
CYBERLAW
by CIJIC

CYBERLAW by CIJIC

EDIÇÃO N.º VII – MAIO DE 2019

REVISTA CIENTÍFICA SOBRE CYBERLAW DO CENTRO DE INVESTIGAÇÃO JURÍDICA DO CIBERESPAÇO – CIJIC – DA FACULDADE DE DIREITO DA UNIVERSIDADE DE LISBOA

CYBERLAW
by CIJIC

CIJIC: CENTRO DE INVESTIGAÇÃO JURÍDICA DO CIBERESPAÇO

ISSN 2183-729

NOTAS DO EDITOR:

Nesta nova edição da revista do Centro de Investigação Jurídica do Ciberespaço da Faculdade de Direito da Universidade de Lisboa, antes de mais, aproveito para anunciar uma nova edição do Curso de Direito do Ciberespaço, em formato novel, a ter lugar em Novembro de 2019. À semelhança do curso anterior, na oportunidade de publicação de alguns artigos, a Revista assumir-se-á como esse veículo de partilha de conhecimento.

No que concerne propriamente às notas desta edição, permitam-me partilhar algumas novidades e preocupações.

No passado dia 23 de maio do corrente, o Conselho de Ministros aprovou a Estratégia Nacional de Segurança do Ciberespaço (ENSC) 2019-2023, que ainda carece de publicação em jornal oficial. Não obstante é já do domínio público que o propósito desta nova ENSC visará *garantir a proteção e a defesa das infraestruturas críticas e dos serviços vitais de informação, e potenciar uma utilização livre, segura e eficiente do ciberespaço por parte de todos os cidadãos, das empresas e das entidades públicas e privadas, procedendo desta forma à revisão da ENSC de 2015*[1], tendo em atenção a evolução digital ocorrida desde então.

1 https://www.portugal.gov.pt/pt/gc21/governo/comunicado-de-conselho-de-ministros?i=278
A propósito, neste conspecto, para quem não tenha estado presente, na Conferência – Cibersegurança, na Universidade de Évora, a 14 de novembro de 2018, será interessante dar uma vista de olhos na apresentação "A Estratégia Nacional de Segurança do Ciberespaço 2.0 – Governação e execução", feita e disponibilizada por parte do CALM Gameiro Marques, da Autoridade Nacional de Segurança, cujo conteúdo pode ser encontrado @ https://www.uevora.pt/media_informacoes/agenda/(item)/25903.

Em efeméride de aniversário do Regulamento Geral de protecção de dados, e estando este em vigor desde *o vigésimo dia seguinte ao da sua publicação no Jornal Oficial da União Europeia*, naturalmente a «Cyberlaw by CIJIC» não poderia passar ao lado do tema, recorrente dos últimos anos.

De facto, nestes 3 anos volvidos, é inconcebível que Portugal ainda não tenha uma lei de execução do mesmo. De igual forma, é inconcebível que as organizações, públicas ou privadas, só conheçam o "consentimento" como fundamento de licitude para o tratamento de dados pessoais, considerando-o um verdadeiro *canivete-suíço*. Ainda havemos de pugnar por um "*direito ao esquecimento*" sobre o consentimento, pois que a livre revogabilidade do mesmo por parte da pessoa titular dos dados pessoais parece sucumbir ante tanto abuso na sua utilização por parte das mais variadas organizações.

Se a estupefação quanto ao uso abusivo da figura do consentimento não cercear a nossa incredulidade, é igualmente inconcebível que o Estado, hoje, 3 anos após a entrada em vigor do RGPD, tenha dado conta de que, por exemplo, pelo menos, 1977 freguesias estarão obrigadas a nomear um encarregado de protecção de dados. Subam ou desçam na hierarquia do Estado e imaginem a confusão em que se vive. Três anos volvidos e o Mercado Único Digital Europeu à espreita…

Não pensem, contudo que a confusão é exclusivo do sector público. Quando o foco deriva para dados pessoais sensíveis, nomeadamente, dados de saúde, notícias como por exemplo, «*Proteção de Dados condena clínicas que recusam tratar doentes por falta de assinaturas*[2]», revelam parte do preocupante e actual estado de coisas.

Com efeito, se a protecção de dados pessoais era até há pouco tempo tema desconhecido do grande público, num ápice passou a ser o *olho do furacão*, gerando leque preenchido de atropelos e violações de dados dos seus titulares. E a autoridade nacional de controlo continua amarrada a constrangimentos de índole múltipla, desde orçamentais à falta de recursos, humanos e tecnológicos. Imaginem o que escapa ao *mainstream* mediático.

Enquanto isso, a evolução do digital continua em passo acelerado. O nível de ameaça ao estado de direito democrático acompanha esta desenfreada marcha.

2 Disponível em https://www.dn.pt/lusa/interior/protecao-de-dados-condena-clinicas-que-recusam-tratar-doentes-por-falta-de-assinaturas-10901005.html,

Infelizmente, o tempo do direito e da justiça teimam em não se adaptar. Está assíncrono. O que, se por um lado até poderá induzir-nos a alguma prudência, por outro pode indiciar um factor de preocupação acrescido. Até pelo nível de risco em que coloca a sociedade, no seu todo.

Pensemos na utilização do uso de UAV's; na condução autónoma de veículos; na constante violação das propriedades essenciais da informação gerando supremacias informacionais ilegais a certos Estados; na massificação das redes sociais; na disseminação em *live streaming* de ataques a pessoas; na dispersão de conteúdo mentiroso e propagandístico *online* para desvirtuar o resultado de eleições livres e democráticas; na disseminação de ódio e violência *online*; nas novas ameaças a toda a actividade policial e de segurança do Estado; no controlo e rastreio individual *online* e no registo de crédito social em função disto; entre outras. A profusão destas notícias é de conhecimento geral. A *digitalização* humana está em curso. O ciberespaço, aparentemente, evolui para uma antiutopia.

Neste ensamble, vertiginoso e fulminante, é pois inconcebível que dois anos volvidos após um pedido de fiscalização sucessiva intentado junto do Tribunal constitucional português, por parte de um conjunto de partidos políticos, este Tribunal ainda não se tenha pronunciado quanto à constitucionalidade do acesso aos metadados, dados de tráfego e duração de comunicações por parte dos serviços secretos portugueses. É inconcebível e preocupante pois que, por um lado o serviço de informações da república esteja parado ou a trabalhar à margem da lei ante esta omissão do Tribunal; por outro lado, é inconcebível que este Tribunal, por excelência, de garantia dos direitos e liberdades fundamentais das pessoas, esteja dois anos para aferir da constitucionalidade de uma dada lei.

O que tanto demora a tomada de decisão? Falta de preparação temática dos juízes do Constitucional? Má técnica legislativa? Teimosia política? Falta de ameaças concretas, conhecidas do público, à segurança do Estado? Neste particular dos metadados, sublinho, o delírio é a nota dominante. Até porque, se *o Sistema de Acesso ao Pedido de Dados aos Prestadores dos Serviços de Comunicações Electrónicas (Sapdoc), foi declarado operacional pelo CFSIRP desde Março e está a funcionar*, no outro plano da acção, consta que poderá estar na iminência *um novo chumbo dos juízes,*

uma vez que a questão de fundo - violação do artigo 34º da CRP- manter-se-á [3]. Ora, parece-nos que este delírio, portanto, promete e vai continuar. Novo procedimento, novas discussões, nova lei, mais discussões, novo pedido de fiscalização, novo entorpecimento, novo regresso ao ponto de partida, que recordo, é a nota dominante desde que o poder político criou o *novo regime do Sistema de Informação da República Portuguesa*, em 2015.

Óbice daqui, ameaça dali, risco dacolá, não haverá uma luz de esperança que contrarie o delinear desta *antiutopia*?

A bem de todos nós, mesmo que tenha passado despercebido o *Christchurch Call*[4], julgamos decisivo o apelo à acção. Até porque o momento, o tempo e o espaço a tal nos obrigam. Aqui chegados, impõe-se-nos o sublinhar de parte das notas dos proponentes iniciais. Por um lado, o *envisage* do Presidente francês, o sr. Macron: «"*We need to build this new cyberspace, a free, open and secure Internet, which allows everyone to share, learn, innovate, but which also allows us to uphold our values, protect our citizen and empower them*"»; por outro, o apelo à adesão pluriparticipada, mundial, a cargo da Primeiro-Ministra Neozelandesa, a sra. Ardern: «"*From here, I will work alongside others signed up to the Christchurch Call to bring more partners on board, and develop a range of practical initiatives to ensure the pledge we have made today is delivered*"». Por um *mundo*, terreno e digital, melhor, de todos e para todos.

Por fim, num plano nacional, com especial saudação para a ousadia da proposta, arbitramos da pertinência do Projeto de Lei 1217/XIII[5], apresentado pelo partido Socialista, já apelidado de Carta de Direitos Fundamentais na Era Digital.

A Carta deverá corresponder a *lei de protecção de direitos, liberdades e garantias centrada nas pessoas, consagradora de valores democráticos essenciais contra ameaças que não devem ser ignoradas* procurando ir além de mera *lei compilatória das normas que na ordem jurídica portuguesa consagram (alguns) direitos*, que enuncie *um elenco diversificado e abrangente, que inove, clarifique e valha também*

3 https://www.dn.pt/poder/interior/-necessidade-inquestionavel-fiscais-das-secretas-validam-acesso-a-dados-das-comunicacoes--10935824.html

4 https://www.beehive.govt.nz/release/christchurch-call-eliminate-terrorist-and-violent-extremist-online-content-adopted

5 Disponível em: https://www.parlamento.pt/ActividadeParlamentar/Paginas/DetalheIniciativa.aspx?BID=43768

como programa de ação vinculativo dos órgãos de poder, pode ler-se no enunciado programático do Projeto de lei. Deixo aqui um apelo a uma participação contributiva entusiasta por forma a melhorar este esboço inicial de consagração de uma Carta de Direitos Fundamentais na Era Digital.

Resta-me, a final, agradecer a todos quantos contribuíram para mais uma edição da Revista, pelo esforço e pelo trabalho, endereçando, em nome do Centro de Investigação Jurídica do Ciberespaço – CIJIC – da Faculdade de Direito da Universidade de Lisboa, um reconhecido: Muito Obrigado.

Cyberlaw by CIJIC, ***Direito: a pensar tecnologicamente*.**

Boas leituras.

Lisboa, FDUL, 24 de Maio de 2019

Nuno Teixeira Castro

CYBERLAW

by CIJIC

DOUTRINA

DIREITO APLICÁVEL À PROTEÇÃO DE DADOS PESSOAIS NA INTERNET: ALGUNS ASPETOS DE DIREITO INTERNACIONAL PRIVADO

LUÍS DE LIMA PINHEIRO [1]

1Professor Catedrático da Faculdade de Direito da Universidade de Lisboa.
O presente estudo representa o desenvolvimento da comunicação apresentada no Curso de Pós-Graduação sobre Direito do Ciberespaço, organizado pelo Instituto de Ciências Jurídico-Políticas e pelo CIJIC da Faculdade de Direito da Universidade de Lisboa.

RESUMO

A privacidade é um valor tutelado pela generalidade dos sistemas jurídicos democráticos, mas há diferenças importantes quanto ao conteúdo e à extensão desta proteção, bem como, em particular, quanto à sua conciliação com a liberdade de expressão e informação. Estas diferenças manifestam-se, designadamente, quanto à proteção de dados pessoais.

Na ordem jurídica portuguesa, a proteção dos dados pessoais constitui um direito fundamental, que não só resulta da concretização do direito à privacidade como também é, em certa medida, autonomizado.

Não cabendo examinar neste estudo a controvérsia suscitada por certas soluções materiais, pode afirmar-se que a vasta uniformização do Direito material aplicável à proteção de dados pessoais na UE é, em princípio, justificada. No entanto, o âmbito espacial de aplicação do RGPD parece demasiado amplo, não assegurando que existe sempre uma ligação significativa com a União Europeia.

Palavras-Chave: Dados pessoais; Privacidade; direitos fundamentais; direitos de personalidade; CRP; RGPD; União Europeia.

1. INTRODUÇÃO

Os *dados pessoais* são informações relativas a uma pessoa singular identificada ou identificável, por exemplo, nome, número de identificação, endereço postal ou de correio eletrónico ou qualquer elemento específico da identidade física, fisiológica, genética, mental, económica, cultural ou social dessa pessoa singular ([1]).

A privacidade é um valor tutelado pela generalidade dos sistemas jurídicos democráticos, mas há diferenças importantes quanto ao conteúdo e à extensão desta proteção, bem como, em particular, quanto à sua conciliação com a liberdade de expressão e informação. Estas diferenças manifestam-se, designadamente, quanto à proteção de dados pessoais ([2]).

Em situações com contactos relevantes com mais de um Estado (situações transnacionais), a proteção de dados pessoais coloca um problema de determinação do Direito aplicável. O Direito aplicável tanto pode ser uma lei estadual, como um instrumento supraestadual, que unifique ou uniformize o regime aplicável nos Estados por ele vinculados.

Na ordem jurídica portuguesa, *a proteção dos dados pessoais constitui um direito fundamental*, que não só resulta da concretização do direito à privacidade como também é, em certa medida, autonomizado.

A Constituição portuguesa consagra o direito à reserva da intimidade da vida privada no art. 26.º/1 e determina que a lei estabelecerá garantias efetivas contra a obtenção e utilização abusivas, ou contrárias à dignidade humana, de informações relativas às pessoas (art. 26.º/2). A Constituição autonomiza o direito à proteção de dados pessoais informatizados no art. 35.º. Por seu turno, o art. 37.º consagra *a liberdade de expressão e informação*, incluindo o direito de informar, de se informar e de ser informado, sem impedimentos nem discriminações. Todos estes direitos podem ser vistos como projeções da dignidade da pessoa humana ([3]).

Também a Convenção Europeia dos Direitos do Homem protege o direito ao respeito pela vida privada e familiar (art. 8.º) e a liberdade de expressão (art. 10.º) que tem, entre

1 - Ver definição contida no art. 4.º/1 do Regulamento Geral sobre a Proteção de Dados.
2 - Ver Paul SCHWARTZ e Karl-Nicolaus PEIFER – "Transatlantic Data Privacy", *LSN Cyberspace Law eJournal, Vol. 22 No. 85, 11/22/2017* (acessível em SSRN), 121 e segs.
3 - Ver JORGE MIRANDA – *Direitos Fundamentais*, 2.ª ed., Coimbra, Almedina, 2017, 233-234.

outras, como concretizações a liberdade de imprensa e o direito à informação. A jurisprudência do Tribunal Europeu dos Direitos do Homem não parece fornecer indicações inteiramente claras sobre o modo de ponderar estes direitos ([4]), dependendo das circunstâncias do caso qual dos direitos deve prevalecer ([5]).

A nível da UE, o direito à proteção dos dados de caráter pessoal está consagrado no Tratado sobre o Funcionamento da União Europeia (art. 16.º/1) e na Carta dos Direitos Fundamentais da União Europeia. Esta Carta, além de consagrar o direito ao respeito pela vida privada e familiar (art. 7.º), autonomiza o direito à proteção dos dados pessoais no art. 8.º. Esta disposição determina, designadamente, que os dados pessoais devem ser objecto de um tratamento leal, para fins específicos e com o consentimento da pessoa interessada ou com outro fundamento legítimo previsto por lei (n.º 2).

A liberdade de expressão e de informação também está consagrada na Carta (art. 11.º).

As restrições aos direitos fundamentais reconhecidos na Carta, designadamente no caso de conflitos de direitos, têm de respeitar o princípio da proporcionalidade (art. 52.º/1): "Qualquer restrição ao exercício dos direitos e liberdades reconhecidos pela presente Carta deve ser prevista por lei e respeitar o conteúdo essencial desses direitos e liberdades. Na observância do princípio da proporcionalidade, essas restrições só podem ser introduzidas se forem necessárias e corresponderem efetivamente a objetivos de interesse geral reconhecidos pela União, ou à necessidade de proteção dos direitos e liberdades de terceiros".

A UE considerou necessário harmonizar as leis dos Estados-Membros em matéria de proteção de dados pessoais através da *Diretiva 95/46/CE* que foi transposta para a ordem jurídica portuguesa pela *Lei da Proteção de Dados Pessoais* (Lei n.º 67/98, de 26/10).

Esta Diretiva apenas aproximou as legislações dos Estados-Membros e, por conseguinte continha no art. 4.º/1 uma norma sobre o âmbito de aplicação no espaço da legislação de transposição da Diretiva de cada Estado-Membro ([6]), que foi transposta para o n.º 3 do artigo

4 - Ver Fomperosa RIVERO – "Right to Be Forgotten in the European Court of Justice Google Spain Case: The Right Balance of Privacy Rights, Procedure, and Extraterritoriality", *LSN Cyberspace Law eJournal, Vol. 22 No. 19, 03/15/2017* (acessível em SSRN), 22.

5 - Ver Stefan KULK e Frederik Borgesius – "Privacy, Freedom of Expression, and the Right to Be Forgotten in Europe", *LSN Transnational Litigation/Arbitration, Private International Law, & Conflict of Laws eJournal, Vol. 4 No. 13, 03/09/2017* (acessível em SSRN), 7 e segs.

6 - "1. Cada Estado-membro aplicará as suas disposições nacionais adoptadas por força da presente directiva ao tratamento de dados pessoais quando:
a) O tratamento for efectuado no contexto das actividades de um estabelecimento do responsável pelo tratamento situado no território desse Estado-membro; se o mesmo responsável pelo tratamento estiver estabelecido no território de vários Estados-membros, deverá tomar as medidas necessárias para garantir que cada um desses estabelecimentos cumpra as obrigações estabelecidas no direito nacional que lhe for aplicável;

4.º da Lei de Proteção de Dados Pessoais em termos que não correspondem inteiramente ao disposto na Diretiva, mas que devem ser entendidos no mesmo sentido segundo uma interpretação conforme à Diretiva ([7]).

Das normas de conexão *ad hoc* contidas nesta lei resultava a aplicação das suas normas materiais em matérias que, por dizerem respeito a direitos de personalidade de estrangeiros, são pelo Direito de Conflitos geral submetidas à lei estrangeira, em termos que são adiante referidos. Estas normas materiais eram, por conseguinte, *suscetíveis de aplicação necessária* ([8]).

O Reg. (UE) n.º 2016/679, Relativo à Proteção das Pessoas Singulares no que diz Respeito ao Tratamento de Dados Pessoais e à Livre Circulação desses Dados (*Regulamento Geral sobre a Proteção de Dados*, doravante RGPD) veio estabelecer um desenvolvido complexo de regras materiais uniformes sobre a proteção de dados pessoais.

O RGPD aplica-se ao tratamento de dados pessoais por meios total ou parcialmente automatizados, bem como ao tratamento por meios não automatizados de dados pessoais contidos em ficheiros ou a eles destinados (art. 2.º/1). São excluídos alguns tratamentos de dados pessoais, designadamente o efetuado por uma pessoa singular no exercício de atividades exclusivamente pessoais ou domésticas (n.º 2/c) ([9]).

O RGPD abrange por isso, designadamente, o tratamento de dados pessoais por fornecedores de bens e serviços na internet.

O RGPD visa não só a proteção de dados pessoais de pessoas singulares, mas também assegurar a livre circulação desses dados no interior da União (art. 1.º) ([10]).

---

b) O responsável pelo tratamento não estiver estabelecido no território do Estado-membro, mas num local onde a sua legislação nacional seja aplicável por força do direito internacional público;
c) O responsável pelo tratamento não estiver estabelecido no território da Comunidade e recorrer, para tratamento de dados pessoais, a meios, automatizados ou não, situados no território desse Estado-membro, salvo se esses meios só forem utilizados para trânsito no território da Comunidade."

7 - O art. 4.º contém um n.º 4, segundo o qual a "lei aplica-se à videovigilância e outras formas de captação, tratamento e difusão de sons e imagens que permitam identificar pessoas sempre que o responsável pelo tratamento esteja domiciliado ou sedeado em Portugal ou utilize um fornecedor de acesso a redes informáticas e telemáticas estabelecido em território português."

8 - Sobre o conceito de norma suscetível de aplicação necessária, ver Luís de LIMA PINHEIRO – *Direito Internacional Privado*, vol. I – *Introdução e Direito de Conflitos – Parte Geral*, 3.ª ed., Coimbra, Almedina, 270 e segs.

9 - Segundo o Considerando n.º 18, as atividades pessoais ou domésticas poderão incluir a troca de correspondência e a conservação de listas de endereços ou a atividade das redes sociais e do ambiente eletrónico no âmbito dessas atividades. Todavia, o RGPD é aplicável aos responsáveis pelo tratamento e aos subcontratantes que forneçam os meios para o tratamento dos dados pessoais dessas atividades pessoais ou domésticas.

10 - O Considerando n. º 2 relaciona estes objetivos com o objetivo mais geral de contribuir para a realização de um espaço de liberdade, segurança e justiça e de uma união económica, para o progresso económico e social, a

O art. 2.º/4 determina que o RGPD não prejudica a aplicação da Diretiva 2000/31/CE (*Diretiva sobre comércio eletrónico*) nomeadamente as normas que limitam a responsabilidade dos prestadores intermediários de serviços nos casos de simples transporte, armazenagem temporária [*caching*] e armazenagem em servidor e estabelecem a ausência de dever geral de vigilância. Mas isto não significa que o regime do RGPD não seja aplicável à proteção de dados pessoais no contexto de serviços da sociedade de informação, até porque essa Diretiva salvaguarda a aplicação plena da legislação europeia sobre proteção de dados pessoais aos serviços da sociedade da informação (Considerando n.º 14) e exclui do seu âmbito de aplicação as questões respeitantes aos serviços da sociedade da informação abrangidas pelo regime europeu da proteção de dados pessoais (art. 1.º/5/b) ([11]).

Já o funcionamento do Direito de Conflitos interno em matéria de responsabilidade extracontratual é limitado pela interpretação dessa Diretiva feita pelo TUE no caso *eDate Advertising,* visto que a matéria parece ser abrangida pelo domínio coordenado (art. 2.º/h/i) ([12]).

De entre *as definições oferecidas pelo art 4.º* importa salientar as de "dados pessoais", já referida, "tratamento", "consentimento" e, mais adiante (II), a de "Estabelecimento principal".

Entende-se por "Tratamento" uma operação ou um conjunto de operações efetuadas sobre dados pessoais ou sobre conjuntos de dados pessoais, por meios automatizados ou não automatizados, tais como a recolha, o registo, a organização, a estruturação, a conservação, a adaptação ou alteração, a recuperação, a consulta, a utilização, a divulgação por transmissão, difusão ou qualquer outra forma de disponibilização, a comparação ou interconexão, a limitação, o apagamento ou a destruição (2).

Entende-se por "Consentimento" do titular de dados, uma manifestação de vontade, livre, específica, informada e explícita, pela qual o titular dos dados aceita, mediante declaração ou ato positivo inequívoco, que os dados pessoais que lhe dizem respeito sejam objeto de

---

consolidação e a convergência das economias a nível do mercado interno e para o bem-estar das pessoas singulares.

11 - Em sentido diferente, Daphne KELLER – "The Right Tools: Europe's Intermediary Liability Laws and the 2016 General Data Protection Regulation", *LSN Cyberspace Law eJournal, Vol. 22 No. 19, 03/15/2017* (acessível em SSRN), 66 e segs.

12 - Ver também Pedro MIGUEL ASENSIO – "Competencia y Derecho aplicable en el reglamento general sobre protección de datos de la Unión Europea", *Rev. Española de Derecho Internacional* 69 (2017) 75-108, 106.

tratamento (11). Esta definição torna claro que o conceito de consentimento relevante para o Regulamento é autónomo e não depende da lei reguladora do contrato ([13]).

No célebre caso *Google* (2014) ([14]), o TUE entendeu que o artigo 2º/b e d da Diretiva 95/46/CE, deve ser interpretado no sentido de que, por um lado, a atividade de um motor de busca que consiste em encontrar informações publicadas ou inseridas na Internet por terceiros, indexá-las automaticamente, armazená-las temporariamente e, por último, pô-las à disposição dos internautas por determinada ordem de preferência deve ser qualificada de "tratamento de dados pessoais", na aceção do artigo 2.º/b, quando essas informações contenham dados pessoais, e de que, por outro, o operador desse motor de busca deve ser considerado "responsável" pelo dito tratamento, na aceção do referido artigo 2º/d.

No caso *Wirtschaftsakademie Schleswig-Holstein* (2018) ([15]), o mesmo tribunal interpretou o artigo 2.º/d da mesma Diretiva no sentido de que o conceito de "responsável pelo tratamento" engloba o administrador de uma página de fãs alojada no *Facebook*.

O RGPD também estabelece um *regime de Direito material especial sobre a transferência de dados para Estados terceiros e organizações internacionais*.

O RGPD contém ainda *inúmeras remissões para o Direito dos Estados-Membros*, que constituem em alguns casos normas de conflitos unificadas, *algumas normas de competência internacional* e uma *norma que limita o reconhecimento de decisões judiciais e administrativas de Estados terceiros*.

O RGPD revogou a Diretiva 95/46/CE com efeitos a partir de 25 de maio de 2018 ([16]).

O legislador europeu entendeu que sendo a proteção dos dados pessoais um direito fundamental e tendo a rápida evolução tecnológica e a globalização um impacto nesta matéria se tornou necessário assegurar um nível de proteção coerente e elevado das pessoas singulares e eliminar os obstáculos à circulação de dados pessoais na União através de uma uniformização das principais regras materiais na matéria ([17]).

---

13 - Ver Christian KOHLER – "Conflict of Law Issues in the 2016 Data protection Regulation of the European Union", *RDIPP* (2016) 653-675, 663 e segs.

14 - 13/5/2014 [ECLI:EU:C:2014:317].

15 - TUE 5/6/2018 [ECLI:EU:C:2018:388].

16 - Ver também art. 99.º/2.

17 - Cf. Considerandos n.ºs 1, 6 e 10. RGPD começa por recordar, no seu Considerando n.º 1, que a proteção das pessoas singulares relativamente ao tratamento de dados pessoais é um direito fundamental. O Considerando n.º 6 assinala o impacto da rápida evolução tecnológica e da globalização em matéria de proteção de dados pessoais:

- aumento significativo da recolha e da partilha de dados pessoais;
- a utilização de dados pessoais numa escala sem precedentes no exercício das atividades das empresas privadas e das entidades públicas;

Quer isto dizer que não se trata agora apenas de aproximar as legislações dos Estados-Membros, em termos que não dispensam a determinação do Direito estadual aplicável, mas de estabelecer um regime europeu uniforme. E esta uniformidade significa que o mesmo regime passa a ser aplicável às situações internas e às situações transnacionais, contrapondo-se assim a uma mera unificação do regime aplicável a situações transnacionais.

Com isto não se eliminam os problemas de determinação do Direito aplicável. Estes problemas colocam-se principalmente a três níveis. Primeiro, *a determinação do âmbito espacial de aplicação do RGPD* (I). Segundo, *a determinação do Direito aplicável quando o RGPD remete para o Direito dos Estados-Membros* (II). Terceiro, *a determinação do Direito estadual aplicável a questões que o RGPD não regula* (III), ainda que por forma remissiva, como, designadamente, se passa com a maior parte das questões relativas à responsabilidade extracontratual por violação das disposições do RGPD.

O tema do presente estudo abrange estes três problemas. Mas trata-se, inevitavelmente, de uma primeira aproximação a este tema uma vez que este abrange questões que são muito vastas, complexas e controversas e que, em alguns casos, só muito recentemente começaram a ser estudadas.

Fica, em princípio, excluído do âmbito do presente trabalho o problema dos limites colocados pelo Direito Internacional Público às competências legislativa, jurisdicional e de execução dos Estados, sem prejuízo de alusões pontuais suscitadas por certas soluções legislativas ou jurisprudenciais.

- crescente disponibilização das informações pessoais de uma forma pública e global.

O mesmo Considerando afirma que as novas tecnologias devem contribuir para facilitar a livre circulação de dados pessoais na União e a sua transferência para países terceiros e organizações internacionais, assegurando simultaneamente um elevado nível de proteção dos dados pessoais.

Nos termos do Considerando n.º 10, a fim de assegurar um nível de proteção coerente e elevado das pessoas singulares e eliminar os obstáculos à circulação de dados pessoais na União, o nível de proteção dos direitos e liberdades das pessoas singulares relativamente ao tratamento desses dados deverá ser equivalente em todos os Estados-Membros.

I. ÂMBITO ESPACIAL DE APLICAÇÃO DO RGPD

Quanto ao âmbito espacial de aplicação, o art. 3.º/1 começa por determinar que o RGPD se aplica *ao tratamento de dados pessoais efetuado no contexto das atividades de um estabelecimento de um responsável pelo tratamento ou de um subcontratante situado no território da União*, independentemente de o tratamento ocorrer dentro ou fora da União.

As principais questões suscitadas pela interpretação deste preceito dizem respeito ao sentido da expressão "contexto das atividades" e do termo "estabelecimento".

Estas questões também se colocavam perante a Dir. 95/46/CE e foram objeto de decisões do TUE, mormente nos casos *Google*, *Weltimmo*, *Verein für Konsumenteninformation* e *Wirtschaftsakademie Schleswig-Holstein*.

Segundo o Considerando n.º 22 do RGPD, o *estabelecimento* pressupõe o exercício efetivo e real de uma atividade com base numa instalação estável e a forma jurídica de tal estabelecimento, quer se trate de uma sucursal quer de uma filial com personalidade jurídica, não é fator determinante nesse contexto.

O alcance da afirmação de que o tratamento pode ser considerado como inserido no contexto das atividades de um estabelecimento situado na União, mesmo que o tratamento em si não seja realizado na União, é ilustrado pela decisão proferida no já referido caso *Google* sobre o direito de apagamento ([18]).

Segundo o parecer que tinha sido elaborado pelo Grupo de Proteção das Pessoas no que diz respeito ao tratamento de dados pessoais instituído nos termos do art. 29.º da Diretiva, a noção de "contexto das atividades" implica que é aplicável a lei do Estado-Membro onde um estabelecimento do responsável de tratamento está envolvido em atividades relacionadas com o tratamento de dados ([19]). O TUE, porém, entendeu que bastava que a *Google* tivesse uma filial que realizava atividade publicitária do grupo *Google* na Espanha, mas não processava dados, para que se aplicasse o regime espanhol harmonizado pela Diretiva e condenou a

18 - 13/5/2014 [ECLI:EU:C:2014:317].

19 - Parecer n.º 8/2010, 12-14. Posteriormente o Grupo atualizou o parecer tendo em conta a decisão do TUE. Ver também, em sentido crítico, Maja BRKAN – "Data Protection and European Private International Law", *LSN Transnational Litigation/Arbitration, Private International Law, & Conflict of Laws eJournal, Vol. 2 No. 43, 07/28/2015* (acessível em SSRN), 32.

Google Spain e a *Google Inc* a suprimir os dados pessoais de um nacional espanhol nos resultados do motor de busca ([20]).

No caso *Wirtschaftsakademie Schleswig-Holstein* (2018) ([21]), o TUE reafirmou, relativamente ao *Facebook*, a aplicabilidade do Direito do Estado-Membro em que está situado um estabelecimento que realiza uma atividade publicitária mesmo que o tratamento dos dados pessoais seja feito conjuntamente por estabelecimentos situados num Estado terceiro e noutro Estado-Membro ([22]).

---

20 - Neste caso, o TUE foi confrontado com questões relativas a uma reclamação feita por um nacional espanhol domiciliado em Espanha, contra o editor de um jornal espanhol, a *Google Spain* e a *Google Inc.*, baseada no facto de que, quando um utilizador da internet inseria o nome dessa pessoa motor de busca do grupo *Google* obtinha ligações a duas páginas do jornal, nas quais figurava um anúncio de uma venda de imóveis em hasta pública decorrente de um arresto com vista à recuperação de dívidas à Segurança Social, que mencionava o nome dessa pessoa. A pessoa pedia designadamente que a *Google Spain* ou a *Google Inc.* suprimissem ou ocultassem os seus dados pessoais, para que deixassem de aparecer nos resultados de pesquisa e de figurar nas ligações do jornal.
O TUE interpretou o art. 4.º/1/a da Diretiva 95/46 no sentido de que é efetuado um tratamento de dados pessoais no contexto das atividades de um estabelecimento do responsável por esse tratamento no território de um Estado-Membro, na aceção desta disposição, quando o operador de um motor de busca cria num Estado-Membro uma sucursal ou uma filial destinada a assegurar a promoção e a venda dos espaços publicitários propostos por esse motor de busca, cuja atividade é dirigida aos habitantes desse Estado-Membro.
A *Google Spain* e a *Google Inc.* tinham argumentado que o tratamento de dados pessoais em causa no processo é efetuado exclusivamente pela *Google Inc.*, que explora o *Google Search* sem intervenção alguma da *Google Spain*, cuja atividade se limita a fornecer apoio à atividade publicitária do grupo Google que é distinta do seu serviço de motor de busca.
O TUE contrapôs que resulta designadamente dos considerandos 18 a 20 e do artigo 4.º da Diretiva 95/46 que o legislador da União pretendeu evitar que uma pessoa seja privada da proteção garantida por essa diretiva e que essa proteção seja contornada, estabelecendo um âmbito de aplicação particularmente amplo e que, a esta luz, é suficiente para essa aplicação que as atividades do operador do motor de busca e as do seu estabelecimento situado no Estado-Membro em causa estejam "indissociavelmente ligadas, uma vez que as atividades relativas aos espaços publicitários constituem o meio para tornar o motor de busca em causa economicamente rentável e que esse motor é, ao mesmo tempo, o meio que permite realizar essas atividades" (n.ºs. 54 e 56).
Segundo Geert van CALSTER – "Regulating the Internet. Prescriptive and Jurisdictional Boundaries to the EU's 'Right to Be Forgotten', *LSN Transnational Litigation/Arbitration, Private International Law, & Conflict of Laws eJournal, Vol. 2 No. 64, 11/12/2015* (acessível em SSRN), 24, referindo RYNGAERT no mesmo sentido, o TUE ter-se-á baseado tecnicamente no critério dos efeitos para justificar a competência do TUE relativamente à situação. Em rigor, porém, o problema não é só de competência jurisdicional e de competência de execução, porque estava em causa o âmbito de aplicação no espaço do regime contido na Diretiva e, por conseguinte, também um problema de competência legislativa da UE. CALSTER, op. cit., 25 e segs., chama atenção para o facto de que a competência legislativa e jurisdicional não é necessariamente acompanhada pela competência de execução e que o TUE não tem competência de execução relativamente ao *site Google.com*. Mas a competência de execução refere-se ao poder de praticar atos de coerção material. Este poder, mesmo no contexto da internet, está em princípio limitado ao território do Estado do foro (cf. *Tallinn Manual 2.0 International Group of Experts and Other Participants*, General Editor Michael Schmitt, Cambridge, Cambridge University Press, 2017, *Rule* 11). Por conseguinte, se a Diretiva puder se aplicada e se houver uma ligação significativa com a UE, o tribunal de um Estado-Membro pode condenar a sociedade-mãe *Google* a suprimir determinados dados, mas não pode praticar atos de coerção material relativamente à sociedade-mãe *Google*. Em sentido diferente, Danial NADEEM – "Territorial Limits to the European Union's Right to be Forgotten: How the CNIL Ignores Jurisdictional Basics in Its March 10, 2016 Decision Against Google", *Creighton Int'l & Comp. L.J.* 8 (2017) 182-199, 191 e segs.; e Dawn NUNZIATO – "The Fourth Year of Forgetting: The Troubling Expansion of the Right to Be Forgotten", *LSN Cyberspace Law eJournal, Vol. 23 No. 49, 07/16/2018* (acessível em SSRN), n.º 4.
21 - TUE 5/6/2018 [ECLI:EU:C:2018:388].
22 - N.ºs 57 e segs. Na mesma decisão, o TUE entendeu que autoridade de controlo desse Estado-Membro é competente para apreciar, de maneira autónoma em relação à autoridade de controlo do Estado-Membro em que está estabelecido o responsável pelo tratamento que violou as regras de proteção dos dados, a legalidade de tal

Penso que a compatibilidade desta solução com os limites colocados pelo Direito Internacional Público à competência legislativa e jurisdicional dos Estados, quando não se exija que o titular de dados seja nacional ou residente no Estado em causa, é duvidosa.

Por outro lado, resulta da decisão no caso *Verein für Konsumenteninformation* que a circunstância de a empresa responsável pelo tratamento de dados não ter filial nem sucursal num Estado-Membro não exclui que possa ter aí um estabelecimento, mas tal estabelecimento não pode existir pelo simples facto de o sítio internet da empresa em questão ser acessível nesse Estado-Membro ([23]).

Nos termos do art. 3.º/2, *o RGPD também se aplica ao tratamento de dados pessoais de titulares que residam no território da União, efetuado por um responsável pelo tratamento ou subcontratante não estabelecido na União*, quando as atividades de tratamento estejam relacionadas com:

- a) A oferta de bens ou serviços a esses titulares de dados na União, independentemente da exigência de os titulares dos dados procederem a um pagamento;

- b) O controlo do seu comportamento, desde que esse comportamento tenha lugar na União.

Aparentemente esta norma não está em sintonia com o Considerando n.º 2, retomado pelo Considerando n.º 14, que afirma que os "princípios e as regras em matéria de proteção das pessoas singulares relativamente ao tratamento dos seus dados pessoais deverão respeitar, independentemente da nacionalidade ou do local de residência dessas pessoas, os seus direitos e liberdades fundamentais, nomeadamente o direito à proteção dos dados pessoais".

---

tratamento de dados e pode exercer os seus poderes de intervenção em relação ao ente estabelecido no seu território sem ter de solicitar previamente a intervenção da autoridade de controlo do outro Estado-Membro (n.º 74).

23 - TUE 28/7/2016 [ECLI:EU:C:2016:612], n.º 76. Por conseguinte, importa avaliar tanto o grau de estabilidade da instalação como a realidade do exercício das atividades no Estado-Membro em questão (n.º 77, reafirmando decisão no caso *Weltimmo*, TUE 1/10/2015 [EU:C:2015:639], n.° 29). Quanto à questão de saber se o tratamento de dados pessoais em causa é efetuado "no contexto das atividades" desse estabelecimento, na aceção do artigo 4.°/1/a), da Diretiva 95/46, o TUE também reafirmou decisão no caso *Weltimmo* (n.º 35), assinalando que esta disposição exige que o tratamento de dados pessoais em questão seja efetuado não "pelo" próprio estabelecimento em causa, mas apenas "no contexto das atividades" (n.º 78). Nesta mesma decisão foi entendido que o artigo 4.°/1/a da Dir. 95/46/CE deve ser interpretado no sentido de que o tratamento de dados pessoais efetuado por uma empresa de comércio eletrónico é regido pelo Direito do Estado-Membro a que se destinam as atividades dessa empresa, se se constatar que essa empresa procede ao tratamento dos dados em questão no contexto das atividades de um estabelecimento situado nesse Estado-Membro. Este Estado-Membro é aquele em que se situa o estabelecimento (n.º 74). O TUE reafirma ainda o entendimento, adotado no caso *Weltimmo*, que o conceito de "estabelecimento" na aceção do artigo 4.°/1/a, da Dir. 95/46, abrange qualquer atividade real e efetiva, ainda que mínima, exercida através de uma instalação estável (n.º 75).

Há, no entanto, a registar uma divergência entre as várias versões linguísticas do RGPD a este respeito. Enquanto as versões portuguesa e espanhola se referem a titulares que residam na União ["titulares residentes no território da União", "*interesados que residan en la Unión*"], as versões inglesa, francesa, alemã e italiana referem-se a titulares que se encontrem na União ["*who are in the Union*", "*personnes concernées qui se trouvent sur le territoire de l'Union*","*betroffenen Personen, die sich in der Union befinden*", "*interessati che si trovano nell'Unione*"]. Tendo em conta que a Proposta de Regulamento nestas versões linguísticas se referia à residência, e que esta referência foi afastada, e o Considerando n.º 14, é forçoso concluir que basta que os titulares se encontrem no território da União no momento em que os bens ou serviços são oferecidos ou que o comportamento é controlado, o que não garante a existência de uma ligação significativa com a União ([24]).

Estender o âmbito de aplicação do RGPD a casos em que nem o responsável pelo tratamento ou o subcontratante estão estabelecidos na União nem o titular dos dados é nacional ou residente na União, porém, constitui uma solução de duvidosa compatibilidade com os limites colocados pelo Direito Internacional Público à competência legislativa dos Estados. *A tutela do direito à proteção dos dados pessoais pelo Direito da União deve fundamentar-se numa ligação significativa com a União*.

Em todo o caso, importa sublinhar que o RGPD só se aplica ao tratamento efetuado por ente não estabelecido na União quando o titular dos dados se encontrar território da União e se verificar um dos dois pressupostos adicionais anteriormente referidos.

Segundo o Considerando n.º 23, a fim de determinar se o responsável pelo tratamento ou subcontratante oferece ou não bens ou serviços aos titulares dos dados que se encontrem na União, há que determinar em que medida é evidente a sua intenção de oferecer serviços a titulares de dados num ou mais Estados-Membros da União. O mero facto de estar disponível na União um sítio *web* do responsável pelo tratamento ou subcontratante ou de um intermediário, um endereço eletrónico ou outro tipo de contactos, ou de ser utilizada uma língua de uso corrente no país terceiro em que o referido responsável está estabelecido, não é suficiente para determinar a intenção acima referida, mas há fatores, como a utilização de uma língua ou de uma moeda de uso corrente num ou mais Estados-Membros, com a possibilidade de encomendar bens ou serviços nessa outra língua, ou a referência a clientes

24 - Em sentido diferente, MIGUEL ASENSIO, "Competencia y Derecho aplicable…", *loc. cit.*, 84-85.

ou utilizadores que se encontrem na União, que podem ser reveladores de que o responsável pelo tratamento tem a intenção de oferecer bens ou serviços a titulares de dados na União.

Este entendimento encontra-se próximo do critério da atividade dirigida tal como ele tem sido concretizado pela jurisprudência do TUE sobre o regime da competência internacional nos contratos com consumidores, designadamente a decisão proferida nos casos *Peter Pammer e Hotel Alpenhof* relativamente ao art. 15.º/1/c do Regulamento Bruxelas I ([25]).

Há, no entanto, diferenças, designadamente porque o regime especial de competência em matéria de contratos com consumidores, à semelhança da norma de conflitos especial sobre o Direito aplicável aos contratos com consumidores contida no Regulamento Roma I, pressupõe a celebração de um contrato, o que não é o caso do RGPD ([26]).

Por conseguinte, por um lado, não basta para a aplicação do RGPD que haja uma oferta de bens ou serviços num *site* da internet que possam ser adquiridos por titulares de dados que se encontram na União ([27]), sendo necessário demonstrar uma intenção de oferecer estes bens ou serviços a estes titulares. Por outro, porém, subsiste considerável incerteza sobre os indícios que podem ser considerados relevantes para demonstrar tal intenção e sobre o seu peso ([28]).

Segundo o Considerando n.º 24, a fim de determinar se uma atividade de tratamento pode ser considerada "controlo do comportamento" de titulares de dados, deverá determinar-se se essas pessoas são seguidas na internet e a potencial utilização subsequente de técnicas de tratamento de dados pessoais que consistem em definir o perfil de uma pessoa singular,

---

25 - Cf. TUE 7/12/2010, nos casos *Peter Pammer e Hotel Alpenhof* [*in* http://curia.europa.eu]. Ver também Daniel COOPER e Cristopher KUNER – "Data Protection Law and International Dispute Resolution", *RCADI* 382 (2015) 9-174 (publicado em 2017), 123-124.

26 Como observa MIGUEL ASENSIO, "Competencia y Derecho aplicable…", *loc. cit.*, 85.

27 - Como resultava da interpretação da Proposta de Regulamento feita por BRKAN, "Data Protection…", *loc. cit.*, 35.

28 - O art. 1.º/6 do Regulamento sobre Bloqueio Geográfico (Reg. (UE) 2018/302) determina que "não se pode considerar, apenas com base nos elementos a seguir indicados, que o comerciante dirige atividades para o Estado-Membro da residência habitual ou do domicílio do consumidor caso, ao agir em conformidade com os artigos 3.º, 4.º e 5.º do presente regulamento, não bloqueie nem limite o acesso dos consumidores a uma interface em linha, não redirecione os consumidores para uma interface em linha com base na nacionalidade ou no local de residência dos consumidores distinta da interface em linha a que os consumidores tenham tentado aceder inicialmente, não aplique condições gerais de acesso diferentes quando vende bens ou presta serviços nas situações previstas no presente regulamento, ou aceite instrumentos de pagamento emitidos noutro Estado-Membro numa base não discriminatória. Também não se pode considerar, apenas com base nesses elementos, que o comerciante dirige atividades para o Estado-Membro da residência habitual ou do domicílio do consumidor, caso preste informações e assistência ao consumidor após a celebração de um contrato resultante do cumprimento do presente regulamento pelo comerciante".

especialmente para tomar decisões relativas a essa pessoa ou analisar ou prever as suas preferências, o seu comportamento e as suas atitudes.

BRKAN refere, relativamente à Proposta de Regulamento, que os elementos de interpretação não são conclusivos sobre o sentido que deve ser atribuído a este preceito: uma interpretação restrita, que abrange apenas as empresas estabelecidas em terceiros Estados que tratam a informação para fins económicos (como o *Google* e o *Facebook*), ou uma interpretação ampla, que abrangeria também o processamento de dados por autoridades públicas, como a NSA ([29]).

A este respeito, deve notar-se que o RGPD exclui a sua aplicação ao tratamento efetuado no exercício de atividades não sujeitas ao Direito da União (art. 2.º/2/a) ou efetuado pelas autoridades competentes para efeitos de prevenção, investigação, deteção e repressão de infrações penais ou da execução de sanções penais, incluindo a salvaguarda e a prevenção de ameaças à segurança pública (art. 2.º/2/d).

Este pressuposto de aplicação do RGPD parece pensado principalmente para os casos em que a colocação de arquivos e programas informáticos no equipamento do utilizador que permitem o acesso a informação (como os *cookies*) não tem lugar no quadro da oferta de bens e serviços ([30]).

Os casos em que se justifica a aplicação do regime do RGPD apesar do tratamento não ser feito no território de um Estado-Membro estão, em princípio, abrangidos pelos critérios de conexão do art. 3.º/2, razão por que não se deveria manter a interpretação extensiva do "contexto de atividades" de um estabelecimento situado num Estado-Membro feita pelo TUE no caso *Google*.

É importante uma certa contenção no exercício de competências legislativas estaduais em relação à internet, uma vez que leis com um âmbito de aplicação no espaço muito vasto entram facilmente em conflito com leis de outros Estados, originando problemas de conflitos de deveres para os seus destinatários e de reconhecimento noutros Estados de decisões nelas baseadas ([31]).

---

29 - "Data Protection…", *loc. cit.*, 35-36.

30 - Neste sentido, MIGUEL ASENSIO, "Competencia y Derecho aplicable…", *loc. cit.*, 86. Ver ainda KELLER, "The Right Tools…", *loc. cit.*, 58.

31 - Ver as considerações de Christopher KUNER – "The Internet and the Global Reach of EU Law", *LSN Cyberspace Law eJournal, Vol. 22 No. 15, 03/01/2017* (acessível em SSRN), 32-33.

O art. 3.º/3 acrescenta que o RGPD se aplica ao tratamento de dados pessoais por um responsável pelo tratamento estabelecido não na União, mas num lugar em que se aplique o Direito de um Estado-Membro por força do Direito Internacional Público.

O Direito de um Estado-Membro é aplicável por força do Direito internacional Público por exemplo numa missão diplomática ou num posto consular de um Estado-Membro (Considerando n.º 25).

O RGPD abandonou o critério de conexão estabelecido no art. 4.º/1/c da Diretiva sobre Proteção de Dados Pessoais – localização de meios para tratamento de dados pessoais, a meios, automatizados ou não, no território de um Estado-Membro, salvo se esses meios só forem utilizados para trânsito no território da Comunidade –, por se entender que este critério conduzia um âmbito de aplicação excessivo do regime europeu, incluindo casos que não têm uma ligação significativa com a UE ([32]).

32 - Ver MIGUEL ASENSIO, "Competencia y Derecho aplicable…", *loc. cit.*, 80-81.

II. DETERMINAÇÃO DO DIREITO APLICÁVEL QUANDO O RGPD REMETE PARA O DIREITO DOS ESTADOS-MEMBROS

O RGPD contém inúmeras remissões para o Direito dos Estados-Membros, que seria fastidioso enumerar aqui.

Em boa parte dos casos, *estas remissões são acompanhadas de uma norma de conflitos que atribui competência do Direito do Estado a que o responsável do tratamento ou o subcontratante estão sujeitos*.

É que se passa nos arts. 6.º/3, 14.º/5/c, 17.º/1/e /3/b, 22.º/2/b, 23.º/1, 26.º/1, 49.º/1/d e /4 e 85.º/2 (conjugado com o Considerando n.º 153).

O responsável pelo tratamento ou o subcontratante estão certamente sujeitos ao Direito do Estado em que estão estabelecidos. Mas suscitam-se dúvidas quando tenham uma pluralidade de estabelecimentos em diferentes Estados-Membros. O art. 4.º/16 contém uma definição de estabelecimento principal que é pelo menos relevante para determinar a autoridade de controlo principal. Segundo esta definição, no "que se refere a um responsável pelo tratamento com estabelecimentos em vários Estados-Membros, o local onde se encontra a sua administração central na União, a menos que as decisões sobre as finalidades e os meios de tratamento dos dados pessoais sejam tomadas noutro estabelecimento do responsável pelo tratamento na União e este último estabelecimento tenha competência para mandar executar tais decisões, sendo neste caso o estabelecimento que tiver tomado as referidas decisões considerado estabelecimento principal" ([33]).

Quando os dados sejam tratados por um estabelecimento secundário considera-se o ente sujeito ao Direito do Estado deste estabelecimento ou ao Direito do Estado de estabelecimento principal?

A favor da competência do Direito do Estado-Membro em que está situado o estabelecimento que trata os dados pode invocar-se o critério em princípio relevante para determinar o âmbito espacial de aplicação do RGPD (art. 3.º/1) e a decisão no caso *Weltimmo* ([34]), relativa ao Direito aplicável à proteção de dados nos termos da Dir. 95/46/CE. Em sentido

33 - Por acréscimo, no "que se refere a um subcontratante com estabelecimentos em vários Estados-Membros, o local onde se encontra a sua administração central na União ou, caso o subcontratante não tenha administração central na União, o estabelecimento do subcontratante na União onde são exercidas as principais atividades de tratamento no contexto das atividades de um estabelecimento do subcontratante, na medida em que se encontre sujeito a obrigações específicas nos termos do presente regulamento".
34 - *Supracit.*, n.ºs 24 e segs.

contrário, pode argumentar-se que o critério relevante para determinar a autoridade de controlo principal para o tratamento transfronteiriço é o do estabelecimento principal. Será desejável que o TUE esclareça o ponto.

Em alguns casos estabelecem-se *critérios de conexão diferentes*.

Assim, no que refere à atuação de membros ou pessoal da autoridade de controlo de um Estado-Membro noutro Estado-Membro, o RGPD determina a aplicação do Direito do Estado-Membro em que atuam, incluindo a responsabilidade por danos causados no decurso de tais atividades (art. 62.º/3 a 5).

Por outro lado, os dados pessoais que constem de documentos oficiais na posse de uma autoridade pública ou de um organismo público ou privado para a prossecução de atribuições de interesse público podem ser divulgados pela autoridade ou organismo nos termos do Direito da União ou do Estado-Membro que for aplicável à autoridade ou organismo público (art. 86.º).

Noutros casos, *a remissão não é acompanhada por um critério de conexão*. Nestes casos, cabe ao Direito interno dos Estados-Membros determinar o âmbito de aplicação da sua lei. Poderão fazê-lo mediante uma mera norma de conflitos unilateral *ad hoc*, i.e., que se limita a definir o âmbito espacial de aplicação das normas materiais em causa, ou, em princípio, formular normas de conflitos bilaterais, que tanto remetam para lei do foro como para a lei de outros Estados-Membros.

Não é inteiramente clara a razão por que, nestes casos, o RGPD não define o critério de conexão relevante. De todo o modo, parece que esta opção não preclude que os Estados-Membros utilizem o critério do estabelecimento do responsável do tratamento ou do subcontratante. No sentido do recurso a este critério, em matérias que digam respeito aos direitos e aos deveres destes entes, pesa o argumento da coerência sistemática com a solução favorecida pelo RGPD. Em sentido contrário, pode argumentar-se que se deveria aplicar uma lei com que os titulares dos dados tenham uma ligação especialmente estreita, visto que o RGPD tem como primeiro objetivo a proteção dos direitos dos titulares. Esta questão será retomada no ponto seguinte.

Já *a localização dos dados eletrónicos é problemática e não me parece constituir um elemento de conexão idóneo para o Direito Internacional Privado*, na determinação do Direito aplicável à proteção de dados pessoais ([35]).

Os dados pessoais são informações, e as informações são criações do espírito e não coisas corpóreas. Os dados, enquanto tais, não têm uma localização física; o que tem uma localização física são os seus suportes materiais. Os dados pessoais eletrónicos podem ser inscritos em diversos suportes, designadamente servidores e discos rígidos de computadores pessoais. No caso dos dados pessoais tratados por empresas, a tendência atual é para estarem armazenados ao abrigo da prestação de serviços de *cloud computing*. Não só o lugar de armazenamento dos ficheiros que contêm esses dados pode resultar de opções meramente técnicas das empresas que prestam serviços na internet, sem qualquer outra conexão com as empresas ou com os titulares de dados, como também segmentos do mesmo ficheiro podem estar armazenados em servidores localizados em diferentes Estados.

Para terminar este ponto, importa assinalar que entre estas remissões para o Direito dos Estados-Membros se conta a do art. 85.º, que determina que *os Estados-Membros conciliam por lei o direito à proteção de dados pessoais nos termos do Regulamento com o direito à liberdade de expressão e de informação* consagrado pelo art. 11.º da Carta, incluindo o tratamento para fins jornalísticos e para fins de expressão académica, artística ou literária (n.º 1 e Considerando n.º 153) ([36]).

Por conseguinte, a ponderação do direito à proteção de dados pessoais com a liberdade de expressão e o direito de informação depende em vasta medida das leis dos Estados-

---

35 - Já é mais controverso se constitui um elemento de conexão idóneo para a delimitação da jurisdição dos Estados ao abrigo do Direito Internacional Público – ver *Tallinn Manual 2.0 International Group of Experts and Other Participants*, Rule 1, n.º 4, e Rule 2, n.º 11; *Microsoft* v. *United States*, decidido em segunda instância pelo *United States Court of Appeals for the Second Circuit* (2016) (acessível em https://cases.justia.com/federal/appellate-courts/ca2/14-2985/14-2985-2016-07-14.pdf?ts=1468508412); Keane WOODS – "Against Data Exceptionalism", *LSN Transnational Litigation/Arbitration, Private International Law, & Conflict of Laws eJournal, Vol. 3 No. 16, 03/24/2016* (acessível em SSRN), 734 e segs. e 754 e segs.; CHRISTAKIS, Theodore – "Data, Extraterritoriality and International Solutions to Transatlantic Problems of Access to Digital Evidence. Legal Opinion on the Microsoft Ireland Case (Supreme Court of the United States)", *LSN Cyberspace Law eJournal, Vol. 23 No. 2, 01/10/2018* (acessível em SSRN), 24 e segs., mas vindo a defender soluções que não se baseiam no lugar de armazenamento dos dados nem no lugar de acesso aos dados; e Sean WATTS e Theodore RICHARD – "Baseline Territorial Sovereignty and Cyberspass", *LSN Public International Law: Foreign Relations & Policy Law eJournal, Vol. 5 No. 18, 03/30/2018* e *LSN Cyberspace Law eJournal, Vol. 23 No. 33, 04/05/2018* (acessível em SSRN), 851 e segs.

36 - Tal deverá ser aplicável, em especial, ao tratamento de dados pessoais no domínio do audiovisual e em arquivos de notícias e hemerotecas (Considerando n.º 153). A fim de ter em conta a importância da liberdade de expressão em qualquer sociedade democrática, há que interpretar de forma lata as noções associadas a esta liberdade, como por exemplo o jornalismo (Considerando n.º 153).

Membros, colocando a questão de saber quais as soluções materiais que devem ser adotadas e qual o seu âmbito de aplicação no espaço.

Relativamente ao art 9.º da Diretiva 95/46/CE, que constitui o precedente normativo desta disposição, o TUE decidiu no caso *Satakunnan Markkinapörssi* e *Satamedia* que para obter uma ponderação equilibrada entre os dois direitos fundamentais, as derrogações e limitações à proteção de dados pessoais devem operar dentro dos limites do estritamente necessário ([37]).

A Proposta inicial do Regulamento Roma II Sobre a Lei Aplicável às Obrigações Não Contratuais estabelecia, no art. 6.º/1, que a "lei aplicável à obrigação extracontratual resultante de uma violação do direito à vida privada ou dos direitos de personalidade é a lei do foro quando a aplicação da lei designada pelo artigo 3º seja contrária aos princípios fundamentais do foro em matéria de liberdade de expressão e de informação".

Por conseguinte, aplicar-se-ia à responsabilidade extracontratual por violação da privacidade a regra geral da competência da lei do lugar do dano, mas a lei do foro sobrepor-se-ia à lei estrangeira competente quando tal fosse exigido por princípios fundamentais da lei do foro em matéria de liberdade de expressão e de informação. Esta regra foi excluída da versão final devido a divergências irreconciliáveis com o Parlamento Europeu.

O art. 85.º do RGPD não impõe a aplicação da lei do foro a esta ponderação, como sucedia nessa Proposta. Pelo contrário, o Considerando n.º 153 aponta, quanto às isenções e derrogações relativas ao tratamento realizado para fins jornalísticos ou para fins de expressão académica, artística ou literária (previstas no art. 85.º/2) para a prevalência do Direito do Estado-Membro a que está sujeito o responsável pelo tratamento.

Em todo o caso, parece defensável que estando em causa uma ponderação de direitos fundamentais, se aplique a lei do foro sempre que a situação tenha uma ligação significativa com o Estado do foro ou com outro Estado (Estado-Membro ou terceiro) em que vigorem conceções fundamentais semelhantes.

Para o efeito, parece de preferir a formulação de uma disposição especial tendo por objeto esta questão, e que defina as conexões relevantes com o Estado do foro, atendendo à

37 - TUE 16/12/2008 [ECLI:EU:C:2008:727], n.º 56. Para uma comparação das soluções adotadas pelos Estados-Membros na transposição deste preceito, ver David ERDOS – "European Union Data Protection Law and Media Expression: Fundamentally Off Balance", *Int. Comp. L. Q.* 65 (2016) 139-184, 150 e segs.

interpretação das normas constitucionais em jogo e aos métodos e critérios de ponderação com respeito à colisão de direitos fundamentais.

III. DETERMINAÇÃO DO DIREITO ESTADUAL APLICÁVEL A QUESTÕES QUE O RGPD NÃO REGULA

A determinação do Direito aplicável às questões de Direito privado que o RGPD não regula tem de basear-se no Direito de Conflitos geral.

Na ordem jurídica portuguesa, o art. 27.º/1 CC estabelece que "Aos direitos de personalidade, no que respeita à sua existência e tutela e às restrições impostas ao seu exercício, é também aplicável a lei pessoal."

Daqui decorre que a atribuição dos direitos, o seu conteúdo e as restrições impostas ao seu exercício são regidos pela lei pessoal. No que se refere às restrições impostas ao exercício do direito, a competência da lei pessoal abrange tanto as restrições legais como a validade e efeitos das limitações voluntárias.

Embora o art. 27.º/1 atribua à lei pessoal a tutela do direito, deve entender-se que a tutela geral – responsabilidade civil por violação de direitos de personalidade – está submetida à lei reguladora da responsabilidade extracontratual ([38]).

Quanto às formas de tutela específica, é necessário ter em conta o disposto no n.º 2 do mesmo artigo, segundo o qual "O estrangeiro ou apátrida não goza, porém, de qualquer forma de tutela jurídica que não seja reconhecida na lei portuguesa". Este preceito suscita algumas dúvidas da interpretação. Tem-se entendido que junto aos tribunais portugueses só poderão ser atuadas as formas de tutela específica (providências preventivas ou repressivas) que sejam admitidas quer pela lei pessoal estrangeira quer pela lei portuguesa ([39]), o que representa um caso de conexão cumulativa. Também já se defendeu tratar-se de uma norma de Direito dos Estrangeiros ([40]), o que conduz ao mesmo resultado prático.

Estes entendimentos não levam em linha de conta a delimitação entre questões processuais, que estão submetidas necessariamente à *lex fori*, e questões substantivas. O preceito pode ser entendido em conformidade com a reserva de competência da lei

38 - Cf. J. BAPTISTA MACHADO – *Lições de Direito Internacional Privado*, (apontamentos das aulas teóricas do ano letivo de 1971/1972 na Faculdade de Direito de Coimbra), 2.ª ed., Coimbra, Almedina, 1982, 343. Sobre as normas de conflitos aplicáveis à violação do *right of publicity*, ver ELSA DIAS OLIVEIRA – "A relevância do *right of publicity* no âmbito da propriedade intelectual", *in Est. de Direito Intelectual/José de Oliveira Ascensão*, 209-232, Coimbra, Almedina, 2015, 228 e segs.

39 - BAPTISTA MACHADO, *Lições*…, 343, e Rabindranath CAPELO DE SOUSA – *O Direito Geral de Personalidade*, Coimbra, Coimbra Editora, 1995, 504.

40 - António MARQUES DOS SANTOS – *Direito Internacional Privado. Sumários*, 2.ª ed., Lisboa, AAFDL, 1987, 246 e seg.

portuguesa, enquanto *lex fori*, em matéria processual ([41]). Nesta ordem de ideias, a lei pessoal estrangeira decide sobre quais as pretensões que o interessado pode atuar, a lei portuguesa sobre quais os meios processuais por que estas pretensões podem ser atuadas. As leis em presença são, em princípio, de aplicação distributiva e não cumulativa embora, em resultado, possa acontecer que certas pretensões fundadas na lei pessoal estrangeira não encontrem meio processual adequado para a sua atuação em tribunais portugueses.

Este raciocínio já não vale para as formas de autotutela. Estas formas de autotutela têm de ser concedidas pela lei pessoal estrangeira; quando envolvam a utilização de meios coercivos têm também de ser permitidas pela lei portuguesa, uma vez que a utilização de meios coercivos depende do Direito local ([42]).

Por outro lado, quanto às formas de tutela específica de direitos de personalidade cuja violação se deva considerar abrangida pelo Regulamento Roma II apesar da exclusão estabelecida no art. 1.º/2/g ([43]), importa atender ao disposto no art. 15.º/d deste Regulamento que sujeita à lei reguladora da obrigação extracontratual "as medidas que um tribunal pode tomar para prevenir ou fazer cessar o dano", nos "limites dos poderes conferidos ao tribunal pelo seu direito processual". Parece, pois, que as formas de tutela específica dependerão neste caso da lei designada pelas normas de conflitos do Regulamento, com os limites decorrentes da competência da *lex fori* em matéria processual. Como adiante se assinalará, deve entender-se que o Regulamento Roma II não abrange a responsabilidade pela violação de direitos conferidos pelo RGPD aos titulares de dados pessoais.

Embora o princípio da personalidade aponte no sentido da competência da lei pessoal para determinar a atribuição dos direitos de personalidade e o seu conteúdo, a solução adotada pela maioria dos sistemas vai no sentido de estas questões serem submetidas à lei reguladora da responsabilidade extracontratual ([44]). Neste sentido invoca-se, designadamente, a vantagem de evitar o *dépeçage* entre a lei reguladora do direito de personalidade e a lei reguladora da responsabilidade pela sua violação; a eficácia *erga omnes* dos direitos de personalidade que reclama a utilização de elementos de conexão que sejam facilmente

41 - Ver Luís de LIMA PINHEIRO – *Direito Internacional Privado*, vol. II – *Direito de Conflitos - Parte Especial*, 4.ª ed., Coimbra, Almedina, 2015, § 52.
42 - Salvo tratado internacional em sentido diferente.
43 - Ver, sobre o ponto, LIMA PINHEIRO, *Direito Internacional Privado*, vol. II, *op. cit.*, 474-475, com mais referências.
44 - Ver, designadamente, *J. von Staudingers Kommentar zum Bürgerlichen Gesetzbuch mit Einführungsgesetz und Nebengesetzen, Einführungsgesetz zum Bürgerlichen Gesetzbuche, Art 38 – 42 EGBGB, Neubearbeitung 2001* /VON HOFFMANN, Berlim, Sellier- De Gruyter, Art. 40 EGBGB n.º 54; e *Münchener Kommentar zum Bürgerlichen Gesetzbuch*/JUNKER, vol. X, 6.ª ed., Munique, C. H. Beck, 2015, EGBGB Art. 40 n.º 83.

cognoscíveis por todos os interessados; e a possibilidade de a situação envolver um conflito de direitos entre o agente e o lesado que exige uma conexão neutra e previsível para ambas as partes.

Contra esta solução objeta-se que os direitos de personalidade não são relevantes apenas quando ocorre a sua violação, mas também em situações em que é apenas necessário determinar a sua existência, por exemplo, para saber se existe um direito de personalidade que seja passível de ser objecto de um negócio jurídico ([45]). Mas a esta objeção pode contrapor-se que independentemente de estar em causa uma violação, é, em princípio, possível consultar a lei do país em que se produziria o dano, caso o direito existisse e fosse violado. Trata-se de um raciocínio hipotético. Se essa lei atribuir o direito, todos os interessados sabem que a sua conduta deve respeitar esse direito, sob pena de responderem pelos danos causados pela sua violação ou de serem objecto de providências preventivas ou repressivas. Se essa lei não atribuir o direito, os interessados sabem que a sua conduta não é condicionada pelo mesmo.

Certo é que esta solução é de preferir a qualquer conexão cumulativa que faça depender a atribuição e conteúdo do direito simultaneamente da lei pessoal e da lei do foro ou da lei reguladora da responsabilidade extracontratual ([46]), que desfavoreceria a proteção dos bens de personalidade.

Dentro do âmbito de aplicação do RGPD, a atribuição dos direitos de proteção dos dados pessoais, o seu conteúdo e as restrições impostas ao seu exercício são, em princípio, regulados por este Regulamento, mesmo que a lei pessoal do titular dos dados seja a lei de um Estado terceiro, porque é diretamente aplicável a estes direitos. O que significa que *a norma de conflitos do art. 27.º/1 CC só pode desempenhar um papel relativamente à proteção de dados pessoais fora do âmbito de aplicação do RGPD ou, eventualmente, relativamente às questões que o RGPD remete para o Direito dos Estados-Membros sem definir o critério de conexão relevante*.

Relativamente a estas questões, vimos que coerência intrassistemática pode apontar para a competência do Direito do Estado a que está sujeito o responsável pelo tratamento ou o

45 - Ver ELSA DIAS OLIVEIRA – *Da Responsabilidade Civil Extracontratual por Violação de Direitos de Personalidade em Direito Internacional Privado*, Coimbra, Almedina, 2011, 292.

46 - Cp. ELSA DIAS OLIVEIRA, *Da Responsabilidade Civil Extracontratual*…, *op. cit.*, 295 e segs., defendendo que o art. 27.º CC, entendido à luz do "princípio da tutela da confiança", dever ser interpretado no sentido de a restrição contida no n.º 2 se referir não apenas às formas de tutela mas também aos direitos tutelados, quando exista um contacto entre a situação e a ordem jurídica portuguesa.

subcontratante (II), enquanto o principal objetivo do RGPD, que é o de tutelar os titulares de dados pessoais, oferece um argumento no sentido da aplicação da lei do Estado que tem a ligação mais estreita com titular dos dados.

Parece inevitável uma diferenciação, designadamente consoante estão em causa interesses públicos ou a constituição, funcionamento e atividade das autoridades de controlo, ou interesses privados.

Quando estiverem diretamente em causa interesses públicos é de esperar que os Estados-Membros que prosseguem esses interesses delimitem por meio de normas de conflitos unilaterais o âmbito de aplicação das normas que os tutelam.

As questões relativas à constituição, funcionamento e atividades das autoridades de controlo deverão, em princípio, estar submetidas ao Direito do Estado-Membro a que pertence a autoridade.

Nos outros casos, parece-me que, em princípio, é de preferir, em conformidade com o princípio da personalidade, a aplicação da lei de um Estado que tenha uma ligação estreita com o titular dos dados. Excetuam-se os casos em que estejam em causa interesses privados que não interfiram diretamente com interesses do titular dos dados, designadamente do responsável pelo tratamento e/ou do subcontratante.

Na determinação dessa lei importa também atender à conveniência de aplicar a mesma lei que rege a responsabilidade extracontratual pela violação dos direitos do titular dos dados e de uma convergência entre a lei aplicável e o foro competente.

Perante o art. 5.º/3 do Regulamento Bruxelas I (competência internacional em matéria extracontratual), o TUE entendeu no caso *eDate Advertising* (2011) ([47]) que o critério do lugar do dano causado a um direito de personalidade suscita dificuldades quando a violação resulta de um conteúdo introduzido na internet, visto que este é acessível universalmente, e, por isso, carece de adaptações. Nesta base, o tribunal entendeu que a competência se pode fundamentar na localização do centro de interesses do lesado, que corresponde, em princípio, à sua residência habitual ([48]).

O TUE acrescentou que uma pessoa pode ter o centro dos seus interesses igualmente num Estado-Membro onde não reside habitualmente, na medida em que outros indícios, como o

47 - 25/10/2011 [*in www.curia.europa.eu*].
48 - N.ºs 47-49.

exercício de uma atividade profissional, podem estabelecer a existência de um nexo particularmente estreito com esse Estado ([49]).

Já tive ocasião de defender anteriormente que embora não se deva fazer uma transposição mecânica desta solução para a determinação do Direito aplicável à responsabilidade extracontratual por danos causados a direitos de personalidade através da internet, é concebível que uma solução adequada nesta matéria atenda igualmente à residência habitual do lesado ou, mais amplamente, ao seu centro de interesses ([50]).

Acrescente-se que o art. 79.º/2 do RGPD determina que os titulares de dados podem optar entre propor a ação contra o responsável pelo tratamento ou o subcontratante nos tribunais do Estado-Membro em que o responsável pelo tratamento ou o subcontratante tenham estabelecimento ou nos tribunais do Estado-Membro em que o titular dos dados tenha a sua residência habitual ([51]).

Estas considerações levam-me a concluir que é *o Direito do Estado em que o titular dos dados pessoais tem o centro dos seus interesses que está em melhor posição para reger os seus direitos no contexto da internet*.

Fora do âmbito de aplicação do RGPD esta solução só parece defensável *de iure condendo*.

Dentro do âmbito de aplicação deste RGPD, mas relativamente às questões que remete para o Direito dos Estados-Membros sem definir o critério de conexão relevante, a necessidade de evitar um excessivo fracionamento das situações, mediante a aplicação do regime do RGPD, da lei pessoal do titular dos dados e da lei reguladora da responsabilidade extracontratual, parece justificar uma redução teleológica do art. 27.º/1 CC, e a integração da lacuna daí resultante com esta solução.

Quanto às questões que o RGPD não regula, a lei reguladora dos contratos obrigacionais, definida nos termos do Regulamento Roma I, tem um papel a desempenhar relativamente a

---

49 - N.º 49.

50 - Ver propostas convergentes em ELSA DIAS OLIVEIRA – "Algumas considerações sobre a responsabilidade civil extracontratual por violação de direitos de personalidade em Direito Internacional Privado", *Cuadernos de Derecho Transnacional* 5 (2013) 139-162, 147-148 ns. 34 e 35 e, para a posição diversa desta autora, loc. cit., 160 e segs.

51 - Ver também Considerando n.º 145 e art. 82.º/6. O foro da residência habitual do titular dados é, porém, excluído, se o responsável pelo tratamento ou o subcontratante for uma autoridade de um Estado-Membro no exercício dos seus poderes públicos (n.º 2 *in fine*).

compromissos livremente assumidos pelo responsável pelo tratamento ou pelo subcontratante perante o titular dos dados ([52]).

Observe-se que quando o contrato for regido pela lei de um terceiro Estado nos termos do Regulamento Roma I, o regime do RGPD sobrepor-se-á, dentro do seu âmbito de aplicação, à lei reguladora do contrato por força própria, e não nos termos do art. 9.º/2 do Regulamento Roma I ([53]).

Na prática, porém, a questão mais importante é a da *responsabilidade extracontratual pela violação de direitos à proteção de dados pessoais* ([54]).

O art. 82.º contém algumas regras sobre a responsabilidade civil do responsável pelo tratamento ou do subcontratante perante qualquer pessoa que tenha sofrido danos materiais ou imateriais devido a uma violação do RGPD.

Estas regras:

- reconhecem a qualquer pessoa que tenha sofrido danos o direito a receber uma indemnização do responsável pelo tratamento ou do subcontratante pelos danos sofridos;

- limitam a responsabilidade dos subcontratantes aos casos de incumprimento das obrigações decorrentes do RGPD que lhes são dirigidas especificamente ou de não observância das instruções lícitas do responsável pelo tratamento;

- exoneram o responsável pelo tratamento ou o subcontratante de responsabilidade se provar que não é de modo algum responsável pelo evento que deu origem aos danos;

- estabelecem a responsabilidade solidária dos responsáveis pelo tratamento ou subcontratantes que estejam envolvidos no mesmo tratamento e sejam responsáveis por eventuais danos.

O Considerando n.º 146 fornece indicações importantes para a interpretação desta disposição.

---

52 - Ver também KOHLER, "Conflict of Law Issues…, *loc. cit.*, 671. Colocando este ponto em dúvida, com referência à supracit. decisão TUE no caso *Verein für Konsumenteninformation*, Sabine CORNELOUP – "De la loi applicable aux activités des entreprises de commerce électronique", *R. crit.* (2017) 112-122, 121-122.

53 - Neste sentido, porém, KOHLER, "Conflict of Law Issues…, *loc. cit.*, 661, e MIGUEL ASENSIO, "Competencia y Derecho aplicable…", *loc. cit.*, 104. Relativamente à Dir. 95/46/CE, ver BRKAN, "Data Protection…", *loc. cit.*, 26 e segs.

54 - MIGUEL ASENSIO, "Competencia y Derecho aplicable…", *loc. cit.*, 105-106, chama a atenção para a possibilidade de delicados problemas de delimitação entre o regime do RGPD, que depende de uma conexão autónoma, e a lei aplicável às obrigações extracontratuais, quando esteja em causa a responsabilidade por violação de regras do RGPD.

Primeiro, o conceito de dano deverá ser interpretado em sentido lato à luz da jurisprudência do Tribunal de Justiça, de uma forma que reflita plenamente os objetivos do RGPD.

Segundo, a disposição não prejudica os pedidos de indemnização por danos provocados pela violação de outras regras do Direito da União ou dos Estados-Membros.

Terceiro, os tratamentos que violem o RGPD abrangem igualmente os que violem os atos delegados e de execução adotados nos termos do RGPD e o Direito dos Estados-Membros que dê execução a regras do RGPD.

Quarto, os titulares dos dados deverão ser integral e efetivamente indemnizados pelos danos que tenham sofrido.

Por último, apesar de cada um dos responsáveis pelo tratamento ou os subcontratantes envolvidos no mesmo tratamento responder pela totalidade dos danos causados, se os processos forem associados a um mesmo processo judicial, em conformidade com o Direito dos Estados-Membros, a indemnização poderá ser repartida em função da responsabilidade que caiba a cada responsável pelo tratamento ou subcontratante pelos danos causados em virtude do tratamento efetuado, na condição de ficar assegurada a indemnização integral e efetiva do titular dos dados pelos danos que tenha sofrido.

Os outros aspetos da responsabilidade extracontratual do responsável pelo tratamento e do subcontratante, como a culpa, as causas de justificação, o nexo de causalidade e, em princípio, o cálculo da indemnização são regidos pela lei aplicável a essa responsabilidade.

Sobre a lei aplicável à responsabilidade extracontratual vigora na ordem jurídica portuguesa o *Regulamento Roma II,* mas o art. 1.º/2/g exclui do seu âmbito de aplicação as obrigações extracontratuais que decorram da violação da vida privada e dos direitos de personalidade. Embora esta exclusão dos direitos de personalidade deva ser interpretada restritivamente, parece de entender que dado o relacionamento da proteção de dados pessoais com a privacidade está excluída a responsabilidade por violação de direitos à proteção de dados pessoais ([55]).

---

55 - Bem como a violação de normas de proteção de dados pessoais que não confiram direitos subjetivos.
Cf. KOHLER , "Conflict of Law Issues…, *loc. cit.*, 673-674, e MIGUEL ASENSIO, "Competencia y Derecho aplicable…", *loc. cit.*, 105-106. Em sentido diferente, BRKAN, "Data Protection…", *loc. cit.*, 26 e segs., com mais referências. MIGUEL ASCENSIO [*loc. cit.*] defende que os interesses em presença apontam no sentido da competência da lei do lugar onde ocorre a lesão dos bens ou direitos do prejudicado, tipicamente a sua residência habitual "ou centro de interesses". Ver, com mais desenvolvimento, Id. – *Derecho Privado de Internet*, 5.ª ed., Cizur Menor (Navarra), Civitas e Thomson Reuters, 2015, 217-218. O autor invoca o paralelismo com a regra de

Importa, por isso, recorrer ao *Direito de Conflitos de fonte interna* contido no art. 45.º CC.

O n.º 1 do art. 45.º CC submete a responsabilidade extracontratual fundada quer em ato ilícito quer no risco ou em qualquer conduta lícita "à lei do Estado onde decorreu a principal atividade causadora do prejuízo; em caso de responsabilidade por omissão, é aplicável a lei do lugar onde o responsável deveria ter agido" ([56]).

No entanto, por força do n.º 2 aplica-se a lei do Estado onde se produziu o efeito lesivo quando esta considerar responsável o agente, mas não o considerar como tal a lei do país onde decorreu a sua atividade, desde que o agente devesse prever a produção de um dano, naquele país, como consequência do seu ato ou omissão.

Nos casos de violação da proteção de dados pessoais no contexto da internet *qual é o lugar da atividade causadora do prejuízo*?

Creio que tanto o lugar onde são tratados os dados pessoais como o lugar em que o responsável pelo tratamento ou subcontratante acede à rede ([57]) poderiam ser relevantes como lugar da atividade causadora de prejuízo. Normalmente coincidem. Se esta coincidência não se verificar, deve relevar, como lugar da atividade principal, aquele em que os dados foram tratados.

A determinação dos lugares onde os dados são tratados e onde o agente acede à rede pode suscitar grandes dificuldades. Este lugar pode não ser cognoscível pelos titulares de dados ou só o ser com custos proibitivos ([58]). Como solução de recurso pode interpretar-se o art. 45.º no sentido de o Direito do lugar do efeito lesivo ser aplicável quando não for possível determinar o lugar da atividade.

---

competência internacional do art. 79.º/2 RGPD, mas este paralelismo apontaria mais no sentido de uma aplicação alternativa da lei do Estado de estabelecimento do responsável pelo tratamento de dados (em princípio, a lei do lugar da atividade) e da lei da residência habitual do titular dos dados

56 - Ver também o art. 16.º da Convenção de Bruxelas Relativa ao Auxílio Mútuo em Matéria Penal entre os Estados-Membros da União Europeia (2000), com respeito à responsabilidade civil dos agentes de um Estado-Membro que se encontrem em missão noutro Estado-Membro.

57 - Cf. Peter MANKOWSKI – "Das Internet im Internationalen Vertrags- und Deliktsrecht", *RabelsZ.* 63 (1999) 203-294, 257. Cp. James FAWCETT e Paul TORREMANS – *Intellectual Property and Private International Law*, 2.ª ed., Oxford, Oxford University Press, 2011, n.º 16.104, entendendo que a ofensa ao bom nome e reputação é perpetrada em todos os Estados em que a informação é "descarregada" recebida, e *Dicey, Morris and Collins on the Conflict of Laws* – 15.ª ed. por LORD COLLINS OF MAPESBURY (ed. geral), Adrian BRIGGS, Andrew DICKINSON, Jonathan HARRIS, J. McCLEAN, Peter McELEAVY, Campbell McLACHLAN e C. MORSE, Londres, Sweet & Maxwell e Thompson Reuters, 2012, n.º 35-119, entendendo como lugar do delito o lugar em que a informação é "descarregada" ou acedida, pelo menos se o lesado sofre uma ofensa à sua reputação nesse lugar.

58 - Ver propostas de solução deste problema em MANKOWSKI, "Das Internet…", *loc. cit.*, 258 e segs.

Além disso, no caso de delitos cometidos através de radiodifusão, transmissão por satélite e rede informática, o risco de manipulação do elemento de conexão lugar da atividade é especialmente elevado. O operador pode facilmente deslocar o lugar da sua atuação para um Estado especialmente permissivo. A possibilidade de aplicar o Direito do lugar do efeito lesivo quando o Direito de o lugar da atividade não considerar o agente responsável não anula este risco, porque o Direito do lugar da atividade pode submeter o agente a um regime de responsabilidade menos severo que o Direito do lugar do efeito lesivo.

Este risco agravado de fraude à lei poderia ser prevenido mediante uma disposição especial segundo a qual em caso de delito cometido por estes meios o lesado pode optar entre a aplicação do Direito do lugar da atividade e a aplicação do Direito da residência habitual ou sede da administração do agente.

Em sentido próximo, o art. 139.º/1 da Lei suíça de Direito Internacional Privado confere ao lesado, com respeito às pretensões fundadas em violação de direitos de personalidade através de meios públicos de comunicação, uma escolha entre o Direito do Estado da residência habitual do lesado, contanto que o agente pudesse contar com a produção do resultado neste Estado, o Direito do Estado do estabelecimento ou residência habitual do agente e o Direito do Estado onde se produz o resultado da violação, contanto que o agente pudesse contar com a produção do resultado neste Estado.

Um segundo problema, é *o da determinação do lugar em que se produz o efeito lesivo*.

Na violação de direitos de personalidade através da colocação de um conteúdo na internet o efeito lesivo pode-se produzir em todos os lugares em que é facultado o acesso dos utilizadores à rede ([59]). Embora esta multiplicação dos lugares do efeito lesivo possa ser restringida, em certos casos, em função do conteúdo do direito de personalidade em causa ([60]), implica sempre potencialmente um fracionamento do Direito aplicável que pode levar a dificuldades dificilmente superáveis e não atende ao princípio geral da conexão mais estreita ([61]). Estas considerações justificam uma adaptação da solução conflitual, que, nos termos anteriormente referidos, se pode *até certo ponto* inspirar na jurisprudência do TUE perante o

59 - Cf. MANKOWSKI, "Das Internet…", *loc. cit.*, 269, com algumas exceções.

60 - Assim, a lesão do bom nome e reputação produz-se apenas nos Estados em que o lesado é conhecido. Com efeito, o bom nome e reputação só pode ser lesado pela afirmação ou divulgação de factos num meio social em que a pessoa atingida seja conhecida. Por razão afim, o tipo de responsabilidade extracontratual contido no art. 484.º CC português (ofensa do crédito ou do bom nome) só está preenchido quando um facto é afirmado ou divulgado no meio social em que a pessoa atingida viva ou exerça a sua atividade – cf. ANTUNES VARELA – *Das Obrigações em geral*, 10.ª ed., Coimbra, 2004, 549.

61 - Ver também MIGUEL ASENSIO, "Competencia y Derecho aplicable…", *loc. cit.*, 217-218.

art. 5.º/3 do Regulamento Bruxelas I (competência internacional em matéria extracontratual) ([62]) e no art. 79.º/2 RGPD (competência internacional para a ação de responsabilidade pela violação dos direitos conferidos pelo RGPD ao titular dos dados) ([63]).

Nesta ordem de ideias, será de considerar como lugar do efeito lesivo aquele em que o titular dos dados tenha a sua residência habitual ou, mais amplamente, o seu centro de interesses.

Em sentido convergente com o art. 4.º/3 do Regulamento Roma II, creio que se justificaria um outro desvio por aplicação da ideia do respeito da interdependência de complexos normativos, à semelhança do disposto no art. 133.º/3 da Lei suíça e no art. 41.º/2/1 da Lei de Introdução do Código Civil alemão, com a redação dada em 1999 ([64]). Segundo este desvio, se entre o agente e o lesado preexiste uma relação jurídica, será a lei aplicável a esta relação que, em princípio, regerá a responsabilidade extracontratual.

Também entendo que o Direito de Conflitos de fonte interna deveria convergir com o Regulamento Roma II quanto à admissibilidade da escolha pelas partes do Direito aplicável às obrigações não voluntárias ([65]).

---

62 - No já referido caso *eDate Advertising* (TUE 25/10/2011 [in http://curia.europa.eu], n.º 52), o TUE entendeu que em caso de alegada violação dos direitos de personalidade através de conteúdos colocados em linha num sítio na Internet, a pessoa que se considerar lesada tem a faculdade de intentar uma ação fundada em responsabilidade pela totalidade dos danos causados, quer nos órgãos jurisdicionais do Estado-Membro do lugar de estabelecimento da pessoa que emitiu esses conteúdos quer nos órgãos jurisdicionais do Estado-Membro onde se encontra o centro dos seus interesses. Esta pessoa pode igualmente, em vez de uma ação fundada em responsabilidade pela totalidade dos danos causados, interpor a sua ação nos órgãos jurisdicionais de cada Estado-Membro em cujo território esteja ou tenha estado acessível um conteúdo em linha. Estes são competentes para conhecer apenas do dano causado no território do Estado-Membro do órgão jurisdicional em que a ação foi intentada.

63 - Os titulares de dados podem optar entre propor a ação nos tribunais do Estado-Membro em que o responsável pelo tratamento ou o subcontratante tenham estabelecimento ou nos tribunais do Estado-Membro em que o titular dos dados tenha a sua residência habitual. Ver também Considerando n.º 145.

64 - O preceito da lei alemã insere esta solução numa cláusula de exceção e alarga-a à existência de uma relação de facto entre os interessados. Ver ainda Jan KROPHOLLER – *Internationales Privatrecht*, 6.ª ed., Tubinga, Mohr Siebeck, 2006, 530 e seg.; as considerações convergentes de António FERRER CORREIA – *Direito Internacional Privado. Alguns problemas*, Coimbra, Almedina, 1981, 105 e segs.; e ANABELA DE SOUSA GONÇALVES – *Da Responsabilidade Extracontratual em Direito Internacional Privado. A Mudança de Paradigma*, Coimbra, Almedina, 2013, 410-411; e as obras indicadas por Rui MOURA RAMOS – *Da Lei Aplicável ao Contrato de Trabalho Internacional*, Coimbra, Almedina, 1991, 378 n. 19. Ver ainda Dário MOURA VICENTE – *Da Responsabilidade Pré-Contratual em Direito Internacional Privado*, Coimbra, Almedina, 2001, 498 e segs., com desenvolvidas referências doutrinais e comparativas, que admite limitadamente este desvio mesmo *de iure constituto*, seguido por ELSA DIAS OLIVEIRA, *Da Responsabilidade Civil Extracontratual*…, *op. cit.*, 523-524.

65 - Ver também o art. 42.º da Lei de Introdução do Código Civil Alemão, com a redação dada em 1999. Já tenho por indefensável a admissibilidade da escolha da lei aplicável perante o Direito constituído, como sustenta NUNO PISSARRA – *O Dano Transnacional em Direito Internacional Privado. Alguns Problemas* (Diss. de Mestrado policopiada), Lisboa, 2004, 153 e segs. O legislador optou inequivocamente, no art. 45.º CC, por elementos de conexão objetivos, pelo que seria manifestamente contrário à intenção legislativa admitir a autonomia conflitual nesta matéria.

O regime que se acaba de referir é também aplicável à responsabilidade extracontratual de prestadores de serviços em linha, visto que o DL n.º 7/2004, de 7/1, interpretado em conformidade com a *Diretiva sobre Comércio Eletrónico*, não afasta a regra de conflitos do art. 45.º CC ([66]). No entanto, decorre do entendimento adotado pelo TUE, no já referido caso *eDate Advertising* (2011), que a lei designada pelo art. 45.º CC não pode estabelecer, para os prestadores de serviços estabelecidos num Estado-Membro, um regime mais rigoroso que o da lei deste Estado-Membro ([67]).

66 - Ver LIMA PINHEIRO, *Direito Internacional Privado*, vol. II, *op. cit.*, § 65 D *in fine* e 68 *B in fine*. Sobre o problema, antes da decisão do TUE no caso *eDate Advertising*, ver LIMA PINHEIRO – "Direito aplicável à responsabilidade extracontratual na *Internet*", *RFDUL* 42 (2001) 825-834, 833 e seg., e – "O Direito de Conflitos e as liberdades comunitárias de estabelecimento e de prestação de serviços", *in Seminário sobre a Comunitarização do Direito Internacional Privado*, 79-109, Coimbra, Almedina, 2005 (=*in Estudos de Direito Internacional Privado*, 357-387, Coimbra, Almedina, 2006) 102 e segs., com mais referências.
67 - N.º 67.

IV. CONSIDERAÇÕES FINAIS

Não cabendo examinar neste estudo a controvérsia suscitada por certas soluções materiais, pode afirmar-se que a vasta uniformização do Direito material aplicável à proteção de dados pessoais na UE é, em princípio, justificada. No entanto, o âmbito espacial de aplicação do RGPD parece demasiado amplo, não assegurando que existe sempre uma ligação significativa com a União Europeia.

O art. 50.º prevê a adoção das medidas necessárias para a cooperação internacional com países terceiros e organizações internacionais que são de grande importância:

- estabelecer regras internacionais de cooperação destinadas a facilitar a aplicação efetiva da legislação em matéria de proteção de dados pessoais;

- prestar assistência mútua a nível internacional no domínio da aplicação da legislação relativa à proteção de dados pessoais, nomeadamente através da notificação, comunicação de reclamações, e assistência na investigação e intercâmbio de informações, sob reserva das garantias adequadas de proteção dos dados pessoais e de outros direitos e liberdades fundamentais;

- associar as partes interessadas aos debates e atividades que visem intensificar a cooperação internacional no âmbito da aplicação da legislação relativa à proteção de dados pessoais; e

- promover o intercâmbio e a documentação da legislação e das práticas em matéria de proteção de dados pessoais, nomeadamente no que diz respeito a conflitos jurisdicionais com países terceiros.

A importância desta cooperação internacional é ilustrada por algumas decisões muito discutidas não só relativamente à proteção internacional de dados pessoais, mas também relativamente à investigação penal transfronteiriça ([68]).

A internet, como realidade global, carece de uma regulação global, que em boa parte pode ser proporcionada por organizações privadas representativas da comunidade dos participantes na internet, mas também carece, em diversos domínios, como é o caso da

68 - Ver, designadamente, CHRISTAKIS, "Data, Extraterritoriality and International Solutions…", *loc. cit.*, 35 e segs.

proteção de dados pessoais, de uma regulação por Convenções internacionais de âmbito universal ([69]).

Já se deram alguns passos no sentido da unificação internacional do regime aplicável à proteção de dados pessoais, mas com significado limitado.

Assim, o Conselho de Europa adotou em 1981 a Convenção para a Proteção das Pessoas Relativamente ao Tratamento Automatizado de Dados de Caráter Pessoal (Convenção 108), de que são partes todos os Estados-Membros do Conselho, mas que só obteve um acolhimento muito limitado de outros Estados. Em 2001, foi aberto à assinatura um Protocolo Adicional à Convenção Respeitante às Autoridades de Controlo e aos Fluxos Transfronteiriços de Dados, de que são partes 36 dos 47 Estados-Membros do Conselho de Europa, incluindo Portugal, e que também só obteve um acolhimento muito limitado de outros Estados. Com vista a modernizar a Convenção 108, designadamente perante o crescente uso de novas tecnologias de informação e comunicação, o Conselho de Europa adotou muito recentemente um novo Protocolo de modificação da Convenção 108. O texto consolidado daí resultante é designado Convenção Modernizada para a Proteção das Pessoas Relativamente ao Processamento de Dados Pessoais (Convenção 108+).

Para além da limitação geográfica, estes instrumentos não estabelecem um regime uniforme, antes obrigam os Estados Contratantes a conformar o seu Direito interno com as disposições convencionais e a assegurar a sua efetividade.

No âmbito da União Europeia, o RGPD opera uma ampla uniformização, mas este RGPD remete muitas questões para o Direito dos Estados-Membros, sendo necessária desenvolvida legislação nacional de execução do RGPD, que tem de oferecer soluções adequadas de Direito material, de Direito Internacional Privado e de Direito Público Internacional para essas questões.

---

69 - Ver Rolf WEBER – *Shaping Internet Governance: Regulatory Challenges*, em colaboração com Mirina Grosz e Romana Weber, Zurique, Basileia e Genebra, Springer, 2009, 16-17; e Luís de LIMA PINHEIRO – "Reflexões sobre a governação e a regulação da internet, com especial consideração da ICANN", *in Estudos de Direito Intelectual em Homenagem ao Prof. Doutor José de Oliveira Ascensão*, 363-385, Coimbra, Almedina, 2015, 371-372. Considerando que a viabilidade política desta unificação internacional é altamente questionável, BRKAN, "Data Protection…", *loc. cit.*, 36-37. Menos adequada, porém, se afigura uma unificação internacional dos regimes da competência internacional e da determinação do Direito aplicável limitada à proteção de dados pessoais, aventada pelo autor.

BIBLIOGRAFIA

BRKAN, Maja – "Data Protection and European Private International Law", *LSN Transnational Litigation/Arbitration, Private International Law, & Conflict of Laws eJournal, Vol. 2 No. 43, 07/28/2015* (acessível em SSRN)

CALSTER, eert van – "Regulating the Internet. Prescriptive and Jurisdictional Boundaries to the EU's 'Right to Be Forgotten', *LSN Transnational Litigation/Arbitration, Private International Law, & Conflict of Laws eJournal, Vol. 2 No. 64, 11/12/2015* (acessível em SSRN)

CHRISTAKIS, Theodore – "Data, Extraterritoriality and International Solutions to Transatlantic Problems of Access to Digital Evidence. Legal Opinion on the Microsoft Ireland Case (Supreme Court of the United States)", *LSN Cyberspace Law eJournal, Vol. 23 No. 2, 01/10/2018* (acessível em SSRN)

CORNELOUP, Sabine – "De la loi applicable aux activités des entreprises de commerce électronique", *R. crit.* (2017) 112-122

CORREIA, António FERRER – *Direito Internacional Privado. Alguns problemas*, Coimbra, Almedina, 1981

Dicey, Morris and Collins on the Conflict of Laws – 15.ª ed. por LORD COLLINS OF MAPESBURY (ed. geral), Adrian BRIGGS, Andrew DICKINSON, Jonathan HARRIS, J. McCLEAN, Peter McELEAVY, Campbell McLACHLAN e C. MORSE, Londres, Sweet & Maxwell e Thompson Reuters, 2012

ERDOS, David – "European Union Data Protection Law and Media Expression: Fundamentally Off Balance", *Int. Comp. L. Q.* 65 (2016) 139-184

FAWCETT, James e Paul TORREMANS – *Intellectual Property and Private International Law*, 2.ª ed., Oxford, Oxford University Press, 2011

GONÇALVES, ANABELA DE SOUSA – *Da Responsabilidade Extracontratual em Direito Internacional Privado. A Mudança de Paradigma*, Coimbra, Almedina, 2013

J. von Staudingers Kommentar zum Bürgerlichen Gesetzbuch mit Einführungsgesetz und Nebengesetzen, Einführungsgesetz zum Bürgerlichen Gesetzbuche, Art 38 – 42 EGBGB, Neubearbeitung 2001 /VON HOFFMANN, Berlim, Sellier- De Gruyter, 2001

KELLER, Daphne – "The Right Tools: Europe's Intermediary Liability Laws and the 2016 General Data Protection Regulation", *LSN Cyberspace Law eJournal, Vol. 22 No. 19, 03/15/2017* (acessível em SSRN)

KOHLER, Christian – "Conflict of Law Issues in the 2016 Data protection Regulation of the European Union", *RDIPP* (2016) 653-675

KROPHOLLER, Jan – *Internationales Privatrecht*, 6.ª ed., Tubinga, Mohr Siebeck, 2006

KULK, Stefan e Frederik Borgesius – "Privacy, Freedom of Expression, and the Right to Be Forgotten in Europe", *LSN Transnational Litigation/Arbitration, Private International Law, & Conflict of Laws eJournal, Vol. 4 No. 13, 03/09/2017* (acessível em SSRN).

MACHADO, J. BAPTISTA – *Lições de Direito Internacional Privado,* (apontamentos das aulas teóricas do ano letivo de 1971/1972 na Faculdade de Direito de Coimbra), 2.ª ed., Coimbra, Almedina, 1982.

MANKOWSKI, Peter – "Das Internet im Internationalen Vertrags- und Deliktsrecht", *RabelsZ.* 63 (1999) 203-294

MIGUEL ASENSIO, Pedro – *Derecho Privado de Internet*, 5.ª ed., Cizur Menor (Navarra), Civitas e Thomson Reuters, 2015

Id. – "Competencia y Derecho aplicable en el reglamento general sobre protección de datos de la Unión Europea", *Rev. Española de Derecho Internacional* 69 (2017) 75-108.

MIRANDA, JORGE – *Direitos Fundamentais*, 2.ª ed., Coimbra, Almedina, 2017

*Münchener Kommentar zum Bürgerlichen Gesetzbuch/*JUNKER, vol. X, 6.ª ed., Munique, C. H. Beck, 2015.

NADEEM, Danial – "Territorial Limits to the European Union's Right to be Forgotten: How the CNIL Ignores Jurisdictional Basics in Its March 10, 2016 Decision Against Google", *Creighton Int'l & Comp. L.J.* 8 (2017) 182-199

NUNZIATO, Dawn – "The Fourth Year of Forgetting: The Troubling Expansion of the Right to Be Forgotten", *LSN Cyberspace Law eJournal, Vol. 23 No. 49, 07/16/2018* (acessível em SSRN)

OLIVEIRA, ELSA DIAS – *Da Responsabilidade Civil Extracontratual por Violação de Direitos de Personalidade em Direito Internacional Privado,* Coimbra, Almedina, 2011

Id. – "Algumas considerações sobre a responsabilidade civil extracontratual por violação de direitos de personalidade em Direito Internacional Privado", *Cuadernos de Derecho Transnacional* 5 (2013) 139-162

Id. – "A relevância do *right of publicity* no âmbito da propriedade intelectual", *in Est. de Direito Intelectual/José de Oliveira Ascensão*, 209-232, Coimbra, Almedina, 2015.

PINHEIRO, Luís de LIMA– "Direito aplicável à responsabilidade extracontratual na *Internet*", *RFDUL* 42 (2001) 825-834

Id. – "O Direito de Conflitos e as liberdades comunitárias de estabelecimento e de prestação de serviços", *in Seminário sobre a Comunitarização do Direito Internacional Privado*, 79-109, Coimbra, Almedina, 2005 (=*in Estudos de Direito Internacional Privado*, 357-387, Coimbra,

Almedina, 2006)

Id. – *Direito Internacional Privado*, vol. I – *Introdução e Direito de Conflitos – Parte Geral*, 3.ª ed., Coimbra, Almedina, 2014

Id. – *Direito Internacional Privado*, vol. II – *Direito de Conflitos-Parte Especial*, 4.ª ed., Coimbra, Almedina, 2015

Id. – "Reflexões sobre a governação e a regulação da internet, com especial consideração da ICANN", *in Estudos de Direito Intelectual em Homenagem ao Prof. Doutor José de Oliveira Ascensão*, 363-385, Coimbra, Almedina, 2015

PISSARRA, NUNO – *O Dano Transnacional em Direito Internacional Privado. Alguns Problemas* (Diss. de Mestrado policopiada), Lisboa, 2004

RAMOS, Rui MOURA – *Da Lei Aplicável ao Contrato de Trabalho Internacional*, Coimbra, Almedina, 1991

RIVERO, Fomperosa – "Right to Be Forgotten in the European Court of Justice Google Spain Case: The Right Balance of Privacy Rights, Procedure, and Extraterritoriality", *LSN Cyberspace Law eJournal, Vol. 22 No. 19, 03/15/2017* (acessível em SSRN).

SANTOS, António MARQUES DOS – *Direito Internacional Privado. Sumários*, 2.ª ed., Lisboa, AAFDL, 1987

SCHWARTZ, Paul e Karl-Nicolaus PEIFER – "Transatlantic Data Privacy", *LSN Cyberspace Law eJournal, Vol. 22 No. 85, 11/22/2017* (acessível em SSRN)

SOUSA, Rabindranath CAPELO DE – *O Direito Geral de Personalidade*, Coimbra, Coimbra Editora, 1995.

Tallinn Manual 2.0 International Group of Experts and Other Participants, General Editor Michael Schmitt, Cambridge, Cambridge University Press, 2017

VARELA, ANTUNES – *Das Obrigações em geral*, 10.ª ed., Coimbra, Almedina, 2004

VICENTE, Dário MOURA – *Da Responsabilidade Pré-Contratual em Direito Internacional Privado*, Coimbra, Almedina, 2001

WATTS, Sean e Theodore RICHARD – "Baseline Territorial Sovereignty and Cyberspass", *LSN Public International Law: Foreign Relations & Policy Law eJournal, Vol. 5 No. 18, 03/30/2018* e *LSN Cyberspace Law eJournal, Vol. 23 No. 33, 04/05/2018* (acessível em SSRN),

WEBER, Rolf – *Shaping Internet Governance: Regulatory Challenges*, em colaboração com Mirina Grosz e Romana Weber, Zurique, Basileia e Genebra, Springer, 2009

WOODS, Keane – "Against Data Exceptionalism", *LSN Transnational Litigation/Arbitration, Private International Law, & Conflict of Laws eJournal, Vol. 3 No. 16, 03/24/2016* (acessível em SSRN).