CADERNOS ELETRÔNICOS
Direito Internacional sem Fronteiras
ISSN 2675-2514
VOLUME 2 | NÚMERO 1 | 2020

O REGULAMENTO GERAL DE PROTEÇÃO DE DADOS (GDPR): UMA ANÁLISE DO *EXTRATERRITORIAL SCOPE* À LUZ DA JURISDIÇÃO INTERNACIONAL

The General Data Protection Regulation: a study of the extraterritorial scope under the perspective of international jurisdiction

João Victor Lima CAETANO
Bacharel em Direito, Centro de Ciências Jurídicas, da Universidade de Fortaleza. E-mail: < jv270699@gmail.com >. ORCID: < https://orcid.org/0000-0002-6886-1486 >.

RESUMO: A aprovação do Regulamento Geral de Proteção de Dados da União Europeia (GDPR) em 2016 representou a maior inovação legislativa do mundo em matéria de proteção de dados pessoais. Paralelamente, a legislação europeia também se revelou bastante inovadora no tocante ao seu escopo territorial, prevendo a possibilidade de sua aplicação fora das fronteiras do bloco europeu. Nesse sentido, a presente pesquisa buscou analisar como o escopo territorial da GDPR coaduna com os princípios de jurisdição internacional. Através da compreensão detalhada do artigo 3º deste regulamento, dos seus conceitos e da posterior explanação dos maiores princípios de jurisdição internacional vigentes, foram feitas considerações a respeito dos substratos jurídicos sobre os quais a legislação europeia está sedimentada.

PALAVRAS-CHAVE: Proteção de Dados. Princípio da Territorialidade. Extraterritorial Scope. Direito Internacional. Execução Normativa.

ABSTRACT: The approval of the General Data Protection Regulation in 2016 by the European Parliament represents the most innovative law worldwide concerning Personal Data Protection. Moreover, the European law has also revealed itself strongly disruptive on its territorial scope, addressing the possibility of application outward its borders. Thereby, the present paper aimed at analysing how the GDPR's territorial scope complies with the principles of international jurisdiction. By means of the detailed

Correspondente: CAETANO, João V. L.
Artigo recebido: 08 junho de 2020
Artigo aceito: 30 junho de 2020

comprehension of article 3 and its main concepts, and the exposition of standards of international jurisdiction in effect nowadays, this paper examined where the GRPR is legally grounded.

KEYWORDS: Data Protection. Territorial Principle. Extraterritorial Scope. International Law. Law Enforcement.

1 INTRODUÇÃO

Com o advento exponencial da tecnologia ao longo dos últimos anos, o fenômeno da circulação de dados tem emergido como uma temática de grande relevância. Diante disso, os meios de conexão em rede, tais como computadores, dispositivos móveis, aplicativos e outros, tem representado uma coleta de dados pessoais em massa.

Como resultado de um mundo cada vez mais globalizado, quase todas as formas de transações da vida cotidiana podem ser feitas por meio virtual, como por exemplo compras online, reuniões de negócios, investimentos e operações financeiras. Em cada uma delas, tem-se um compartilhamento constante de dados para fins comerciais de segurança e de controle de informações, fatores que figuram como razões para o presente estudo (SOLOVE; SCHWARTZ, 2018, p. 02).

É diante da dependência dos fluxos desses dados, viabilizados pelos avanços tecnológicos, que há a necessidade de elaboração de regulamentações que garantam a segurança das informações dos usuários (PINHEIRO. 2018, p. 17). Para tanto, o Regulamento Geral de Proteção de Dados (*General Data Protection Regulation - GDPR)*, que entrou em vigor em 2018, surge com o intuito de promover novos parâmetros legais para o tratamento dessas informações. Atualmente, este regulamento figura como a maior inovação legislativa, inclusive em âmbito internacional, no que tange a proteção ao processamento de dados.

O Regulamento Europeu expressa uma intenção de transpor fronteiras físicas para se adequar ao mundo virtual sem fronteiras. É a partir dessa extrapolação jurisdicional, que o presente artigo se constrói. Diante disso, viu-se a importância de promover o entendimento a respeito do processo de proteção de dados no âmbito internacional, em aspectos de jurisdição e de execução normativa, especialmente no que diz respeito ao objeto de estudo que aqui é trazido: o escopo extraterritorial do Regulamento de Proteção de Dados da União Europeia

Assim, este artigo responde às seguintes questões principais: Como o escopo extraterritorial da GDPR se adequa ao princípio da territorialidade? Como se dará a execução das normas de proteção de dados fora do âmbito da União Europeia, e qual a sua força executiva? E, também, responde às seguintes questões secundárias, que permeiam à discussão em epígrafe: O legislador europeu realmente teve a intenção de alcançar uma realidade extra à União Europeia? A lei em questão tem os mecanismos necessários para executar suas normas de *compliance*?

Este trabalho é composto por pesquisas exploratórias, fundamentadas por meio de referências bibliográficas, como livros, artigos, periódicos, jornais, revistas e dados oriundos de institutos especializados. Quanto à finalidade, a pesquisa é descritiva, de modo que se teceu uma conjectura detalhada da realidade à época da investigação, de modo a interpretar e classificar os fatos. Quanto aos resultados, a pesquisa é caracterizada como pura, uma vez que a finalidade principal é a ampliação do conhecimento sobre o tema em tela.

Para tanto, no primeiro capítulo foi feita uma introdução às primeiras formas de proteção de dados no mundo, através de uma breve linha do tempo até desembocar no surgimento da GDPR, momento em que foi abordado o seu contexto histórico, importância, e quais seus objetivos em comparação à sua predecessora, a *Directive of Data Protection (DPD)*. No segundo capítulo, foi construída uma análise detalhada do

Cadernos Eletrônicos Direito Internacional sem Fronteiras, Vol. 2, Núm. 1, Jan-Jun 2020, e:11

artigo 3 da GDRP. Por fim, foram apresentados os princípios de jurisdição internacional mais pertinentes para o tema em tela.

2 HISTÓRICO DA PROTEÇÃO DE DADOS

A evolução tecnológica tem resultado em uma revolução na maneira como o ser humano se relaciona com os dispositivos de conexão em rede. Para cadastros virtuais, criação de contas em aplicativos, acesso à informação, todos os aspectos da vida dentro da estrutura social associada ao crescente fluxo informacional, a chamada sociedade em rede (CASTELLS; CARDOSO. 2005, p 03) são alimentados por dados pessoais (CASTELLS. 2010, p. 254).

Assim, ao longo desta evolução tecnológica, a preocupação com a maneira com que esses dados eram tratados e protegidos se tornou cada vez mais premente, à medida em que as primeiras concepções de direito à privacidade foram surgindo.

Analisando a breve linha do tempo da proteção de dados no mundo, as primeiras manifestações do direito à privacidade remontam ao ano de 1890, com dois advogados norte-americanos, Samuel D. Warren e Louis Brandeis (MONTI;WACKS, 2019, p. 04), os quais escreveram o artigo O Direito à Privacidade (*The Right to Privacy)*, aclamado como influência excepcional sobre os demais periódicos americanos. Nesta primeira manifestação, o direito à privacidade foi definido como "o direito de ser deixado sozinho"[1].

Em 1948, a Declaração Universal dos Direitos Humanos (1948), através do seu artigo 12, regulou que ninguém poderá ser sujeito à violação da sua privacidade. Neste ponto, a privacidade foi arrolada não apenas como um direito, mas também como um

[1] "The makers of the Constitution conferred the most comprehensive of rights and the right most valued by all civilized men—the right to be left alone." - Justice Louis D. Brandeis. SKOUSEN, Mark**. The Right to Be Left Alone - The Enjoyment of Financial and Personal Privacy Is Fundamental to a Free and Civil Society**. Disponível em: https://fee.org/articles/the-right-to-be-left-alone/. Acesso em: 07 de maio de 2020.

valor essencial para o desenvolvimento da personalidade individual para a proteção da dignidade humana.

Já no âmbito da União Europeia, o ano de 1950 foi marcado pela aprovação da Convenção Europeia de Direitos Humanos (*EU Convention on Human Rights)*, que trouxe, em seu artigo 8º, a tutela da vida privada, que não deveria sofrer nenhum tipo de interferência. Mais tarde, no ano de 1981, o Conselho Europeu adotou a Convenção de Proteção de dados, que demonstrou um avanço significativo no tocante ao rol de proteções à privacidade, alcançando todas as esferas da vida social, como raça, posicionamento político, saúde, religião, vida sexual e ficha criminal.[2]

Em sequência, no ano de 1995, foi aprovada a Diretiva de Proteção de Dados (*Directive Protection Data – DPD 1995/46 EC)*, doravante denominada "*DPD",* com o potencial de representar a legislação de maior influência no âmbito europeu, no tocante à proteção de dados. Aprovada após a criação de muitas leis domésticas em cada país europeu, a *DPD* nasceu com dois objetivos principais: harmonizar todas as leis nacionais em um só diploma e promover a alta proteção de dados pessoais, para proporcionar um fluxo livre entre os países da União.

Entretanto, de acordo com os sistemas jurisdicionais europeus, a *DPD* não poderia ser aplicada diretamente, devendo ser recepcionada por cada país, de acordo com suas leis nacionais para, assim, ser aplicada ao caso concreto (LEE. 2018, p. 34). Tal requisito consistiu em uma grande margem de discricionariedade por parte dos estados membros.

[2] In addition to providing guarantees in relation to the collection and processing of personal data, it outlaws the processing of "sensitive" data on a person's race, politics, health, religion, sexual life, criminal record, etc., in the absence of proper legal safeguards. **Treaty nº 108. Summary, Council of Europe.** Disponível em: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108. Acesso em 07 de maio de 2020.

Cadernos Eletrônicos Direito Internacional sem Fronteiras, Vol. 2, Núm. 1, Jan-Jun 2020, e:11

Assim, não obstante o principal objetivo da *DPD* fosse harmonizar as disposições legais em todos os países do bloco, a discrepância na aplicação das regras a cada caso concreto, de acordo com as diferenças entre os estados, foi um resultado inevitável. Somado a isso, o nível de aplicação e a força executória da Diretiva variava de estado para estado. Por essas e outras razões é que emergiu a necessidade de uma profunda reforma na legislação europeia. De acordo com Leenes *et al.* (2012, p. 134, tradução nossa):

> Embora a situação jurídica dos cidadãos dispostos a defender os seus direitos de privacidade tenha melhorado em muitos estados europeus, as diferentes leis de proteção de dados criaram uma complicada gama de retalhos de previsões legais repletas de incerteza jurídica, o que causou enormes impedimentos para o setor privado, principalmente no caso da transferência de dados pessoais de um país europeu para outro.

Assim, embora houvesse uma previsão legal que em linhas gerais devesse ser aplicada de maneira uniforme, o que se reproduziu de maneira fática foi uma grande variedade de leis nacionais, através das quais cada estado europeu retirava uma grande margem de discricionariedade quando da aplicação da Diretiva.

Destaca-se também que em virtude de tal discrepância legal, muitas empresas norte americanas apoiavam-se nas brechas das leis para não adotar as medidas de *compliance* (DENLEY, et al. 2018, p. 05). Isso também se deu em razão de haver diferenças principiológicas entre o padrão norte americano de proteção de dados e o padrão europeu.

Estava claro que a visão europeia em relação à proteção da privacidade dos seus consumidores estava fragilizada, o que resultou na decisão de criar nova uma legislação pan-europeia que protegeria os seus cidadãos com maior efetividade. Diante disso, com o objetivo de uma vez por todas harmonizar as divergências legais entre os membros

Cadernos Eletrônicos Direito Internacional sem Fronteiras, Vol. 2, Núm. 1, Jan-Jun 2020, e:11

do bloco, e também objetivando elevar o nível de proteção de dados para os cidadãos europeus, a União Europeia apostou na adoção da GDPR (VOIT; et al**.** 2017, p. 01).

3 O REGULAMENTO GERAL DE PROTEÇÃO DE DADOS (*GENERAL DATA PROTECTION REGULATION – GDPR)*

Após 4 anos de discussões sobre como a reforma legislativa europeia se daria, em 14 de abril de 2016 o Parlamento Europeu aprovou o texto base que seria a nova regulação jurídica – e marco legal – para a proteção de dados em toda a extensão europeia e, de maneira inovadora, também além das fronteiras do bloco. A lei passou por um período de dois anos de vacância, visando permitir que as empresas, companhias e organizações, ou como a própria lei trata, os *processors*[3] ou *controllers*[4]*,* que tratam com dados pessoais, pudessem tomar medidas de alinhamento com os padrões da lei.

Então, no dia 25 de maio de 2018 entrou em vigor a *General Data Protection Regulation – GDPR* (Regulamento Geral de Proteção de Dados), a lei que tem como alvo precípuo a proteção, com máxima eficácia, ao direito à privacidade, através de dados pessoais e dados sensíveis, ao passo em que, em paralelo, estimula e facilita a circulação desses dados dentro do território dos estados membros, o que também significa uma tentativa de avançar na economia de dados (CUSTERS; et al. 2019, p 01).

[3] 'Processor' means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller. Article 4(8) of the GDPR. Disponível em: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679. Acesso em 15 de maio de 2020.

[4] 'Controller' means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law. Article 4(7) of the GDPR. Disponível em: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679. Acesso em 15 de maio de 2020.

Com 173 considerandos, 11 capítulos e 99 artigos[5], a GDPR foi incorporada ao ordenamento jurídico europeu como um grande avanço para a proteção de dados não só na Europa, mas também no mundo, com o entendimento de que, assim como o ambiente virtual não tem fronteiras, assim também o deve ser a lei, de modo que possa transpor os limites nacionais.

Dentre os fundamentos jurídicos que deram ensejo ao novo regulamento europeu, é premente destacar a harmonização das leis de proteção de dados existentes em cada país do continente europeu (LEE. 2018, p 68). Pois, ao contrário da sua predecessora *(DPD),* que tinha caráter de diretriz, que consistia em um mero conjunto de normas que previam um resultado a ser alcançado, GDPR tem uma estrutura jurídica de regulamento. Isto significa que o Regulamento Europeu é uma ordem que deve ser executada de modo homogêneo por cada estado membro, vindo a tornar-se lei nacional em cada um deles e, com exceção de alguns casos específicos de segurança nacional, não há nenhuma oportunidade de mudanças ao passar pelo processo legislativo doméstico (DIBLLE, 2020, p. 13).

3.1 O EXTRATERRITORIAL SCOPE DA GDPR

Visando se adequar à realidade virtual e ao caráter transnacional da ciência da proteção de dados[6], o Regulamento Geral de Proteção de Dados Europeu trouxe como inovação, em seu texto legal, o chamado Escopo Extraterritorial (*Extraterritorial Scope)*.

[5] Official Journal of the European Union. Disponível em: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679. Acesso em 15 de maio de 2020.

[6] "Last, but not least, data privacy has acquired a transnational aspect. While, not a long time ago, the data controller, the data subject and the means used for data processing were often located in one country, [2] the development of international trade, the new technologies and the new corporate structures of multinational companies have increased the importance of the international processing and transfer of data. This new borderless environment does not give much credibility to data protection laws with a domestic territorial scope. A "territorial scope 2.0" [3] is now required". **The Challenges Faced by the Extraterritorial Scope of the General Data Protection Regulation.** Disponível em: https://www.jipitec.eu/issues/jipitec-9-2-2018/4723. Acesso em 21 de maio de 2020.

Seu objetivo principal é transpor as barreiras físicas e alcançar também toda e qualquer conduta de empresas e organizações que manipulam dados pessoais de cidadãos europeus, seja em parte ou em totalidade, fora do território comum do bloco (VERMEULEN; LIEVENS, 2017, P. 78).

Previsto em seu artigo 3º, o escopo extraterritorial da GDPR será aplicado fora da União Europeia nos seguintes casos: i) quando o processamento de dados pessoais se der no contexto das atividades de um estabelecimento de *controller* ou *processor* na União, independentemente se o processamento se dá dentro da União ou não; ii) quando o processamento de dados dos indivíduos que estão na União, por *controller* ou *processor* não estabelecidos na União, for relacionado à oferta de produtos ou serviços, ou ao monitoramento de comportamento, à medida em que o comportamento do indivíduo seja dentro da União[7].

Sob este espectro, duas são as discussões centrais a partir das vertentes dentro do referido artigo, a saber: a presença considerável do estabelecimento de um *controller* ou *processor* no território da União, e o monitoramento dos titulares de dados dentro da UE (VERMEULEN; LIEVENS. 2017, p. 79).

3.1.1 Artigo 3(1): conceitos de *"establishment"* e *"in the context of the activities"*

Dentre os conceitos presentes no artigo 3(1), os mais importantes para o presente estudo são: a) dados pessoais: qualquer informação relacionada à uma pessoa física identificada ou identificável; b) processamento: qualquer operação ou conjunto de operações, compostas por dados pessoais, sendo ou não por meios automatizados; c) controlador: pessoa física ou pessoa jurídica, autoridade pública, agência ou outro agente que, individualmente ou em conjunto com outros, determinam as finalidades e

[7]Article 3 of the General Data Protection Regulation. Disponível em: https://eur-lex.europa.eu/eli/reg/2016/679/oj. Acesso em 21 de maio de 2020.

Cadernos Eletrônicos Direito Internacional sem Fronteiras, Vol. 2, Núm. 1, Jan-Jun 2020, e:11

meios pelos quais o processamento de dados se dará; d) processador: pessoa física ou pessoa jurídica, autoridade pública, agência ou outro agente que processa dados pessoais em nome do controlador[8].

Nessa toada, o artigo 3(1) predica que o regulamento se aplica ao processamento de dados pessoais no contexto das atividades (*in the context of the activities)* de um estabelecimento (*establishment)* de um controlador ou processador (*controller* ou *processor)*, independentemente se o processamento se dá dentro do território da União ou não. Tal é a disposição do texto oficial (General Data Protection Regulation, 2016):

> Artigo 3(1): Este Regulamento aplica-se ao processamento de dados pessoais no contexto das atividades de um estabelecimento de um controlador ou processador na União, independentemente se o processamento se dá dentro da União ou não (tradução nossa)[9].

De acordo com a interpretação do artigo supracitado, para que o indivíduo ou empresa estejam sujeitos à aplicação da GDPR, é necessário mais do que a mera presença física dentro do território europeu. E quando não houver presença física, é necessário mais do que o simples processamento de dados de modo aleatório. Em síntese, é preciso que o processamento se dê dentro do contexto das atividades de um estabelecimento.

Em alusão ao conceito de estabelecimento (*establishment),* pondera-se que a GDPR não o conferiu uma definição clara. Não obstante, o considerando nº 22 (*recital),* servindo meramente como instrumento de interpretação do texto legal e sem qualquer

[8] The General Data Protection Regulation. Disponível em: https://eur-lex.europa.eu/eli/reg/2016/679/oj. Acesso em: 28 de maio de 2020.
[9] Article 3(1): This Regulation applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not. Disponível em: https://eur-lex.europa.eu/eli/reg/2016/679/oj. Acesso em 08 de jun. de 2020.

força vinculante, expressou que o estabelecimento "implica no real e efetivo exercício de atividades através de instrumentações estáveis"[10].

Em casos recentes julgamentos sobre a liberdade de estabelecimento, o Tribunal de Justiça da União Europeia - TJUE tem considerado estabelecimento como sendo "ambas fontes humanas, e técnicas, que são necessárias para a provisão de serviços privados que estão permanentemente disponíveis" (VERMEULEN; LIEVENS. 2017, p. 80). Já quanto ao contexto de proteção de dados, o conceito de estabelecimento tem recebido uma ampla interpretação.

Ainda sob a regência da *Directive*, no *Weltimmo Case*[11] (*CJEU. Weltimmo s.r.o. v Nemzeti Adatvédelmi, 2014)*, um processo entre uma empresa localizada na Eslováquia e as autoridades de proteção de dados Húngaras, o TJUE expressou no julgamento uma interpretação mais flexível, não se apegando às formalidades.

Entendeu-se que o conceito de estabelecimento se estende para toda e qualquer atividade real e efetiva, até mesmo as menores, exercidas através de arranjos estáveis[12],

[10] "Establishment implies the effective and real exercise of activity through stable arrangements. The legal form of such arrangements, whether through a branch or a subsidiary with a legal personality, is not the determining factor in that respect.". Recital 22 of The General Data Protection Regulation. Disponível em: https://eur-lex.europa.eu/eli/reg/2016/679/oj. Acesso em: 28 de maio de 2020.

[11] The request has been made in proceedings between Weltimmo s. r. o. ('Weltimmo'), a company which has its registered office in Slovakia, and the Nemzeti Adatvédelmi és Információszabadság Hatóság (the national authority for data protection and freedom of information; 'the Hungarian data protection authority') concerning a fine imposed by the latter for infringement of Law CXII of 2011 on the right to self-determination as regards information and freedom of information (az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény; 'the Law on information'), which transposed Directive 95/46 into Hungarian law. Disponível em: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62014CJ0230. Acesso em 28 de maio de 2020.

[12] "Article 4(1)(a) of Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data must be interpreted as permitting the application of the law on the protection of personal data of a Member State other than the Member State in which the controller with respect to the processing of those data is registered, in so far as that controller exercises, through stable arrangements in the territory of that Member State, a real and effective activity — even a minimal one — in the context of which that processing is carried out." Court of Justice of the European Union. Disponível em:

não mencionando ser necessário haver, de modo estrito, os recursos humanos ou técnicos disponíveis citados pelo considerando 22.

Sob este ângulo, o Tribunal também se manifestou sobre o que poderia constituir um arranjo estável e uma atividade efetiva e real. O entendimento foi que a análise do que é um arranjo estável poderia ser feita de acordo com o caso concreto, avaliando a natureza do produto ou serviço que é prestado pela empresa, organização, indivíduo ou agência. Assim, seria levado em consideração o grau mínimo de estabilidade para cada caso.

Ademais, não se pode negar que, em virtude da natureza dos serviços que são oferecidos apenas por meio virtual, é possível, em certas circunstâncias, que a presença de um único representante possa bastar para constituir um arranjo estável, à medida em que este representante atue com um certo grau de estabilidade, valendo-se de equipamento mínimo necessário para o oferecimento de determinado serviço[13].

Portanto, o conceito de estabelecimento pode ser sintetizado como sendo atividades padrões e efetivas, pois são essenciais à prestação do serviço ou disponibilização do produto, exercidas através de arranjos estáveis, como equipamentos, elementos técnicos ou estrutura física para o alcance do consumidor ou destinatário do serviço.

Em sequência, o conceito de "no contexto das atividades" (*in the context of the activities)* está diretamente ligado ao de estabelecimento. Este conceito predica, de modo precípuo, que a mera presença no território da União, sem nenhuma relação com

https://eurlex.europa.eu/legalcontent/EN/TXT/?uri=CELEX%3A62014CJ0230. Acesso em 28 de maio de 2020.

[13] Weltimmo, CJEU, paragraph 30, 2014. Disponível em: https://eurlex.europa.eu/legalcontent/EN/ALL/?uri=CELEX%3A62014CJ0230. Acesso em 28 de maio de 2020.

Cadernos Eletrônicos Direito Internacional sem Fronteiras, Vol. 2, Núm. 1, Jan-Jun 2020, e:11

as atividades que visam o consumidor europeu, não é suficiente para render a aplicação da GDPR.

Conforme expressa o texto legal, o processamento precisa ser feito no contexto das atividades de um estabelecimento. A partir da análise conjunta dos julgados do Tribunal Europeu nos casos da *Google Spain, Weltimmo,* e *Verein für Konsumenteninformatio* (VERMEULEN; LIEVENS. 2017, p 78) - todos os três casos ainda sob a regência da *Directive* -, tem-se uma compreensão mais profunda sobre o tema.

No *Google Spain Case (CJEU. Google Spain v AEPD, Mario Gonzalez, 2014*)[14], o Tribunal foi solicitado para determinar se as atividades das ferramentas de busca do *Google Inc.* poderiam ser vistas como enquadradas dentro do conceito de "no contexto das atividades" do estabelecimento de uma de suas subsidiárias, a *Google Spain SL*. Inicialmente, o resultado da apreciação do juízo europeu foi que, para se estar no contexto das atividades, não é necessário que o estabelecimento esteja ativamente envolvido, engajado no processamento[15].

Isto é, clarifica-se aqui que nem sempre no estabelecimento se encontra o operador direto (processador ou controlador) do processamento. E, não obstante os dois elementos não se confundam, suas atividades se comunicam. Por conseguinte, não importando o engajamento real ou não, as atividades do operador estão

[14] "The request has been made in proceedings between, on the one hand, Google Spain SL ('Google Spain') and Google Inc. and, on the other, the Agencia Española de Protección de Datos (Spanish Data Protection Agency; 'the AEPD') and Mr Costeja González concerning a decision by the AEPD upholding the complaint lodged by Mr Costeja González against those two companies and ordering Google Inc. to adopt the measures necessary to withdraw personal data relating to Mr Costeja González from its index and to prevent access to the data in the future". Court of Justice of European Union. Disponível em: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62012CJ0131. Acesso em: 29 de maio de 2020.

[15] Case C-131/12 Google Spain SL, Google Inc. v Agencia Española de Protección de Datos (AEPD), Mario Costeja González EU:C:2014:317, paragraph 52 (hereafter: "Google Spain").

intrinsecamente ligadas ao estabelecimento[16], não havendo, portanto, como dissociá-las no que tange a natureza do serviço.

Com sedimento nessas considerações, o Tribunal concluiu que o processamento de dados pessoais é feito no contexto das atividades de um estabelecimento quando "o operador da ferramenta de busca firmar uma empresa em um Estado Membro, de apoio ou subsidiária, com a intenção de promover e vender um espaço de anúncios e propagandas oferecidos por aquela ferramenta, e que orienta sua atividade em direção aos habitantes daquele Estado Membro"[17].

Em nova referência, no *Weltimmo Case,* o entendimento seguiu a mesma lógica do caso anterior. O caso envolvia uma empresa administradora de sites de negociação imobiliária que era formalmente registrada na Eslováquia, mas fazia anúncios e propagandas de imóveis localizados na Hungria[18], o que consequentemente levava à operação de dados de nacionais Húngaros.

Assim, em um determinado momento, a Agência de Proteção de Dados Húngara foi acionada para investigar tal atividade, recebendo, em resposta da empresa *Weltimmo*, a alegação de que a Agência não era competente para fazê-lo e que, nesse caso, a lei Húngara não poderia ser aplicada à uma empresa de prestação de serviços localizada em outro estado membro. [19]

Estabelecida a querela judicial, ao ser demandado para julgar se no caso em epígrafe o processamento se dava no contexto das atividades de um estabelecimento, isto é, se é que havia estabelecimento, o Tribunal seguiu o entendimento positivo de

[16] Google Spain. Paragraph 56.
[17] Google Spain. Paragraph 60.
[18] Weltimmo. Paragraph 9.
[19] Weltimmo. Paragraph 12.

que havia, à medida em que atividade em pauta era diretamente destinada àquele Estado Membro específico.

Também foi levado em consideração o fato de que havia um representante no país que respondia em nome da empresa quanto à assuntos jurídicos, fiscais e administrativos. Portanto, o processamento por parte da empresa foi enquadrado no contexto das atividades do estabelecimento. [20]

Por fim, no *Verein für Konsumenteninformation Case (CJEU, Verein für Konsumenteninformation v Commission of the European Communities, 2005)*[21], o Tribunal foi questionado sobre se o processamento de dados resultante das atividades exercidas pela *Amazon EU* deveria estar em conformidade com a lei de cada país membro do bloco aos quais suas atividades eram direcionadas. Assim, embora a empresa tivesse seus escritórios centrais no Luxemburgo, o pretório europeu decidiu pela interpretação de que as atividades da Amazon deveriam se adequar à legislação de cada estado membro à que dirigia seus escopos comerciais.[22]

Portanto, baseando-se nas interpretações acima expostas, é concluso que a ideia de 'no contexto das atividades' faz referência às práticas primeiras, indispensáveis para a disponibilização de serviço ou produto, e, de modo correlato, o conceito de estabelecimento afigura-se, em síntese, como os insumos, materiais ou técnicos, básicos para o suporte de determinada atividade ou serviço.

Ainda, a avaliação da destinação intencional à determinado país está totalmente atrelada ao enquadramento do processamento dentro desses conceitos apresentados.

[20] Weltimmo. Paragraph 41.
[21] ECLI identifier: ECLI:EU: T: 2005:125. Judgment of the Court of First Instance (First Chamber, extended composition) of 13 April 2005. Verein für Konsumenteninformation v Commission of the European Communities. Disponível em: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62003TJ0002. Acesso em 29 de maio de 2020.
[22] Verein für Konsumenteninformation. Paragraph 81.

Pois pressupõe-se que, para haver a reprodução das práticas comerciais visando determinada região, é preciso ter o mínimo de suporte técnico e representatividade naquele lugar.

Ademais, cumpre destacar que, embora as interpretações dos casos arrolados tenham sido sob a vigência da *Directive*, elas preservam o seu valor, uma vez que ainda não existem precedentes jurídicos que se deleitem sobre essas definições sob o império da GDPR. Ainda, entende-se que os conceitos são comuns à ambos os textos legais, tendo sido modificado apenas a maneira como foram dispostos na legislação, a fim de se construir o referido escopo extraterritorial.

3.1.2 Artigo 3(2): conceitos de *"offering goods and services"* e *"the monitoring of behaviour"*

O artigo 3(2) da GDPR trata da previsão do processamento de dados de pessoas que estão na União, quando for relacionado ao oferecimento de produtos e serviços ou ao monitoramento de comportamento. Cita-se o texto legal:

> Artigo 3(2): Este Regulamento aplica-se ao processamento de dados pessoais de indivíduo que estão na União [Europeia] por um controlador ou processador não estabelecido na União, onde as atividades de processamento são relacionadas: a) à oferta de produtos ou serviços, independentemente de ser requerido um pagamento do titular dos dados, a esses titulares na União; ou b) ao monitoramento do comportamento dos titulares desde que comportamento ocorra dentro da União (tradução nossa).[23]

Destaca-se que o artigo 3(2) aplica-se tão somente ao processamento de dados pessoais de indivíduos que estão dentro do território do bloco europeu. E ainda, a mera

[23] Article 3(2). This Regulation applies to the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union, where the processing activities are related to: a) the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union; or b) the monitoring of their behavior as far as their behavior takes place within the Union. Disponível em: https://eur-lex.europa.eu/eli/reg/2016/679/oj. Acesso em 08 de jun. de 2020.

acessibilidade ao site da organização, empresa ou agência não pode se encaixar nessa previsão (VERMEULEN; LIEVENS. 2017, p 85). Isto posto, o centro da análise recai sobre os conceitos de oferecimento de produtos e serviços, e monitoramento de comportamento – quando este for dentro da União.

O considerando 23 da GDPR esclarece que a caracterização do oferecimento de produtos e serviços será constatada quando o processador ou controlador personaliza o acesso à sua rede virtual de acordo com o país do indivíduo que está acessando, como por exemplo, a utilização do idioma ou moeda oficiais daquele país membro.

Assim, a especificação do idioma e da moeda de pagamento de modo personalizado de acordo com a nacionalidade dos indivíduos que estão acessando não é apenas suficiente, como também é o fator que comprova a intencionalidade do titular do produto ou serviço de oferece-lo naquele determinado país[24].

Analisando como se daria a aplicação da GDPR dentro da dinâmica do oferecimento de produtos e serviços, cita-se o exemplo de uma entidade localizada fora da União Europeia, que oferece produtos dentro dos países membros do bloco (VOIGT, 2017, p. 27. Tradução nossa):

> Empresa H, localizada na Austrália. Tem como serviço principal vendas online. A empresa não tem nenhuma filial ou representantes no exterior e as compras online estão disponíveis apenas em inglês. H armazena dados pessoais dos consumidores. O pagamento dos produtos pode ser feito em dólares australianos ou em euros, e são possíveis entregas para a Alemanha, França e Itália. Se os consumidores desses países membros da EU entrarem no site da empresa H, eles serão redirecionados da página de domínio "H.au." para outra página na web com o domínio "H.com/de", "H.com/fr" e assim por diante, de acordo com cada país. Nesse exemplo, fatores como: a separação dos nomes do domínio dos sites para consumidores europeus, a possibilidade de o pagamento das compras ser em euro e a disponibilidade de entrega para certos países membros do bloco nos

[24] Recital 23 of the GDPR.

> permitem concluir que a empresa H tem os consumidores que habitam na União como destinatários dos seus produtos. Portanto, nesses casos a GDPR é aplicável.

Em face desse exemplo, fica claro como se dão os caminhos para o oferecimento por parte do fornecedor. A situação apresentada ainda responde ao possível questionamento sobre quem poderia estar visando quem, em caso de o próprio consumidor estar em busca de um determinado site. Como já posto, a personalização da acessibilidade é um fator que comprova torna a intencionalidade aparente, perceptível[25].

Em sequência, o considerando 24, ao mencionar ao monitoramento de comportamento, é de grande auxílio na interpretação da Lei. Descreve que quando o processador ou controlador não se valer de estabelecimento na União (ausente a caraterização do artigo 3(1)), a GDPR será aplicada quando no processamento houver monitoramento de comportamento, sendo imprescindível que o comportamento se dê dentro da União.

Nesta perspectiva, o monitoramento de comportamento consiste principalmente no rastreamento dos indivíduos e na criação de perfil a partir dos dados coletados, de moto a caracterizar gostos pessoais, e prever possíveis preferências, comportamentos e atitudes[26]. Cita-se o exemplo de um cidadão europeu que sai em viagem aos Estados Unidos por alguns dias. Durante o tempo de sua viagem, esse cidadão não estará acobertado pela GDPR, uma vez que o seu comportamento não se dá dentro da União Europeia (VOIGT, 2017, p. 29).

4 PRINCÍPIOS E COSTUMES DE JURISDIÇÃO INTERNACIONAL

[25] The Challenges Faced by the Extraterritorial Scope of the General Data Protection Regulation. Disponível em: https://www.jipitec.eu/issues/jipitec-9-2-2018/4723. Acesso em 21 de maio de 2020.
[26] Recital 24 of the GDPR.

Diante do exposto, tonou-se evidente a intenção do Parlamento Europeu de ter um alcance extraterritorial como nunca antes visto no âmbito jurídico da sociedade internacional. Então, a partir dessa reivindicação transfronteiriça, a harmonização da extraterritorialidade da lei europeia com os standards do Direito Internacional é entendida com base em ao menos 5 princípios gerais de jurisdição internacional (VERMEULEN; LIEVENS. 2017, p. 90).

São eles: princípio da territorialidade (objetiva e subjetiva); princípio da nacionalidade (ativa ou passiva); princípio (ou doutrina) dos efeitos; princípio protetor e princípio da universalidade. Notadamente, o princípio da territorialidade figura como o mais relevante na presente questão.

No que tange a jurisdição internacional, existem duas grandes correntes de abordagem que permeiam a matéria. A primeira diz respeito à uma jurisdição permissiva, na qual os países podem exercer sua jurisdição deliberadamente sobre outros países, sendo impedidos apenas se houver disposição internacional que proíba.

A segunda, e mais difundida e aceita pela doutrina e pelas cortes internacionais, dispõe sobre um exercício jurisdicional restritivo, proibitivo, na qual um país não pode exercer seu poderio sobre outro, a menos que haja regulação que assim o permita. Esta última abordagem tem como corolário os princípios da soberania estatal e da não intervenção, os maiores pilares de jurisdição internacional.

No cerne da segunda abordagem encontra-se o princípio da territorialidade, o princípio mais básico de jurisdição internacional (RYNGAERT, 2015, p. 49). Consiste na determinação do exercício jurisdicional tendo como referência o lugar onde o crime foi praticado. Denota que um estado tem jurisdição sobre as condutas que ocorrem dentro das suas fronteiras (LEE, 2018, p. 181).

Cadernos Eletrônicos Direito Internacional sem Fronteiras, Vol. 2, Núm. 1, Jan-Jun 2020, e:11

Este princípio dispõe do teu tipo subjetivo, no qual a conduta ocorre totalmente dentro do território do estado, ou começou nele, mas foi completada ou consumada em um outro estado; e objetivo, no qual a conduta ocorre parcialmente em estado A e parcialmente em estado B.

Nesse sentido, a partir da valorização do poder territorial estrito às fronteiras nacionais, observa-se que o princípio da territorialidade é uma forte reprodução jurídica dos princípios da soberania, que predica que cada estado exerce seu poder sobre o seu próprio território, e da não-intervenção, significando que a regra de máxima de convivência da sociedade internacional é a não intervenção de um estado nos assuntos e negócios de um outro estado.

Assim, desde já se infere que a GDPR não retira seus fundamentos do princípio da territorialidade. Primeiro pois, à medida em que o mundo torna-se mais e mais globalizado, passa-se da ênfase da territorialidade ao reconhecimento da interdependência jurídica entre os estados, apesar na noção territorial (ACCIOLY, 2019, p. 529); e segundo, pois, dada a natureza desterritorializada da internet, essa abordagem estritamente territorial torna-se cada vez mais problemática (RYNGAERT, 2015, p. 49).

Por sua vez, o princípio da nacionalidade ou da personalidade diz respeito à possibilidade de um determinado estado exercer jurisdição sobre condutas praticadas por seus nacionais fora das suas fronteiras, e, em alguns casos, até sobre condutas dos seus residentes não nacionais. Manifesta-se em duas modalidades, a ativa e a passiva. A primeira ocorre quando um estado reivindica a persecução de uma conduta na qual o autor da conduta é seu nacional; e a segunda, ao contrário, quando o nacional é a vítima, e não o infrator.

Cadernos Eletrônicos Direito Internacional sem Fronteiras, Vol. 2, Núm. 1, Jan-Jun 2020, e:11

A doutrina ou princípio do efeito predica que um estado pode reivindicar jurisdição sobre uma conduta que foi praticada fora do seu território, mas os efeitos recaem sobre esse estado e são sentidos dentro do seu território. Os propósitos desse princípio não são consolidados no seio internacional, figurando cada vez mais como uma questão controversa e litigiosa, considerando que em um mundo globalizado as atitudes e condutas dos estados e dos indivíduos facilmente podem gerar efeitos em outras localidades, tanto no âmbito político, econômico e jurídico, quanto no geográfico.

Em sequência, o princípio protetor predica que um estado A poderá buscar a persecução de uma conduta feita por um estado B que ponha em risco os seus interesses nacionais, como segurança nacional, estabilidade política do governo, integridade ou soberania. Nota-se que tal princípio também pode ser invocado ainda que haja uma divergência entre os estados em relação à consideração da legalidade da conduta.

Por fim, o princípio da universalidade consiste na prerrogativa de um estado exercer jurisdição sobre atos que ponham em risco questões de importância internacional, como a paz e segurança internacionais, independentemente da nacionalidade dos autores. Está sedimentado nos bens juridicamente tutelados pela sociedade internacional que, quanto postos em risco por condutas criminosas, qualquer estado está autorizado a aceder à persecução criminal.

Nesta perspectiva, não se pode absolutamente afirmar sobre qual princípio ou substrato jurídico específico a GDPR está consolidada. Ao contrário, a sua aplicação se dará em maior medida como resultado a análise conjunta de todos eles (LEE, 2018, p. 209).

Cadernos Eletrônicos Direito Internacional sem Fronteiras, Vol. 2, Núm. 1, Jan-Jun 2020, e:11

Paralelamente, em termos de força executória, não é possível traçar uma cartilha unânime, uma vez que a comissão europeia não estabeleceu o trâmite sequencial para a aplicação de sanções, tema obscuro até o presente momento em razão da inexistência de precedentes jurídicos dessa natureza.

Isso poderia resultar em conflitos quando ocorrer infrações no processamento de dados, considerando que quando a aplicação extraterritorial for juridicamente e moralmente justificável, é arriscado que a empresa ou organização alvo a ignore alegando falta de legitimidade (SVANTENSSON, 2015, P. 233).

Entretanto, neste cenário de incerteza, a cooperação jurídica internacional tornar-se cada vez mais presente no Direito. Embora a GDPR represente também uma grande inovação legislativa quanto à aplicação extraterritorial, esta não figura como única. Nota-se que a produção de leis de proteção de dados que têm um escopo transnacional por parte dos estados é cada vez maior em todo o mundo (GREENLEAF, 2014, p. 07), em resposta à necessidade urgente de adequação ao ambiente virtual (AZZI, 2018, online).

Então, não como uma solução para todos os problemas sobre o tema, mas como uma solução em grande medida eficaz, a cooperação internacional não visa a harmonização das leis entre os estados, mas o reconhecimento das reivindicações jurisdicionais de um estado por outro, de modo que as decisões daquele que reivindica sejam deferidas perante os atores internacionais (LEE, 2018, 195). Com uma cooperação bem coordenada, seria possível evitar conflitos de jurisdição.

5 CONSIDERAÇÕES FINAIS

Diante do exposto, nota-se que a questão em epígrafe tem raízes muito mais profundas, e que remetem a questões minuciosas de Direito Internacional Público,

Cadernos Eletrônicos Direito Internacional sem Fronteiras, Vol. 2, Núm. 1, Jan-Jun 2020, e:11

notadamente no que diz respeito à Jurisdição Internacional e Executoriedade Extraterritorial.

De acordo com os princípios anteriormente citados, conclui-se que o Regulamento Geral de Proteção de Dados não se adequa ao princípio da territorialidade. Ao contrário, pode-se dizer que escopo extraterritorial, objeto deste estudo, operou uma total desvinculação com tal princípio. Ademais, tornou-se nítido que a GDPR está sedimentada principalmente no princípio da nacionalidade passiva, à medida em que o legislador europeu almejou conferir total proteção aos seus nacionais, reivindicando, portanto, o exercício jurisdicional quando estes são lesados quanto aos seus dados pessoais.

Ainda, a partir das diretrizes da GDPR ora expostas, conclui-se também que o legislador europeu muito deixou a desejar quanto à execução normativa, uma vez que não estabeleceu parâmetros procedimentais de aplicação extraterritorial, o que coloca em xeque a força executória do Regulamento em face dos sujeitos que dela são alvos. Tal obscuridade de aplicação faz com que a sua legitimidade seja facilmente questionada e tão logo não respeitada, pois carece de meios coercitivos para a persecução dos seus objetivos.

Ao mesmo tempo, em face destes problemas de executoriedade, a cooperação internacional emerge como a melhor solução para a questão, à medida em que promove uma maior efetividade na solução dos litígios internacionais por meio do reconhecimento das reivindicações de um país por outro, se sobressaindo ao apego às normas internacionais. E ainda, uma vez que as legislações de proteção de dados no mundo seguem cada vez mais uma tendência de alcance extraterritorial, a cooperação internacional figura como o fator do qual todas as normas dependem para uma efetiva aplicação e consequente execução por parte de seus destinatários.

Cadernos Eletrônicos Direito Internacional sem Fronteiras, Vol. 2, Núm. 1, Jan-Jun 2020, e:11

REFERÊNCIAS

ACCIOLY, Hildebrando; et al. **Manual de Direito Internacional Público.** São Paulo. Saraiva Educação. 24 ed. 2019, 968 p.

AZZI, Adèle. **The Challenges Faced by the Extraterritorial Scope of the General Data Protection**. Disponível em: <https://www.jipitec.eu/issues/jipitec-9-2-2018/4723>. Acesso em 08 de jun. de 2020.

CASTELLS, Manuel; CARDOSO, Gustavo. **The Network Society: From the Knowledge to Policy**. Washington, DC. Johns Hopkins Center for Transatlantic Relations, 2005, 80 p.

CASTELLS, Manuel. **End of Millennium.** Oxford. Blackwell Publishing. 2010, 489 p.

CUSTERS, Bart; et al. **EU Personal Data Protection in Policy and Practice.** Berlin. Asser Press, 2019, 257 p.

DENLEY, Andrew; et al. **GDPR: How to Achieve and Maintain Compliance.** New York. Routledge Publishing. 2018, 257 p.

DIBBLE, Suzanne. **GDPR for Dummies.** New Jersey. John Wiley & Sons, Inc. 2020, 464 p.

GREENLEAF, Graham. **Asian Data Privacy Laws: Trade and Human Rights Perspectives.** Oxford. Oxford University Press, 2014.

LEENES, Ronald; et al. **European Data Protection: In Good Health?** New York. Springer Publishing. 2012, 368 p.

LEE, Sangwoo. **A Study on the Extraterritorial Application of the General Data Protection Regulation with a Focus on Computing.** PHD Dissertation. (Phd in International Law). China University of Political Science and Law. Beijing. 2018, 539 p.

MONTI, Andrea; WACKS, Raymond. **Protecting Personal Information: The Right to Privacy Reconsidered.** Ebook. Londres. Editora Bloomsbury Publisher, 2019, 204 p.

PINHEIRO, Patríci Peck. **Proteção de Dados Pessoais: comentários à Lei nº 13.709/2018 (LGPD).** São Paulo. Saraiva Educação, 2018.

RYNGAERT, Cedric. **Jurisdiction in International Law.** Oxford. Oxford University Press. 2 ed, 2015, 245 p.

SOLOVE, Daniel J; SCHWARTZ, Paul M. **Information Privacy Law.** Ebook. 6ed. Nova Iorque. Editora Wolters Kluwer, 2018, 1254 p.

SVANTESSON, Dan Jerker B. **Extraterritoriality and targeting in EU data privacy law: the weak sport undermining the regulation**. Copenhagen. International Data Privacy Law, 2015.

VERMEULEN, Gert; LIEVENS, Eva. **Data Protection and Privacy under Pressure.** Antwerp. Maklu Publishing. 2017, 341 p.

VOIGT, Paul; BUSSCHE, Axel Von Dem. **The EU General Data Protection Regulation (GDPR) - A Practical Guide.** Ebook. Gewerbestrasse. Ed. Springer, 2017, 385 p.