT, Juliane e SOBOTTA, Christoph, "The Distinction between Privacy and Data Protection in the Jurisprudence of the CJEU and the ECtHR", *IDPL,* nº 3, 2013, p. 222 e ss.

KOHLER, Christian, "Conflict of law issues in the 2016 Data Protection Regulation of the European Union", *RDIPP,* vol. 52, n.º 3, 2016, p. 653 e ss.

KONARSKI, Xawery, KARWALA, Damian, SCHULTE-NOKE, Hans e CHARLTON, Shaun, "Reforming the Data Protection Package: Study for the European Parliament's Committee on Internal Market and Consumer Protection", 2012, disponível em http://www.europarl.europa.eu/document/activities/cont/201209/20120928ATT52488/20120928ATT52488EN.pdf

KONG, Lingjie, "Data Protection and Transborder Data Flow in the European and Global Context", *TEJIL,* vol. 21, n.º 2, 2010, p. 441 e ss.

KORFF, Douwe, "Data protection laws in the EU: the difficulties in meeting the challenges posed by global social and technical developments", 2010, disponível em https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1638949

- "Comparative study on different approaches to new privacy challenges in particular in the light of technological developments: Working paper n.º 2 – Data Protection Laws in the EU: the difficulties in meeting the challenges posed by global social and technical developments", Comissão Europeia, 2010

- "Existing case-law on compliance with data protection laws and principles in the member states of European Union: annex to the annual report 1998 (XV D-5047-98) of the working party established by article 29 of Directive 95-46-EC", Office for Official Publications of the European Communities, 1998, disponível em https://searchworks.stanford.edu/view/4025981

- "EC Study on Implementation of Data Protection Directive. Comparative Summary of national laws", setembro de 2002, disponível em

http://194.242.234.211/documents/10160/10704/Stato+di+attuazione+della+Direttiva+95-46-CE

KRASNER, Stephen, "Abiding Sovereignty", *IPSR,* vol. 22, n.º 3, 2001, p. 231 e ss.

KRISCH, Nico, "Pluralism in International Law and Beyond", Jean D'ASPREMONT e Sahib SINGH (eds.), *Fundamental Concepts for International Law: The Construction of a Discipline,* Edward Elgar Publishing, Cheltenham/Northampton, 2016

- "The Decay of Consent: International Law in an Age of Public Goods", *AJIL,* n.º 108, 2014, p. 7 e ss.

- "The pluralism of global administrative law", *EJIL,* n.º 17, 2006, p. 269 e ss.

- *Beyond Constitutionalism. The Pluralist Structure of Postnational Law,* Oxford University Press, Oxford, 2011

KRONKE, Herbert, "Capital markets and Conflict of Laws", *RCADI,* vol. 286, 2000, p. 245 e ss.

KUCZERAWY, Aleksandra, "Facebook and Its EU Users – Applicability of the EU Data Protection Law to US Based SNS in Advances", *Information and Communication Technology,* n.º 320, 2010, p. 75 e ss.

KULESZA, Joanna, "Transboundary data protection and international business compliance", *IDPL,* vol. 4, n.º 4, 2014, p. 298 e ss.

KUNER, Christopher, "Court of Justice International agreements, data protection, and fundamental rights on the international stage: Opinion 1/15, *EU-Canada PNR*", *CMLR*, vol. 55, n.º 3, 2018, p. 857 e ss..

- "The Internet and the global reach of EU law", LSE Law Working Paper Series 04/2017, University of Cambridge Faculty of Law, Research Paper No. 24/2017

- "The Court of Justice of the EU Judgment on Data Protection and Internet Search Engines", Burkhard HESS e Cristina MARIOTTINI, (eds.), *Protecting Privacy in International and Procedural Law and By Data Protection (European and American Developments),* Nomos, Baden-Baden, 2015, p. 19 e ss.

- "Risk Management in Data Protection", *IDPL,* n.º 5, 2015, p. 95 e ss.

- "Data Nationalism and its Discontents", *EmLR,* 2015, n.º 64, p. 2089 e ss.

- "The European Union and the Search for an International Data Protection Framework", *GJIL,* vol. 2, n.º 2, 2014, p. 55 e ss.

- "Foreign Nationals and Privacy protection: A Comparative Transatlantic Analysis", Hielke HIJMANS e Herke KRANENBORG (eds.), *Data Protection 2014: How to Restore Trust,* Intersentia, Cambridge, 2014, p. 213 e ss.

- *Transborder Data Flows and Data Privacy Law,* Oxford University Press, Oxford, 2013

- "The European Commission's Proposed Data Protection Regulation: A Copernican Revolution in European Data Protection Law", *Bloomberg BNA Privacy and Security Law Report,* 6 de fevereiro de 2012

- "Data Protection Law and International Jurisdiction on the Internet (Part 1)", *IJLIT,* vol. 18, n.º 2, 2010, p. 176 e ss.

- "Data Protection Law and International Jurisdiction on the Internet (Part 2)", *IJLIT,* vol. 18, n.º 3, p. 227 e ss.

- *European Data Protection Law. Corporate Compliance and Regulation,* Oxford University Press, Oxford, 2007

- *European Data Privacy Law & Online Business*, Oxford University Press, Oxford, 2003

KUNER, Christopher, CATE, Fred, MILLARD, Christopher, SVANTESSON, Dan "The (Data Privacy) Law hasn't Even Checked in when technology takes off", *IDPL,* n.º 4, 2014, p. 175 e ss.

KUNER, Christopher, CATE, Fred, MILLARD, Christopher, SVANTESSON, Dan e LYNSKEY, Orla, "The Data Protection Credibility Crisis", *IDPL,* vol. 5, n.º 3, 2015, p. 161 e ss.

LACHAUD, Eric, "The General Data Protection Regulation and the rise of certification as a regulatory instrument", *CLSR,* vol. 34, n.º 2, 2018, p. 244 e ss.

LA RUE, Frank, "Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Expression", 17 de abril de 2013, disponível em https://www.ohchr.org/EN/Issues/FreedomOpinion/Pages/Annual.aspx

LAUTERPACHT, Hersch, "The International Protection of Human Rights", *RCADI,* vol. 70, 1947-I, p. 24 e ss.

LAYTON, Alexander e PARRY, Angharad, "Extraterritorial Jurisdiction – European Responses", *HJIL,* vol. 26, n.º 2, 2004, p. 309 e ss.

LENAERTS, Koen e DESOMER, Marlies, "New Models Of Constitution-Making in Europe: The Quest For Legitimicay", *CMLR*, vol. 29, 2002, p. 1223 e ss..

LE SIEUR, François, "Regulating cross-border data flows and privacy in the networked digital environment and global knowledge economy", *IDPL*, vol. 2, n.º 2, 2012, p. 93 e ss.

LINDSAY, David, "The Role of Proportionality in Assessing Trans-Atlantic Personal Data Flows", Dan SVANTESSON e Dariusz KLOZA (eds.), *Trans-Atlantic Data Privacy Relations As a Challenge for Democracy,* Intersentia, Cambridge, 2017, p. 49 e ss.

LOPES, Dulce, "A jurisdição extraterritorial dos Estados: entre tradição e modernidade", *Estudos em Homenagem ao Conselheiro Presidente Rui Moura Ramos*, vol. 1, 2016, p. 1071 e ss.

- *Eficácia, Reconhecimento e Execução de Atos Administrativos Estrangeiros*, Policopiado, 2015

LOPES, José Azeredo, *Entre Solidão e Intervencionismo. Direito de Autodeterminação dos povos e reações de estados terceiros*, Universidade Católica, Porto, 2003

LOUREIRO, João, "Da sociedade técnica de massas à sociedade de risco – Prevenção, precaução e tecnociência: algumas questões juspublicísticas", *Estudos em Homenagem ao Prof. Doutor Rogério Soares,* Coimbra Editora, Coimbra, 2001*,* p. 797 e ss.

LOWE, Vaughan, "Jurisdiction", Malcolm EVANS (ed.) *International Law,* 2ª ed., Oxford University Press, Oxford, 2006, p. 335 e ss..

- "Ends and Means in the Settlement of International Disputes over Jurisdiction", *RIS*, vol. 11, n.º 3, Julho, 1985, p. 183 e ss.

LUGARESI, Nicola, "Internet Law Trends in Europe: A Case Law Perspective", *Revista da Faculdade de Direito da UFMG*, n.º especial – 2nd Conference Brazil-Italy, 2017, p. 305 e ss.

LYNSKEY, Orla, *The Foundations of EU Data Protection Law,* Oxford University Press, Oxford, 2015

MACHADO, João Baptista, *Âmbito de Eficácia e Âmbito de Competência das Leis*, Almedina, Coimbra, 1998

MACHADO, Jónatas, *Direito Internacional: do paradigma clássico ao pós-11 de setembro,* 4ª edição, Coimbra Editora, Coimbra, 2013

MAGALHÃES, José, "A aplicação extraterritorial de leis nacionais", *RFDUSP,* vol. 80, 1985, p. 171 e ss.

MAIER, Bernhard, "How Has the Law Attempted to Tackle the Borderless Nature of the Internet?", *IJLIT*, vol. 18, n.º 2, 2010, p. 142 e ss.

MAIER, Harold, "Jurisdictional Rules in Customary International Law", Karl MEESSEN, (ed.) *Extraterritorial Jurisdiction in Theory and Practice*, Kluwer Law, 1996, p. 64 e ss.

- "Interest Balancing and Extraterritorial Jurisdiction", *AJCL,* vol. 31, n.º 4, Autumn, 1983, p. 581 e ss.

- "Extraterritorial Jurisdiction at a Crossroads: An Intersection between Public and Private International Law", *AJIL,* vol. 76, n.º 2, 1982, p. 280 e ss.

MAJONE, Giandomenico, "Mutual Recognition in Federal Type Systems", Anne MULLINS e Cheryl SAUNDERS (eds.), *Economic Union in Federal Systems,* Sidney, The Federation Press, 1994, p. 69 e ss..

MAKULILO, Alex, "Privacy and Data protection in Africa: a state of the art", *IDPL,* vol. 2, n.º 3, 2012, p. 163 e ss.

MALDOFF, Gabe e TENE, Omer, "'Essential Equivalence' and European Adequacy after Schrems: The Canadian Example", *WILJ,* n.º 34, 2016, p. 211 e ss..

MALONE, David e KHONG, Yuen, "Unilateralism and US Foreign Policy: International Perspective", David MALONE, Yuen KHONG (eds.), *Unilateralism and US Foreign Policy: International Perspective,* Lynne Rienner, Boulder, 2003, p. 3 e ss.

MAÑAS, José Piñar, "Introducción. Hacia un nuevo modelo europeo de protección de datos", José Piñar MAÑAS (dir.), *Reglamento General De Protección De Datos. Hacia um nuevo modelo europeo de privacidade,* Reus, Madrid, 2016, p. 15 e ss.

- "Transferencias de datos personales a terceros países u organizaciones internacionales", José Piñar MAÑAS, *Reglamento General de Protección de Datos. Hacia un nuevo modelo europeo de privacidade,* Reus, 2016, p. 427 e ss.

MANN, Frederick, "The doctrine of jurisdiction in international law", *ADIRC,* n.º 111, I, 1964, p. 9 e ss., reimpresso em *Studies in International Law,* Oxford, Clarendon Press Oxford, 2008, p. 11 e ss.

- "The doctrine of international jurisdiction revisited after twenty years", *ADIRC,* n.º 186, III, 1984, p. 13 e ss..

- "Anglo-American Conflict of International Jurisdiction", *ICLQ*, vol. 13, n.º 4, outubro de 1964, p. 1463

MANN, Michael e BARRY, William, "Developments in the Internationalization of Securities Enforcement", *Corporate Law and Practice Handbook Series,* PLI Order Number 3011, May 2004, p. 355 e 365 e ss.

MAYER-SCHONBERGER, Viktor, "Generational Development of Data Protection in Europe", Philip AGRE e Marc ROTENBERG (eds.), *Technology and Privacy: The New Landscape,* MIT Press, Cambridge, 1998, p. 225 e ss.

MARQUES, João, "Direito ao Esquecimento. A Aplicação Do Acórdão Google Pela CNPD", *FDPD*, 2016, p. 48 e ss.

- "And [they] built a crooked h[arbour] – the Schrems ruling and what it means for the future of data transfers between the EU and US", *EU Law Journal,* vol. 2, n.º 2, junho de 2016, p. 54 e ss.

MARQUES DOS SANTOS, António*, Algumas reflexões sobre a nacionalidade das sociedades em direito internacional privado e em direito internacional público,* Coimbra Editora, Coimbra, 1985

- *As normas de aplicação imediata no Direito Internacional Privado – Esboço de uma teoria geral,* vol. I e II, Almedina, Coimbra, 1991

MARTINS, Ana Maria, "Algumas Notas sobre o Espaço de Liberdade, Segurança e Justiça no Tratado de Lisboa", *Cadernos O Direito,* n.º 5, 2010, p. 13 e ss.

MATHIEU, Bertrand, "L'avenir du principe de précaution?", *JCP,* n.º 45, 2001, p. 2025 e ss..

MATWYSHYN, Andrea, "Of Nodes and Power Laws: A Network Theory Approach to Internet Jurisdiction Through Data Privacy", *NWULR,* n.º 98, 2003-2004, p. 540.

MCCLENNA, Jennifer e SCHICK, Vadim, "'O, Privacy'. Canada's Importance in the Development of the International Data Privacy Regime", *GJIL,* vol. 38, 2007, p. 669 e ss.

MCLACHLAN, Campbell, "The Influence of International Law on Civil Jurisdiction", *HYIL,* vol. 6, 1993, p. 125 e ss.

MEAL, Douglas, "Governmental compulsion as a defence under United States and European Community Antitrust Law", *CJTL,* n.º 20, 1981, p. 51 e ss.

MEESSEN, Karl, "Conflicts of Jurisdiction under the new Restatement", *LCLP,* vol. 50, n.º 3, 1987, p. 47 e ss.

MENON, Anand e WEATHERHILL, Stephen, "Transnational Legitimacy in a Globalising World: How the European Union Rescues its States", *WEP*, vol. 31, n.º 3, 2008, p. 397 e ss.

MESQUITA, Maria Rangel, *A Actuação Externa da União Europeia depois do Tratado de Lisboa,* Almedina, Coimbra, 2011

MESTRAL, Armand, "The Extraterritorial Extension of Laws: How Much as Changed?", *AJICL,* vol. 31, n.º 1, 2014, p. 46 e ss..

MEYER, Jeffrey, "Dual Illegality and Geoambiguous Law: A New Rule for Extraterritorial Application of U.S. Law", *MLR,* vol. 95, 2010, p. 114 e ss..

MEXÍA, Pablo, "La singular naturaleza jurídica del reglamento general de protección de datos de la UE. Sus efectos en acervo nacional sobre protección de datos", José Piñar MAÑAS (dir.), *Reglamento General De Protección De Datos. Hacia um nuevo modelo europeo de privacidade,* Reus, Madrid, 2016

MICHAELS, Ralf e PAUWELYN, Joost, "Conflict of Norms or Conflict of Laws? Different Techniques in the Fragmentation of International Law", *Duke Scholarship Repository,* 4/2012, disponível em https://scholarship.law.duke.edu/djcil/vol22/iss3/3/

MIGLIO, Alberto, "Back to Yahoo!? Regulatory clashes in cyberspace in the light of EU data protection law", Gert VERMEULEN & Eva LIEVENS (eds.), *Data Protection and*

Privacy under Pressure. Transatlantic tensions, EU surveillance and big data, Maklu, Antuérpia/Apeldoorn/Portland, 2017*,* p. 101 e ss..

MILANOVIC, Marko, *Extraterritorial Application of Human Rights Treaties,* Oxford University Press, Oxford, 2013

MILLS, Alex, "Rethinking Jurisdiction in International Law", *BYIL,* vol. 84, n.º 1, 2014, p. 187 e ss..

MOEREL, Lokke, "Export of the rule of law. Corporate Self-regulation of Global Data Transfers", *Think Piece for the Hague Institute for International Law Global Conference*, 2012, p. 329 e ss.

- *Binding Corporate Rules: Corporate Self-Regulation of Global Data Transfers,* Oxford University Press, Oxford, 2012

MONCADA, Luís Cabral, *Ensaio sobre a lei,* Coimbra Editora, Coimbra, 2002

MONIZ, Graça Canto, "Direitos do titular dos dados pessoais: o direito à portabilidade", Francisco PEREIRA COUTINHO e Graça CANTO MONIZ, *Anuário da proteção de dados,* CEDIS, 2018, p. 11 e ss.

- "Compreender o ativismo judicial do Tribunal de Justiça da União Europeia. A "Explicação" de Ronald Dworkin", *Themis,* ano XVIII, n.º 32, 2017, p. 125 e ss..

MONTERO, Javier, *Algunas consideraciones sobre Cloud Computing,* AEPD, Madrid, 2013

MOREIRA, Adriano, "Território, Fronteira e Soberania no Mundo Atual", *Estudos em Homenagem ao Prof. Doutor Martim de Albuquerque*, vol. I, Coimbra Editora, Coimbra, 2010, p. 29 e ss.

MORAIS, Carlos, "As Autoridades Administrativas independentes na Ordem Jurídica Portuguesa", *ROA,* ano 61, n.º 1, 2001, p. 103 e ss.

MOREIRA, Teresa, *A Privacidade dos Trabalhadores e as Novas Tecnologias de Informação e Comunicação: contributo para um estudo dos limites do poder de controlo eletrónico do empregador,* Almedina, Coimbra, 2010

MOREIRA, Vital, *Auto-Regulação Profissional e Administração Pública,* Almedina, Coimbra, 1997

MOREIRA Vital e MAÇAS, Fernanda, *Autoridades Reguladoras Independentes – Estudo e Projecto de Lei-Quadro,* Coimbra Editora, Coimbra, 2003

MORIJN, John, "Balancing Fundamental Rights and common market freedoms in Union Law: Schmidberger and Omega in the light of the European Constitution", *ELJ,* vol. 12, n.º 1, 2006, p. 15 e ss.

MORIMOTO, Tetsuya, "Growing industrialization and our damaged planet: The extraterritorial application of developed countries' domestic environmental laws to transnational corporations abroad", *ULR,* n.º 1, 2005, p. 134 e ss.

MORENO-LAX, Violeta e COSTELO, Cathryn, "The extraterritorial application of the EU Charter of Fundamental Rights: from territoriality to facticity, the effectiveness model", Steve PEERS, Jeff KENNER, Angela WARD e Tamara HERVEY, *The EU Charter of Fundamental Rights: A Commentary,* Hart Publishing, Oxford/Portland, 2014, p. 1657 e ss.

NAVARRO, Susana, *La personalidade virtual del usuário de Internet,* Tirant lo Blanch, Valencia, 2015

NEWMAN, Abraham, *Protectors of Privacy. Regulating Personal Data in the Global Economy,* Cornell University Press, Ithaca, 2008

- "Building Transnational Civil Liberties: Transgovernmental Entrepreneurs and the European Data Privacy Directive", *IO,* vol. 62, n.º 1, 2008, p. 103 e ss.

NEWMAN, Abraham e POSNER, Elliot, "Putting the EU in its place: policy strategies and the global regulatory context", *JEPP*, vol. 22, n.º 9, 2015, p. 1316 e ss..

- "International interdependence and regulatory power: Authority, mobility and markets", *EJIR,* vol. 17, n.º 4, 2011, p. 589 e ss.

NICOLAIDIS, Kalypso e SHAFFER, Gregory, "Transnational Mutual Recognition Regimes: Governance Without Global Government", *LCP,* vol. 68, 2005, p. 263 e ss.

ODUDU, Okeoghene e BAILEY, David, "The single economic entity doctrine in EU competition law", *CMLR,* n.º 51, 2014, p. 1721 e ss.

OJANEN, Tuomas, "Privacy is More than Just a Seven-Letter Word: The Court of Justice of the European Union Sets Constitutional Limits on Mass Surveillance", *ECLR,* n.º 10, 2014, p. 528 e ss.

O'KEEFE, Roger,"Universal Jurisdiction. Clarifying the basic concept", *JICJ*, n.º 2, 2004, p. 736 e ss.

OMMESLAGHE, Pierre, "Le Droit Public Existe-t-il?", *Revue de la faculte de droit et de criminologie de l'ULB,* n.º 33, 2006, p. 15 e ss.

OSULA, Anna-Maria, "Mutual Legal Assistance & Other Mechanisms for Accessing Extraterritorially Located Data", *MUJLT,* n.º 9, 2015, p. 43 e ss.

OTERO, Paulo, *Legalidade e Administração Pública – O sentido da vinculação administrativa à juridicidade,* Almedina, Coimbra, 2003

OXMAN, Bernard, "Jurisdiction of States", *The Max Planck Encyclopedia of Public International Law,* vol. IV, Rudiger Wolfrum (dir.), Oxford University Press, Oxford, 2012, p. 546 e ss.

PARRISH, Austen, "Kiobel, Unilateralism, and the Retreat from Extraterritoriality, *MJOL*, vol. 28, 2013, p. 208 e ss..

- "Reclaiming International Law From Extraterritoriality", *MiLR*, vol. 93, 2009, p. 865 e ss.

- "The Effects Test: Extraterritoriality's Fifith Business", *VLR,* vol. 61, n.º 5, 2008, p. 1455 e ss.

PARK, Whon-il, "South Korea's GDPR preparation: Hurdles ahead", *PLBIR,* n.º 149, outubro de 2017, p. 23 e ss.

PEREIRA, Alexandre, *Direitos de Autor e Liberdade de Informação*, Almedina, Coimbra, 2008

PEREIRA, Maria de Assunção Vale, *A Intervenção Humanitária no Direito Internacional Contemporâneo*, Coimbra Editora, Coimbra, 2009

PELKMANS, Jacques, "Mutual Recognition in Goods and Services: An Economic Perspective", Fiorella SCHIOPP, (ed.), *The Principle of Mutual Recognition in the European Integration Process,* Palgrave Macmillan, Basingstoke, 2005, p. 85 e ss.

PETERS, Anne, "Privacy, *Rechtsstaatlichkeit,* and legal limits on extraterritorial surveillance", Russell MILLER (ed.), *Privacy and Power. A Transatlantic Dialogue in the Shadow of the NSA-Affair,* Cambridge University Press, Cambridge, 2017, p. 145 e ss.

PETKOVA, Bilyana, "Domesticating the 'foreign' in making transatlantic data privacy law", *IJCL,* vol. 15, n.º 4, 2017, p. 1135 e ss.

- "Towards na Internal Hierarchy of Values in the EU Legal Order: Balancing the Freedom of Speech and Data Privacy", *MJECL,* vol. 23, n.º 3, 2016, p. 421 e ss.

PICONE, Paolo, "Introduzione – Parte IX Tutela della Concorrenza", Paulo PICONE, Giordio SACERDOTI e Manlio FRIGO (eds.), *Diritto internazionale dell'economia: raccolta sistemática dei principal atti normativi internazionali ed interni com testi introduttivi e note*, Franco Angeli, Milão,1982, p. 865 e ss..

PINHEIRO, Alexandre Sousa, *Privacy e proteção de dados pessoais: a construção dogmática do direito à identidade informacional,* policopiado, 2015

PINHEIRO, Luís Lima, "The 'Denationalization' of Transnational Relationships: Regulation of Transnational Relationships by Public International Law, European Community Law, and Transnational Law", *Estudos de Direito Internacional Privado – Direito de Conflitos, Competência Internacional e Reconhecimento de Decisões Estrangeiras,* Almedina, Coimbra, 2006, p. 189 e ss.

- *Direito Internacional Privado*, vol. I, Almedina, Coimbra, 2003

- *Direito Internacional Privado,* vol. II, Almedina, Coimbra, 2003

PIRES, Francisco Lucas, *Introdução à Ciência Política,* Universidade Católica Portuguesa, Porto, 1998

POLLICINO, Oreste e BASSINI, Marco, "The law of the Internet between Globalisation and localization", Miguel POAIRES MADURO, Kaarlo TUORI e Suvi SANKARI, (eds.), *Transnational Law. Rethinking European Law and Legal Thinking*, Cambridge University Press, Cambridge, 2014, p. 346 e ss.

POLCÁK, Radim e SVANTESSON, Dan, *Information Sovereignty. Data Privacy, Sovereign Powers and the Rule of Law,* Cheltenham, Edward Elgar, Cheltenham/Northampton, 2017

POULLET, Yves, "Vers la confiance: vues de Bruxelles: um droit européen de l'Internet? Quelques considérations sur la spécificité de l'approche réglementaire européene du cyberspace", Georges CHATILLON, (org.), *Le droit international de l'Internet,* Bruylant, Bruxelas, 2002

POULLET, Yves, LOUVEAUX, Sophie e ASINARI, Maria, "Data Protection and Privacy in Global Networks: a European Approach", *EDILR,* vol. 8, n.º 2 e 3, 2001, p. 147 e ss.

PORCEDDA, Maria, "Use of the Charter of Fundamental Rights by national data protection authorities and the EDPS", *RSCAS Research. Project Reports, Center for Judicial Cooperation,* Junho de 2017

POWLES, JULIA e LARSEN, REBEKAH, "Academic Commnetary: Google Spain", *Cambridge Code*, disponível em http://www.cambridge-code.org/googlespain.html

PURTOVA, Nadezhda, *Property Rights in Personal Data: A European Perspective,* Kluwer Law, Haia, 2011

QUAGLIA, Lucia, "The politics of 'Third Country Equivalence' in Post-crisis Financial Services Regulation in the European Union", *WEP,* vol. 38, n.º 1, 2015, p. 167 e ss..

QUEIROZ, Cristina, *Direito Constitucional Internacional,* Coimbra Editora, Coimbra, 2011

RAMOS, Rui Moura, *Da Lei Aplicável ao Contrato de Trabalho Internacional,* Coimbra, Almedina, 1991

RAMSEY, Michael, "Escaping 'International comity'", *ILR,* n.º 83, 1998, p. 893 e ss.

READING, Viviane, "The EU data protection Regulation: Promoting technological innovation and safeguarding citizen's rights – Intervention at the Justice Council", 4 de março de 2014, disponível em http://europa.eu/rapid/press-release_SPEECH-14-175_en.htm

- "The European data protection Framework for the twenty-first century", *IDPL,* n.º 2, 2012, p. 119 e ss.

REED, Chris, *Making Laws for Cyberspace,* Oxford University Press, Oxford, 2012

- "The law of unintended consequences: embedded business models IT regulation", *JILT*, n.º 2, 2007, p. 1 e ss.

REESE, Willis, "Legislative Jurisdiction", *CLAR,* n.º 78, n.º 8, December, 1978, p. 1587 e ss.

REIDENBERG, Joel, "E-Commerce and Trans-Atlantic Privacy", *HLR,* n.º 38, 2001, p. 717 e ss.

- "Rules of the Road for Global Electronic Highways: Merging the Trade and Technical Paradigms", *HJLT,* n.º 6, 1992-1993, p. 287 e ss.

RIGAUDIAS, Cecilia, "Condiciones para las transferências internacionales de datos personales em servicioes de cloud", Ricardo MARTINEZ, *Derecho Y Cloud Computing,* Thomson Reuter, 2012, p. 109 e ss.

RIGAUX, François, "Droit économique et conflits de souverainetés", *Rabels Zeitschrift fur auslandisches und internationals Privatrecht,* Ano 52, vol.1/2, 1988, p. 112 e ss.

- "La loi applicable à la protection des individus à l'égard du traitement automatisé des données à caractere personnel", *RCDIP,* 1980, p. 443 e ss.

- "Refléxions sur les rapports entre le droit international privé et le droit des gens", *Estudios de Derecho Internacional – Homenaje a D. Antonio de Luna*, Instituto Francisco Vitoria, 1968, p. 569 e ss.

RIVERO, Álvaro, "Right to Be Forgotten in the European Court of Justice Google Spain Case: The Right Balance of Privacy Right, Procedure, and Extraterritoriality", *European Union Law Working Paper,* n.º 19, 2017, disponível em https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2916608

RICHARDS, Neil, "The Dangers of Surveillance", *HLR*, n.º 126, 2013, p. 1935 e ss.

ROBINSON, Neil, GRAUX, Hans, BOTTERMAN, Maarten e VALERI, Lorenzo, "Review of the European Data Protection Diretive", *RAND Cambridge,* 2009, disponível em https://www.rand.org/pubs/technical_reports/TR710.html

RODOTÀ, Stefano, "Data Protection as a Fundamental Right", Serge GUTWIRTH, Yves POULLET, Paul de HERT e Cécile de TERWANGNE (eds.), *Reinventing Data Protection?* Springer, Dordrecht, 2009, p. 77 e ss.

ROQUE, Miguel Prata, *A Dimensão Transnacional do Direito Administrativo,* AAFDL, Lisboa, 2014

ROSENFELD, Rachel, "The European Union Aviation Directive and U.S. Resistance: A Deadlock on Aviation Emissions Control", *GIELR,* n.º 25, 2012-2013, p. 589 e ss.

ROTENBERG, Marc, "Fair Information Practices And The Architecture of Privacy (What Larry Doesn't Get", *STLR ,* vol. 44, 2001, p. 1 e ss.

ROTHWELL, DONALD e STEPHEN, Tim, *The International Law of the Sea,* Hart Publishing, Oxford/Portland, 2016.

ROUVROY, Antoinette e POULLET, Yves, "The Right to Informational Self-Determination and the Value of Self-Development: Reassessing the Importance of Privacy for Democracy", Serge GUTWIRTH, Yves POULLET, Paul de HERT e Cécile de TERWANGNE (eds.), *Reinventing Data Protection?* Springer, Dordrecht, 2009, p. 45 e ss.

RUBINSTEIN, Ira e PETKOVA, Bilyana, "The international impact of the General Data Protection Regulation", Marc COLE & Franziska BOEHM (eds.), *Commentary on the General Data Protection Regulation,* Edward Elgar Publishing, Cheltenham/Northampton, 2018

RUBINSTEIN, Ira, NOJEIM, Gregory e LEE, Ronald, "Systematic government access to personal data: a comparative analysis", *IDPL,* vol. 4, n.º 2, 2014, p. 96 e ss.

RUGGIE, John, "Doctrinal Unilateralism and its Limits: American and Global Governance in the New Century", David FORSYTHE, Patrice MCMAHON e Andrew WEDEMAN (eds.), *American Foreign Policy in a Globalized World,* 2006, p. 8 e ss.

- "Territoriality and Beyond: Problematizing Modernity in International Relations", *IO,* vol. 47, n.º 1, 1993, p. 139 e ss.

RYNGAERT, Cedric, *Jurisdiction in International Law,* Oxford University Press, Oxford 2015

- "Conflicts of Jurisdiction over orders to produce documents located abroad: reappraising 'conflict of international jurisdiction: ordering the production of documents in violation of the law of the situs' (Ivo Onkelinx 1971-I), *Revue Belge de Droit International,* vol. 1, n.º 2, 2015, p. 423 e ss.

- *Unilateral Jurisdiction and Global Values,* eleven international publishing, Haia, 2015

- "Whither Territoriality? The European Union's Use of Territoriality to Set Norms with Universal Effects", Cedric RYNGAERT, Erik MOLENAAR e Satah NOUWEN (eds.), *What's Wrong with International Law. Liber Amicorum A.H.A. Soons,* Brill, Leiden, 2015, p. 434 e ss.

- "Core values beyond territories and borders: the internal and external dimension of EU regulation and enforcement", Ton BRINK, Michiel LUCHTMAN e Miroslava SCHOLTEN, (eds.), *Sharing sovereignty in the European legal order?* Intersentia, Cambridge/Antuérpia 2015, p. 13 e ss.

SALCEDO, Juan, *El Derecho Internacional em un Mundo em cambio*, Tecnos, Madrid, 1985

SAMPAIO, Jorge, *O Acto Administrativo Pela Estrada Fora*, AAFDL, Lisboa, 2014

SAMUELSON, Pamela, "Privacy as Intellectual Property", *SLR,* n.º 52, 2000, p. 1125 e ss.

SÁNCHEZ, Carlos e GAYO, Miguel, "Certificación em protección de datos personales", José Piñar MAÑAS (dir.), *Reglamento General De Protección De Datos. Hacia um nuevo modelo europeo de privacidade,* Reus, Madrid, 2016, p. 413 e ss.

SASSEN, Saskia, *Losing Control – Sovereignty in an Age of Globalization,* Columbia University Press, Nova Iorque, 1996

SCHARTUM, Dag, "Intelligible Data Protection Legislation: A Procedural Approach", *OLR,* vol. 4, n.º 1, 2017, p. 48 e ss.

SHAW, Malcolm, *International Law,* Cambridge University Press, Cambridge, 6ª ed., 2008

SCHEININ, Martin, "Towards evidence-based discussion on surveillance: A Rejoinder to Richard A. Epstein", *ECL,* n.º 12, 2016, p. 341 e ss.

SCHENCK, Daniel, "Jurisdiction over the foreign multinational in the EEC: lifting the veil on the economic entity theory", *UPJIL,* vol. 11, n.º 2, 1980, p. 495 e ss.

SCHERZER, Dov, "EU Regulation of Processing of Personal Data by Wholly Non-Europe-Based Websites", *EIPLR,* vol. 25, n.º 7, 2003, p. 292 e ss.

SCHUSTER, Gunnar, "Extraterritoriality of Securities Law: An Economic Analysis of Jurisdiction Conflicts", *LPIB*, n.º 26, 1994, p. 165 e ss.

SCHWARTZ, Paul e SOLOVE, Daniel, *Information Privacy Law,* 3ª edição, Wolters Kluwer, Nova Iorque, 2009

SCHWARTZ, Paul, "The EU-U.S. Privacy Collision: A Turn to Institutions and Procedures", *HLR*, n.º 126, 2013, p. 1966 e ss.

- "Managing global data privacy: cross-border information flows in a networked environment", *The Privacy Projects*, 2009, disponível em http://theprivacyprojects.org/wp-content/uploads/2009/08/The-Privacy-Projects-Paul-Schwartz-Global-Data-Flows-20093.pdf

SCHUMAN, Jacob, "Extraterritoriality and International norm internalization", *HLR,* vol. 124, 2011, p. 1280 e ss.

SCHWEIGHOFER, Erich, "Principles for US-EU Data Flow Attangements", Dan SVANTESSON e Dariusz KLOZA (eds.), *Trans-atlantic data privacy as a challenge for democracy,* Intersentia, Cambridge/Antuérpia, 2017, p. 27 e ss.

SCHULTZ, Thomas, "Carving up the Internet: Jurisdiction, Legal Orders, and the Private/Public International Law Interface", *TEJIL,* vol. 19, n.º 4, 2008, p. 799 e ss.

SCHULHOFER, Stephen, "A Transatlantic Privacy Pact?: A Sceptical View", David COLE, Frederico FABBRINI e Stephen SCHULHOFER (eds.), *Surveillance, Privacy and Trans-Atlantic Relations,* Hart Publishing, Oxford/Portland, 2017, p. 173 e ss.

SCHUTZ, Philip, "The Set Up of Data Protection Authorities as a New Regulatory Approach", Serge GUTWIRTH, Paul DE HERT e Ronald LEENES (eds.), *European Data Protection: In Good Health?* Springer, Dordrecht, p. 125 e ss.

SCOTT, Joanne, "Extraterritoriality and Territorial Extension of EU Law", *AJCL*, vol. 62, n.º 1, 2014, p. 87 e ss.

- "The New EU 'Extraterritoriality'", *CMLR,* vol. 51, 2014, p. 1343 e ss.

- "Contingent Unilateralism: International Aviation in the European Emissions Trading Scheme", Bart VAN VOOREN, Steve BLOCKMANS e Jan WOUTERS (eds.), *The EU Role in Global Governance: The Legal Dimension,* Oxford, Oxford University Press, 2013

- "Territorial Sovereignty and Territorial Extension in an Inter-Connected World", Richard, RAWLINGS, Peter LEYLAND e Alison YOUNG (eds.), *Sovereignty and the Law. Domestic, European and International Perspectives,* Oxford, Oxford University Press, 2013

SCOTT, Joanne e RAJAMANI, Lavanya, "EU Climate Change Unilateralism", *EJIL*, vol. 23, n.º 2, p. 469 e ss.

SELVADURAI, Niloufer, "The Proper Basis for Exercising Jurisdiction in Internet Disputes: Strengthening State Boundaries or Moving Towards Unification?", *JTLP,* vol. 13, n.º 2, 2012, p. 17 e ss.

SHAFFER, Gregory, "Globalization and Social Protection: the Impact of EU and International Rules in Ratcheting Up Privacy Standards", *YJIL,* n.º 25, 2000, p. 2 e ss.

SILVA, Jorge Pereira da, *Deveres do Estado de Proteção de Direitos Fundamentais,* Universidade Católica, Lisboa, 2015

SILVA, Paula Costa e, "As autoridades administrativas independentes", *O Direito,* ano 138.º, tomo III, 2006, p. 558 e ss.

SIMMONS, Beth, "The International Politics of Harmonization: The Case of Capital Market Regulation", *IO,* vol. 55, n.º 3, 2001, p. 589 e ss.

SLOT, Piet e GRABANDT, Eric, "Extraterritoriality and Jurisdiction", *CMLR,* vol. 23, n.º 3, 1986, p. 545 e ss.

SOLOVE, Daniel, "Digital Dossiers and the Dissipation of Fourth Amendment Privacy", *CalLR*, n.º 75, 2002, p. 1803 e ss.

STAIGER, Dominic, "Cross-border data flow in the cloud between the EU and the US", Anne CHEUNG e Rolf WEBER, *Privacy and Legal Issues in Cloud Computing,* Edward Elgar Publishing, Cheltenham/Northampton 2015, p. 96 e ss.

STERN, Brigitte, "L'extraterritorialité 'revisitée': où il est question des affaires Alvarez-Machain, Pâte Bois et de quelques autres", *AFDI*, vol. 38, n.º 1, 1992, p. 239 e ss.

- "Quelques observations sur les règles internationals relatives à l'application extraterritoriale du droit", *AFDI,* 1986, p. 30 e ss.

STIGLITZ, Joseph, *Globalisation and its Discontents,* Norton, Nova Iorque, 2002

SUDA, Yuko, *The Politics of Data Transfer. Transatlantic conflict and cooperation over data privacy,* Routledge, Londres, 2018

- "Transatlantic Politics of Data Transfer: Extraterritoriality, Counter-Extraterritoriality and Counter-Terrorism", *JCMS,* vol. 51, n.º 4, 2013, p. 774 e ss.

SVANTESSON, Dan, "Article 3", Lee BYGRAVE, Christopher KUNER e Christopher DOCKSEY (eds.), *Commentary on the EU General Data Protection Regulation,* Oxford University Press, Oxford, Forthcoming in 2019, p. 1, disponível em https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3179907

- *Solving the Internet Jurisdiction Puzzle,* Oxford University Press, Oxford, 2017

- "Enforcing Privacy across different jurisdictions", David WRIGHT e Paul de HERT (eds.), *Enforcing privacy: regulatory, legal and technological approaches,* Springer, 2016, p. 195 e ss.

- "The Google Spain case: part of a harmful trend of jurisdictional overreach", *EUI Working Papers*, 2015, disponível em http://cadmus.eui.eu/bitstream/handle/1814/36317/RSCAS_2015_45.pdf?sequence=1&isAllowed=y

- "Delineating the Reach of Internet Intermediaries's Content Blocking – "ccTLD Blocking", "Strict Geolocation Blocking" or a "Country Lens Approach", *SCRIPTed,* vol. 11, n.º 2, 2014, p. 153 e ss.

- *Extraterritoriality in Data Privacy Law,* Copenhaga, Ex Tuto, 2013

- "Time for the Law to Take Internet Geo-Location Technologies Seriously", *JPIL,* vol. 8, n.º 3, 2012, p. 473 e ss.

- "The regulation of cross-border data flows", *IDPL,* vol. 1, n.º 3, 2011, p. 180 e ss.

- "Pammer and Hotel Alpenhof – ECJ Decision Creates Further Uncertainty about When E-Business 'Direct Activities' to a Consumer's State under the Brussels I Regulation", *CLSR,* vol. 27, n.º 3, 2011, p. 298 e ss.

- "Privacy, The Internet and Transborder Data Flows. An Australian Perspective", *MUJLT,* vol. 4, n.º 1, 2010, p. 2 e ss.

SVANTESSON, Dan e KLOZA, Dariusz, "Landscape with the rise of data privacy protections", Dan SVANTESSON e Dariusz KLOZA (eds.), *Trans-atlantic data privacy as a challenge for democracy,* Intersentia, Cambridge/Antuérpia, 2017, p. 564 e ss.

SWIRE, Peter, "Of Elephants, Mice, and Privacy: International Choice of Law and the Internet", *UPLR,* vol. 153, 2005, p. 1977 e ss.

TAYLOR, Mistale, "*Google Spain* Revisited: The Misunderstood Implementation of a Landmark Decision and How Public International Law Could Offer Guidance", *EDPL,* n.º 2, 2017, p. 195 e ss.

- "The EU's human rights obligations in relation to its data protection laws with extraterritorial effect", *IDPL,* vol. 5, n.º 4, 2015, p. 247 e ss.

TENE, Omar, "Reforming Data Protection in Europe and beyond: A Critical Assessment of the Second Wave of Global Privacy Laws", Artemi LOMBARTE e Rosario MAHAMUT (eds.), *Hacia Un Nuevo Derecho Europeo de Protección de Datos,* Tirant Lo Blanch, Valencia, 2015, p. 197 e ss.

- "For Privacy, European Commission must be innovative", *Center for Democracy & Technology,* 2011, disponível em https://cdt.org/blog/for-privacy-european-commission-must-be-innovative/

- "Privacy: the new generations", *IDPL,* vol. 1, n.º 1, 2011, p. 15 e ss.

TENE, Omar e WOLF, Christopher "Overextended: Jurisdiction and Applicable Law under the EU General Data Protection Regulation", White Paper, *The Future of Privacy Forum*, 2013, disponivel online em https://pt.scribd.com/document/121642254/Overextended-Jurisdiction-and-Applicable-Law-under-the-EU-General-Data-Protection-Regulation

TERWAGNE, Cécile e LOUVEAUX, Sophie, "Data Protection and Online Networks", *CLSR,* n.º 13, 1997, p. 234 e ss.

THIERER, Adam, "Privacy Law's Precautionary Principle Problem", *MLR,* vol. 66, n.º 2, 2014, p. 468 e ss..

THOMAS-SERTILLANGE, Jean-Baptiste e QUILLATRE, Elisabeth, "Libre circulation des données à caractere personnel au sein du marche intérieur et de l'espace de Liberté Sécurité Justice: Vers une diversification des instruments de régulation", *Petites Affiches,* n.º 400, 2011

TORREMANS, Paul, "Extraterritorial Application of E.C. and U.S. Competition Law", *ELR,* vol. 21, 1996, p. 280 e ss.

TRAUTMAN, Donald, "The Role of Conflicts Thinking in Defining the International Reach of American Regulatory Legislation", *OSLJ*, vol. 22, n.º 3, 1961, p. 586 e ss.

TRIMBLE, Marketa, "Extraterritorial Enforcement of National Laws in Connection with Online Commercial Activity", John ROTHCHILD (ed.), *Research Handbook of Electronic Commerce Law,* Edward Elgar Publishing, Cheltenham/Northampton, 2015, p. 261 e ss.

- "Advancing National Intellectual Property Policies in a Transnational Context", *MLR*, n.º 74, 2014, p. 203 e ss.

- "The Future of Cybertravel: Legal Implications of the Evasion of Geolocation", *FIPMELJ,* vol. 21, n.º 3, 2012, p. 567 e ss.

TRIEPEL, Heinrich, "Les Rapports entre le Droit Interne et le Droit International", *RCADI,* Tomo I, 1923, p. 73 e ss.

TUORI, Kaarlo, "Transnational law: on legal hybrids and legal perspectivism", Miguel POAIRES MADURO, Kaarlo TUORI e Suvi SANKARI, (eds.), *Transnational Law. Rethinking European Law and Legal Thinking*, Cambridge, Cambridge University Press, 2014, p. 11 e ss..

- *Critical Legal Positivism,* Ashgate, Aldershot, 2002

TZANOU, Maria, *The Fundamental Right to Data Protection. Normative Value in the Context of Counter-Terrorism Surveillance,* Hart Publishing, Oxford/Portland, 2017

- "The war against terror and transatlantic information sharing: spillovers of privacy or spillovers of security", *UJIEL,* n.º 31, vol. 80, 2015, p. 87 e ss.

- "Data Protection as a Fundamental Right Next to Privacy?" 'Reconstructing' a Not So New Right", *IDPL,* n.º 3, 2013, p. 88 e ss.

VARGHESE, Tracy, "The WTO's *Shrimp-Turtle* Decisions: the Extraterritorial Enforcement of U.S. Environmental Policy via Unilateral Trade Embargos", *TEL,* vol. 8, n.º 2, 2001/2002, p. 421 e ss.

VENTURA, Catarina Sampaio, "Contexto e Justificação da Carta", AA.VV., *Carta dos Direitos Fundamentais da União Europeia,* Coimbra Editora, Coimbra, 2001, p. 39 e ss.

VERMEULEN, Gert, "The Paper Shield. On the degree of Protection of the EU-US Privacy Shield against Unnecessary or Disproportionate Data Collection by the US Intelligence and Law Enforcement Services", Dan SVANTESSON e Dariusz KLOZA (eds.), *Trans-atlantic data privacy as a challenge for democracy,* Intersentia, Cambridge/Antuérpia, 2017, p. 127 e ss.

VEIL, Winfried, "DS-GVO: Risikobasierter Ansatz statt rigidez Verbotsprinzip – Eine erste Bestandsaufnahme", *Zeitschrift fur Datenschutz,* vol. 5, n.º 8, 2015, p. 347 e ss.

VERBIEST, Thibault e WÉRY, Etienne, *Le Droit de L'Internet et de la Société de l'Information,* Larcier, Paris, 2001

VERHENNEMAN, Griet e COUDERT, Fanny, "Widening and strengthening the appeal of Convention 108", *DPLP,* Março de 2015, p. 8 e ss.

VICENTE, Dário Moura, "International Harmonization and Unification of Private Law in a Globalized Economy", Anthony D'SOUZA e Carmo D'SOUZA (eds.), *Civil Law Studies: An Indian Perspective,* Cambridge Scholars Publishing, Oxford, 2009, p. 47 e ss.

VILLA, Diana, *Negocios internacionales de tratamiento de datos personales,* Civitas, Pamplona, 2010

VOENEKY, Silja, "Espionage, Security Interests, and Human Rights in the Second Machine Age: NSA Mass Surveillance and the Framework of Public International Law", Russell MILLER (ed.), *Privacy and Power. A Transatlantic Dialogue in the Shadow of the NSA-Affair,* Cambridge University Press, Cambridge, 2017, p. 492 e ss.

VOGEL, David, *The Politics of Precaution. Regulating Health, Safety, and Environmental Risks in Europe and the United States,* Princeton University Press, New Jersey, 2010

VOIGT, Paul e BUSSCHE, Axel, *The EU General Data Protection Regulation (GDPR). A Practical Guide*, Springer, Dordrecht, 2017

XAVIER, Alberto, *Direito Tributário Internacional*, 2ª edição, Almedina, Coimbra, 2009

YOUNG, Alasdair, "The European Union as a Global Regulator? Context and Comparison", *JEPP,* vol. 22, 2015, p. 1233 e ss.

- "Political Transfer and 'Trading up'? Transatlantic Trade in Genetically Modified Food and US Politics", *WP,* n.º 55, Julho, 2003, p. 457 e ss.

WALEN, Alan, "Fourth Amendment Rights for Nonresident Aliens", Russell MILLER (ed.), *Privacy and Power. A Transatlantic Dialogue in the Shadow of the NSA-Affair,* Cambridge University Press, Cambridge, 2017, p. 282 e ss.

WALKER, Neil, "Late Sovereignty in the European Union", Neil WALKER (ed.), *Sovereignty in Transition,* Hart Publishing, Oxford/Portland, 2003, p. 3 e ss..

WALLER, Spencer, "The Twilight of Comity", *CJTL,* vol. 38, 2000, p. 563 e ss.

WATERS, Nigel, "The European influence on privacy law and practice", *PLPR,* n.º 2, 2003, disponível em http://www.austlii.edu.au/au/journals/PLPR/2003/2.html

WEBER, Rolf, "Transnational Data Privacy in the EU Digital Single Market", Dan SVANTESSON e Dariusz KLOZA (eds.), *Trans-atlantic data privacy as a challenge for democracy,* Intersentia, Cambridge/Antuérpia, 2017, p. 5 e ss..

- "Transborder data transfers: concepts, regulatory approach and new legislative initiatives", *IDPL,* vol. 3, n.º 2, 2013, p. 117 e ss.

WEILER, Joseph, "The Judicial Après Nice", Gráinne DE BURCA e Joseph WEILER (eds), *The European Court of Justice,* Oxford University Press, Oxford, 2001, p. 215 e ss.

WHITAKER, Simon, "Consumer Law and the distinction between public law and private law", *The Public Law/Private Law Divide – Une entente assez cordiale,* Mark

FREEDLAND, e Jean-Bernard AUBY (eds.), Hart Publishing, Oxford/Portland, 2006, p. 247 e ss.

WIENER, Jonathan, HAMMIT, James, ROGERS, Michael e SAND, Peter, (eds.), *The Reality of Precaution: Comparing Risk Regulation in the United States and Europe,* Routledge, Londres, 2010

WINN, Jane, "Technical standards as data protection regulation", Serge GUTWIRTH, Yves POULLET, Paul de HERT e Cécile de TERWANGNE (eds.), *Reinventing Data Protection?* Springer, Dordrecht, 2009, p. 191 e ss..

WISH, Richard e BAILEY, David, *Competition law,* 7ª ed., Oxford University Press, Oxford, 2012

WITTES, Benjamin, "Privacy, Hypocrisy, and a Defense of Surveillance", Russell MILLER (ed.), *Privacy and Power. A Transatlantic Dialogue in the Shadow of the NSA-Affair,* Cambridge University Press, Cambridge, 2017, p. 180 e ss.

WOJTAN, Boris, "The new EU Model Clauses: one step forward, two steps back?", *IDPL,* n.º 1, vol. 1, 2011, p. 76 e ss.

WRIGHT, David e KREISSL, Reinhard, "European responses to the Snowden revelations: A discussion paper", *Increasing Resilience in Surveillance Societies (IRISS),* Dezembro de 2013, disponível em http://irissproject.eu/wp-content/uploads/2013/12/IRISS_European-responses-to-the-Snowden-revelations_18-Dec-2013_Final.pdf

ZANFIR, Gabriela, "How CJEU's 'Privacy Spring' Construed the Human Rights Shield in the Digital Age", *European judicial systems as a challenge for democracy,* Intersentia, Cambridge/Antuérpia, 2015, p. 111 e ss.

ZERK, Jennifer, "Extraterritorial Jurisdiction: Lessons from the Business and Human Rights Sphere from Six Regulatory Areas", *Harvard Corporate Social Responsibility Initiative Working Paper No. 59,* disponível online em https://www.hks.harvard.edu/m-rcbg/CSRI/publications/workingpaper_59_zerk.pdf

ZEKOLL, Joachim, "Jurisdiction in Cyberspace", Gunther HANDL, Joachim ZEKOLL e Peer ZUMBANSEN, *Beyond Territoriality. Transnational Legal Authority in an Age of Globalization,* Martinus Nijhoff Publisher, Leiden/Boston, 2012, p. 369 e ss.

ZINSER, Alexander, "The European Commission Decision on Standard Contractual Clauses for the Transfer of Personal Data to Third Countries: an Effective Solution?", *CKJIP*, n.º 3, 2003, p. 24 e ss.

ZUMBANSEN, Peer, "Transnational Law", Jan SMITS (ed.), *Encyclopedia of Comparative Law,* Edward Elgar Publishing, Cheltenham/Northampton, p. 738 e ss.

Jurisprudência consultada e outra documentação

Jurisprudência consultada

1927

Acórdão do TPJI, França c. Turquia, 7 de setembro de 1927

1984

Acórdão do TIJ, Bélgica c. Espanha, 24 de Julho de 1984

1992

COM, "Amended proposal for a Council Directive on the protection of individuals with regard to the processing of personal data and on the free movement of such data. Explanatory Memorandum", 15 de outubro de 1992

2001

OMC, "Dispute Panel Report on United States – Import Prohibition of Certain Shrimp and Shrimp Products", WT/DS58/R, junho de 2001

2002

Acórdão do TIJ, República Democrática do Congo c. Bélgica, 2002

2003

Acórdão do TJ, Österreichischer Rundfunk *et alii* c. Christa Neukomm e Joseph Lauermann, C-465/00, 20 de maio de 2003

Acórdão do TJ, Bodil Lindqvist c. Göta hovrätt, 6 de novembro de 2003

2010

Acórdão do TJ, Peter Pammer c. Reederei Karl Schluter GmbH & Co KG, C-585/08 e C-144/09, 7 de dezembro de 2010

Acórdão do TJ, Volker und Markus Schecke GbR e Hartmut Eifert c. Land Hessen, C-92/09 e C-93/09, 9 de novembro de 2010

2011

Acórdão do TJ, Air Transport Association of America *et alii* c. Secretary of State for Energy and Climate Change*,* C-366/10, 21 de dezembro de 2011

2012

Acórdão do TJ, Daniela Muhlleitner c. Ahmad Yusufi e Wadat Yusufi*,* C-190/11, 6 de setembro de 2012

2013

Acórdão do TJ, Lokman Emrek c. Vlado Sabranovic*,* C-218/12, 17 de outubro de 2013

2014

Acórdão do TJ, Google Spain SL e Google Inc. c. Agencia Española de Protección de Datos (AEPD) e Mario Costeja González*,* C-131/12, 13 de maio de 2014

Acórdão do TJ, Digital Rights Ireland *et alii* c. Minister for Communications, Marine and Natural Resources *et alii,* C-293/12, 8 de abril de 2014

2015

Acórdão do TJ, Weltimmo s. r. o. c. Nemzeti Adatvédelmi és Információszabadság Hatóság*,* C-230/14, 1 de outubro de 2015

Acórdão do TJ, Maximillian Schrems c. Data Protection Commissioner, C-363/14, 6 de outubro de 2015

2016

Acórdão do TJ, Tele2 Sverige AB c. Post-och telestyrelsen e Secretary of State for the Home Department *et alii*, C-203/15 e C-698/15, 21 de dezembro de 2016

Acórdão do TJ, Verein für Konsumenteninformation c. Amazon EU Sàrl*,* C-191/15, 28 de julho de 2016

Acórdão do USCASC, Microsoft Corporation c. United States of America, 14-2985, 14 de julho de 2016

2017

Parecer 1/15 do TJ, 26 de julho de 2017

Acórdão do TJ, Peter Nowak c. Data Protection Commissioner*,* C-434/16, 20 de dezembro de 2017

2018

Acórdão do SCJ, United States of America c. Microsoft Corporation, 584 U.S., 17 de abril de 2018

Outra documentação

1987

Câmara do Comércio Internacional, *The Extraterritorial Application of National Laws – The International Chamber of Commerce*, ICC Publishing S. A., 1987

1997

G29, "Primeiras orientações sobre as transferências de dados para países terceiros – eventual metodologia a adotar para avaliar a adequação do grau de proteção", 26 de junho de 1997

1998

G29, "Documento de Trabalho: Observações preliminares relativas ao uso de cláusulas contratuais no contexto da transferência de dados pessoais para países terceiros", adotado em 22 de abril de 1998

G29, "Documento de Trabalho. Transferência de dados pessoais para países terceiros: aplicação dos artigos 25.º e 26.º da Diretiva comunitária relativa à proteção dos dados", 24 de julho de 1998

COM, "Handbook on Cost Effective Compliance with Directive 95/46/EC", Anexo ao "Annual Report 1998 (XV D/5047/98) of the Working Party Established by Article 29 of the Directive 95/46/EC", Directorate-General Internal Market and Financial Services, 1998

1999

G29, "Recommendation 4/99 on the inclusion of the fundamental right to data protection in the European catalogue of fundamental rights", 7 de setembro de 1999

2000

G29, "Privacidade na Internet – uma abordagem integrada da UE no domínio da proteção de dados em linha", 21 de novembro de 2000

Decisão da COM, de 26 de julho de 2000, nos termos da Diretiva 95/46, relativa ao nível de proteção assegurado pelos princípios de "porto seguro" e pelas respetivas questões mais frequentes (FAQ) emitidos pelo Department of Commerce dos Estados Unidos da América (Decisão 2000/520/CE)

2001

G29, "Parecer 2/2001 relativo ao nível de adequação proporcionado pela lei canadiana sobre dados pessoais e documentos eletrónicos (*Personal Information and Electronic Documents Act*)", 26 de janeiro de 2001

G29, "Parecer 7/2001 sobre o projeto de decisão da Comissão (versão de 31 de Agosto de 2001) relativa às cláusulas contratuais-tipo aplicáveis à transferência de dados pessoais para subcontratantes estabelecidos em países terceiros, em conformidade com o n.º 4 do artigo 26.º da Diretiva 95/46/CE", 13 de setembro de 2001

Decisão da Comissão de 15 de junho de 2001 relativa às cláusulas contratuais-tipo aplicáveis à transferência de dados pessoais para países terceiros, nos termos da Diretiva 95/46/CE (Decisão 2001/497/EC)

2002

G29, "Documento de trabalho sobre a determinação da aplicação internacional da legislação da UE em matéria de proteção de dados ao tratamento de dados pessoais na Internet efetuado por sites não europeus", 30 de maio de 2002

G29, "Parecer sobre o nível de proteção dos dados pessoais na Argentina", 3 de outubro de 2002

2003

G29, "Working Document on Transfers of personal data to third countries: Applying Article 26 (2) of the EU Data Protection Directive to Binding Corporate Rules for International Data Transfers", 3 de junho de 2003

Decisão da COM de 30 de junho de 2003, nos termos da Diretiva 95/46/CE do Parlamento Europeu e do Conselho relativa à adequação do nível de proteção de dados pessoais na Argentina (Decisão 2003/490/EC)

COM, "Analysis and Impact Study on the Implementation of Directive EC 95/46 in Member States. Technical Annex to First Report", 2003

COM, "Primeiro relatório sobre a implementação da diretiva relativa à proteção de dados 95/46/CE", 15 de maio de 2003

2004

G29, "Model Checklist Application for approval of Binding Corporate Rules", 25 de novembro de 2004

Information and Privacy Commissioner for British Columbia, "Privacy and the USA Patriot Act: Implications for British Columbia Public Sector Outsourcing", Outubro de 2004

Decisão da COM de 27 de Dezembro de 2004 que altera a Decisão 2001/497/EC no que se refere à introdução de um conjunto alternativo de cláusulas contratuais típicas aplicáveis à transferência de dados pessoais para países terceiros (Decisão 2004/915/EC)

2005

G29, "Working Document Setting Forth a Co-Operation procedure for issuing Common Opinions on Adequate Safeguards Resulting From 'Binding Corporate Rules'", 14 de abril de 2005

G29, "Working Document Establishing a Model Checklist Application for Approval of Binding Corporate Rules", 14 de abril de 2005

2006

G29, "Parecer 10/2006 sobre o tratamento de dados pessoais pela Sociedade das Telecomunicações Financeiras Interbancárias no Mundo (Worldwide Interbank Financial Telecommunication – SWIFT)", 22 de novembro de 2006

CDI, "Report on the Work of its Fifty-Eight Session", 1 May-9 June and 3 July-11 August 2006, UN Doc. A/61/10, Annex E

2007

G29, "Recommendation 1/2007 on the Standard Application for Approval of Binding Corporate Rules for the Transfer of Personal Data", 10 de janeiro de 2007

Dusseldorf Kreis, "Fallgruppen zur Internationalen Auftragsdatenverarbeitung, Handreichung des Dusseldorf Kreises zur rechtlichen Bewertung", 28 de março de 2007

OCDE, "Recommendation on Cross-border Co-operation in the Enforcement of Laws Protecting Privacy", 12 de junho de 2007

College bescherming persoonsgegevens (autoridade de controlo holandesa), "Publication of Personal Data on the Internet", dezembro de 2007

2008

G29, "Working Document setting up a table with the elements and principles to be found in Binding Corporate Rules", 24 de junho de 2008

G29, "Working Document setting up a framework for the structure of Binding Corporate Rules", 24 de junho de 2008

G29, "Working Document on Frequently Asked Questions (FAQs) related to Binding Corporate Rules", 24 de junho de 2008

International Bar Association, *Report of the Task Force on Extraterritorial Jurisdiction,* 2008

2009

G29, "Documento de Trabalho 1/2009 sobre a troca preliminar de informação ("*pre-trial discovery")* nos litígios cíveis transfronteiriços", 11 de fevereiro de 2009

G29, "The Future of Privacy. Joint contribution on the Consultation of the European Commission on the legal Framework for the fundamental right to protection of personal data", 1 de dezembro de 2009

COM, "Frequently Asked Questions Relating To Transfers of Personal Data From the EU/EEA to Third Countries", 2009

2010

G29, "Parecer 1/2010 sobre os conceitos de "responsável pelo tratamento" e "subcontratante"", 16 de fevereiro de 2010

G29, "Parecer 2/2010 sobre publicidade comportamental em linha", 22 de junho de 2010

G29, "Parecer 6/2010 sobre o nível de proteção dos dados pessoais na República Oriental do Uruguai", 12 de outubro de 2010

ICO, "The Eight Data Protection Principle in International Data Transfers v4", 2010

ICO, "The Guide to Data Protection", 2010

Decisão da COM de 5 de fevereiro de 2010 relativa a cláusulas contratuais-tipo aplicáveis à transferência de dados pessoais para subcontratantes estabelecidos em países terceiros nos termos da Diretiva 95/46/CE do Parlamento Europeu e do Conselho (Decisão 2010/87/EU)

COM, "Summary of Replies to the Public Consultation about the Future Legal Framework for Protecting Personal Data", 2010

Hague Conference on Private International Law, "Cross-Border Data Flows and Protection of Privacy", 2010

2011

G29, "Parecer 1/2011 sobre o nível de proteção de dados pessoais na Nova Zelândia", 4 de abril de 2011

SEPD, "Parecer da AEPD sobre a Comunicação da Comissão – 'Uma abordagem global da proteção de dados pessoais na União Europeia'", 14 de janeiro de 2011

Datatilsynet, *Processing of sensitive personal data in a cloud situation,* 2011

Datainspektionen, *Salems*, 2011

OCDE, "Report on the Implementation of the OECD Recommendation on Cross-Border Co-operation in the Enforcement of Laws Protecting Privacy", 2011

Working Party for Information and Security and Privacy (WPISP), *The evolving privacy landscape: 30 years after the OECD Privacy Guidelines,* Directorate for Science, Technology and Industry – Committee for Information, Computer and Communitactions Policy, 2011

2012

G29, "Parecer 01/2012 sobre as propostas de reforma em matéria de proteção de dados", 23 de março de 2012

G29, "Working Document 02/2012 setting up a table with the elements and principles to be found in Processor Binding Corporate Rules", 6 de junho de 2012

G29, "Parecer 5/2012 relativo a computação em nuvem", 1 de julho de 2012

G29, "Recommendation 1/2012 on the Standard Application form for Approval of Binding Corporate Rules for the Transfer of Personal Data for Processing Activities", 17 de setembro de 2012

SEPD, "Opinion of the European Data Protection Supervisor on the Data Protection Reform Package", 7 de março de 2012

SEPD, "Opinion on the Commission's Communication on 'Unleashing the Potential of Cloud Computing in Europe'", 2012

Information and Privacy Commissioner of Ontario, "Reviewing the Licensing Automation System of the Ministry of National Resources", 2012

ICO, "Personal Data Protection & Could Computing", 2012

ICO, "Information Commissioner's Office: Initial Analysis of the European Commission's Proposals for a Revised Data Protection Legislative Framework", 27 de fevereiro de 2012

Decisão de execução da COM, de 21 de agosto de 2012, nos termos da diretiva 95/46/CE do Parlamento Europeu e do Conselho relativa à adequação do nível de proteção de dados pessoais pela República Oriental do Uruguai no que se refere ao tratamento automatizado de dados (Decisão 2102/484/EU)

COM, "Proteção da privacidade num mundo interligado. Um quadro europeu de proteção de dados para o século XXI", de 25 de janeiro de 2012

COM, "Impact Assessment Accompanying the document Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) and Directive of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by competent

authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data", 25 de janeiro de 2012

COM, "Proposta de regulamento do Parlamento Europeu e do Conselho relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados", 25 de janeiro de 2012

Câmara do Comércio Internacional, "Cross-border law enforcement access to company data – current issues under data protection and privacy law", Doc. Nº 373/507, 7 de fevereiro de 2012

2013

G29, "Parecer 3/2013 sobre limitação da finalidade", 2 de abril de 2013

Office of the Privacy Commissioner of Canada, "The Case for Reforming the Personal Information Protection and Electronic Documents Act", 2013

AEPD, "Guía para clientes que contraten servicios de Cloud Computing", 2013

Datainspektionen, *Salems*, 2013

COM, "What does the Commission Mean by Secure Cloud Computing Services in Europe?", MEMO/13/898, 2013

COM, "Restabelecer a confiança nos fluxos de dados entre a UE e os EUA", de 27 de novembro de 2013

COM, "Sobre o funcionamento do sistema 'porto seguro' na perspetiva dos cidadãos da UE e das empresas estabelecidas na UE", de 27 de novembro de 2013

2014

G29, "Opinion 02/2014 on 'Referential for requirements for Binding Corporate Rules submitted to national data protection authorities in the EU and Cross Border Privacy Rules submitted to APEC CBPR Accountability Agents", 27 de fevereiro de 2014

G29, "Opinion 02/2014 on a referential for requirements for Binding Corporate Rules submitted to national Data Protection Authorities in the EU and Cross Border Privacy Rules submitted to APEC CBPR Accountability Agents", 27 de fevereiro de 2014

G29, "Parecer 06/2014 sobre o conceito de interesses legítimos do responsável pelo tratamento dos dados na aceção do artigo 7.º da Diretiva 95/46/CE", 9 de abril de 2014

G29, "Parecer 04/2014 sobre a vigilância de comunicações eletrónicas para efeitos de informações e segurança nacional", 10 de abril de 2014

G29, "Statement on the role of a risk-based approach in data protection legal framework", 30 de maio de 2014

G29, "Guidelines on the implementation of the court of justice of the European Union Judgement on 'Google Spain and Inc V. Agencia Española de Protección de Datos (AEPD) And Mario Costeja González" C-131/12", 26 de novembro de 2014

G29, "Working Document on surveillance of electronic communications for intelligence and national security purposes", 5 de dezembro de 2014

SEPD, "The Transfer of Personal Data to Third Countries and International Organisations by EU Institutions and Bodies", 14 de julho de 2014

Konferenz der Datenschutzbeauftragten des Bundes und der Länder & Düsseldorfer Kreises, "Orientierungshilfe: Cloud Computing Version 2.0", outubro de 2014

2015

G29, "Explanatory Document on the Processor Binding Corporate Rules", 19 de abril de 2013 e revisto a 22 de maio de 2015

AEPD, "Resolución n.º R/01976/2015", 2015

COM, "Sobre a transferências de dados pessoais da UE para os Estados Unidos da América ao abrigo da Diretiva 95/46/CE na sequência do acórdão proferido pelo Tribunal de Justiça no processo C-362/14 (Schrems), 6 de novembro de 2015

OCDE, *Roundtable of Competition Neutrality,* Directorate for Financial and enterprises affairs competition Committee, 12 de junho de 2015

2016

G29, "Statement on Schrems Judgement", 3 de fevereiro de 2016

G29, "Letter of the Chair of Article 29 data protection working party", 16 de dezembro de 2016

SEPD, "Opinion on the EU-U.S. Privacy Shield Draft Adequacy Decision. Opinion 4/2016", 30 de maio de 2016

Decisão de execução da COM de 12 de julho de 2016, relativa ao nível de proteção assegurado pelo Escudo de Proteção da Privacidade UE-EUA, com fundamento na Diretiva 95/46/CE do Parlamento Europeu e do Conselho (Decisão 2016/1250/EU)

UNCTAD, "Data protection regulations and international flows: Implications for trade and development", 2016

2017

COM, "Construir uma economia europeia dos dados", 10 de janeiro de 2017

G29, "Guidelines on the application and setting of administrative fines for the purposes of the Regulation 2016/679, 3 de outubro de 2017

G29, "Orientações relativas à Avaliação de Impacto sobre a Proteção de Dados (AIPD) e que determinam se o tratamento é suscetível de resultar num elevado risco para efeitos do Regulamento (EU) 2016/679", 4 de outubro de 2017

G29, "Statement on electronic evidence", 27 de outubro de 2017

G29, "Working Document setting up a table with the elements and principles to be found in Binding Corporate Rules", 27 de novembro de 2017

G29, "Guidelines on Consent under Regulation 2016/679", 28 de novembro de 2017

G29, "EU-U.S. Privacy Shield – First annual Joint Review", 28 de novembro de 2017

2018

G29, "Adequacy Referential", 6 de fevereiro de 2018

G29, "EU general data protection regulation. General Information Document", 12 de fevereiro de 2018

G29, "Guidelines on consent under Regulation 2016/679", 10 de abril de 2018

G29, "Guidelines on transparency under Regulation 2016/679", 11 de abril de 2018

G29, "Working Document Setting Forth a Co-Operation Procedure for the approval of 'Binding Corporate Rules' for controllers and processors under the GDPR", 11 de abril de 2018

G29, "Working Party 29 Position Paper on the derogations from the obligation to maintain records of processing activities pursuant to Article 30 (5) GDPR", de 19 de abril de 2018

CNPD, "Parecer n.º 20/2018", 2018

CNIL, Premiers éléments d'analyse de la CNIL. Blockchain, setembro de 2018

CdE, "Draft Explanatory Report: Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data", maio de 2018

AEDF, CdE, AEPD, *Handbook on European data protection law,* 2018

Índice