O Direito ao apagamento de dados como realidade global

Francisco Arga e Lima*
Mateus Magalhães de Carvalho**

Resumo: Num mundo cada vez mais informatizado e global, a proteção de dados pessoais tem ganho destaque a nível europeu. Em especial, a faculdade de apagar (ou "esquecer") dados de um motor de busca da *Internet* mostra evidentes dificuldades técnicas e jurídicas que importam descortinar, de modo a assegurar uma eficaz proteção dos dados pessoais, segundo os elevados padrões europeus. Propomo-nos, assim, discutir que titulares de dados se encontram protegidos pelo âmbito de aplicação do direito ao apagamento de dados, bem como em que moldes deverá tal apagamento lograr a maior eficácia possível, no respeito pelos normativos internacionais.

Palavras-chave: *RGPD; Apagamento; Ciberespaço; Extraterritorialidade; Geoblocking.*

---

* Francisco Arga e Lima encontra-se no quarto e último ano da sua licenciatura, na Faculdade de Direito da Universidade Nova de Lisboa (FDUNL). Frequenta igualmente o I Curso de Pós-Graduação em Proteção de Dados e Empresas, na Faculdade de Direito da Universidade de Lisboa. Participou em vários moot courts ao longo da sua formação académica, tendo sido vencedor da VII Edição do Moot Court Nacional de Direito Internacional Público, finalista na I edição do Moot Court Português de Direito da Concorrência e vencedor da V Edição do EUROPA Moot Court, em Kavala (este último versando sobre Proteção de Dados). Iniciou a sua produção científica em 2017, com o artigo "Direito a ser Esquecido: Um Conceito em Construção", o qual foi menção honrosa para o Prémio Pessoa Jorge, promovido pela SRS Advogados.

** Mateus Magalhães de Carvalho frequenta o quarto ano da Licenciatura em Direito, na Faculdade de Direito da Universidade Nova de Lisboa. Participou em diversos moot courts, tendo sido vencedor na VII Edição do Moot Court Nacional de Direito Internacional Público, bem como vencedor e melhor orador na V Edição do EUROPA Moot Court, em Kavala (este último subordinado à temática da Proteção de Dados). É, desde 2017, membro do Conselho Pedagógico da Faculdade de Direito da Universidade Nova de Lisboa.

Abstract: In a increasingly informatical and global world, personal data protection has gained the spotlight in the European Union. Especially, the power to erase (or "to forget") data from an Internet search engine shows clear technical and legal problems that must be uncovered, in order to ensure an effective data protection, according to the high European standards. Therefore, we seek to discuss which data subjects are protected by the scope of application of the right of erasure of personal data, as well as how such erasure should achieve effectiveness, in accordance with the international regulatory instruments.

Keywords: *GDPR; Erasure; Cyberspace; Extraterritoriality; Geoblocking.*

Introdução

Foi em maio de 2018 que se tornou aplicável na UE a mais recente ferramenta legislativa em matéria de proteção de dados pessoais: o RGPD[1]. Este novo diploma procura garantir um elevado e uniforme nível de proteção das pessoas singulares neste campo através de vários direitos subjetivos, como o direito ao apagamento dos dados postulado no art. 17.º, n.º 1, RGPD[2-3].

É propósito do presente artigo discutir o campo de aplicação deste direito quando uma sua pretensão se reporte a dados na posse de motores de busca, numa análise bipartida, realizada nos seguintes termos:

i) em primeiro lugar, tentaremos compreender quais os titulares de dados que poderão recorrer a esta figura, já que não pode, no nosso entender, a sua existência estar desligada de considerações territoriais relacionadas com os Estados terceiros cujos ordenamentos não contemplam o direito ao apagamento;
ii) em segundo lugar, iremos, ainda, procurar determinar quais as consequências territoriais de tal apagamento de dados. Para tal,

---

[1] Regulamento (UE) 2016/679 relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE.

[2] *Vide*, por exemplo, o Considerando 10 do RGPD.

[3] Este elevado padrão de proteção das pessoas singulares vem, por exemplo, reconhecido no artigo 8º da CDFUE.

apoiar-nos-emos no recente reenvio prejudicial que opõe a *Google, Inc.* à autoridade francesa de proteção de dados, a CNIL, em que é perguntado ao TJ quais as vestes que uma supressão de hiperligações deve assumir, se globais ou se circunscritas a um qualquer âmbito territorial menor. Sondaremos as questões suscitadas neste processo à luz do RGPD, assim procurando determinar qual o escopo territorial do apagamento de dados e já não da supressão de hiperligações, em função da normal sucessão de atos legislativos europeus que desembocou na entrada em vigor deste regulamento.

1. Breve síntese da evolução das concepções normativas do esquecimento e seu escopo aplicativo

Antes de mergulharmos no objeto do presente estudo, importa descrever os principais acontecimentos que se relacionam com a origem do direito ao apagamento de dados, bem como a clarificação do âmbito territorial dos atos normativos europeus relativos à proteção de dados. Em particular, cabe analisar o caso *Google Spain*, em que foi consagrado um direito à supressão de hiperligações e foi discutida a sua aplicação geral a entidades situadas fora da União Europeia. Este direito é, no mínimo, uma forma embrionária do direito ao apagamento, pelo que cumpre igualmente distinguir estes dois direitos já elencados.

1.1. Acórdão Google Spain

Em 2010, M. Costeja González apresentou uma reclamação à Agência Espanhola de Proteção de Dados contra o jornal *La Vanguardia Ediciones SL* e contra a *Google Spain* e *Google Inc*, procurando ocultar informação de plataformas dos demandados, relativa a dívidas suas à Segurança Social.

Nestes termos, M. Costeja González pediu a remoção dos seus dados da notícia do jornal, bem como a eliminação das referências à notícia no motor de pesquisa da *Google Inc*. A autoridade espanhola de proteção de dados, a *Agencia Española de Protección de Datos* considerou que apenas a *Google Spain* e a *Google Inc*. deveriam suprimir a informação controvertida (sob a forma de hiperligações). Estas interpuseram recurso para o Supremo Tribunal

de Justiça Espanhol, que remeteu três questões prejudiciais ao TJ, tendo sido emitido acórdão em 13 de maio de 2014[4].

Para o presente estudo, importa focar principalmente duas delas: será que a Diretiva 95/46/EC[5] consagra um "Direito a ser Esquecido", ou seja, um direito a partir do qual um sujeito possa exigir a um motor de pesquisa que suprima certos resultados de pesquisa? E será que o Supremo Tribunal de Justiça Espanhol pode aplicar as normas de proteção de dados europeias contra uma entidade sediada nos EUA (a *Google Inc.*)?

Começando pela primeira pergunta, importa analisar a Diretiva 95/46/CE, já revogada, e ver quais as disposições que podem ajudar a responder a essa questão. Neste diploma não se encontrava vertido, expressamente, um "Direito a ser Esquecido", mas eram previstos outros dois direitos bastante importantes: o direito de acesso (art. 12.º e 14.º) e de oposição (art. 14.º e 15.º). O primeiro dividia-se em dois outros direitos complementares: o direito de acesso aos próprios dados[6] e o direito de retificação, apagamento e bloqueio (art. 14.º)[7]. O segundo direito analisado pelo TJ dividia-se no direito de oposição a decisões automatizadas (art. 15.º), de oposição devido à situação particular da pessoa em causa (art. 14.º, al a)), e de oposição à utilização dos dados para efeitos de *marketing* direto (art. 14.º, al. b)).

No presente contexto, importa fundamentalmente definir o direito de retificação, apagamento e bloqueio. Na sua égide, podia um titular de dados pessoais, por "razões preponderantes e legítimas relacionadas com a sua situação particular", opor-se a que os dados que lhe dissessem respeito fossem objeto de tratamento.

O TJ decidiu conjugar os direitos de acesso e de oposição no sentido de o operador do motor de busca, a pedido de um titular de dados pessoais,

---

[4] Acórdão do TJ, C-131/12, *Google Spain*, ECLI:EU:C:2014:317.

[5] Diretiva 95/46/EC do Parlamento Europeu e do Conselho de 24 de Outubro de 1995 relativa à protecção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados.

[6] Este direito permitia aos sujeitos em causa saberem, a cada momento, se os seus dados estão a ser alvo de qualquer tipo de tratamento e, se tal se verificar, para que fins estão a ser tratados que categorias de dados são objeto de tratamento, a que destinatários vão os mesmos ser comunicados e a origem dos dados pessoais, etc.

[7] Conferia aos titulares dos dados a faculdade de obterem do responsável pelo tratamento de dados a retificação, o apagamento, ou mesmo o bloqueio dos dados em causa, caso considerassem que o tratamento não ia de acordo com os cânones da Diretiva 95/46/EC.

ser obrigado a suprimir da lista de resultados, apresentada na sequência de uma pesquisa feita a partir do seu nome, as ligações que contenham informações sobre si. Concluiu, assim, pela existência de um direito à supressão de hiperligações na Diretiva 95/46/EC[8].

Contudo, o TJ não discutiu apenas a existência de um direito à supressão de hiperligações, mas também apreciou o escopo territorial da Diretiva no seu todo. De facto, foi perguntado ao TJ até que ponto poderia o Supremo Tribunal de Justiça Espanhol aplicar os direitos de acesso e oposição contra uma empresa com sede nos EUA (neste caso, a *Google Inc.*).

O TJ considerou que a Diretiva era aplicável à *Google Inc.*, apesar desta ser uma empresa americana, já que esta detinha um estabelecimento num Estado-Membro da UE: a *Google Spain*. Deste modo, o Tribunal conferiu à Diretiva um âmbito de aplicação particularmente amplo, extensível para fora da União, desde que cumpridas as condições do seu art. 4º, n.º 1, alínea a)[9].

1.2. Google Spain *vs. RGPD*

Procede da exposição anterior a sedimentação no ordenamento europeu de um direito à supressão de hiperligações ou à desindexação. Contudo, em maio de 2018, começou a produzir efeitos o RGPD. Este regulamento consagra um direito ao apagamento de dados pessoais (art. 17.º). Conforme o n.º 1 de tal artigo, pode o titular dos dados "obter do responsável pelo tratamento o apagamento dos seus dados pessoais, sem demora injustificada", caso se cumpra alguma das condições aí plasmadas, nomeadamente a ilicitude do tratamento (alínea d)).

Por questões de ordem prática relativas à economia do presente estudo, esta nossa análise incidirá sobre o direito ao apagamento, já que a Diretiva na qual o TJ se baseou para construir o direito à supressão de uma hiperligação se encontra, agora, revogada, em consequência da entrada em vigor do RGPD.

---

[8] *Vide* Acórdão do TJ, C-131/12, *Google Spain*, cit., para. 100; *Vide*, igualmente, Kuner, Christopher. "EU Judgment on Internet Data Protection and Search Engines", in *Society and Economy Working Papers*, LSE Law, 2015, p. 8.

[9] Ver, em particular, Acórdão do TJ, C-131/12, *Google Spain*, cit., paras. 50 a 58.

Ora, os critérios de aplicação do RGPD, constantes do art. 3º, são, em termos gerais, similares aos estabelecidos no Acórdão *Google Spain* para o direito à desindexação, pelo que as variações de vulto entre os dois documentos legislativos consistirão nos direitos neles consagrados para assegurar o esquecimento das pessoas singulares. Deste modo, resta-nos distingui-los. Serão o direito à desindexação e o direito ao apagamento de dados um e o mesmo direito?

Podemos alvitrar do andamento do processo legislativo europeu (revogação da antiga Diretiva e sua substituição pelo RGPD) que foi intenção legiferante definir como única cláusula operativa da supressão de dados o art. 17.º do RGPD e o seu direito ao apagamento[10]. Confirmemos, então, a correção de tal asserção.

Ora, o direito à desindexação não se traduz em mais que a supressão de hiperligações dos resultados de buscas operadas com base no nome do titular dos dados. Não possibilita o apagamento da informação constante dos *websites* para os quais tais hiperligações remetem (cujos servidores são estranhos ao controlo do motor de busca), nem tão pouco, e mais decisivamente, o apagamento da informação pessoal do sujeito dos servidores de indexação[11] a partir dos quais os motores de busca geram os resultados das pesquisas realizadas. Com efeito, o direito à desindexação não possibilita

---

[10] Esta é, de facto, uma das interpretações possíveis do considerando n.º 66 do RGPD quando refere que, para "reforçar o direito ao esquecimento", o direito ao apagamento deve ser implementado com recurso ao disposto no art. 17.º, n.º 2, daqui se podendo retirar que tudo aquilo que compõe o direito ao esquecimento que não seja o apagamento de dados é, precisamente, a obrigação de notificação de tal pedido a responsáveis subsequentes. In Xanthoulis; Napoleon. "Conceptualising a Right to Oblivion in the Digital World: A human rights-based approach", disponível em: https://ssrn.com/abstract=2064503 ou http://dx.doi.org/10.2139/ssrn.2064503, p. 16. (acedido a 09/03/2019).

[11] Bases de armazenamento e organização dos dados utilizados para gerar resultados de buscas, governados segundo um modelo de otimização dessas tarefas, que visa promover uma maior latência dos resultados de busca apresentados em cada pesquisa. Estas são compostas, em constante mudança, por todos os dados recolhidos indiscriminadamente por um motor de busca na Internet, através de um processo denominado de web crawling. Os dados pessoais de um sujeito são, de forma muito sintética, tratados na sua recolha de toda a Internet, na sua organização em servidores de indexação e na sua submissão a algoritmos de produção de resultados de busca. Ver Brin, Sergey; Page, Lawrence. "The Anatomy of a Large-Sclae Hypertextual Web Search Engine; Stanford University", disponível em: http://infolab.stanford.edu/~backrub/google.html (acedido a 09/03/2019), bem como Patil, Yugandhara; PATIL,

a supressão de hiperligações geradas por qualquer outra combinação de palavras inseridas no motor de busca que não a dos nomes dos titulares de dados[12].

Por seu turno, no direito ao apagamento a impossibilidade de aceder à informação pessoal do titular de dados alcança-se, em teoria, mediante o verdadeiro apagamento dos dados pessoais dos repositórios onde estes estejam armazenados em cada motor de busca.

Podemos até concluir que a desindexação é, por inerência lógica, consumida nas suas utilidades pelo direito ao apagamento. Se os dados pessoais de um sujeito são apagados no seu lugar de armazenamento originário, então não podem ser transferidos para servidores de indexação e, consequentemente, organizados em hiperligações como resultado de buscas.

Torna-se, então, intuitivo, que o direito à supressão de uma hiperligação e o direito ao apagamento são dois direitos distintos, de naturezas e implicações práticas diferentes, mais não seja pelo facto de o primeiro permitir que um motor de busca mantenha os dados pessoais de determinado sujeito na sua posse, ao invés do direito ao apagamento.

É no direito ao apagamento que centraremos a nossa análise, discutindo: (i) os limites territoriais inerentes a uma sua aplicabilidade numa realidade transfronteiriça como a *Internet*; e (ii) as consequências que pode assumir por forma a assegurar a eficiência da proteção dos dados pessoais das pessoas singulares, quando compatibilizada com todos os outros interesses em jogo.

2. A extraterritorialidade do direito ao apagamento: titulares

No nosso entender será fundamental para o presente estudo a compreensão de que o direito ao apagamento de dados é, como todos os direitos previstos no RGPD, territorialmente limitado pela natureza das competências e poderes da União Europeia.

Sonal. "Review of Web Crawlers with Specification and Working", in *International Journal of Advanced Research in Computer and Communication Engineering*; v. 5, 2016, p. 220-223.

[12] É claro que este direito pode ser alargado a outras combinações introduzidas num motor de busca, mas existirão sempre outras possibilidades de obter, nos resultados de uma busca, as hiperligações que contêm os dados pessoais do seu titular.

É nessa senda que importa articular o art. 17.º com o art. 3.º, n.º 1 do RGPD, que versa sobre o âmbito territorial deste diploma, dizendo que o mesmo se aplica a todos os tratamentos de dados pessoais efetuados no contexto de atividades do responsável do tratamento que se manifestem no território da União, *independentemente de o tratamento ocorrer dentro ou fora da União*[13].

No entanto, não podemos deixar de notar o seguinte: uma coisa é a aplicação do RGPD (que se quer global), outra bem distinta é a extensão territorial dos direitos por ele criados (*maxime* o direito ao apagamento), que assumirá contornos variáveis em função das particularidades concretas da pretensão do titular dos dados[14].

Não há dúvida que, se interpretadas literalmente, as provisões do RGPD em análise podem ser potencialmente aplicadas a toda a *Internet*, estando, desse modo, ao dispor de todos os titulares de dados, em qualquer parte do mundo, como ferramenta jurídica de salvaguarda da proteção das suas informações pessoais.

Com efeito, tal entendimento de aplicação global das regras europeias de proteção de dados já brotava da jurisprudência europeia e, em especial, do caso *Google Spain*[15]. Entende-se do art. 3.º que a aplicação do RGPD não apresenta quaisquer limites territoriais ou relacionados com a nacionalidade do titular dos dados, sendo antes definida *ratione materiae*, em função de um tratamento de dados pessoais ter ocorrido no contexto de atividades que se manifestem na União.

Foi esta a intenção manifestada pelo legislador europeu, justificada pelo desejo de concretizar um direito fundamental dos cidadãos e de tornar

---

[13] Kuner, Christopher. "EU Judgment on Internet Data Protection and Search Engines", in *Society and Economy Working Papers*, LSE Law, 2015, p. 12; Svantesson, Dan. "Extraterritoriality In The Context Of Data Privacy Regulation", in *Masaryk University Journal of Law and Technology*, v. 7 (1), 2012, p. 87-96.

[14] O antigo GT29 sublinhou a necessidade de avaliar as pretensões dos titulares de dados numa base casuística, *vide* GT29, "Guidelines On The Implementation Of The Court Of Justice Of The European Union Judgment In "Google Spain And Inc V. Agencia Española De Protección De Datos (AEPD) And Mario Costeja González", 26 de novembro de 2014, p. 12.

[15] *Vide* Acórdão do TJ, C-131/12, *Google Spain*, cit., para. 60; ver também, entre outros, Acórdão do TJ, Proc. C-324/09, *L'Oréal e o.*, ECLI:EU:C:2011:474, para. 67.

a UE um padrão de referência global no que diz respeito à garantia da privacidade no mundo digital[16].

Mas será juridicamente aceitável que a União estenda, com base nesta norma, a sua competência extraterritorial de forma absoluta e incondicionada nos termos de uma leitura literal do art. 3º do RGPD quando articulado com o art. 17.º do RGPD? Esta questão terá de merecer uma resposta negativa da nossa parte, em face dos fundamentos apresentados em seguida.

2.1. Abrangência do direito ao apagamento de dados no direito internacional

2.1.1. Soberania territorial no ciberespaço

Em primeiro lugar, cabe olhar para o Direito Internacional e, especificamente, para as regras de soberania a que os Estados estão vinculados, de modo a averiguar qual pode ser a extensão do braço normativo europeu. Contudo, o âmbito do nosso estudo conduz-nos para um domínio que não se confunde com os tradicionais espaços de desenvolvimento humano (a terra, o mar, o espaço aéreo ou o espaço exterior).

Realmente, as questões relacionadas com a *Internet* estão intimamente ligadas a um novo domínio, que começa agora a ganhar importância na orla internacional: o ciberespaço. Este caracteriza-se por ser um domínio operacional diferenciado pelo uso de meios eletrónicos, através do espectro eletromagnético, que permitem a criação, armazenamento, modificação, troca e uso de informação, através de redes interdependentes e conectas, usando tecnologias de comunicação e informação[17]. Assim sendo, qualquer tipo de tratamento de dados realizado através da *Internet* implica a passagem pelo ciberespaço, na medida em que aquela utiliza meios eletrónicos e o espectro eletromagnético, para partilhar, alterar e criar informação, numa rede global.

---

[16] CE, *Press Release*: "European Commission sets out strategy to strengthen EU data protection rules", *IP/10/1462*, Brussels, 4 de novembro de 2010.

[17] Kuehl; Daniel T.. "From cyberspace to cyberpower: Defining the problem", in *Cyberpower and national security*, National Defense University Press, 2009, p. 27.

Ainda que não existam fontes normativas consolidadas em relação a este domínio, podemos vislumbrar certas produções doutrinárias que visam auxiliar na resolução dos problemas de conciliação da soberania estadual com o ciberespaço e, consequentemente, permitem determinar quando é que um sujeito se pode valer do art. 17.º RGPD.

Em 2013, o *Cooperative Cyber Defence Centre of Excellence* da NATO divulgou o *Tallinn Manual*[18], que consiste num compêndio de regras vistas como direito internacional costumeiro, aplicáveis ao ciberespaço e acompanhadas de comentários sobre a sua base legal e possíveis divergências entre os especialistas que as elaboraram[19].

Logo num ponto inicial, afirmam os autores do documento que nenhum Estado pode arrogar soberania sobre a totalidade do ciberespaço. Contudo, constatam também que os Estados podem exercer prerrogativas sobre qualquer ciberinfraestrutura situada no seu território, bem como sobre as atividades associadas a essas infraestruturas[20]. Assim, reconhecem os autores a aplicabilidade do princípio da soberania territorial ao ciberespaço, nos termos do qual um Estado exerce poderes soberanos plenos e exclusivos no seu território[21].

Com a aplicação deste princípio ao ciberespaço, as ciberinfraestruturas situadas no território de um determinado Estado estão sujeitas à soberania territorial desse Estado, pelo que este tem o poder de controlar entradas e saídas do seu território, até de quaisquer formas de comunicação e, transpondo este raciocínio para o nosso estudo, quaisquer tipos de dados[22]. Que conclusões podemos fazer da aplicação deste princípio ao ciberespaço?

---

[18] Schmitt; Michael N. (ed). *Tallinn Manual on the international law applicable to cyber warfare: Prepared by the International Group of Experts at the Invitation of the NATO Cooperative Cyber Defense Centre of Excellence*, Cambridge University Press, 2013.

[19] Schmitt, Michael N.. "International Law in Cyberspace: The Koh Speech and the Tallinn Manual" Justaposed, *Harvard International Law Journal,* v. 54, 2012, p. 15.

[20] *Idem*, p. 15 e ss.

[21] *Vide* Acórdão do TPJI, *S.S. Lotus (Fr. v. Turk.),* (ser. A) Nº. 10, 7 de Setembro de 1927, p. 18 e ss.; Acórdão do TPJI, *Free Zones of Upper Savoy and District of Gex (Fr. v. Switz.),* (ser.A/B) Nº. 46, 7 de junho de 1932, p. 166 e ss.; Heinegg, Wolff Heintschel von, "Legal implications of territorial sovereignty in cyberspace", *4th International Conference on Cyber Conflict (CYCON),* 2012, p. 8.

[22] Heinegg, Wolff Heintschel von. "Legal implications of territorial sovereignty in cyberspace", *4th International Conference on Cyber Conflict (CYCON)*, 2012, p. 8 e 11.

A primeira consequência que podemos retirar é a de que ciberinfraestruturas localizadas em locais cobertos pela soberania territorial de um Estado se encontram protegidas contra a interferência dos demais, independentemente da sua pertença ou por quem sejam utilizadas[23].

Aceitando este raciocínio, então parece ser evidente que, não obstante possíveis limitações por parte do corpo normativo internacional, as ciberinfraestruturas e ciberoperações exercidas dentro do território nacional de um Estado (ou da UE, no âmbito das competências que lhe foram atribuídas pelos Estados-Membros) estão sujeitas ao poder regulatório e sancionatório do Estado em causa. Transpondo isto para a realidade do direito ao apagamento de dados, então todos os dados pessoais tratados dentro da UE são, naturalmente, suscetíveis de conduzir à aplicação do art. 17.º do RGPD, por se traduzirem numa ciberoperação efetuada no território europeu.

A segunda conclusão que se retira da aplicação da soberania territorial ao ciberespaço, e a mais decisiva para o presente estudo, está relacionada com a grande abrangência do direito de um Estado a exercer a sua jurisdição sobre ciberinfraestruturas e ciberatividades.

Esta ideia segue o postulado no *Tallinn Manual*, de que um Estado pode exercer a sua jurisdição de três formas distintas: (i) sob agentes que fazem parte de operações cibernáuticas no seu território; (ii) sob infraestruturas do ciberespaço, baseadas no seu território ou (iii) extraterritorialmente, de acordo com o direito internacional. Daqui derivam potenciais bases para o exercício da jurisdição de um Estado, fora da sua circunscrição territorial, sobre operações no ciberespaço, como a nacionalidade do agente, nacionalidade da vítima, violação de normas de direito internacional ou motivos de segurança nacional.

Um outro princípio que permite o exercício da jurisdição de um Estado sobre atos praticados no estrangeiro, consubstancia-se na doutrina dos efeitos, a partir da qual um Estado pode exercer jurisdição sobre um facto que ocorreu no estrangeiro, mas produziu efeitos significativos no seu território[24].

---

[23] *Idem*.

[24] Nas palavras do Advogado-Geral do M. Darmon: "Dois fundamentos da competência dos estados são incontestados em direito internacional: a territorialidade e a nacionalidade. A primeira reconhece competência jurisdicional a um Estado desde que a pessoa ou o bem

2.1.2. O confronto com a extraterritorialidade do apagamento de dados

Com base nestas ideias, estamos em condições de formular o nosso primeiro argumento. Realmente, advém da ordem jurídica internacional a necessidade de o direito da UE cumprir um dos mais basilares princípios da ordem internacional: o princípio da não ingerência nos assuntos internos de Estados terceiros.

Surge então, de forma premente, a necessidade de desenhar o limite entre (i) a legítima aplicabilidade extraterritorial de direitos europeus (como o do apagamento), em função de um âmbito *ratione materiae* que vise salvaguardar direitos previstos na CDFUE; e (ii) a extensão de competências jurisdicionais para dentro de Estados onde tais direitos a salvaguardar não foram soberanamente criados, nem lograram o consenso axiológico-valorativo da respetiva comunidade.

Não é por acaso que o TIJ, em casos como o *Barcelona Traction*[25], impõe a todos os Estados a obrigação de darem provas de moderação e prudência quanto à extensão da competência dos seus órgãos, como bem relembra o Advogado-Geral Darmon, na sua opinião do caso *Ahlström*[26].

Ademais, uma aplicação incondicionada do RGPD a todo o globo poderia fazer grassar práticas de *forum shopping* junto de DPA e tribunais europeus. Por exemplo, como bem teoriza Kuner face aos comandos do caso *Google Spain*, não parecem existir quaisquer razões, à luz do RGPD, pelas

---

em causa nele estejam situados ou que o evento em questão nele se tenha desenrolado (...). A territorialidade, ela mesmo, gerou dois princípios de competência distintos: a territorialidade subjectiva, que permite sujeitar à competência de um Estado os actos que tenham origem no seu território, mesmo que a sua consumação tenha ocorrido no estrangeiro; a territorialidade objetiva, que lhe permite, inversamente, conhecer dos actos cujo início de execução tenha ocorrido no estrangeiro mas cujo cumprimento, pelo menos parcial, ocorreu no seu próprio território.". Heinegg, Wolff Heintschel von. "Legal implications of territorial sovereignty in cyberspace", *Cyber Conflict (CYCON)*, 2012, p. 14 e 15; Opinião do Advogado-Geral (Marco Darmon) do TJ, Proc. Apensos 89/85, 104/85, 114/85, 116/85, 17/85 e 125/85 a 9/85, de 25 de maio de 1988, para. 19 e ss. A análise da Opinião do Advogado-Geral M. Darmon será desenvolvida nos pontos seguintes.

[25] Acórdão do TIJ, *Case Concerning the Barcelona Traction, Light and Power Company, Limited (Belgium v. Spain)*, 5 de fevereiro de 1970.

[26] Ver Opinião do Advogado-Geral (Marco Darmon) do TJ, Proc. Apensos 89/85, 104/85, 114/85, 116/85, 17/85 e 125/85 a 9/85, ECLI:EU:C:1988:258, p. 24.

quais um cidadão chinês que usasse um motor de busca estabelecido nos EUA com uma subsidiária na Hungria não pudesse reivindicar, por meio da agência de proteção de dados húngara, um seu direito ao apagamento contra tal motor de busca por forma a ter os seus dados pessoais eliminados em todo o globo e não só na União[27].

Existe, neste caso, um especial interesse europeu na salvaguarda da privacidade deste cidadão de um Estado terceiro? Existe algum fator suficientemente acutilante de ligação do sujeito ao fórum no qual ele pretende fazer valer os seus direitos? Pelo contrário, este alcançaria o absurdo de, nestes termos, demandar uma entidade americana com base no direito da União não tendo qualquer outra ligação à União que não fosse o uso de um serviço de *internet* igualmente acessível em território europeu; e de, logrando um acolhimento das suas pretensões, eliminar informação que lhe seja relativa não só na União Europeia como em toda a *Internet*.

Com base nestes pressupostos, parece ser mais correta a adoção de uma primeira coordenada genérica definitória da extensão do direito ao apagamento, que sustenta uma interpretação restritiva do art. 3.º, n.º 1 do RGPD quando articulado com o art. 17.º do RGPD: se o único interesse substancial do titular dos dados é o de evitar o acesso à informação de cidadãos de um Estado terceiro sem qualquer conexão à União Europeia, então este não poderá invocar o direito ao apagamento. Flui do que foi dito que, ainda que o RGPD tenha um âmbito de aplicação potencialmente global, a União Europeia só deve proceder à concretização do direito ao apagamento por ele criado naquilo que consistir um interesse substantivo e merecedor de tutela à luz do ordenamento europeu.

Deste modo, o RGPD, por meio do art. 17.º, será aplicável a todas as ações, independentemente da nacionalidade dos sujeitos envolvidos ou do território onde tais ações tenham lugar, que produzam efeitos significativos em espaço europeu, ao serem disruptivos dos valores e direitos fundamentais que a União, através dos arts. 7.º e 8.º da CDFUE, pretende assegurar em matéria de privacidade e proteção de dados.

Procede-se assim à corporização da teoria dos efeitos, delimitadora das competências extraterritoriais dos vários Estados. Este princípio permite aos Estados regular comportamentos que ocorram fora do seu território,

---

[27] Kuner, Christopher. "EU Judgment on Internet Data Protection and Search Engines", in *Society and Economy Working Papers*, 2015, LSE Law, p. 12 e 13.

desde que estes produzam efeitos substanciais nesse mesmo território[28]. E, sem dúvida, a disponibilização de certos tipos de resultados em motores de busca, mesmo que tal processamento afete titulares não europeus ou que se dê fora da UE, pode produzir um efeito substancial em território europeu, pondo em causa objetivos europeus nesta matéria[29].

2.1.3. A teoria dos efeitos aplicada ao apagamento de dados: o auxílio interpretativo do TJ

Não podemos ignorar, contudo, que estes efeitos de que falamos constituem uma realidade imaterial e transfronteiriça, algo que pode ser um óbice à aplicação desta teoria neste campo. Torna-se, nesta altura, urgente convocar alguma jurisprudência europeia, referente a ramos de direito análogos, em que a teoria dos efeitos é pressuposto do exercício de competências normativas por parte das autoridades europeias (neste caso, jurisdicionais). E, neste sentido, pode a aplicação do RGPD beneficiar em muito dos ensinamentos do TJ em matéria concorrencial.

Vejamos, por exemplo, o caso *Ahlström*[30], começando pela opinião do Advogado-Geral Marco Darmon, na sequência da apensação de uma série de processos condenatórios concorrenciais relativos a práticas concertadas no setor industrial da pasta papel, em função da contestação, em todos eles, da competência da União em matéria de aplicação das regras europeias deste ramo de direito a empresas de Estados terceiros.

Ora, com base numa análise à jurisprudência do TJ, à jurisprudência do TIJ e até numa viagem comparativa aos ditames do direito norte-americano em matéria de competência extraterritorial, o Advogado-Geral concluiu que: (i) a jurisprudência do TJ não rejeita a aplicação da teoria dos efeitos em matéria de competência extraterritorial da União; (ii) tal exercício de competência baseada num efeito qualificado manifestado no domínio europeu é conforme às normas e princípios do Direito Internacional; e que

---

[28] Alsenoy, Brendan van; Koekkoek, Marieke. "The extra-territorial reach of the EU's "right to be forgotten", *KU Leuven Centre for IT & IP Law*, 2015, p. 23.

[29] *Vide* considerandos 1, 7, 9, 10 e 13 do RGPD.

[30] Acórdão do TJ, Proc. Apensos 89/85, 104/85, 114/85, 116/85, 17/85 e 125/85 a 9/85, *Ahlstrom Osakeyhtio and Other/Comission*, ECLI: EU:C:1993:120.

(iii) a teoria dos efeitos deveria ser adotada como critério da competência comunitária[31].

Com efeito, é curioso notar que as conclusões do Advogado-Geral se arrimam em conceitos originários da doutrina e jurisprudência norte-americanas, onde é já traquejada, em campos como a responsabilidade civil, a prática de limitar a jurisdição de algum fórum quando a controvérsia ou as partes não apresentam com ele uma conexão suficiente[32]. São convocados conceitos como o da *rule of reason* ou o do *judicial interest balancing* para defender o caráter razoável do exercício de competências pelo qual a União também se deve pautar[33].

Não deixa de ser sintomático do acerto das conclusões de Marco Darmon que o Tribunal tenha seguido o critério de competência por ele proposto, tendo, em decisão posterior, rejeitado os argumentos das empresas de Estados terceiros relacionados com a incompetência da União, com base nesta ideia de que as autoridades da União deveriam impor as regras europeias às empresas de Estados terceiros cujas ações, mesmo que praticadas fora de território europeu, tivessem um efeito qualificado (e, por isso, digno da reivindicação de competência comunitária) no mercado interno, realidade imaterial que não deixa de integrar o conceito de efeitos interterritoriais[34]. É, ainda, de extrema valia estudar a jurisprudência do TJ referente à propriedade intelectual no contexto de motores de busca de fins comerciais, *maxime* o caso que opôs a *L'Oréal* ao *eBay* (Caso *L'Oréal*)[35].

Neste processo era discutida a aplicação do direito europeu às atividades comerciais e de marketing desenvolvidas pela plataforma eletrónica *eBay*

---

[31] Ver Opinião do Advogado-Geral (Marco Darmon) do TJ, Proc. Apensos 89/85, 104/85, 114/85, 116/85, 17/85 e 125/85 a 9/85, ECLI:EU:C:1988:258, para. 14, 27, 53 e 58.

[32] Christopher Kuner advoga, aproveitando tais ensinamentos do ordenamento norte-americano, que: "similar action may be needed to limit the right to suppression", referindo-se à desindexação, num raciocínio que não deixa, no entanto, de se revelar pertinente em sede do direito ao apagamento. *Vide*, igualmente Alsenoy, Brendan van; Koekkoek, Marieke. "The extra-territorial reach of the EU's "right to be forgotten"", *KU Leuven Centre for IT & IP Law*, 2015, p. 13.

[33] Ver Opinião do Advogado-Geral (Marco Darmon) do TJ, Proc. Apensos 89/85, 104/85, 114/85, 116/85, 17/85 e 125/85 a 9/85, ECLI:EU:C:1988:258, paras. 38, 40, 41 e 48.

[34] *Idem*, paras. 14, 16, 18 e 19.

[35] Acórdão do TJ, Proc. C-324/09, *L'Oréal e o.,* ECLI:EU:C:2011:474.

(que contém um motor de busca de produtos), por forma a apurar se direitos de propriedade intelectual da *L'Oréal* teriam sido violados, algo que fluiria da aplicação das regras europeias[36].

Embora reconheça que o efeito útil das normas europeias seria posto em causa se a sua aplicação fosse precludida pelo simples facto do prevaricador das mesmas operar num Estado-terceiro, e que tal dê força a uma aplicação que não se norteie por barreiras territoriais, o Tribunal deixa claro que o mero facto de a plataforma eletrónica ser acessível em território europeu não constitui base suficiente para a aplicação do direito da União Europeia[37].

Afirma, igualmente, que deve ser feita uma análise casuística da existência de fatores de conexão suficientemente relevantes entre as práticas *sub judice* e o domínio europeu para determinar a aplicação àquelas das regras europeias em matéria de propriedade intelectual[38].

É, assim, míster transpor esta última ideia para o direito da proteção de dados, corporizando outra coordenada genérica da extensão do direito ao apagamento, no contexto da sua sujeição à teoria dos efeitos. Qualquer Estado, e por isso também a União Europeia, quando fazendo cumprir as suas normas no ordenamento internacional, não está munido de qualquer *carte blanche*, devendo sempre assegurar que a pretensão de uma implementação extraterritorial das suas normas é razoável, numa análise casuística[39].

Devem assim as DPA sondar, em cada pretensão de apagamento dos titulares de dados, fatores de conexão do quadro factual de cada processo ao ordenamento europeu, *i. e.*, um efeito do processamento controvertido que seja significativamente disruptivo dos interesses europeus e que, por isso, torne razoável a aplicação das suas normas legais de proteção de dados, nomeadamente, do artigo 17.º, RGPD. Este processo de indagação é mais premente em casos em que tal conexão não é tão clara, como aqueles em

---

[36] Para um maior detalhe do quadro factual, *vide Idem* paras. 26-50.

[37] *Idem*, paras. 63-64.

[38] *Idem* paras. 65-66, onde o Tribunal afirma esta ideia e conclui pela existência de fatores de conexão suficientes entre as atividades do eBay e a UE.

[39] Alsenoy, Brendan van; Koekkoek, Marieke. "The extra-territorial reach of the EU's "right to be forgotten"", *KU Leuven Centre for IT & IP Law*, 2015, p. 23-25.

que o titular dos dados ou a entidade por ele demandada (ou ambos) não sejam europeus[40].

É defendido por alguns autores que um desses fatores de conexão pode ser a harmonização normativa entre os ordenamentos jurídicos relevantes[41]. Por exemplo, se a norma europeia que prevê a possibilidade de apagamento de dados pessoais encontrar uma norma similar, por exemplo, no ordenamento jurídico japonês, tornar-se-á menos problemática uma demanda extraterritorial das entidades europeias. Tal já não será o caso se tal norma não se encontrar replicada, por exemplo, no ordenamento norte-americano.

2.2. As autoridades de proteção de dados no plano global

Suponhamos que o direito ao apagamento de dados assumiria um escopo global de aplicação, desprovido de limites territoriais ou de razoabilidade do exercício da jurisdição da União. Qual seria a legitimidade jurídico-política da União para o aplicar, "criando" autênticos "direitos ao apagamento" em ordenamentos estrangeiros como efeito direto da aplicação de uma norma europeia? Torna-se esta questão ainda mais bizarra se considerarmos a força que uma resposta positiva atribuiria às entidades administrativas encarregadas de fazer cumprir o RGPD: as DPA.

Por um lado, é clara a falta de recursos (humanos e financeiros) destas agências para lidar com o enorme volume de pedidos de apagamento vindos de todo globo, expectável num quadro como o descrito *supra*, o qual é potencialmente catalisador de práticas de *forum shopping*[42]. Se uma DPA se encontrar obstruída com pedidos de apagamento de indivíduos que não apresentem qualquer conexão relevante com a União, como irá lidar efetivamente com aqueles pedidos cujo tratamento consubstancia um interesse substantivo do ordenamento europeu, fruto da clara conexão dos casos ao domínio europeu?

---

[40] Não podemos deixar de sublinhar o cariz meramente indiciário destes fatores face à aplicação *ratione materiae* do RGPD.

[41] Alsenoy, Brendan van; Koekkoek, Marieke. "The extra-territorial reach of the EU's "right to be forgotten"", *KU Leuven Centre for IT & IP Law*, p. 26 e 27.

[42] Ver *supra*, p. 66.

Por outro lado, se existem requisitos exigentes a ser cumpridos antes de uma DPA de um Estado-Membro aplicar direito da União num outro Estado-Membro, como o TJ avança no Acórdão *Weltimmo*[43], não deveriam existir requisitos ainda mais exigentes no que concerne a extensão dos poderes de uma tal agência em relação a Estados terceiros? E não seria o cumprimento de tais ditames ainda mais imperativo (ou até inibidor da atuação de uma DPA) quando o pedido de apagamento não apresenta qualquer conexão relevante ao Estado-Membro no qual dada DPA opera? O art. 55.º, n.º 1, RGPD diz que as DPA são competentes no território do seu próprio Estado-Membro, algo que exclui liminarmente a sua competência extraterritorial.

Efetivamente, e transpondo as palavras de Kuner do direito à desindexação para o direito ao apagamento, é necessário tornar o âmbito deste direito proporcional à sua aplicabilidade prática, impedindo que se torne tão abrangente ao ponto de se tornar insignificante[44]. É do maior interesse da União Europeia que o direito ao apagamento assuma, no plano global da sua aplicação que a ubiquidade da *Internet* exige, o escopo que, realisticamente e em consonância com os princípios do Direito Internacional, pode, na prática, assumir. Só deste modo se poderá assegurar o seu efeito útil (bem como do regulamento que o encerra) evitando que um instrumento legal com o potencial de inspirar desenvolvimentos extremamente positivos no campo da proteção de dados seja fragilizado pelas críticas daqueles que apontam à União a imposição dos seus valores em jurisdições não-europeias[45].

Fazemos nossas as palavras do Conselho da Europa quando defende que "*as medidas adotadas pelas autoridades estatais europeias no combate a conteúdo e atividades ilegais na Internet não devem resultar num impacto desnecessário e desproporcionado para lá das fronteiras desse Estado*"[46].

---

[43] Acórdão do TJ, Proc. C- 230/14, *Weltimmo,* ECLI:EU:C:2015:639, paras. 56 e 57.

[44] Kuner, Christopher. "EU Judgment on Internet Data Protection and Search Engines", in *Society and Economy Working Papers*, LSE Law, 2015, p. 23.

[45] Alsenoy, Brendan van; Koekkoek, Marieke. "The extra-territorial reach of the EU's "right to be forgotten"", *KU Leuven Centre for IT & IP Law*, 2015, p. 3.

[46] Ver Conselho da Europa, Committee of Ministers to member States on the free, transboundary flow of information on the Internet, CM/Rec(2015)6, de 1 de Abril de 2015.

Cabe, por fim, sinalizar, em matéria já estritamente referente ao direito da proteção de dados, alguns casos em que se descortina a apologia da necessidade de aferição de fatores de conexão relevantes entre o pedido de apagamento e a UE como ponto prévio da aplicação das respetivas normas europeias.

Por exemplo, o GT29 pareceu deixar implícita a necessidade do estabelecimento de limites em relação a quem pode se socorrer do apoio das DPA, ao afirmar que, na prática, estas ir-se-iam concentrar nos pedidos que apresentassem uma conexão clara entre o titular dos dados pessoais e a UE[47]. No entanto, e até por uma questão de honestidade intelectual, não podemos deixar de sublinhar que a ideia transmitida pelo GT29 é tão-somente uma de *prioridade* e não tanto de *exclusividade* da alocação de recursos das DPA aos pedidos que manifestem uma ligação clara com a União; até porque tal afirmação é precedida da asserção de que o artigo 8º da CDFUE reconhece a todos o direito à proteção de dados[48].

Mas aquilo que é uma subliminar referência deste grupo à maneira como os óbices de natureza prática da aplicação deste direito podem acabar por concorrer para a determinação do seu escopo, é posteriormente confirmada por um dos seus membros, a *Agencia Española de Protección de Datos*, no quadro de um pedido de apagamento, efetuado por um cidadão paraguaio, de hiperligações de domínios exteriores à União.

Com efeito, em 2015, a *Agencia Española de Protección de Datos* considerou inadmissível o pedido de apagamento do mencionado cidadão, por considerar que este não mantinha nenhuma vinculação clara com um Estado-Membro[49]. Esta decisão foi judicialmente confirmada em 2017 por um tribunal espanhol, um órgão judicial europeu vinculado à aplicação de

---

[47] Grupo de Trabalho do Artigo 29, *Guidelines On The Implementation Of The Court Of Justice Of The European Union Judgment In "Google Spain And Inc V. Agencia Española De Protección De Datos (AEPD) And Mario Costeja González"*, 26 de novembro de 2014, para. 19; Alsenoy, Brendan van; Koekkoek, Marieke. "The extra-territorial reach of the EU's "right to be forgotten"", *KU Leuven Centre for IT & IP Law*, 2015, p. 15.

[48] É utilizada a expressão *"DPA's will focus on claims (...)"*; ao invés de, por exemplo, *"DPA's will only focus on claims"*.

[49] *Agencia Española de Protección de Datos*, Procedimiento Nº: TD/01176/2015, Resolución Nº.: R/01976/2015, p. 8.

direito europeu, o mesmo que realizou o pedido de reenvio para o TJ no Caso *Google Spain*[50].

Ainda que tais decisões (administrativa e judicial) tenham sido tomadas à luz da antiga Diretiva, não deixa de ser elucidativa a afirmação da necessidade de limitar a extensão dos direitos dos cidadãos em matéria de proteção de dados, quando não estão em causa quaisquer interesses relevantes da União.

3. A extraterritorialidade do direito ao apagamento: consequência e modo do apagamento

Todo o raciocínio feito na secção anterior refere-se aos limites de aplicação do direito ao apagamento de dados, proveniente da articulação entre os artigos 3.º n.º 1, e 17.º do RGPD. Porém, todos estes fundamentos concorrem, igualmente, para a determinação do âmbito do apagamento de dados quando as pretensões do seu titular são acolhidas.

Ora, encontra-se presentemente diante do TJ um processo prejudicial que opõe a *Google Inc.* e a CNIL[51]. Esta, face a pedidos fundamentados no direito à supressão de uma hiperligação, resultante do acórdão *Google Spain*, exigiu à *Google Inc.* que suprimisse os resultados referentes aos dados em causa, não apenas dos domínios europeus (como a *Google.fr*), mas também dos domínios exteriores à UE, como a *Google.com*, de modo a salvaguardar o efeito útil deste direito.

Apesar de a Google ter apresentado recurso, a CNIL reiterou a sua posição, insistindo na supressão de resultados a nível global, já que, caso contrário, o direito a ser esquecido poderia ser facilmente contornado e esvaziado de efeitos práticos[52]. Não tendo a *Google* acatado a ordem, a autoridade francesa iniciou um processo judicial contra a empresa.

---

[50] *Vide* http://cyberlaw.stanford.edu/blog/2017/12/right-be-forgotten-and-global--desindexação-some-news-spain (acedido a 09/03/2019)

[51] Acórdão do TJ, C-507/17, pedido de decisão prejudicial apresentado pelo *Conseil d'État* (França) em 21 de agosto de 2017.

[52] No mesmo sentido, entre nós, Marques, João. "Direito ao Esquecimento: A aplicação do Acórdão Google pela CNPD", in *Fórum de Proteção de Dados*, n. 3, 2016, p. 55.

Nesta senda, a *Google* implementou um sistema de bloqueio geográfico, alargando o suprimento de resultados a qualquer extensão do motor de busca, desde que tal extensão esteja a ser operada por um utilizador situado no Estado-Membro da UE onde o pedido foi aprovado[53].

A CNIL, contudo, considerou a medida insuficiente para garantir a proteção dos utilizadores franceses, impondo uma coima de €100.000 à *Google*[54]. Afirmou que o suprimento dos resultados com base num sistema de geolocalização seria insatisfatório, já que os resultados continuariam acessíveis fora de França. Por outro lado, e mais decisivamente, seria igualmente possível aos utilizadores contornarem este sistema, utilizando um endereço estrangeiro, mesmo estando em território francês[55].

Insatisfeita, a *Google* recorreu para o *Conseil d'État*, estando, à data do presente estudo, o processo suspenso face a um reenvio prejudicial para o TJ[56].

As três questões prejudiciais colocadas ao Tribunal, lidas de acordo com o RGPD conforme nos propusemos fazer, podem unir-se sob a seguinte questão de fundo: que extensão deve ser dada ao direito ao apagamento dos dados? Deve este levar a um apagamento global e absoluto dos dados controvertidos; deve tal apagamento ser restringido aos domínios europeus de um motor de busca (*vide Google*.pt ou *Google*.es); e ainda, e independentemente da resposta às questões anteriores, deve ser adotado, pelos motores de busca, um sistema de *geoblocking* em articulação com um dos anteriores modelos?

Qual a opção que deve tormar o TJ à luz do RGPD?

---

[53] Kulk, Stefan; Borgesius, Frederik Zuiderveen. "Privacy, freedom of expression, and the right to be forgotten in Europe", in *Cambridge Handbook of Consumer Privacy*, 2017, p. 29 e 30. Ver, igualmente, *infra,* Ponto 4.3.

[54] https://www.legifrance.gouv.fr/affichCnil.do?oldAction=rechExpCnil&id=CNILTEXT000032291946&fastReqId=273825503&fastPos=1 (acedido a 09/03/2019)

[55] *Idem*.

[56] Acórdão do TJ, Proc. C-507/17, pedido de decisão prejudicial apresentado pelo *Conseil d'État* (França) em 21 de agosto de 2017; Lomas, Natasha. "Google's right to be forgotten appeal heading to Europe's top court", *TechCrunch*, 2017, p. 21.

3.1. Apagamento global

Começando pela primeira pergunta feita ao TJ, relativa ao alegado escopo global do apagamento de dados, teremos de regressar ao Direito Internacional e averiguar se tal abordagem não interfere com o princípio da não ingerência nos assuntos de Estado terceiro, ou seja, se é permitida à luz da soberania territorial no ciberespaço.

De facto, aquando de um apagamento de informação na *Internet*, entramos novamente no ciberespaço, pelo uso de meios eletrónicos e através de redes interdependentes e conectas. Assim sendo, para que o apagamento seja global, teremos de responder a uma questão de vital importância: poderá a UE, respeitando as normas e princípios do Direito Internacional, exigir aos motores de busca o apagamento de informação em domínios não europeus?

Primeiramente, podemos vislumbrar que as estruturas que acedem ao ciberespaço (por exemplo, computadores pessoais) e, neste caso, a um motor de busca, são objeto do poder soberano do respectivo Estado onde se localizam. Ora, conforme a teoria da soberania territorial, pode um Estado criar e aplicar regras às ciberinfraestruturas que se encontrem no seu território. Por exemplo, os EUA podem regular o acesso dos computadores situados no seu território, e a UE poderá regular o acesso dos computadores localizados na UE.

Por outro lado, não são só as ciberinfraestruturas situadas num certo Estado que são alvo da soberania desse Estado, mas também as ciberopeações que ocorram no seu território. O que é, então, uma ciberoperação? Tal conceito prende-se com a criação, modificação, armazenamento e transmissão de informação, através do espectro eletromagnético, em conjugação com aparelhos eletrónicos[57]. Assim sendo, qualquer tipo de transmissão de informação entre uma infraestrutura, situada num Estado terceiro, que suporte um motor de pesquisa e, por exemplo, um computador pessoal situado na UE (ou outra qualquer ciber-infraestrutura), será merecedor de poderes soberanos da União[58].

---

[57] Kuehl; Daniel T.. "From cyberspace to cyberpower: Defining the problem", in *Cyberpower and national security*, National Defense University Press, 2009, p. 28 e 29.

[58] Por esta razão se justifica, por exemplo, que o acórdão Google Spain não infrinja o Direito Internacional. Muito embora o tratamento de dados tenha sido feito nos EUA, os dados

Já as situações contrárias, em que a UE exerce poderes soberanos sobre as ciberinfraestruturas situadas em Estado terceiros, que conduzam ciberoperações sem interferência no território europeu, parecem ser mais difíceis de conceber, pelo facto daquelas não se encontrarem no espaço europeu, nem estas se intersetarem com a UE. Encontramos, assim, como grande obstáculo a um tal apagamento de dados o princípio da não ingerência em assuntos de Estados terceiros.

Contudo, e como concluído anteriormente, poderá um Estado aplicar as suas normas a entidades ou atividades localizadas fora do seu território, em certas situações, *maxime* de acordo com a teoria dos efeitos. Cabe assim perguntar: será que o armazenamento, criação e modificação de informação, num Estado terceiro, bem como a transmissão de informação, através da *Internet*, entre Estado terceiros poderão ser submetidos ao braço normativo europeu, com base nestes princípios?

Ora, uma resposta a esta questão não é, de todo, fácil. Situações podem existir em que, por exemplo, por motivos de pura segurança nacional, é argumentável que um Estado possa exigir o apagamento global de informação disponível na *internet*, mesmo que essa não chegue a ser transmitida no seu território, até face ao dever de toda a comunidade internacional de evitar que as suas ciberinfraestruturas e ciberoperações causem danos a outros Estados.

Contudo, estas situações são excepcionais, pelo que, por regra, dar-se-á uma resposta negativa à anterior questão. Realmente, se as ciberoperações não penetram no território europeu, nem estão as ciberinfraestruturas que as conduzem sob o domínio de aplicação do direito da UE, então só se estiver em causa uma situação que justifique a invocação dos outros princípios de soberania para lá da territorialidade se poderá arguir a possibilidade de a UE exigir o apagamento global. Assim sendo, exigir um apagamento global como regra geral da aplicação do art. 17.º do RGPD violaria os princípios da independência e igualdade entre Estados e o da não ingerência em assuntos internos de Estados terceiros.

Por último, também poderão estar em causa problemas na compatibilização entre direitos fundamentais de Estados diferentes. Realmente, grande parte dos Estados não europeus (*maxime* EUA) ainda não consagraram um

---

eram transmitidos em espaço europeu, pelo que a União Europeia podia aplicar o normativo de proteção de dados a essa ciberoperação.

direito ao apagamento de dados, pelo que, se se recorrer ao apagamento global, estar-se-á a eliminar informação sem que tal mecanismo esteja previsto no ordenamento jurídico do Estado em causa. Pode até ser colocada a seguinte pergunta: será que a aplicação de requisitos europeus a uma escala global afeta, em grande medida, a liberdade de expressão em Estados terceiros?

3.2. Apagamento baseado no domínio

A segunda metodologia de apagamento de dados possível é a baseada nos domínios utilizados para as pesquisas realizadas num motor de busca (uma *domain-based erasure*). Esta abordagem ao processo de apagamento permite modificar os resultados de uma pesquisa em função da extensão utilizada para aceder ao motor de busca (por exemplo, se esta for .pt, .es, .fr, .us ou .com)[59], ou seja, proceder a operações de apagamento em relação às versões europeias do motor de busca e não o fazer em relação às demais.

Na senda do caso *Google Spain* e da operacionalização do direito à desindexação, esta metodologia fundada no domínio foi advogada pelos vários motores de busca demandados por titulares de dados pessoais, com destaque para a *Google Inc*. Esta decidiu limitar a remoção de resultados de busca decorrente da aplicação do direito europeu de proteção de dados às suas versões europeias, permanecendo inalteradas as restantes, como por exemplo a *Google.com*.

Esta solução mereceu, de imediato, críticas das autoridades europeias de proteção de dados, pela ausência de medidas suplementares de limitação de acesso a dados cuja supressão fosse ordenada[60]. Foi por estas entidades observado que o efeito útil da supressão de uma hiperligação seria posto em causa se dados removidos dos domínios europeus de um dado motor de busca pudessem ser consultados através de uma simples mudança da extensão utilizada para aceder a tal plataforma de

---

[59] Alsenoy, Brendan van; Koekkoek, Marieke. "The extra-territorial reach of the EU's "right to be forgotten", *KU Leuven Centre for IT & IP Law,* 2015, p. 16 e ss.

[60] *Idem*, p. 4.

pesquisa[61-62]. Esta mesma posição foi seguida por inúmeros tribunais nacionais, como por exemplo o *Tribunal de Grande Instance de Paris* que, num caso que opôs dois cidadãos franceses à *Google*, rejeitou tal abordagem baseada no domínio, considerando-a insuficiente[63].

Não podemos deixar de seguir tais opiniões, transpondo-as para o contexto do apagamento de dados. Uma *domain-based erasure* encontra como óbice a sua (in)eficiência, ao não permitir assegurar o efeito útil de um apagamento de dados, em relação a qualquer pesquisa realizada por qualquer sujeito, constatada a facilidade que o utilizador normal tem de mudar a extensão do *site* do motor de busca, assim consultando informação removida por meio deste modelo de apagamento. Com efeito, a proteção de qualquer conjunto de dados pessoais nunca poderá ser eficiente e completa se os expedientes utilizados para a assegurar forem facilmente contornáveis, como é o caso de um método exclusivamente baseado no domínio[64].

3.3. Apagamento híbrido fundado na geo-localização: o "modelo Youtube*"*

Chegamos, por fim, à última metodologia de apagamento a discutir que se compatibiliza com a técnica do "bloqueio geográfico", ou seja, que conforma os resultados de uma pesquisa (revelando ou não dados cujo

---

[61] Grupo de Trabalho do Artigo 29; *Guidelines On The Implementation Of The Court Of Justice Of The European Union Judgment In "Google Spain And Inc V. Agencia Española De Protección De Datos (AEPD) And Mario Costeja González"*, 26 de novembro de 2014, para. 20.

[62] Por exemplo, bastaria a um cidadão português que não conseguisse, através da google.pt aceder a uma notícia sobre M. González (em função da supressão de links ordenada no processo Google Spain) mudar a sede da sua pesquisa para a google.com para consultar tal informação e esvaziar o efeito da supressão de hiperligações já realizada.

[63] "It is in vain that Google France asks (...) that the injunction be limited to links on Google.fr, seeing as it does not establish the impossibility to connect from French territory to other domain name extension of Google's search engine.", tradução inglesa de um extrato retirado do Acórdão do Tribunal de Grande Instance de Paris, *M. et Mme X et M. Y v. Google France*, 16 de setembro de 2014, disponível em http://www.legalis.net/spip.php?page=jurisprudence-decision&id_article=4291. (acedido a 09/03/2019)

[64] Alsenoy, Brendan van; Koekkoek, Marieke. "The extra-territorial reach of the EU's "right to be forgotten"*, KU Leuven Centre for IT & IP Law*, 2015, p. 4 e 5.

apagamento foi ordenado) com a localização do IP utilizado para a fazer[65]. Deixamos já patente que este é o método por nós preconizado como consequência, por defeito, de um pedido para apagamento bem-sucedido. A nossa tese baseia-se na convicção de que esta abordagem dá resposta às falhas apontadas quer ao apagamento global quer ao apagamento baseado no domínio, surgindo como complemento imprescindível a este último.

Em primeiro lugar, um apagamento mediante *geoblocking* permitiria (regra geral) um exercício razoável e moderado da competência normativa da UE em direção a Estados-terceiros onde o direito ao apagamento não existe, assim cumprindo todos os crivos do Direito Internacional Público, da jurisprudência da União e dos pareceres das DPA europeias já avançados anteriormente, que tornam criticável uma extensão global do apagamento de dados[66].

Ora, tendo, por via da regra, a UE apenas a possibilidade de controlar ciberoperações que interfiram com o seu território, então, através do *geoblocking* tal seria respeitado, permitindo às autoridades europeias estender a sua jurisdição sobre processamentos externos e, ao mesmo tempo, confinar o impacto da sua atuação ao espaço europeu[67]. De facto, a partir do momento em que dada informação seja transmitida, através de qualquer domínio, para uma ciberinfraestrutura situada na UE, terá esta o poder de aplicar as suas normas a essas transmissões de dados. Caso estas não passem pelo espaço europeu então, por via da regra, tal aplicação parece violar o Direito Internacional. Nesta senda, o *geoblocking* apresenta-se como um meio termo razoável, em que a UE apaga os dados de todos os domínios acedidos através de uma ciberinfraestrutura situada na UE, sendo respeitados os princípios internacionais da soberania estatal.

Em segundo lugar, este método cumpriria a exigência de uma fórmula eficiente (porque onerosa de contornar) de garantia dos direitos dos titulares de dados pessoais, formulada pelas DPA e tribunais na crítica à *domain-based approach* posta em prática pela *Google*. E, neste campo, não

---

[65] Um Endereço de Protocolo da Internet (endereço IP), é um rótulo numérico atribuído a cada dispositivo conectado a uma rede de computadores que utilize a Internet para comunicação. Um endereço IP serve, sobretudo, uma função de localização do seu respetivo dispositivo.

[66] Ver, genericamente, Capítulo 3 deste artigo.

[67] Alsenoy, Brendan van; Koekkoek, Marieke. "The extra-territorial reach of the EU's "right to be forgotten", *KU Leuven Centre for IT & IP Law*, 2015, p. 19.

podemos ignorar que as técnicas de *geoblocking* utilizadas pela *Google* foram, de facto, consideradas inadequadas porque ineficientes para garantir o efeito útil das normas europeias de proteção de dados (na instância do direito à desindexação)[68]. Cumpre sinalizar que a abordagem deste motor de busca consistiu numa utilização cumulada de um suprimento de informação em função do domínio e do denominado *soft geoblocking*.

Ora, a abordagem da *Google* faz com que, tendo sido ordenado um suprimento de informação no espaço europeu, quaisquer utilizadores a operar a partir de tal território que queiram consultar domínios exteriores à União (*i.e. Google.com*) são automaticamente redirecionados para a versão do motor de busca específica do país onde se localiza o IP da infraestrutura utilizada na pesquisa (como um computador pessoal)[69]. O *geoblocking* presente neste modelo corresponde a este redirecionamento, mas é facilmente contornável visto que podem os utilizadores reverter tal procedimento: (i) clicando numa opção disponibilizada de "mudar para *Google.com*"; ou (ii) voltando a escrever a versão *.com* do motor de busca na barra de pesquisa.

Tal facilidade de contornar este expediente de geo-localização valeu-lhe o epíteto de *soft geoblocking*[70], por oposição ao *hard geoblocking*, em que tal possibilidade de reverter a filtragem de resultados de busca baseada na localização geográfica de quem os pretende produzir não existe. É um tal modelo de *hard geoblocking* aquele cuja transposição para a realidade do apagamento de dados defendemos, cumulado com as outras abordagens acima explicadas, como passamos a descrever.

Quando seja realizado um apagamento de dados, este restringir-se-á, por princípio, ao espaço europeu. Como? Ainda que não detalhando as vicissitudes tecnológicas que encerrariam tal operação (ao pretendermos somente focar as questões jurídicas da temática subjacente), não podemos deixar de reconhecer que a mesma implicaria, com a maior das probabilidades, uma alteração da estrutura de funcionamento dos motores de busca no processo de armazenamento e tratamento de dados, uma vez que exigiria a separação dos servidores de indexação utilizados para o espaço

---

[68] *Idem*, p.15.

[69] *Idem*, p.18.

[70] Outra expressão possível para designar tais realidades é *soft geofiltering tools*.

europeu e fora dele[71]. Uma vez tendo procedido a tal apagamento, os resultados modificados em conformidade com a legislação europeia seriam disponibilizados exclusivamente em domínios europeus (em articulação com a *domain-based approach*), domínios esses que seriam os únicos. Estes, tendo sido identificada a sua localização, não conseguiriam ter acesso, por nenhuma das vias possíveis acima identificadas, às versões não-europeias do motor de busca usado.

Semelhantes abordagens são realizadas em plataformas como o *Youtube* ou a *Comedy Central*, em que alguns dos seus conteúdos só estão disponíveis para utilizadores americanos, estando os restantes utilizadores – cuja geolocalização extravase aquele âmbito – impedidos de o consultar ou de contornar o seu suprimento.

Um óbice significativo a estas técnicas não deixa de ser a impossibilidade de uma completa eficácia das mesmas, que podem ser contornadas, por exemplo, através da utilização de *proxy servers* que obnubilem o IP utilizado numa pesquisa. No entanto, é nossa convicção de que a eficácia destas técnicas não implica uma *impossibilidade de circunvenção*, mas antes uma *onerosidade de circunvenção*. Fazendo nossas as palavras de Schultz, um expediente informático nesta matéria será eficiente se tornar a ação que visa evitar substancialmente mais difícil de executar, onerando significativamente quem a deseje levar a cabo[72]. Tal ónus parece-nos existir na necessidade de utilização de um *proxy server*, uma vez que este é uma ferramenta não conhecida pelo utilizador médio, que é aquele que não possui conhecimentos especiais de informática.

Em suma, o modelo acima descrito oferece o complemento necessário à *domain-based approach* por forma a concretizar o art. 17.º do RGPD no mundo da *Internet*, que tanto exige em matéria de conformidade e coordenação interjurisidicional. Deve, por isso, constituir o modelo-regra aquando da aplicação do RGPD. Não podemos deixar, no entanto, de avançar que este

---

[71] Muito provavelmente, funcionando em *data centers* (locais onde estão concentrados os sistemas computacionais de uma qualquer empresa, como por exemplo, sistemas de telecomunicações ou de armazenamento de dados) exclusivamente para operações dentro da UE.

[72] Schultz; Thomas. "Carving Up the Internet: Jurisdiction, Legal Orders, and the Private/Public International Law Interface", in *European Journal of International Law*, v. 19, n. 4, 2008, p. 822.

modelo não pode deixar de contemplar exceções em que um apagamento global se justifica quando seja a única forma de assegurar o efeito útil do direito em análise.

3.4. A opinião do advogado-geral M. Szpunar

No âmbito do processo C-507/17 (Google v. CNIL), foi muito recentemente divulgada a opinião do Advogado-Geral M. Szpunar sobre a extensão territorial do direito à desindexação, cujas conclusões podemos transpor para o presente estudo, muito embora se baseiem na interpretação da Diretiva 95/46/EC[73].

Como ponto de partida, afirma o Advogado-Geral que nem o art. 4.º da Diretiva nem o Acórdão *Google Spain* tratam especificamente a questão do âmbito territorial do direito à desindexação, ainda que delimitem o âmbito territorial do diploma no qual este se insere. Estando estas orientações vertidas no art. 3.º RGPD, não se nos afigura nenhuma razão para não transpor, também, este raciocínio para o direito ao apagamento (art. 17.º RGPD)[74].

Assim, considera o Advogado-Geral que, aquando da definição da extensão territorial do direito à desindexação, devem ser distinguidas as buscas, conforme sejam feitas dentro ou fora da EU. Em relação às segundas, não devem os respetivos resultados ser afetados pela supressão de hiperligações[75]. Neste sentido, propõe um modelo em que os motores de busca não têm de levar a cabo a supressão em todos os seus domínios, afastando, por isso, uma extensão global do direito à desindexação[76]. No entanto, afirma que, uma vez efetuada a desindexação nas versões europeias de um dado motor de busca, devem ser adotadas todas as medidas necessárias para assegurar a efetividade de tal direito, nomeadamente através do *geoblocking*[77].

---

[73] Opinião do Advogado-Geral (M. Maciej Szpunar) do TJ, Proc. C-507/17, *Google*, ECLI:EU:C:2019:15.

[74] *Idem*, para. 45.

[75] *Idem*, paras. 45 e 46.

[76] *Idem*, paras. 62, 63 e 79.

[77] *Idem*, paras. 71, 74 e 78.

Para fundamentar as suas conclusões, o Advogado-Geral argumenta que (i) uma desindexação global seria desconforme ao Direito Internacional Público[78] e que (ii) poderia abrir um precedente a práticas de restrição de acesso à informação, nomeadamente por parte de regimes autoritários[79].

Como é fácil de observar, a proposta do Advogado-Geral vai de encontro ao modelo de apagamento híbrido fundado na geolocalização defendido no presente artigo, ainda que se refira ao direito à desindexação. No entanto, não nos parece incorreto aplicar a mesma lógica ao direito ao apagamento de dados.

Por fim, o Advogado-Geral equaciona a possibilidade de, em casos excecionais, conferir à desindexação um âmbito global, à luz do que já é prática quanto a atividades exteriores à UE que afetem o mercado interno europeu. No entanto, pela imaterialidade inerente à Internet, considera difícil efetuar uma analogia entre ela e o mercado interno, cujas fronteiras estão já estabelecidas[80]. No nosso entender, tal analogia será possível para plenamente aplicar a teoria dos efeitos ao apagamento de dados, se recorrermos às teses da soberania no ciberespaço já por nós abordadas *supra*.

Conclusão

Cumpre, por fim, sistematizar as soluções defendidas no presente artigo, assentando tal raciocínio no normal *ictus* de um pedido para o apagamento de dados.

Primeiramente, devem as DPAs avaliar, caso a caso, se o apagamento de dados requerido corresponde a um interesse significativo da UE, quando comparado com os interesses de outros Estados terceiros com os quais a querela *sub judice* se relacione. Tal acontecerá se uma ciberoperação for realizada na União ou, tendo sida realizada fora dela, tenha um efeito manifestamente disruptivo no ordenamento europeu em matéria de proteção de dados. Se não se verificar esta conexão relevante do pedido ao fórum europeu, então tal demanda não deve ser admitida perante as DPAs.

---

[78] *Idem*, paras. 47 a 49.

[79] *Idem*, paras. 60 e 61.

[80] *Idem*, paras. 48 a 53.

Se, pelo contrário, tal ligação ao ordenamento europeu se verificar, deve o apagamento proceder e devem as autoridades atender a uma segunda camada de compatibilização de interesses, as relativas à extensão extra-europeia do apagamento. Por defeito, consideramos que em relação à informação disponibilizada fora da União prevalecerá o interesse do Estado terceiro em mantê-la acessível aos seus cidadãos. Além do mais, o apagamento global tem como obstáculo direto a sua difícil compatibilização com o princípio da não ingerência em assuntos internos de outros Estados.

Assim, num confronto teórico entre o apagamento global e o baseado nos domínios, é o segundo modelo aquele que permite à União controlar condutas externas de tratamento de dados sem interferir na soberania de Estados terceiros. Mas este modelo, por si só, mostra-se ineficaz na proteção dos direitos fundamentais dos titulares de dados. Nesse sentido, será de aplicar um modelo híbrido fundado num *hard geoblocking*, nunca fugindo à possibilidade de arguir um apagamento global, quando os interesses da UE se sobreponham àqueles de Estados terceiros no que diz respeito ao apagamento extraterritorial de dados de um certo titular.

Deste modo, pode a UE assegurar a verdadeira eficácia das disposições do RGPD, mais concretamente do seu art. 17.º, através de um exercício de competências jurisdicionais – dos tribunais e DPA – moderado e razoável no espaço internacional que, por não se pretender estender até onde não terá a devida legitimidade (sempre atento às nuances da natureza global da *Internet*), se torna incomparavelmente mais eficaz.