

ESTUDO SOBRE A REALIZAÇÃO DO DIREITO DA PROTECÇÃO DE DADOS PESSOAIS ATRAVÉS DA JURISPRUDÊNCIA DO TRIBUNAL DE JUSTIÇA DA UNIÃO EUROPEIA

Estudio sobre la aplicación del Derecho de la Protección de Datos Personales a través de la jurisprudencia del Tribunal de Justicia de la Unión Europea

DOI: <http://dx.doi.org/10.15304/dereito.29.1.6519>

RITA DE SOUSA COSTA¹

Membro da Equipa de Tecnologias, Mobilidade & Comunicações (TMT)

PLMJ Advogados, SP, RL

rita@ritasousacosta.com

Resumen

En el contexto de los constantes desafíos a la aplicación del derecho fundamental a la protección de datos, es esencial comprender cómo la interpretación del derecho positivo se ve influida por otras fuentes de derecho, en particular por la jurisprudencia de la máxima autoridad competente para la interpretación del derecho de la Unión Europea. Este texto presenta las líneas generales de la aplicación del derecho europeo de la protección de datos tal como se establece en la jurisprudencia del TJUE, con el objetivo de demostrar cómo y en qué medida este Tribunal ha configurado -y sigue configurando- el marco jurídico vigente.

Palabras clave: Derecho europeo de la protección de datos; jurisprudencia del TJUE; densificación de principios y conceptos; “justo equilibrio” en la colisión de derechos; anulación de legislación.

Abstract

Within the context of the challenges posed to the fundamental right to data protection, it is of utmost importance to understand the effect of other sources of the law, notably the case-law of the Court of Justice of the European Union, into statutory law. The paper outlines the implementation of the European data protection law as laid down in the case-law of the Court of Justice. It is aimed to demonstrate how and to what extent the Court has shaped – and continues to shape – the current legal framework.

Keywords: European data protection law; CJEU’s case-law; implementing principles and concepts; the ‘fair balance’ criterion *vis-à-vis* collision of rights; annulment of legislation.

¹ <https://orcid.org/0000-0001-6752-3760>.

Todas as posições expressas no presente texto são estritamente pessoais e apenas vinculam a respectiva autora.

Resumo

No contexto dos constantes desafios colocados à realização do direito fundamental à protecção de dados, torna-se fundamental compreender de que forma a interpretação do direito positivo é influenciada por outras fontes do direito, concretamente pela jurisprudência da mais alta instância competente para a interpretação do direito da União Europeia. No presente texto, apresentamos as grandes linhas de aplicação do direito europeu da protecção de dados conforme gizadas pela jurisprudência do Tribunal de Justiça da União Europeia, com o objectivo de demonstrar como e em que medida este Tribunal modelou – e continua a modelar – o quadro jurídico em vigor.

Palavras-chave: Direito europeu da protecção de dados; jurisprudência do TJUE; densificação de princípios e de conceitos; “justo equilíbrio” na colisão de direitos; anulação de legislação.

SUMÁRIO

1.- INTRODUÇÃO.; 2.- A CONCILIAÇÃO ENTRE OS PRINCÍPIOS DO DIREITO DA PROTECÇÃO DE DADOS E O PRINCÍPIO DA TRANSPARÊNCIA ENQUANTO PRINCÍPIO CLÁSSICO DA ACTIVIDADE ADMINISTRATIVA.; 3.- O PREENCHIMENTO DO CONTEÚDO PROGRAMÁTICO DE PRINCÍPIOS: O CASO PARADIGMÁTICO DO PRINCÍPIO DA TOTAL INDEPENDÊNCIA DAS AUTORIDADES DE CONTROLO.; 4.- A DENSIFICAÇÃO DE CONCEITOS OPERATIVOS DA PROTECÇÃO DE DADOS: O CASO PARADIGMÁTICO DOS CONCEITOS DE “DADOS PESSOAIS” E DE “RESPONSÁVEL PELO TRATAMENTO”.; 5.- AS COLISÕES DE DIREITOS (I): O “JUSTO EQUILÍBRIO” ENTRE O DIREITO À PROTECÇÃO DOS DADOS PESSOAIS E O DIREITO À LIBERDADE DE EXPRESSÃO.; 6.- AS COLISÕES DE DIREITOS (II): O “JUSTO EQUILÍBRIO” ENTRE O DIREITO À PROTECÇÃO DOS DADOS PESSOAIS E OS DIREITOS DE PROPRIEDADE INTELECTUAL.; 7.- O “JUSTO EQUILÍBRIO” ENTRE O DIREITO À PROTECÇÃO DE DADOS E OS INTERESSES DOS ESTADOS RELACIONADOS COM A MANUTENÇÃO DA SEGURANÇA PÚBLICA.; 8.- CONCLUSÃO.; 9.- BIBLIOGRAFIA.

1. INTRODUÇÃO

A União Europeia tem experienciado, nos últimos anos, profundas reformas legislativas em matéria de protecção de dados², algumas das quais ainda não concluídas³. Estas reformas coincidem com um momento em que a União atravessa(va) uma “*crise existencial*”⁴, impulsionada,

² Designadamente, o “*data protection package*” publicado em 2016, i.e., o RGPD e a Directiva (UE) 2016/680, de 27 de Abril de 2016 (*law enforcement*).

³ Nomeadamente, a revisão do regime *ePrivacy*: cfr. “Proposta de Regulamento relativo à privacidade e às comunicações electrónicas”, COM/2017/010 final – 2017/03 (COD).

⁴ Cfr. R. DE SOUSA COSTA / T. SÉRGIO CABRAL, “A crise existencial da União Europeia: ensaio em torno da realização do projecto europeu no quadro dos desafios geopolíticos e jurídico-institucionais actuais” [Texto agraciado com o Prémio Professor Doutor Paulo de Pitta e Cunha 2017], Instituto Europeu da Faculdade de Direito da Universidade de Lisboa, Lisboa, 2017 (o texto encontra-se também publicado em inglês em: R. DE SOUSA

inter alia, por acontecimentos como o assombro do terrorismo, a incapacidade de gerir a crise dos refugiados, a retirada de um Estado-Membro ou o crescente entusiasmo dos eleitores europeus perante alternativas políticas de pendor eurocético. Em simultâneo, vivem-se tempos de disrupção tecnológica, nos quais o desenvolvimento do mercado único digital constitui uma prioridade assumida da União e em que enormes fluxos de dados (pessoais e não pessoais) são recolhidos pelas mais diversas áreas de negócio e para os mais diversos (e, por vezes, controversos) fins. Casos como “Cambridge Analytica”⁵ demonstram que o direito da protecção de dados coloca permanentes desafios à cidadania na União e à própria democracia. Emergências sanitárias, como a recente COVID-19, demonstram que a efectividade do direito da protecção de dados, enquanto direito fundamental, não pode encontrar-se subalternizada relativamente a outros direitos fundamentais⁶.

É neste contexto de reforma e de constantes desafios colocados à realização do direito fundamental à protecção de dados que se torna pertinente compreender de que forma a interpretação do direito positivo é influenciada por outras fontes do direito, concretamente pela jurisprudência da mais alta instância competente para a interpretação do direito da União Europeia: o TJUE. A realização do direito da protecção de dados, tal como sucede noutras áreas do direito, está, pois, indelevelmente marcada pela relevância das fontes de carácter jurisprudencial. Esta asserção é sustentada pelas soluções preconizadas pelo legislador europeu da protecção de dados, que, não raro, reflectem os corolários jurisprudenciais do TJUE.

No presente texto, apresentamos seis grandes linhas de aplicação do direito europeu da protecção de dados conforme gizadas pela jurisprudência do TJUE, com o objectivo de demonstrar como e em que medida este Tribunal modelou – e continua a modelar – o quadro jurídico em vigor. Em cada secção do texto, será destacada cada uma das

COSTA / T. SÉRGIO CABRAL, “The European Union’s existential crisis: current challenges from populism to Donald Trump”, *UNIO EU Law Journal*, Vol. 4, n.º 1, 2018).

⁵ Cfr. C. CADWALLADR / E. GRAHAM-HARRISON, “Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach”, *The Guardian* (Londres, 17.03.2018), disponível em <https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election> [consultado em 05.01.2020].

⁶ Sobre o tema, cfr. EDPB, “Statement on the processing of personal data in the context of the COVID-19 outbreak”, Bruxelas, 19.03.2020, disponível em https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_statement_2020_processingpersonaldataandcovid-19_en.pdf [consultado em 26.06.2020]; assim como o Relatório da CE sobre a avaliação da aplicação do RGPD, mencionando a respectiva flexibilidade, mesmo no contexto de emergências sanitárias globais como a Covid-19: COMISSÃO EUROPEIA, “Data protection as a pillar of citizens’ empowerment and the EU’s approach to the digital transition – two years of application of the General Data Protection Regulation”, COM(2020) 264 final, Bruxelas, 24.06.2020, disponível em https://ec.europa.eu/info/sites/info/files/1_en_act_part1_v6_1.pdf [consultado em 26.06.2020].

referidas linhas de aplicação, as quais serão descritas e analisadas, permitindo, ulteriormente, derivar as conclusões vertidas na secção final.

2. A CONCILIAÇÃO ENTRE OS PRINCÍPIOS DO DIREITO DA PROTECÇÃO DE DADOS E O PRINCÍPIO DA TRANSPARÊNCIA ENQUANTO PRINCÍPIO CLÁSSICO DA ACTIVIDADE ADMINISTRATIVA

I. O facto de o direito à protecção de dados pessoais ser um direito fundamental reconhecido em diversos instrumentos jurídicos internacionais, na União Europeia e nalgumas Constituições dos Estados-Membros demonstra, inequivocamente, a importância que assume o respeito pelo mesmo⁷. No entanto, o direito à protecção de dados, como outros direitos fundamentais, admite restrições, mediante certas ponderações.

O princípio da transparência administrativa, na vertente da publicidade de certas actuações administrativas, encontra-se também inscrito na ordem jurídica da União e dos Estados-Membros⁸. Ora, esta publicidade pode, em determinados casos, conflitar com o direito à protecção de dados das pessoas singulares envolvidas⁹. Não surpreende, por isso, que alguns dos primeiros acórdãos do TJ, em matéria de protecção de dados, respeitassem a ponderações relativas à publicidade de actuações administrativas.

II. Os princípios gerais da Directiva 95/46/CE foram chamados à colação no acórdão *Fisher*¹⁰. Apesar de, à data dos factos, a Directiva 95/46/CE ainda não ter encetado a sua vigência, o TJ aplicou a referida directiva, considerando que os princípios da protecção das liberdades e dos direitos fundamentais, nomeadamente a protecção do direito à vida privada, já

⁷ O TJ referiu-se ao direito da protecção de dados como um direito fundamental pela primeira vez no acórdão de 29 de Janeiro de 2008, *Promusicae*, C-275/06, ECLI:EU:C:2008:54. Cfr., neste sentido, O. LYNSKEY, *The Foundations of EU Data Protection Law*, Oxford University Press, Oxford, 2015, p. 173. O direito fundamental à protecção dos dados pessoais está, actualmente, consagrado no artigo 8.º da CDFUE, encontrando também protecção ao nível do artigo 16.º do TFUE. No âmbito do Conselho da Europa, a jurisprudência do TEDH trata os temas da protecção de dados a partir do artigo 8.º da CEDH referente ao direito ao respeito pela vida privada e familiar. No direito constitucional português, o direito fundamental à protecção dos dados pessoais encontra consagração no artigo 35.º da Constituição da República Portuguesa. Para uma perspectiva espanhola sobre este direito fundamental, cfr. R. MARTÍNEZ MARTÍNEZ, "El derecho fundamental a la protección de datos: perspectivas", *Revista d'Internet, Dret i Política*, n.º 5, 2007.

⁸ Cfr., neste sentido e para mais desenvolvimentos, S. PEREZ FERNANDES, *Da vinculação dos Estados-Membros ao «direito a uma boa administração» previsto na Carta dos Direitos Fundamentais da União Europeia – argumentos para uma internormatividade administrativa* [inédito], Tese de Doutoramento em Ciências Jurídicas Públicas apresentada à Universidade do Minho, Braga, 2016, p. 132-137.

⁹ Sobre o tema em linhas gerais, na doutrina espanhola, cfr. M. ANTONINO DE LA CÁMARA, "Transparencia y Derecho de Acceso a la Información versus Protección de Datos", *Revista Internacional de Transparencia e Integridad*, n.º 4, 2017.

¹⁰ Acórdão de 14 de Setembro de 2000, *Fisher*, C-369/98, ECLI:EU:C:2000:443.

decorriam do direito dos Estados-Membros¹¹. No caso, estava em causa a divulgação de dados relativos a culturas arvenses exploradas em anos precedentes por outra pessoa, com vista à nova pessoa encarregue de explorar as culturas saber se as mesmas seriam elegíveis para ajudas comunitárias. A pessoa anteriormente encarregue da exploração negou-se a prestar essas informações e o Ministry of Agriculture, Fisheries & Food (MAFF) invocou a lei da protecção de dados do Reino Unido para também negar o acesso a essas informações. Sem estas, a nova exploração incorria no risco de apresentar um pedido de ajudas irregular, sujeitando-se a um procedimento sancionatório. A aplicação da alínea f) do artigo 7.º da Directiva 95/46/CE permitiu ao TJ considerar que o requerente da ajuda tinha um *interesse legítimo* na comunicação desses dados¹², possibilitando ao MAFF a sua divulgação. *Fisher* é, por isso, um acórdão sobre o *interesse legítimo de terceiros*¹³ no acesso à informação, matéria que não deve ser confundida com a do “direito de acesso” enquanto um dos direitos da protecção de dados conferidos aos respectivos titulares, uma vez que, neste último caso, não está em causa o acesso de terceiros a dados pessoais (para efeito de transparência administrativa), mas sim o acesso do próprio titular aos respectivos dados (para efeito da *transparência* do próprio tratamento de dados pessoais)¹⁴.

¹¹ Cfr. *Fisher*, n.º 34.

¹² Cfr. *Fisher*, n.os. 35 a 37.

¹³ Trata-se de um dos fundamentos de licitude do tratamento, encontrando-se, actualmente, consagrado no artigo 6.º, n.º 1, alínea f), do RGPD.

¹⁴ O direito de acesso conferido aos titulares dos dados assume uma particular importância na construção dogmática do direito fundamental à protecção de dados. No plano supralegal, o artigo 8.º, n.º 2, da CDFUE, relativo ao direito fundamental à protecção de dados, refere expressamente que «[t]odas as pessoas têm o direito de aceder aos dados coligidos que lhes digam respeito». Trata-se, pois, de uma dimensão fundamental do direito à autodeterminação informativa (sobre o tema, *vd.*, na doutrina portuguesa, A. SOUSA PINHEIRO, *Privacy e Protecção de Dados Pessoais: A Construção Dogmática do Direito à Identidade Informacional*, AAFDL, Lisboa, 2015, *passim*; e, ainda, C. SARMENTO E CASTRO, “40 anos de ‘Utilização da Informática’ – o artigo 35.º da Constituição da República Portuguesa”, *e-Pública – Revista Eletrónica de Direito Público*, Vol. 3, n.º 3, 2016, pp. 50-51). A jurisprudência do TJ, relativa ao direito de acesso conforme gizado na Directiva, foi seguindo o entendimento de que o direito de acesso aos dados pessoais é um direito anterior e que está na base de outros direitos dos titulares dos dados, como a rectificação, a limitação, o apagamento, a portabilidade, a oposição ou o recurso (cfr. acórdão de 20 de Dezembro de 2017, *Nowak*, C-434/16, ECLI:EU:C:2017:994, n.º 57, *in fine*, e jurisprudência pretérita citada no acórdão). Nestes termos, a efectivação destes direitos depende, pois, da consecução do primeiro. No acórdão de 7 de Maio de 2009, *Rijkeboer*, C-553/07, ECLI:EU:C:2009:293 (cfr. n.º 49), e, mais tarde, em *Nowak* (cfr. n.º 57), o TJ explica, com clareza, que decorre da natureza do direito fundamental à protecção de dados que o titular tenha a possibilidade de assegurar que os respectivos dados são exactos e tratados de forma lícita. O titular dos dados tem, assim, o direito de acesso aos respectivos dados, pois é este direito que lhe confere a possibilidade de realizar as referidas “verificações” e exercer todos os demais direitos já descritos que estão dependentes da materialização do direito de acesso. Sobre o direito de acesso, cfr., na doutrina espanhola, V. L. GUTIÉRREZ CASTILLO, “Aproximación a la Protección Jurídica Internacional del Derecho de Acceso y Protección de Datos en Europa”, *Derecho y conocimiento*, Vol. 3, n.º 1, 2005; analisando

*Österreichischer Rundfunk*¹⁵ é, também, um acórdão sobre o direito à informação, na vertente do acesso a dados de terceiros para fins de interesse público. Neste aresto, estava em causa a divulgação massiva ao público do nome e do montante dos rendimentos anuais que excediam um determinado valor das pessoas empregadas por entidades sujeitas à auditoria do Tribunal de Contas austríaco. O TJ considerou que a Directiva não se opunha a uma legislação nacional desta natureza, se se comprovasse que a mesma seria «adequada ao objectivo de boa gestão dos fundos públicos»¹⁶. Mais tarde, em *Volker und Markus Schecke*¹⁷, o TJ aborda, de novo, a questão da ponderação entre a transparência da utilização de dinheiros públicos (em concreto, os interesses dos contribuintes no direito à informação) e os direitos à privacidade e protecção de dados das pessoas singulares visadas¹⁸, tendo concluído, neste caso, que as instituições da União excederam os limites do princípio da proporcionalidade, violando, por conseguinte, estes direitos¹⁹.

Já numa fase, porém, de maior mediatização do direito da protecção de dados e num período em que, não obstante ainda vigorar a Directiva 95/46/CE, o RGPD já havia sido publicado, o Tribunal proferiu o acórdão *Manni*²⁰. Neste aresto, o TJ teve de contrabalançar o direito à protecção de dados com os interesses de terceiros (*in casu*, a segurança jurídica nas relações entre as sociedades comerciais e terceiros) se houvesse lugar à compressão do princípio da publicidade dos registos das sociedades. Em concreto, o titular dos dados pretendia, fundando-se no facto do decurso do tempo, que a informação constante do registo de que havia sido administrador único de uma sociedade insolvente em 1992 e com inscrição no registo cancelada em 2005 fosse anonimizada ou bloqueada. O titular dos dados, à data dos factos administrador de uma outra sociedade no ramo do imobiliário, considerava que o acesso por potenciais adquirentes a esta informação era causa directa de não conseguir vender os imóveis de um complexo turístico cuja construção havia sido adjudicada à empresa que, à data, administrara²¹. Ora, o Tribunal considerou que, dada a heterogeneidade dos direitos nacionais dos Estados-Membros (*v.g.*, quanto a prazos de prescrição, etc), cabia aos mesmos a modelação desta matéria²². No entanto, de acordo com o TJ, por princípio, os Estados-Membros não podem, neste contexto fáctico, garantir ao titular o apagamento ou a limitação dos dados²³.

o acórdão *Rijkeboer*, veja-se G. GONZÁLEZ FUSTER, *The Emergence of Personal Data Protection as a Fundamental Right of the EU*, Springer, Heidelberg, 2014, pp. 228-229.

¹⁵ Acórdão de 20 de Maio de 2003, *Österreichischer Rundfunk*, processos apensos C-465/00, C-138/01 e C-139/01, ECLI:EU:C:2003:294.

¹⁶ *Österreichischer Rundfunk*, n.º 94.

¹⁷ Acórdão de 9 de Novembro de 2010, *Volker und Markus Schecke*, C-92/09, ECLI:EU:C:2010:662.

¹⁸ Cfr. *Volker und Markus Schecke*, n.º 79.

¹⁹ Cfr. *Volker und Markus Schecke*, n.º 86.

²⁰ Acórdão de 9 de Março de 2017, *Manni*, C-398/15, ECLI:EU:C:2017:197.

²¹ Cfr. *Manni*, n.os 24 e 25.

²² Cfr. *Manni*, n.º 63.

²³ Cfr. *Manni*, n.º 56.

III. A jurisprudência aqui destacada permite, desde logo, esclarecer um frequente equívoco em torno do entendimento da protecção de dados, segundo o qual esta teria uma força irreductível que obliteraria outros princípios e valores fundamentais, como sendo o acesso a documentos administrativos. Tal não é assim e o Tribunal tem vindo a explicitá-lo, com recorte, desde a primeira fase de prolação jurisprudencial a respeito da Directiva 95/46/CE.

3. O PREENCHIMENTO DO CONTEÚDO PROGRAMÁTICO DE PRINCÍPIOS: O CASO PARADIGMÁTICO DO PRINCÍPIO DA TOTAL INDEPENDÊNCIA DAS AUTORIDADES DE CONTROLO

I. As autoridades de controlo são as entidades administrativas independentes dos Estados-Membros encarregues da supervisão e controlo do cumprimento da legislação de protecção de dados²⁴.

O controlo do cumprimento da legislação de protecção de dados por parte de entidades independentes constitui uma imposição do n.º 3 do artigo 8.º da CDFUE. Assim, no plano do direito derivado, decorria da leitura conjugada do considerando 62 com o artigo 28.º, n.º 1, da Directiva – e decorre, actualmente, da leitura conjugada do considerando n.º 117 com o artigo 52.º, n.º 1, do RGPD – que um dos elementos essenciais da materialização dos direitos de protecção de dados das pessoas singulares é a criação, por parte dos Estados-Membros, de autoridades de controlo dotadas de *total independência*.

No célebre acórdão *Schrems I*²⁵, o TJ declarou a invalidade da Decisão 2000/520/CE (Decisão *Safe Harbor*), relativa à transferência internacional de dados para os EUA, porque, *inter alia*, a Comissão não indicou, conforme exigia a Directiva 95/46/CE, expressa e fundamentadamente, que os EUA (o Estado terceiro visado pela Decisão *Safe Harbor*, para o qual os dados pessoais dos cidadãos da União poderiam ser transferidos) asseguravam um nível de protecção dos direitos fundamentais equivalente ao que vigora na União²⁶, e porque esta Decisão limitava os poderes das

²⁴ Cfr., numa formulação ligeiramente distinta, o artigo 51.º, n.º 1, do RGPD.

²⁵ Acórdão de 6 de Outubro de 2015, *Schrems I*, C-362/14, ECLI:EU:C:2015:650. Acrescentámos um “I” à designação do acórdão, porque este é o primeiro de três casos que são reenviados ao TJ em que o Sr. Maximillian Schrems é parte no processo principal. O segundo acórdão (de 15 de Janeiro de 2018, *Schrems II*, C-498/16, ECLI:EU:C:2018:37) reporta-se à interpretação de uma disposição do Regulamento Bruxelas I. O terceiro caso (C-311/18), por seu turno, encontra-se, à data da redacção deste texto, pendente e reporta-se a um conjunto de importantes questões concernentes à Decisão da Comissão relativa às cláusulas contratuais-tipo aplicáveis à transferência de dados pessoais para subcontratantes estabelecidos em países terceiros. O AG SAUGMANDSGAARD ØE já teve oportunidade de se pronunciar, em 19.12.2019, no sentido de propor ao TJ a resposta à questão prejudicial no sentido de confirmar a validade da Decisão.

²⁶ Sobre o debate em torno daquele que é um dos acórdãos *landmark* do TJ em matéria de protecção de dados, veja-se, entre outros, T. OJANEN, “Making the Essence of Fundamental Rights Real: The Court of Justice of the European Union Clarifies the Structure of Fundamental Rights under the Charter ECJ 6 October 2015, Case C-362/14, *Maximillian Schrems v Data Protection Commissioner*”, *European Constitutional Law Review*, n.º 12, 2016; N. COHEN, “The Privacy Follies: A Look Back at the CJEU’s

autoridades nacionais de controlo conferidos pela Directiva²⁷. De acordo com o Tribunal, é a garantia de independência das autoridades de controlo que assegura um controlo da legislação de protecção de dados de forma eficaz e a fiável²⁸, tendo as autoridades de controlo, sem prejuízo de Decisões adoptadas pela Comissão, poderes²⁹ para examinar, com *total independência*, as transferências de dados para países terceiros³⁰.

II. A exigência da *total independência* das autoridades de controlo suscitou dúvidas em acórdãos pretéritos. Sobre a mesma, de resto, a Directiva apenas a consagrava, não estabelecendo nenhum elenco típico que concorresse para a densificação da referida exigência. Tal situação gerou alguma litigância entre certos Estados-Membros e a Comissão Europeia, que discordou, nesta matéria, de determinadas soluções vertidas na legislação daqueles e instaurou, por conseguinte, os competentes procedimentos por incumprimento.

Algumas das soluções que hoje constam dos artigos 52.º e 53.º do RGPD – acto legislativo que, na perspectiva da doutrina, apresenta o modelo de independência das autoridades de controlo mais avançado da UE³¹ – encontram arrimo na jurisprudência do TJ que analisou as sobreditas acções instauradas pela Comissão.

III. No acórdão *Comissão/Alemanha*³², a Comissão considerou que a Alemanha transpôs erroneamente o artigo 28.º, n.º 1, da Directiva, ao prever que as autoridades de controlo dos *Länder* responsáveis pelo

Invalidation of the EU/US Safe Harbor Framework”, *European Data Protection Law Review*, Vol. 1, n.º 3, 2015; P. E. FISCHER, “Getting Privacy to a new Safe Harbour Comment on the CJEU Judgment of 6 October 2015, Schrems v Data Protection Commissioner”, *Journal of Intellectual Property, Information Technology and Electronic Commerce Law*, Vol. 6, n.º 3, 2015; M. L. FLÓREZ ROJAS, “Legal implications after Schrems case: are we trading fundamental rights?”, *Information & Communications Technology Law*, Vol. 25, n.º 3, 2016; Numa crítica contundente à posição do TJ, invocando os ataques terroristas ocorridos em Paris, *vd.* R. A. EPSTEIN, “The ECJ’s Fatal Imbalance: Its cavalier treatment of national security issues poses serious risk to public safety and sound commercial practices”, *European Constitutional Law Review*, n.º 12, 2016. Em resposta à perspectiva do Autor, no mesmo volume da revista, veja-se M. SCHEININ, “Towards evidence-based discussion on surveillance: A Rejoinder to Richard A. Epstein”. Pela caneta do próprio MAX SCHREMS, veja-se a respectiva posição quanto ao *Privacy Shield*, no rescaldo da invalidade da Decisão *Safe Harbor*, M. SCHREMS, “The Privacy Shield is a Soft Update of the Safe Harbor”, *European Data Protection Law Review*, Vol. 2, n.º 2, 2016. Sobre o *Privacy Shield*, com mais detalhe, *cfr.* C. KUNER, “Reality and Illusion in EU Data Transfer Regulation Post Schrems” *German Law Journal*, Vol. 18, n.º 4, 2017.

²⁷ *Cfr.* *Schrems I*, n.º 103.

²⁸ *Cfr.* *Schrems I*, n.º 41.

²⁹ Sobre os poderes das autoridades de controlo, *vd.* o acórdão de 1 de Outubro de 2015, *Weltimmo*, C-230/14, ECLI:EU:C:2015:639, em particular os n.ºs 42-60.

³⁰ *Cfr.* *Schrems I*, n.º 57.

³¹ *Cfr.* M. SZYDŁO, “The independence of data protection authorities in EU law: between the safeguarding of fundamental rights and ensuring the integrity of the internal market”, *European Law Review*, Vol. 42, n.º 3, 2017, p. 374.

³² Acórdão de 9 de Março de 2010, *Comissão/Alemanha*, C-518/07, ECLI:EU:C:2010:125.

controlo dos tratamentos de dados pessoais efectuados por entidades de natureza privada estavam submetidas à tutela do Estado. A tarefa do Tribunal foi, pois, a de determinar o alcance da expressão “total independência”. Para o TJ, o adjectivo “total” implica um «poder decisório isento de qualquer influência, directa ou indirecta, externa à autoridade de controlo»³³ «e não apenas []a influência dos organismos controlados»³⁴. Ademais, o Tribunal também esclareceu que o mero risco de as autoridades de controlo poderem estar a sofrer aquelas influências na sua actuação é suficiente para não estar verificado o requisito de as mesmas serem dotadas de *total independência*³⁵. O TJ postulou, assim, uma interpretação ampla da referida exigência³⁶, dando provimento à posição da Comissão. Por fim, frisou, também que a mesma exigência não coloca em causa o princípio democrático³⁷, apresentando exemplos de possíveis formas de os Estados-Membros exercerem influência parlamentar sobre as autoridades de controlo, designadamente mediante a nomeação dos membros da respectiva Direcção ou mediante o convite à apresentação de relatórios junto do Parlamento³⁸.

O acórdão analisado estabeleceu o precedente sobre a forma como deve ser interpretada a exigência de *total independência*, tendo o mesmo, hoje, reflexo na redacção dos seis números do artigo 52.º do RGPD, com particular destaque para os n.os 1 e 2.

IV. Os princípios estabelecidos no acórdão analisado foram, subsequentemente, retomados em *Comissão/Áustria*³⁹. Neste caso, o TJ deu, também, provimento à posição da Comissão, declarando que o facto de a autoridade de controlo austríaca ser composta por funcionários integrados na Chancelaria Federal, tendo esta poder hierárquico sobre aqueles, e de os mesmos exercerem actividades paralelas às de membros da autoridade de controlo constitui uma influência indirecta incompatível com a exigência de *total independência* e com os critérios consagrados em *Comissão/Alemanha*⁴⁰.

Ora, é possível ver estes corolários da jurisprudência *Comissão/Áustria* claramente transpostos no n.º 3 e no n.º 5 do artigo 52.º do RGPD.

V. Em *Comissão/Hungria*⁴¹, estava em causa o facto de a Hungria ter feito cessar antecipadamente o mandato do presidente da autoridade de controlo. O Tribunal, retomando o argumento, gizado em

³³ *Comissão/Alemanha*, n.º 19.

³⁴ *Comissão/Alemanha*, n.º 25, *in fine*.

³⁵ Cfr. *Comissão/Alemanha*, n.º 36.

³⁶ Cfr. *Comissão/Alemanha*, n.º 51.

³⁷ Cfr. *Comissão/Alemanha*, n.º 46.

³⁸ Cfr. *Comissão/Alemanha*, n.os 44-45.

³⁹ Acórdão de 16 de Outubro de 2012, *Comissão/Áustria*, C-614/10, ECLI:EU:C:2012:631. Para um comentário a este aresto, cfr. M. SZYDŁO, “Principles underlying independence of national data protection authorities: Commission v. Austria”, *Common Market Law Review*, Vol. 50, n.º 6, 2013.

⁴⁰ Cfr. *Comissão/Áustria*, n.os 59 e 65.

⁴¹ Acórdão de 8 de Abril de 2014, *Comissão/Hungria*, C-288/12, ECLI:EU:C:2014:237.

Comissão/Alemanha, do risco de as autoridades de controlo poderem sofrer influências, considerou que, com tal actuação, poderia pairar uma ameaça de cessação antecipada do mandato o que, por conseguinte, «pode levar a uma forma de obediência desta [autoridade de controlo] ao poder político, incompatível com a referida exigência de independência»⁴². E acrescentou, ainda, que a exigência de *total independência* contempla uma obrigação de manutenção do mandato até ao termo⁴³, sem prejuízo das garantias da lei.

Ainda que constitua uma referência indirecta, o n.º 2 do artigo 52.º do RGPD também espelha o espírito de *Comissão/Hungria*. A disposição legal que, no entanto, configura uma transposição integral do corolário deste acórdão são os n.os 3 e 4 do artigo 53.º do RGPD: os membros das autoridades de controlo cessam funções no fim do mandato e os mesmos só podem ser afastados em caso de falta considerada grave ou não cumprimento das condições exigidas para a função⁴⁴.

VI. O princípio da total independência das autoridades de controlo constitui, como se pode constatar, um caso paradigmático da densificação de princípios operada pelo Tribunal. Destarte, o alcance do conceito de “total independência” foi esclarecido pelo TJ, encontrando, hoje, arrimo em várias disposições normativas do RGPD, num esforço legislativo mais apurado quando comparado com o teor normativo das disposições análogas vertidas na Directiva 95/46/CE.

4. A DENSIFICAÇÃO DE CONCEITOS OPERATIVOS DA PROTECÇÃO DE DADOS: O CASO PARADIGMÁTICO DOS CONCEITOS DE “DADOS PESSOAIS” E DE “RESPONSÁVEL PELO TRATAMENTO”

I. Para além de ser chamado a preencher o conteúdo programático de princípios, como o princípio da total independência das autoridades de

⁴² *Comissão/Hungria*, n.º 54.

⁴³ Cfr. *Comissão/Hungria*, n.º 55.

⁴⁴ A título ilustrativo, parece-nos que pronúncias de desaplicação de normas legais de Direito nacional como as que a autoridade de controlo portuguesa (“CNPD”) tem proferido (cfr. Deliberação da CNPD n.º 1008/2017 e Deliberação da CNPD n.º 2019/494), escoradas na jurisprudência *Costanzo* (acórdão de 22 de Junho de 1989, *Costanzo*, C-103/88, ECLI:EU:C:1989:256), só são, pragmaticamente, e do ponto de vista prático, possíveis por força das garantias robustas oferecidas pelo princípio da total independência. Neste particular, assume assaz importância a forma como devem ser entendidas as relações entre direito nacional e direito europeu, num contexto de interconstitucionalidade e pluralismo constitucional, para garantir a efectividade, quer do referido princípio, quer das referidas pronúncias. Cfr. a este respeito N. WALKER, “The Idea of Constitutional Pluralism”, *Modern Law Review*, Vol. 65, n.º 3, 2002, p. 337; M. POIARES MADURO, “Contrapunctual Law: Europe’s Constitutional Pluralism in Action” in N. WALKER (ed.), *Sovereignty in Transition*, Hart Publishing, Oxford, 2003, p. 501-537; D. BURCHARDT, “The relationship between the law of the European Union and the law of its Member States – a norm-based conceptual framework”, *European Constitutional Law Review*, Vol. 15, n.º 1, 2019, p. 84-85; J. J. GOMES CANOTILHO, *Direito Constitucional e Teoria da Constituição*, 7.ª ed., Almedina, Coimbra, 2003, p. 824. Na jurisprudência do TJUE, cfr. o acórdão de 17 de Dezembro de 1970, *Internationale Handelsgesellschaft*, 11/70, ECLI:EU:C:1970:114.

controlo, já analisado, o TJ tem sido também chamado a pronunciar-se amiudadamente sobre o alcance de determinados conceitos operativos-chave que se encontram definidos na legislação ordinária do direito da protecção de dados. Os dois casos paradigmáticos que trazemos à colação são o conceito de “dados pessoais” e o conceito de “responsável pelo tratamento”. Estes conceitos são paradigmáticos, porque *i)* marcam indelevelmente a abordagem conceptual do Tribunal; *ii)* no caso do conceito de “dados pessoais”, este perpassa toda a jurisprudência prolatada pelo TJ em matéria de protecção de dados; e *iii)* no caso do conceito de “responsável pelo tratamento”, o mesmo protagoniza uma linha jurisprudencial estável do próprio Tribunal, como teremos oportunidade de explicitar.

Outros indícios também permitem chegar a semelhantes conclusões. Repare-se que o *soft law* do GT29⁴⁵ mais vezes citado pelos AG, por referência a Janeiro de 2020, é o «Parecer 4/2007 sobre o conceito de dados pessoais» (01248/07/PT, WP136), referenciado em cinco Conclusões⁴⁶, seguido do «Parecer 1/2010 sobre os conceitos de “responsável pelo tratamento” e “subcontratante”» (00264/10/PT, WP169), referenciado em quatro Conclusões⁴⁷. Ademais, o Parecer 1/2010 é o único instrumento de *soft law* do GT29 referenciado pelo TJ na respectiva jurisprudência⁴⁸, concretamente no acórdão *Jehovan todistajat*⁴⁹.

⁴⁵ Entendemos por *soft law*, no contexto do direito da União Europeia, a definição clássica oferecida por FRANCIS SNYDER, segundo a qual trata-se de «regras de conduta que, em princípio, não possuem força jurídica vinculativa, mas que, no entanto, produzem efeitos práticos» (F. SNYDER, “The Effectiveness of European Community Law: Institutions, Processes, Tools and Techniques”, *Modern Law Review*, n.º 56, 1993, pp. 19-56, tradução nossa. Sobre o tema, cfr. também L. SENDEN, *Soft Law in European Community Law*, Hart Publishing, Oxford, 2004, p. 112 e ss.; e, com um relevante enquadramento quantitativo do *soft law* emitido nos sectores da concorrência e dos auxílios de Estado, cfr. O. STEFAN, *Soft Law in Court. Competition Law, State Aid and the Court of Justice of the European Union*, Kluwer Law International, The Netherlands, 2012, p. 120 e ss.). No caso do *soft law* do GT29, falamos de “pareceres” (*opinions*), directrizes (*guidelines*), documentos de trabalho (*working documents*), linhas gerais e outras designações para documentos emitidos pelo GT29, que era um ente consultivo, instituído pela Directiva 95/46/CE, e constituído por representantes das autoridades de controlo. Actualmente, o GT29 foi substituído pelo CEPD, uma entidade instituída pelo RGPD, que encontra a sua génese no GT29, conservando a sua atribuição consultiva, mas que é simultaneamente dotada de muitas mais atribuições (e.g., mecanismo de controlo de coerência).

⁴⁶ Conclusões proferidas nos processos *Scarlet Extended*; *Google Spain e Google*; *Breyer, YS*; *Fashion ID*.

⁴⁷ Conclusões proferidas nos processos *Google Spain e Google*; *Wirtschaftsakademie Schleswig-Holstein*; *Jehovan todistajat*; e *Fashion ID*. O *soft law* que se segue, no que concerne à frequência de citação, é o «Parecer 8/2010 sobre a lei aplicável» (0836-02/10/PT, WP 179) e o «Parecer 6/2014 sobre o conceito de interesses legítimos do responsável pelo tratamento» (844/14/PT, WP 217), ambos referenciados respectivamente em três Conclusões (Conclusões de *Google Spain e Google*; *Weltimmo*; *Wirtschaftsakademie Schleswig-Holstein*; por um lado, e Conclusões de *Bara*; *Rigas*; e *Fashion ID*, por outro lado).

⁴⁸ Deve, no entanto, ter-se presente que, diversamente do que sucede com as conclusões dos AG e do que sucede na prática judiciária de outros órgãos jurisdicionais

Posto isto, vejamos como o TJ densificou os conceitos em escrutínio.

II. “Dados pessoais” é um conceito jurídico-normativo ínsito, primeiramente, no artigo 2.º, al. a), da Directiva 95/46/CE e, mais tarde, no artigo 4.º, 1), do RGPD. A definição consagrada pelo RGPD, globalmente considerada, altera tenuemente a definição da Directiva 95/46/CE. Ora, transcrevendo parcialmente a definição do RGPD, “dado pessoal” é a «informação relativa a uma pessoa singular identificada ou identificável (“titular dos dados”)». Em síntese, um “dado” para ser considerado “pessoal” *i)* tem de se reportar a uma pessoa singular; e *ii)* tem de a identificar ou permitir identificá-la. Exemplos de dados que não são considerados dados pessoais, nos termos de *i)*, seriam os dados referentes estritamente a uma pessoa colectiva, e, nos termos de *ii)*, os dados anonimizados.

No plano do direito aplicado, o TJ tem considerado que se subsumem à definição de “dado pessoal”, designadamente, e entre muitas outras, as seguinte situações fácticas (vejamos dez exemplos impressivos): *i)* as respostas escritas dadas por um candidato num exame profissional e as eventuais anotações do examinador relativas a essas respostas⁵⁰; *ii)* dados biométricos (impressões digitais)⁵¹; *iii)* certos *cookies*⁵²; *iv)* dados como o número de identificação, apelido, nome próprio, data e local de nascimento, estado civil, sexo, endereço, historial das entradas e saídas de um dado território nacional, estatuto de residente, identificação de pessoas pelo nome, número de telefone, condições de trabalho, passatempos, etc⁵³; *v)* o endereço IP dinâmico (provisório), quando o responsável pelo tratamento dispuser de meios legais que lhe permitam obter dados suplementares sobre o titular dos dados junto do respectivo ISP⁵⁴; *vi)* dados fiscais⁵⁵; *vii)* dados referentes a pessoas que actuam

de outras ordens jurídicas, não é habitual os acórdãos do TJUE apresentarem referências que não correspondam estritamente a acórdãos prolatados no passado por esta instituição (ou, em certos casos especiais, referências a acórdãos do TEDH). Não contabilizámos a referência ao GT29 constante no acórdão de 30 de Maio de 2006, *Parlamento/Conselho*, processos apensos C-317/04 e C-318/04, ECLI:EU:C:2006:346, por não constituir uma base de fundamentação de argumentos do Tribunal, mas um elemento de facto (cfr. n.º 35 do acórdão).

⁴⁹ Acórdão de 10 de Julho de 2018, *Jehovan todistajat*, C-25/17, ECLI:EU:C:2018:551.

⁵⁰ Matéria de facto do acórdão *Nowak*, já referenciado.

⁵¹ Matéria de facto do acórdão de 17 de Outubro de 2013, *Schwarz*, C-291/12, ECLI:EU:C:2013:670; acórdão de 16 de Abril de 2015, *Willems e o*, processos apensos C-446/12 a C-449/12, ECLI:EU:C:2015:238.

⁵² Matéria de facto do acórdão de 01 de Outubro de 2019, *Planet49*, C-673/17, ECLI:EU:C:2019:801.

⁵³ Matéria de facto do acórdão de 4 de Maio de 2017, *Rīgas*, C-13/16, ECLI:EU:C:2017:336; acórdão *Rijkeboer*, já referenciado; acórdão de 16 de Dezembro de 2008, *Huber*, C-524/06, ECLI:EU:C:2008:724; acórdão de 6 de Novembro de 2003, *Lindqvist*, C-101/01, ECLI:EU:C:2003:596.

⁵⁴ Matéria de facto do acórdão de 19 de Outubro de 2016, *Breyer*, C-582/14, ECLI:EU:C:2016:779. Para o aresto pioneiro na consagração do endereço IP como dado pessoal, veja-se o acórdão de 14 de Novembro de 2011, *Scarlet Extended*, C-70/10, ECLI:EU:C:2011:771.

como agentes imobiliários⁵⁶; *viii*) os dados necessários para encontrar e identificar a fonte, o destino, a data, a hora e a duração de uma comunicação, o equipamento de comunicação móvel dos utilizadores e a respectiva localização⁵⁷; *ix*) a imagem de uma pessoa gravada através de uma câmara montada para uso doméstico, mas que vigia igualmente o espaço público⁵⁸; *x*) registo dos tempos de trabalho (horas de início e de termo do tempo de trabalho e interrupções ou intervalos) de trabalhadores⁵⁹.

Como se pode inferir, actualmente é um facto consumado o de que o conceito de "dados pessoais", conforme esboçado pela jurisprudência do TJ, é um conceito amplo⁶⁰.

III. Também o conceito de "responsável pelo tratamento", conforme construído pelo Tribunal, é um conceito amplo. Tal construção encontra a sua *raison d'être* no facto de só um conceito amplamente definido poder garantir uma maior protecção – *rectius*, uma protecção "eficaz" e "completa" – dos titulares dos dados⁶¹. A título ilustrativo, em *Wirtschaftsakademie Schleswig-Holstein*, o TJUE declarou que o administrador de uma página de fãs criada no Facebook é, tal como o Facebook, (conjuntamente) responsável pelo tratamento dos dados dos utilizadores que acedem à página⁶².

Uma das operações de qualificação jurídica mais complexas do direito da protecção de dados é, pois, a de determinar a posição que cada parte ocupa na relação jurídica. O RGPD determina que o "responsável pelo tratamento" é a pessoa singular ou colectiva (pública ou privada) que determina, isolada ou conjuntamente, as finalidades (o "porquê") e os meios (o "como") do tratamento. Por seu turno, o subcontratante é a pessoa singular ou colectiva (pública ou privada) que trata dados pessoais por conta do responsável pelo tratamento, ou seja, o subcontratante não influencia as finalidades do tratamento, podendo, contudo, definir alguns

⁵⁵ Matéria de facto do acórdão de 1 de Outubro de 2015, *Bara*, C-201/14, ECLI:EU:C:2015:638.

⁵⁶ Matéria de facto do acórdão de 7 de Novembro de 2013, *IPI*, C-473/12, ECLI:EU:C:2013:715.

⁵⁷ Matéria de facto do acórdão de 8 de Abril de 2014, *Digital Rights Ireland*, processos apensos C-293/12 e C-594/12, ECLI:EU:C:2014:238; do acórdão de 21 de Dezembro de 2016, *Tele2 Sverige*, processos apensos C-203/15 e C-698/15, ECLI:EU:C:2016:970.

⁵⁸ Matéria de facto do acórdão de 11 de Dezembro de 2014, *Ryneš*, C-212/13, ECLI:EU:C:2014:2428.

⁵⁹ Matéria de facto do acórdão de 30 de Maio de 2013, *Worten*, C-342/12, ECLI:EU:C:2013:355.

⁶⁰ Alertando para as limitações que, no futuro, uma definição tão ampla implicará, veja-se N. PURTOVA, "The law of everything. Broad concept of personal data and future of EU data protection law", *Law, Innovation and Technology*, Vol. 10, n.º 1, 2018.

⁶¹ Cfr. acórdão de 13 de Maio de 2014, *Google Spain e Google*, C-131/ ECLI:EU:C:2014:317, n.º 34; acórdão de 5 de Junho de 2018, *Wirtschaftsakademie Schleswig-Holstein*, C-210/16, ECLI:EU:C:2018:388, n.º 28; *Jehovan todistajat*, n.º 66.

⁶² Cfr. *Wirtschaftsakademie Schleswig-Holstein*, n.º 39.

dos meios do mesmo⁶³. Determinar a posição jurídica das partes envolvidas num concreto tratamento permite, desde logo, espartilhar as respectivas obrigações legais e contratuais a cumprir.

Quando a responsabilidade pelo tratamento é conjunta⁶⁴, de acordo com a jurisprudência do Tribunal, nem sequer é exigido que cada responsável tenha acesso aos dados pessoais⁶⁵. Consequentemente, da responsabilidade pelo tratamento conjunta não decorre que o grau de responsabilização seja idêntico, podendo cada responsável estar envolvido em diferentes fases e diferentes graus de tratamento⁶⁶. O acesso aos dados, todavia, pode ser relevante para a determinação do grau de responsabilidades entre os responsáveis⁶⁷. Neste sentido, em *Jehovan todistajat*, o TJUE considerou que a Comunidade das Testemunhas de Jeová é conjuntamente responsável pelo tratamento dos dados com os pregadores porta-a-porta⁶⁸. O TJUE cita o Parecer 1/2010 do GT29, já referenciado, segundo o qual «importa ter em conta, designadamente, o poder de controlo efetivo e a perceção que as pessoas cujos dados são objeto de tratamento têm do responsável pelo tratamento»⁶⁹. Neste acórdão, é ainda relevante notar que o TJUE extravasa a definição legal e torna o conceito de responsável pelo tratamento ainda mais amplo, ao acrescentar que o responsável pelo tratamento pode ser uma pessoa que «influencia» o tratamento «para fins que lhe são próprios», contribuindo, deste modo, para a «determinação da finalidade»⁷⁰. No entanto, e de forma mais restrita, explicita o acórdão *FashionID* que «uma pessoa singular ou coletiva apenas parece poder ser responsável (...) conjuntamente com outras, pelas operações de tratamento de dados pessoais cujas finalidades e meios sejam conjuntamente determinados por essa pessoa»⁷¹.

Atendendo à dificuldade prática de qualificação das partes na relação jurídico-material, em matéria de direito da protecção de dados, esta é uma linha jurisprudencial de assaz importância, aportando subsídios interpretativos fundamentais.

IV. Conforme se pode constatar, também na interpretação e densificação de conceitos operativos da protecção de dados a intervenção do TJUE tem sido decisiva. A amplitude com que o Tribunal gizou os conceitos de

⁶³ Cfr. GT29, «Parecer 1/2010 sobre os conceitos de “responsável pelo tratamento” e “subcontratante”», *cit.*, p. 17.

⁶⁴ Cfr. artigo 26.º do RGPD.

⁶⁵ Cfr. *Wirtschaftsakademie Schleswig-Holstein*, n.º 38.

⁶⁶ Cfr. *Wirtschaftsakademie Schleswig-Holstein*, n.º 43.

⁶⁷ Cfr., neste sentido, AEPD, “EDPS Guidelines on the concepts of controller, processor and joint controllership under Regulation (EU) 2018/1725”, 07.11.2019, p. 24. Não obstante as *guidelines* da EDPS se destinarem à interpretação do Regulamento (UE) 2018/1725, é inequívoca a harmonização conceptual deste Regulamento com o RGPD.

⁶⁸ Cfr. *Jehovan todistajat*, n.º 73.

⁶⁹ *Jehovan todistajat*, n.º 21.

⁷⁰ *Jehovan todistajat*, n.º 68.

⁷¹ Cfr. Acórdão de 29 de Julho de 2019, *Fashion ID*, C-40/17, ECLI:EU:C:2019:629, n.º 74.

“dados pessoais” e de “responsável pelo tratamento”, dotados dos matizes acima descritos, é paradigmática de uma protecção reforçada do direito fundamental, comportando evidentes consequências conceptuais, que se materializam, na prática, não só nos próprios conceitos, mas também, indirectamente, em conceitos de fronteira.

5. AS COLISÕES DE DIREITOS (I): O “JUSTO EQUILÍBRIO” ENTRE O DIREITO À PROTECÇÃO DOS DADOS PESSOAIS E O DIREITO À LIBERDADE DE EXPRESSÃO

I. As relações de tensão entre o direito à protecção de dados e outros direitos fundamentais são um dos temas jurisprudenciais mais relevantes da prática do TJ. O Tribunal tem vindo a advertir para o facto de que «o direito à protecção dos dados pessoais não é uma prerrogativa absoluta, mas deve ser tomado em consideração relativamente à sua função na sociedade»⁷² e a jurisprudência que trata de situações nas quais estão em causa colisões entre o direito à protecção dos dados pessoais e o direito à liberdade de expressão⁷³, ainda que não referencie a asserção transcrita, na nossa perspectiva, parte precisamente dessa premissa para, subsequentemente, pôr à prova a aplicação do critério do “justo equilíbrio” entre os direitos em ponderação. Vejamos, então, alguns acórdãos paradigmáticos.

II. *Lindqvist* envolvia um tratamento de dados pessoais que implicava, nomeadamente, a identificação de pessoas pelo nome e outros dados pessoais numa página na internet, sem precedência de pedidos de consentimento⁷⁴. Colocava-se, *inter alia*, a questão de saber se a Directiva 95/46/CE introduzia restrições incompatíveis com o direito à liberdade de expressão consagrado na ordem jurídica da (à época) Comunidade⁷⁵. O TJ pronunciou-se no sentido de que a Directiva, em si mesma, não impunha restrições incompatíveis com esse direito, sendo que eventuais compressões do mesmo teriam de ser aferidas mediante a ponderação de um “justo equilíbrio” entre os direitos e interesses em contenda⁷⁶. O princípio-chave para a aferição do justo equilíbrio, na perspectiva do Tribunal, era, pois, o princípio da proporcionalidade, porquanto a sua aplicação deveria evitar incompatibilidades entre ambos os direitos⁷⁷.

⁷² Conclusões do AG YVES BOT, no acórdão C-398/15, *Manni*, apresentadas em 08.09.2016, n.º 47; acórdãos *Schwarz*, n.º 33, e *Volker und Markus Schecke*, n.º 48.

⁷³ Considerando que o direito europeu da protecção de dados assenta numa profunda relação de tensão com o direito à liberdade de expressão, veja-se o estudo aprofundado de D. ERDOS, “From the Scylla of Restriction to the Charybdis of Licence? Exploring the Scope of the ‘Special Purposes’ Freedom of Expression Shield in European Data Protection”, *Common Market Law Review*, Vol. 52, n.º 1, 2015.

⁷⁴ Cfr. *Lindqvist*, n.º 14.

⁷⁵ Cfr. *Lindqvist*, n.º 85.

⁷⁶ Cfr. *Lindqvist*, n.º 90.

⁷⁷ Cfr. *Lindqvist*, n.os 86-88.

III. Também *Satamedia*⁷⁸ constitui um acórdão paradigmático relativamente à confrontação dos princípios do direito da protecção de dados com os princípios enformadores do direito à liberdade de expressão dos meios de comunicação social e conseqüente direito à informação dos leitores. No caso, um jornal finlandês procedia à recolha junto da autoridade tributária finlandesa de dados públicos de contribuintes com rendimentos superiores a um dado montante, publicando posteriormente uma lista ordenada com os nomes, as respectivas categorias de rendimentos e a classificação por município. A esta factualidade acrescia a cedência dessa lista à *Satamedia*, sociedade detida pelos mesmos accionistas do jornal, que oferecia um serviço pago de SMS com a referida lista. Ora, o TJ foi chamado a pronunciar-se sobre a questão de saber se a respectiva factualidade se inseria no âmbito de um tratamento de dados para fins jornalísticos⁷⁹, tendo considerado que um tratamento de dados daquela natureza terá fins exclusivamente jornalísticos «se tiver[] por única finalidade a divulgação ao público de informações, de opiniões ou de ideias»⁸⁰.

IV. O tema da derrogação para fins jornalísticos e os corolários da jurisprudência precedente foram retomados em *Buivids*⁸¹. Este acórdão é também relevante pelas referências e pelo diálogo que estabelece com os critérios firmados na jurisprudência do TEDH, nomeadamente no acórdão *Satamedia c. República da Finlândia*, já referenciado neste texto.

No caso em apreço, o Sr. *Buivids*, encontrando-se numa esquadra policial a prestar declarações relativas a um processo contra-ordenacional que lhe fora instaurado, filmou o respectivo depoimento, bem como os agentes da polícia. Posteriormente, publicou o referido vídeo no sobejamente conhecido *website* youtube.com. Estava, por isso, em causa, neste acórdão, a questão de saber que direitos deveriam prevalecer, nomeadamente se deveria prevalecer o direito à liberdade de expressão

⁷⁸ Acórdão de 16 de Dezembro de 2008, *Satamedia*, C-73/07, ECLI:EU:C:2008:727.

⁷⁹ Considerando *Satamedia* uma “pronúncia enigmática” do TJ, veja-se P. OLIVER, “The Protection of Privacy in the Economic Sphere Before the European Court of Justice”, *Common Market Law Review*, Vol. 46, n.º 5, 2009, p. 1459-1463.

⁸⁰ *Satamedia*, n.º 62. Ao nível interno, este processo culminou numa queixa junto do Tribunal Europeu dos Direitos Humanos (queixa n.º 931/13 – acórdão *Satakunnan Markkinapörssi Oy and Satamedia Oy c. República da Finlândia*). A tarefa do TEDH foi, *inter alia*, a de analisar se, no caso, se estava em presença de uma violação do artigo 10.º da CEDH. Para um comentário ao acórdão do TEDH, cfr. M. JOZWIAK, “The Scale Matters: The EctHR Grand Chamber Finds That Prohibition of Mass Publication of Raw Taxation Data Does Not Infringe Right to Freedom of Expression”, *European Data Protection Law Review*, Vol. 4, n.º 1, 2018.

⁸¹ Acórdão de 14 de Fevereiro de 2019, *Buivids*, C-345/17, ECLI:EU:C:2019:122. Para uma pertinente análise a este acórdão, numa perspectiva de articulação com o RGPD, cfr. D. ERDOS, “European Data Protection and Freedom of Expression after *Buivids*: An Increasingly Significant Tension”, in *European Law Blog*, 21.02.2019, disponível em <https://europeanlawblog.eu/2019/02/21/european-data-protection-and-freedom-of-expression-after-buivids-an-increasingly-significant-tension/> [consultado em 05.01.2020].

do Sr. Buivids ou o direito à protecção de dados das pessoas que surgiam na gravação de vídeo.

O TJ, considerando a Directiva 95/46/CE aplicável a uma situação fáctica como a descrita⁸², declarou, todavia, que, naquele caso concreto, se aplicava a derrogação da Directiva relativa a tratamentos de dados realizados para fins jornalísticos⁸³. O Tribunal chegou a esta conclusão por força da noção ampla de “jornalismo” que adoptara em *Satamedia*⁸⁴. Desta noção ampla decorre que uma pessoa (como o Sr. Buivids) não necessita de exercer a profissão de jornalista para poder praticar tratamentos de dados pessoais (como a publicação do referido vídeo em youtube.com) que se insiram na derrogação para fins jornalísticos prevista na Directiva⁸⁵. Ademais, o TJ teve, também, em conta a evolução dos meios de comunicação e informação⁸⁶.

Há, no entanto, uma conclusão fundamental do TJ, no que concerne à aplicação da derrogação para fins jornalísticos: trata-se do precedente estabelecido em *Satamedia*, ou seja, a publicação do vídeo terá de ter «por única finalidade a divulgação ao público de informações, opiniões ou ideias»⁸⁷.

V. O acórdão, porventura, mais controverso do ponto de vista da prevalência do direito à liberdade de expressão será *Google Spain e Google*, que constitui a famigerada jurisprudência relativa ao «direito a ser esquecido»⁸⁸. Entre outras coisas, estava em causa a ponderação entre, por um lado, a gravidade da ingerência na vida privada de um cidadão e, por outro lado, os interesses dos internautas no acesso a informação. No caso, o TJ analisou, *inter alia* e *grosso modo*, a questão de saber se um operador de motor de pesquisa, em determinadas circunstâncias, para dar cumprimento ao quadro normativo europeu de protecção de dados pessoais, tem de suprimir certos resultados de pesquisa. Com efeito, o Tribunal frisou que uma eventual solicitação de supressão de páginas contendo informações que consubstanciam dados pessoais junto dos editores de websites por parte de um titular dos dados não é passível de lhe assegurar uma protecção eficaz e completa, visto que o tratamento pode ser lícito por parte do *website* e já não o ser por parte do motor de pesquisa, e visto que a pesquisa pelo nome próprio de um cidadão num motor de pesquisa permite, potencialmente, a apresentação de um conjunto de resultados estruturalmente organizados

⁸² Cf. *Buivids*, n.º 47.

⁸³ Cf. *Buivids*, n.º 69.

⁸⁴ Cfr. *Buivids*, n.º 51.

⁸⁵ Cfr. *Buivids*, n.º 55.

⁸⁶ Cfr. *Buivids*, n.º 57.

⁸⁷ *Buivids*, n.os 68 e 69.

⁸⁸ Repare-se que, não sendo, de todo, uma singularidade, não é, todavia, muito comum, na prática judiciária do TJUE, o conteúdo decisório da jurisprudência prolatada ser radicalmente tão distinto das propostas de decisão do(a) correspectivo(a) AG. Foi justamente esta situação que sucedeu em *Google Spain e Google*: a maioria das conclusões de NIILO JÄÄSKINEN não foi acolhida no Acórdão.

de muito mais simples difusão e acesso. O Tribunal estabeleceu, por conseguinte, a obrigação de os operadores de motores de pesquisa, perante determinadas circunstâncias, acederem a solicitações de supressão de concretos resultados de pesquisas indexados⁸⁹.

Diga-se que o impacto de *Google Spain e Google* transcende as fronteiras geográficas da União e as perspectivas futuras dos corolários aí firmados estiveram, recentemente, em análise na mais alta instância judicial da UE. É que *Google Spain e Google* teve uma seqüela⁹⁰, num litígio que opôs a Google à CNIL (autoridade de controlo francesa). A CNIL, contrariamente à posição da Google, considerava que o direito à supressão de uma hiperligação deveria ter aplicação universal⁹¹, a única solução capaz de dotar de efeito útil o pedido de supressão e, por conseguinte, a protecção do direito fundamental à protecção dos dados pessoais do titular que solicitou tal pedido. Qualquer outra solução, seja de cariz “minimalista” ou de cariz “intermédio”⁹², não permitiria acautelar uma elevada protecção deste direito⁹³. O AG MACIEJ SZPUNAR, nas suas Conclusões proferidas em 10 de Janeiro de 2019, considerou, todavia, que o direito à supressão de uma hiperligação deve ser de cariz meramente europeu⁹⁴. O TJ, no

⁸⁹ Por isso, o acórdão em escrutínio consagra uma modalidade do – e não um pleno e integral – direito a ser esquecido, *i.e.*, o direito à supressão de uma hiperligação. Este é, assim, alheio ao apagamento – ou não apagamento – da informação no *website* de origem, porquanto se basta com o facto de as páginas que retornam os resultados de pesquisa controvertidos no motor de pesquisa deixarem de surgir. É neste sentido que é enquadrável numa modalidade de direito a ser esquecido; na medida em que torna o acesso às páginas originais e replicadas por páginas *web* terceiras bastante mais difícil. No entanto, toda esta construção do direito a ser esquecido era inexistente na Directiva, que apenas estabelecia que os titulares tinham direito a obter, *inter alia*, o “apagamento” dos dados pessoais, numa norma que correspondia a uma alínea de um artigo epigrafado de “direito de acesso” (o artigo 12.º, al. b), da Directiva).

⁹⁰ Acórdão de 24 de Setembro de 2019, *Google LCC*, C-507/17, ECLI:EU:C:2019:772.

⁹¹ Cfr. I. FALQUE-PIERROTIN, “Pour un droit au déréférencement mondial”, 12/01/2017, disponível em <https://www.cnil.fr/fr/pour-un-droit-au-dereferencement-mondial> [consultado em 05.01.2020]; CNIL, “Délibération n.º 2016-054 du 10 mars 2016 – Délibération de la formation restreinte n.º 2016-054 du 10 mars 2016 prononçant une sanction pécuniaire à l’encontre de la société X”, pesquisável em <https://www.legifrance.gouv.fr> [consultado em 05.01.2020].

⁹² Na senda da formulação de DÁRIO MOURA VICENTE. Cfr. D. MOURA VICENTE, “Opinião: O direito ao esquecimento na internet”, in *Dinheiro Vivo*, 21/05/2018, disponível em <https://www.dinheirovivo.pt/opiniao/o-direito-ao-esquecimento-na-internet-novo-direito-ou-limite-a-liberdade-de-expressao/> [consultado em 05.01.2020].

⁹³ Neste sentido, cfr. GT29, “Guidelines on the Implementation of the Court of Justice of the European Union Judgment on ‘Google Spain and Inc v. Agencia Española de Protección de Datos (AEDP) and Mario Costeja González’ C-131/12”, WP225, 26.11.2014, p. 3. Estas *guidelines* foram entretanto actualizadas pelo CEPD (versão para consulta pública): EDPB, “Guidelines 5/2019 on the criteria of the Right to be Forgotten in the search engines cases under the GDPR”, 02.12.2019 (version 1.1., “minor corrections”, 17.02.2020), disponível em https://edpb.europa.eu/sites/edpb/files/consultation/edpb_guidelines_201905_rtbsearch_engines_forpublicconsultation.pdf [consultado em 26.06.2020].

⁹⁴ Conclusões de MACIEJ SZPUNAR, proferidas no processo *Google LLC/CNIL*, C-507/17, em 10.01.2019, n.º 2. O próprio AG MACIEJ SZPUNAR (Conclusões de *Google LLC c. CNIL*, n.os 60 e 61) colocou a hipótese, na circunstância de o TJ responder às questões prejudiciais

acórdão prolatado em 24 de Setembro de 2019, concluiu no sentido do AG, *i.e.*, que o direito à supressão de uma hiperligação não tem carácter mundial⁹⁵.

Ora, tratava-se, como se pode inferir, de um problema relacionado com a própria efectividade do direito da União fora do seu território. Problema que adquire dimensões mais complexas quando a respectiva aplicação extraterritorial se vê confrontada com o Direito de Estados terceiros com uma cultura jurídica distinta no que concerne à privacidade e à protecção de dados. A título ilustrativo, o direito a ser esquecido constitui um caso paradigmático de um direito que enfrenta oposição em solo norte-americano⁹⁶, pela sua difícil compatibilização com a Primeira Emenda à *Bill*

no sentido da aplicação mundial do direito à supressão de uma hiperligação, de os Estados terceiros poderem criar leis locais que impedissem as pessoas localizadas na União de aceder a informação. Seria, nas palavras do AG, uma “*race to the bottom*” da liberdade de expressão à escala europeia e mundial.

⁹⁵ O operador de motor de pesquisa não fica obrigado a suprimir os resultados de todas as versões do motor, mas apenas daquelas que correspondam aos Estados-Membros da União. Cfr. *Google LLC*, n.º 73.

⁹⁶ Ao passo que a regulação na União Europeia se efectua mediante instrumentos normativos de carácter geral (o RGPD e, até 25 de Maio de 2018, a Directiva 95/46/CE), os EUA, a nível federal, apenas possuem legislação de carácter sectorial (*v.g.*, entre outros, a *Health Insurance Portability and Accountability Act*, “HIPAA”), sem prejuízo de, desde a implementação do RGPD, alguns Estados norte-americanos terem encetado esforços legislativos no sentido de, nalgumas matérias, aproximar procedimentos (*v.g.* a *California Consumer Privacy Act of 2018*, de 28 de Junho de 2018, que entrou em vigor em 1 de Janeiro de 2020). Em parte, tal poderá encontrar arrimo, de forma genérica, nas diferenças jurídicas e filosófico-sociológicas relativas aos fundamentos constitucionais vigentes nos EUA e nos Estados da Europa (em particular, da Europa continental de tradição romano-germânica): enquanto para o primeiro a *liberdade* é um valor que assume preponderância medular, para os segundos o valor que assume preponderância equivalente é o da *dignidade humana* (cfr. J. Q. WHITMAN, “The Two Western Cultures of Privacy: Dignity versus Liberty”, *Yale Law Journal*, n.º 113, 2004, p. 1115-1221; F. URBANO CALVÃO, *Direito da Protecção de Dados. Relatório sobre o programa, os conteúdos e os métodos de ensino da disciplina*, Universidade Católica Editora, Porto, 2018, p. 39). Consequentemente, a protecção reforçada dos direitos de liberdade nos EUA esbarra com uma construção do direito da protecção de dados conforme consagrada na Europa (continental), por força das colisões que podem emergir, designadamente em matéria de liberdade de expressão. Sobre o direito a ser esquecido e a forte oposição que enfrenta nos EUA, cfr. M. L. RUSTAD / S. KULEVSKA, “Reconceptualizing the Right to be Forgotten to Enable Transatlantic Data Flow”, *Harvard Journal of Law & Technology*, Vol. 28, n.º 2, 2015, p. 349-417. Não se pretende, naturalmente, significar que os EUA deveriam importar as construções dogmáticas do direito europeu da protecção de dados – de resto, tal seria contrário à metodologia de análise do direito comparado –, mas apenas colocar em evidência as dificuldades de harmonização. Curiosamente, “*The Right to Privacy*” (S. D. WARREN / L. D. BRANDEIS, “The Right to Privacy”, *Harvard Law Review*, Vol. 4, n.º 5, 1890, p. 193-220), um artigo histórico que constrói a “*privacy*” a partir do “direito a não ser incomodado” (“*right to be let alone*”), com o objectivo de encontrar expedientes (*torts* e *injunctions*) que a visassem proteger, unanimemente considerado o artigo mais citado e influente nesta matéria nos EUA, é hoje encarado por alguma doutrina norte-americana como estando mais próximo de uma tentativa fracassada de “transplante” do direito europeu continental (cfr. J. Q. WHITMAN, “The Two Western Cultures of Privacy: Dignity versus Liberty”, *cit*, p. 1204).

of Rights, i.e., com a protecção conferida pelo direito constitucional norteamericano à liberdade de expressão⁹⁷.

Sem prejuízo da decisão cautelosa do TJ em *Google LLC*, perante esta situação de dissemelhança de culturas jurídicas em matéria de protecção de dados, será fundamental perceber em que sentido evoluirá a *privacy policy* e *enforcement* nos Estados terceiros, na certeza de que, inelutavelmente, influenciará o direito europeu da protecção de dados.

6. AS COLISÕES DE DIREITOS (II): O “JUSTO EQUILÍBRIO” ENTRE O DIREITO À PROTECÇÃO DOS DADOS PESSOAIS E OS DIREITOS DE PROPRIEDADE INTELECTUAL

I. Os direitos de propriedade intelectual gozam de protecção reforçada, desde o Tratado de Lisboa, no artigo 118.º do TFUE, e também no artigo 17, n.º 2, da CDFUE, tratando-se, desde há muito, de uma matéria regulada pelo direito derivado da União⁹⁸.

O acórdão *Promusicae* foi a jurisprudência que encetou o grupo de arestos do TJ relativo à tensão entre a privacidade e a protecção dos direitos de propriedade intelectual⁹⁹. No caso, a *Promusicae*, uma associação sem fins lucrativos que agrupava produtores e editores de gravações musicais e audiovisuais, pretendia que o ISP (fornecedor de serviços de internet) lhe possibilitasse o acesso a dados pessoais de terceiros, concretamente a identidade e a morada de determinadas pessoas às quais se conhecia o endereço IP e a data e hora de ligação, uma vez que estas eram utilizadoras de um programa P2P (*peer-to-peer*), o que lhes permitia “descarregar” ficheiros de cujos direitos patrimoniais e de exploração pertenciam a associados da *Promusicae*¹⁰⁰. O TJ seguiu uma metodologia trifásica: primeiro, começou por indagar se a Directiva 2002/58/CE (ePrivacy) exclui a obrigação de transmissão de dados dos utilizadores a titulares de direitos de autor, com vista a que estes possam propor acções judiciais contra aqueles; tendo concluído pela negativa, seguidamente, foi

⁹⁷ Cfr. R. G. LARSON III, “Forgetting the First Amendment: How Obscurity-Based Privacy and a Right to be Forgotten are Incompatible with Free Speech”, *Communication Law and Policy*, Vol. 18, n.º 1, 2013, p. 91-120; J. ROSEN, “The Deciders: The Future of Privacy and Free Speech in the Age of Facebook and Google”, *Fordham Law Review*, Vol. 80, n.º 4, 2012, p. 1525-1538. Algumas vozes consideram mesmo que o direito a ser esquecido se trata de uma forma de censura. Para uma sùmula desta linha de pensamento, cfr. S. C. BENNETT, “The ‘Right to Be Forgotten’: Reconciling EU and US Perspectives”, *Berkeley Journal of International Law*, Vol. 30, n.º 1, 2012, p. 161-195.

⁹⁸ Para mais desenvolvimentos, cfr. J. P. REMÉDIO MARQUES, “Artigo 118.º”, in M. LOPES PORTO / G. ANASTÁCIO (Coord.), *Tratado de Lisboa Anotado e Comentado*, Almedina, Coimbra, 2012, p. 549-553; L. COUTO GONÇALVES / M. M. CARVALHO, “Artigo 17.º”, in A. SILVEIRA / M. CANOTILHO (Coord.), *Carta dos Direitos Fundamentais da União Europeia Comentada*, Almedina, Coimbra 2013, p. 226-231; L. COUTO GONÇALVES / C. TRABUCO / M. M. CARVALHO, “Capítulo XI – Propriedade Intelectual”, in A. SILVEIRA / P. M. FROUFE / M. CANOTILHO (Coord.), *Direito da União Europeia – Elementos de Direito e Políticas da União*, Almedina, Coimbra, 2016, p. 663 e ss.; P. SOUSA E SILVA, *Direito Industrial*, 2.ª ed., Almedina, Coimbra, 2019, p. 467 e ss.

⁹⁹ Cfr. P. CRAIG / G. DE BÚRCA, *EU Law Text, Cases, and Materials*, 5.ª ed., Oxford University Press, Oxford, 2011, p. 383.

¹⁰⁰ *Promusicae*, n.os 29 e 30.

indagar se as directivas de propriedade intelectual e do comércio electrónico estipulavam a obrigação de os Estados-Membros preverem essa obrigação de transmissão de dados; concluindo igualmente pela negativa, foi, por fim, verificar se as normas da CDFUE poderiam oferecer uma leitura distinta. A conclusão a que o tribunal chegou foi a de que, analisado todo esse acervo legislativo, o direito da União, por um lado, não obriga e, por outro, não proíbe que os Estados-Membros contemplem a possibilidade de demandar os ISPs para aquele propósito, devendo os mesmos assegurar um “justo equilíbrio” entre os direitos fundamentais em disputa que afaste possíveis colisões¹⁰¹.

Situação com alguns contornos fácticos semelhantes é a do acórdão *Scarlet Extended*, no qual uma associação com funções análogas às da Promusicae demandou o ISP com vista a que fosse declarada a violação de direitos de autor e, subseqüentemente, que este instalasse um sistema de filtragem que tornasse impossível o acesso a esses conteúdos por parte dos clientes utilizadores de programas de P2P, algo que implicava o processamento dos seus endereços IP e um conhecimento dos ficheiros “baixados” que não seria capaz de distinguir o carácter lícito ou ilícito dos mesmos. Conseqüentemente, o TJ considerou que esta medida solicitada não constitui um justo equilíbrio entre a protecção dos direitos de propriedade intelectual e, por outro lado, a liberdade de empresa, o direito da protecção de dados e a liberdade de expressão (na vertente da «liberdade de receber ou de enviar informações»)¹⁰². A conclusão semelhante, no âmbito da instalação de sistemas de filtragem, chegou o tribunal em *SABAM*¹⁰³. Posteriormente, no acórdão *Bonnier Audio*¹⁰⁴, o TJ teve a oportunidade de confirmar as conclusões enunciadas, já que o Estado-Membro em causa tinha previsto, no diploma de transposição, a obrigação de transmissão de dados para fins de propositura de acção cível¹⁰⁵.

II. Desta jurisprudência do TJ, que tratou questões relacionadas com a relação de tensão entre direitos de propriedade intelectual e o direito da protecção de dados, parece-nos decorrer dois corolários fundamentais. Primeiro: uma vez que o quadro normativo europeu não obriga – nem proíbe – a possibilidade de demandar em tribunal os ISPs para efeitos de transmissão dos dados pessoais dos clientes transgressores das normas de propriedade intelectual, está na disposição dos Estados-Membros todo o processo decisório, quer do ponto de vista legislativo, *i.e.*, da consagração ou não de legislação que determine ou proíba esta situação,

¹⁰¹ Cfr. *Promusicae*, n.º 70. Cfr., também, O. LYNSKEY, *The Foundations of EU Data Protection Law*, cit., p. 155; para uma análise sobre a dificuldade em estabelecer um “justo equilíbrio”, veja-se F. COUDERT / E. WERKERS, “In the Aftermath of the Promusicae Case: How to Strike the Balance?”, *International Journal of Law and Information Technology*, Vol. 18, n.º 1, 2010, p. 50-71.

¹⁰² Cfr. *Scarlet Extended*, n.º 53.

¹⁰³ Acórdão de 16 de Fevereiro de 2012, *SABAM*, C-360/10, ECLI:EU:C:2012:85.

¹⁰⁴ Acórdão de 19 de Abril de 2012, *Bonnier Audio*, C-461/10, ECLI:EU:C:2012:219.

¹⁰⁵ Cfr. *Bonnier Audio*, n.os 57, 60 e 61.

quer do ponto de vista da apreciação do critério do justo equilíbrio, *i.e.*, em última análise, da decisão sobre qual dos valores fundamentais deve prevalecer. Isto significa que esta é uma matéria de harmonização muito complexa, com potencial para colocar obstáculos no mercado único digital. Segundo: o TJ é relutante à implementação por parte de ISPs de sistemas de filtragem de conteúdos, com vista à protecção dos direitos de propriedade intelectual, considerando que não se trata de mecanismos aptos a conduzir a um justo equilíbrio entre valores em tensão.

A este propósito, tendo por referência a sobredita jurisprudência, numa óptica de direito da protecção de dados, vemos com alguma dificuldade a concretização de algumas disposições da recentemente aprovada Directiva 2019/790, relativa aos direitos de autor e direitos conexos no mercado único digital. É que, embora o tema seja sobejamente delicado do ponto de vista da compatibilização entre os direitos de propriedade intelectual e o direito à liberdade de expressão, questiona-se também, sob o prisma do direito da protecção de dados, se determinadas obrigações dirigidas aos prestadores de serviços de partilha de conteúdos em linha não poderão violar os direitos dos titulares (putativos infractores de direitos de autor de terceiros) à protecção de dados pessoais¹⁰⁶.

7. O "JUSTO EQUILÍBRIO" ENTRE O DIREITO À PROTECÇÃO DE DADOS E OS INTERESSES DOS ESTADOS RELACIONADOS COM A MANUTENÇÃO DA SEGURANÇA PÚBLICA

I. Nas últimas décadas, e previamente às recentes entradas em vigor do RGPD e do Regulamento (UE) n.º 2018/1725, a Directiva 95/46/CE, relativa à protecção dos dados pessoais das pessoas singulares, e o Regulamento (CE) 2001/45, relativo à protecção dos dados nas instituições da UE, constituíam o quadro normativo geral em matéria de protecção de dados na União. No entanto, rapidamente o legislador europeu compreendeu que seria necessário legislar sobre determinados sectores especiais, cuja recolha e conservação de dados poderia ser determinante para a manutenção do interesse fundamental dos Estados-Membros em promover a segurança pública, num início de milénio dramaticamente marcado por fenómenos de criminalidade grave, com o terrorismo à escala global a assumir um papel central que cumpria – e cumpre – combater.

Assim, no que respeita à cronologia da publicação de legislação especial, em 2002, foi publicada a Directiva 2002/58/CE – vulgarmente conhecida por Directiva *ePrivacy* –, relativa à privacidade no sector das comunicações electrónicas, que era *lex specialis* da Directiva 95/46/CE (e, actualmente, do RGPD), e fora alterada pela Directiva 2009/136/CE, seguida, em 2006, pela Directiva 2006/24/CE – vulgarmente conhecida

¹⁰⁶ Veja-se, neste sentido, a perspectiva do Juiz M. ENGELER ("Copyright Directive: Does the best effort principle comply with GDPR?", in *Telemedicus – Recht der Informationsgesellschaft*, 23.03.2019, disponível em <https://www.telemedicus.info/article/3402-Copyright-Directive-Does-the-best-effort-principle-comply-with-GDPR.html> [consultado em 05.01.2020]).

por “Directiva Retenção” –, relativa à conservação de dados no contexto das comunicações electrónicas, e, em 2008, pela Decisão-Quadro 2008/977/JAI do Conselho, relativa à cooperação policial e judiciária em matéria penal (sector que, actualmente, é regulado pela Directiva 2016/680). Entretanto, ao longo da década, foram também sendo firmados alguns acordos entre a União e Estados terceiros, relativos ao registo dos dados dos passageiros de viagens aéreas (PNR), surgindo como uma das medidas de segurança adoptadas pelos Estados, com o objectivo de evitar situações semelhantes às do atentado terrorista do 11 de Setembro de 2001¹⁰⁷.

II. A Directiva *ePrivacy* reporta-se às regras sobre a protecção do direito à intimidade da vida privada relativas ao tratamento de dados no sector das comunicações electrónicas disponíveis nas redes públicas de comunicações da União¹⁰⁸. A sensibilidade dos dados gerados neste contexto, aliada aos progressos tecnológicos que se verificaram desde a publicação da Directiva 95/46/CE, justificou a regulação especial conferida a esta matéria, mediante o reforço do princípio da confidencialidade, designadamente através da obrigação de eliminar ou tornar anónimos os dados quando já não forem necessários para efeitos de facturação¹⁰⁹. Atenta, todavia, a necessidade de combater fenómenos de criminalidade grave, o legislador da União, em 2006, publicou a Directiva Retenção, que estabelecia uma derrogação ao princípio da confidencialidade instituído na Directiva *ePrivacy*. A Directiva Retenção impunha a obrigação de os fornecedores de serviços conservarem dados de tráfego e de localização – estando proibida a conservação de dados de conteúdo –, para, se

¹⁰⁷ No acórdão *Parlamento/Conselho*, já referenciado, o TJ declarou inválidas a Decisão 2004/496/CE do Conselho e a Decisão 2004/535/CE da Comissão, relativas, *grosso modo*, ao nível de protecção adequado, ao tratamento e à transferência de dados contidos no *Passenger Name Record* por parte das transportadoras aéreas para as autoridades aduaneiras dos EUA, com base na exclusão do âmbito de aplicação da Directiva 95/46/CE, nunca se tendo pronunciado, porém, sobre o conteúdo material das Decisões (que surgiram num contexto posterior aos atentados do 11 de Setembro de 2001 e como estratégia preventiva do ponto de vista da segurança pública). Sobre este acórdão, veja-se a análise de M. MENDEZ, “Passenger Name Record Agreement, European Court of Justice Annulment of Commission Adequacy Decision and Council Decision Concerning Conclusion of Passenger Name Record Agreement with US”, *European Constitutional Law Review*, n.º 3, 2007. Mais recentemente, embora tratando-se de uma situação distinta, no Parecer n.º 1/15, de 26 de Julho de 2017, ECLI:EU:C:2016:656, relativo ao Projecto de acordo PNR entre o Canadá e a União, o TJ fez extensas considerações sobre a (in)compatibilidade de algumas normas com os direitos fundamentais à privacidade e protecção de dados, considerando que o acordo não poderia ser celebrado na forma que fora apresentado. Sobre o Parecer do TJ, cfr. A. VEDASCHI, “The European Court of Justice on the EU-Canada Passenger Name Record Agreement ECJ, 26 July 2017, Opinion 1/15”, *European Constitutional Law Review*, n.º 14, 2018. Em matéria de PNR, actualmente, vigora na União a Directiva (UE) 2016/681, de 27 de Abril de 2016.

¹⁰⁸ Cfr. artigo 3.º, n.º 1, da Directiva *ePrivacy*.

¹⁰⁹ Neste sentido, cfr. acórdãos *Digital Rights Ireland*, n.º 32, e C-119/12, *Probst* (3.ª Secção, 22.11.2012), n.º 23.

solicitado, os disponibilizarem às autoridades nacionais competentes¹¹⁰, impondo, conseqüentemente, uma ingerência no direito fundamental à protecção de dados¹¹¹. Tratava-se, no entanto, de uma ingerência que não afectava o conteúdo essencial do direito fundamental, por força de não serem retidos dados de conteúdo¹¹², e que correspondia a objectivos gerais do direito da União, designadamente a luta contra o terrorismo¹¹³. A Directiva Retenção foi, porém, anulada pelo TJ, no acórdão *Digital Rights Ireland*¹¹⁴. Neste aresto, o TJ declarou a invalidade da Directiva, por considerar que «o legislador da União excedeu os limites impostos pelo respeito do princípio da proporcionalidade»¹¹⁵, tendo analisado os critérios da adequação, da necessidade e do justo equilibrio.

III. Alguns aspectos de *Digital Rights Ireland* foram, posteriormente, retomados no acórdão *Tele2 Sverige* e, recentemente, no acórdão *Ministerio Fiscal*¹¹⁶, que surgem no contexto das dúvidas geradas em torno do alcance do acórdão *Digital Rights Ireland*. Nestes arestos, o TJ esclareceu que só a luta contra a criminalidade grave, e não a mera luta contra a criminalidade¹¹⁷, justifica uma ingerência grave e, conseqüentemente, a existência de um acto normativo nacional de conteúdo semelhante ao da Directiva Retenção¹¹⁸. Do mesmo modo, uma ingerência que não seja considerada grave é considerada legítima quando haja «um objetivo de prevenção, de investigação, de deteção e de repressão de “infrações penais” em geral»¹¹⁹.

¹¹⁰ Cfr. *Digital Rights Ireland*, n.os 25.º e 26.

¹¹¹ Cfr. *Digital Rights Ireland*, n.º 36.

¹¹² Cfr. *Digital Rights Ireland*, n.º 40.

¹¹³ Cfr. *Digital Rights Ireland*, n.º 44.

¹¹⁴ Para uma análise e comentários ao acórdão *Digital Rights Ireland*, cfr. O. LYNSKEY, “The Data Retention Directive is incompatible with the rights to privacy and data protection and is invalid in its entirety: Digital Rights Ireland”, *Common Market Law Review*, Vol. 51, n.º 6, 2014, pp. 1789-1811; T. OJANEN, “Privacy Is More Than Just a Seven-Letter Word: The Court of Justice of the European Union Sets Constitutional Limits on Mass Surveillance: Court of Justice of the European Union Decision of 8 April 2014 in Joined Cases C-293/12 and C-594/12, Digital Rights Ireland and Seitlinger and Others”, *European Constitutional Law Review*, n.º 10, 2014, pp. 528-541. Para uma análise às implicações da invalidade da Directiva, cfr. D. SILVA RAMALHO / J. D. COIMBRA, “A declaração de invalidade da Directiva 2006/24/CE: presente e futuro da regulação sobre conservação de dados de tráfego para fins de investigação, deteção e repressão de crimes graves”, *O Direito*, Vol. 147, n.º IV, 2015.

¹¹⁵ Cfr. *Digital Rights Ireland*, n.º 69.

¹¹⁶ Acórdão de 2 de Outubro de 2018, *Ministerio Fiscal*, C-207/16, ECLI:EU:C:2018:788. Para um comentário, cfr. X. TRACOL, “*Ministerio Fiscal*: Access of Public Authorities to Personal Data Retained by Providers of Electronic Communications Services”, *European Data Protection Law Review*, Vol. 5, n.º 1, 2019.

¹¹⁷ Note-se, também, que, embora noutra contexto, o TJ já havia considerado que o tratamento de dados pessoais, para efeitos de combate à criminalidade, dirigido apenas a cidadãos da União que não os cidadãos nacionais de um Estado-Membro constituía uma discriminação proibida. Cfr. *Huber*, n.os 78-81.

¹¹⁸ Cfr. *Tele2 Sverige*, n.º 102.

¹¹⁹ *Ministerio Fiscal*, n.º 57.

IV. Em *Digital Rights Ireland*, o TJ, no uso das competências instituídas pelos Tratados, anulou um acto jurídico da União. Trata-se, pois, de uma das menos frequentes¹²⁰, mas, indubitavelmente, de uma das mais impressionantes formas de realização do direito da protecção de dados, a qual constitui, de entre todas, estamos convicta, a intervenção mais cristalina do Tribunal enquanto guardião do direito fundamental.

8. CONCLUSÃO

Muitas foram as questões e os desafios com que o TJUE se debateu nas últimas duas décadas. No presente texto, procedemos à identificação de algumas linhas jurisprudenciais do Tribunal em matéria de aplicação do direito europeu da protecção de dados.

Um dos primeiros corolários da primeira fase de proliferação jurisprudencial do TJ é o de que, não obstante o reconhecimento da necessidade de se garantir um estrito cumprimento das disposições que enformam o direito fundamental à protecção de dados, este não oblitera os direitos de informação administrativa. O referido corolário assume uma importância fundamental no âmbito da publicidade das actuações administrativas, uma vez que permite não só acautelar o princípio da transparência administrativa como, simultaneamente, informar as entidades públicas no que concerne à forma como devem efectuar as operações de tratamento de dados pessoais necessárias à consecução daquele desiderato, sem, todavia, comprometer os direitos dos titulares dos dados.

A densificação de princípios por parte do Tribunal constitui um caso evidente de influência da prática do TJ nas soluções mais tarde consagradas na legislação positiva. O exemplo paradigmático é o do aprofundamento do princípio da total independência das autoridades de controlo. Este princípio tinha uma configuração meramente programática na Directiva 95/46/CE. Com o RGPD, porém, todas as soluções preconizadas pelo Tribunal, na jurisprudência sobre o referido princípio, foram acolhidas nalgumas das disposições legais dos artigos 52.º e 53.º do Regulamento. O caso da densificação do princípio da total independência das autoridades de controlo permite, assim, demonstrar que o direito da protecção de dados também se realiza mediante a transposição de precedentes jurisprudenciais para a legislação positiva.

Para além de burilar princípios, o Tribunal operou também uma densificação de conceitos operativos da protecção de dados absolutamente basilares, como sendo o conceito de dados pessoais e o conceito de responsável pelo tratamento. Com efeito, a interpretação dada pelo TJ é crucial para a forma como as relações jurídicas, em matéria de protecção de dados, se concretizam, particularmente por força da fixação de noções amplas.

Uma outra linha jurisprudencial relevante do TJ é a da resolução de colisões de direitos. O Tribunal tem esclarecido que «o direito à protecção de dados não é uma prerrogativa absoluta» e, por isso, em caso de

¹²⁰ Neste particular, recorde-se que, em 2015, o TJ procedeu à anulação da Decisão *Safe Harbor*, no acórdão *Schrems*, conforme já aludido neste texto.

colisão de direitos – *v.g.*, colisão do direito à protecção de dados com o direito à liberdade de expressão ou com os direitos de propriedade intelectual –, é necessário operar o critério de ponderação do “justo equilíbrio”, o mesmo sucedendo quando em cotejo estejam os interesses dos Estados-Membros em assegurar a segurança pública. Neste particular, o critério do “justo equilíbrio”, para além de reclamar a materialização do juízo de proporcionalidade intrinsecamente inerente, determina, a jusante, e quando apropriado, a aplicação de exclusões de âmbito (*v.g.*, o caso da derrogação para fins jornalísticos). Ademais, o critério do “justo equilíbrio” pode, ainda, determinar a anulação de legislação (*v.g.*, o caso da anulação da Directiva Retenção), pelo que esta é também um dos modos de realização do direito da protecção de dados através da jurisprudência do TJ.

Em síntese, pode concluir-se que concorrem para a realização do direito da protecção de dados através da jurisprudência do TJ, *inter alia*, (i) a densificação de princípios, direitos e conceitos, geralmente mediante a fixação de noções amplas; (ii) a transposição de corolários jurisprudenciais para o plano do direito positivo; (iii) a conceptualização do critério do “justo equilíbrio”, nas situações de colisão de direitos e/ou interesses; e (iv) a anulação de legislação.

9. BIBLIOGRAFIA

- A. SOUSA PINHEIRO, *Privacy e Protecção de Dados Pessoais: A Construção Dogmática do Direito à Identidade Informacional*, AAFDL, Lisboa, 2015.
- A. VEDASCHI, “The European Court of Justice on the EU-Canada Passenger Name Record Agreement ECJ, 26 July 2017, Opinion 1/15”, *European Constitutional Law Review*, 14, 2018, <https://doi.org/10.1017/S1574019618000202>.
- C. CADWALLADR / E. GRAHAM-HARRISON, “Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach”, *The Guardian* (Londres, 17.03.2018), disponível em <https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election> [consultado em 26.06.2020].
- C. KUNER, “Reality and Illusion in EU Data Transfer Regulation Post Schrems” *German Law Journal*, Vol. 18, n.º 4, 2017, <https://doi.org/10.1017/S2071832200022197>.
- C. SARMENTO E CASTRO, “40 anos de ‘Utilização da Informática’ – o artigo 35.º da Constituição da República Portuguesa”, *e-Pública – Revista Eletrónica de Direito Público*, Vol. 3, n.º 3, 2016.
- D. BURCHARDT, “The relationship between the law of the European Union and the law of its Member States – a norm-based conceptual framework”, *European Constitutional Law Review*, Vol. 15, n.º 1, 2019, <https://doi.org/10.1017/S1574019618000512>.
- D. ERDOS, “European Data Protection and Freedom of Expression after Buivids: An Increasingly Significant Tension”, in *European Law Blog*, 21.02.2019, disponível em

- <https://europeanlawblog.eu/2019/02/21/european-data-protection-and-freedom-of-expression-after-buivids-an-increasingly-significant-tension/> [consultado em 05.01.2020].
- “From the Scylla of Restriction to the Charybdis of Licence? Exploring the Scope of the ‘Special Purposes’ Freedom of Expression Shield in European Data Protection”, *Common Market Law Review*, Vol. 52, n.º 1, 2015.
- D. MOURA VICENTE, “Opinião: O direito ao esquecimento na internet”, in *Dinheiro Vivo*, 21/05/2018, disponível em <https://www.dinheirovivo.pt/opiniao/o-direito-ao-esquecimento-na-internet-novo-direito-ou-limite-a-liberdade-de-expressao/> [consultado em 05.01.2020].
- D. SILVA RAMALHO / J. DUARTE COIMBRA, “A declaração de invalidade da Diretiva 2006/24/CE: presente e futuro da regulação sobre conservação de dados de tráfego para fins de investigação, deteção e repressão de crimes graves”, *O Direito*, Vol. 147, n.º IV, 2015.
- F. COUDERT / E. WERKERS, “In the Aftermath of the Promusicae Case: How to Strike the Balance?”, *International Journal of Law and Information Technology*, Vol. 18, n.º 1, 2010, <https://doi.org/10.1093/ijlit/ean015>.
- F. SNYDER, “The Effectiveness of European Community Law: Institutions, Processes, Tools and Techniques”, *Modern Law Review*, 56, 1993.
- F. URBANO CALVÃO, *Direito da Proteção de Dados. Relatório sobre o programa, os conteúdos e os métodos de ensino da disciplina*, Universidade Católica Editora, Porto, 2018.
- G. GONZÁLEZ FUSTER, *The Emergence of Personal Data Protection as a Fundamental Right of the EU*, Springer, Heidelberg, 2014.
- J. J. GOMES CANOTILHO, *Direito Constitucional e Teoria da Constituição*, 7.ª ed., Almedina, Coimbra, 2003.
- J. P. REMÉDIO MARQUES, “Artigo 118.º”, in M. LOPES PORTO / G. ANASTÁCIO (Coord.), *Tratado de Lisboa Anotado e Comentado*, Almedina, Coimbra, 2012.
- J. Q. WHITMAN, “The Two Western Cultures of Privacy: Dignity versus Liberty”, *Yale Law Journal*, Vol. 113, 2004.
- J. ROSEN, “The Deciders: The Future of Privacy and Free Speech in the Age of Facebook and Google”, *Fordham Law Review*, Vol. 80, n.º 4, 2012.
- L. COUTO GONÇALVES / C. TRABUCO / M. M. CARVALHO, “Capítulo XI – Propriedade Intelectual”, in A. SILVEIRA / P. MADEIRA FROUFE / M. CANOTILHO (Coord.), *Direito da União Europeia – Elementos de Direito e Políticas da União*, Almedina, Coimbra, 2016.
- L. COUTO GONÇALVES / M. MIGUEL CARVALHO, “Artigo 17.º”, in A. SILVEIRA / M. CANOTILHO (Coord.), *Carta dos Direitos Fundamentais da União Europeia Comentada*, Almedina, Coimbra, 2013.
- L. SENDEN, *Soft Law in European Community Law*, Hart Publishing, Oxford, 2004.

- M. ANTONINO DE LA CÁMARA, "Transparencia y Derecho de Acceso a la Información versus Protección de Datos", *Revista Internacional de Transparencia e Integridad*, n.º 4, 2017.
- M. ENGELER, "Copyright Directive: Does the best effort principle comply with GDPR?", in *Telemedicus – Recht der Informationsgesellschaft*, 23.03.2019, [disponible en https://www.telemedicus.info/article/3402-Copyright-Directive-Does-the-best-effort-principle-comply-with-GDPR.html](https://www.telemedicus.info/article/3402-Copyright-Directive-Does-the-best-effort-principle-comply-with-GDPR.html) [consultado em 05.01.2020]).
- M. JOZWIAK, "The Scale Matters: The EctHR Grand Chamber Finds That Prohibition of Mass Publication of Raw Taxation Data Does Not Infringe Right to Freedom of Expression", *European Data Protection Law Review*, Vol. 4, n.º 1, 2018, <https://doi.org/10.21552/edpl/2018/1/20>.
- M. L. RUSTAD / S. KULEVSKA, "Reconceptualizing the Right to be Forgotten to Enable Transatlantic Data Flow", *Harvard Journal of Law & Technology*, Vol. 28, n.º 2, 2015.
- M. LORENA FLÓREZ ROJAS, "Legal implications after *Schrems* case: are we trading fundamental rights?", *Information & Communications Technology Law*, Vol. 25, n.º 3, 2016, <https://doi.org/10.1080/13600834.2016.1239564>.
- M. MENDEZ, "Passenger Name Record Agreement, European Court of Justice Annulment of Commission Adequacy Decision and Council Decision Concerning Conclusion of Passenger Name Record Agreement with US", *European Constitutional Law Review*, 3, 2007, <https://doi.org/10.1017/S1574019607001277>.
- M. POIARES MADURO, "Contrapunctual Law: Europe's Constitutional Pluralism in Action" in N. WALKER (ed.), *Sovereignty in Transition*, Hart Publishing, Oxford, 2003.
- M. SCHEININ, "Towards evidence-based discussion on surveillance: A Rejoinder to Richard A. Epstein", *European Constitutional Law Review*, 12, 2016, <https://doi.org/10.1017/S1574019616000201>.
- M. SCHREMS, "The Privacy Shield is a Soft Update of the Safe Harbor", *European Data Protection Law Review*, Vol. 2, n.º 2, 2016, <https://doi.org/10.21552/EDPL/2016/2/4>.
- M. SZYDŁO, "Principles underlying independence of national data protection authorities: Commission v. Austria", *Common Market Law Review*, Vol. 50, n.º 6, 2013.
- "The independence of data protection authorities in EU law: between the safeguarding of fundamental rights and ensuring the integrity of the internal market", *European Law Review*, Vol. 42, n.º 3, 2017.
- N. COHEN, "The Privacy Follies: A Look Back at the CJEU's Invalidation of the EU/US Safe Harbor Framework", *European Data Protection Law Review*, Vol. 1, n.º 3, 2015, <https://doi.org/10.21552/EDPL/2015/3/15>.
- N. PURTOVA, "The law of everything. Broad concept of personal data and future of EU data protection law", *Law, Innovation and Technology*, Vol. 10, n.º 1, 2018.

- N. WALKER, "The Idea of Constitutional Pluralism", *Modern Law Review*, Vol. 65, n.º 3, 2002.
- O. LYNSKEY, "The Data Retention Directive is incompatible with the rights to privacy and data protection and is invalid in its entirety: Digital Rights Ireland", *Common Market Law Review*, Vol. 51, n.º 6, 2014.
- *The Foundations of EU Data Protection Law*, Oxford University Press, Oxford, 2015.
- O. STEFAN, *Soft Law in Court. Competition Law, State Aid and the Court of Justice of the European Union*, Kluwer Law International, The Netherlands, 2012.
- P. CRAIG / G. DE BÚRCA, *EU Law Text, Cases, and Materials*, 5.ª ed., Oxford University Press, Oxford, 2011.
- P. E. FISCHER, "Getting Privacy to a new Safe Harbour Comment on the CJEU Judgment of 6 October 2015, Schrems v Data Protection Commissioner", *Journal of Intellectual Property, Information Technology and Electronic Commerce Law*, Vol. 6, n.º 3, 2015.
- P. OLIVER, "The Protection of Privacy in the Economic Sphere Before the European Court of Justice", *Common Market Law Review*, Vol. 46, n.º 5, 2009.
- P. SOUSA E SILVA, *Direito Industrial*, 2.ª ed., Almedina, Coimbra, 2019.
- R. A. EPSTEIN, "The ECJ's Fatal Imbalance: Its cavalier treatment of national security issues poses serious risk to public safety and sound commercial practices", *European Constitutional Law Review*, n.º 12, 2016, <https://doi.org/10.1017/S1574019616000195>.
- R. DE SOUSA COSTA / T. SÉRGIO CABRAL, "The European Union's existential crisis: current challenges from populism to Donald Trump", *UNIO EU Law Journal*, Vol. 4, n.º 1, 2018, <https://doi.org/10.21814/unio.4.1.2>.
- R. G. LARSON III, "Forgetting the First Amendment: How Obscurity-Based Privacy and a Right to be Forgotten are Incompatible with Free Speech", *Communication Law and Policy*, Vol. 18, n.º 1, 2013, <https://doi.org/10.1080/10811680.2013.746140>.
- R. MARTÍNEZ MARTÍNEZ, "El derecho fundamental a la protección de datos: perspectivas", *Revista d'Internet, Dret i Política*, n.º 5, 2007.
- S. C. BENNETT, "The 'Right to Be Forgotten': Reconciling EU and US Perspectives", *Berkeley Journal of International Law*, Vol. 30, n.º 1, 2012.
- S. D. WARREN / L. D. BRANDEIS, "The Right to Privacy", *Harvard Law Review*, Vol. 4, n.º 5, 1890.
- S. PEREZ FERNANDES, *Da vinculação dos Estados-Membros ao «direito a uma boa administração» previsto na Carta dos Direitos Fundamentais da União Europeia – argumentos para uma internormatividade administrativa* [inédito], Tese de Doutoramento em Ciências Jurídicas Públicas apresentada à Universidade do Minho, Braga, 2016.
- T. OJANEN, "Making the Essence of Fundamental Rights Real: The Court of Justice of the European Union Clarifies the Structure of Fundamental Rights under the Charter ECJ 6 October 2015, Case C-362/14,

- Maximillian Schrems v Data Protection Commissioner*", *European Constitutional Law Review*, n.º 12, 2016, <https://doi.org/10.1017/S1574019616000225>.
- "Privacy Is More Than Just a Seven-Letter Word: The Court of Justice of the European Union Sets Constitutional Limits on Mass Surveillance: Court of Justice of the European Union Decision of 8 April 2014 in Joined Cases C-293/ 12 and C-594/12, Digital Rights Ireland and Seitlinger and Others", *European Constitutional Law Review*, n.º 10, 2014, <https://doi.org/10.1017/S1574019614001345>.
- V. L. GUTIÉRREZ CASTILLO, "Aproximación a la Protección Jurídica Internacional del Derecho de Acceso y Protección de Datos en Europa", *Derecho y conocimiento*, Vol. 3, n.º 1, 2005.
- X. TRACOL, "Ministerio Fiscal: Access of Public Authorities to Personal Data Retained by Providers of Electronic Communications Services", *European Data Protection Law Review*, Vol. 5, .º 1, 2019, <https://doi.org/10.21552/edpl/2019/1/20>.